UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Colonnes dans les automates cellulaires et suites généralisées de Rudin–Shapiro

THÈSE

présentée et soutenue publiquement le 17 décembre 2020

pour l'obtention du

Doctorat de l'Université de Lorraine

(mention mathématiques)

par

Pierre-Adrien Tahay

Composition du jury

Président :	Emmanuel Jeandel	Professeur, Université de Lorraine
Rapporteurs :	Jean-Paul Allouche	Directeur de recherche émérite, CNRS et Sorbonne Université
	Mathieu Sablik	Professeur, Université Toulouse III - Paul Sabatier
Examinateurs :	Nathalie Aubrun	Chargée de recherche, CNRS et Université Paris-Saclay
	Cécile Dartyge	Maîtresse de conférences, Université de Lorraine
	Élise Janvresse	Professeure, Université de Picardie - Jules Verne
Encadrants :	Irène Marcovici	Maîtresse de conférences, Université de Lorraine
	Thomas Stoll	Professeur, Université de Lorraine

Institut Élie Cartan de Lorraine (IECL) — UMR 7502

Mis en page avec la classe thesul.

Je dédie cette thèse à Geneviève Bedel (1948-2021).
"Les grandes choses prennent racine et puisent leur force sur des commencements de petite apparence."

Remerciements

Cette thèse représente un peu plus de trois années de ma vie. Aussi, j'aimerais remercier toutes les personnes qui d'une manière ou d'une autre, ont permis l'aboutissement de ce travail et ont rendu cette période aussi agréable.

Tout d'abord, mes remerciements vont à Irène et Thomas, sans qui tout ceci n'aurait jamais vu le jour. Je me revois, il y a presque quatre ans maintenant, à la recherche d'un stage pour mon M2 recherche. Je suis allé frapper à la porte du bureau de Thomas, par une après-midi grisonnante de janvier dont nous avons l'habitude en Lorraine. Le sujet de stage que tu m'as proposé, en collaboration avec Irène, m'a tout de suite plu. Pendant quatre mois, ce fut un plaisir de travailler avec vous deux, et de découvrir le monde de la recherche avec de belles mathématiques que je ne connaissais pas. Puis nous avons eu la possibilité de poursuivre le stage par une thèse, et nous voilà à la fin de celle-ci désormais. Un grand merci à vous deux, pour votre encadrement de près de quatre ans, pour votre bienveillance, votre patience, vos précieux conseils, votre grande disponibilité et tout ce que vous m'avez apporté au cours de ces années.

Je tiens à remercier également la région Grand Est, l'ANR Mudera et l'ANR Graal, pour avoir financé ces trois années de recherche.

J'aimerais aussi remercier tous les membres de mon jury, pour avoir porté de l'intérêt à mes travaux. Tout d'abord mes rapporteurs, Jean-Paul Allouche et Mathieu Sablik, qui m'ont permis d'améliorer la qualité de ce manuscrit grâce à leurs nombreuses remarques et suggestions pertinentes. Merci également à Nathalie Aubrun, Cécile Dartyge, Élise Janvresse, et Emmanuel Jeandel d'avoir accepté d'être dans mon jury. J'ai une pensée particulière pour Cécile et Emmanuel qui ont fait partie de mes comités de suivi de thèse, et suivent donc l'avancée de mes travaux depuis la première année.

J'ai la particularité d'avoir effectué tout mon cursus universitaire à Nancy, depuis ma première année de licence, dans la classe préparatoire universitaire (CPU), en 2011. Par conséquent, bon nombre de mes collègues de l'IECL ont d'abord été mes enseignants.

J'aimerais commencer par remercier Lionel Bérard-Bergery, qui nous a quittés l'année dernière, et qui est le premier à m'avoir parlé de la CPU. J'ai une pensée particulière pour Didier Schmitt, qui fut déterminant dans mon choix d'intégrer la CPU qui m'a permis de rebondir après une période difficile. Je remercie ensuite tous les enseignants qui m'ont donné le goût pour les mathématiques. Ne pouvant garantir que la liste est exhaustive, je présente toutes mes excuses aux personnes que je risque éventuellement d'oublier. Merci à Wolfgang Bertram, François Chargois, Benoît Daniel, Cécile Dartyge, Anne de Roton, David Dos Santos Ferreira, Bruno Duchesne, Olivier Garet, Françoise Geandier, Anne Gégout-Petit, Jean-Sébastien Giet, Jean-François Grosjean, Khalid Koufany, Anna Kowalska-Chassaing, Aline Kurtzmann, Vladimir Latocha, Manfred Madritsch, Régine Marchand, Julien Maubon, Séraphin Mefire, Damien Mégy, Frédéric Robert, Gérald Tenenbaum, Matei Toma, Jean-François Weisse. Je ne peux m'empêcher de terminer la liste par mon professeur de mathématiques du lycée, Hervé Lecompte, qui est pour beaucoup dans mon choix de poursuivre mes études dans cette discipline.

Je souhaite aussi remercier les personnes avec qui j'ai effectué des enseignements, et qui m'ont permis de les faire dans de bonnes conditions. Des personnes déjà citées précédemment, Aline, Damien et Irène, et d'autres dont j'ai fait la connaissance à cette occasion, Damian Brotbek, Angelo Koudou et Sophie Mézières ainsi qu'Imene Djebour qui soutient sa thèse le même jour que moi.

Un grand merci également à Nathalie Benito, Élodie Cunat, Laurence Quirot et Paola Schneider qui sont toujours là pour nous aider dans les démarches administratives et logistiques, et permettent ainsi le bon fonctionnement de ce laboratoire avec des conditions de travail agréables.

Je tiens maintenant à remercier toutes les personnes avec qui j'ai pu créer des liens pendant mes années de doctorat, en commençant par mes deux co-bureaux, également théoriciens des nombres. D'abord Johann qui me suit dans cette aventure depuis la première année de licence en CPU et qui a soutenu sa thèse quelques semaines plus tôt, et Pierre avec qui je me suis tout de suite bien entendu. Une pensée particulière pour Rodolphe dans le bureau juste en face et que je pourrais presque considérer comme un troisième co-bureau. Ensuite je tiens à remercier Vincent, qui a en commun d'avoir fait la CPU et d'avoir

eu Hervé Lecompte comme professeur au lycée, et avec qui il est toujours très agréable de se remémorer nos souvenirs respectifs de ces périodes. Merci également à Robin pour les nombreuses pauses cafés que nous avons prises dans son bureau, à Clémence pour sa bonne humeur et sa gentillesse, à Éloïse pour ses bons mots et ses analyses pertinentes, à Ibtissem pour les nombreuses pauses toujours très agréables que nous avons pu partager, à Simon que j'ai connu en master et dont j'apprécie toujours les discussions, le Bon Temps avec Valentin, Paul et Gabriel autour d'une bonne bière, ou parfois directement chez eux, les connaissances de Rémi Peyre sur des sujets très variés qui permettent des échanges enrichissants. Un merci particulier à Coralie, pour ses précieux conseils, son soutien infaillible, sa joie de vivre, sa grande capacité d'écoute et tout ce que tu as pu m'apporter. De manière générale, merci à toutes les personnes que j'ai rencontrées pendant ma thèse, Dimitry, Matthieu, Florian, David, Jérémy, Benjamin, Rémi Côme, Philippe, Ulysse, Édouard, Christophe, Nicolas, Jocelyn, Thomas, Charles, Hassan, Nassim, Tom, Youssef, Iury, Marco, Zhiwei...

Sur un plan personnel, j'aimerais remercier le père Guy, pour tous les échanges et les réflexions que nous avons pu avoir, notamment dans les périodes difficiles. Merci au groupe des jeunes pros que vous m'avez fait découvrir et qui fut l'occasion de partager des moments conviviaux sur des sujets divers toujours très intéressants.

Merci aux musiciens de la Bandabera pour nos moments musicaux, nos concerts et tout ce que notre groupe m'a apporté depuis que j'ai la chance d'en faire partie. Merci à Claire, Hélène, Bernard, Mathilde, Monika, Anne, Marie-Christine, Serge, Frédéric, Caroline et Axel. Une pensée pour Annette qui nous a accompagné pendant longtemps mais qui a été contrainte de s'arrêter. De même pour Véronique, François et Annie qui sont partis vers d'autres horizons. Enfin, j'ai une pensée toute particulière pour notre chef, Alain Bérat, sans qui rien ne serait possible. Alain, depuis plus de 20 ans maintenant j'ai la chance de faire de la musique à tes côtés. Tu fais partie des enseignants qui ont eu un impact majeur dans ma scolarité et mon cursus universitaire. Tu m'as appris la rigueur, le travail, la patience, la persévérance et le goût pour la bonne musique. Je n'en serais probablement pas là si je n'avais pas croisé ta route, alors pour tout ceci, un immense merci à toi Alain.

Je remercie mes amis qui m'accompagnent pour certains depuis plus de 20 ans maintenant. Mention spéciale pour le groupe CPU avec qui j'ai fait une bonne partie de mes études, en particulier Johann qui a poursuivi jusqu'en thèse avec moi, mais aussi Joël, Arthur, Daniel, Nour, Manon, Mathilde, Claire, Florian, Gautier, Richard, Primaël. Merci à Séréna et Audrey, issues d'une autre génération de CPU, et peut-être bientôt d'une future génération de doctorants. Merci aussi à Aurore, qui fait également partie des anciens étudiants en mathématiques de Nancy dont c'est toujours un plaisir d'avoir des nouvelles.

Un grand merci à Maxime, Élise, Joris, Célia, Jean-François, Élodie, Maxence, Laurie-Anne, Julien, Jade, Mélanie, Thomas, Jérémy, Justine et leur petit Gaëtan. C'est toujours un plaisir de se retrouver.

Mes derniers remerciements sont pour les membres de ma famille. Je pense à mes sœurs, Amélie, Camille et Constance avec qui j'ai eu la chance de vivre en colocation à tour de rôle pendant mes études à Nancy jusqu'au début de mon doctorat. Vous avez largement contribué à rendre ces années très agréables. Merci à mon beau-frère Christophe, toujours là pour un trait d'humour ou un bon mot. Merci à mes grands-parents, Jean-Claude, Jeannine, Jean-Marie et Sophoeun (ma grand-mère de cœur), que j'ai beaucoup de chance d'avoir. Une pensée pour ma grand-mère Marie-Pierre, partie bien trop tôt pour que je puisse réellement la connaître. Et enfin, merci à ma nièce, Coline, qui fait le bonheur de toute la famille depuis un peu plus de quatre mois maintenant.

Enfin, je tiens à remercier mes parents, Hélène et Jean-Pierre, pour le soutien sans faille que vous m'avez apporté sur tous les plans depuis toujours. Merci pour l'éducation que j'ai reçue de votre part, pour les valeurs que vous m'avez transmises et un certain goût pour les mathématiques que je dois probablement à mon côté paternel. Merci à vous deux de m'avoir permis de devenir l'homme que je suis. Cette thèse n'aurait jamais existé sans vous. Merci pour tout.

Table des matières

Table des figures

Introduction

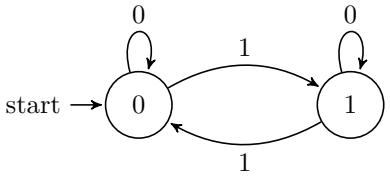
La théorie des automates est un vaste sujet qui s'est développé au cours du XXème siècle. Initialement, des logiciens tels que Gödel ou Turing souhaitaient formaliser la notion de calcul et de machine. Cela a permis l'émergence de l'informatique, qui occupe aujourd'hui une place importante dans la recherche en mathématiques. Ces dernières décennies, de nombreux travaux utilisant des méthodes diverses, notamment combinatoires et algébriques, ont permis de constituer une littérature importante sur les différents types d'automates qui existent.

Dans cette thèse nous nous intéresserons d'une part à l'étude des automates finis et des suites automatiques qui en découlent, et d'autre part aux automates cellulaires. Nous verrons qu'il est possible de relier ces deux types d'automates de manière très concrète.

Automates finis, suites automatiques

Un automate fini consiste à se donner une machine à qui l'on donne en entrée un nombre fini de symboles pris dans un ensemble fini que l'on s'est fixé au départ et qui après lecture de chaque symbole l'un après l'autre, exécute des instructions et renvoie en sortie un certain élément pris dans un ensemble fini, éventuellement distinct de celui de départ. Dans le contexte des automates finis, un ensemble fini sera appelé un alphabet, ses éléments des lettres, et une succession de lettres un mot. Un alphabet fini peut aussi bien désigner un ensemble fini de lettres comme $\{A, T, C, G\}$, de chiffres $\{0, 1\}$ ou de symboles quelconques $\{\uparrow, \downarrow, \leftarrow, \rightarrow\}$. On peut alors définir les suites automatiques, qui sont les suites construites à partir d'un automate fini lorsqu'on lui donne en entrée les chiffres de l'entier n représenté en base k. Plus formellement, pour un automate fini sur une certaine base k, une suite $(u_n)_{n\geq 0}$ telle que pour tout $n \in \mathbb{N}$ la valeur de u_n est celle renvoyée par l'automate fini en sortie lorsqu'on lui donne l'entier n en entrée, sera dite k-automatique. Pour avoir un bon aperçu des automates finis et des suites automatiques on pourra consulter le livre d'Allouche et Shallit [6] qui est une référence en la matière.

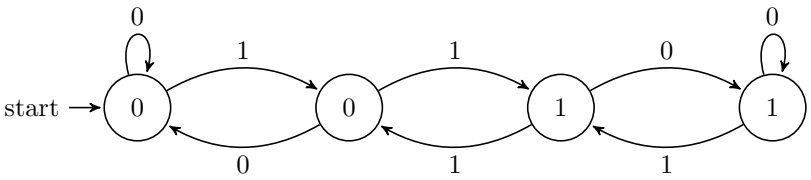
Les suites automatiques ont été largement étudiées en combinatoire des mots. L'une des plus célèbres est la suite de Thue–Morse (ou Prouhet–Thue–Morse), qui est issue de l'automate fini suivant :



Il s'agit d'une suite 2-automatique, définie sur l'alphabet $\{0, 1\}$, et qui calcule le nombre de 1 modulo 2 dans la décomposition binaire de l'entier n qu'on lui donne en entrée. L'automate fini commence la lecture sur la bulle de gauche. Il lit ensuite tous les chiffres de l'entier n en base 2, reste sur la même bulle à l'étape suivante s'il s'agit d'un 0 ou va sur l'autre bulle s'il s'agit d'un 1. Les instructions sont représentées par les flèches. Lorsqu'il a lu le dernier chiffre, il est alors sur l'une des deux bulles et renvoie en sortie la valeur indiquée par celle-ci, soit 0, soit 1. Si on termine sur la bulle de gauche, cela signifie donc qu'on a fait un nombre pair de trajets entre les deux bulles, et par conséquent qu'il y a un nombre pair de 1 dans la décomposition binaire de l'entier n donné en entrée. Si on termine sur la bulle de droite, alors on a fait éventuellement plusieurs allers-retours entre les deux bulles puis un dernier trajet entre la

bulle de gauche et la bulle de droite, ce qui signifie donc que l'entier n que l'on s'est donné au départ contient un nombre impair de 1 dans sa décomposition binaire.
On peut également définir la suite de Thue–Morse par la substitution σ définie par $0 \mapsto 01$ et $1 \mapsto 10$. En partant d'un 0 initial et en itérant successivement la substitution σ on obtient une suite de mots. La limite infinie de ces mots est l'unique point fixe de σ qui commence par un 0, et est appelé mot de Thue–Morse, la n-ième lettre du mot étant le n-ième terme de la suite de Thue–Morse, en commençant au rang 0.
La suite de Thue–Morse a été redécouverte plusieurs fois de manière indépendante afin de résoudre des problèmes différents (voir [5]). Le plus connu d'entre eux est celui de Thue qui cherchait à construire une suite binaire infinie évitant les cubes, c'est-à-dire telle qu'il n'y ait pas trois fois de suite le même motif apparaissant dans la suite. Les deux articles qu'il a publiés sur le sujet en 1906 et en 1912 sont considérés comme l'acte fondateur de la combinatoire des mots.

De nombreuses suites automatiques font partie des suites de références étudiées en combinatoire des mots. On peut par exemple citer la suite 2-automatique de Rudin–Shapiro (ou Golay–Rudin–Shapiro), qui compte le nombre de blocs "11" dans la décomposition binaire d'un entier. Elle est engendrée par l'automate fini suivant :



On peut se convaincre rapidement que cet automate compte bien le nombre de blocs "11". La suite de Rudin–Shapiro peut également se définir sur l'alphabet $\{-1, 1\}$, mais l'automate fini reste le même, il suffit juste de changer la valeur des bulles. Selon le contexte, il est plus commode de travailler avec un alphabet ou l'autre. Concernant la paternité de la suite, certains auteurs préfèrent utiliser le nom Golay–Shapiro, Golay et Shapiro étant les premiers à la mentionner de manière indépendante en 1951 [19, 43]. À ce sujet, on pourra consulter l'article d'Allouche [1].
Il existe de nombreuses généralisations de cette suite dans la littérature, notamment sur des alphabets de taille plus grande (voir [2, 4, 20, 30, 31, 38, 40]). Souvent, la généralisation est obtenue à partir d'une propriété de la suite classique de Rudin–Shapiro que l'on aimerait conserver dans un cadre plus général. Nous donnerons plusieurs exemples dans la deuxième partie de la thèse où nous avons étudié une des généralisations.

Pour déterminer si une suite est automatique ou non, le moyen qui paraît le plus naturel est de construire explicitement un automate fini qui permet d'obtenir la suite. Cependant, dans la pratique, il existe un certain nombre de critères d'automaticité ou de non-automaticité permettant de nous affranchir de la détermination explicite d'un automate fini. Cela peut s'avérer très utile dans le cas où le nombre d'états est important, ou si la suite a des propriétés que l'on peut facilement exploiter. Parmi ces critères, le plus classique consiste à s'intéresser au k-noyau de la suite, qui est défini pour une suite $\mathbf{u} = (u_n)_{n\geq 0}$ et un entier $k \geq 2$, par l'ensemble $\mathcal{N}_k(\mathbf{u}) = \{(u_{k^n a+b})_{n\geq 0}, \quad a \geq 0, \quad 0 \leq b \leq k^a - 1\}$. On sait que le k-noyau est fini si et seulement si la suite est k-automatique. Par exemple, dans le cas de la suite de Thue–Morse $(t_n)_{n\geq 0}$, son noyau ne contient que deux éléments qui sont la suite elle-même $(t_n)_{n\geq 0}$ et la suite $(t_{2n+1})_{n\geq 0}$ qui est la suite miroir de Thue–Morse que l'on obtient en remplaçant tous les 0 par des 1 et les 1 par des 0.
Nous avons également un résultat de Cobham [12] qui donne une caractérisation des suites automatiques à l'aide des suites issues d'un morphisme (ou une substitution). On dira qu'un morphisme (ou une substitution) σ, défini sur un alphabet fini $\mathcal{A}$, est k-uniforme si l'image par σ de chaque lettre de $\mathcal{A}$ est un mot de longueur k. Par exemple, la substitution qui définit la suite de Thue–Morse est 2-uniforme. Le théorème de Cobham énonce qu'une suite est k-automatique si et seulement si c'est l'image d'un point fixe d'un morphisme k-uniforme par un morphisme lettre à lettre. La suite de Thue–Morse étant l'image d'un morphisme 2-uniforme, nous retrouvons directement le fait qu'elle soit 2-automatique.
Dans le cas où k est une puissance d'un nombre premier, nous avons un résultat que l'on doit à Christol [11] qui nous indique qu'une suite est k-automatique si et seulement si sa série génératrice est algébrique sur le

corps fini à k éléments. Ce théorème permet d'étudier les suites automatiques à l'aide d'outils algébriques et de résultats sur les séries. Ces outils sont également utilisés pour étudier les automates cellulaires.

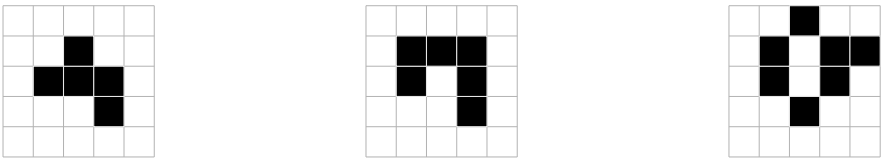
Automates cellulaires

Un automate cellulaire est un modèle de calcul, introduit dans les années 1940 par von Neumann qui cherchait à modéliser un problème d'auto-reproduction. Son collègue Ulam, qui avait étudié des croissances de cristaux en les modélisant sur une grille, lui avait conseillé de s'inspirer de ses travaux. Par la suite ces objets mathématiques ont suscité beaucoup d'intérêt chez les physiciens (von Neumann étant lui-même aussi bien mathématicien que physicien) et les biologistes. Pour plus d'informations sur le sujet, on pourra consulter le livre édité par Burks [45] qui reprend de manière posthume les travaux de von Neumann. Le principe est le suivant, on se donne une grille avec des cases, appelées également cellules, et un nombre d'états fixé à l'avance. On attribue un état à chacune des cellules de notre grille ce qui nous fournit une configuration initiale. Puis on définit des règles d'évolution locales, que l'on applique à toutes les cellules de la grille. On génère ainsi une nouvelle configuration dans laquelle un nouvel état, déterminé en suivant les règles locales, a été attribué à chaque case de la grille. On peut alors itérer le processus et engendrer une succession de remplissages de la grille en suivant les mêmes règles d'évolution à chaque fois. Une cellule peut éventuellement garder le même état d'une configuration à l'autre. Ainsi, une fois les règles locales fixées, chaque remplissage initial de la grille que l'on se donne engendrera de manière automatique une suite de configurations dans laquelle on pourra observer une évolution. Le premier automate cellulaire, utilisé par von Neumann pour son problème d'auto-reproduction, reposait sur une grille à deux dimensions, avec 29 états possibles pour chaque cellule.
En plus de reprendre et de compléter les travaux de von Neumann, le livre édité par Burks [45] en 1966, recensait alors la plupart des problèmes sur les automates cellulaires de l'époque. Les automates cellulaires commencèrent alors à susciter de plus en plus d'intérêt.
Dans les années 1970, Conway introduisit son célèbre jeu de la vie, qui est probablement l'automate cellulaire le plus connu. Il repose uniquement sur deux règles très simples. On considère qu'une cellule est soit morte (ce qu'on représente en générale par une case blanche), soit vivante (ce qu'on représente par une case noire). Chaque cellule possède huit voisines qui déterminent son évolution de la manière suivante :

— Une cellule morte ayant exactement trois voisines vivantes devient vivante à l'étape suivante.

— Une cellule vivante ayant deux ou trois voisines vivantes le reste à l'étape suivante, et meurt sinon.

Les règles étant fixées, il suffit simplement de choisir une configuration initiale et le système évolue automatiquement en engendrant des grilles successives.



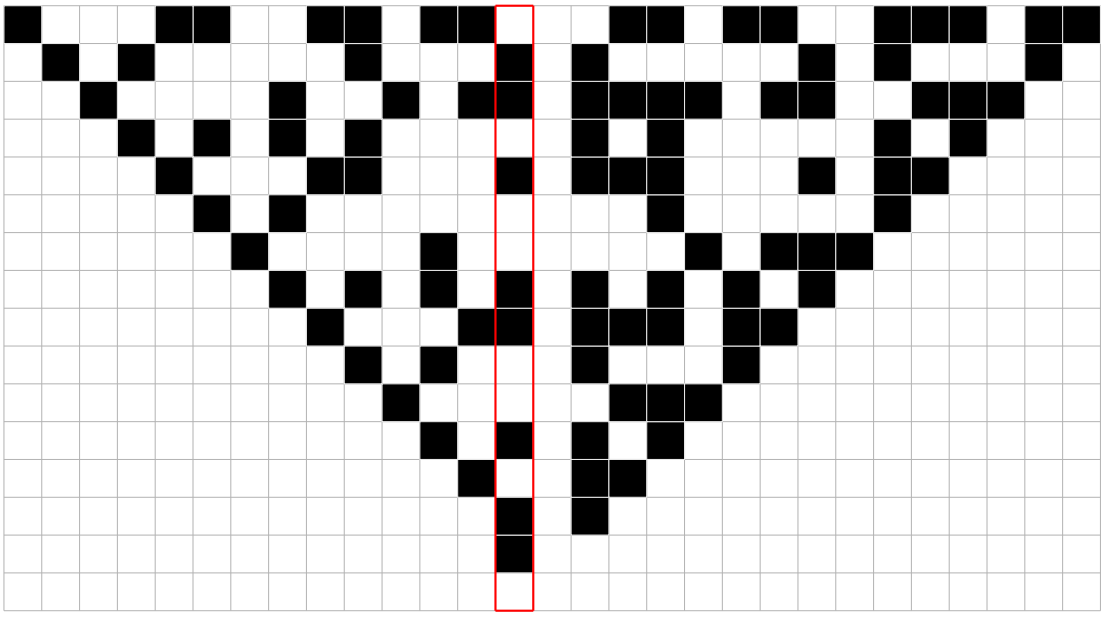
Ici nous avons pris comme grille initiale celle de gauche. En appliquant les règles une première fois, on obtient la grille du milieu, puis celle de droite en appliquant à nouveau les règles, et ainsi de suite.
Bien qu'il soit défini de manière extrêmement simple, le jeu de la vie possède des propriétés tout à fait remarquables. En effet, Rendell a démontré qu'il était possible de simuler n'importe quelle machine de Turing à partir du jeu de la vie [39].
Dans les années 1980, Wolfram s'intéressa aux automates cellulaires dits élémentaires, qui sont parmi les plus simples que l'on puisse définir. On se donne une grille unidimensionnelle dans laquelle chaque cellule peut prendre deux états, soit 0 (case blanche), soit 1 (case noire). Le voisinage pour définir les règles d'évolution est constitué de la cellule elle-même et de ses deux voisines adjacentes. Chaque cellule pouvant prendre deux états, il existe $2^3 = 8$ motifs possibles pour définir les règles. Et comme on a le choix entre deux états à attribuer à chacun des 8 motifs, il existe en tout $2^8 = 256$ automates cellulaires élémentaires. Les configurations que l'on obtient après avoir engendré plusieurs lignes, peuvent être très différentes.

On peut obtenir des motifs réguliers, des fractales ou des comportements complètement chaotiques qui ne semblent pas suivre de schéma logique prédéfini. On trouvera une étude détaillée de ces automates et de nombreuses illustrations dans le livre de Wolfram [46].

Les premiers résultats que nous avons obtenus s'inscrivent dans la lignée des travaux relativement récents de Rowland et Yassawi, qui établissent un lien assez fort entre les suites p-automatiques et les automates cellulaires [41]. Ils démontrent qu'une suite est p-automatique, dans le cas où p est un nombre premier, si et seulement si elle peut être obtenue comme colonne d'un automate cellulaire linéaire à valeurs dans $\mathbb{F}_p$ à partir d'une configuration initiale finie. De plus leur preuve est constructive, car elle permet à partir d'une suite p-automatique donnée d'obtenir à la fois un automate cellulaire qui convient et la configuration initiale. Bien que la méthode qu'ils proposent puisse s'appliquer à n'importe quelle suite p-automatique en théorie, dans la pratique les calculs peuvent vite devenir assez lourds. Nous traitons différents exemples, où en exploitant d'autres propriétés des suites auxquelles nous nous intéressons, il est possible d'alléger les calculs et d'obtenir un autre automate cellulaire qui construit la suite, mais avec une mémoire plus faible. Nous explicitons d'ailleurs une manière d'obtenir une construction pour toute une famille de suites p-automatiques, appelées suites généralisées de Rudin–Shapiro, que nous étudierons en détail dans les deux derniers chapitres de la thèse.
Nous pouvons par exemple construire un automate cellulaire linéaire dans lequel la suite 2-automatique de Thue–Morse apparaît dans l'une des colonnes. On identifiera les cases blanches à des 0 et les cases noires à des 1. Si $\phi(m,n)$ désigne la valeur de la case dans la colonne de rang m et dans la ligne de rang n, alors on peut montrer avec le résultat de Rowland et Yassawi, que l'automate cellulaire engendré par la règle suivante :

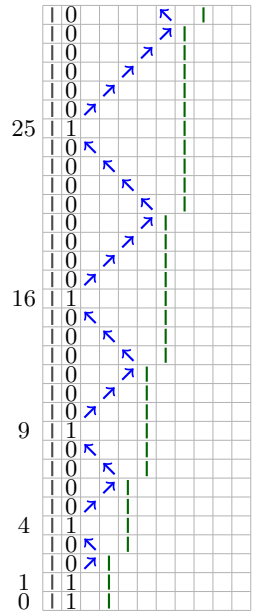
$$\begin{aligned}\phi(m,n+4) = {} & \phi(m-1,n+3) + \phi(m+1,n+3) + \phi(m,n+2) + \phi(m+1,n+2) \\ & + \phi(m-1,n+1) + \phi(m+1,n+1) + \phi(m-1,n) + \phi(m+1,n)\end{aligned}$$

contient la suite de Thue–Morse dans la colonne de rang -2, encadrée en rouge sur la figure. La ligne du bas est celle de rang -1 :



Dans la suite nous nous sommes intéressés à des constructions de suites non-automatiques en colonnes d'automates cellulaires, qui au vu du résultat de Rowland et Yassawi, sont nécessairement non-linéaires [28]. Un exemple de suite non-automatique, pour lequel une construction en colonne d'un automate cellulaire était connue depuis longtemps, est la suite indicatrice des nombres premiers [15, 23]. Fischer donna une première construction en 1965, mais qui comptait plus de 30 000 états, puis en 1997, Korec réussi à réduire à 11 états seulement. Plus tard, Mazoyer et Terrier établissent d'autres résultats

concernant la construction de l'indicatrice des polynômes, à l'aide de constructions géométriques avec des signaux [34] qui se propagent à différentes vitesses. Nous proposons une simplification de ces constructions [28] en généralisant celle introduite par Delacourt, Poupet, Sablik et Theyssier pour l'indicatrice des carrés [13] que l'on peut obtenir de cette manière :



On génère le signal bleu en diagonale vers la droite, et le signal vert, quant à lui, se propage verticalement. Lorsque les deux signaux se rencontrent, le signal vert se décale d'une case vers la droite et continue à se propager verticalement, tandis que le signal bleu repart en diagonale dans le sens opposé jusqu'à atteindre la colonne la plus à gauche dans laquelle on construit l'indicatrice des carrés, et ainsi de suite.
Enfin, nous proposons une construction du mot de Fibonacci, qui est une suite non-automatique de référence en combinatoire des mots, et qui s'obtient en itérant une infinité de fois à partir d'un 0 initial, la substitution σ définie par $0 \mapsto 01$ et $1 \mapsto 0$. Le mot que l'on obtient à la n-ième itération est de longueur F_n, où F_n désigne le n-ième nombre de la suite de Fibonacci.
Nous établissons ensuite des résultats sur des recodages, afin de réduire le nombre de symboles dans les automates cellulaires. Cela permet notamment de construire une suite 3-automatique sur un alphabet binaire, en colonne d'un automate cellulaire à 2 états, non-périodique à partir d'un certain rang, répondant ainsi à une question posée par Rowland et Yassawi dans leur article.

Suites généralisées de Rudin–Shapiro, corrélations

Les chapitre 3 et 4 sont consacrés à l'étude des corrélations discrètes de suites généralisées de Rudin–Shapiro. Initialement, la suite classique de Rudin–Shapiro que nous avons évoquée précédemment dans le cadre des suites automatiques a été introduite pour un tout autre problème. Shapiro est le premier à en faire mention dans son mémoire de thèse en 1951 [43]. Il cherchait une suite $(\varepsilon_n)_{n\geq 0}$ de 1 et de -1, vérifiant la propriété suivante, appelée parfois propriété "du racine de N", où C est une constante absolue :

$$\forall N \geq 0, \quad \sup_{\theta\in\mathbb{R}} \left| \sum_{n<N} \varepsilon_n e^{in\theta} \right| \leq C\sqrt{N}. \tag{1}$$

Le fait que le n-ième terme de cette suite corresponde au nombre de blocs "11" dans la décomposition binaire de n a été remarqué explicitement par Brillhart et Carlitz [8].
Il existe de nombreuses généralisations de cette suite, construites afin d'étudier des problèmes divers.

Certaines consistent à étendre la propriété "du racine de N" à des suites définies sur des alphabets de taille plus grande. On peut citer notamment la toute première généralisation, que l'on doit à Rider [40] ainsi que les travaux d'Allouche et Liardet [4]. Martine Queffélec s'est intéressée à une généralisation de la suite de Rudin–Shapiro dans le but d'en étudier les propriétés spectrales [38]. Les travaux que nous avons effectués s'incrivent dans la lignée de ceux de Grant, Shallit et Stoll [20] qui en exploitant les propriétés de récursivité de la suite de Rudin–Shapiro, ont étudié les corrélations discrètes d'une famille de suites automatiques qui constituent une généralisation de la suite de Rudin–Shapiro. Pour un entier $k \geq 2$ et $x = x_0 x_1 \cdots$ un mot infini sur l'alphabet $\{0, 1, \ldots, k-1\}$, le coefficient de corrélation discrète d'ordre 2 est défini de la manière suivante :

$$\delta(i,j) = \begin{cases} 0, & \text{si } x_i = x_j, \\ 1, & \text{sinon.} \end{cases}$$

Autrement dit, lorsqu'on compare deux lettres du mot, le coefficient de corrélation discrète d'ordre 2 vaut 0 si les deux lettres sont identiques et 1 si elles sont différentes. On peut alors se fixer un certain écart r et regarder la moyenne empirique des coefficients de corrélation discrète de tous les couples de lettres du mot distantes de r. Grant et al. établissent le fait remarquable que les suites généralisées de Rudin–Shapiro qu'ils considèrent, bien qu'elles soient déterministes, se comportent comme des suites aléatoires pour la corrélation discrète d'ordre 2 dans le cas où la taille de l'alphabet sur lequel nous travaillons est sans facteur carré. Cela confère à ces suites un caractère pseudo-aléatoire. De plus, ils obtiennent un terme d'erreur explicite qui permet de quantifier la vitesse de convergence. Les preuves utilisent notamment la théorie des sommes d'exponentielles, ainsi que des matrices très particulières appelées matrices de différence.

Matrices de différence

Une matrice de différence, est une matrice définie sur un groupe additif fini, telles que toutes les différences possibles entre deux colonnes distinctes contiennent tous les éléments du groupe avec le même nombre d'occurrences pour chacun.

Par exemple, les deux matrices suivantes sont des matrices de différence, respectivement de taille 3×3 sur $\mathbb{Z}/3\mathbb{Z}$ et de taille 8×4 sur $\mathbb{Z}/4\mathbb{Z}$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 2 \\ 0 & 2 & 1 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \\ 0 & 3 & 2 & 1 \end{pmatrix}.$$

Selon la taille de la matrice que l'on considère, il est possible d'obtenir des constructions explicites, ou à l'inverse des preuves de non-existence de matrices de différence. Les trois paramètres à prendre en compte dans l'étude des matrices de différences sont le nombre de lignes, le nombre de colonnes et le groupe sous-jacent. On peut montrer par exemple qu'il n'existe aucune matrice de différence de taille 4×4 sur $\mathbb{Z}/4\mathbb{Z}$, en revanche on peut vérifier facilement que la matrice suivante, de taille 4×4, définie sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est une matrice de différence :

$$\begin{pmatrix} (0,0) & (0,0) & (0,0) & (0,0) \\ (0,0) & (0,1) & (1,0) & (1,1) \\ (0,0) & (1,0) & (1,1) & (0,1) \\ (0,0) & (1,1) & (0,1) & (1,0) \end{pmatrix}.$$

On trouvera de nombreux résultats sur le sujet dans le livre très complet [21] de Hedayat, Sloane et Stufken. On pourra également consulter la thèse de Lampio [24] ainsi que l'article de Lampio et Östergård [24, 25] qui proposent une classification des matrices de différence en fonction de leur taille et

du groupe sous-jacent. En effet, il est possible de définir une relation d'équivalence entre deux matrices de différence. On dira que deux matrices de différence sont dans la même classe d'équivalence si elles ont le même nombre de lignes et de colonnes, le même groupe sous-jacent et si l'une peut être obtenue à partir de l'autre à l'aide des opérations suivantes :

1. Permuter l'ordre des lignes.
2. Permuter l'ordre des colonnes.
3. Ajouter un élément fixé du groupe sous-jacent à une ligne.
4. Ajouter un élément fixé du groupe sous-jacent à une colonne.
5. Appliquer un automorphisme du groupe sous-jacent à chaque élément de la matrice de différence.

On peut montrer que dans le cas où le groupe sous-jacent est un groupe abélien muni d'un ordre total, chaque classe d'équivalence possède un représentant qui est une matrice, dite ordonnée-normalisée et qui a la forme suivante :

1. la première ligne contient uniquement l'élément identité,
2. la première colonne contient uniquement l'élément identité,
3. les lignes sont rangées dans l'ordre lexicographique croissant du haut vers le bas (induit par la relation d'ordre total du groupe sous-jacent sur les vecteurs lignes), et
4. les colonnes sont rangées dans l'ordre lexicographique croissant de la gauche vers la droite (induit par la relation d'ordre total du groupe sous-jacent sur les vecteurs colonnes).

Ainsi, pour classifier les matrices de différence, on se ramène à l'étude des matrices de différence ordonnées-normalisées. Cependant, pour des paramètres fixés, il peut y avoir plusieurs classes d'équivalence. Par exemple, les matrices de différence de taille 9×9 sur $\mathbb{Z}/3\mathbb{Z}$ possèdent deux classes d'équivalence, dont voici des représentants :

$$\begin{pmatrix} 0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&2&2&2\\ 0&0&0&2&2&2&1&1&1\\ 0&1&2&0&1&2&0&1&2\\ 0&1&2&1&2&0&2&0&1\\ 0&1&2&2&0&1&1&2&0\\ 0&2&1&0&2&1&0&2&1\\ 0&2&1&1&0&2&2&1&0\\ 0&2&1&2&1&0&1&0&2 \end{pmatrix} \qquad \begin{pmatrix} 0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&2&2&2\\ 0&0&0&2&2&2&1&1&1\\ 0&1&2&0&1&2&0&1&2\\ 0&1&2&1&2&0&2&0&1\\ 0&1&2&2&0&1&1&2&0\\ 0&2&1&0&2&1&1&0&2\\ 0&2&1&1&0&2&0&2&1\\ 0&2&1&2&1&0&2&1&0 \end{pmatrix}.$$

Plus généralement, voici la classification obtenue par Lampio et Östergård pour des groupes de petits cardinaux et une taille bornée. Ici r représente le nombre de lignes de la matrice et c le nombre de colonnes :

On constate que le nombre de classes peut être relativement grand par rapport à la taille des paramètres. On trouvera un représentant de chaque classe sous la forme d'une matrice ordonnée-normalisée sur le site de Lampio. [1] Il semble que la classification générale des matrices de différence est une question difficile, qui pour le moment est établie uniquement pour des petits paramètres.
Dans toute la thèse, nous avons pris la convention inverse entre les lignes et les colonnes par rapport aux références précitées [21, 24, 25] mais il suffit simplement de transposer les matrices pour passer de l'une à l'autre.

À l'aide des matrices de différence, nous avons été en mesure de généraliser le résultat établi par Grant, Shallit et Stoll, dans un premier temps pour les alphabets dont la taille est une puissance d'un nombre premier, puis à tous les alphabets [44]. Nous étendons leur construction à l'aide des matrices de différences, puis nous utilisons des arguments similaires avec des sommes d'exponentielles. Pour les alphabets dont la taille est un produit d'au moins deux facteurs premiers, mais sans facteur carré, nous avons d'ailleurs affiné le terme d'erreur obtenu par Grant, Shallit et Stoll.

1. `https://wiki.aalto.fi/display/DifferenceMatrices/Home` (consulté le 16/12/2020)

r	c	G	#
r	2	$\mathbb{Z}_2$	1
3	3	$\mathbb{Z}_3$	1
6	6	$\mathbb{Z}_3$	1
9	9	$\mathbb{Z}_3$	2
12	12	$\mathbb{Z}_3$	1
15	9	$\mathbb{Z}_3$	5
18	18	$\mathbb{Z}_3$	53
4	2	$\mathbb{Z}_4$	1
8	4	$\mathbb{Z}_4$	6
12	2	$\mathbb{Z}_4$	1
16	16	$\mathbb{Z}_4$	13
20	2	$\mathbb{Z}_4$	1

r	c	G	#
4	4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1
8	8	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1
12	12	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1
16	16	$\mathbb{Z}_2 \times \mathbb{Z}_2$	226
5	5	$\mathbb{Z}_5$	1
10	10	$\mathbb{Z}_5$	1
15	8	$\mathbb{Z}_5$	2
6	2	$\mathbb{Z}_6$	1
4	12	$\mathbb{Z}_6$	7
18	2	$\mathbb{Z}_6$	1
7	7	$\mathbb{Z}_7$	1
14	14	$\mathbb{Z}_7$	2

Nous terminons par une généralisation des résultats précédents à l'aide de méthodes combinatoires et en exploitant la représentation en base k de certains entiers qui interviennent dans les preuves. Nous utilisons toujours la structure des matrices de différence, mais pas la théorie des sommes d'exponentielles. Cela permet notamment une amélioration du terme d'erreur dans le cas où la taille de l'alphabet est un nombre composé, avec éventuellement des facteurs carrés, mais en utilisant une seule matrice de différence, contrairement au précédent résultat [44] qui utilisait une matrice de différence pour chaque facteur premier dans la décomposition. Au passage on remarque qu'en plus du comportement pseudo-alétoire de ces suites généralisées de Rudin–Shapiro, la convergence de la moyenne empirique est plus rapide. En effet, alors que le terme d'erreur est de l'ordre de $1/\sqrt{N}$, quand $N \to \infty$, dans le cas aléatoire, nous obtenons un terme d'erreur d'ordre $\log(N)/N$, quand $N \to \infty$, dans le cas de nos suites généralisées de Rudin–Shapiro, et ce quelle que soit la taille de l'alphabet. Nous généralisons la définition du coefficient de corrélation d'ordre 2 défini au Chapitre 3 de la manière suivante. Pour une suite u à valeurs dans un groupe abélien fini $(G, +)$, des entiers $n \in \mathbb{N}$ et $r \in \mathbb{N} \setminus \{0\}$, et un vecteur $(i, j) \in G^2$ on définit

$$\delta_{i,j}^r(n) = \begin{cases} 1 & \text{si } (u_n, u_{n+r}) = (i, j); \\ 0 & \text{sinon.} \end{cases}$$

Pour une suite généralisée de Rudin–Shapiro, on définit alors la matrice de corrélations par la matrice de taille $|G| \times |G|$, qui a pour coefficient à la ligne i et à la colonne j, la quantité $\lim_{N\to\infty} C_{i,j}^r(N) = \frac{1}{N}\sum_{n=0}^{N-1} \delta_{i,j}^r(n)$. On montre alors, que chacune de ces limites est identique à celle que l'on obtient dans le cas aléatoire Les résultats de cette partie concernent toute la matrice de corrélations, alors que ceux du Chapitre 3 portent uniquement sur la trace de la matrice de corrélations. Nous évoquons également le cas de la dimension supérieure, et donnons plusieurs exemples explicites [29].

Annonce du plan

Nous présentons maintenant plus en détail la structure de la thèse. Les deux premiers chapitres traitent de la partie sur les automates finis et les automates cellulaires, et les deux derniers concernent la partie sur les corrélations discrètes des suites généralisées de Rudin–Shapiro. Les chapitres 2, 3 et 4 se terminent chacun par une sélection de questions ouvertes.

Chapitre 1

Nous commençons par un chapitre permettant de donner différents exemples d'automates finis et de suites automatiques, parmi les plus connus de la théorie, ainsi que des résultats classiques, dont notamment des critères d'automaticité et de non-automaticité. La plupart de nos énoncés peuvent se retrouver et être approfondis dans le livre d'Allouche et Shallit [6]. Nous introduisons également les automates cellulaires avec la définition de manière formelle et le théorème de Curtis–Hedlund–Lyndon largement utilisé dans la pratique [22] pour les manipuler.

Chapitre 2

Dans ce chapitre, nous rappelons les résultats obtenus par Rowland et Yassawi ainsi que les outils et les méthodes utilisées, notamment l'utilisation des séries de Laurent et des corps finis. Nous donnons ensuite différentes constructions explicites de suites automatiques de référence, en application directe de leur méthode. Nous réussissons à améliorer leur construction de la suite classique de Rudin–Shapiro en obtenant un automate cellulaire linéaire avec une mémoire plus faible, puis nous généralisons la méthode à toute une famille de suites généralisées de Rudin–Shapiro, qui constituent un cas particulier de celles que nous étudions dans le Chapitre 3. Nous nous intéressons ensuite aux constructions de certaines suites non-automatiques en donnant les résultats généraux de notre méthode et en traitant explicitement quelques exemples, à savoir la construction de l'indicatrice de la somme des carrés et la construction de l'indicatrice des cubes. Nous traitons de manière explicite l'indicatrice des nombres de Fibonacci, qui nous permet de construire le mot de Fibonacci en colonne d'un automate cellulaire non-linéaire. Nous terminons ce chapitre par nos résultats sur les recodages binaires. Nous construisons l'indicatrice des puissances de 3 avec la méthode de Rowland et Yassawi, que nous recodons ensuite grâce à nos résultats sur les recodages binaires, ce qui permet d'obtenir cette suite 3-automatique en colonne d'un automate cellulaire à 2 états, non-périodique à partir d'un certain rang, répondant ainsi à une question posée par Rowland et Yassawi [41]. On pourra retrouver l'ensemble de nos réultats dans [28].

Chapitre 3

Dans cette deuxième partie de la thèse, nous étudions les corrélations discrètes d'ordre 2 de suites généralisées de Rudin–Shapiro. Après avoir évoqué un petit historique concernant la genèse de la suite classique de Rudin–Shapiro, ainsi que différentes généralisations, nous définissons celle à laquelle nous nous sommes intéressés en reprenant les travaux de Grant, Shallit et Stoll [20]. Pour cela, nous avons besoin de la théorie des matrices de différence, que nous illustrons par de nombreux résultats et exemples que l'on retrouvera notamment dans [21, 24, 25]. Après avoir rappelé les résultats principaux sur les corrélations d'ordre 2 de Grant et al. nous énonçons les nôtres et donnons deux preuves utilisant les sommes d'exponentielles, l'une pour les alphabets dont la taille est une puissance d'un seul nombre premier, où nous obtenons le même terme d'erreur que Grant et al. dans le cas où la taille de l'alphabet est juste un nombre premier, et l'autre dans le cas général avec un produit de plusieurs puissances de nombres premiers et où nous réussissons à améliorer le terme d'erreur obtenu par Grant et al. dans le cas d'un produit de plusieurs nombres premiers distincts. On pourra retrouver ces résultats dans [44].

Chapitre 4

Enfin, le dernier chapitre de cette thèse s'intéresse aux mêmes problématiques sur les corrélations d'ordre 2 du Chapitre 3 mais dans un cadre plus général et avec une approche combinatoire à la place de l'utilisation des sommes d'exponentielles. Toutefois, nous continuons à exploiter la structure des matrices de différence qui définissent nos généralisations de Rudin–Shapiro. Nos résultats portent sur la matrice de corrélations et plus uniquement sur la trace de cette matrice, comme pour le Chapitre 3. Nous évoquons également le cas de la dimension supérieure et traitons quelques exemples explicitement. On retrouvera ces résultats dans [29].

Résumé

Cette thèse se situe à la frontière entre mathématiques et informatique théorique. Nous nous intéressons dans un premier temps aux automates finis et aux automates cellulaires. Bien qu'ils s'agissent de deux objets mathématiques assez différents, il est possible de les relier par des constructions explicites, en regardant la réalisation des suites automatiques dans les diagrammes espace-temps des automates cellulaires. Dans un second temps, nous étudions les corrélations discrètes de certaines suites automatiques, appelées suites généralisées de Rudin–Shapiro, qui se comportent comme des suites aléatoires pour la corrélation discrète d'ordre 2, bien qu'elles soient déterministes.

Après une introduction des objets d'étude, que nous illustrons par plusieurs exemples, nous rappelons le résultat de Rowland et Yassawi, qui ont montré en 2015 qu'il était possible de construire de manière explicite toute suite p-automatique, dans le cas où p est un nombre premier, en colonne d'un automate cellulaire linéaire, à partir d'une configuration initiale finie. En utilisant leur méthode, nous obtenons différentes constructions de suites automatiques de référence, puis nous établissons un moyen explicite de construire toute une famille de suites p-automatiques, appelées suites généralisées de Rudin–Shapiro, que nous étudions dans la deuxième partie de la thèse, dans un cadre plus général. Nous nous intéressons également au cas de certaines suites non-automatiques, telles que l'indicatrice des polynômes et le mot de Fibonacci, que nous réussissons à construire en colonne d'automates cellulaires non-linéaires. Puis nous obtenons des résultats sur des recodages binaires, permettant de réduire le nombre de symboles dans les automates cellulaires. Grâce à un recodage binaire, nous avons également construit explicitement une suite 3-automatique sur un alphabet binaire, en colonne d'un automate cellulaire à 2 états, non-périodique à partir d'un certain rang, ce qui répond à une question posée par Rowland et Yassawi.

Dans la deuxième partie de cette thèse, nous reprenons les travaux de Grant, Shallit et Stoll, qui ont établi en 2009 des résultats sur les corrélations discrètes de suites infinies sur des alphabets finis. En exploitant les propriétés de récursivité de la suite classique de Rudin–Shapiro, ils construisent une famille de suites déterministes sur des alphabets plus grands, pour lesquelles ils montrent que dans le cas où la taille de l'alphabet est sans facteur carré, la moyenne empirique des coefficients de corrélation d'ordre 2 a la même limite que dans le cas de suites où les lettres sont tirées aléatoirement, de manière uniforme et indépendamment. De plus, ils arrivent à quantifier explicitement le terme d'erreur. En généralisant leur construction à l'aide de la théorie des matrices de différence, nous arrivons à établir un résultat similaire pour des alphabets de taille quelconque ainsi qu'une amélioration du terme d'erreur dans certains cas. Tout comme Grant et al., nous nous servons de la théorie des sommes d'exponentielles pour démontrer notre résultat sur les corrélations discrètes d'ordre 2 de nos suites généralisées de Rudin–Shapiro.

Dans la troisième partie, nous terminons par une approche combinatoire de ces questions, qui nous a permis d'obtenir une amélioration du terme d'erreur dans le cas où la taille de l'alphabet est un produit d'au moins deux nombres premiers distincts, et de généraliser certains de nos résultats.

Mots-clés: combinatoire des mots, automates, informatique théorique, corrélations discrètes, sommes d'exponentielles.

Abstract

This thesis is at the interface between mathematics and theoretical computer science. In the first part, our main objects are finite automata and cellular automata. While relatively different in nature, it is possible to link both by explicit constructions. More specifically, it is possible to realise automatic sequences in the space-time diagrams of cellular automata. In the second part, we study discrete correlation properties of so-called generalised Rudin–Shapiro sequences. These are automatic sequences, hence deterministic, but show similar properties as random sequences with respect to their discrete correlation of order 2.

After introducing the objects of study, illustrated by several examples, we first recall the result of Rowland and Yassawi. They showed in 2015 via an algebraic approach that it is possible to construct explicitly any p-automatic sequence (p is a prime number) as a column of a linear cellular automaton with a finite initial configuration. By using their method, we obtain several constructions of classical automatic sequences, and an explicit way to build a family of p-automatic sequences that we study in a more general context in the second part of the thesis. We also investigate several non-automatic sequences, such as the characteristic sequence of integer-valued polynomials and the Fibonacci word, which both can be realised as columns of non-linear cellular automata. We end this part by some results about binary recodings in order to reduce the number of symbols in the cellular automata. Under a binary recoding, we give explicitly a 3-automatic sequence on a binary alphabet, as a column of a cellular automaton with 2 states, that is not eventually periodic. This answers a question asked by Rowland et Yassawi.

In the second part of the thesis, we take up research from 2009 of Grant, Shallit, and Stoll about discrete correlations of infinite sequences over finite alphabets. By using the recursivity properties of the classical Rudin–Shapiro sequence, they built a family of deterministic sequences over larger alphabets, called generalised Rudin–Shapiro sequences, for which they showed that when the size of the alphabet is squarefree, the empirical means of the discrete correlation coefficients of order 2 have the same limit as in the case of random sequences where each letter is independently and uniformly chosen. Moreover, they gave explicit error terms. We extend their construction by means of difference matrices and establish a similar result on alphabets of arbitrary size. On our way, we obtain an improvement of the error term in some cases. The methods stem, as those used by Grant et al., from the theory of exponential sums.

In the third part, we use a more direct combinatorial approach to study correlations. This allows for an improvement of the error term when the size of the alphabet is a product of at least two distinct primes, and allows to generalise some of our results of the second part.

Keywords: combinatorics on words, automata, theoretical computer science, discrete correlations, exponential sums.

Chapitre 1

Automates et suites automatiques

Sommaire

Apparue dans la première moitié du XXème siècle, la théorie des automates fut développée dans le but de formaliser la notion de calcul et de machine. Les automates finis constituent le modèle de machine le plus simple de la théorie des automates mais ne furent définis formellement que vers 1950, bien après les machines de Turing. Au cours des dernières décennies, de nombreux résultats utilisant notamment des méthodes combinatoires et algébriques ont été établis.

Un automate fini est une machine qui prend en entrée des mots définis sur un alphabet et qui après lecture des lettres qui constituent le mot, renvoie une lettre en sortie. Nous étudierons également les automates cellulaires que l'on associera à une grille avec des cases dans laquelle chaque ligne est obtenue à partir des précédentes par le biais d'une règle locale et de conditions initiales données. Il est possible d'engendrer des suites à partir d'un automate fini où l'on prend en entrée un nombre entier n que l'on écrit en base k, ensuite l'automate lit les chiffres qui composent le nombre et rend en sortie une lettre d'un alphabet fini que l'on définit comme étant le n-ième terme de la suite. De telles suites sont dites k-automatiques. Nous donnerons plusieurs caractérisations de ces suites ainsi que des exemples concrets pour illustrer les résultats.

Ce premier chapitre sera essentiellement consacré à définir les objets de notre étude.

1.1 Suites automatiques, automates finis

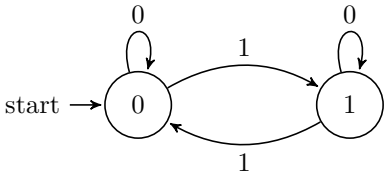
1.1.1 Définitions et premiers exemples

Définition 1.1.1. [3, 41] Un automate fini déterministe avec sortie (DFAO) est un 6-uplet $(Q, \Sigma_k, \delta, q_0, \mathcal{A}, \omega)$ où Q est un ensemble fini d'"états", $\Sigma_k = \{0, 1, \ldots, k-1\}$, $q_0 \in Q$ est l'état initial, $\mathcal{A}$ est un alphabet fini, $\omega : Q \longrightarrow \mathcal{A}$ est la fonction de sortie et $\delta : Q \times \Sigma_k \longrightarrow Q$ est la fonction de transition.

Remarque 1.1.1. [41] Si $n = \sum_{i=0}^{l} a_i k^i$ est la représentation standard en base k de $n \geq 1$ avec $0 \leq a_i \leq k-1$ et $a_l \neq 0$, on définit $(n)_k$ comme étant le mot $a_0 a_1 \cdots a_l$.
On définit alors pour tout $q \in Q$, $\quad \delta(q, a_0 a_1 \cdots a_l) = \delta(\delta(s, a_0), a_1 \cdots a_l)$ de manière récursive.
Le mot vide sera noté ε.

Définition 1.1.2. [3, 41] Une suite $(u_n)_{n\geq 0}$ d'éléments de $\mathcal{A}$ est dite k-automatique s'il existe un DFAO $(Q, \Sigma_k, \delta, q_0, \mathcal{A}, \omega)$ tel que $u_n = \omega(\delta(q_0, (n)_k)$ pour tout $n \geq 0$.

Exemple 1.1.1. [3, 41] La suite de Thue–Morse $(t_n)_{n\geq 0} = 0, 1, 1, 0, 1, 0, 0, 1, \ldots$ définie par $t_n = 0$ si le nombre de 1 dans le représentation binaire de n est pair et $t_n = 1$ sinon est une suite 2-automatique. Elle est engendrée par l'automate suivant, où les deux états sont étiquetés par leurs images par ω :



On note $\mathbf{t} = t_0 t_1 t_2 \cdots = 01101001 \cdots$ le mot infini engendré par cette suite, que l'on appelle mot de Thue–Morse ou mot de Prouhet–Thue–Morse [5].

Remarque 1.1.2. La suite de Thue–Morse peut aussi se définir de la manière suivante. Soit $n = \sum_{i=0}^{l} a_i 2^i$ la représentation binaire de n. On pose $s_2(n) = \sum_{i=0}^{l} a_i$ et $t_n = s_2(n) \bmod 2$. En particulier on a pour tout $n \geq 0$, $t_{2n} = t_n$ et $t_{2n+1} = 1 - t_n$.

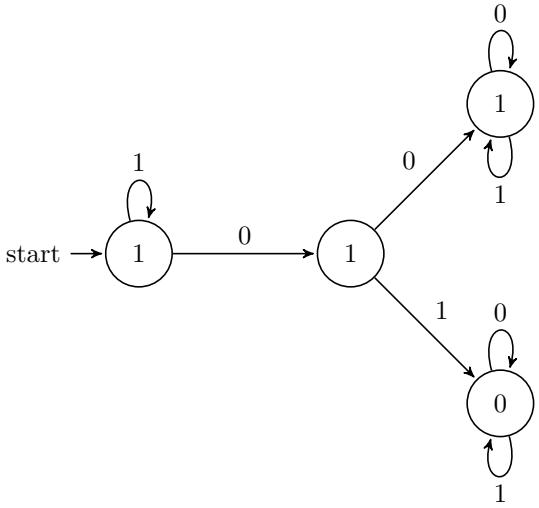
Il est également possible de définir la suite de Thue–Morse à l'aide d'un morphisme.

Définition 1.1.3. [6, Example 1.4.2] Considérons le morphisme (ou la substitution) σ défini par $0 \mapsto 01$ et $1 \mapsto 10$. On définit de manière récursive une suite de mots par $w_1 = 0$ et pour tout $n \geq 1, w_{n+1} = \sigma(w_n)$. Voici les premiers mots que l'on obtient :

$$\begin{aligned} w_1 &= 0 \\ w_2 &= 01 \\ w_3 &= 0110 \\ w_4 &= 01101001 \\ w_5 &= 0110100110010110 \\ w_6 &= 01101001100101101001011001101001. \end{aligned}$$

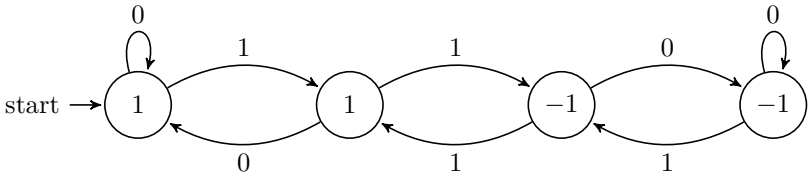
La limite infinie de ces mots est l'unique point fixe de σ qui commence par un 0, et est appelé mot de Thue–Morse, la n-ième lettre du mot étant le n-ième terme de la suite de Thue–Morse, en commençant au rang 0.

Exemple 1.1.2. [6, Example 5.1.6 et Observation 6.5.1] Soit $(w_n)_{n\geq 0}$ la suite de mots définie sur $\{0, 1\}$ par : $w_0 = 1$, et pour tout $n \geq 0$, $w_{n+1} = w_n 1 w_n'$ où x' désigne le "retourné" du mot x dont on a échangé les 0 et les 1. On a $w_1 = w_0 1 w_0' = 110$, $w_2 = w_1 1 w_1' = 1101(110)' = 1101100, \ldots$
La limite de cette suite est le mot infini $w = 110110011100100 \cdots$ La suite $(u_n)_{n\geq 0}$ où u_n désigne le n-ième symbole du mot w est appelée suite du pliage de papier $(u_0 = 1, u_1 = 1, u_2 = 0, u_3 = 1, \ldots)$. Notons au passage que pour tout $n \geq 0$ le mot w_n est de longueur $2^{n+1} - 1$. La suite du pliage de papier est engendrée par l'automate suivant :



Il s'agit donc d'une suite 2-automatique.

Exemple 1.1.3. [6, Example 3.3.1] La suite de Rudin–Shapiro (ou Golay–Rudin–Shapiro) $(\varepsilon_n)_{n\geq 0} = 1, 1, 1, -1, 1, 1, -1, 1, \ldots$ est définie de la manière suivante :
Si $n = \sum_{i=0}^{l} a_i 2^i$ est la représentation binaire de n, on pose $f(n) = \sum_{i=0}^{l-1} a_{i+1}a_i$ et $\varepsilon_n = (-1)^{f(n)}$. Cette suite est 2-automatique. Elle est engendrée par l'automate suivant :



Remarque 1.1.3. [3, 20, 41] La suite de Rudin–Shapiro peut aussi être définie sur l'alphabet $\{0, 1\}$ pour tout $n \in \mathbb{N}$ par

$$r_n = (\text{nombre de blocs “11” dans la représentation binaire de } n) \bmod 2.$$

On a alors, $(r_n)_{n\geq 0} = 0, 0, 0, 1, 0, 0, 1, 0, \ldots$ On en déduit facilement la définition équivalente suivante :

$$r_0 = 0,\ r_{2n} = r_n \text{ et } r_{2n+1} = \begin{cases} (r_n + 1) \bmod 2 & \text{si } n \equiv 1 \pmod 2, \\ r_n & \text{si } n \equiv 0 \pmod 2. \end{cases}$$

Ainsi, la suite de Rudin–Shapiro peut se définir de manière récursive par :

$$r_0 = 0 \text{ et } r_{2n+j} = (r_n + jn) \bmod 2 \quad \text{où } j \in \{0, 1\}$$

La suite de Rudin–Shapiro fera l'objet d'une étude approfondie dans le Chapitre 3. Dans la littérature, il existe de nombreuses généralisations sur des alphabets de taille plus grande. Nous y reviendrons plus en détail dans la suite. Néanmoins nous pouvons donner une première généralisation pour les alphabets dont la taille est un nombre premier, qui découle directement de la remarque précédente.

Définition 1.1.4. [20] Soit k un nombre premier. La suite $(a(n))_{n\geq 0}$ définie sur l'alphabet $\{0, 1, \ldots, k-1\}$ de manière récursive par :

$$a(kn + j) = (a(n) + jn) \bmod k \quad \text{pour } 0 \leq j \leq k - 1,\ n \geq 1,$$

où les valeurs de $a(0), \ldots, a(k-1)$ peuvent être choisies arbitrairement, est une *suite généralisée de Rudin–Shapiro*.

1.1.2 Noyau d'une suite automatique

Pour savoir si une suite donnée est automatique, on peut par exemple construire explicitement l'automate fini qui l'engendre. Il existe différents critères d'automaticité et de non-automaticité. L'un des plus connus, consiste à étudier ce qu'on appelle le k-noyau.

Définition 1.1.5. [6, p. 185] Soit k un entier, $k \geq 2$. On appelle k-noyau de la suite $\mathbf{u} = (u_n)_{n\geq 0}$ l'ensemble $\mathcal{N}_k(\mathbf{u}) = \{(u_{k^n a+b})_{n\geq 0}, \quad a \geq 0, \quad 0 \leq b \leq k^a - 1\}$.

Exemple 1.1.4. [6, Example 6.6.1] Le 2-noyau de la suite de Thue–Morse est

$$\{(t_n)_{n\geq 0}, (1-t_n)_{n\geq 0}\}.$$

Avec la définition de la suite de Thue–Morse on a directement $t_{2^a n+b} = t_n + t_b$ avec $t_b \in \{0,1\}$. D'où le résultat.

Exemple 1.1.5. [6, Example 6.6.3] Le 2-noyau de la suite de Rudin–Shapiro est

$$\{(r_n)_{n\geq 0}, (r_{2n+1})_{n\geq 0}, (r_{4n+3})_{n\geq 0}, (r_{8n+3})_{n\geq 0}\}.$$

En notant $n = \sum_{i=0}^{+\infty} \varepsilon_i 2^i$ et $b = \sum_{i=0}^{+\infty} \eta_i 2^i$ les représentations binaires de n et b on a alors $f(2^a n + b) = f(n) + f(b) + \varepsilon_0\eta_{a-1}$. D'où $r_{2^a n+b} = (-1)^{f(2^a n+b)} = r_n r_b (-1)^{n\eta_{a-1}}$. Il suffit ensuite de distinguer les cas selon la valeur de b qui nous donne $r_b = -1$ ou $r_b = 1$ et $\eta_{a-1} = 0$ ou $\eta_{a-1} = 1$.

Remarque 1.1.4. Pour une suite k-automatique, la taille du k-noyau est majorée par le nombre d'états de l'automate qui engendre la suite. En effet pour lire $k^a n + b$ on lit d'abord b qui nous conduit à un état de l'automate qui devient le nouvel état initial, puis on lit n, étant donné que les chiffres de $k^a n$ à partir du $a+1$-ème, en commençant la lecture par la droite, sont les mêmes que ceux de n.

Exemple 1.1.6. Le 2-noyau de la suite de pliage de papier $(u_n)_{n\geq 0}$ est

$$\{(u_n)_{n\geq 0}, (u_{4n})_{n\geq 0}, (u_{4n+2})_{n\geq 0}, (u_{2n})_{n\geq 0}\},$$

où $(u_{4n})_{n\geq 0}$ est en fait la suite identiquement égale à 1, $(u_{4n+2})_{n\geq 0}$ la suite identiquement égale à 0 et $(u_{2n})_{n\geq 0}$ la suite 2-périodique $10101010\cdots$.

Démonstration. On reprend les notations de l'Exemple (1.1.2). L'automate de la suite du pliage de papier que l'on a construit ayant 4 états, il y a donc au plus 4 suites dans le 2-noyau. Nous allons d'abord montrer à l'aide d'un raisonnement par récurrence que pour tout $n \geq 0$, $u_{4n} = 1$ et $u_{4n+2} = 0$. Pour tout $n \geq 0$ on pose

H_n : Pour tout $i \in [\![0, 2^n - 2]\!]$ la i-ème lettre du mot w_n est 1 si $i \equiv 0 \bmod 4$ et 0 si $i \equiv 2 \bmod 4$.

On a $w_0 = 1$ et la lettre de rang 0 est 1. On a $w_1 = 110$ et la lettre de rang 0 est 1 et celle de rang 2 est 0. On a $w_2 = 1101100$, les lettres de rang 0 et 4 sont 1 et celles de rang 2 et 6 sont 0. Donc H_0, H_1 et H_2 sont vraies.
Soit $n \geq 2$ tel que H_n soit vraie. Par définition de la suite du pliage de papier on a $w_{n+1} = w_n 1 w'_n$. On doit montrer que pour tout $i \in [\![0, 2^{n+1} - 2]\!]$ la i-ème lettre du mot w_{n+1} est 1 si $i \equiv 0 \pmod 4$ et 0 si $i \equiv 2 \pmod 4$. Pour $i \in [\![0, 2^n - 2]\!]$ les lettres de rang i de w_{n+1} sont celles de rang i de w_n donc d'après H_n la i-ème lettre du mot w_{n+1} est 1 si $i \equiv 0 \pmod 4$ et 0 si $i \equiv 2 \pmod 4$. Il reste donc à montrer le résultat pour $i \in [\![2^n, 2^{n+1} - 2]\!]$. Or pour $i \in [\![2^n, 2^{n+1} - 2]\!]$ la $(2^n - i)$-ème lettre de w_{n+1} et la $(2^{n+1} - i - 2)$-ème de w_{n+1} sont symétriques par rapport au 1 qui se trouve entre w_n et w'_n. Par définition ces lettres sont opposées (si l'une vaut 1 l'autre vaut 0 et inversement). De plus comme $n \geq 2$ on a $2^n - 2 \equiv 2 \pmod 4$. Ainsi si $2^n - i \equiv 0 \pmod 4$ alors $2^{n+1} - i - 2 = 2^n - 2 + 2^n - i \equiv 2 + 0 \equiv 2 \pmod 4$ et inversement. On en déduit donc que pour tout $i \in [\![2^n, 2^{n+1} - 2]\!]$ la i-ème lettre du mot w_{n+1} est 1 si $i \equiv 0 \pmod 4$ et 0 si $i \equiv 2 \pmod 4$. Donc H_{n+1} est vraie.
Le principe de récurrence assure que pour tout $n \geq 0$, $u_{4n} = 1$ et $u_{4n+2} = 0$. Il y a donc 2 suites

constantes dans le 2-noyau. On en déduit directement que $(u_{2n})_{n\geq 0} = 1010101010\cdots$. On a ainsi trouvé 3 suites différentes dans le 2-noyau, distinctes de la suite du pliage de papier elle-même. Cette dernière faisant également partie du 2-noyau il est entièrement déterminé. □

Le résultat suivant est un critère classique permettant de déterminer si une suite est automatique.

Théorème 1.1.1. [6, Theorem 6.6.2] Soit $k \geq 2$. La suite $\mathbf{u} = (u_n)_{n\geq 0}$ est k-automatique si et seulement si $\mathcal{N}_k(\mathbf{u})$ est fini.

En effet, d'après la Remarque 1.1.4 on a déjà le sens direct et la réciproque s'obtient en donnant une construction d'un automate qui engendre une suite dont le noyau est fini.

1.1.3 Caractérisation par morphisme

Il existe une autre caractérisation de l'automaticité à l'aide des suites engendrées par un morphisme.

Définition 1.1.6. [6, p. 9] On dira qu'un morphisme (ou une substitution) σ, défini sur un alphabet fini $\mathcal{A}$, est k-uniforme si l'image par σ de chaque lettre de $\mathcal{A}$ est un mot de longueur k.

Nous avons le résultat suivant, démontré par Cobham en 1972.

Théorème 1.1.2. [12] Une suite est k-automatique si et seulement si c'est l'image d'un point fixe d'un morphisme k-uniforme par un morphisme lettre à lettre.

Exemple 1.1.7. D'après la Définition 1.1.3, la suite de Thue–Morse est 2-uniforme, et par conséquent on retrouve directement grâce au théorème de Cobham, qu'il s'agit d'une suite 2-automatique.

1.1.4 Un critère de non-automaticité

Nous présentons ici un critère de non-automaticité du à Minsky et Papert [35] qui peut se révéler plus pratique que l'étude du noyau dans certains cas.

Proposition 1.1.1. [35] Soit $f : \mathbb{N} \to \mathbb{N}$ une fonction croissante. On définit $\pi_f(x) = \#\{n : f(n) \leq x\}$. Si $\lim_{x\to\infty} \pi_f(x)/x = 0$ et $\lim_{n\to\infty} f(n+1)/f(n) = 1$, alors la suite $u = \mathbf{1}_{f(\mathbb{N})}$ n'est pas automatique.

Exemple 1.1.8. On note $\mathbb{P}$ l'ensemble des nombres premiers. La suite $\mathbf{1}_{\mathbb{P}(\mathbb{N})}$ n'est pas automatique.
En effet, si on note $f : \mathbb{N} \longrightarrow \mathbb{N}$, avec $f(n) = n$-ième nombre premier, f est bien une fonction croissante et d'après le théorème des nombres premiers on sait que $\pi_f(x) \sim \dfrac{x}{\log(x)}$ $(x \to \infty)$ et que $f(n) \sim n\log(n)$ $(n \to \infty)$. Le critère de Minsky–Papert nous donne directement le fait que la suite $u = \mathbf{1}_{f(\mathbb{N})}$ n'est pas automatique.

Exemple 1.1.9. Si $P \in \mathbb{Q}[X]$ est un polynôme de degré $d \geq 2$ tel que $P(\mathbb{N}) \subset \mathbb{N}$, et P est strictement croissant sur $\mathbb{N}$, alors le critère de Minsky–Papert est satisfait, car $\pi_P(x)$ est de l'ordre de $x^{1/d}$. On en déduit que la suite $\mathbf{1}_{P(\mathbb{N})}$ n'est pas automatique.

1.2 Automates cellulaires

Soit $\mathcal{A}$ un alphabet fini munit de la topologie discrète. On munit $\mathcal{A}^{\mathbb{Z}}$ de la topologie produit. On appelle configuration, un élément de $\mathcal{A}^{\mathbb{Z}}$ que l'on notera $R = (R(m))_{m\in\mathbb{Z}}$. Pour une configuration R on définit le décalage à droite $\sigma : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ par $(\sigma(R))(m) = R(m+1)$.

Définition 1.2.1. [41] Un automate cellulaire avec mémoire d est une application $\Phi : (\mathcal{A}^d)^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ continue pour la topologie produit et qui commute avec le décalage à droite σ.
Autrement dit $\Phi : (\mathcal{A}^d)^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ est un automate cellulaire si Φ est continue pour la topologie produit et $\sigma \circ \Phi = \Phi \circ \sigma$ avec σ le décalage à droite.

Remarque 1.2.1. Lorsque $d = 1$ la définition précédente correspond à la définition classique des automates cellulaires sans mémoire.

Le théorème de Curtis–Hedlund–Lyndon [22] énonce que Φ est un automate cellulaire avec mémoire d si et seulement s'il y a une règle locale $\phi : (\mathcal{A}^d)^{l+r+1} \longrightarrow \mathcal{A}$ pour un certain $l \geq 0$ (le rayon à gauche de ϕ) et un certain $r \geq 0$ (le rayon à droite de ϕ), telle que pour tout $R \in \mathcal{A}^{\mathbb{Z}}$ et pour tout $m \in \mathbb{Z}$,

$$(\Phi(R))(m) = \phi(R(m-l), R(m-l+1), \ldots, R(m+r)). \tag{1.1}$$

Réciproquement, n'importe quelle règle locale ϕ définit un automate cellulaire Φ en utilisant la relation (1.1).
Dans le cas où $l = r = 1$ et $\mathcal{A} = \{0, 1\}$, les automates cellulaires sont appelés automates cellulaires élémentaires. Il en existe $2^8 = 256$.

Remarque 1.2.2. [41] L'ensemble $\mathcal{A}^{\mathbb{Z}}$ est muni de la topologie produit induite par la distance d définie pour tout $x, y \in \mathcal{A}^{\mathbb{Z}}$ par :

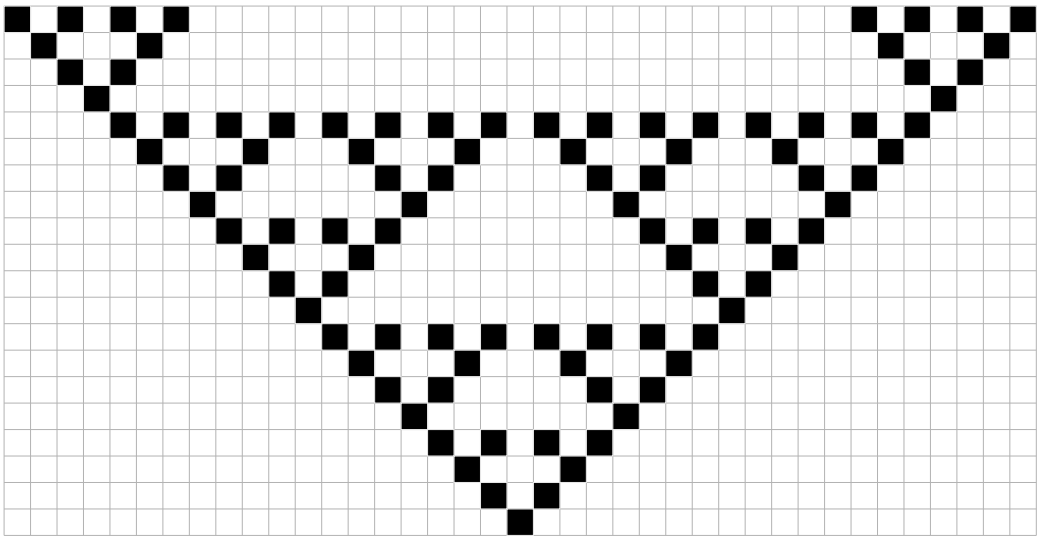
$$d(x,y) = \begin{cases} 2^{-\min\limits_{n\in\mathbb{Z}}\{|n|, x_n \neq y_n\}} & \text{si } x \neq y, \\ 0 & \text{si } x = y. \end{cases}$$

Définition 1.2.2. [41] Si $\Phi : (\mathcal{A}^d)^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ est un automate cellulaire avec mémoire d, alors un diagramme espace-temps pour Φ avec conditions initiales $R_0, \ldots, R_{d-1}$ est la suite $(R_n)_{n\geq 0}$ que l'on définit de manière récurrente par $R_n = \Phi(R_{n-d}, \ldots, R_{n-1})$ pour $n \geq d$.
La n-ième ligne R_n représente la configuration au temps n, et $R_n(m)$, l'entrée sur la ligne n et la colonne m du diagramme espace-temps, est l'état de la m-ième cellule au temps n.
Par conséquent dans un automate cellulaire avec mémoire d chaque ligne est déterminée par les d premières lignes.

On se place désormais dans le cas où $\mathcal{A}$ est le corps fini $\mathbb{F}_q$.

Définition 1.2.3. [41] On dit qu'un automate cellulaire $\Phi : (\mathbb{F}_q^d)^{\mathbb{Z}} \longrightarrow \mathbb{F}_q^{\mathbb{Z}}$ avec mémoire d est linéaire si Φ est une application $\mathbb{F}_q$-linéaire.
Le théorème de Curtis–Hedlund–Lyndon permet de montrer que l'automate cellulaire Φ avec mémoire d est linéaire si et seulement s'il existe des coefficients $f_{j,i} \in \mathbb{F}_q$ pour $-l \leq j \leq r$ et $0 \leq i \leq d-1$ tels que $(\Phi(R_0, \ldots, R_{d-1}))(m) = \sum\limits_{i=0}^{d-1} \sum\limits_{j=-l}^{r} f_{j,i} R_i(m+j)$ pour tout $R_0, \ldots, R_{d-1} \in \mathbb{F}_q^{\mathbb{Z}}$ et $m \in \mathbb{Z}$.

Exemple 1.2.1. [41] On se place sur $\mathbb{F}_2$ avec comme règle locale $\phi(a, b, c) = a + c$ et comme condition initiale R_0 où $R_0(0) = 1$ et $R_0(m) = 0$ pour tout $m \neq 0$. On définit ainsi un automate cellulaire avec mémoire 1. On peut représenter les lignes de l'automate cellulaire sous forme d'un diagramme en codant une case noire pour un 1 et une case blanche pour un 0. On prendra comme convention l'évolution du temps vers le haut.



La figure que l'on obtient présente une structure auto-similaire bien connue, appelée triangle de Sierpiński. Selon la règle locale, les diagrammes espace-temps que l'on obtient peuvent être très différents. Les 256 automates cellulaires élémentaires donnent déjà un bon aperçu des différentes structures que l'on peut observer. On trouvera une liste complète des 256 diagrammes espace-temps dans le célèbre livre de Wolfram [46, p. 55-56].

Chapitre 2

Construction de suites en colonnes d'automates cellulaires

Sommaire

Les résultats de cette partie ont fait l'objet d'une publication en 2018 [28]. Nous trouverons également dans ce chapitre des améliorations plus récentes, et de nouvelles constructions, en lien direct avec l'article de Rowland et Yassawi [41] qui fut le point de départ de cette partie. Le résultat établi par Rowland et Yassawi en 2015, relie les suites p-automatiques, où p est un nombre premier, aux automates cellulaires linéaires. Ils exposent une manière explicite de construire une suite p-automatique donnée comme colonne d'un automate cellulaire linéaire avec une configuration initiale finie. En 1993, Litow et Dumas [27] avaient déjà établi que pour un nombre premier p et $\mathbb{F}_q$ un corps fini de caractéristique p, chaque colonne d'un automate cellulaire linéaire sur $\mathbb{F}_q$, avec une configuration initiale finie, est une suite p-automatique. Le résultat de Rowland et Yassawi établit une réciproque à celui de Litow et Dumas. Nous avons donc une équivalence qui nous donne une caractérisation des suites p-automatiques et des automates cellulaires linéaires. De plus la preuve de Rowland et Yassawi est constructive car elle donne un algorithme qui permet à partir d'une suite p-automatique donnée de construire explicitement un automate cellulaire dans lequel la suite apparaît dans l'une des colonnes. Pour une suite donnée, il existe plusieurs automates qui permettent de la construire avec cette méthode mais pas nécessairement avec la même mémoire. Par exemple, dans le cas de la suite de Rudin–Shapiro, nous verrons qu'il est possible de construire un automate cellulaire avec une mémoire plus faible que celui obtenu par Rowland et Yassawi dans leur article.

De manière plus générale, la construction de suites définies sur un alphabet fini en colonne du diagramme espace-temps d'un automate cellulaire est un sujet encore très ouvert. D'autres constructions de suites non nécessairement automatiques avaient déjà été étudiées dans des travaux plus anciens, comme ceux de Fischer en 1965 [15] qui donne une première construction de la suite indicatrice des nombres

premiers par un automate cellulaire, résultat ensuite amélioré par Korec en 1997 [23] qui réduit considérablement le nombre d'états de l'automate, le faisant passer d'environ 30000 à seulement 11. En 1999, Mazoyer et Terrier [34] établissent différentes constructions géométriques de l'indicatrice de certaines fonctions croissantes ainsi que différentes propriétés de clôture sur cette classe de fonctions dites Fischer constructibles au sens de la construction de l'indicatrice des nombres premiers de Fischer. Nous nous intéresserons à ce type de constructions dans la deuxième partie de ce chapitre.

Nous commençons par introduire quelques définitions et notations qui nous serviront dans tout ce chapitre.
Soit $\mathcal{A}$ un ensemble fini contenant un élément noté 0, et soit $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ un automate cellulaire. On dit que Φ est 0-*stable* si $\Phi(0^{\mathbb{Z}}) = 0^{\mathbb{Z}}$.
Une configuration $x \in \mathcal{A}^{\mathbb{Z}}$ est dite finie si l'ensemble $\{k \in \mathbb{Z} : x_k \neq 0\}$ est fini. On notera $\mathcal{C}_0(\mathcal{A})$ l'ensemble des configurations finies de $\mathcal{A}^{\mathbb{Z}}$.
L'ensemble $\mathcal{S} = \{(\Phi^n(x)_0)_{n\geq 0} \in \mathcal{A}^{\mathbb{N}} : \Phi$ automate cellulaire 0-stable sur $\mathcal{A}^{\mathbb{Z}}$ et $x \in \mathcal{C}_0(\mathcal{A})\}$ sera l'objet principal de notre étude des automates cellulaires dans ce chapitre. On définit également $\mathcal{S}_d = \{(\Phi^n(x)_0)_{n\geq 0} \in \mathcal{A}^{\mathbb{N}} : \Phi$ automate cellulaire avec mémoire d sur $\mathcal{A}^{\mathbb{Z}}$ et $x \in \mathcal{C}_0(\mathcal{A})\}$. Pour commencer, nous allons introduire quelques outils algébriques.

2.1 Utilisation des séries de Laurent

Les automates cellulaires constituent un sujet d'étude très vaste. Il existe différentes manières de les aborder. Une possibilité est de les représenter par des séries formelles à deux variables qui permettent d'encoder le rang de la ligne et celui de la colonne dans le diagramme espace-temps. Nous présentons ici quelques résultats classiques, que l'on doit à Furstenberg [16], ainsi que le théorème de Christol [11] qui fait le lien entre les suites automatiques et les séries formelles algébriques.

Dans toute la suite, sauf indication contraire, p désigne un nombre premier et q une puissance de p. On note $\mathbb{F}_q$ le corps fini à q éléments. $\mathbb{F}_q[t], \mathbb{F}_q(t)$ et $\mathbb{F}_q((t))$ désignent respectivement l'ensemble des polynômes, des fractions rationnelles et des séries formelles de Laurent à coefficients dans $\mathbb{F}_q$. Les éléments de $\mathbb{F}_q((t))$ sont les expressions de la forme $F(t) = \sum_{n\geq n_0} u_n t^n$ où $u_n \in \mathbb{F}_q$ et $n_0 \in \mathbb{Z}$. On peut aussi définir les polynômes, les fractions rationnelles et les séries formelles de Laurent en plusieurs variables.
Si $E(t,x) = \sum_{n\geq n_0} \sum_{m\in\mathbb{Z}} a_{n,m} t^n x^m$ désigne une série formelle de Laurent en deux variables, sa diagonale est la série formelle de Laurent :

$$\sum_{n\geq n_0} a_{n,n} t^n$$

en une seule variable.
De manière similaire on définit la m-ième colonne de $E(t,x)$ par :

$$\sum_{n\geq n_0} a_{n,m} t^n$$

Une série de Laurent $F(t)$ est dite algébrique sur $\mathbb{F}_q(t)$ s'il existe un polynôme non-nul $P(t,x) \in \mathbb{F}_q[t,x]$ tel que $P(t,F(t)) = 0$. On dit aussi que $E(t,x)$ est une série rationnelle s'il existe deux polynômes $Q(t,x)$ et $P(t,x)$ tels que $P(t,x)E(t,x) = Q(t,x)$.
Nous rappelons les résultats suivants sans démonstration, et renvoyons aux références pour plus de précisions.

Théorème 2.1.1. [41] Pour qu'une série de Laurent $F(t) \in \mathbb{F}_q((t))$ soit algébrique sur $\mathbb{F}_q(t)$, il est nécessaire et suffisant qu'elle soit la diagonale d'une série rationnelle de Laurent $E(t,x) \in \mathbb{F}_q((x))((t))$.

Proposition 2.1.1. [16, 41] Supposons que la série de Laurent $F(t) = \sum_{n\geq n_0} c_n t^n \in \mathbb{F}_q((t))$ est algébrique sur $\mathbb{F}_q(t)$. Alors il existe $r^* \geq n_0, m \geq 0$, et un polynôme

$$P^*(t,x) = {A_0}^*(t)x + {A_1}^*(t)x^p + \cdots + {A_m}^*(t)x^{p^m} + B^*(t),$$

avec ${A_i}^*(t), B^*(t) \in \mathbb{F}_q[t]$ et ${A_0}^*(t)$ non-divisible par t, tels que

$$F(t) = R^*(t) + t^{r^*} G^*(t), R^*(t) = \sum_{n=n_0}^{r^*-1} c_n t^n, \text{ et } P^*(t, G^*(t)) = 0.$$

Proposition 2.1.2. [41] Supposons que $F(t) = \sum_{n\geq 0} u_n t^n \in \mathbb{F}_q((t))$ est algébrique sur $\mathbb{F}_q(t)$. Alors il existe $G(t) \in \mathbb{F}_q((t))$ et $P(t,x) \in \mathbb{F}_q[t,x]$ de la forme

$$P(t,x) = A_0(t)x + A_1(t)x^p + \cdots + A_m(t)x^{p^m} + B(t),$$

avec $A_i(t), B(t) \in \mathbb{F}_q[t]$ pour $0 \leq i \leq m$ tels que

$$F(t) = R(t) + t^r G(t) \quad \text{pour un certain} \quad r \geq 0 \quad \text{et} \quad R(t) \in \mathbb{F}_q[t], \tag{2.1}$$
$$G(0) = 0, \tag{2.2}$$
$$A_0(0) \neq 0, \tag{2.3}$$
$$B(0) = A_i(0) = 0 \quad \text{pour1} \leq i \leq m, \quad \text{et} \tag{2.4}$$
$$P(t, G(t)) = 0. \tag{2.5}$$

Les résultats précédents permettent de démontrer la proposition suivante, que l'on doit à Furstenberg, et qui joue un rôle central dans la preuve de Rowland et Yassawi.

Proposition 2.1.3. [16, 41] Notons $P^{(0,1)}$ la dérivée de la fonction P par rapport à la seconde variable. Supposons que la série $G(t) = \sum_{n\geq 1} c_n t^n \in \mathbb{F}_q((t))$ avec $G(0) = 0$ satisfait $P(t, G(t)) = 0$, où $P(t,x) \in \mathbb{F}_q[t,x]$ et $P^{(0,1)}(0,0) \neq 0$. Alors $G(t)$ est la diagonale de l'unique développement en série de

$$\frac{x^2 P^{(0,1)}(tx, x)}{P(tx, x)}.$$

Remarque 2.1.1. La détermination d'un polynôme P satisfaisant les conditions de la Proposition 2.1.3 pour une certaine série génératrice G, permet à l'aide du développement en série de $\frac{x^2 P^{(0,1)}(tx,x)}{P(tx,x)}$ de construire de manière explicite un automate cellulaire dans lequel la suite définissant la série génératrice G apparaît dans l'une des colonnes. Le théorème suivant, qui est dû à Christol, garantit l'existence d'un tel polynôme pour une suite q-automatique donnée.

Théorème 2.1.2. [6, 11, 41] Une suite $(u_n)_{n\geq 0}$ est q-automatique si et seulement si $F(t) = \sum_{n\geq 0} u_n t^n$ est algébrique sur $\mathbb{F}_q(t)$.

Exemple 2.1.1. [6, Example 12.1.5] Soit $(c_n)_{n\geq 0}$ la suite de Cantor, définie par :

$$c_n = \begin{cases} 1 & \text{si } (n)_3 \text{ contient seulement des 0 et des 2 ;} \\ 0 & \text{si } (n)_3 \text{ contient au moins un 1.} \end{cases}$$

On a pour tout $n \in \mathbb{N}$ $c_{3n} = c_n = c_{3n+2}$ et $c_{3n+1} = 0$. Ainsi

$$\begin{aligned} F(t) &= \sum_{n\geq 0} c_n t^n \\ &= \sum_{n\geq 0} c_{3n} t^{3n} + \sum_{n\geq 0} c_{3n+1} t^{3n+1} + \sum_{n\geq 0} c_{3n+2} t^{3n+2} \\ &= \sum_{n\geq 0} c_n t^{3n} + t^2 \sum_{n\geq 0} c_n t^{3n} \\ &= F(t^3) + t^2 F(t^3) \\ &= (1+t^2) F(t)^3 \end{aligned}$$

La série $F(t)$ est algébrique sur $\mathbb{F}_3(t)$ donc d'après le théorème de Christol $(c_n)_{n\geq 0}$ est 3-automatique.

Remarque 2.1.2. La démonstration du théorème de Christol assure que pour une suite q-automatique dont le q-noyau est de taille d, il existe un polynôme annulateur de sa série génératrice, de degré au plus q^d. Cependant, dans la pratique, cette majoration n'est pas optimale.

2.2 Le cas des suites p-automatiques

2.2.1 Résultat principal, principe de la méthode

Désormais nous avons tous les outils nécessaires pour le résultat principal de Rowland et Yassawi [41].

Théorème 2.2.1. [41] Une suite d'éléments de $\mathbb{F}_q$ est p-automatique si et seulement si c'est la colonne d'un diagramme espace-temps d'un automate cellulaire, avec mémoire, sur $\mathbb{F}_q$, et dont les conditions initiales sont périodiques à partir d'un certain rang dans les deux directions.

Remarque 2.2.1. L'ensemble des suites p-automatiques constitue donc une première famille de suites de l'ensemble $\mathcal{S}$, que nous avons défini au début du chapitre. Il s'ensuit qu'une suite p-automatique construite par un automate cellulaire de mémoire d est un élément de $\mathcal{S}_d$

Le résultat suivant permet d'étendre le résultat de Rowland et Yassawi sur les suites p-automatiques avec p premier, aux suites q-automatiques dans le cas où q est une puissance d'un nombre premier.

Théorème 2.2.2. [6, Theorem 6.6.4] Pour tout $m \geq 1$, une suite est k-automatique si et seulement si elle est k^m-automatique.

Démonstration. Si $(u_n)_{n\geq 0}$ est une suite k-automatique, alors d'après le Théorème 1.1.6 c'est l'image d'un point fixe d'un certain morphisme Φ lettre à lettre et k-uniforme. Il suffit alors de considérer le morphisme $\gamma = \Phi^m$ pour en déduire que $(u_n)_{n\geq 0}$ est k^m-automatique.

La réciproque se démontre avec des résultats sur les langages réguliers que nous ne développerons pas ici. Nous renvoyer à [6] pour plus de détails. □

Nous représenterons le diagramme espace-temps d'un automate cellulaire par une série à deux variables. Si $a_{n,m}$ représente l'entrée du diagramme espace-temps pour la ligne $n \in \mathbb{N}$ et la colonne $m \in \mathbb{Z}$, alors la série $E(t,x) = \sum_{n\geq 0}\sum_{m\in\mathbb{Z}} a_{n,m}t^n x^m$ encode l'évolution de l'automate cellulaire tout entier à partir de la condition initiale R_0. On identifie la n-ième ligne R_n du diagramme espace-temps par la série $R_n(x) = \sum_{m\in\mathbb{Z}} a_{n,m}x^m$ qui est le coefficient de t^n dans $E(t,x) = \sum_{n\geq 0} R_n(x)t^n$.
La preuve du Théorème 2.2.1 est constructive car elle nous donne un moyen de construire l'automate cellulaire à partir de la suite automatique. Il suffit pour cela de trouver un polynôme annulateur $P(t,x)$ de la série génératrice de la suite automatique qui remplit les conditions de la Proposition 2.1.3. Il reste ensuite à calculer les coefficients $R_n(x)$ qui apparaissent dans le développement en série de $\dfrac{P^{(0,1)}(t,x)}{P(t,x)}$.
La procédure donnée par Rowland et Yassawi [41] repose sur la démonstration du théorème de Christol qui assure que pour une suite q-automatique dont le q-noyau est de taille d, il existe un polynôme annulateur de la série génératrice, de degré au plus q^d en x. Pour fixer les idées, notons $(u_n)_{n\geq 0}$ la suite p-automatique que l'on cherche à obtenir en colonne d'un automate cellulaire et $F(t) = \sum_{n\geq 0} u_n t^n$ sa série génératrice. Si son q-noyau contient d éléments, notons pour $1 \leq i \leq d$, $F_i(t)$ les fonctions génératrices associées aux d suites du q-noyau. Comme la suite elle-même est toujours un élément du noyau, on peut considérer par exemple que $F_1(t) = F(t)$. On exprime chaque $F_i(t)$ comme une combinaison linéaire des fonctions $F_1(t^q), \ldots, F_d(t^q)$ et on répète d fois la procédure afin d'exprimer chaque $F_j(t^{q^i})$, pour $1 \leq j \leq d$ et $0 \leq i \leq d$, comme une combinaison linéaire, dans le corps $\mathbb{F}_q(x)$, de $F_1(t^{q^{d+1}}), \ldots, F_d(t^{q^{d+1}})$. On obtient alors une relation linéaire entre $F_1(t), \ldots, F_1(t^{q^d})$ qui donne un polynôme annulateur pour $F_1(t) = F(t)$. Il est souvent nécessaire ensuite de le modifier par une transformation linéaire pour qu'il satisfasse aux conditions de la Proposition 2.1.3, ce qui peut se faire de manière mécanique.

Cependant, dans la pratique cette procédure n'est pas optimale. Selon les propriétés de la suite ou la forme du q-noyau, il est possible d'obtenir un polynôme annulateur de la série génératrice plus rapidement et de degré plus faible.

2.2.2 Exemples

Nous allons traiter ici plusieurs exemples de suites p-automatiques connues. Nous commençons par deux exemples de suites automatiques qui n'ont pas été traitées par Rowland et Yassawi, à savoir la suite 2-automatique du pliage de papier, définie au Chapitre 1 (Exemple 1.1.2), et la suite 3-automatique de Cantor (Exemple 2.1.1), pour lesquelles l'obtention d'un polynôme annulateur est relativement simple. Puis nous donnerons l'exemple de la suite 2-automatique de Rudin–Shapiro qui est traitée par Rowland et Yassawi dans leur article avec leur procédure, où ils montrent qu'il s'agit d'un élément de $\mathcal{S}_{20}$. Nous donnerons une autre construction qui permet de montrer qu'il s'agit en fait d'un élément de $\mathcal{S}_9$, et qui permet de traiter toutes les suites généralisées de Rudin–Shapiro introduites au Chapitre 1. Nous expliciterons l'automate cellulaire que l'on obtient pour la suite généralisée de Rudin–Shapiro sur l'alphabet $\{0, 1, 2\}$.

2.2.2.1 Suite du pliage de papier

Exemple 2.2.1. Soit $(u_n)_{n\geq 0}$ la suite régulière du pliage de papier. Cette suite étant 2-automatique et ayant un noyau de taille 4, il est donc possible de trouver un polynôme annulateur de la série génératrice $P(t, x)$ de degré au plus $2^4 = 16$ en x.
Nous allons voir qu'en fait, on peut trouver un polynôme annulateur de degré 2 en x. La suite régulière du pliage de papier n'est pas ultimement périodique (voir [6, Theorem 6.5.3]) et par conséquent sa série génératrice ne peut pas être une fraction rationnelle, autrement dit, on ne peut pas avoir de polynôme annulateur de degré 1 en x. En particulier, si l'on trouve un polynôme annulateur de degré 2 en x, il sera donc de degré minimal.
D'après le calcul du 2-noyau, pour tout $n \in \mathbb{N}$ on a $u_{4n} = 1$ et $u_{4n+2} = 0$. De plus, la suite (u_{2n+1}) fait partie du 2-noyau et n'est ni la suite identiquement égale à 1, ni la suite identiquement égale à 0, ni la suite périodique $101010\cdots$. On en déduit donc que pour tout $n \in \mathbb{N}$ on a $u_{2n+1} = u_n$. Ainsi, comme on travaille dans le corps fini $\mathbb{F}_2$ on a :

$$\begin{aligned} x = F(t) &= \sum_{n\geq 0} u_n t^n \\ &= \sum_{n\geq 0} u_{2n} t^{2n} + \sum_{n\geq 0} u_{2n+1} t^{2n+1} \\ &= \sum_{n\geq 0} u_{4n} t^{4n} + \sum_{n\geq 0} u_{4n+2} t^{4n+2} + t \sum_{n\geq 0} u_n t^{2n} \\ &= \sum_{n\geq 0} t^{4n} + tF(t^2) \\ &= \frac{1}{1-t^4} + tF(t)^2 \\ &= \frac{1}{1+t^4} + tF(t)^2 \end{aligned}$$

D'où $1 + (1 + t^4)x + (t + t^5)x^2 = 0$. On obtient un polynôme annulateur de la série $F(t)$. On va maintenant utiliser la Proposition 2.1.2. Pour cela nous allons devoir modifier notre polynôme car ici on a $F(0) = 1$. On effectue la transformation $x \mapsto 1 + t + tx$ dans notre équation. Ainsi, comme les calculs se font dans le corps $\mathbb{F}_2$, on obtient

$$\begin{aligned}&1+(1+t^4)(1+t+tx)+(t+t^5)(1+t^2+t^2x^2)\\&=1+1+t+tx+t^4+t^5+t^5x+t+t^3+t^3x^2+t^5+t^7+t^7x^2\\&=(t^3+t^4+t^7)+(t+t^5)x+(t^3+t^7)x^2.\end{aligned}$$

On peut diviser tous les termes par t. On pose alors $P(t,x)=(t^2+t^3+t^6)+(1+t^4)x+(t^2+t^6)x^2$, qui satisfait $P(t,G(t))=0$ avec $G(t)=\sum_{n\geq 1}u_{n+1}t^n$ qui satisfait $G(0)=0$ et $F(t)=1+t+tG(t)$. De plus, $P^{(0,1)}(t,x)=1+t^4$ donc en particulier $P^{(0,1)}(0,0)\neq 0$.
On peut maintenant appliquer la Proposition 2.1.3 à la série $G(t)$. Ainsi, pour tout $n\geq 1$, u_{n+1} est le coefficient de x^{-2} dans $R_n(x)$ où $R_n(x)$ est le coefficient de t^n dans la série

$$\frac{P^{(0,1)}(t,x)}{P(t,x)}=\sum_{n\geq 0}R_n(x)t^n.$$

En réordonnant le polynôme $P(t,x)$ selon les puissances de t on a

$$P(t,x)=x+(1+x^2)t^2+t^3+xt^4+(1+x^2)t^6,$$

d'où l'on déduit la relation de récurrence

$$R_n(x)=\left(\frac{1}{x}+x\right)R_{n-2}(x)+\frac{1}{x}R_{n-3}(x)+R_{n-4}(x)+\left(\frac{1}{x}+x\right)R_{n-6}(x),$$

valable pour tout $n\geq 7$.
Finalement, on a construit à partir de la suite 2-automatique du pliage régulier de papier une relation de récurrence qui donne une règle permettant d'engendrer un automate cellulaire Φ avec mémoire 6. Nous pouvons étendre la mémoire à $d+r+1=6+1+1=8$ sans introduire de dépendance sur les $r+1=2$ premières lignes. On pose $R_{-1}(x)=u_0x^{-2}=x^{-2}$ et $R_0(x)=u_1x^{-2}=x^{-2}$. La suite $(u_n)_{n\geq 0}$ apparaît alors, en lisant verticalement vers le haut, dans la colonne -2 du diagramme espace-temps de Φ qui commence par les conditions initiales $R_{-1},\ldots,R_6$.

La Figure 2.1 représente les premières lignes de l'automate cellulaire. La colonne avec les cases grises est celle de rang -2 où apparaît la suite régulière du pliage de papier. Les cases noires représentent les 1 et les cases blanches ou grises les 0.

Remarque 2.2.2. Remarquons que la règle qui définit l'automate cellulaire peut s'écrire pour tous $m\in\mathbb{Z}$ et $n\geq 1$:

$$\begin{aligned}\phi(m,n+6)=&\phi(m-1,n+4)+\phi(m+1,n+4)+\phi(m-1,n+3)\\&+\phi(m,n+2)+\phi(m-1,n)+\phi(m+1,n).\end{aligned}$$

2.2.2.2 Suite de Cantor

Exemple 2.2.2. Considérons la suite 3-automatique $(c_n)_{n\geq 0}$ de l'Exemple 2.1.1. Nous avions montré que $x=F(t)=\sum_{n\geq 0}c_nt^n$ satisfait $(1+t^2)x^3-x=0$. On effectue la transformation $x\mapsto 1+tx$. On pose alors $P(t,x)=t-x+(t^2+t^4)x^3$ qui est un polynôme annulateur de la série $G(t)=\sum_{n\geq 1}c_{n+1}t^n$ qui satisfait $G(0)=0$ et $F(t)=1+tG(t)$. De plus $P^{(0,1)}(t,x)=-1$ donc en particulier $P^{(0,1)}(0,0)\neq 0$. On peut donc appliquer la Proposition 2.1.3 à la série $G(t)$.
Ainsi, pour tout $n\geq 1$, u_{n+1} est le coefficient de x^{-2} dans $R_n(x)$ où $R_n(x)$ est le coefficient de t^n dans la série

$$\frac{P^{(0,1)}(t,x)}{P(t,x)}=\sum_{n\geq 0}R_n(x)t^n.$$

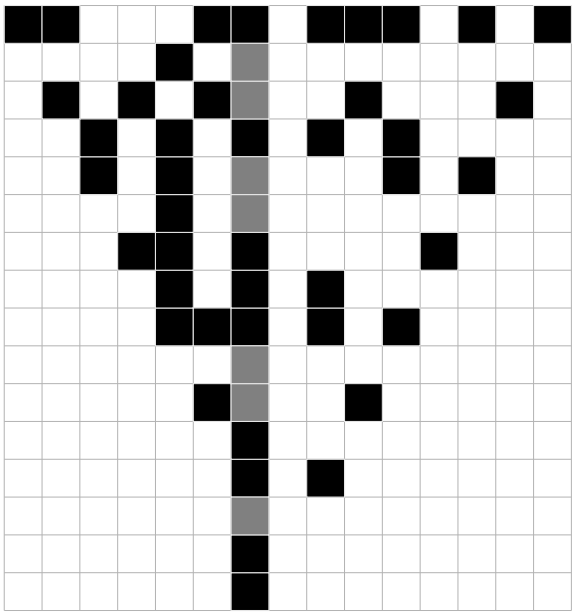


FIGURE 2.1 – Automate cellulaire contenant la suite 2-automatique de pliage de papier.

On en déduit la relation de récurrence $R_n(x) = \frac{1}{x}R_{n-1}(x) + x^2R_{n-2}(x) + x^2R_{n-4}(x)$, valable pour tout $n \geq 5$. On pose $R_{-1}(x) = c_0x^{-2} = x^{-2}$ et $R_0(x) = c_1x^{-2} = 0$ et on définit ainsi un automate cellulaire avec mémoire 6 où la suite $(c_n)_{n\geq 0}$ apparaît dans la colonne -2.

La figure représente les premières lignes de l'automate cellulaire. La colonne avec les cases grises est celle de rang -2 où apparaît la suite $(c_n)_{n\geq 0}$. Les cases rouges représentent les 2, les cases noires les 1 et les cases blanches ou grises les 0.

Remarque 2.2.3. Comme précédemment on peut définir la règle qui génère l'automate cellulaire pour tous $m \in \mathbb{Z}$ et $n \geq 1$ par :

$$\phi(m, n+4) = \phi(m-1, n+3) + \phi(m+2, n+2) + \phi(m+2, n).$$

2.2.2.3 Suites généralisées de Rudin–Shapiro

Exemple 2.2.3. [41] Nous présentons ici le cas de la suite de Rudin–Shapiro traité explicitement par Rowland et Yassawi. Nous avons déjà vu qu'il s'agit d'une suite 2-automatique dont le noyau comporte 4 éléments (Exemple 1.1.5). Notons $F_1(t), F_2(t), F_3(t)$, et $F_4(t)$ les séries génératrices associées aux 4 suites du noyau et considérons que $F_1(t)$ est celle associée à la suite elle-même. Il suffit d'écrire chaque $F(t^{2^i})$ pour $0 \leq i \leq 4$ comme une combinaison linéaire des $F_j(t^{32})$ pour $1 \leq j \leq 4$, ce qui permet ensuite d'avoir un polynôme annulateur pour $x = F_1(t) = F(t)$. Après modification, afin de satisfaire aux conditions de la Proposition 2.1.3, le polynôme annulateur qu'ils obtiennent est

$$P(t, x) = (t^2 + t^5 + t^7 + t^9 + t^{11}) + x + (t + t^4)x^2 + (t^9 + t^{11} + t^{13} + t^{15})x^4$$

et qui satisfait, pour $G(t) = \sum_{n\geq 1} u_{n+4}t^n$, $P(t, G(t)) = 0$.

Ainsi, pour tout $n \geq 1$, u_{n+4} est le coefficient de x^{-2} dans $R_n(x)$ où $R_n(x)$ est le coefficient de t^n dans la série

$$\frac{P^{(0,1)}(t, x)}{P(t, x)} = \sum_{n\geq 0} R_n(x)t^n.$$

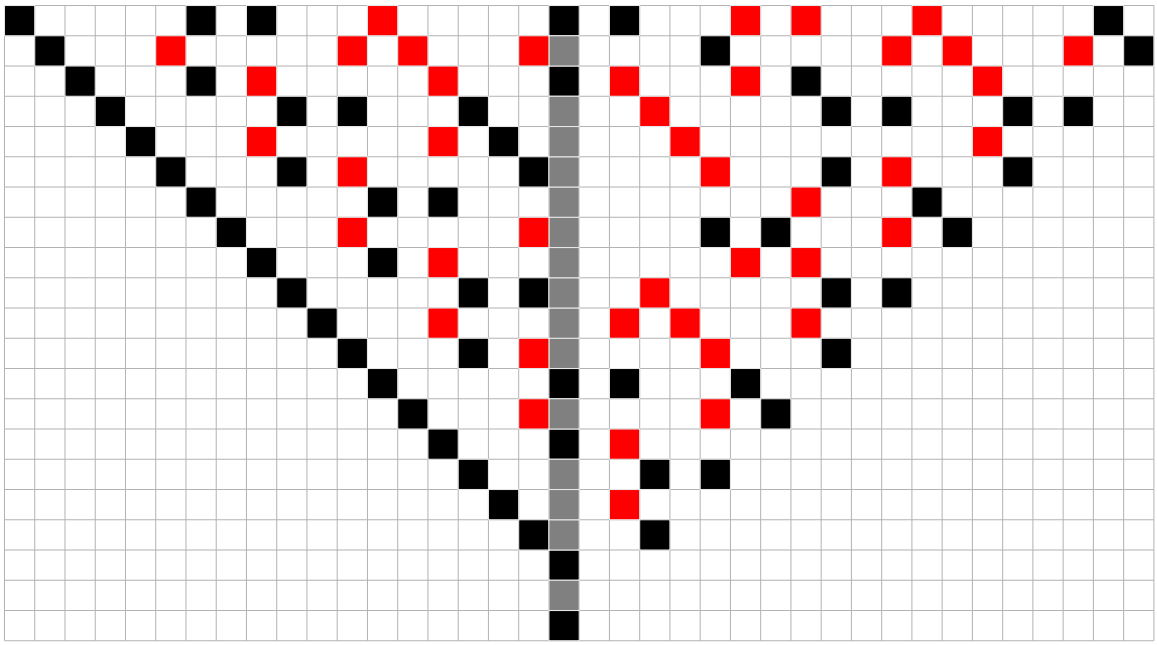


FIGURE 2.2 – Automate cellulaire contenant la suite 3-automatique de Cantor.

On en déduit la relation de récurrence

$$\begin{aligned} R_n(x) =& xR_{n-1}(x) + \frac{1}{x}R_{n-2}(x) + xR_{n-4}(x) + \frac{1}{x}R_{n-5}(x) + \frac{1}{x}R_{n-7}(x) \\ &+ \left(\frac{1}{x} + x^3\right) R_{n-9}(x) + \left(\frac{1}{x} + x^3\right) R_{n-11}(x) + x^3 R_{n-13}(x) + x^3 R_{n-15}(x), \end{aligned}$$

valable pour tout $n \geq 16$. On pose $R_{-4}(x) = u_0 x^{-2} = 0$, $R_{-3}(x) = u_1 x^{-2} = 0$, $R_{-2}(x) = u_2 x^{-2} = 0$, $R_{-1}(x) = u_3 x^{-2} = x^{-2}$ et $R_0(x) = u_4 x^{-2} = 0$ et on définit ainsi un automate cellulaire avec mémoire 20 où la suite de Rudin–Shapiro apparaît dans la colonne -2.

Remarque 2.2.4. De la même manière on peut définir la règle qui génère l'automate cellulaire pour tous $m \in \mathbb{Z}$ et $n \geq 1$ par :

$$\begin{aligned} \phi(m, n+15) = &\phi(m+1, n+14) + \phi(m-1, n+13) + \phi(m+1, n+11) \\ &+ \phi(m-1, n+10) + \phi(m-1, n+8) + \phi(m-1, n+6) \\ &+ \phi(m+3, n+6) + \phi(m-1, n+4) + \phi(m+3, n+4) \\ &+ \phi(m+3, n+2) + \phi(m+3, n). \end{aligned}$$

Nous rappelons la définition des suites généralisées de Rudin–Shapiro introduites au Chapitre 1 :

Définition 2.2.1. Soit p un nombre premier. La suite $(a(n))_{n\geq 0}$ définie sur l'alphabet $\{0, 1, \ldots, p-1\}$ de manière récursive par

$$a(pn + j) = (a(n) + jn) \bmod p \quad \text{pour } 0 \leq j \leq p-1,\ n \geq 1,$$

où les valeurs de $a(0), \ldots, a(p-1)$ peuvent être choisies arbitrairement, est une *suite généralisée de Rudin–Shapiro*.

Remarque 2.2.5. Nous prendrons ici $a(0) = \cdots = a(p-1) = 0$, de sorte que pour $p = 2$ on retrouve la suite classique de Rudin–Shapiro.

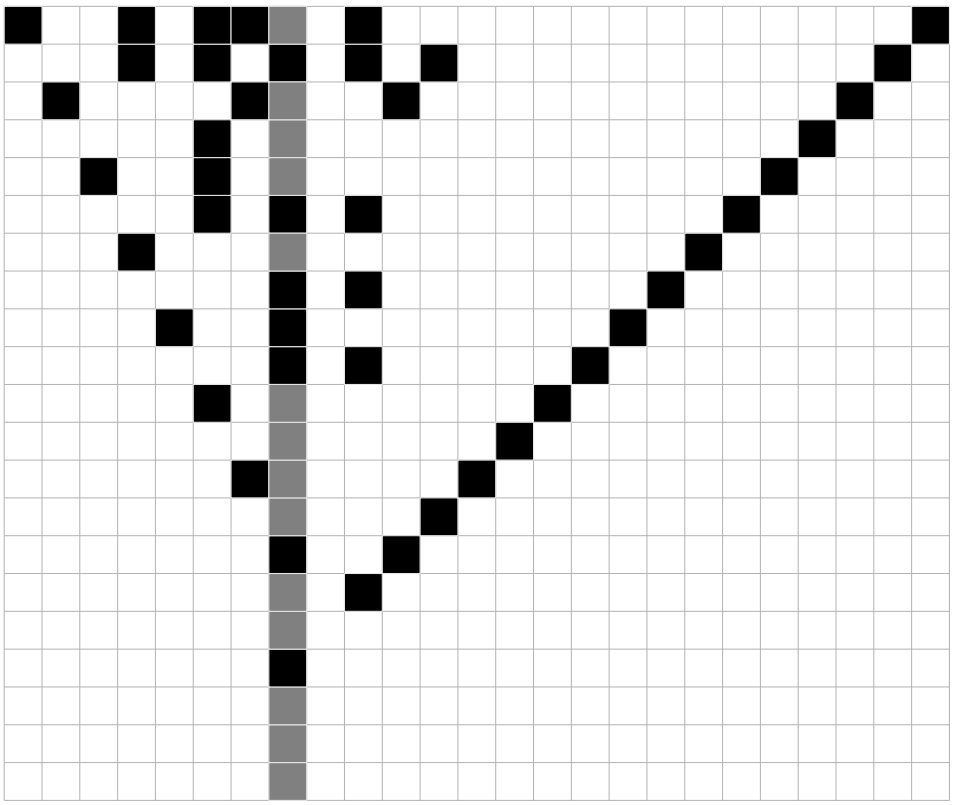


FIGURE 2.3 – Automate cellulaire avec mémoire 20 contenant la suite 2-automatique de Rudin–Shapiro.

Soit p un nombre premier quelconque et $(a(n))_{n\geq 0}$ une suite généralisée de Rudin–Shapiro. On note $F(t) = \sum_{n\geq 0} a(n)t^n$ sa série génératrice. On a alors,

$$\begin{aligned}
F(t) &= \sum_{n\geq 0} a(n)t^n \\
&= \sum_{j=0}^{p-1}\sum_{n\geq 0} a(pn+j)t^{pn+j} \\
&= \sum_{j=0}^{p-1} t^j \sum_{n\geq 0} (a(n)+jn \bmod p)t^{pn} \\
&= \sum_{j=0}^{p-1} t^j F(t^p) + \sum_{j=0}^{p-1} t^j \sum_{n\geq 0} (jn \bmod p)t^{pn} \\
&= \sum_{j=0}^{p-1} t^j F(t)^p + \sum_{j=0}^{p-1} t^j \sum_{i=0}^{p-1}\sum_{n\geq 0} (j(pn+i) \bmod p)t^{p(pn+i)} \\
&= \sum_{j=0}^{p-1} t^j F(t)^p + \sum_{j=0}^{p-1} jt^j \sum_{i=0}^{p-1} it^{pi} \sum_{n\geq 0} t^{p^2 n}.
\end{aligned}$$

En multipliant de chaque côté de l'égalité par $1-t^{p^2}$, on obtient

$$(1-t^{p^2})F(t) = (1-t^{p^2})\sum_{j=0}^{p-1} t^j F(t)^p + \sum_{j=0}^{p-1} jt^j \sum_{i=0}^{p-1} it^{pi}.$$

On pose

$$P(t,x) = \sum_{j=0}^{p-1} jt^j \sum_{i=0}^{p-1} it^{pi} + (t^{p^2}-1)x + (1-t^{p^2})\sum_{j=0}^{p-1} t^j x^p,$$

qui est alors un polynôme annulateur pour $x = F(t)$. En effectuant la transformation $x \mapsto tx$, on obtient

$$P(t,x) = \sum_{j=1}^{p-1} jt^{j-1} \sum_{i=1}^{p-1} it^{pi} + (t^{p^2}-1)x + (t^{p-1}-t^{p(p+1)-1})\sum_{j=0}^{p-1} t^j x^p,$$

qui est un polynôme annulateur de la série $G(t) = \sum_{n\geq 1} a(n+1)t^n$, qui satisfait $G(0) = 0$ et $F(t) = tG(t)$.

Remarquons que $P^{(0,1)}(t,x) = t^{p^2}-1$ et donc en particulier $P^{(0,1)}(0,0) \neq 0$. On peut alors appliquer la Proposition 2.1.3 à la série $G(t)$.

Ainsi, pour tout $n \geq 1$, $a(n+1)$ est le coefficient de x^{-2} dans $R_n(x)$ où $R_n(x)$ est le coefficient de t^n dans la série

$$\frac{P^{(0,1)}(t,x)}{P(t,x)} = \sum_{n\geq 0} R_n(x)t^n.$$

Pour la variable t, le polynôme $P(t,x)$ est de degré $p(p+1)-1+p-1 = p^2+2p-2$. En posant $R_{-1}(x) = a(0)x^{-2} = 0$ et $R_0(x) = a(1)x^{-2} = 0$, la suite $(R_n(x))_{n\geq -1}$ définit un automate cellulaire avec mémoire $p^2+2p-2+2+1 = (p+1)^2$ et dans lequel la suite $(a(n))_{n\geq 0}$ apparaît dans la colonne -2.

Exemple 2.2.4. Pour $p = 2$, qui correspond à la suite de Rudin–Shapiro classique, on obtient

$$P(t,x) = t^2 + (t^4-1)x + (t-t^5)(1+t)x^2 = t^2 + (t^4+1)x + (t+t^2+t^5+t^6)x^2.$$

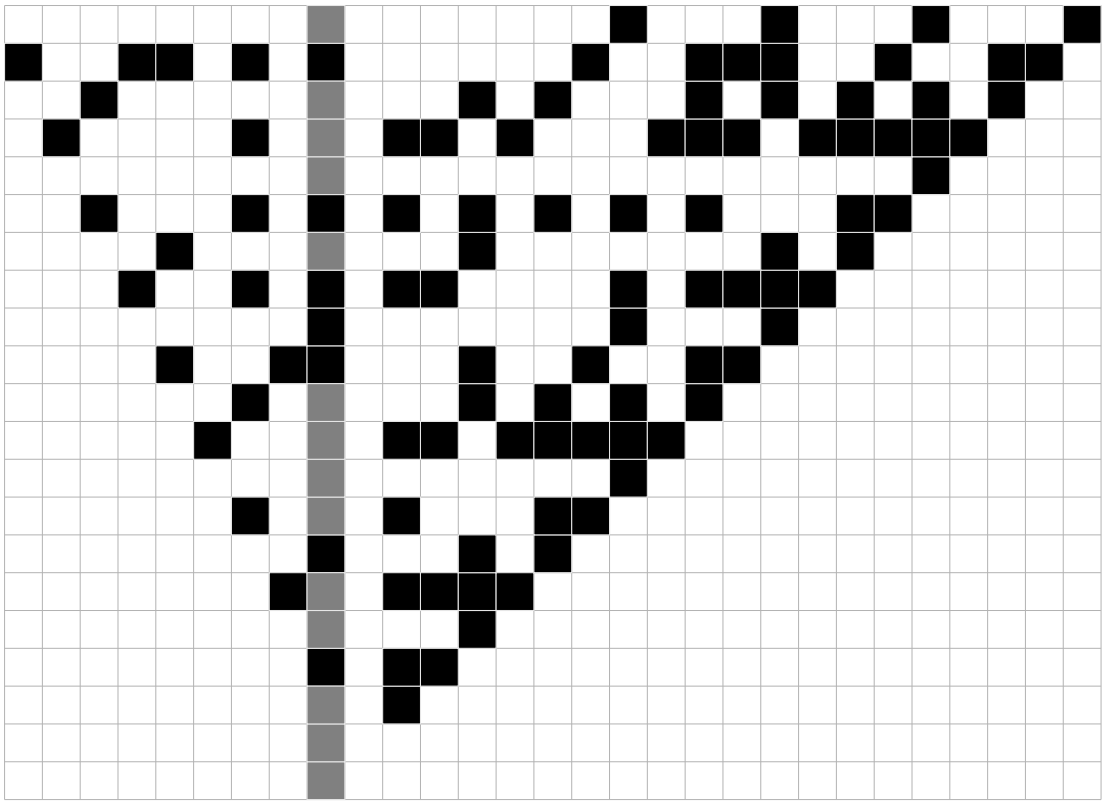


FIGURE 2.4 – Automate cellulaire avec mémoire 9 contenant la suite 2-automatique de Rudin–Shapiro.

En réordonnant le polynôme selon les puissances de t, on en déduit la relation de récurrence

$$R_n(x) = xR_{n-1}(x) + \left(\frac{1}{x} + x\right) R_{n-2}(x) + R_{n-4}(x) + xR_{n-5}(x) + xR_{n-6}(x),$$

valable pour tout $n \geq 7$. On pose $R_{-1}(x) = 0$ et $R_0(x) = 0$ et on obtient alors un automate cellulaire avec mémoire 9, dans lequel la suite de Rudin–Shapiro apparaît dans la colonne -2 (voir Figure 2.4).

Remarque 2.2.6. Nous obtenons une règle différente que l'on peut définir pour tous $m \in \mathbb{Z}$ et $n \geq 1$ par :

$$\begin{aligned}\phi(m, n+6) = \phi(m+1, n+5) + \phi(m-1, n+4) + \phi(m+1, n+4) \\ + \phi(m, n+2) + \phi(m+1, n+1) + \phi(m+1, n).\end{aligned}$$

Remarque 2.2.7. L'automate cellulaire que l'on obtient est assez différent de celui de Rowland et Yassawi. On constate que pour le polynôme annulateur le degré en t est passé de 15 à 6 et celui en x de 4 à 2. Le polynôme obtenu par Rowland et Yassawi n'était donc pas le polynôme minimal parmi les polynômes annulateurs de la série génératrice. De plus, nous avons ici un automate avec mémoire 9 au lieu de 20. Notons que le polynôme annulateur que nous obtenons est de degré minimal en x mais pas nécessairement en t.

Exemple 2.2.5. Pour $p = 3$, on a

$$P(t, x) = t^3 + 2t^4 + 2t^6 + t^7 + (t^9 - 1)x + (t^2 + t^3 + t^4 + 2t^{11} + 2t^{12} + 2t^{13})x^3.$$

En réordonnant le polynôme selon les puissances de t, on en déduit la relation de récurrence

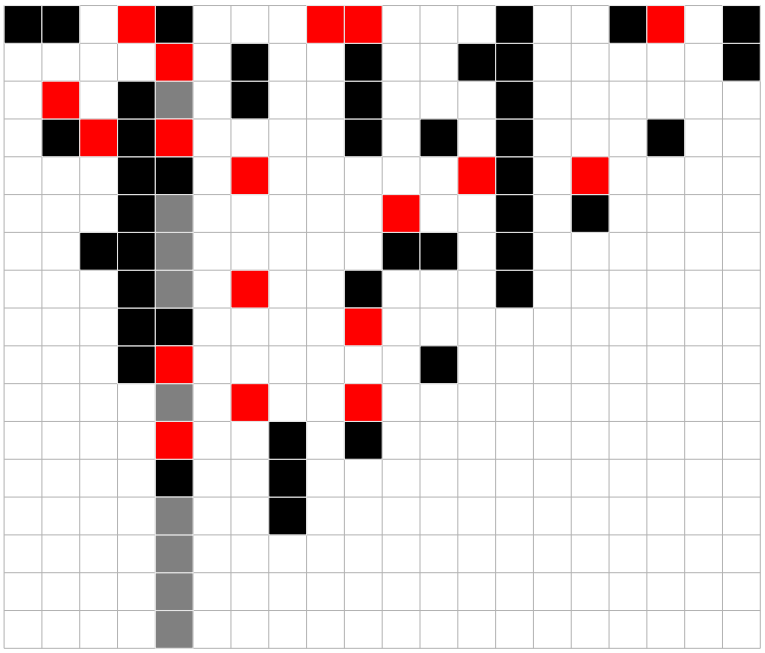


FIGURE 2.5 – Automate cellulaire contenant la suite 3-automatique de Rudin–Shapiro généralisée.

$$\begin{aligned} R_n(x) =& x^2 R_{n-2}(x) + \left(\frac{1}{x} + x^2\right) R_{n-3}(x) + \left(\frac{2}{x} + x^2\right) R_{n-4}(x) + \frac{2}{x} R_{n-6}(x) \\ &+ \frac{1}{x} R_{n-7}(x) + R_{n-9}(x) + 2x^2 R_{n-11}(x) + 2x^2 R_{n-12}(x) + 2x^2 R_{n-13}(x), \end{aligned}$$

valable pour tout $n \geq 14$. On pose $R_{-1}(x) = 0$ et $R_0(x) = 0$ et on obtient alors un automate cellulaire avec mémoire 16, dans lequel la suite généralisée de Rudin–Shapiro 3-automatique, apparaît dans la colonne -2 (voir Figure 2.5).

Remarque 2.2.8. La règle qui génère l'automate cellulaire peut se définir pour tous $m \in \mathbb{Z}$ et $n \geq 1$ par :

$$\begin{aligned} \phi(m, n+13) = &\phi(m+2, n+11) + \phi(m-1, n+10) + \phi(m+2, n+10) \\ &+ 2\phi(m-1, n+9) + \phi(m+2, n+9) + 2\phi(m+2, n) \\ &+ 2\phi(m-1, n+7) + \phi(m-1, n+6) + \phi(m, n+4) \\ &+ 2\phi(m+2, n+2) + 2\phi(m+2, n+1). \end{aligned}$$

Nous verrons dans les Chapitres 3 et 4 qu'il existe d'autres généralisations de la suite de Rudin–Shapiro. Nous terminons cette section en donnant l'exemple d'une généralisation de Rudin–Shapiro sur un alphabet à 4 lettres que nous allons construire explicitement en colonne d'un automate cellulaire. Cette construction peut se généraliser à n'importe quelle puissance d'un nombre premier [44]. Elle repose sur la notion de matrice de différence [21, 24] que nous développerons plus en détail dans le Chapitre 3.

Définition 2.2.2. [44] Considérons la matrice

$$M = (m_{ij})_{\substack{0 \leq i \leq 3 \\ 0 \leq j \leq 3}} = \begin{pmatrix} (0,0) & (0,0) & (0,0) & (0,0) \\ (0,0) & (0,1) & (1,0) & (1,1) \\ (0,0) & (1,0) & (1,1) & (0,1) \\ (0,0) & (1,1) & (0,1) & (1,0) \end{pmatrix}.$$

Soit

$$\begin{aligned} g : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \\ (j, n) &\longmapsto m_{n \bmod 4,\ j \bmod 4} \end{aligned}$$

On note g_1, g_2 les fonctions à valeurs dans $\mathbb{Z}_2$ telles que

$$g(j, n) = (g_1(j, n), g_2(j, n)).$$

La suite $(a(n))_{n\geq 0} = (a_1(n), a_2(n))_{n\geq 0}$ définie par $a(0) = (0, 0)$ et

$$a(4n + j) = a(n) + g(j, n), \quad 0 \leq j \leq 3, \quad n \geq 0, \quad (j, n) \neq (0, 0)$$

est une *suite de Rudin–Shapiro associée à la matrice* M définie sur $\mathbb{Z}_2 \times \mathbb{Z}_2$. En recodant $(0, 0)$ par 0, $(0, 1)$ par 1, $(1, 0)$ par 2 et $(1, 1)$ par 3, on peut définir à partir de $(a(n))_{n\geq 0}$, une suite $(\tilde{a}(n))_{n\geq 0}$ sur l'alphabet $\{0, 1, 2, 3\}$, dont les premiers termes sont les suivants :

$$(\tilde{a}(n))_{n\geq 0} = 0, 0, 0, 0, 0, 1, 2, 3, 0, 2, 3, 1, 0, 3, 1, 2, 0, 0, 0, 0, 1, 0, 3, 2, 2, 0, 1, 3, \ldots$$

Exemple 2.2.6. Nous allons commencer par construire la suite $(a(n))_{n\geq 0}$ que nous représenterons dans un automate cellulaire à double colonne sur l'alphabet $\{0, 1\}$. Pour cela nous allons traiter séparément les deux composantes qui peuvent être vues comme deux suites 2-automatiques distinctes. Nous obtiendrons la construction de la suite $(\tilde{a}(n))_{n\geq 0}$ en recodant, ce qui nous donnera un automate cellulaire avec des colonnes simples contenant des suites 4-automatiques sur l'alphabet $\{0, 1, 2, 3\}$.
On note $F(t) = \sum_{n\geq 0} a(n)t^n = \sum_{n\geq 0}(a_1(n), a_2(n))t^n$ la série génératrice de la suite $(a(n))_{n\geq 0}$. On a alors,

$$\begin{aligned} F(t) &= \sum_{n\geq 0} a(n)t^n \\ &= \sum_{n\geq 0} a(4n)t^{4n} + \sum_{n\geq 0} a(4n + 1)t^{4n+1} + \sum_{n\geq 0} a(4n + 2)t^{4n+2} + \sum_{n\geq 0} a(4n + 3)t^{4n+3} \\ &= (1 + t + t^2 + t^3)F(t^4) \\ &+ \sum_{n\geq 0} g(0, n)t^{4n} + \sum_{n\geq 0} g(1, n)t^{4n+1} + \sum_{n\geq 0} g(2, n)t^{4n+2} + \sum_{n\geq 0} g(3, n)t^{4n+3} \end{aligned}$$

En lisant la première colonne de la matrice M on remarque que pour tout $n \geq 0$ on a $g(0, n) = (0, 0)$. À partir de la deuxième colonne on obtient

$$\begin{aligned} \sum_{n\geq 0} g(1, n)t^{4n+1} &= \sum_{n\geq 0} g(1, 4n)t^{16n+1} + \sum_{n\geq 0} g(1, 4n + 1)t^{16n+5} \\ &+ \sum_{n\geq 0} g(1, 4n + 2)t^{16n+9} + \sum_{n\geq 0} g(1, 4n + 3)t^{16n+13} \\ &= \sum_{n\geq 0}(0, 1)t^{16n+5} + \sum_{n\geq 0}(1, 0)t^{16n+9} + \sum_{n\geq 0}(1, 1)t^{16n+13} \\ &= \left(\sum_{n\geq 0} t^{16n+9} + \sum_{n\geq 0} t^{16n+13}, \sum_{n\geq 0} t^{16n+5} + \sum_{n\geq 0} t^{16n+13}\right) \\ &= \left(\frac{t^9 + t^{13}}{1 - t^{16}}, \frac{t^5 + t^{13}}{1 - t^{16}}\right). \end{aligned}$$

De même, à partir de la troisième et de la quatrième colonne on obtient

$$\sum_{n\geq 0} g(2, n)t^{4n+2} = \left(\frac{t^6 + t^{10}}{1 - t^{16}}, \frac{t^{10} + t^{14}}{1 - t^{16}}\right),$$

et

$$\sum_{n\geq 0} g(3,n)t^{4n+3} = \left(\frac{t^7+t^{15}}{1-t^{16}}, \frac{t^7+t^{11}}{1-t^{16}}\right).$$

Ainsi $x = F(t)$ satisfait l'équation

$$x = (1+t+t^2+t^3)x^4 + \frac{1}{1-t^{16}}(t^6+t^7+t^9+t^{10}+t^{13}+t^{15}, t^5+t^7+t^{10}+t^{11}+t^{13}+t^{14}).$$

Notons $x_1 = F_1(t) = \sum_{n\geq 0} a_1(n)t^n$ et $x_2 = F_2(t) = \sum_{n\geq 0} a_2(n)t^n$, de sorte que $x = (x_1, x_2)$.

On pose

$$\begin{aligned} P(t,x) &= (t^6+t^7+t^9+t^{10}+t^{13}+t^{15}, t^5+t^7+t^{10}+t^{11}+t^{13}+t^{14}) \\ &\quad + (t^{16}-1)x + (1-t^{16})(1+t+t^2+t^3)x^4 \\ &= (t^6+t^7+t^9+t^{10}+t^{13}+t^{15}, t^5+t^7+t^{10}+t^{11}+t^{13}+t^{14}) \\ &\quad + (1+t^{16})x + (1+t+t^2+t^3+t^{16}+t^{17}+t^{18}+t^{19})x^4. \end{aligned}$$

Alors on a $P(t, F(t)) = 0$. En effectuant la transformation $x \mapsto tx$, on obtient

$$\begin{aligned} P(t,x) &= (t^5+t^6+t^8+t^9+t^{12}+t^{14}, t^4+t^6+t^9+t^{10}+t^{12}+t^{13}) \\ &\quad + (1+t^{16})x + (t^3+t^4+t^5+t^6+t^{19}+t^{20}+t^{21}+t^{22})x^4. \end{aligned}$$

qui est un polynôme annulateur de la série $G(t) = \sum_{n\geq 1} a(n+1)t^n$, qui satisfait $G(0) = (0,0)$ et $F(t) = tG(t)$.

Si on pose

$$P_1(t,x_1) = t^5+t^6+t^8+t^9+t^{12}+t^{14} + (1+t^{16})x_1 + (t^3+t^4+t^5+t^6+t^{19}+t^{20}+t^{21}+t^{22})x_1^4,$$

et

$$P_2(t,x_1) = t^4+t^6+t^9+t^{10}+t^{12}+t^{13} + (1+t^{16})x_2 + (t^3+t^4+t^5+t^6+t^{19}+t^{20}+t^{21}+t^{22})x_2^4,$$

on a alors $P_1(t, F_1(t)) = 0$, $P_2(t, F_2(t)) = 0$ et $P(t,x) = (P_1(t,x_1), P_2(t,x_2))$.

On peut maintenant construire la suite $(a_1(n))_{n\geq 0}$ à partir du polynôme P_1 et la suite $(a_2(n))_{n\geq 0}$ à partir du polynôme P_2. Remarquons que $P_1^{(0,1)}(t,x) = 1+t^{16}$ et $P_2^{(0,1)}(t,x) = 1+t^{16}$ et donc en particulier $P_1^{(0,1)}(0,0) \neq 0$ et $P_2^{(0,1)}(0,0) \neq 0$. On peut alors appliquer la Proposition 2.1.3.
Ainsi, pour tout $n \geq 1$, $a_1(n+1)$ est le coefficient de ${x_1}^{-2}$ dans $R_n^1(x_1)$ où $R_n^1(x_1)$ est le coefficient de t^n dans la série

$$\frac{P_1^{(0,1)}(t,x_1)}{P_1(t,x_1)} = \sum_{n\geq 0} R_n^1(x_1)t^n.$$

Et de même, pour tout $n \geq 1$, $a_2(n+1)$ est le coefficient de ${x_2}^{-2}$ dans $R_n^2(x_2)$ où $R_n^2(x_2)$ est le coefficient de t^n dans la série

$$\frac{P_2^{(0,1)}(t,x_2)}{P_2(t,x_2)} = \sum_{n\geq 0} R_n^2(x_2)t^n.$$

En réordonnant les polynômes P_1 et P_2 selon les puissances de t en on déduit les relations de récurrence

$$\begin{aligned} R_n^1(x_1) &= {x_1}^3 R_{n-3}^1(x_1) + {x_1}^3 R_{n-4}^1(x_1) + \left(\frac{1}{x_1} + {x_1}^3\right) R_{n-5}^1(x_1) + \left(\frac{1}{x_1} + {x_1}^3\right) R_{n-6}^1(x_1) \\ &\quad + \frac{1}{x_1} R_{n-8}^1(x_1) + \frac{1}{x_1} R_{n-9}^1(x_1) + \frac{1}{x_1} R_{n-12}^1(x_1) \frac{1}{x_1} R_{n-14}^1(x_1) \\ &\quad + {x_1}^3 R_{n-19}^1(x_1) + {x_1}^3 R_{n-20}^1(x_1) + {x_1}^3 R_{n-21}^1(x_1) + {x_1}^3 R_{n-22}^1(x_1), \end{aligned}$$

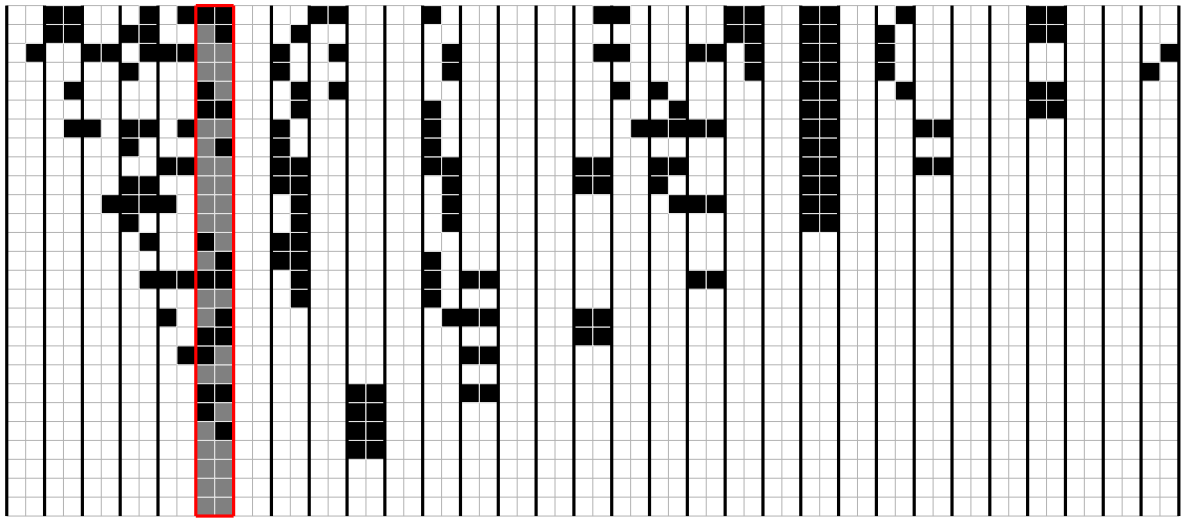


FIGURE 2.6 – Automate cellulaire contenant la suite 4-automatique de Rudin–Shapiro généralisée sur $\{0,1\} \times \{0,1\}$.

et

$$\begin{aligned} R^2_n(x) = {} & x^3 R^1_{n-3}(x) + \left(\frac{1}{x} + x^3\right) R^1_{n-4}(x) x^3 R^1_{n-5}(x) + \left(\frac{1}{x} + x^3\right) R^1_{n-6}(x) \\ & + \frac{1}{x} R^1_{n-9}(x) + \frac{1}{x} R^1_{n-10}(x) + \frac{1}{x} R^1_{n-12}(x) \frac{1}{x} R^1_{n-13}(x) \\ & + x^3 R^1_{n-19}(x) + x^3 R^1_{n-20}(x) + x^3 R^1_{n-21}(x) + x^3 R^1_{n-22}(x), \end{aligned}$$

valables pour $n \geq 23$. On pose $R^1_{-1}(x_1) = a_1(0){x_1}^{-2} = 0$, $R^1_0(x_1) = a_1(1){x_1}^{-2} = 0$, $R^2_{-1}(x_2) = a_2(0){x_2}^{-2}$, $R^2_0(x_2) = a_2(0){x_2}^{-2}$ et on obtient alors un automate cellulaire de mémoire 25, dans lequel la suite généralisée de Rudin–Shapiro associée à la matrice M, de la Définition 2.2.2, apparaît dans la double colonne encadrée en rouge Figure 2.6.

En projetant, on en déduit à partir de l'automate cellulaire précédent, un automate cellulaire qui construit la suite généralisée de Rudin–Shapiro associée à la matrice M, sur l'alphabet $\{0,1,2,3\}$ (voir Figure 2.7). Les cases blanches et grises correspondent aux 0, les noires aux 1, les rouges aux 2 et les bleus aux 3.

Rowland et Yassawi ont donc résolu la question de la construction des suites q-automatiques comme colonne d'un automate cellulaire, lorsque q est la puissance d'un nombre premier. On peut alors s'interroger sur la construction des suites k-automatiques (lorsque k n'est pas la puissance d'un nombre premier), comme colonne d'un automate cellulaire. Pour le moment ce problème reste ouvert.

Une autre question concerne la construction de suites non-automatiques. Nous allons nous y intéresser dans la dernière partie de ce chapitre. Nous verrons que dans certains cas il existe également des manières explicites de construire des suites non-automatiques comme colonne d'un automate cellulaire.

2.3 Constructions de suites non-automatiques

Le résultat de Rowland et Yassawi étant une équivalence, les suites non-automatiques qui appartiennent à l'ensemble $\mathcal{S}$, que nous avons introduit au début du chapitre, sont nécessairement obtenues par des automates cellulaires non-linéaires. Nous nous intéresserons à la construction des fonctions indicatrices de polynômes à valeurs entières, dont nous avons observé au Chapitre 1, par le critère de

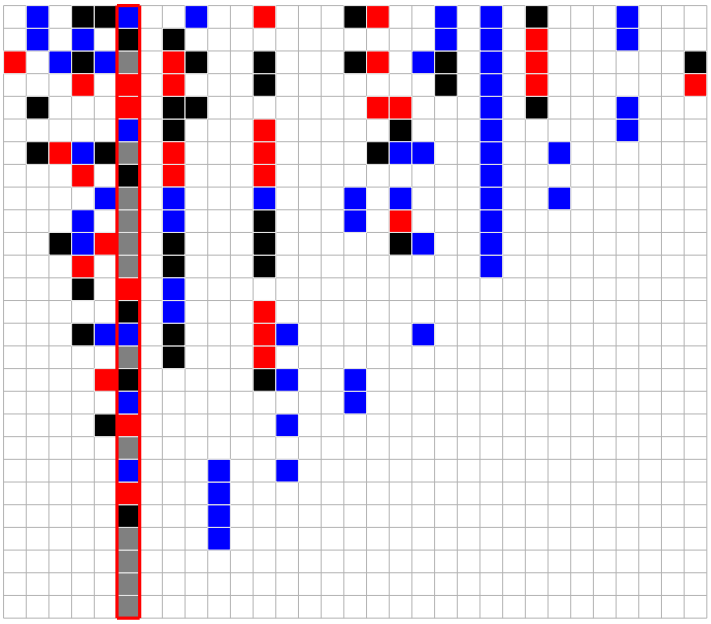


FIGURE 2.7 – Automate cellulaire contenant la suite 4-automatique de Rudin–Shapiro généralisée sur $\{0, 1, 2, 3\}$.

Minsky et Papert, qu'elles constituaient une famille de suites non-automatiques, ainsi qu'à la construction du mot de Fibonacci, par l'intermédiaire de l'indicatrice des nombres de Fibonacci, qui est une suite non-automatique bien connue en combinatoire des mots. Les suites seront obtenues à chaque fois dans la colonne 0 de l'automate cellulaire et n'utiliseront que les colonnes à droite de celle-ci. Enfin, nous montrerons comment nous pouvons réduire le nombre de symboles utilisés par les automates cellulaires, pour nous restreindre uniquement aux symboles qui apparaissent dans la suite que nous cherchons à construire. En particulier, ce dernier point répond à une question posée par Rowland et Yassawi [41, troisième question p. 80].

2.3.1 Suites polynomiales

En 1999, Mazoyer et Terrier [34] montrèrent que les fonctions indicatrices de polynômes (sous des conditions appropriées) sont constructibles par un automate cellulaire. Nous proposons ici une méthode permettant de simplifier leurs constructions, notamment celle pour les carrés [34, Figure 5] en généralisant celle introduite en 2011 par Delacourt, Poupet, Sablik et Theyssier [13, Section 3]. Tandis que les constructions proposées par Mazoyer et Terrier pour les polynômes de degrés plus élevés utilisent des signaux qui zigzaguent entre d'autres signaux et la suite que l'on cherche à construire, nos constructions permettent d'obtenir $\mathbf{1}_{P(\mathbb{N})}$ en interceptant un seul signal avec la colonne 0.

Commençons par rappeler la construction pour les carrés [13]. Un signal (représenté par une flèche) démarre dans la première colonne en direction du Nord-Est. Chaque fois qu'il rencontre un mur (représenté par une barre verticale), le mur se décale d'une cellule vers la droite et continue de se propager verticalement dans la même colonne, jusqu'à ce qu'il rencontre à nouveau un signal. Lorsqu'il rencontre le mur, le signal change de direction et progresse en direction Nord-Ouest cette fois-ci. Enfin quand le signal rencontre la colonne 0, on marque un 1 dans celle-ci et le signal change à nouveau de direction à l'étape suivante pour repartir vers la droite.

Commençons par établir une première généralisation qui permet d'obtenir pour une suite que l'on sait construire, la somme des termes de cette suite en colonne 0. Un résultat similaire a été établi par Mazoyer et Terrier [34, Corollaire 2], pour leurs constructions géométriques.

Proposition 2.3.1. [28] Soit $f : \mathbb{N} \longrightarrow \mathbb{N}$ une fonction strictement croissante à partir d'un certain rang,

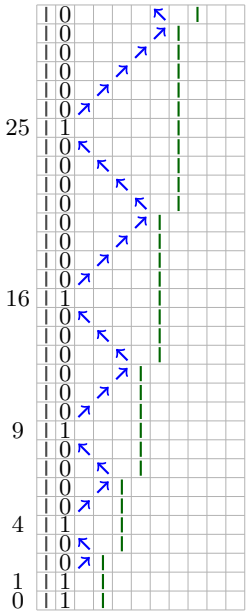


FIGURE 2.8 – Automate cellulaire pour les carrés.

et soit g sa suite sommatoire, définie par $g(n) = \sum_{k=0}^{n} f(k)$ pour tout $n \geq 0$. Supposons que $u = \mathbf{1}_{f(\mathbb{N})}$ est un élément de $\mathcal{S}$. Alors $v = \mathbf{1}_{g(\mathbb{N})}$ est aussi un élément de $\mathcal{S}$.

Démonstration. Appelons F l'automate cellulaire qui construit $u = \mathbf{1}_{f(\mathbb{N})}$ et notons G celui qui va construire $v = \mathbf{1}_{g(\mathbb{N})}$. Comme f est strictement croissante à partir d'un certain rang n_0, la fonction g est aussi croissante pour $n \geq n_0$. Nous pouvons donc considérer les valeurs de g pour $n < n_0$ comme conditions initiales de G. Sans perte de généralité, on peut considérer le cas où f est strictement croissante pour tout $n \geq 0$, étant donné qu'il est possible de rajouter un nombre fini de cas dans les conditions initiales de G.
Supposons dans un premier temps que la condition suivante est satisfaite :

$$(\star) \qquad 2g(i) > f(i+1) \text{ for all } i \geq 1.$$

Dans un second temps, nous montrerons comment adapter la construction dans le cas où $(\star)$ n'est pas satisfaite. Mais par souci de clarté, nous considérerons d'abord que $(\star)$ est satisfaite. Cette condition permet d'obtenir la construction en trois étapes.

(i) Marquage des colonnes :
La première étape consiste à marquer les colonnes $f(0), f(1), \ldots, f(n), \ldots$. Pour cela, nous partons de la construction de $u = \mathbf{1}_{f(\mathbb{N})}$ et pour tout entier i, on décale toutes les cellules de la ligne i exactement de i cellules vers la droite, ce qui revient à considérer le diagramme espace-temps de l'automate cellulaire $\sigma \circ F$, avec la même configuration initiale, et où σ désigne le décalage à droite qui apparaît dans la définition des automates cellulaires. Dans la construction de $u = \mathbf{1}_{f(\mathbb{N})}$, la colonne 0 contient un 1 aux lignes $f(0), f(1), \ldots, f(n), \ldots$, par conséquent dans le diagramme espace-temps de G, les lignes $f(0), f(1), \ldots, f(n), \ldots$ sont marquées mais aux colonnes $f(0), f(1), \ldots, f(n), \ldots$ désormais, ce qui correspond à la diagonale du nouveau diagramme espace-temps. Comme f est strictement croissante, ces colonnes sont distinctes les unes des autres.

(ii) Construction des murs :
Ensuite, on définit un nouveau signal de vitesse 1 qui se propage sur la diagonale du diagramme espace-temps. Les intersections entre ce signal et les colonnes $f(0), f(1), \ldots, f(n), \ldots$ génèrent un nouveau signal de vitesse 0 qui par analogie à la construction des carrés sont appelés les murs.

(iii) Passage d'un signal issu de la colonne 0 au suivant :
Supposons que nous avons un 1 sur une certaine ligne dans la colonne 0. Nous allons montrer comment engendrer le signal suivant qui part de la colonne 0. Définissons un signal de vitesse 2 qui avance vers la droite. Quand le signal rencontre un mur, qui se trouve dans une colonne $f(i)$ pour un certain i, le signal change de direction et avance vers la gauche à la même vitesse. Quand le signal rencontre à nouveau la colonne 0, on marque un nouveau 1. Selon la parité, il y a deux possibilités pour qu'un signal et un mur se rencontrent. Soit les deux signaux sont dans deux colonnes l'une à côté de l'autre, et dans ce cas, le signal de vitesse -2 commence dans la même colonne que le dernier symbole du signal de vitesse 2 mais une ligne au-dessus, soit il y a une cellule entre les deux signaux et alors, le signal de vitesse -2 commence dans la même colonne que le dernier symbole du signal de vitesse 2 mais deux lignes au-dessus. Dans les deux cas, le signal mur s'interrompt une fois que le signal de vitesse 2 est reparti dans l'autre sens à la vitesse -2. Comme f est strictement croissante, on ne peut pas avoir deux murs dans la même colonne, et la procédure est donc bien définie.

Maintenant supposons que nous avons construit les premières lignes de l'automate cellulaire, autrement dit, nous avons un 1 dans la colonne 0 aux lignes $f(0), f(0)+f(1), \ldots, f(0)+\cdots+f(i)$ pour un certain i. On applique les règles précédentes pour continuer la procédure. En particulier, le 1 de la colonne 0 à la ligne $f(0)+\cdots+f(i)$ envoie un signal de vitesse 2 jusqu'à l'intersection avec le mur de la colonne $f(i+1)$. Si $f(i+1)$ est impair, nous sommes dans le cas où les deux signaux sont dans deux colonnes côte à côte. La distance parcourue par le signal de vitesse 2 à partir du 1 initial est $\dfrac{f(i+1)-1}{2}$ et le signal de vitesse -2 parcourt la même distance. On place le nouveau 1 dans la colonne 0 une ligne au-dessus. Ainsi, ce nouveau 1 est sur la ligne :

$$f(0)+\cdots+f(i)+2\left(\frac{f(i+1)-1}{2}\right)+1 = f(0)+\cdots+f(i)+f(i+1).$$

Si $f(i+1)$ est pair, nous sommes dans l'autre cas et le nouveau 1 dans la colonne 0 est sur la ligne :

$$f(0)+\cdots+f(i)+\left(\frac{f(i+1)}{2}-1\right)+1+\left(\frac{f(i+1)}{2}-1\right)+1 = f(0)+\cdots+f(i)+f(i+1).$$

Remarquons que la condition $(\star)$, peut être réécrite ainsi :

$$f(0)+f(1)+\cdots+f(i)+\frac{f(i+1)}{2} > f(i+1),$$

ce qui assure que le mur de la colonne $f(i+1)$ a déjà été créé quand le signal de vitesse 2 arrive à sa rencontre. Selon la fonction f, la condition $(\star)$ n'est pas toujours satisfaite.
Dans le cas où $(\star)$ serait satisfaite pour $n \geq n_0$, une possibilité pour régler le problème est de considérer les premières lignes du diagramme espace-temps comme des conditions initiales. Une autre possibilité est de décaler la construction des points $f(i)$ de plusieurs lignes sous la diagonale principale, de manière à ce que les murs apparaissent suffisamment tôt. Il est alors possible d'utiliser la procédure décrite précédemment de manière analogue. Soit E l'ensemble de tous les entiers tels que $(\star)$ n'est pas satisfaite. Considérons pour tout $n \in E$ les différences $f(n)-2g(n)$ et soit M le maximum de ces différences. Il est alors suffisant de décaler la construction sous la diagonale de M lignes en-dessous.
Dans le cas où il y aurait une infinité de valeurs de n tels que $(\star)$ n'est pas satisfaite, on utilise une autre stratégie. Il suffit de changer les signaux de vitesses 2 et -2 à l'étape *(iii)* en signaux de vitesse 1 et -1. Dans ce cas, la suite qui est construite n'est pas $\mathbf{1}_{g(\mathbb{N})}$ mais $\mathbf{1}_{2g(\mathbb{N})}$. Cependant, il est possible d'obtenir la suite $\mathbf{1}_{g(\mathbb{N})}$ avec l'automate cellulaire G^2. □

Exemple 2.3.1. [28](*Construction de la fonction indicatrice de la somme des carrés*) Soit $f(n) = n^2$ et $g(n) = \sum_{k=0}^{n} k^2 = n(n+1)(2n+1)/6$. Ici, la condition $(\star)$ est satisfaite pour $n \geq 2$, et pour la construction de $\mathbf{1}_{g(\mathbb{N})}$, on considère que les trois premières lignes du diagramme espace-temps sont des conditions initiales. Dans la représentation de l'automate cellulaire, nous avons décalé la construction d'une ligne sous la diagonale, et les conditions initiales correspondent aux deux premières lignes.

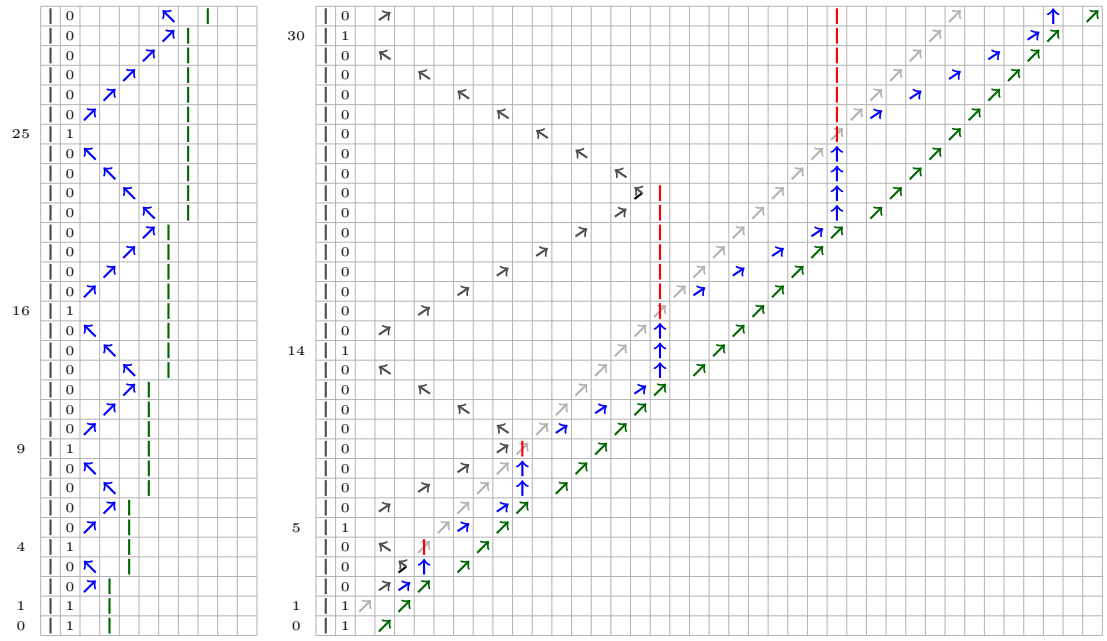


FIGURE 2.9 – Automates cellulaires pour les carrés (à gauche) et pour la somme des carrés (à droite).

Remarque 2.3.1. Dans l'Exemple 2.3.1 on constate que l'on a construit un polynôme de degré 3. Cela suggère que la méthode peut se généraliser pour construire en colonne d'un automate cellulaire la fonction indicatrice de n'importe quel polynôme de degré plus élevé. Nous commençons par donner la construction explicite de la fonction indicatrice des cubes, avant d'énoncer le résultat général.

Exemple 2.3.2. [28](*Construction de la fonction indicatrice des cubes*) Pour tout $n \in \mathbb{N}$ on a $(n+1)^3 - n^3 = 3n^2 + 3n + 1$. Avec la construction pour les carrés, il est facile d'obtenir la fonction caractéristique de $3n^2$. Il suffit de diviser la vitesse des signaux de vitesse ± 1 par 3. Les cellules rouges, bleus et noires dans la colonne 0 de l'automate cellulaire de gauche de la Figure 2.10 correspondent au terme $3n$. On en déduit ainsi la construction de la fonction caractéristique du polynôme $3n^2 + 3n + 1$. Les huit premières lignes sont les conditions initiales. Maintenant, pour obtenir la fonction caractéristique des cubes, il suffit de remarquer que pour tout $n \geq 1$, $\quad \sum_{k=0}^{n-1} \left((k+1)^3 - k^3\right) = n^3$ et on peut donc utiliser la construction décrite dans la preuve de la Proposition 2.3.1. Les cinq premières lignes sont les conditions initiales et la construction a été décalée de trois lignes sous la diagonale.

Voici maintenant le résultat général sur la construction des suites polynomiales.

Théorème 2.3.1. [28] Soit $P(X) \in \mathbb{Q}[X]$ un polynôme de degré $d \geq 1$ tel que $P(\mathbb{N}) \subset \mathbb{N}$. Alors la suite $u = \mathbf{1}_{P(\mathbb{N})}$ est un élément de $\mathcal{S}$ et peut-être obtenue par l'intersection d'un seul signal avec la colonne 0.

Démonstration. Ici, la condition $(\star)$ de la Proposition 2.3.1 est satisfaite pour une valeur de n suffisamment grande. Le résultat du Théorème 2.3.1 est clair pour tout polynôme de degré 1. En effet, si P est de la forme $P(X) = aX + b$ avec $a \in \mathbb{N}, b \in \mathbb{Z}$, on peut construire la suite par un signal qui rebondit sur un mur qui se propage dans la colonne $\lfloor a/2 \rfloor$. La translation de b se fait simplement en fixant les conditions initiales. Remarquons que l'on peut traiter des coefficients rationnels en multipliant et en divisant de manière adéquate la vitesse des symboles. Supposons maintenant que le résultat est vrai pour tout polynôme de degré $k < d$, pour un certain $d \geq 2$. Montrons alors que l'on peut construire n'importe quel polynôme P de degré d avec seulement un signal rencontrant la colonne 0. Pour cela, on observe que $Q(X) = P(X+1) - P(X)$ est un polynôme de degré au plus $d-1$. De plus, comme $P(\mathbb{N}) \subset \mathbb{N}$, le

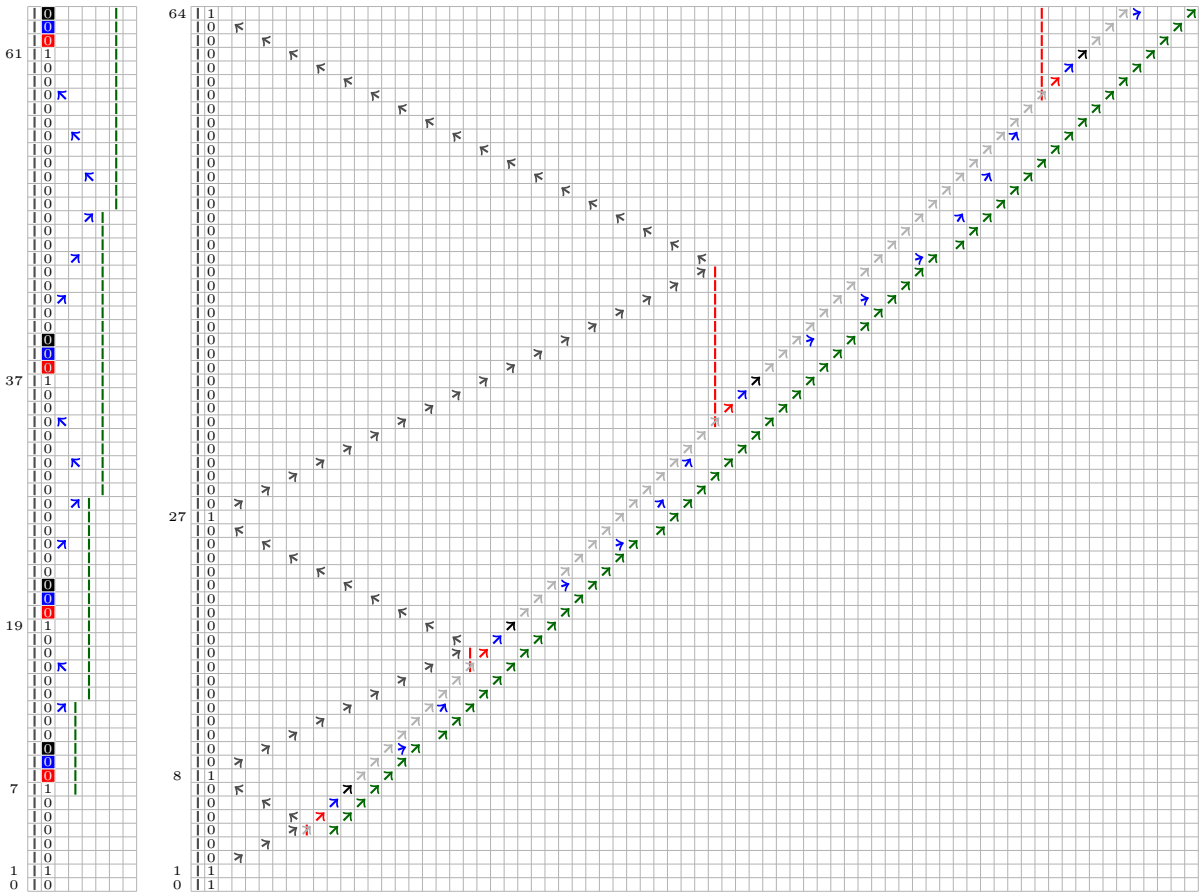


FIGURE 2.10 – Automates cellulaires pour la différence des cubes (à gauche) et pour les cubes (à droite).

coefficient dominant de P est positif, et par conséquent il existe $c \in \mathbb{N}$, dépendant uniquement de P, tel que le polynôme $\tilde{Q}(X) = Q(X + c)$ satisfait à $\tilde{Q}(\mathbb{N}) \subset \mathbb{N}$. De plus

$$P(n) - P(0) = \sum_{k=0}^{n-1} (P(k+1) - P(k)) = \sum_{k=0}^{n-1} Q(k)$$

Par récurrence, nous savons maintenant que $\mathbf{1}_{\tilde{Q}(\mathbb{N})}$ est constructible. Peu importe les conditions initiales finies dues à c et à $P(0)$, la Proposition 2.3.1 implique que $\mathbf{1}_{P(\mathbb{N})}$ est un élément de $\mathcal{S}$, obtenu par l'intersection d'un seul signal avec la colonne 0. □

2.3.2 Mot de Fibonacci

Avec les polynômes, nous avons maintenant toute une famille de suites non-automatiques que l'on peut construire explicitement et de manière simple comme colonne d'un automate cellulaire. Parmi les suites non-automatiques de référence en combinatoire des mots, il y a la suite binaire que l'on appelle mot de Fibonacci et qui se construit de manière récursive à l'aide d'un morphisme. Nous allons voir qu'il est également possible de l'obtenir en colonne d'un automate cellulaire, en s'appuyant sur la construction des nombres de Fibonacci.

La suite de Fibonacci est définie de manière récursive par $F_0 = 0, F_1 = 1$, et $\forall n \geq 0, F_{n+2} = F_{n+1} + F_n$. Notons $\mathbf{F}$ l'ensemble des nombres qui apparaissent dans la suite de Fibonacci, $\mathbf{F} = \{F_n : n \in \mathbb{N}\}$. Nous proposons de construire la suite $u = \mathbf{1}_{\mathbf{F}}$, qui par définition, satisfait à : $u_n = 1 \iff \exists k \in \mathbb{N}, n = F_k$. Notre construction présente des similarités avec une proposition de Mazoyer et Terrier pour les suites linéaires récurrentes [34, Proposition 4].

Proposition 2.3.2. [28] La fonction indicatrice $\mathbf{1}_{\mathbf{F}}$ des nombres de Fibonacci est un élément de $\mathcal{S}$.

Démonstration. Nous proposons une construction explicite qui utilise des signaux de vitesse 0 (les murs), ± 1, et 2. Supposons que sur la ligne F_n, on a marqué les positions $0, F_{n-2}, F_{n-1}$ et F_n, et montrons comment obtenir les mêmes marques au temps F_{n+1}. En particulier, la procédure va nous permettre de repérer dans l'ordre les points F_n dans la colonne 0 du diagramme espace-temps. Le principe est le suivant :

— Depuis le point $(0, F_n)$, on envoie un signal de vitesse 1.

— Depuis le point (F_{n-2}, F_n) on envoie un signal de vitesse 1 et un de vitesse 2.

— Depuis le point (F_{n-1}, F_n) on envoie un signal de vitesse 0 (mur) et un de vitesse -1.

— Depuis le point (F_n, F_n) on envoie un signal de vitesse 0 (mur) et un de vitesse 1.

Le signal de vitesse 1 issu du point $(0, F_n)$ et celui de vitesse 0 issu du point (F_{n-1}, F_n) s'intersectent après avoir parcouru $F_{n-1} - 0 = F_{n-1}$ cases en hauteur. Celui de vitesse 1 issu de (F_{n-2}, F_n) et celui de vitesse 0 issu de (F_n, F_n) s'intersectent après avoir parcouru $F_n - F_{n-2} = F_{n-1}$ cases en hauteur. Enfin, le signal de vitesse 2 issu de (F_{n-2}, F_n) et celui de vitesse 1 issu de (F_n, F_n) s'intersectent après avoir parcouru $\frac{F_{n+1} - F_{n-2}}{2} = F_{n-1}$ cases en hauteur. Les trois intersections sont donc sur la ligne $F_n + F_{n-1} = F_{n+1}$ et marquent les points $0, F_{n-1}, F_n$ et F_{n+1} (voir Figure 2.11).

□

Le mot de Fibonacci est la suite morphique $v \in \mathcal{A}^{\mathbb{N}}$ qui est l'unique point fixe de la substitution σ définie par $0 \mapsto 01$ et $1 \mapsto 0$. On définit de manière récursive une succession de mots par $w_1 = 0$ et pour

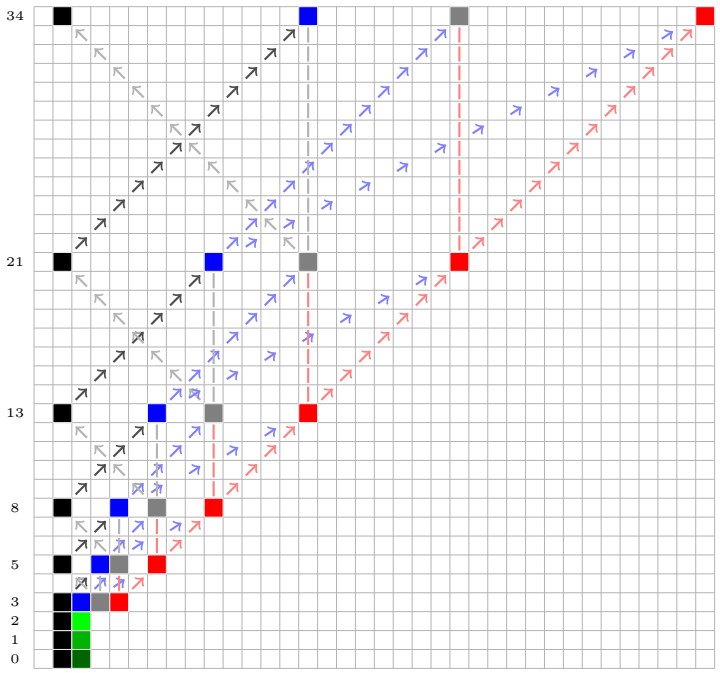


FIGURE 2.11 – Construction des nombres de Fibonacci.

tout $n \geq 1, w_{n+1} = \sigma(w_n)$. Les premiers mots obtenus sont les suivants :

$$\begin{aligned}
w_1 &= 0\\
w_2 &= 01\\
w_3 &= 010\\
w_4 &= 01001\\
w_5 &= 01001010\\
w_6 &= 0100101001001\\
w_7 &= 01001010010010100 1\\
w_8 &= 0100101001001010010100100101001001\\
w_9 &= 010010100100101001010010010100100101001010010100101001010,
\end{aligned}$$

et le mot de Fibonacci $v \in \mathcal{A}^{\mathbb{N}}$ est la limite de ces mots.

Proposition 2.3.3. [28] Le mot de Fibonacci est un élément de $\mathcal{S}$.

Démonstration. Il découle directement de la définition que pour tout $n \geq 1$, la longueur du mot w_n est égale à F_n.
De plus, on peut vérifier que pour tout $n \geq 1$, on a :

$$w_{n+1} = w_n \cdot w_{n-1} = w_{n-1} \cdot w_{n-2} \cdot w_{n-2} \cdot w_{n-3} = \underbrace{w_{n-2} \cdot w_{n-3} \cdot w_{n-2}}_{w_n} \cdot w_{n-2} \cdot w_{n-3},$$

où le symbole $\cdot$ représente la concaténation des mots. Il s'ensuit que si un mot w_n est déjà construit, pour obtenir le mot w_{n+1}, on peut d'abord concaténer à la suite de w_n le mot w_{n-2}, qui apparaît dans les F_{n-2} dernières lettres de w_n, et le mot w_{n-3}, qui apparaît dans w_n entre les positions F_{n-2} et $F_{n-2} + F_{n-3} = F_{n-1}$. On peut faire cela avec un automate cellulaire comportant un nombre fini d'états : le bloc w_{n-2} qui apparaît à la fin de w_n est translaté à droite jusqu'à ce qu'il rencontre un mur placé dans

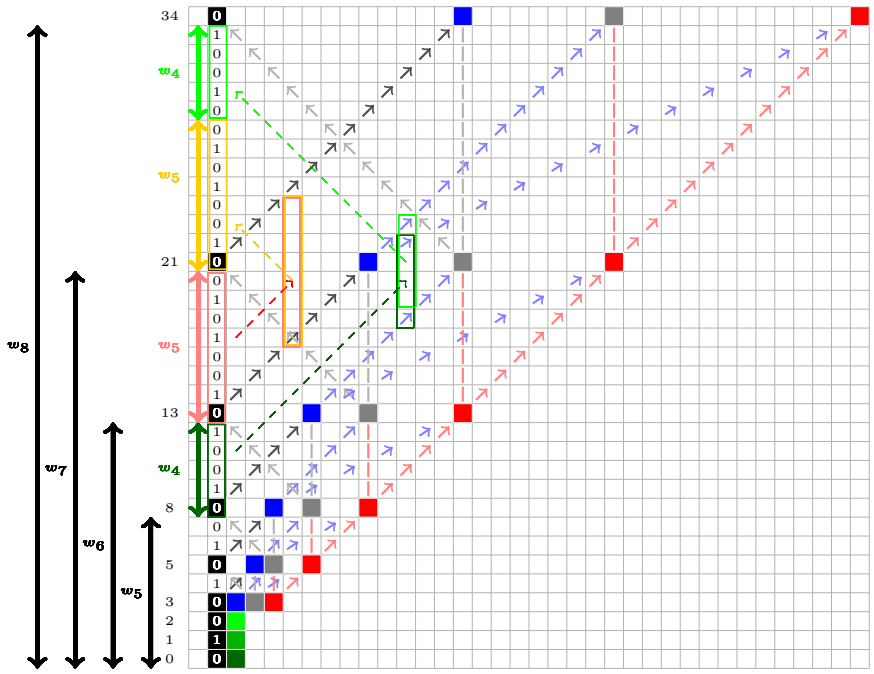


FIGURE 2.12 – Construction des nombres de Fibonacci et du mot de Fibonacci.

la colonne $F_{n-2}/2$ et est ensuite translaté vers la gauche. De la même manière, le bloc w_{n-3} qui apparaît entre les positions F_{n-2} et F_{n-1} est translaté vers la droite jusqu'à ce qu'il rencontre un mur placé dans la colonne $(F_{n-2}+F_{n-1})/2 = F_n/2$ pour être ensuite translaté vers la gauche. Les murs aux positions $F_{n-2}/2$ et $(F_{n-2}+F_{n-1})/2$ peuvent être engendrés sans trop de difficulté. La construction des murs en position $F_{n-2}/2$ est illustrée sur Figure 2.12. Pour la construction des murs en position $(F_{n-2}+F_{n-1})/2$, on peut envoyer des signaux de vitesses respectives 1 et -1 à partir des positions F_{n-2} et F_{n-1} au temps F_{n-1}. □

2.3.3 Recodage, réduction du nombre de symboles

Comme nous l'avons vu, les constructions précédentes avec les signaux utilisent beaucoup de symboles différents. Dans le cas des polynômes, le nombre de symboles augmente assez rapidement avec le degré. Nous allons voir dans cette partie qu'en réalité ce n'est pas vraiment un problème car il est possible de se restreindre uniquement aux symboles qui apparaissent dans la suite que l'on cherche à construire, à l'aide d'un recodage. En particulier, cela répond à une question posée par Rowland et Yassawi, concernant la construction en colonne d'un automate cellulaire à 2 états, d'une suite 3-automatique sur un alphabet binaire, non-périodique à partir d'un certain rang [41, troisième question p. 80]. Nous traiterons un exemple explicite avec la fonction indicatrice des puissances de 3.

Dans cette partie nous allons travailler avec l'alphabet binaire $\mathcal{A} = \{0, 1\}$.

Proposition 2.3.4. [28] Soit $\mathcal{B}$ un ensemble fini de symboles tel que $\mathcal{B} \supsetneq \mathcal{A}$, soit $F : \mathcal{B}^{\mathbb{Z}} \to \mathcal{B}^{\mathbb{Z}}$ un automate cellulaire 0-stable, et soit $x \in \mathcal{B}^{\mathbb{Z}}$ une configuration finie. Si $\forall n \in \mathbb{N}, F^n(x)_0 \in \mathcal{A}$, alors, $(F^n(x)_0)_{n\geq 0} \in \mathcal{S}$.

Démonstration. Sans perte de généralité, on peut considérer que $\mathcal{B} = \{0, \dots, k-1\}$ pour un certain $k \geq 3$. On recode les k symboles de l'alphabet $\mathcal{B}$ par des mots binaires de longueur $2k-1$, en utilisant l'application $\tau : \mathcal{B} \to \mathcal{A}^{2k-1}$ définie de la manière suivante :

$$\tau(0) = \underbrace{00\cdots0}_{2k-1}, \quad \text{et pour } i \in \{1, \dots, k-1\},\ \tau(i) = 1\underbrace{0\cdots0}_{i-1}1\underbrace{0\cdots0}_{2k-i-2}.$$

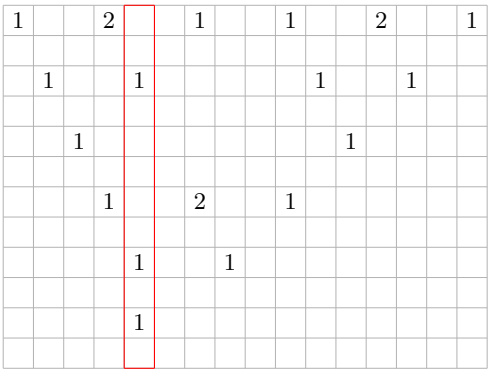


FIGURE 2.13 – Construction des puissances de 3.

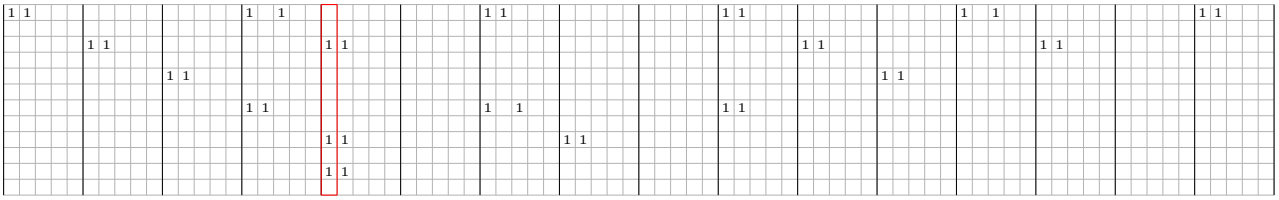


FIGURE 2.14 – Construction des puissances de 3, après recodage.

À partir d'une configuration $x \in \mathcal{B}^{\mathbb{Z}}$, la concaténation des blocs $\tau(x_i)$ pour $i \in \mathbb{Z}$ engendre une nouvelle configuration $\tilde{x} \in \mathcal{A}^{\mathbb{Z}}$, où on considère que $\tau(x_0)$ commence à la position 0 dans la nouvelle configuration, autrement dit $(\tilde{x}_i)_{0 \leq i \leq 2k-2} = \tau(x_0)$. Avec ce recodage, il est possible de déterminer localement les limites entre les blocs dans la nouvelle configuration, sauf si on a une longue chaîne de 0. Mais dans ce cas, comme F est 0-stable, on sait que la fonction locale va donner un 0. Ainsi, en utilisant le recodage, on peut définir un nouvel automate cellulaire $G : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ de rayon $(2k-1)r+2k-2 = (2k-1)(r+1)-1$ qui reproduit sur $\mathcal{A}^{\mathbb{Z}}$ le mécanisme de l'automate cellulaire d'origine $F : \mathcal{B}^{\mathbb{Z}} \to \mathcal{B}^{\mathbb{Z}}$, et G est lui-même un automate cellulaire 0-stable. Comme les premières lettres de $\tau(0)$ et de $\tau(1)$ sont respectivement 0 et 1, s'il n'y a aucune apparition de symbole de $\mathcal{B} \backslash \mathcal{A}$ dans la colonne centrale, alors on a : $\forall n \in \mathbb{N}, F^n(x)_0 = G^n(x)_0$. □

Exemple 2.3.3. [28] En particulier, si $\mathcal{B} = \{0, 1, 2\}$, le recodage τ introduit précédemment est défini par : $\tau(0) = 00000, \tau(1) = 11000, \tau(2) = 10100$, et la construction prouve que n'importe quelle suite 3-automatique $(u_n)_{n \geq 0}$ sur un alphabet binaire peut-être obtenue comme colonne d'un automate cellulaire (non-linéaire) dont le diagramme espace-temps a 2 états, ce qui répond à une question posée par Rowland et Yassawi [41, troisième question p. 80]. En Figure 2.13, nous illustrons ce résultat avec l'exemple de la suite 3-automatique définie par $u_n = \mathbf{1}_T$, où $T = \{3^n : n \in \mathbb{N}\}$. Nous pouvons utiliser la méthode de Rowland et Yassawi [41] pour obtenir cette suite comme la colonne d'un automate cellulaire linéaire de mémoire 2, avec une configuration initiale finie. Notons $\phi(m, n)$ la valeur de la cellule à la colonne $m \in \mathbb{Z}$ et à la ligne $n \in \mathbb{N}$. La règle locale obtenue pour engendrer le diagramme espace-temps est définie, pour tous $m \in \mathbb{Z}$ et $n \geq 2$, par : $\phi(m, n+2) = \phi(m+1, n) + \phi(m-2, n)$. En particulier toutes les lignes de rang pair contiennent uniquement des 0. Pour plus de lisibilité, nous représentons les 0 par des cellules vides. Comme dans les autres exemples d'automates cellulaires, nous gardons la convention du temps qui s'écoule vers le haut. Les quatre premières lignes correspondent aux conditions initiales, et la suite $(u_n)_{n \geq 0}$ apparaît dans la colonne encadrée en rouge. Le diagramme espace-temps après recodage est présenté dans la Figure 2.14 .

Remarque 2.3.2. Le rayon de l'automate cellulaire permettant le recodage augmente avec la taille de l'alphabet.

Remarque 2.3.3. [28] Pour un alphabet plus grand $\mathcal{A} = \{0, \ldots, q-1\}$ avec $q > 2$, si $\mathcal{B}$ est un ensemble fini de symboles tel que $\mathcal{B} \supsetneq \mathcal{A}$, il est également possible de recoder les éléments de $\mathcal{B}$ par des blocs constitués uniquement d'éléments de $\mathcal{A}$. Supposons que $\mathcal{B} = \{0, \ldots, k-1\}$, avec $k > q$. On recode les k symboles de l'alphabet $\mathcal{B}$ par des mots de longueur $2k-1$, en utilisant l'application $\omega : \mathcal{B} \to \mathcal{A}^{2k-1}$ définie de la manière suivante :

$$\begin{aligned} &\omega(0) = \underbrace{00\cdots0}_{2k-1}, \\ &\omega(i) = i\underbrace{0\cdots0}_{i-1}1\underbrace{0\cdots0}_{2k-i-2} \quad \text{for } i \in \{1, \ldots, q-1\}, \\ \text{et} \quad &\omega(i) = 0\underbrace{0\cdots0}_{i-1}1\underbrace{0\cdots0}_{2k-i-2} \quad \text{for } i \in \{q, \ldots, k-1\}. \end{aligned}$$

Remarque 2.3.4. [28] Afin d'optimiser la taille des blocs dans le recodage, il existe différents résultats sur les *codes sans chevauchement* [7]. Deux mots u et v (non nécessairement distincts) sont dits avec chevauchement si un préfixe propre non vide de u est égal à un suffixe propre non vide de v, ou inversement. Un code $C \subseteq \mathcal{A}^n$ est dit sans chevauchement si pour tous (non nécessairement distincts) $u, v \in C$, les mots u et v sont sans chevauchement. Pour un entier $k \in \{0, \ldots, n-1\}$, il est possible de construire un code sans chevauchement $C_n^{(k)}$, de longueur n en considérant la famille de mots $c \in \mathcal{A}^n$ qui satisfait à la propriété suivante : $c_i = 0$ pour $1 \leq i \leq k$, $c_{k+1} = 1$, $c_n = 1$, et les suites $c_{k+2}, c_{k+3}, \ldots, c_{n-1}$ ne contiennent pas k occurrences consécutives de 0. Pour des références sur le sujet, on pourra consulter [10, 18, 26]. Notons $F_n^{(k)}$ le nombre de mots codes obtenus, qui est le cardinal de $C_n^{(k)}$. On peut vérifier que la suite $(F_n^{(k)})_{n \geq 1}$ satisfait à la relation de récurrence :

$$F_{n+k}^{(k)} = F_{n+k-1}^{(k)} + F_{n+k-2}^{(k)} + \cdots + F_{n+1}^{(k)} + F_n^{(k)},$$

ce qui correspond à la suite de Fibonacci d'ordre k (la suite d'ordre 2 étant la suite classique de Fibonacci).

Si $\mathcal{B}$ est un alphabet avec k lettres, on peut faire correspondre chaque lettre i pour $1 \leq i \leq k$ avec un mot code sans chevauchement, et faire correspondre 0 avec un bloc $0\cdots0$ de la même taille que les mots codes. L'ensemble obtenu n'est pas exactement un code sans chevauchement, mais c'est suffisant pour notre problème, car on peut déterminer localement les limites entre les blocs dès qu'un 1 apparaît quelque part, et l'automate cellulaire F est supposé 0-stable. Par exemple, pour une longueur $n = 9$, si on considère les mots commençant par deux 0, avec un 1 à la troisième position et un 1 à la dernière position, la construction précente donne 13 mots codes, et avec le recodage du symbole 0 par un bloc constitué uniquement de 0, cela permet de traiter un alphabet de 14 lettres. Si on compare avec l'application τ introduite précédemment, dès que l'alphabet contient plus de 5 lettres, la longueur du recodage est déjà plus grande que 9.

Remarque 2.3.5. [28] La Proposition 2.3.4 peut-être généralisée de la manière suivante. Soit $\pi : \mathcal{B} \to \mathcal{A}$ une projection de symbole à symbole de $\mathcal{B}$ vers $\mathcal{A}$. Supposons que $u \in \mathcal{B}^{\mathbb{N}}$ apparaît en colonne d'un automate cellulaire sur $\mathcal{B}$ avec une configuration initiale finie, et considérons la suite $v = \pi(u)$, définie par $v_n = \pi(u_n)$ pour tout $n \in \mathbb{N}$. Alors, la suite v apparaît en colonne d'un automate cellulaire sur $\mathcal{A}$ avec une configuration initiale finie.

2.4 Questions ouvertes

1. Le théorème de Rowland et Yassawi permet de construire explicitement toute suite q-automatique, lorsque q est une puissance d'un nombre premier. Qu'en est-t-il des suites k-automatiques lorsque k n'est pas une puissance d'un nombre premier ? Cette question apparaît déjà dans [41].
2. Nous avons obtenu une construction du mot de Fibonacci. Peut-on généraliser la construction au mot de Tribonacci, défini comme l'unique point fixe en partant de 0 du morphisme σ donné par $0 \mapsto 01$, $1 \mapsto 02$ et $2 \mapsto 0$? Si on note (t_n) la suite définissant le mot de Tribonacci, de manière analogue au mot de Fibonacci, on a pour tout $n \geq 5$,

$$t_{n+1} = t_n \cdot t_{n-1} \cdot t_{n-2} = \underbrace{t_{n-2} \cdot t_{n-3} \cdot t_{n-4} \cdot t_{n-2} \cdot t_{n-3}}_{t_n} \cdot t_{n-2} \cdot t_{n-3} \cdot t_{n-4} \cdot t_{n-2}.$$

On pourrait ainsi s'inspirer de la construction du mot de Fibonacci, mais cela semble plus difficile à obtenir de manière effective. Plus généralement, peut-on construire d'autres mots de k-bonacci ? Peut-on construire d'autres suites morphiques non-automatiques ?

Chapitre 3

Suites généralisées de Rudin–Shapiro et corrélations

Sommaire

Les résultats de cette partie ont fait l'objet d'une publication en 2020 [44]. Dans le Chapitre 1, nous avons défini la suite classique de Rudin–Shapiro, qui est une suite 2-automatique qui compte le nombre de blocs "11" dans la décomposition binaire de chaque entier. On peut obtenir explicitement l'automate fini qui l'engendre et la définir de manière récursive.

Par la suite, de nombreuses généralisations de cette suite sur des alphabets binaires ou de taille plus grande ont été introduites et étudiées. Les différentes constructions ont été obtenues en exploitant une ou plusieurs propriétés de la suite classique de Rudin–Shapiro et en faisant en sorte qu'elles soient conservées pour ses généralisations.

Dans une première partie, nous présenterons un historique de la suite de Rudin–Shapiro et différentes généralisations. La deuxième partie sera consacrée à l'étude des matrices de différence qui joueront un rôle essentiel dans la construction des suites généralisées de Rudin–Shapiro auxquelles nous nous intéresserons plus particulièrement. Enfin, la troisième partie sera consacrée aux résultats que nous avons obtenus [44] et qui étendent ceux de Grant, Shallit, et Stoll [20].

3.1 Suites de Rudin–Shapiro, différentes généralisations

Initialement, la suite de Rudin–Shapiro a été introduite par Shapiro [43] dans son mémoire de thèse en 1951. La même année, Golay a publié un article qui étudie cette suite du point de vue de la physique [19]. Ce n'est qu'en 1959 que Rudin, dont le nom est resté associé à la suite, l'étudiera [42].Étant donné que Rudin était dans le jury de thèse de master et dans celui de thèse de doctorat où Shapiro étudie ces notions, certains auteurs préconisent de l'appeler plutôt suite de Golay–Shapiro au lieu de suite de Rudin–Shapiro.

Pour plus de précision sur la paternité de cette suite, on pourra consulter le papier d'Allouche [1]. Dans ce chapitre, afin de rester cohérent avec nos résultats récemment publiés sur le sujet [44], nous garderons le nom de Rudin–Shapiro.

À l'origine, Shapiro cherchait à construire une suite $(\varepsilon_n)_{n\geq 0}$ à valeurs dans $\{-1,1\}$ telle que :

$$\forall N \geq 0, \quad \sup_{\theta\in\mathbb{R}} \left| \sum_{n<N} \varepsilon_n e^{in\theta} \right| \leq C\sqrt{N}. \tag{3.1}$$

où C est une constante absolue.
La méthode utilisée pour résoudre ce problème a été de définir deux suites de polynômes trigonométriques $P_n(x)$ et $Q_n(x)$ de manière récursive par :

$$\begin{aligned} P_{n+1}(x) &= P_n(x) + x^{2^n} Q_n(x) \\ Q_{n+1}(x) &= Q_n(x) - x^{2^n} P_n(x) \end{aligned}$$

avec $P_0(x) = Q_0(x) = 1$.
Les nombres ε_n pour $n < 2^k$ définis comme étant les coefficients du polynôme $P_k(e^{i\theta})$, de degré $2^k - 1$, satisfont à la propriété (3.1).

Plus tard, Brillhart et Carlitz [8] remarqueront que si $n = \sum_{i=0}^{l} a_i 2^i$ est la décomposition binaire de l'entier n, alors $\varepsilon_n = (-1)^{f(n)}$, où $f(n) = \sum_{i=0}^{l-1} a_{i+1}a_i$.
La suite introduite par Rudin et Shapiro est donc bien celle qui compte le nombre de blocs "11" dans l'écriture binaire de n.
La propriété (3.1) est souvent appelée propriété du "racine de N". De plus, on peut même montrer que pour la suite de Rudin–Shapiro on peut prendre $C = 2 + \sqrt{2}$.
Les premières généralisations de la suite de Rudin–Shapiro s'articulent autour de la propriété du "racine de N". La première est due à Rider [40] qui a démontré le résultat suivant.

Théorème 3.1.1. Soit r un nombre premier et $\alpha = \exp(2i\pi/r)$. Il existe une suite $(\varepsilon_r(n))_{n\geq 0}$ prenant les valeurs $1, \alpha, \ldots, \alpha^{r-1}$ et telle que pour tout $N \geq 1$ et tout $0 \leq \theta \leq 2\pi$:

$$\left| \sum_{n=1}^{N} \varepsilon_r(n) e^{in\theta} \right| \leq r(1+\sqrt{r})\sqrt{N}. \tag{3.2}$$

Pour établir ce résultat, Rider donne une construction explicite. Il définit des suites de polynômes par $P_0^0(x) = P_0^1(x) = \cdots = P_0^{r-1}(x) = x$ et pour tout $s \geq 0$ et $k \geq 0$,

$$P_{k+1}^s(x) = \sum_{j=0}^{r-1} x^{jr^k} \alpha^{sj} P_k^j(x).$$

La suite $(\varepsilon_r(n))_{n\geq 0}$ est définie comme étant le n-ème coefficient du polynôme P_k^0 pour $n < r^k$ et on peut vérifier qu'elle satisfait à la propriété (3.2).

Par la suite, Martine Queffélec [38] étendra cette généralisation sur $\mathbb{Z}/q\mathbb{Z}$ pour tout entier $q \geq 2$ de la manière suivante :
Notons

$$H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & z & z^2 & \cdots & z^{q-1} \\ 1 & z^2 & z^4 & \cdots & z^{2(q-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & z^{q-1} & z^{2(q-1)} & \cdots & z^{(q-1)(q-1)} \end{pmatrix},$$

où $z = \exp(2i\pi/q)$. On définit q suites de polynômes trigonométriques $(P_n^0), (P_n^1), \ldots, (P_n^{q-1})$ par :

$$\begin{pmatrix} P_{n+1}^0(t) \\ P_{n+1}^1(t) \\ \vdots \\ P_{n+1}^{q-1}(t) \end{pmatrix} = H \begin{pmatrix} P_n^0(t) \\ e^{iq^n t} P_n^1(t) \\ \vdots \\ (e^{iq^n t})^{q-1} P_n^{q-1}(t) \end{pmatrix},$$

où $P_0^j(t) = 1$ pour tout $j \in [\![0, q-1]\!]$.

Définition 3.1.1. On appelle suite de Rudin–Shapiro généralisée d'ordre q, la suite $(g_n)_{n\geq 0}$, dont les q^n premiers termes sont les coefficients du polynôme trigonométrique P_n^0, pour tout $n \in \mathbb{N}$.

On a alors le résultat suivant.

Proposition 3.1.1. Les suites de Rudin–Shapiro généralisée d'ordre q satisfont :

$$\left| \sum_{n=0}^{N-1} g_n e^{int} \right| \leq q(1+\sqrt{q})\sqrt{N}.$$

Ainsi, nous avons toujours la propriété du "racine de N" pour cette généralisation. Queffélec s'est notamment intéressée à l'étude spectrale de ces suites. Nous donnons son résultat principal

Théorème 3.1.2. La partie continue du spectre de la suite de Rudin–Shapiro généralisée d'ordre q a une composante de Lebesgue de multiplicité $q\varphi(q)$, où φ désigne l'indicatrice d'Euler, et pour chaque diviseur d non trivial de q, un produit de Riesz généralisé, de multiplicité $d\varphi(d)$.

Allouche et Liardet [4] ont également étudié des propriétés de mesures spectrales de suites généralisées de Rudin–Shapiro qui étendent la construction de Queffélec et ont prouvé que ces suites avaient encore la mesure de Lebesgue comme mesure spectrale. Cependant nous ne développerons pas ces aspects. La généralisation de Rudin–Shapiro à laquelle nous nous intéresserons est celle qui a été étudiée par Grant, Shallit et Stoll [20]. Un cas particulier de cette généralisation est la famille de suites que nous avons introduite au Chapitre 1 dans la Remarque 1.1.4 et dont nous avons montré au Chapitre 2 qu'il était possible de les construire en colonne d'un automate cellulaire linéaire dont on peut expliciter la règle. Notons également que ces suites coïncident avec celles introduites par Martine Queffélec dans le cas où la taille de l'alphabet est un nombre premier. Mais avant cela, nous allons introduire les matrices de différence qui joueront un rôle clé dans l'étude des suites généralisées de Rudin–Shapiro introduites par Grant, Shallit, et Stoll.

3.2 Matrices de différence et applications

3.2.1 Définitions et exemples de construction

Les matrices de différence constituent un vaste sujet pour lequel les applications sont multiples, dont notamment la construction de matrices de Hadamard, de carrés latins, de tableaux orthogonaux ou encore les codes correcteurs. Dans cette partie nous nous appuyerons essentiellement sur [21] et [24]. Sans perte de généralité, nous échangerons le rôle des lignes et des colonnes par rapport à ces deux références.

Dans toute la suite nous utiliserons les notations suivantes $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}_p^k = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{k}$.

Définition 3.2.1 ([21, 24])**.** Soit $(G, +)$ un groupe abélien fini d'ordre s. Une *matrice de différence* $D = (d_{ij})$ de taille $r \times c$ à coefficients dans G, est une matrice telle que pour tout i et j avec $1 \leq i, j \leq c$, $i \neq j$, l'ensemble

$$\{d_{li} - d_{lj} : 1 \leq l \leq r\}$$

contient chaque élément de G avec le même nombre d'occurrences.

Exemple 3.2.1. $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$ est une matrice de différence sur $\mathbb{Z}_3$.

On notera $D(r, c, G)$ l'ensemble de toutes les matrices de différence de tailles $r \times c$ à coefficients dans le groupe G.

Exemple 3.2.2. [21, Example 6.3] Soit k un nombre premier. Alors, la matrice carrée $A = (a_{ij})$ de taille $k \times k$ définie par $a_{ij} = ij \bmod k$ pour tout i et pour tout j tels que $1 \leq i, j \leq k$ est une matrice de $D(k, k, \mathbb{Z}_k)$.

Il existe d'autres constructions explicites de matrice de différence. Cependant, en fonction du groupe que l'on choisit et de la taille de la matrice, cela n'est pas toujours possible, comme le montre le résultat suivant qui se démontre de manière élémentaire.

Proposition 3.2.1. [17, Lemma 3.1] Soit k un nombre pair avec $k \geq 4$. L'ensemble $D(k, k, \mathbb{Z}_k)$ est vide.

Démonstration. Soit k un nombre pair supérieur ou égal à 4. Pour $0 \leq i, j \leq k-1$ avec $i \neq j$ on note D_{ij} le vecteur colonne obtenu en faisant la différence modulo k (dans le sens où les valeurs sont prises sur $\mathbb{Z}_k$) entre la colonne C_i et la colonne C_j. On note Σ_{ij} la somme des coefficients du vecteur D_{ij}.
Supposons par l'absurde qu'il existe une matrice appartenant à $D(k, k, \mathbb{Z}_k)$. Notons $C_0, \ldots, C_{k-1}$ ses colonnes. Par hypothèse, pour tout $i \neq j$, chaque colonne D_{ij} est une permutation des éléments de $\mathbb{Z}_k$. Ainsi, pour tous $0 \leq i, j \leq k-1$ avec $i \neq j$ on a $\Sigma_{ij} = \frac{k(k-1)}{2}$. Comme k est pair, on a $\frac{k(k-1)}{2} \equiv \frac{k}{2} \bmod k$. Ainsi pour tous i et j tels que $0 \leq i, j \leq k-1$ avec $i \neq j$ on a $\Sigma_{ij} \equiv \frac{k}{2} \bmod k$. Comme $k \geq 3$ il y a au moins trois colonnes et on peut donc considérer Σ_{01}, Σ_{12} et Σ_{02}. Par hypothèse on a $\Sigma_{01} \equiv \frac{k}{2} \bmod k$, $\Sigma_{12} \equiv \frac{k}{2} \bmod k$ et $\Sigma_{02} \equiv \frac{k}{2} \bmod k$. De plus $\Sigma_{01} + \Sigma_{12} \equiv \Sigma_{02} \bmod k$. Or $\Sigma_{02} = \Sigma_{01} + \Sigma_{12} \equiv \frac{k}{2} + \frac{k}{2} \bmod k \equiv 0 \bmod k$. D'où la contradiction. □

En particulier l'ensemble $D(4, 4, \mathbb{Z}_4)$ est vide. Autrement dit il n'existe pas de matrice carrée de différence de taille 4 sur $\mathbb{Z}_4$. En revanche, l'ensemble $D(4, 4, \mathbb{Z}_2 \times \mathbb{Z}_2)$ est non vide. En effet on peut vérifier aisément que la matrice

$$M = \begin{pmatrix} (0,0) & (0,0) & (0,0) & (0,0) \\ (0,0) & (0,1) & (1,0) & (1,1) \\ (0,0) & (1,0) & (1,1) & (0,1) \\ (0,0) & (1,1) & (0,1) & (1,0) \end{pmatrix} \tag{3.3}$$

est un élément de cet ensemble [21, Table 6.22].
De manière générale nous avons le résultat suivant :

Théorème 3.2.1. [21, Theorem 6.6] Pour tout nombre premier p et tous entiers k et n tels que $k \geq n \geq 1$, il existe un groupe abélien G de cardinal p^n tel que l'ensemble $D(p^k, p^k, G)$ soit non vide.

Démonstration. Soit $\mathbb{F}_{p^k}$ le corps fini a p^k éléments. Représentons ses éléments sous la forme polynomiale

$$\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} + \cdots + \beta_{m-1} x^{m-1}$$

où $\beta_0, \ldots, \beta_{m-1} \in \mathbb{Z}_p$.
Le corps fini $\mathbb{F}_{p^n}$ peut être vu comme un sous-groupe additif de $\mathbb{F}_{p^k}$ en identifiant ses éléments sous la forme $\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}$. (Bien que la multiplication des éléments de $\mathbb{F}_{p^n}$ soit généralement différente dans $\mathbb{F}_{p^k}$ ce n'est pas un problème ici car seule la structure additive de $\mathbb{F}_{p^n}$ nous intéresse). Notons D^* la table de multiplication de $\mathbb{F}_{p^k}$.
Soit $\phi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^n}$ l'application qui associe à chaque élément $\beta_0 + \beta_1 x + \cdots + \beta_{m-1} x^{m-1}$ de D^* l'élément $\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}$. Appliquons ϕ à chaque élément de la table D^* et notons D la nouvelle table ainsi obtenue. Alors D est une matrice de différence de $D(p^k, p^k, \mathbb{F}_{p^n})$. En effet, par construction D est bien une matrice de taille $p^k \times p^k$ dont les coefficients sont des éléments de $\mathbb{F}_{p^n}$.
Notons $\alpha_0, \ldots, \alpha_{p^k-1}$ les éléments de $\mathbb{F}_{p^k}$. Alors la différence entre deux colonnes de la matrice D peut s'écrire sous la forme

$$\begin{pmatrix} \phi(\beta\alpha_0) \\ \vdots \\ \phi(\beta\alpha_{p^k-1}) \end{pmatrix} - \begin{pmatrix} \phi(\gamma\alpha_0) \\ \vdots \\ \phi(\gamma\alpha_{p^k-1}) \end{pmatrix}$$

où $\beta, \gamma \in \mathbb{F}_{p^k}, \beta \neq \gamma$.

De plus par définition de ϕ on a $\phi(\beta\alpha_i) - \phi(\gamma\alpha_i) = \phi(\beta\alpha_i - \gamma\alpha_i)$. La différence entre deux colonnes s'écrit alors

$$\begin{pmatrix} \phi((\beta-\gamma)\alpha_0) \\ \vdots \\ \phi((\beta-\gamma)\alpha_{p^k-1}) \end{pmatrix}.$$

Comme chaque élément de $\mathbb{F}_{p^k}$ apparaît une fois parmi les éléments $(\beta-\gamma)\alpha_i,\ 0 \leq i < p^k$, chaque élément de $\mathbb{F}_{p^k}$ apparaît p^{m-n} fois parmi les éléments $\phi((\beta-\gamma)\alpha_i),\ 0 \leq i < p^k$. □

Exemple 3.2.3. À partir de la table du corps fini $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1)$, on obtient la matrice de $D(8,8,\mathbb{Z}_2^3)$ suivante :

$$\begin{pmatrix}
(0,0,0) & (0,0,0) & (0,0,0) & (0,0,0) & (0,0,0) & (0,0,0) & (0,0,0) & (0,0,0) \\
(0,0,0) & (0,0,1) & (0,1,0) & (0,1,1) & (1,0,0) & (1,0,1) & (1,1,0) & (1,1,1) \\
(0,0,0) & (0,1,0) & (1,0,0) & (1,1,0) & (0,1,1) & (0,0,1) & (1,1,1) & (1,0,1) \\
(0,0,0) & (0,1,1) & (1,1,0) & (1,0,1) & (1,1,1) & (1,0,0) & (0,0,1) & (0,1,0) \\
(0,0,0) & (1,0,0) & (0,1,1) & (1,1,1) & (1,1,0) & (0,1,0) & (1,0,1) & (0,0,1) \\
(0,0,0) & (1,0,1) & (0,0,1) & (1,0,0) & (0,1,0) & (1,1,1) & (0,1,1) & (1,1,0) \\
(0,0,0) & (1,1,0) & (1,1,1) & (0,0,1) & (1,0,1) & (0,1,1) & (0,1,0) & (1,0,0) \\
(0,0,0) & (1,1,1) & (1,0,1) & (0,1,0) & (0,0,1) & (1,1,0) & (1,0,0) & (0,1,1)
\end{pmatrix}$$

Exemple 3.2.4. Hedayat, Sloane, et Stufken [21, Table 6.9] donnent un exemple de matrice de $D(9,9,\mathbb{Z}_3)$ à partir de la table du corps fini $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+1)$ à 9 éléments :

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\
0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\
0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\
0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\
0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\
0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\
0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\
0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0
\end{pmatrix}$$

L'existence des matrices de différence a été largement étudiée. Le Théorème 3.2.1 donne une méthode explicite pour construire une matrice de différence dont les paramètres sont donnés. Cependant, ce n'est pas la seule manière qui existe pour construire des matrices de différence.

Théorème 3.2.2. [21, Theorem 6.33] Pour tout nombre premier impair p et pour tout entier $n \geq 1$, il existe un groupe abélien G de cardinal p^n tel que l'ensemble $D(2p^n, 2p^n, G)$ soit non vide.

Construction 3.2.1. Nous présentons uniquement la construction d'une telle matrice de différence. Pour les détails de la preuve que la matrice obtenue est bien un élément de $D(2p^n, 2p^n, G)$ nous référons à [21].

Soit α un élément primitif du corps fini $\mathbb{F}_{p^n}$. Notons $\alpha_0, \alpha_1, \ldots, \alpha_{p^n-1}$ les éléments de $\mathbb{F}_{p^n}$, où $\alpha_0 = 0$ et pour tout $i \in [\![1, p^n-1]\!], \alpha_i = \alpha^i$. En particulier, on a $\alpha_{p^n-1} = \alpha^{p^n-1} = 1$.
On construit quatre matrices de taille $p^n \times p^n$, $U = (u_{ij}), V = (v_{ij}), W = (w_{ij}), X = (x_{ij})$, avec $0 \leq i, j \leq p^n - 1$, définies par :

$$\begin{aligned} u_{ij} &= \alpha_i\alpha_j, \\ v_{ij} &= \alpha_i\alpha_j + \beta\alpha_j^2, \\ w_{ij} &= \alpha_i\alpha_j + \gamma\alpha_i^2, \\ x_{ij} &= \nu\alpha_i\alpha_j + \delta\alpha_j^2 + \varepsilon\alpha_i^2, \end{aligned}$$

où $\beta, \gamma, \delta, \varepsilon, \nu$ sont des éléments de $\mathbb{F}_{p^n}$ qui satisfont à

$$\begin{aligned} &\nu \text{ n'est pas un carré dans } \mathbb{F}_{p^n}, \\ &\nu = 1 + 4\beta\varepsilon = \frac{\varepsilon}{\gamma} = \nu^2 - 4\delta\varepsilon. \end{aligned} \tag{3.4}$$

En particulier, pour satisfaire à la condition (3.4) on peut prendre

$$\nu = \alpha,\ \beta = \frac{1}{2},\ \gamma = \frac{\alpha - 1}{2\alpha},\ \delta = \frac{\alpha}{2}, \varepsilon = \frac{\alpha - 1}{2}. \tag{3.5}$$

Alors, si G désigne le groupe additif de $\mathbb{F}_{p^n}$, la transposée de la matrice par blocs

$$\begin{pmatrix} U & W \\ V & X \end{pmatrix}$$

est un élément de $D(2p^n, 2p^n, G)$.

Exemple 3.2.5. [21, Table 6.37] Pour $p = 3$ et $n = 1$, on peut prendre $\alpha = 2$ comme élément primitif de $\mathbb{F}_3$, de sorte qu'avec les notations précédentes on ait $\alpha_0 = 0, \alpha_1 = 2^1 = 2, \alpha_2 = 2^2 = 1$. En prenant la condition particulière (3.5) pour satisfaire à la condition (3.4), on obtient les matrices

$$U = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \quad V = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad W = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 & 1 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{pmatrix}$$

et ainsi, la matrice

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 2 & 2 \\ 0 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 1 & 2 \end{pmatrix}$$

est un élément de $D(6, 6, \mathbb{Z}_3)$.

Exemple 3.2.6. [21, Theorem 6.35] De la même manière, on peut obtenir la matrice suivante, qui est un élément de $D(10, 10, \mathbb{Z}_5)$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 3 & 1 & 2 & 2 & 1 & 0 & 3 & 4 \\ 0 & 3 & 1 & 2 & 4 & 3 & 1 & 4 & 0 & 2 \\ 0 & 1 & 2 & 4 & 3 & 2 & 3 & 4 & 1 & 0 \\ 0 & 2 & 4 & 3 & 1 & 3 & 0 & 2 & 1 & 4 \\ 0 & 1 & 4 & 1 & 4 & 0 & 2 & 3 & 2 & 3 \\ 0 & 0 & 2 & 2 & 1 & 4 & 4 & 3 & 3 & 1 \\ 0 & 4 & 0 & 3 & 3 & 1 & 4 & 1 & 2 & 2 \\ 0 & 2 & 1 & 0 & 2 & 4 & 3 & 1 & 4 & 3 \\ 0 & 3 & 3 & 4 & 0 & 1 & 2 & 2 & 4 & 1 \end{pmatrix}$$

Nous donnons maintenant quelques résultats sur les matrices de différence de taille impaire.

Théorème 3.2.3. [21, Theorem 6.65] Soit c un nombre impair et soit G un groupe abélien d'ordre s. Supposons que l'ensemble $D(c, c, G)$ est non vide. Si p est un nombre premier impair divisant s, et $b \not\equiv 0 \bmod p$ un entier divisant la partie sans facteur carré de c, alors l'ordre multiplicatif de $b \equiv 0 \bmod p$ est impair.

Théorème 3.2.4. [17, Theorem 3.2.] Il existe des matrices de différence dans $D(g, 3, \mathbb{Z}_g)$ si et seulement si $g \geq 3$ et g est impair.

Théorème 3.2.5. [17, Theorem 3.12.] Si $g \geq 5$ est un nombre impair tel que $\text{pgcd}(g, 27) \neq 9$ alors l'ensemble $D(g, 4, \mathbb{Z}_g)$ est non vide.

Une recherche informatique, permet de montrer que l'ensemble $D(9, 4, \mathbb{Z}_9)$ est vide (voir [17, Lemma 3.9.]). On pourra également consulter la Table 1 de [17] qui liste les ensembles $D(g, k, \mathbb{Z}_g)$ non vides pour tous les nombres impairs $3 \leq g \leq 299$.

3.2.2 Classification des matrices de différence

Lampio et Östergård [24, 25] proposent une classification des matrices de différence. Pour cela, ils définissent une relation d'équivalence dans l'ensemble de toutes les matrices de différence, qui à partir d'une matrice de différence donnée, en génère une autre avec les mêmes paramètres (le nombre de lignes, le nombre de colonnes, et le groupe sous-jacent) en utilisant les opérations suivantes.

1. Permuter l'ordre des lignes.
2. Permuter l'ordre des colonnes.
3. Ajouter un élément fixé du groupe G à une ligne.
4. Ajouter un élément fixé du groupe G à une colonne.
5. Appliquer un automorphisme du groupe G à chaque élément de la matrice de différence.

Définition 3.2.2 ([25])**.** On dit que deux matrices de différence A et B sont *équivalentes*, et on note $A \cong B$, si elles ont les mêmes paramètres et que B peut être obtenue à partir de A en appliquant les Opérations 1-5 un nombre fini de fois.

La relation $\cong$ est une relation d'équivalence dans l'ensemble de toutes les matrices de différence, et chaque classe d'équivalence est un sous-ensemble de l'ensemble des matrices de différence avec les mêmes paramètres.

Définition 3.2.3 ([25])**.** Soit G un groupe abélien avec un ordre total $\leq_G$ sur les éléments, où l'élément identité de G est l'élément minimal pour cet ordre. Une matrice de différence de $D(r, c, G)$ est une *matrice de différence ordonnée-normalisée* si

1. la première ligne contient uniquement l'élément identité,
2. la première colonne contient uniquement l'élément identité,
3. les lignes sont rangées dans l'ordre lexicographique croissant du haut vers le bas (induit par $\leq_G$ sur les vecteurs lignes), et
4. les colonnes sont rangées dans l'ordre lexicographique croissant de la gauche vers la droite (induit par $\leq_G$ sur les vecteurs colonnes).

Théorème 3.2.6 ([25])**.** Chaque matrice de différence de $D(r, c, G)$ est équivalente à une matrice de différence ordonnée-normalisée de $D(r, c, G)$.

La preuve consiste à utiliser les Opérations 1, 2, 3 et 4 qui définissent la relation d'équivalence et ainsi construire une matrice de différence ordonnée-normalisée à partir de la matrice de différence donnée de $D(r, c, G)$.

Remarque 3.2.1. Ce résultat implique qu'il suffit d'étudier les matrices de différence ordonnées-normalisées dans la recherche de l'existence des matrices de différence dont les paramètres sont donnés.

r	c	G	#
r	2	$\mathbb{Z}_2$	1
3	3	$\mathbb{Z}_3$	1
6	6	$\mathbb{Z}_3$	1
9	9	$\mathbb{Z}_3$	2
12	12	$\mathbb{Z}_3$	1
15	9	$\mathbb{Z}_3$	5
18	18	$\mathbb{Z}_3$	53
4	2	$\mathbb{Z}_4$	1
8	4	$\mathbb{Z}_4$	6
12	2	$\mathbb{Z}_4$	1
16	16	$\mathbb{Z}_4$	13
20	2	$\mathbb{Z}_4$	1

r	c	G	#
4	4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1
8	8	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1
12	12	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1
16	16	$\mathbb{Z}_2 \times \mathbb{Z}_2$	226
5	5	$\mathbb{Z}_5$	1
10	10	$\mathbb{Z}_5$	1
15	8	$\mathbb{Z}_5$	2
6	2	$\mathbb{Z}_6$	1
4	12	$\mathbb{Z}_6$	7
18	2	$\mathbb{Z}_6$	1
7	7	$\mathbb{Z}_7$	1
14	14	$\mathbb{Z}_7$	2

Remarque 3.2.2. La preuve du Théorème 3.2.1 donne une construction d'une matrice de différence qui remplit déjà les conditions 1 et 2 dans la définition des matrices de différence ordonnées-normalisées. Il suffit alors de permuter les lignes et les colonnes pour obtenir les matrices de différence ordonnées-normalisées qui sont dans la même classe d'équivalence.

La Table 2 de [25] donne le nombre de classes d'équivalence des matrices de différence selon les paramètres.

Exemple 3.2.7. Dans $D(9, 9, \mathbb{Z}_3)$, il y a deux classes d'équivalence de matrice de différence. Un représentant de chacune des deux classes est donné dans [25] :

$$\begin{pmatrix} 0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&2&2&2\\ 0&0&0&2&2&2&1&1&1\\ 0&1&2&0&1&2&0&1&2\\ 0&1&2&1&2&0&2&0&1\\ 0&1&2&2&0&1&1&2&0\\ 0&2&1&0&2&1&0&2&1\\ 0&2&1&1&0&2&2&1&0\\ 0&2&1&2&1&0&1&0&2 \end{pmatrix} \qquad \begin{pmatrix} 0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&1&2&2&2\\ 0&0&0&2&2&2&1&1&1\\ 0&1&2&0&1&2&0&1&2\\ 0&1&2&1&2&0&2&0&1\\ 0&1&2&2&0&1&1&2&0\\ 0&2&1&0&2&1&1&0&2\\ 0&2&1&1&0&2&0&2&1\\ 0&2&1&2&1&0&2&1&0 \end{pmatrix}$$

Remarque 3.2.3. En permutant les lignes, la matrice obtenue dans l'Exemple 3.2.4 est équivalente à la matrice de différence ordonnée-normalisée de gauche dans l'Exemple 3.2.7. Par conséquent, la matrice de la seconde classe d'équivalence a été nécessairement obtenue d'une autre manière.

Lampio [24] a entrepris de faire la classification de toutes les matrices de différence de $D(r, c, G)$ où le nombre de lignes $r < 20$ et où G est un groupe abélien d'ordre g avec $3 \leq g \leq 7$.
Notons que pour tout r il y a une unique classe d'équivalence dans $D(r, 2, \mathbb{Z}_2)$ dans le cas où cet ensemble est non vide.
Le tableau suivant liste tous les cas possibles des matrices de différence que l'on peut construire avec la restriction sur la taille des paramètres que nous avons imposée. On constate que le nombre de classes d'équivalence peut être très élevé. De plus, Lampio donne un exemple pour chaque classe d'équivalence d'un représentant sous la forme ordonnée normalisée. [2]

3.2.3 Application aux matrices de Hadamard

Nous allons voir que les matrices de différence sont reliées aux matrices de Hadamard, qui jouent un rôle important dans les codes correcteurs, par exemple.

2. `https://wiki.aalto.fi/display/DifferenceMatrices/Home` (consulté le 16/12/2020)

Définition 3.2.4. [21] Soit $n \geq 1$. Une matrice de Hadamard d'ordre n est une matrice H_n de taille $n \times n$ de 1 et de -1 telle que les lignes sont orthogonales. Autrement dit, H_n vérifie la relation :

$$H_n {}^t H_n = nI_n,$$

où ${}^t H_n$ désigne la matrice transposée de H_n.

Exemple 3.2.8. [21] Par exemple, les matrices suivantes d'ordres $1, 2$ et 4 sont des matrices de Hadamard :

$$H_1 = \begin{pmatrix} 1 \end{pmatrix} \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Remarque 3.2.4. [21] Si H_n est une matrice de Hadamard d'ordre n, alors $H_n^{-1} = n^{-1} {}^t H_n$ et donc on a également :

$${}^t H_n H_n = nI_n,$$

ce qui implique que les colonnes de H_n sont aussi orthogonales.

En utilisant les relations d'orthogonalité on peut montrer le résultat suivant

Proposition 3.2.2 (Corollary 7.2.)**.** [21] Si une matrice de Hadamard H_n existe alors $n = 1, n = 2$ ou n est un multiple de 4.

La réciproque de ce résultat, i.e., montrer que l'on peut toujours construire une matrice de Hadamard H_n si n est un multiple de 4 (les cas $n = 1$ et $n = 2$ étant traités dans l'Exemple 3.2.8) est connue sous le nom de conjecture de Hadamard et reste un domaine actif de la recherche. Actuellement, le plus petite multiple de 4 pour lequel on ne connaît pas de construction d'une matrice de Hadamard est 668 [24].

Le résultat suivant, fait le lien entre les matrices de Hadamard et les matrices de différence.

Théorème 3.2.7 (Theorem 7.6.)**.** [21] Une matrice de Hadamard H_n existe si et seulement s'il existe une matrice de différence dans $D(n, n, \mathbb{Z}_2)$.

3.3 Corrélations discrètes d'ordre 2 de suites généralisées de Rudin–Shapiro

Nous avons maintenant tous les outils nécessaires pour parler de la généralisation de Rudin–Shapiro introduite par Grant, Shallit, et Stoll [20] ainsi que des extensions que nous avons obtenues.

Dans toute cette section nous utiliserons la notation $\mathrm{e}(x) = e^{2i\pi x}$ pour tout $x \in \mathbb{R}$. Nous utiliserons la notation de Bachmann–Landau usuelle $O()$ pour les termes d'erreur. Nous ajouterons un indice pour indiquer une éventuelle dépendance de la constante implicite (par exemple $O_k()$ pour une dépendance en k). Nous utiliserons également la notation classique de Vinogradov $\ll$.

3.3.1 État de l'art

Dans leurs deux articles [32, 33], Mauduit et Sárközy s'intéressent au caractère pseudo-aléatoire de suites binaires, par rapport aux progressions arithmétiques, aux faibles (auto-)corrélations et à la normalité. Pour une suite binaire $E_N = \{e_1, e_2, \ldots, e_N\} \in \{-1, 1\}^N$ et pour un vecteur $\mathbf{r} = (r_1, \ldots, r_m)$ satisfaisant à $0 \leq r_1 < \cdots < r_m$ on considère la quantité :

$$V(E_N, M, \mathbf{r}) \sum_{n=1}^{M} e_{n+r_1} e_{n+r_2} \cdots e_{n+r_m}.$$

La mesure de corrélation d'ordre m de E_N est définie par :

$$C_k(E_N) = \max_{M, \mathbf{r}} |V(E_N, M, \mathbf{r})|,$$

où le maximum est pris sur tous les $\mathbf{r} = (r_1, \ldots, r_m)$ tels que $0 \leq r_1 < \cdots < r_m$ et M tel que $M + r_m \leq N$.

Dans la lignée de travaux de Grant, Shallit, et Stoll [20], nous nous sommes intéressés aux corrélations discrètes de suites infinies de k symboles, où nous détectons lorsque deux symboles sont identiques ou non. Nous définissons alors une autre mesure de corrélation.

Définition 3.3.1. Soit $k \geq 2$ un entier et soit $x = x_0 x_1 \cdots$ un mot infini sur l'alphabet $\{0, 1, \ldots, k-1\}$. Soit $m \geq 2$. Pour un vecteur $(i_1, \ldots, i_m)$ satisfaisant à $0 \leq i_1 < \cdots < i_m$, on définit *le coefficient de corrélation discrète* $\delta(i_1, \ldots, i_m)$ d'ordre m par

$$\delta(i_1, \ldots, i_m) = \begin{cases} 0, & \text{si } x_{i_1} = \cdots = x_{i_m}, \\ 1, & \text{sinon.} \end{cases}$$

De plus, on définit $C_{\mathbf{r}}$ pour tout $\mathbf{r} = (r_1, \ldots, r_m)$ avec $0 \leq r_1 < \cdots < r_m$ par

$$C_{\mathbf{r}} = \liminf_{N \to \infty} \frac{1}{N} \sum_{n < N} \delta(n + r_1, \ldots, n + r_m).$$

La quantité $C_{\mathbf{r}}$ mesure en quelque sorte le "pseudo-aléa" d'une suite (voir la remarque suivante). Nous permettons à $\mathbf{r}$ de dépendre de n ce qui généralise grandement le cas où l'on fixe un vecteur constant $\mathbf{r} = (r_1, \ldots, r_m)$.

Remarque 3.3.1. Pour une suite aléatoire où chaque lettre est tirée indépendamment avec probabilité $1/k$ on a $C_{\mathbf{r}} = 1 - 1/k^{m-1}$ avec probabilité 1.

Démonstration. On définit la suite de variables aléatoires $(X_n)_{n \geq 0}$ par

$$X_n = \delta(n + r_1, n + r_2, \ldots, n + r_m).$$

Elles suivent une loi de Bernoulli de paramètre $1 - 1/k^{m-1}$. Décomposons selon les congruences modulo r_2. On a

$$\begin{aligned} \frac{1}{N} \sum_{n < N} X_n &= \frac{1}{N} \left(\sum_{\substack{n < N \\ n \equiv 0 \bmod r_2}} X_n + \cdots + \sum_{\substack{n < N \\ n \equiv r_2 - 1 \bmod r_2}} X_n \right) \\ &= \frac{1}{r_2} \left(\frac{r_2}{N} \sum_{\substack{n < N \\ n \equiv 0 \bmod r_2}} X_n + \cdots + \frac{r_2}{N} \sum_{\substack{n < N \\ n \equiv r_2 - 1 \bmod r_2}} X_n \right). \end{aligned}$$

Chaque somme est constituée de $\lfloor N/r_2 \rfloor$ variables aléatoires indépendantes suivant une loi de Bernoulli. D'après la loi des grands nombres, chacune de ces sommes multipliée par $\dfrac{r_2}{N}$ converge avec probabilité 1 vers $\mathbb{E}(X_n) = 1 - 1/k$. Comme il y a r_2 sommes on a bien le résultat annoncé. □

Dans la suite, sauf mention contraire, nous nous intéresserons au cas où $m = 2$. Nous rappelons les propriétés de récursivité qui permettent de définir la suite de Rudin–Shapiro classique.

Remarque 3.3.2. La suite de Rudin–Shapiro peut être définie de la manière suivante :

$$r_0 = 0 \text{ et } r_{2n+j} = (r_n + g(j, n)) \bmod 2$$

avec $g(j, n) = \begin{cases} 1, & \text{si } j = 1,\ n \equiv 1 \pmod 2, \\ 0, & \text{sinon.} \end{cases}$

À partir de cette observation, Grant, Shallit, et Stoll [20] ont donné une définition de suites généralisées de Rudin–Shapiro.

Définition 3.3.2. Soit

$$\begin{aligned} g : \{0,1,\dots,k-1\} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (j,n) &\longmapsto g(j,n) \end{aligned}$$

telle que pour tout j, la fonction $n \mapsto g(j,n)$ est k-périodique. De plus, on définit g telle que pour tous entiers $u, i \in \mathbb{N}$ avec $0 \leq u < u+i \leq k-1$ on ait

$$\{(g(u+i,n) - g(u,n)) \bmod k : 0 \leq n \leq k-1\} = \{0,1,\dots,k-1\}.$$

Une suite $(\hat{a}(n))_{n\geq 0}$ sur l'alphabet $\{0,1,\dots,k-1\}$ est appelée une *suite généralisée de Rudin–Shapiro* s'il existe une suite d'entiers $(a(n))_{n\geq 0}$ telle que $\hat{a}(n) \equiv a(n) \bmod k$ et

$$a(nk+j) = a(n) + g(j,n) \quad \text{for } 0 \leq j \leq k-1,\ n \geq 1.$$

Remarque 3.3.3. Afin de définir complètement la suite, on peut fixer (arbitrairement) les premières valeurs $a(0),\dots,a(k-1)$ et les autres sont obtenues récursivement par la relation.

Remarque 3.3.4. Si l'on représente $g(j,n)$ comme le coefficient de la j-ième colonne et de la n-ième ligne d'une matrice de taille k, alors la propriété 3.3.2 peut être vue comme la différence entre deux colonnes distinctes de la matrice. Ainsi l'existence de telles fonctions g est reliée à l'existence de matrices de différence correspondantes.

Nous présentons ici les deux résultats principaux de Grant, Shallit, et Stoll [20].

Théorème 3.3.1 (Theorem 3.1)**.** [20] Soit $(\hat{a}(n))_{n\geq 0}$ une suite généralisée de Rudin–Shapiro sur $\{0,1,\dots,k-1\}$ avec k premier. De plus, soient r_1 et r_2 tels que $0 \leq r_1 < r_2$. Alors, quand $N \to \infty$, on a

$$\sum_{n<N} \delta(n+r_1, n+r_2) = N\left(1-\frac{1}{k}\right) + O_k\left((r_2-r_1)\log\frac{N}{r_2-r_1} + r_2\right).$$

Notons que le terme principal correspond exactement à celui obtenu dans le cas probabiliste.
Maintenant, en utilisant une bijection entre $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_d}$ et $\mathbb{Z}_{p_1\cdots p_d}$, il est possible de construire une suite sur un alphabet dont la taille est sans facteur carré et obtenir une propriété similaire pour les corrélations d'ordre 2 de la suite.

Théorème 3.3.2 (Theorem 3.3)**.** [20] Soit $d \geq 2$ et soit $k = p_1 \cdots p_d$ un produit de nombres premiers deux à deux distincts. Soit $c_1 = 1$ et $c_i = p_1 \cdots p_{i-1}$ pour $2 \leq i \leq d$. On définit la suite $(\hat{a}(n))_{n\geq 0}$ par

$$\hat{a}(n) \equiv a(n) \bmod k,$$

où $(a(n))_{n\geq 0}$ est définie par $a(n) = c_1 a_1(n) + \cdots + c_d a_d(n)$ et $(a_i(n))_{n\geq 0}$ satisfait la relation de récurrence

$$a_i(p_i n + j) = a_i(n) + g_i(j,n), \quad 1 \leq i \leq d,$$

pour $n \geq 1$ et $0 \leq j \leq p_i - 1$ et où les g_i sont des fonctions qui satisfont les conditions de la Définition 3.3.2. De plus, soient r_1 et r_2 tels que $0 \leq r_1 < r_2$ et $0 < \gamma < 1$. Alors, quand $N \to \infty$, on a

$$\begin{aligned} &\sum_{n<N} \delta(n+r_1, n+r_2) \\ &= N\left(1-\frac{1}{k}\right) + O_k\left((r_2-r_1)N^{1-\frac{\gamma}{d}} + (r_2-r_1)N^{1-\gamma}\log\frac{N^{\frac{\gamma}{d}}}{r_2-r_1} + N^{\gamma} + r_2\right). \end{aligned}$$

Remarque 3.3.5. La construction précédente ne peut pas être utilisée pour un alphabet dont la taille n'est pas sans facteur carré, car la preuve du Théorème 3.3.2 utilise le résultat du Théorème 3.3.1 qui est seulement valable pour un nombre premier et non une puissance d'un nombre premier. Pour contourner cet obstacle, nous allons utiliser de nouvelles constructions obtenues grâce aux matrices de différence.

3.3.2 Résultats principaux

Dans un premier temps, nous donnons un résultat pour les alphabets dont la taille est une puissance d'un nombre premier. La preuve reprend essentiellement les arguments de celle du Théorème 3.3.1, dont nous donnons les détails dans la sous-section 3.3.3.
À partir du Théorème 3.2.1, nous allons définir une généralisation de la Définition 3.3.2 pour les puissances de nombres premiers.

Définition 3.3.3. Soit p un nombre premier, soit $k \geq 1$ et soit $M = (m_{ij})_{\substack{0\leq i<p^k \\ 0\leq j<p^k}}$ une matrice de différence de $D(p^k, p^k, \mathbb{Z}_p^k)$. Soit

$$\begin{aligned} g : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z}_p^k \\ (j, n) &\longmapsto m_{n \bmod p^k,\ j \bmod p^k}. \end{aligned}$$

On note $g_1, \ldots, g_k$ les fonctions à valeurs dans $\mathbb{Z}_p$ telles que

$$g(j, n) = (g_1(j, n), \ldots, g_k(j, n)).$$

On dit qu'une suite définie par $(a(n))_{n\geq 0} = (a_1(n), \ldots, a_k(n))_{n\geq 0}$ et

$$a(p^k n + j) = a(n) + g(j, n), \quad 0 \leq j \leq p^k - 1, \quad n \geq 0, \quad (j, n) \neq (0, 0)$$

est la *suite de Rudin–Shapiro associée à la matrice* M.

Remarque 3.3.6. On peut fixer arbitrairement la valeur de $a(0)$ et les autres sont définies de manière récursive.

Remarque 3.3.7. Quand la taille de l'alphabet est p, avec p premier, les Définitions 3.3.2 et 3.3.3 coïncident, excepté éventuellement pour les p premières valeurs de la suite.

Remarque 3.3.8. Par définition de g, pour tout entier u et tout entier i avec $0 \leq u < u + i \leq p^k - 1$ l'ensemble $\big\{(g(u + i, n) - g(u, n)) : 0 \leq n \leq p^k - 1\big\}$ est égal à l'ensemble des éléments de $\mathbb{Z}_p^k$.

Nous pouvons maintenant énoncer nos deux résultats qui étendent ceux obtenus par Grant, Shallit, et Stoll.

Théorème 3.3.3. Soit p un nombre premier et $k \geq 1$. Soit M une matrice de différence de $D(p^k, p^k, \mathbb{Z}_p^k)$ et soit $(a(n))_{n\geq 0}$ une suite de Rudin–Shapiro associée à M. De plus, soient r_1 et r_2 tels que $0 \leq r_1 < r_2$. Alors, quand $N \to \infty$, on a

$$\sum_{n<N} \delta(n + r_1, n + r_2) = N\left(1 - \frac{1}{p^k}\right) + O_{p,k}\left((r_2 - r_1)\log\frac{N}{r_2 - r_1} + r_2\right).$$

Exemple 3.3.1. Soit $(\tilde{a}(n))_{n\geq 0}$ la suite obtenue à partir de la suite généralisée de Rudin–Shapiro $(a(n))_{n\geq 0}$ associée à la matrice (3.3) sur $D(4, 4, \mathbb{Z}_2 \times \mathbb{Z}_2)$ en recodant $(0, 0)$ par 0, $(0, 1)$ par 1, $(1, 0)$ par 2 et $(1, 1)$ par 3. Alors, $(\tilde{a}(n))_{n\geq 0}$ est une suite sur l'alphabet $\{0, 1, 2, 3\}$, dont les premiers termes sont les suivants :

$$(\tilde{a}(n))_{n\geq 0} = 0, 0, 0, 0, 0, 0, 1, 2, 3, 0, 2, 3, 1, 0, 3, 1, 2, 0, 0, 0, 0, 0, 1, 0, 3, 2, 2, 0, 1, 3, \ldots$$

De plus, soient r_1 et r_2 tels que $0 \leq r_1 < r_2$. Alors, quand $N \to \infty$, on a

$$\sum_{n<N} \delta(n + r_1, n + r_2) = \frac{3}{4}N + O\left((r_2 - r_1)\log\frac{N}{r_2 - r_1} + r_2\right).$$

Remarque 3.3.9. Il est possible d'utiliser un recodage similaire pour n'importe quel choix de p^k.

On a également le corollaire suivant.

Corollaire 3.3.1. Sous les conditions du Théorème 3.3.3, si $r_2 = o(N)$ alors

$$\sum_{n<N} \delta(n+r_1, n+r_2) \sim N\left(1 - \frac{1}{p^k}\right).$$

Par conséquent, dans l'Exemple 3.3.1, pour $r_2 = o(N)$, nous avons le même résultat que Grant, Shallit, et Stoll pour un alphabet de taille 4,

$$\sum_{n<N} \delta(n+r_1, n+r_2) \sim \frac{3}{4}N.$$

Maintenant, nous présentons le cas général pour n'importe quel alphabet.

Théorème 3.3.4. Soit $d \geq 2$, et soit $p_1, \ldots, p_d$ des nombres premiers deux à deux distincts, et $k_1, \ldots, k_d$ des entiers positifs. On considère l'alphabet $\{0, \ldots, k-1\}$, où $k = p_1^{k_1} \cdots p_d^{k_d}$.
Pour chaque $1 \leq i \leq d$, on considère une matrice de différence M_i de $D(p_i^{k_i}, p_i^{k_i}, \mathbb{Z}_{p_i}^{k_i})$, à laquelle on associe une fonction $g^i(j,n) = (g_1^i(j,n), \ldots, g_{k_i}^i(j,n))$ et une suite $a^i(n) = (a_1^i(n), \ldots, a_{k_i}^i(n))$ définie comme précédemment. On définit la suite $(\hat{a}(n))_{n\geq 0}$ par

$$\hat{a}(n) = (a^1(n) \bmod p_1, \ldots, a^d(n) \bmod p_d).$$

De plus, soient r_1 et r_2 tels que $0 \leq r_1 < r_2$. Alors, quand $N \to \infty$, on a

$$\sum_{n<N} \delta(n+r_1, n+r_2) = N\left(1 - \frac{1}{k}\right) + O_k\left(\left((r_2 - r_1)\log\frac{N^{\frac{1}{d}}}{r_2 - r_1} + r_2\right) N^{\frac{d-1}{d}}\right).$$

Comme précédemment, on obtient aussi le corollaire suivant.

Corollaire 3.3.2. Sous les hypothèse du Théorème 3.3.3, si $r_2 = o(N^{\frac{1}{d}})$ alors

$$\sum_{n<N} \delta(n+r_1, n+r_2) \sim N\left(1 - \frac{1}{k}\right).$$

Remarque 3.3.10. En comparant les termes d'erreur des Théorèmes 3.3.2 et 3.3.4 quand la taille de l'alphabet est sans facteur carré, on constate que quand $r_2 - r_1 = O(1)$, le choix optimal de γ dans le Théorème 3.3.2 est tel que $1 - \frac{\gamma}{d} = \gamma$, i.e., $\gamma = \frac{d}{d+1}$. Cela nous donne un terme d'erreur borné par $N^{\frac{d}{d+1}}$. Dans le Théorème 3.3.4, le terme d'erreur correspondant est borné par $r_2 N^{\frac{d-1}{d}}$, de plus, pour obtenir une amélioration on doit avoir $r_2 N^{\frac{d-1}{d}} \ll N^{\frac{d}{d+1}}$, i.e., $r_2 = o(N^{\frac{1}{d(d+1)}})$. Par conséquent, si $r_2 - r_1 = O(1)$ et $r_2 = o(N^{\frac{1}{d(d+1)}})$, notre résultat est une amélioration pour les alphabets dont la taille est sans facteur carré et avec au moins deux nombres premiers dans la décomposition.

3.3.3 Preuves des théorèmes

3.3.3.1 Preuve du Théorème 3.3.3

Pour la preuve du Théorème 3.3.3, nous avons besoin du lemme suivant.

Lemme 3.3.1. Soit G une matrice de différence de $D(p^k, p^k, \mathbb{Z}_p^k)$. On note $G_1, \ldots, G_k$ les matrices obtenues à partir de G en prenant respectivement les premières,..., les k-ème coordonnées. Soit $0 \leq h_1, \ldots, h_k < p$ avec $(h_1, \ldots, h_k) \neq (0, \ldots, 0)$. Alors la matrice $H = h_1 G_1 + \cdots + h_k G_k$ est une matrice de différence de $D(p^k, p^k, \mathbb{Z}_p)$.

Démonstration. Notons $(g_1(j,n),\dots,g_k(j,n))$ les coefficients de G de la j-ème colonne et de la n-ème ligne. La différence entre deux colonnes distinctes i et j de H s'écrit de la manière suivante :

$$C_{i,j}=\begin{pmatrix} h_1(g_1(j,0)-g_1(i,0))+\cdots+h_k(g_k(j,0)-g_k(i,0)) \\ \vdots \\ h_1(g_1(j,p^k-1)-g_1(i,p^k-1))+\cdots+h_k(g_k(j,p^k-1)-g_k(i,p^k-1)) \end{pmatrix}.$$

Comme G est une matrice de différence, on a

$$\left\{(g_1(j,n)-g_1(i,n),\dots,g_k(j,n)-g_k(i,n)),\ 0\le n<p^k\right\}=\mathbb{Z}_p^k.$$

Par conséquent, les éléments qui apparaissent dans $C_{i,j}$ sont tous les éléments de la forme $h_1c_1+\cdots+h_kc_k$, pour $(c_1,\dots,c_k)\in\mathbb{Z}_p^k$. Ainsi, dans $C_{i,j}$, pour tout $d\in\mathbb{Z}_p$, chaque élément apparaît $\#\left\{(c_1,\dots,c_k)\in\mathbb{Z}_p^k : h_1c_1+\cdots+h_kc_k=d\right\}=p^{k-1}$ fois. Il s'en suit que H est une matrice de différence de $D(p^k,p^k,\mathbb{Z}_p)$. □

Désormais, nous avons tous les outils pour la preuve du Théorème 3.3.3.

Démonstration. Soient r_1 et r_2 tels que $0\le r_1<r_2$. On a

$$\begin{aligned}
&\sum_{n<N}\delta(n+r_1,n+r_2)\\
&=N-\sum_{n<N}\frac{1}{p^k}\prod_{i=1}^{k}\sum_{0\le h_i<p}\mathrm{e}\left(\frac{h_i}{p}(a_i(n+r_2)-a_i(n+r_1))\right)\\
&=N-\sum_{n<N}\frac{1}{p^k}\sum_{0\le h_1,\dots,h_k<p}\mathrm{e}\left(\frac{1}{p}\sum_{i=1}^{k}h_i(a_i(n+r_2)-a_i(n+r_1))\right)\\
&=N\left(1-\frac{1}{p^k}\right)-\frac{1}{p^k}\sum_{\substack{0\le h_1,\dots,h_k<p\\(h_1,\dots,h_k)\neq(0,\dots,0)}}S_N(h_1,\dots,h_k),
\end{aligned}$$

avec

$$S_N(h_1,\dots,h_k)=\sum_{n<N}\mathrm{e}\left(\frac{1}{p}\sum_{i=1}^{k}h_i(a_i(n+r_2)-a_i(n+r_1))\right).$$

Posons $r=r_2-r_1$.
Il suffit alors de montrer que pour tous $h_1,\dots,h_k$ tels que $0\le h_1,\dots,h_k<p$ avec $(h_1,\dots,h_k)\neq(0,\dots,0)$ on a

$$S_N(h_1,\dots,h_k)=O_{p,k}\left(r\log\frac{N}{r}+r\right).$$

Soit $b(n)=h_1a_1(n)+\cdots+h_ka_k(n)$ et $g^*(j,n)=h_1g_1(j,n)+\cdots+h_kg_k(j,n)$ de sorte que $b(p^kn+j)=b(n)+g^*(j,n)$. Par le Lemme 3.3.1, pour tous entiers u et i tels que $0\le u<u+i\le p^k-1$, l'ensemble $\left\{(g^*(u+i,n)-g^*(u,n))\ : 0\le n\le p^k-1\right\}$ contient p^{k-1} fois chaque élément de $\mathbb{Z}_p$.
On définit

$$\gamma_N(r,f)=\sum_{n<N}\mathrm{e}\left(\frac{b(n+r)-b(n)}{p}\right)\mathrm{e}\left(\frac{f(n)}{p}\right),$$

où $f:\mathbb{N}\to\mathbb{Z}$ est une fonction quelconque p^k-périodique.
Commençons par montrer que $\gamma_N(1,f)=O(\log N)$ pour $N>p^k$. Pour cela nous allons décomposer n

modulo p^k. Nous remplaçons également N par p^kN+j, avec $0 \le j \le p^k-1$. Alors, on a

$$\begin{aligned}
\gamma_{p^kN+j}(1,f) &= \sum_{n<p^kN+j} \mathrm{e}\left(\frac{1}{p}(b(n+1)-b(n))\right)\mathrm{e}\left(\frac{f(n)}{p}\right)\\
&= \sum_{u=0}^{p^k-1} \sum_{p^kn+u<p^kN+j} \mathrm{e}\left(\frac{1}{p}(b(p^kn+u+1)-b(p^kn+u))\right)\mathrm{e}\left(\frac{f(u)}{p}\right)\\
&= \sum_{u=0}^{j-1} \mathrm{e}\left(\frac{1}{p}(b(p^kN+u+1)-b(p^kN+u))\right)\mathrm{e}\left(\frac{f(u)}{p}\right) \qquad (3.6)\\
&+ \sum_{u=0}^{p^k-2} \mathrm{e}\left(\frac{f(u)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^kn+u+1)-b(p^kn+u))\right) \qquad (3.7)\\
&+ \mathrm{e}\left(\frac{f(p^k-1)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^kn+p^k)-b(p^kn+p^k-1)\right). \qquad (3.8)
\end{aligned}$$

Le terme (3.6) est majoré trivialement par $j \le p^k-1$.
Pour (3.7) on a pour $0 \le u \le p^k-2$,

$$\begin{aligned}
&\sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^kn+u+1)-b(p^kn+u))\right)\\
&\qquad = \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n)+g^*(u+1,n)-b(n)-g^*(u,n))\right)\\
&\qquad = \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(g^*(u+1,n)-g^*(u,n))\right).
\end{aligned}$$

Pour $0 \le n \le p^k-1$ et à u fixé, les différences $g^*(u+1,n)-g^*(u,n)$ contiennent p^{k-1} fois chaque élément de $\mathbb{Z}_p$. Par conséquent, cette somme est majorée par $\dfrac{p^k}{2}$. Ainsi, la somme (3.7) est majorée par $\dfrac{(p^k-1)p^k}{2}$.
Enfin, pour (3.8) on a

$$\begin{aligned}
&\sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^kn+p^k)-b(p^kn+p^k-1)\right)\\
&\qquad = \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n+1)+g^*(0,n+1)-b(n)-g^*(p^k-1,n)\right)\\
&\qquad = \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n+1)-b(n))\right)\mathrm{e}\left(\frac{\tilde{f}(n)}{p}\right),
\end{aligned}$$

où $\tilde{f}(n) = g^*(0,n+1)-g^*(p^k-1,n)$ est p^k-périodique.
Nous en déduisons que $|\gamma_{p^kN+j}(1,f)| \le |\gamma_N(1,\tilde{f})| + \dfrac{(p^k-1)(p^k+2)}{2}$.
De plus, étant donné que $|\gamma_n(1,f)| \le p^k-1$ pour $1 \le n \le p^k-1$ et toute fonction f p^k-périodique, il s'en suit par récurrence que pour toute fonction f, p^k-périodique, et pour tout $N > p^k$,

$$|\gamma_N(1,f)| \le \frac{(p^k-1)(p^k+2)}{2k\log p}\log N + p^k - 1. \qquad (3.9)$$

En effet, supposons que pour tout $N > p^k$ on ait (3.9) pour toute fonction f p^k-périodique. Alors, soit f une fonction p^k-périodique et $0 \le j \le p^k - 1$. On a

$$\begin{aligned}
|\gamma_{p^kN+j}(1,f)| &\le |\gamma_N(1,\tilde{f})| + \frac{(p^k-1)(p^k+2)}{2} \\
&\le \frac{(p^k-1)(p^k+2)}{2k\log p}\log N + p^k - 1 + \frac{(p^k-1)(p^k+2)}{2} \\
&\le \frac{(p^k-1)(p^k+2)}{2k\log p}(\log N + k\log p) + p^k - 1 \\
&\le \frac{(p^k-1)(p^k+2)}{2k\log p}\log(p^kN+j) + p^k - 1.
\end{aligned}$$

Remarquons que la somme $\gamma_N(0,f) = \sum_{n<N} \mathrm{e}\left(\frac{f(n)}{p}\right)$ satisfait

$$|\gamma_N(0,f)| \le \frac{p^k}{2} \text{ if } f(\{0,\dots,p^k-1\}) \text{ contains } p^{k-1} \text{ times each element of } \mathbb{Z}_p. \tag{3.10}$$

Maintenant, considérons le cas général avec $r = p^kM + i > 0$ où $M \ge 0$ et $0 \le i \le p^k - 1$ mais $(M,i) \ne (0,0)$. On a

$$\begin{aligned}
&\gamma_{p^kN+j}(p^kM+i,f) \\
&\quad= \sum_{n<p^kN+j} \mathrm{e}\left(\frac{1}{p}(b(n+p^kM+i)-b(n))\right)\mathrm{e}\left(\frac{f(n)}{p}\right) \\
&\quad= \sum_{n<p^kN} \mathrm{e}\left(\frac{1}{p}(b(n+p^kM+i)-b(n))\right)\mathrm{e}\left(\frac{f(n)}{p}\right) + O_{p,k}(1) \\
&\quad= \sum_{u=0}^{p^k-1}\sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^kn+u+p^kM+i)-b(p^kn+u))\right)\mathrm{e}\left(\frac{f(u)}{p}\right) \\
&\qquad + O_{p,k}(1) \\
&\quad= \sum_{u=0}^{p^k-1} \mathrm{e}\left(\frac{f(u)}{p}\right)\sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^kn+u+p^kM+i)-b(p^kn+u))\right) \\
&\qquad + O_{p,k}(1),
\end{aligned} \tag{3.11}$$

où la constante implicite provient du terme $n = N$ et est majorée par $p^k - 1$. La dernière partie consiste à établir une estimation de la somme (3.11). Dans un premier temps, nous supposons que $i \ne 0$. Alors

$$\sum_{u=0}^{p^k-1} \mathrm{e}\left(\frac{f(u)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^k n+u+p^k M+i)-b(p^k n+u))\right)$$

$$= \sum_{u=0}^{p^k-1-i} \mathrm{e}\left(\frac{f(u)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n+M)+g^*(u+i,n+M)-b(n)-g^*(u,n))\right)$$
$$+ \sum_{u=p^k-i}^{p^k-1} \mathrm{e}\left(\frac{f(u)}{p}\right)$$
$$\times \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n+M+1)+g^*(u+i-p^k,n+M+1)-b(n)-g^*(u,n))\right)$$
$$= \sum_{u=0}^{p^k-1-i} \mathrm{e}\left(\frac{f(u)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n+M)-b(n))\right) \mathrm{e}\left(\frac{f_1(n)}{p}\right)$$
$$+ \sum_{u=p^k-i}^{p^k-1} \mathrm{e}\left(\frac{f(u)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(n+M+1)-b(n))\right) \mathrm{e}\left(\frac{f_2(n)}{p}\right),$$

avec $f_1(n)=g^*(u+i,n+M)-g^*(u,n)$ pour $0\le u\le p^k-1-i$,
et $f_2(n)=g^*(u+i-p^k,n+M+1)-g^*(u,n)$ pour $p^k-i\le u\le p^k-1$.

Pour plus de clarté, ici et dans la suite, nous n'écrirons pas la dépendance en u de ces fonctions. Ainsi

$$\left|\sum_{u=0}^{p^k-1} \mathrm{e}\left(\frac{f(u)}{p}\right) \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{p}(b(p^k n+u+p^k M+i)-b(p^k n+u))\right)\right|$$
$$\le \left|\sum_{u=0}^{p^k-1-i} \mathrm{e}\left(\frac{f(u)}{p}\right)\gamma_N(M,f_1)\right| + \left|\sum_{u=p^k-i}^{p^k-1} \mathrm{e}\left(\frac{f(u)}{p}\right)\gamma_N(M+1,f_2)\right|.$$

Soit $\tilde{f}_1$ et $\tilde{f}_2$ deux fonctions telles que

$$|\gamma_N(M,\tilde{f}_1)| = \max_{0\le u\le p^k-1-i} |\gamma_N(M,f_1)| \text{ et } |\gamma_N(M,\tilde{f}_2)| = \max_{p^k-i\le u\le p^k-1} |\gamma_N(M,f_2)|.$$

Nous en déduisons l'estimation suivante :

$$|\gamma_{p^k N+j}(p^k M+i,f)| \le (p^k-i)|\gamma_N(M,\tilde{f}_1)| + i|\gamma_N(M+1,\tilde{f}_2)| + p^k - 1. \tag{3.12}$$

Remplaçons par $M=0$ dans (3.12). Comme $i\neq 0$, l'image de l'ensemble $\{0,\dots,p^{k-1}\}$ par la fonction $f_1(n)=g^*(u+i,n)-g^*(u,n)$ est le multi-ensemble $\{\underbrace{0,\dots,0}_{p^{k-1}},\dots,\underbrace{p-1,\dots,p-1}_{p^{k-1}}\}$.

En utilisant (3.9) et (3.10) on a

$$(p^k-i)|\gamma_N(0,\tilde{f}_1)| \le (p^k-i)\times\frac{p^k}{2}.$$

et

$$i|\gamma_N(1,\tilde{f}_2)| \le i\left(\frac{(p^k-1)(p^k+2)}{2k\log p}\log N + p^k - 1\right).$$

Par conséquent,

$$\begin{aligned}|\gamma_{p^kN+j}(i,f)| &\le (p^k-i)\frac{p^k}{2}+i\left(\frac{(p^k-1)(p^k+2)}{2k\log p}\log N+p^k-1\right)+p^k-1\\ &\le i\left(\frac{(p^k-1)(p^k+2)}{2k\log p}\log N\right)+(p^k-i)\frac{p^k}{2}+i(p^k-1)+p^k-1\\ &\le \frac{(p^k-1)^2(p^k+2)}{2k\log p}\log N+\frac{p^k}{2}(p^k-i+2i+2)-i-1\\ &\le \frac{(p^k-1)^2(p^k+2)}{2k\log p}\log N+\frac{p^k}{2}(2p^k+1)-p^k.\end{aligned}$$

Ainsi, pour tout $i\in[\![1,p^k-1]\!]$ et toute fonction f p^k-périodique, on a, pour $N>p^k$,

$$|\gamma_N(i,f)|\le\frac{(p^k-1)^2(p^k+2)}{2k\log p}\log\frac{N}{p^k}+\frac{p^k}{2}(2p^k+1)-p^k. \tag{3.13}$$

Il reste à établir une majoration pour $i=0$. Pour $0\le u\le p^k-1$ on a

$$b(p^kn+u+p^kM)-b(p^kn+u)=b(n+M)-b(n)+g^*(u,n+M)-g^*(u,n)$$

et donc, pour $M\neq 0$, par (3.11)

$$|\gamma_{p^kN+j}(p^kM,f)|\le\sum_{u=0}^{p^k-1}|\gamma_N(M,f_3)|+p^k-1 \tag{3.14}$$

avec $f_3(n)=g^*(u,n+M)-g^*(u,n)$. En utilisant (3.9) et en remplaçant $M=1$ dans (3.14), on en déduit, pour $N>p^k$,

$$|\gamma_N(p^k,f)|\le p^k\left(\frac{(p^k-1)(p^k+2)}{2k\log p}\log\frac{N}{p^k}+p^k\right).$$

D'où, en utilisant (3.13), pour tout $N>p^k$ et tout $1\le i\le p^k$,

$$|\gamma_N(i,f)|\le p^k\left(\frac{(p^k-1)(p^k+2)}{2k\log p}\log\frac{N}{p^k}+p^k\right). \tag{3.15}$$

En se servant de (3.12), on a pour $1\le i\le p^k-1$, $0\le m\le p^{k(s-1)}(p^k-1)-1$, $M=p^{k(s-1)}+m$ avec $s\ge 1$, et pour tout $N>p^{k(s+1)}$,

$$\begin{aligned}&|\gamma_{p^kN+j}(p^k(p^{k(s-1)}+m)+i,f)|\\ &\quad\le(p^k-i)|\gamma_N(p^{k(s-1)}+m,\tilde f_1)|+i|\gamma_N(p^{k(s-1)}+m+1,\tilde f_2)|+p^k-1\\ &\quad\le p^k\max(|\gamma_N(p^{k(s-1)}+m,\tilde f_1)|,|\gamma_N(p^{k(s-1)}+m+1,\tilde f_2)|)+p^k-1.\end{aligned}$$

Soit $N=p^kN_1+j_1$. Selon que p^k soit un facteur ou non de $p^{k(s-1)}+m$ (resp. $p^{k(s-1)}+m+1$), on peut utiliser (3.12) ou (3.14) pour majorer $|\gamma_{p^kN_1+j_1}(p^{k(s-1)}+m,\tilde f_1)|$ (resp. $|\gamma_{p^kN_1+j_1}(p^{k(s-1)}+m+1,\tilde f_2)|$). En itérant s fois, et en utilisant (3.15) pour la dernière majoration, on obtient pour $r=p^{ks}+1,\dots,p^{ks}+p^k-1,p^{ks}+p^k+1,\dots,p^{k(s+1)}-p^k-1,p^{k(s+1)}-p^k+1,\dots,p^{k(s+1)}-1$ avec $s\ge1$, et pour tout $N>p^{k(s+1)}$,

$$|\gamma_N(r,f)|\le p^{ks}\left(p^k\frac{(p^k-1)(p^k+2)}{2k\log p}\log\frac{N}{p^{k(s+1)}}+p^k+1\right)+\sum_{j=0}^{s-1}(p^k-1)p^{kj}. \tag{3.16}$$

Pour $r = p^{ks} + p^k, p^{ks} + 2p^k, \ldots, p^{k(s+1)}$ on utilise (3.14). Soit $\tilde{f_3}$ une fonction telle que $|\gamma_N(M, \tilde{f_3})| = \max_{0 \leq u \leq p^k - 1} |\gamma_N(M, f_3)|$. Alors, on a pour tout $N > p^{k(s+1)}$.

$$\begin{aligned} |\gamma_{p^k N + j}(r, f)| &\leq \sum_{u=0}^{p^k - 1} |\gamma_N(\frac{r}{p^k}, f_3)| + p^k - 1 \\ &\leq p^k |\gamma_N(\frac{r}{p^k}, \tilde{f_3})| + p^k - 1. \end{aligned}$$

On peut alors à nouveau itérer (3.12) ou (3.14), et (3.15) pour la dernière majoration. Avec (3.15) et (3.16), on en déduit pour $r = p^{ks} + 1, \ldots, p^{k(s+1)}$ avec $s \geq 0$ et pour tout $N > p^{k(s+1)}$,

$$\begin{aligned} |\gamma_N(r, f)| &\leq p^{ks} \left(p^k \frac{(p^k - 1)(p^k + 2)}{2k \log p} \log \frac{N}{p^{k(s+1)}} + p^k + 1 \right) + \sum_{j=0}^{s-1} (p^k - 1) p^{kj} \\ &\leq p^{ks} \left(p^k \frac{(p^k - 1)(p^k + 2)}{2k \log p} \right) \log \frac{N}{p^{k(s+1)}} + p^{ks}(p^k + 2) - 1. \end{aligned}$$

Finalement, pour tout $N > rp^k$, on a

$$|\gamma_N(r, f)| \leq r \left(p^k \frac{(p^k - 1)(p^k + 2)}{2k \log p} \right) \log \frac{N}{r} + r(p^k + 2).$$

Ceci achève la preuve du Théorème 3.3.3. □

3.3.3.2 Preuve du Théorème 3.3.4

Soit $n \in \mathbb{N}$. On note $[\alpha_s, \alpha_{s-1}, \ldots, \alpha_1, \alpha_0]_k$ la décomposition de n en base k, où $\alpha_s \neq 0$ est le poids fort, de sorte que $n = \alpha_s k^s + \alpha_{s-1} k^{s-1} + \cdots + \alpha_1 k + \alpha_0$. Par convention on pose $\alpha_{s+1} = 0$. Pour la preuve du Théorème 3.3.4 nous aurons besoin du lemme élémentaire suivant :

Lemme 3.3.2. Soit $k \geq 2$ et soit $(a(n))_{n \geq 0}$ une suite associée à une suite généralisée de Rudin–Shapiro, au sens de la Définition 3.3.2, qui satisfait la relation

$$a(nk + j) = a(n) + g(j, n), \quad 0 \leq j \leq k - 1, \quad n \geq 0, \quad (j, n) \neq (0, 0).$$

Alors, pour $n = [\alpha_s, \alpha_{s-1}, \ldots, \alpha_1, \alpha_0]_k$ on a

$$a(n) = a(\alpha_s) + \sum_{i=0}^{s-1} g(\alpha_i, \alpha_{i+1}) = a(0) + \sum_{i=0}^{s} g(\alpha_i, \alpha_{i+1}).$$

Démonstration. Par définition, la fonction g est k-périodique en la seconde variable. Par récurrence sur s, on a

$$\begin{aligned} a(n) &= a(\alpha_s k^s + \alpha_{s-1} k^{s-1} + \cdots + \alpha_1 k + \alpha_0) \\ &= a(\alpha_s k^{s-1} + \alpha_{s-1} k^{s-2} + \cdots + \alpha_2 k + \alpha_1) + g(\alpha_0, \alpha_1) \\ &= \cdots = a(\alpha_s) + \sum_{i=0}^{s-1} g(\alpha_i, \alpha_{i+1}). \end{aligned}$$

□

Maintenant, étant donné que $a(\alpha_s) = a(0) + g(\alpha_s, 0) = a(0) + g(\alpha_s, \alpha_{s+1})$, on en déduit

$$a(n) = a(0) + \sum_{i=0}^{s} g(\alpha_i, \alpha_{i+1}).$$

Nous terminons cette partie par la preuve du Théorème 3.3.4.

Démonstration. Commençons par introduire quelques notations.
On pose $r = r_2 - r_1$. Soit N un entier et soit $\mathbf{b} = (b_1, \dots, b_d)$, définissons

$$P_{\mathbf{b}} = \{n \in \mathbb{N} : \forall i \in \{1, \dots, d\}, n \equiv b_i \pmod{{p_i}^{s_i}}\},$$

où s_i est l'unique entier avec ${p_i}^{s_i} \leq N^{\frac{1}{d}} < {p_i}^{s_i+1}$. Comme première estimation , on a

$$\#\{n \in \mathbb{N} : n \in P_{\mathbf{b}},\ n < N\} = \frac{N}{\prod_{i=1}^{d} {p_i}^{s_i}} + O(1).$$

On considère les ensembles

$$\mathcal{B} = \{(b_1, \dots, b_d) : 0 \leq b_i < {p_i}^{s_i}\},$$
$$\mathcal{B}_0 = \{(b_1, \dots, b_d) : 0 \leq b_i < {p_i}^{s_i} - r\}.$$

Fixons $1 \leq i \leq d$ et $1 \leq j \leq k_i$. Maintenant, considérons n tel que $n = n_i {p_i}^{s_i} + b_i$ où $(b_1, \dots, b_d) \in \mathcal{B}_0$. On écrit

$$b_i + r = \beta'_{s_i-1,i} {p_i}^{s_i-1} + \beta'_{s_i-2,i} {p_i}^{s_i-2} + \cdots + \beta'_{0,i},$$
$$b_i = \beta_{s_i-1,i} {p_i}^{s_i-1} + \beta_{s_i-2,i} {p_i}^{s_i-2} + \cdots + \beta_{0,i},$$

où $\beta_{\nu,i}, \beta'_{\nu,i} \in \{0, 1, \dots, p_i - 1\}$ pour $0 \leq \nu < s_i$. De plus, considérons

$$v_i = \max(\kappa : \beta'_{\kappa,i} \neq 0,\ 0 \leq \kappa \leq s_i - 1),$$

$$w_i = \max(\kappa : \beta_{\kappa,i} \neq 0,\ 0 \leq \kappa \leq s_i - 1),$$

qui correspondent aux coefficient non nuls les plus élevés dans les décompositions en base p_i. En utilisant la relation de récursivité de la suite $(a_j^i(n))_{n \geq 0}$, et d'après le Lemme 3.3.2 on a d'une part

$$a_j^i(n + r) = a_j^i(n_i) + g_j^i(\beta'_{s_i-1,i}, n_i) + \sum_{\nu=0}^{s_i-2} g_j^i(\beta'_{\nu,i}, \beta'_{\nu+1,i}),$$

et d'autre part

$$a_j^i(n) = a_j^i(n_i) + g_j^i(\beta_{s_i-1,i}, n_i) + \sum_{\nu=0}^{s_i-2} g_j^i(\beta_{\nu,i}, \beta_{\nu+1,i}).$$

Ceci implique que

$$\begin{aligned} &a_j^i(n + r) - a_j^i(n) \\ &= g_j^i(\beta'_{s_i-1,i}, n_i) + \sum_{\nu=0}^{s_i-2} g_j^i(\beta'_{\nu,i}, \beta'_{\nu+1,i}) - g_j^i(\beta_{s_i-1,i}, n_i) - \sum_{\nu=0}^{s_i-2} g_j^i(\beta_{\nu,i}, \beta_{\nu+1,i}). \end{aligned}$$

De manière similaire, comme $b_i + r = [\beta'_{v_i,i}, \dots, \beta'_{1,i}, \beta'_{0,i}]_p$ et $b_i = [\beta_{w_i,i}, \dots, \beta_{1,i}, \beta_{0,i}]_p$, et $\beta'_{v_i+1,i} = 0$ et $\beta_{w_i+1,i} = 0$, par définition de v_i et w_i, on obtient

$$a_j^i(b_i + r) = a_j^i(0) + \sum_{\nu=0}^{v_i} g_j^i(\beta'_{\nu,i}, \beta'_{\nu+1,i})$$

et

$$a_j^i(b_i) = a_j^i(0) + \sum_{\nu=0}^{w_i} g_j^i(\beta_{\nu,i}, \beta_{\nu+1,i}).$$

Ainsi, on a

$$a_j^i(n+r) - a_j^i(n) = a_j^i(b_i+r) - a_j^i(b_i) + \mu_{i,j}(b_i, r, n_i) \tag{3.17}$$

où

$$\begin{aligned}&\mu_{i,j}(b_i, r, n_i)\\ &= g_j^i(\beta'_{s_i-1,i}, n_i) - g_j^i(\beta_{s_i-1,i}, n_i) + \sum_{\nu=v_i+1}^{s_i-2} g_j^i(\beta'_{\nu,i}, \beta'_{\nu+1,i}) - \sum_{\nu=w_i+1}^{s_i-2} g_j^i(\beta_{\nu,i}, \beta_{\nu+1,i}).\end{aligned}$$

De plus, on a $a(n+r) = a(n)$ si et seulement si $a_j^i(n+r) = a_j^i(n)$ pour tout $i \in [\![1, d]\!]$ et $j \in [\![1, k_i]\!]$. Dans la suite, nous utiliserons la notation

$$\mathbf{a} = \mathbf{a}(n) = \begin{pmatrix} a_1^1(n+r) - a_1^1(n) \\ \vdots \\ a_{k_1}^1(n+r) - a_{k_1}^1(n) \\ \vdots \\ \vdots \\ a_1^d(n+r) - a_1^d(n) \\ \vdots \\ a_{k_d}^d(n+r) - a_{k_d}^d(n) \end{pmatrix}$$

pour le vecteur $a(n+r) - a(n)$. On introduit également la notation

$$\mathbf{h} = \left(\frac{h_1^1}{p_1}, \ldots, \frac{h_{k_1}^1}{p_1}, \ldots\ldots, \frac{h_1^d}{p_d}, \ldots, \frac{h_{k_d}^d}{p_d} \right).$$

Ainsi,

$$\sum_{n<N} \delta(n+r_1, n+r_2) = N\left(1 - \frac{1}{k}\right) - \frac{1}{k} \sum_{n<N} \sum_{\mathbf{h}\neq\mathbf{0}} \mathrm{e}(\mathbf{h}\cdot\mathbf{a}).$$

Fixons un vecteur $\mathbf{h} \neq \mathbf{0}$ tel que pour tout i tel que $1 \leq i \leq d$ et tout j tel que $1 \leq j \leq k_i$ on ait $0 \leq h_j^i < p_i$.
Il suffit d'estimer $\displaystyle\sum_{n<N} \mathrm{e}(\mathbf{h}\cdot\mathbf{a})$. On définit

$$\mathbf{a'} = \begin{pmatrix} a_1^1(n_1 {p_1}^{s_1} + b_1 + r) - a_1^1(n_1 {p_1}^{s_1} + b_1) \\ \vdots \\ a_{k_1}^1(n_1 {p_1}^{s_1} + b_1 + r) - a_{k_1}^1(n_1 {p_1}^{s_1} + b_1) \\ \vdots \\ \vdots \\ a_1^d(n_d {p_d}^{s_d} + b_d + r) - a_1^d(n_d {p_d}^{s_d} + b_d) \\ \vdots \\ a_{k_d}^d(n_d {p_d}^{s_d} + b_d + r) - a_{k_d}^d(n_d {p_d}^{s_d} + b_d) \end{pmatrix},$$

$$\mathbf{a''} = \begin{pmatrix} a_1^1(b_1+r) - a_1^1(b_1) \\ \vdots \\ a_{k_1}^1(b_1+r) - a_{k_1}^1(b_1) \\ \vdots \\ \vdots \\ a_1^d(b_d+r) - a_1^d(b_d) \\ \vdots \\ a_{k_d}^d(b_d+r) - a_{k_d}^d(b_d) \end{pmatrix} \quad \text{et} \quad \boldsymbol{\mu} = \begin{pmatrix} \mu_{1,1}(b_1, r, n_1) \\ \vdots \\ \mu_{1,k_1}(b_1, r, n_1) \\ \vdots \\ \vdots \\ \mu_{d,1}(b_d, r, n_d) \\ \vdots \\ \mu_{d,k_d}(b_d, r, n_d) \end{pmatrix}$$

En utilisant (3.17) on a

$$\begin{aligned} \sum_{n<N} \mathrm{e}(\mathbf{h}\cdot\mathbf{a}) &= \sum_{\mathbf{b}\in\mathcal{B}_0} \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} \mathrm{e}(\mathbf{h}\cdot\mathbf{a'}) + \sum_{\mathbf{b}\in\mathcal{B}\setminus\mathcal{B}_0} \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} \mathrm{e}(\mathbf{h}\cdot\mathbf{a'}) \\ &= \sum_{\mathbf{b}\in\mathcal{B}_0} \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} \mathrm{e}(\mathbf{h}\cdot(\mathbf{a''}+\boldsymbol{\mu})) + \sum_{\mathbf{b}\in\mathcal{B}\setminus\mathcal{B}_0} \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} \mathrm{e}(\mathbf{h}\cdot\mathbf{a'}) \\ &= \sum_{\mathbf{b}\in\mathcal{B}} \mathrm{e}(\mathbf{h}\cdot\mathbf{a''}) \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} \mathrm{e}(\mathbf{h}\cdot\boldsymbol{\mu}) \qquad (3.18) \\ &\quad + \sum_{\mathbf{b}\in\mathcal{B}\setminus\mathcal{B}_0} \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} (\mathrm{e}(\mathbf{h}\cdot\mathbf{a'}) - \mathrm{e}(\mathbf{h}\cdot(\mathbf{a''}+\boldsymbol{\mu}))). \qquad (3.19) \end{aligned}$$

Notons que $\mathcal{B}\setminus\mathcal{B}_0 = \{(b_1,\dots,b_d) : 0 \le b_i < {p_i}^{s_i},\ \exists j \in \{1,\dots,d\},\ b_j \ge {p_j}^{s_j} - r\}$.
De sorte que, $|\,\mathcal{B}\setminus\mathcal{B}_0\,| \ll \sum_{i=1}^{d} \frac{r}{{p_i}^{s_i}} \prod_{j=1}^{d} p_j^{s_j}$.
Par conséquent, la somme (3.19) est trivialement majorée par

$$\begin{aligned} 2\,|\,\mathcal{B}\setminus\mathcal{B}_0\,|\,\#\{n<N : n\in P_{\mathbf{b}}\} &\ll_k \left(\sum_{i=1}^{d} \frac{r}{{p_i}^{s_i}} \prod_{j=1}^{d} p_j^{s_j}\right)\left(\frac{N}{\prod_{i=1}^{d} {p_i}^{s_i}} + O(1)\right) \\ &\ll_k \ rN^{1-\frac{1}{d}}. \end{aligned}$$

Nous avons déjà un premier terme d'erreur de l'estimation finale. Maintenant, pour terminer la preuve, nous avons besoin d'estimer (3.18). Soit

$$\mathcal{B}^r = \left\{\mathbf{b}\in\mathcal{B} : v_i = w_i \text{ and } \beta_{v_i,i} = \beta'_{w_i,i},\ \text{for all } 1\le i\le d\right\}.$$

Pour chaque $\mathbf{b}\in\mathcal{B}^r$ on a $\mu_{i,j}(b_i,r,n_i) = 0$, pour tout $n<N, n\in P_{\mathbf{b}}$. En utilisant un argument similaire où $\mathcal{B}^r$ joue le rôle de $\mathcal{B}_0$, on peut majorer la somme (3.18) par

$$\ll \sum_{\mathbf{b}\in\mathcal{B}} \mathrm{e}(\mathbf{h}\cdot\mathbf{a''}) \sum_{\substack{n<N \\ n\in P_{\mathbf{b}}}} 1 + 2\,|\,\mathcal{B}\setminus\mathcal{B}^r\,| \left(\frac{N}{\prod_{i=1}^{d} {p_i}^{s_i}} + O(1)\right).$$

La dernière partie, consiste à établir une borne pour $|\,\mathcal{B}\setminus\mathcal{B}^r\,|$. Considérons t_i tel que ${p_i}^{t_i} \le r < {p_i}^{t_i+1}$. Nous allons compter le nombre de b_i satisfaisant $0\le b_i < {p_i}^{s_i}$ et pour lesquels nous avons une propagation de retenue depuis le chiffre $\beta_{v_i,i}$ de b_i lorsqu'on ajoute r. Pour cela, une condition nécessaire est

$$\beta_{t_i+1,i} = \beta_{t_i+2,i} = \cdots = \beta_{s_i-2,i} = p_i - 1.$$

Alors, $| \mathcal{B} \setminus \mathcal{B}^r | \leq \sum_{i=1}^{d} {p_i}^{t_i+1} + (s_i - 2 - t_i){p_i}^{t_i+2}$.

En utilisant le fait que $s_i \leq \frac{\log N^{\frac{1}{d}}}{\log p_i}$, et $-t_i - 1 < -\frac{\log r}{\log p_i}$, on en déduit

$$| \mathcal{B} \setminus \mathcal{B}^r | \leq \sum_{i=1}^{d} \left(r p_i + r {p_i}^2 \left(\frac{\log(N^{\frac{1}{d}})}{\log p_i} - \frac{\log r}{\log p_i} \right) \right) \ll_k r \sum_{i=1}^{d} \log N^{\frac{1}{d}}.$$

Pour tout i tel que $1 \leq i \leq d$ et tout j tel que $1 \leq j \leq k_i$, on définit $\mathbf{h}^i = \left(\frac{h_1^i}{p_i}, \ldots, \frac{h_{k_i}^i}{p_i} \right)$ et $\mathbf{a}^i = (a_1^i(b_i + r) - a_1^i(b_i), \ldots, a_{k_i}^i(b_i + r) - a_{k_i}^i(b_i))$.

En ajoutant tous les termes, on a

$$\begin{aligned} \sum_{n<N} \mathrm{e}(\mathbf{h} \cdot \mathbf{a}) &= \sum_{\mathbf{b} \in \mathcal{B}} \mathrm{e}(\mathbf{h} \cdot \mathbf{a"}) \sum_{\substack{n<N \\ n \in P_{\mathbf{b}}}} 1 + O_k \left(r N^{1-\frac{1}{d}} + r \sum_{i=1}^{d} \log N^{\frac{1}{d}} \right) \\ &= \left(\prod_{i=1}^{d} \sum_{b_i=0}^{{p_i}^{s_i}-1} \mathrm{e}(\mathbf{h}^i \cdot \mathbf{a}^i) \right) \left(\frac{N}{\prod_{i=1}^{d} {p_i}^{s_i}} + O(1) \right) + O_k \left(r N^{1-\frac{1}{d}} \right). \end{aligned}$$

Par hypothèse, $\mathbf{h} \neq \mathbf{0}$, donc il existe $1 \leq l \leq d$ tel que $\mathbf{h}^l \neq \mathbf{0}$. En reprenant les notations de la preuve du Théorème 3.3.3 on a

$$\sum_{n<N^{1/d}} \mathrm{e}(\mathbf{h}^l \cdot \mathbf{a}^l) = S_{N^{1/d}}(h_1^l, \ldots, h_{k_l}^l) = O_{p_l,k_l} \left(r \log \frac{N^{\frac{1}{d}}}{r} + r \right).$$

Pour $i \neq l$, on majore les autres facteurs trivialement, et comme $\forall i \in \{1, \ldots, d\},\ {p_i}^{s_i} \leq N^{\frac{1}{d}} < {p_i}^{s_i+1}$, on obtient

$$\begin{aligned} \sum_{n<N} \mathrm{e}(\mathbf{h} \cdot \mathbf{a}) &\ll_k \left(N^{1-\frac{1}{d}} + N^{\frac{d-1}{d}} \right) \left(r \log \frac{N^{\frac{1}{d}}}{r} + r \right) + r N^{1-\frac{1}{d}} \\ &\ll_k N^{\frac{d-1}{d}} \left(r \log \frac{N^{\frac{1}{d}}}{r} + r \right). \end{aligned}$$

Pour $\mathbf{h} \neq \mathbf{0}$, on a $\underbrace{p_1 \times \cdots \times p_1}_{k_1} \times \cdots \times \underbrace{p_d \times \cdots \times p_d}_{k_d} - 1 = k - 1$ choix possibles. Finalement nous arrivons à l'estimation

$$\sum_{n<N} \sum_{\mathbf{h} \neq \mathbf{0}} \mathrm{e}(\mathbf{h} \cdot \mathbf{a}) \ \ll_k (k-1) \left(N^{\frac{d-1}{d}} \left(r \log \frac{N^{\frac{1}{d}}}{r} + r \right) \right),$$

où la constante implicite dépend seulement de k. Ceci achève la preuve du Théorème 3.3.4. □

3.4 Questions ouvertes

1. Nous avons quelques résultats sur les matrices de différence $\mathbb{Z}_k$ lorsque k est un nombre impair, non nécessairement premier (Théorèmes 3.2.4 et 3.2.5). Plus généralement, peut-on avoir d'autres résultats sur les matrices de différence de $D(g, k, \mathbb{Z}_g)$ avec g impair et $k \geq 4$? Cette question est évoquée par Aaron Montgomery [36] dans les conclusions de son article, où il obtient une formule

asymptotique sur le nombre de matrices de différence construites sur des groupes cycliques, à l'aide de techniques d'analyse de Fourier et d'une approche probabiliste utilisant les marches aléatoires. Cependant, il n'utilise pas la relation d'équivalence définie par Lampio et Östergård [24, 25].

2. En dehors des matrices de différence de $D(r, 2, \mathbb{Z}_2)$ où il y a une seule classe d'équivalence pour tout r où cet ensemble est non vide, la classification obtenue par Lampio concerne des matrices dont la taille est limitée. De plus, la classification se restreint aux groupes de petits cardinaux. Est-il possible de classifier les matrices de différence avec au moins un paramètre non borné ?
3. Nous avons vu que pour une suite aléatoire tirée de manière indépendante et équiprobable, pour tout $m \geq 2$, $C_{\mathbf{r}} = 1 - 1/k^{m-1}$. Est-il possible de construire une famille de suites automatiques dont la moyenne empirique des coefficients de corrélation a le même terme principal que dans le cas aléatoire, pour un ou plusieurs $m \geq 3$?

Chapitre 4

Suites généralisées de Rudin–Shapiro : approche combinatoire

Sommaire

Les résultats de cette partie font l'objet d'une prépublication [29]. Dans le chapitre précédent, nous avons étudié les corrélations discrètes d'ordre 2 des suites généralisées de Rudin–Shapiro, construites à l'aide des matrices de différence. Pour cela nous avons travaillé dans le même esprit que l'article de Grant et al. [20] en utilisant les sommes d'exponentielles.

Ici, nous proposons une nouvelle approche de ces questions par des méthodes combinatoires. Nous élargissons les résultats obtenus au Chapitre 3 (Théorème 3.3.3 et Théorème 3.3.4) et améliorons le terme d'erreur du Théorème 3.3.4. Nous généralisons la définition du coefficient de corrélation d'ordre 2 du Chapitre 3 (Définition 3.3.1). Pour une suite u, des entiers $n \in \mathbb{N}$ et $r \in \mathbb{N} \setminus \{0\}$, et un couple (i, j) donné, on définit un coefficient de corrélation $\delta_{i,j}^r(n)$ en lui attribuant la valeur 1 si $(u_n, u_{n+r}) = (i, j)$ et 0 sinon. Nous travaillons avec des suites u à valeurs dans un groupe abélien fini $(G, +)$ et $(i, j) \in G^2$. On montre alors que si u est une suite généralisée de Rudin–Shapiro, pour tout $(i, j) \in G^2$, la moyenne empirique des coefficients de corrélation $\delta_{i,j}^r(n)$ a le même comportement que pour une suite tirée aléatoirement de manière uniforme. Ainsi, en définissant la matrice de corrélations de la suite u comme la matrice des limites des moyennes empiriques pour chaque couple $(i, j) \in G^2$, nous avons des résultats sur toute la matrice, alors que les résultats du Chapitre 3 portent uniquement sur la trace de la matrice de corrélations. En effet, dans le Chapitre 3, nous avons étudié le cas où $u_n = u_{n+r}$ ce qui implique pour un couple (u_n, u_{n+r}) tel que $(u_n, u_{n+r}) = (i, j)$ que $i = j$. Cela correspond donc à la trace de la matrice de corrélations uniquement. Nous évoquons également le cas de la dimension supérieure en traitant un exemple explicite. Nous nous plaçons dans le cadre des suites, dites *bloc-additives*, qui ont été étudiées dans les articles [14, 37]. Nous reprenons le formalisme de Cateland qui lui les appelle *suites digitales* [9] dans sa thèse. Ces suites

s'obtiennent en considérant la décomposition d'un entier n dans une certaine base k. On associe un poids à chaque couple de chiffres dans la décomposition, et le n-ième terme de la suite est alors défini comme la somme de tous les poids des couples de chiffres consécutifs de la décomposition en base k. On peut également considérer la matrice carrée de taille k dont les entrées sont les poids de tous les couples possibles, que l'on appellera matrice de poids. Dans le cas où cette matrice est une matrice de différence, on dira que la suite associée à cette matrice est une suite généralisée de Rudin–Shapiro. Ainsi, bien que nous utilisions une approche combinatoire à la place de l'utilisation des sommes d'exponentielles dans le Chapitre 3, nous gardons la structure des matrices de différence, pour démontrer que ces suites ont les mêmes corrélations discrètes d'ordre 2 que les suites aléatoires tirées uniformément.

4.1 Définitions et résultats principaux

4.1.1 Suites bloc-additives de rang 2

Pour $k \in \mathbb{N} \setminus \{0\}$, on rappelle que l'on définit $\Sigma_k = \{0, \dots, k-1\}$, et on note $[n]_k$ la représentation de l'entier $n \in \mathbb{N}$ en base k. On peut également la voir comme l'unique suite $x = (x_i)_{i\in\mathbb{N}} \in \Sigma_k^{\mathbb{N}}$ contenant un nombre fini de valeurs non nulles et telle que

$$n = \sum_{i\in\mathbb{N}} x_i k^i.$$

En introduisant la notation $\ell_n = \min\{i \in \mathbb{N} : \forall j > i,\ x_j = 0\}$, on définit la somme des chiffres en base k de l'entier n par

$$\sigma_k(n) = \sum_{i\in\mathbb{N}} x_i = \sum_{i=0}^{\ell_n} x_i.$$

Définition 4.1.1. Soit $(G, +)$ un groupe abélien fini, soit $k \in \mathbb{N} \setminus \{0\}$, et soit $g : \Sigma_k \times \Sigma_k \to G$ une fonction telle que $g(0, 0) = 0$. On dit que la suite $u = (u_n)_{n\in\mathbb{N}} \in G^{\mathbb{N}}$ est une *suite bloc-additive (de rang 2) en base k* de *fonction (ou matrice) de poids g* si pour chaque entier $n \in \mathbb{N}$, on a

$$u_n = \sum_{i\in\mathbb{N}} g(x_i, x_{i+1}),$$

où $[n]_k = x$.

Remarque 4.1.1. Notons que d'après la démonstration du Lemme 3.3.2, les suites généralisées de Rudin–Shapiro de la Définition 3.3.2 pour lesquelles $a(0) = 0$ sont des suites bloc-additives.

Exemple 4.1.1. La suite de Thue–Morse, définie au Chapitre 1, est une suite bloc-additive en base $k = 2$, avec $G = \mathbb{Z}_2$ et pour fonction de poids $g : \Sigma_2 \times \Sigma_2 \to G$ définie par : $\forall (i, j) \in G^2, g(i, j) = i$.

Exemple 4.1.2 (Suite de Rudin–Shapiro (classique))**.** La suite de Rudin–Shapiro (classique) sur $G = \mathbb{Z}_2$ peut aussi être définie comme une suite bloc-additive en base $k = 2$ de fonction de poids $g : \Sigma_2 \times \Sigma_2 \to G$ définies par $\forall (i, j) \in G^2, \quad g(i, j) = ij$.

Ces deux exemples de suites bloc-additives en base 2 sont aussi des suites 2-automatiques. Plus généralement, nous avons le résultat suivant.

Proposition 4.1.1. Si une suite est bloc-additive en base k, alors elle est k-automatique.

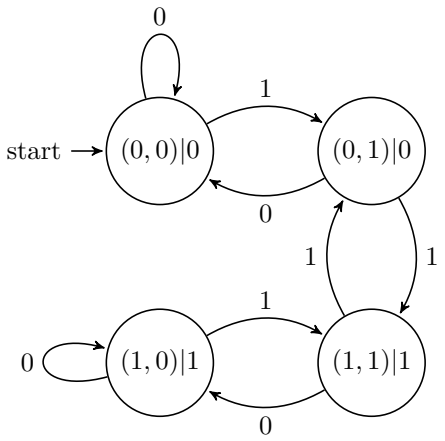
Démonstration. Soit $Q = G \times \Sigma_k$, $q_0 = (0, 0)$, soit $\delta : Q \times \Sigma_k \to Q$ défini par

$$\delta((l, i), j) = (l + g(j, i), j),$$

et soit $\tau : Q \to G$ défini par $\tau(g, i) = g$. L'automate fini déterministe avec sortie $(Q, \Sigma_k, \delta, q_0, \tau)$ calcule la suite bloc-additive $u = (u_n)_{n\in\mathbb{N}}$ de fonction de poids g, en lisant la représentation en base k de l'entier n en commençant par le chiffre de poids fort, et en utilisant la fonction de sortie τ. □

Remarque 4.1.2. Le caractère k-automatique d'une suite bloc-additive peut aussi s'établir à l'aide de la description morphique suivante. On fixe de nouveau $Q = G \times \Sigma_k$ et $q_0 = (0,0)$, et soit $\phi : Q^* \to Q^*$ le morphisme k-uniforme qui satisfait, pour un état $s = (l,i) \in Q$, à $\phi(s) = s_0 \cdots s_{k-1}$, avec $s_j = (l + g(j,i), j)$. Considérons le point fixe $\phi^\omega(q_0) \in Q^{\mathbb{N}}$. Alors, la projection lettre à lettre de $\phi^\omega(q_0)$ par τ est une suite bloc-additive de fonction de poids g.

Exemple 4.1.3. Ci-dessous, voici l'automate fini déterministe avec sortie obtenu par la preuve de la Proposition 4.1.1 pour la suite (classique) de Rudin–Shapiro.



Avec les notations $q_0 = (0,0), q_1 = (0,1), q_2 = (1,0), q_3 = (1,1)$, le 2-morphisme uniforme décrit précédemment est explicité ici par

$$\phi(q_0) = q_0 q_1,\ \phi(q_1) = q_0 q_2,\ \phi(q_2) = q_3 q_1,\ \phi(q_3) = q_3 q_2,$$

avec $\tau(q_0) = \tau(q_1) = 0, \tau(q_2) = \tau(q_3) = 1$.

4.1.2 Principaux résultats

À partir des suites bloc-additives, nous définissons une nouvelle généralisation des suites de Rudin–Shapiro, en utilisant de nouveau les matrices de différence que nous avons étudiées au Chapitre refCh3.

Définition 4.1.2. Une suite bloc-additive est une *suite généralisée de Rudin–Shapiro* si sa fonction de poids g est telle que la matrice $(g(i,j))_{(i,j)\in\Sigma_k\times\Sigma_k} \in G^{\Sigma_k\times\Sigma_k}$ est une matrice de différence.

Exemple 4.1.4.

1. La suite de Thue–Morse *n'est pas* une suite généralisée de Rudin–Shapiro, car sa fonction de poids est donnée par la matrice $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, qui n'est pas un élément de $D(2,2,\mathbb{Z}_2)$.
2. La suite classique de Rudin–Shapiro est une suite généralisée de Rudin–Shapiro, car sa fonction de poids est donnée par la matrice $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, qui est un élément de $D(2,2,\mathbb{Z}_2)$.

Nous présentons ici nos résultats sur ces suites généralisées de Rudin–Shapiro dans le cas de la dimension 1. Nous utiliserons la notation $\log_k(N)$ pour désigner le logarithme de N en base k.

Théorème 4.1.1. Si u est une suite généralisée de Rudin–Shapiro, alors pour chaque $r \in \mathbb{N}\setminus\{0\}$, $g \in G$, et $N \in \mathbb{N}$,

$$\Big|\frac{1}{N}\mathrm{card}\Big\{n \in [\![0, N-1]\!] : u_{n+r} - u_n = g\Big\} - \frac{1}{|G|}\Big| \le r\,k\,\frac{1+\log_k(N)}{N}.$$

La limite $1/|G|$ est donc la même que pour une suite i.i.d. de symboles uniformément distribués dans G. Cependant la convergence est ici beaucoup plus rapide que dans le cas aléatoire, étant donné que le terme d'erreur est de l'ordre de $\log(N)/N$, tandis que pour des suites i.i.d., le théorème central limite nous dit qu'il est en $1/\sqrt{N}$.

Remarque 4.1.3. Dans le cas où k est premier ou une puissance d'un nombre premier, la borne dans le Théorème 4.1.1 est la même que celle obtenue dans les résultats du Chapitre 3 récemment publiés [44, Theorem 4]. Étant donné que les objets sous-jacents (suites de Rudin–Shapiro généralisées obtenues par des matrices de différence) sont les mêmes, c'est assez naturel. Cependant, dans le cas où k est composé, cette nouvelle généralisation avec les suites bloc-additives est différente de celle que nous avons étudiée au Chapitre 3. Elle provient directement d'une unique matrice de différence de taille k, tandis que nous avions utilisé la décomposition en facteurs premiers de k, d'où il résultait un terme d'erreur en $N^{-1/d}$ où d est le nombre de facteurs premiers distincts qui apparaissent dans la décomposition en produit de nombres premiers de k 3.3.4. La taille du terme d'erreur pour cette nouvelle généralisation est de l'ordre de $\log N/N$ ce qui est bien plus petit pour un r fixé et indépendant de la structure arithmétique de k.

Théorème 4.1.2. Si u est une suite généralisée de Rudin–Shapiro, alors pour tout $r \in \mathbb{N} \setminus \{0\}$, et tout couple $(i,j) \in G^2$,

$$\lim_{N\to\infty} \frac{1}{N} \operatorname{card}\Big\{ n \in [\![0, N-1]\!] : (u_n, u_{n+r}) = (i,j) \Big\} = \frac{1}{|G|^2}.$$

4.2 Corrélations discrètes d'ordre 2 des suites généralisées de Rudin–Shapiro

Dans cette partie nous allons prouver le Théorème 4.1.1 et le Théorème 4.1.2. Il s'agit donc de montrer que les suites généralisées de Rudin–Shapiro ont les mêmes corrélations discrètes d'ordre 2 qu'une suite i.i.d. de symboles, et de donner une estimation de la vitesse de convergence.

4.2.1 Fréquences des lettres dans les suites généralisées de Rudin–Shapiro

Nous commençons par quelques résultats sur les suites généralisées de Rudin–Shapiro, dont nous aurons besoin dans la suite.

Lemme 4.2.1. Une suite généralisée de Rudin–Shapiro est une suite morphique primitive.

Démonstration. Comme dans la preuve de la Proposition 4.1.1, fixons $Q = G \times \Sigma_k$, et soit M la matrice indexée par Q, à valeurs dans $\{0,1\}$, définie par $M((l,i),(l',i')) = 1$ si et seulement s'il existe $j \in \Sigma_k$ tel que $(l',i') = (l + g(j,i), j)$. Cette matrice permet donc de décrire les transitions dans l'automate fini déterministe avec sortie donné dans la preuve de la Proposition 4.1.1, ou de manière équivalente, la matrice d'incidence du morphisme k-uniforme défini dans la Remarque 4.1.2. On montre que toutes les entrées de $M^{2|G|+3}$ sont positives (la borne n'étant pas nécessairement optimale). Soit $s_1 = (l_1, i_1)$ et $s_2 = (l_2, i_2)$ deux éléments de Q. Par la condition sur les différences, il existe au moins un $h \in G$ tel que $g(1,h) - g(0,h) = l_2 - l_1 - g(0,1) - g(0,i_1) - g(i_2,0)$. À partir de l'état i_1, on peut lire dans l'automate la suite $(0,h,0,h,0,h,\ldots,0,h,0,h,1,0,i_2)$, faite de $|G|$ fois le motif $(0,h)$, suivi par le motif $(1,0,i_2)$. Alors, le nouvel état sera s_2, car

$$\begin{aligned}
&g(0,i_1) + g(h,0) + g(0,h) + g(h,0) + \cdots + g(0,h) + g(h,0) + g(1,h) + g(0,1) + g(i_2,0)\\
&= |G| g(h,0) + (|G|-1) g(0,h) + g(1,h) + g(0,1) + g(0,i_1) + g(i_2,0)\\
&= g(1,h) - g(0,h) + g(0,1) + g(0,s_1) + g(s_2,0) = l_2 - l_1,
\end{aligned}$$

d'où le résultat. □

Proposition 4.2.1. Si u est une suite généralisée de Rudin–Shapiro, alors chaque motif a une fréquence dans la suite u. De plus, la fréquence de chaque élément de G (correspondant aux motifs de longueur 1) est égal à $1/|G|$.

Démonstration. L'existence des fréquences pour tous les motifs provient du fait que la suite $\phi^\omega(q_0) \in Q^{\mathbb{N}}$ est une suite morphique primitive, où ϕ est le morphisme donné dans la Remarque 4.1.2 [6, Proposition 8.4.1]. De plus, chaque élément de Q a exactement k images réciproques, étant donné que l'état $s = (l,j) \in Q$, peut provenir de l'état $(l - g(j,i), i)$, pour chaque $i \in G$ (en lisant j). Ainsi, tous les éléments de Q ont la même fréquence dans $\phi^\omega(q_0)$, et par conséquent, chaque élément de G a la même fréquence dans l'image de $\phi^\omega(q_0)$ par τ. □

4.2.2 Fibre d'un entier

Nous introduisons la notion de *fibre d'un entier* qui sera très pratique dans notre étude des corrélations d'ordre 2 des suites généralisées de Rudin–Shapiro.

Soit $r \in \mathbb{N} \setminus \{0\}$ un entier fixé. Pour $n \in \mathbb{N}$, notons les représentations de n et $n+r$ en base k comme suit

$$\begin{aligned} [n]_k &= x, \\ [n+r]_k &= y. \end{aligned}$$

On définit l'entier

$$c_n = \min\{i \in \mathbb{N} : \forall j > i, x_j = y_j\}.$$

Notons que c_n dépend de r, mais afin de simplifier, nous ne mentionnons pas cette dépendance dans la notation. L'entier c_n mesure la propagation de la retenue lorsque l'on additionne r à n. Par définition, $x_{c_n} \neq y_{c_n}$ et $\forall j > c_n$, $x_j = y_j$. La définition de c_n peut se représenter ainsi.

$$\begin{array}{rccccccc} [n]_k = & x_0 & x_1 & \cdots & x_{c_n} & x_{c_n+1} & x_{c_n+2} & \cdots \\ [n+r]_k = & y_0 & y_1 & \cdots & y_{c_n} & x_{c_n+1} & x_{c_n+2} & \cdots \end{array} \tag{4.1}$$

On définit la *fibre* de n comme l'ensemble

$$\begin{aligned} \mathcal{F}(n) &= \{m \in \mathbb{N} : x' = [m]_k \text{ satisfait } \forall i \in \mathbb{N} \setminus \{c_n + 1\},\ x'_i = x_i\} \\ &= \{n + (\alpha - x_{c_n+1})\, k^{c_n+1} : \alpha \in \Sigma_k\}. \end{aligned}$$

On a alors

$$\begin{array}{rccccccc} \mathcal{F}(n) = \{\ x_0 & x_1 & \cdots & x_{c_n} & 0 & x_{c_n+2} & x_{c_n+3} & \cdots, \\ x_0 & x_1 & \cdots & x_{c_n} & 1 & x_{c_n+2} & x_{c_n+3} & \cdots, \\ x_0 & x_1 & \cdots & x_{c_n} & 2 & x_{c_n+2} & x_{c_n+3} & \cdots, \\ & & & & \vdots & & & \\ x_0 & x_1 & \cdots & x_{c_n} & k-1 & x_{c_n+2} & x_{c_n+3} & \cdots\}. \end{array}$$

Notons que si $m \in \mathcal{F}(n)$, alors $c_m = c_n$, et donc

$$m \in \mathcal{F}(n) \iff n \in \mathcal{F}(m).$$

De plus, soit $m \in \mathcal{F}(n)$, et soit $x' = [m]_k$, $y' = [m+r]_k$. Alors, on a

$$y'_{c_n+1} = x'_{c_n+1}, \quad \text{and} \quad \forall i \in \mathbb{N} \setminus \{c_n + 1\}, \quad y'_i = y_i,$$

qui se représente ainsi :

$$\begin{array}{rccccccc} [m]_k = x' = & x_0 & x_1 & \cdots & x_{c_n} & x'_{c_n+1} & x_{c_n+2} & \cdots \\ [m+r]_k = y' = & y_0 & y_1 & \cdots & y_{c_n} & x'_{c_n+1} & x_{c_n+2} & \cdots \end{array} \tag{4.2}$$

Soit u une suite bloc-additive en base k de poids g, et rappelons la notation $\pi = k/|G|$. Pour $n \in \mathbb{N}$, on introduit aussi la notation $\Delta_r(n) = u_{n+r} - u_n$.

Proposition 4.2.2. Si u est une suite généralisée de Rudin–Shapiro, alors pour chaque $n \in \mathbb{N}$,

$$\forall g \in G, \quad \operatorname{card}\{m \in \mathcal{F}(n) : \Delta_r(m) = g\} = \pi.$$

Démonstration. Par définition d'une suite bloc-additive, avec les notations de (4.1), on a

$$\begin{aligned} \Delta_r(n) &= \sum_{i \in \mathbb{N}} g(y_i, y_{i+1}) - \sum_{i \in \mathbb{N}} g(x_i, x_{i+1}) \\ &= \sum_{i=0}^{c_n} \Big(g(y_i, y_{i+1}) - g(x_i, x_{i+1}) \Big). \end{aligned}$$

Si $m \in \mathcal{F}(n)$, avec les notations de (4.2), on a

$$\Delta_r(m) = \sum_{i=0}^{c_n} (g(y'_i, y'_{i+1}) - g(x'_i, x'_{i+1})),$$

et ainsi

$$\begin{aligned}\Delta_r(m) - \Delta_r(n) &= \Big(g(y'_{c_n}, y'_{c_n+1}) - g(x'_{c_n}, x'_{c_n+1})\Big) - \Big(g(y_{c_n}, y_{c_n+1}) - g(x_{c_n}, x_{c_n+1})\Big) \\ &= \Big(g(y_{c_n}, x'_{c_n+1}) - g(x_{c_n}, x'_{c_n+1})\Big) - \Big(g(y_{c_n}, x_{c_n+1}) - g(x_{c_n}, x_{c_n+1})\Big).\end{aligned}$$

Il s'ensuit que pour tout $g \in G$,

$$\operatorname{card}\{m \in \mathcal{F}(n) : \Delta_r(m) - \Delta_r(n) = g\} = \operatorname{card}\Big\{\alpha \in \Sigma_k : g(y_{c_n}, \alpha) - g(x_{c_n}, \alpha) - A_n = g\Big\},$$

avec $A_n = g(y_{c_n}, x_{c_n+1}) - g(x_{c_n}, x_{c_n+1})$.
Par conséquent, si u est une suite généralisée de Rudin-Shapiro, alors pour chaque $n \in \mathbb{N}$, on a

$$\forall g \in G, \quad \operatorname{card}\{m \in \mathcal{F}(n) : \Delta_r(m) - \Delta_r(n) = g\} = \pi,$$

et on en déduit la Proposition 4.2.2. □

4.2.3 Preuve du Théorème 4.1.1

En utilisant la notion de fibre développée précédemment, on obtient la proposition suivante, d'où découle directement le Théorème 4.1.1, étant donné que $\sum_{g\in G} \operatorname{card}\Big\{n \in [\![0, N-1]\!] : \Delta_r(n) = g\Big\} = N$.

Proposition 4.2.3. Si u est une suite généralisée de Rudin–Shapiro, alors pour chaque $g \in G$,

$$\begin{aligned}\operatorname{card}\Big\{n \in [\![0, N-1]\!] : \Delta_r(n) = g\Big\} &\geq \frac{\pi N}{k} - \pi\, r\, k - \pi\, r\, \sigma_k(N) \\ &\geq \frac{N}{|G|} - \pi\, r\, k(1 + \log_k(N)).\end{aligned}$$

Démonstration. Soit $N \in \mathbb{N} \setminus \{0\}$, et soit $a = [N]_k$. On détermine les conditions sous lesquelles un entier $n \in [\![0, N-1]\!]$ satisfait $\mathcal{F}(n) \subset [\![0, N-1]\!]$. Rappelons la notation $\ell_N = \min\{i \in \mathbb{N} : \forall j > i, a_i = 0\}$. On peut alors écrire

$$[N]_k = a_0\ a_1\ \cdots\ a_{\ell_N - 1}\ a_{\ell_N}\ 0\ 0\ \cdots$$

— Si $n = a'_{\ell_N}\, k^{\ell_N} + \alpha\, k^{\ell_N - 1} + \gamma$, pour $\alpha \leq k-1$, $a'_{\ell_N} < a_{\ell_N}$, et $\gamma < k^{\ell_N - 1} - r$, on a $c_n \leq \ell_N - 2$, et alors $\mathcal{F}(n) \subset [\![0, N-1]\!]$.

$$\begin{aligned}[n]_k &= \underbrace{x_0\ x_1\ \cdots\ x_{\ell_N - 2}}_{\gamma < k^{\ell_N - 1} - r}\ \alpha\ \underbrace{a'_{\ell_N}}_{< a_{\ell_N}}\ 0\ 0\ \cdots \\ [n+r]_k &= x'_0\ x'_1\ \cdots\ x'_{\ell_N - 2}\ \alpha\ a'_{\ell_N}\ 0\ 0\ \cdots\end{aligned}$$

— Si $n = a_{\ell_N}\, k^{\ell_N} + a'_{\ell_N - 1}\, k^{\ell_N - 1} + \alpha\, k^{\ell_N - 2} + \gamma$, pour $\alpha \leq k-1$, $a'_{\ell_N - 1} < a_{\ell_N - 1}$, et $\gamma < k^{\ell_N - 2} - r$, on a $c_n \leq \ell_N - 3$, et ainsi $\mathcal{F}(n) \subset [\![0, N-1]\!]$.

$$\begin{aligned}[n]_k &= \underbrace{x_0\ x_1\ \cdots\ x_{\ell_N - 3}}_{\gamma < k^{\ell_N - 2} - r}\ \alpha\ \underbrace{a'_{\ell_N - 1}}_{< a_{\ell_N - 1}}\ a_{\ell_N}\ 0\ 0\ \cdots \\ [n+r]_k &= x'_0\ x'_1\ \cdots\ x'_{\ell_N - 3}\ \alpha\ a'_{\ell_N - 1}\ a_{\ell_N}\ 0\ 0\ \cdots\end{aligned}$$

— Si $n = a_{\ell_N}\, k^{\ell_N} + a_{\ell_N-1}\, k^{\ell_N-1} + a'_{\ell_N-2}\, k^{\ell_N-2} + \alpha\, k^{\ell_N-3} + \gamma$, pour $\alpha \leq k-1$, $a'_{\ell_N-2} < a_{\ell_N-2}$, et $\gamma < k^{\ell_N-3} - r$, on a $c_n \leq \ell_N - 4$, et ainsi $\mathcal{F}(n) \subset [\![0, N]\!]$.

$$[n]_k = \underbrace{x_0\ x_1\ \cdots\ x_{\ell_N-4}}_{\gamma<k^{\ell_N-3}-r}\ \alpha\ \underbrace{a'_{\ell_N-2}}_{<a_{\ell_N-2}}\ a_{\ell_N-1}\, a_{\ell_N}\ 0\, 0\ \cdots$$
$$[n+r]_k = x'_0\, x'_1\ \cdots\ x'_{\ell_N-4}\ \alpha\ a'_{\ell_N-2}\ a_{\ell_N-1}\, a_{\ell_N}\ 0\, 0\ \cdots$$

— Et enfin, la dernière condition que nous pouvons avoir est dans le cas où $n = a_{\ell_N}\, k^{\ell_N} + a_{\ell_N-1}\, k^{\ell_N-1} + \ldots + a_{\ell_r+3}\, k^{\ell_r+3} + a'_{\ell_r+2}\, k^{\ell_r+2} + \alpha\, k^{\ell_r+1} + \gamma$, pour $\alpha \leq k-1$, $a'_{\ell_r+2} < a_{\ell_r+2}$, et $\gamma < k^{\ell_r+1} - r$, on a $c_n \leq \ell_r$, et ainsi $\mathbb{F}(n) \subset [\![0, N-1]\!]$.

Le nombre d'entiers différents $n \in [\![0, N-1]\!]$ satisfaisant $\mathcal{F}(n) \subset [\![0, N-1]\!]$ que nous avons exhibés précédemment est égal à

$$\begin{aligned} & a_{\ell_N} k(k^{\ell_N-1} - r) + a_{\ell_N-1} k(k^{\ell_N-2} - r) + a_{\ell_N-2} k(k^{\ell_N-3} - r) + \ldots + a_{\ell_r+2} k(k^{\ell_r+1} - r) \\ = \ & N - (a_{\ell_r+1} k^{\ell_r+1} + a_{\ell_r} k^{\ell_r} + \ldots + a_1 k + a_0) - r\, k\, (a_{\ell_N} + a_{\ell_N-1} + a_{\ell_N-2} + \ldots + a_{\ell_r+2}) \\ > \ & N - r\, k^2 - r\, k\, \sigma_k(N). \end{aligned}$$

Pour la dernière inégalité, on remarque que $a_{\ell_r+1} k^{\ell_r+1} + a_{\ell_r} k^{\ell_r} + \ldots + a_1 k + a_0 < k^{\ell_r+2} \leq r\, k^2$. La Proposition 4.2.3 provient alors directement de la Proposition 4.2.2. □

4.2.4 Matrice de corrélations

Afin de prouver le Théorème 4.1.2, nous commençons par introduire la notion de matrice de corrélations, et nous formulons les résultats précédents avec cette terminologie.

Soit $u \in G^{\mathbb{N}}$ une suite fixée. Pour $r \in \mathbb{N} \setminus \{0\}$, $(i,j) \in G^2$ et $n \in \mathbb{N}$, on définit

$$\delta^r_{i,j}(n) = \begin{cases} 1 & \text{si } (u_n, u_{n+r}) = (i,j); \\ 0 & \text{sinon.} \end{cases}$$

et

$$C^r_{i,j}(N) = \frac{1}{N} \sum_{n=0}^{N-1} \delta^r_{i,j}(n).$$

Comme conséquence directe de la Proposition 4.2.1, si u est une suite généralisée de Rudin–Shapiro, alors pour tout $r \in \mathbb{N} \setminus \{0\}$ et tout $(i,j) \in G^2$, la suite $C^r_{i,j}(N)$ converge quand N tend vers l'infini et par conséquent nous pouvons introduire la quantité

$$C^r_{i,j} = \lim_{N\to\infty} C^r_{i,j}(N).$$

De plus, toujours grâce à la Proposition 4.2.1, pour chaque $i \in G$, la fréquence asymptotique du symbole i est

$$\sum_{j\in G} C^r_{i,j} = \frac{1}{|G|}.$$

On appelle matrice de corrélations, la matrice de taille $|G| \times |G|$ où pour tout couple $(i,j) \in G^2$ le coefficient ligne i et colonne j est $C^r_{i,j}$.
Comme conséquence de la Proposition 4.2.3, nous obtenons les résultats suivants.

Corollaire 4.2.1. Si u est une suite généralisée de Rudin–Shapiro, alors pour chaque couple $(i,j) \in G^2$,

$$\sum_{\ell\in G} C^r_{i-\ell,j-\ell}(N) \geq \frac{1}{|G|} - \pi\, r\, k \frac{1 + \log_k(N)}{N}.$$

Corollaire 4.2.2. Si u est une suite généralisée de Rudin–Shapiro, alors pour chaque couple $(i,j) \in G^2$,

$$\sum_{\ell \in G} C^r_{i-\ell,j-\ell} = \frac{1}{|G|}.$$

Démonstration. C'est une conséquence du Corollaire 4.2.1 et du fait que $\sum_{(i,j)\in G^2} C^r_{i,j} = 1$. □

Notons que ces résultats élargissent ceux obtenus au Chapitre 3 (Théorème 3.3.3 et Théorème 3.3.4) qui détectent quand deux symboles diffèrent ou non (voir Remarque 4.1.3). Plus précisément, les deux résultats du Chapitre 3 prouvent que

$$\sum_{i \in G} C^r_{i,i} = \frac{1}{|G|}.$$

4.2.5 Preuve du Théorème 4.1.2

Avec les notations ci-dessus, le Théorème 4.1.2 est équivalent à la proposition suivante. Notons que ce résultat est plus fort que le Corollaire 4.2.2 car il donne les valeurs de chaque terme dans la somme.

Proposition 4.2.4. Si u est une suite généralisée de Rudin–Shapiro, alors pour tout couple $(i,j) \in G^2$,

$$C^r_{i,j} = \frac{1}{|G|^2}.$$

Démonstration. Fixons un certain $\alpha \in \Sigma_k$ et considérons les entiers $n \in [\![0, k^{2N+1}-1]\!]$ qui sont tels que la décomposition en base k $x = [n]_k$ de n satisfait $x_{N+1} = \alpha$. En d'autres termes, $n = m_1\, k^{N+1} + \alpha\, k^N + m_2$, avec des entiers $m_1, m_2 \in [\![0, k^N - 1]\!]$. De plus, supposons que $m_2 < k^N - r$, et nous aurons ainsi $c_n < N$, de sorte que

$$(u_n, u_{n+r}) = (u_{km_1+\alpha}, u_{km_1+\alpha}) + (u_{\alpha k^N+m_2}, u_{\alpha k^N+m_2+r}),$$

par définition d'une suite bloc-additive.

La preuve se fonde sur l'idée suivante : lorsque l'on prend aléatoirement et indépendamment des entiers m_1, m_2 uniformément distribués dans $[\![0, k^N - 1]\!]$, la distribution de $u_{km_1+\alpha}$ converge vers la distribution uniforme sur G quand N tend vers l'infini, tandis que pour le deuxième terme $(u_{\alpha k^N+m_2}, u_{\alpha k^N+m_2+r})$, la distribution est donnée asymptotiquement par les valeurs $C_{i,j}$ de la matrice de corrélations. Maintenant, on a $(u_n, u_{n+r}) = (i,j)$ si $u_{km_1+\alpha} = \ell$ pour un certain ℓ et $(u_{\alpha k^N+m_2}, u_{\alpha k^N+m_2+r}) = (i-\ell, j-\ell)$. En utilisant l'indépendance de m_1 et m_2, on obtient alors

$$C^r_{i,j} = \sum_{\alpha\in\Sigma_k} \frac{1}{k} \sum_{\ell \in G} \frac{1}{|G|} C_{i-\ell,j-\ell} = \sum_{\alpha\in\Sigma_k} \frac{1}{k} \frac{1}{|G|} \frac{1}{|G|} = \frac{1}{|G|^2},$$

étant donné que l'on savait déjà avec le Corollaire 4.2.2 que pour tout couple $(i,j) \in G^2$, $\sum_{\ell\in G} C_{i-\ell,j-\ell} = \frac{1}{|G|}$.

Plus formellement, introduisons les notations suivantes, pour tous $i, j, \ell \in G$,

$$A^\alpha_\ell(N) = \mathrm{card}\{m \in [\![0, k^N - 1]\!] : u_{km+\alpha} = \ell\}$$
$$B^{r,\alpha}_{i,j}(N) = \mathrm{card}\{m \in [\![0, k^N - r - 1]\!] : \delta^r_{i,j}(\alpha\, k^N + m) = 1\}.$$

Pour n'importe quel $\alpha \in \Sigma_k$ nous avons les limites suivantes :

$$\lim_{N\to\infty} \frac{A^\alpha_\ell(N)}{k^N} = \frac{1}{|G|}, \quad \text{and} \quad \lim_{N\to\infty} \sum_{\ell\in G} \frac{B^{r,\alpha}_{i-\ell,j-\ell}(N)}{k^N} = \frac{1}{|G|}.$$

Pour la première limite, on utilise les mêmes outils que pour la Proposition 4.2.1. Soit ϕ le morphisme primitif de la Remarque 4.1.2, tel que la suite u est l'image de $\phi^\omega(q_0)$ par τ. On peut remarquer que la suite $(u_{kn+\alpha})_{n\in\mathbb{N}}$ est l'image de $\phi^\omega(q_0)$ par la fonction $\tau' : Q \to G$ définie par $\tau'(l,i) = l + g(i,\alpha)$. Comme nous l'avions déjà montré dans la Proposition 4.2.1, tous les éléments de Q ont la même fréquence dans

$\phi^\omega(q_0)$. Par conséquent, chaque élément de G a la même fréquence dans l'image de $\phi^\omega(q_0)$ par τ'. En effet, pour chaque $l' \in G$ et $i \in \Sigma_k$, il existe exactement un $l \in G$ tel que $\tau'(l,i) = l'$, et ainsi le cardinal $\tau'^{-1}(\{l'\})$ ne dépend pas du choix de l'.

La deuxième limite est une légère variation du Corollaire 4.2.2, et peut-être calculée exactement de la même manière, en utilisant les mêmes étapes que dans la Proposition 4.2.3. De plus, pour chaque couple $(i,j) \in G^2$, on a

$$\sum_{n=0}^{k^{2N+1}-1} \delta_{i,j}^r(n) \geq \sum_{\alpha\in\Sigma_k} \sum_{\ell\in G} A_\ell^N(\alpha)\, B_{i-\ell,j-\ell}^N(\alpha).$$

Il s'ensuit que

$$C_{i,j}^r(k^{2N+1}) \geq \frac{1}{k} \sum_{\alpha\in\Sigma_k} \sum_{\ell\in G} \frac{A_\ell^N(\alpha)}{k^N}\, \frac{B_{i-\ell,j-\ell}^N(\alpha)}{k^N}.$$

Quand N tend vers l'infini, on sait que la limite du terme de gauche existe et est égale à $C_{i,j}^r$. On obtient alors

$$C_{i,j}^r \geq \frac{1}{|G|^2}.$$

Comme $\sum_{(i,j)\in G^2} C_{i,j}^r = 1$, ceci termine la preuve. □

4.3 Suites généralisées de Rudin–Shapiro en dimension supérieure

Nous proposons une extension naturelle des Définitions 4.1.1 et 4.1.2 en dimension d. Pour une meilleure lisibilité, nous représentons les éléments de Σ_k^d en vecteurs colonnes.

Définition 4.3.1. Soit $(G,+)$ un groupe abélien fini, et soit $k \in \mathbb{N}\setminus\{0\}$. On dit que la suite $u = (u_{n_1,\dots,n_d})_{(n_1,\dots,n_d)\in\mathbb{N}^d} \in G^{\mathbb{N}^d}$ est une *suite bloc-additive d-dimensionnelle en base k* s'il existe une application $g : \Sigma_k^d \times \Sigma_k^d \to G$ satisfaisant $g\left(\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}, \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}\right) = 0$, telle que pour tout entier $n \in \mathbb{N}$, on a

$$u_{n_1,\dots,n_d} = \sum_{i\in\mathbb{N}} g\left(\begin{pmatrix}x_i^1\\ \vdots\\ x_i^d\end{pmatrix}, \begin{pmatrix}x_{i+1}^1\\ \vdots\\ x_{i+1}^d\end{pmatrix}\right) = \sum_{i\in\mathbb{N}} g(x_i, x_{i+1}),$$

où $x = (x_i)_{i\in\mathbb{N}} = \begin{pmatrix}x^1\\ \vdots\\ x^d\end{pmatrix} = \begin{pmatrix}(x_i^1)_{i\in\mathbb{N}}\\ \vdots\\ (x_i^d)_{i\in\mathbb{N}}\end{pmatrix} = \begin{pmatrix}[n_1]_k\\ \vdots\\ [n_d]_k\end{pmatrix}$.

De plus on dit que la suite u est une *suite généralisée de Rudin–Shapiro d-dimensionnelle* si la fonction g satisfait

$$\forall (i,j) \in \Sigma_k^d \times \Sigma_k^d \text{ with } i \neq j, \quad \forall l \in G, \quad \operatorname{card}\Big\{h \in \Sigma_k^d : g(i,h) - g(j,h) = l\Big\} = \frac{k}{|G|}.$$

De manière équivalente, cela revient à dire que la matrice $(g(i,j))_{(i,j)\in\Sigma_k^d\times\Sigma_k^d}$ est une matrice de différence.

Comme dans le cas 1-dimensionnel, une suite d-dimensionnelle qui est bloc-additive en base k est une suite k-automatique.

Soit $r \in \mathbb{N}^d \setminus \{(0,\dots,0)\}$. Pour $n = (n_1,\dots,n_d) \in \mathbb{N}^d$, on introduit les représentations de n et $n+r$ en base k comme suit

$$[n]_k = x = \begin{pmatrix}x^1\\ \vdots\\ x^d\end{pmatrix}, \qquad [n+r]_k = y = \begin{pmatrix}y^1\\ \vdots\\ y^d\end{pmatrix},$$

et on définit l'entier

$$c_n = \min\{i \in \mathbb{N} : \ \forall j > i,\, x_j = y_j\},$$

qui mesure la propagation de la retenue quand on ajoute r à n.

À nouveau, on définit la *fibre* de n comme l'ensemble

$$\mathcal{F}(n) = \{m \in \mathbb{N} : x' = [m]_k \text{ satisfaisant } \forall i \in \mathbb{N} \setminus \{c_n + 1\},\ x'_i = x_i\},$$

et on utilise la notation $\Delta_r(n) = u_{n+r} - u_n$.

Comme la suite d-dimensionelle a d composantes qui sont toutes 1-dimensionnelles et indépendantes, les arguments précédents peuvent être repris mot pour mot.

Proposition 4.3.1. Si u est une suite généralisée de Rudin–Shapiro d-dimensionnelle, alors pour tout $n \in \mathbb{N}$,

$$\forall l \in G, \quad \text{card}\{m \in \mathcal{F}(n) : \Delta_r(m) = l\} = \pi.$$

Nous pouvons également étendre les notations δ^r et C^r aux suites d-dimensionelles. Précisément, pour $N = (N_1, \ldots, N_d)$, on définit

$$C^r_{i,j}(N) = \frac{1}{N_1 \cdots N_d} \sum_{\{n \in \mathbb{N}^d \,:\, n < N\}} \delta^r_{i,j}(n),$$

où l'on écrit $n < N$ pour $\forall i \in \{1, \ldots, d\}, n_i < N_i$. On introduit aussi

$$C^r_{i,j} = \lim_{N \to \infty} C^r_{i,j}(N).$$

Comme dans le cas 1-dimensionnel, on peut montrer que si u est une suite généralisée de Rudin–Shapiro d-dimensionnelle, alors pour chaque couple $(i, j) \in G^2$,

$$\sum_{\ell \in G} C^r_{i-\ell, j-\ell} = \frac{1}{|G|},$$

ce qui permet également d'obtenir la généralisation suivante de la Proposition 4.2.4.

Proposition 4.3.2. Si u est une suite généralisée de Rudin–Shapiro d-dimensionnelle, alors pour tout couple $(i, j) \in G^2$,

$$C^r_{i,j} = \frac{1}{|G|^2}.$$

Exemple 4.3.1. Nous représentons dans la Figure 4.3.1 quatre exemples différents de suites généralisées de Rudin–Shapiro, pour $d = 2$, $k = 2$, $G = \mathbb{Z}_2$. Pour chaque exemple, les valeurs de la fonction $g : \Sigma_2^2 \to \mathbb{Z}_2$ sont données par une matrice, avec les éléments de Σ_2^2 rangés dans l'ordre lexicographique. Sur la première ligne de la matrice, on peut donc lire successivement

$$g\left(\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix}\right), \quad g\left(\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right), \quad g\left(\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\right), \quad g\left(\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right),$$

et donc sur la deuxième ligne

$$g\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix}\right), \quad g\left(\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right), \qquad \cdots$$

et ainsi de suite. Sur les images, la cellule $(n_1, n_2) \in \mathbb{N}^2$ est coloriée en bleue si $u_{n_1,n_2} = 1$ et en blanc si $u_{n_1,n_2} = 0$. La valeur $u_{0,0}$ se situe dans le coin inférieur gauche.

Nous présentons plus en détail le premier exemple. Pour $i, j \in \Sigma_2^2$, la fonction de poids satisfait $g(i, j) = 0$ si $i = j$, et $g(i, j) = 1$ sinon. En exemple, nous calculons ci-dessous $u_{436,48}$.

$$\begin{array}{rcccccccccccc}
[436]_2 & = & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & \cdots \\
[48]_2 & = & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots \\
\hline
u_{436,48} & \equiv & 0 + & 1 + & 1 + & 1 + & 0 + & 1 + & 1 + & 0 + & 1 + & 0 + & \cdots & \equiv 0 \pmod 2
\end{array}$$

La table suivante donne les premières valeurs de u_{n_1,n_2}, pour $(n_1, n_2) \in [\![0, 2^3 - 1]\!]^2$.

7	1	0	1	0	0	1	0	1
6	0	0	1	1	1	1	0	0
5	1	1	1	1	1	1	1	1
4	0	1	1	0	0	1	1	0
3	1	0	0	1	0	1	1	0
2	0	0	0	0	1	1	1	1
1	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1
$n_2 \diagdown n_1$	0	1	2	3	4	5	6	7

Ces valeurs sont également présentes dans le coin inférieur gauche de taille carrée 8×8 des deux images de la première ligne de la Figure 4.3.1.

Concernant le deuxième exemple, on peut remarquer que la fonction poids satisfait

$$g\left(\binom{i_1}{i_2}, \binom{j_1}{j_2}\right) \equiv i_1 j_1 + i_2 j_2 \pmod 2.$$

Par conséquent, la suite obtenue peut aussi être calculée par $u_{m,n} = v_m + v_n$, où v est la suite classique 1-dimensionnelle de Rudin–Shapiro.

4.4 Questions ouvertes

Jusqu'ici nous avons considéré seulement les suites blocs-additives de rang 2. Plus généralement, on peut considérer la notion de fonction bloc-additive de rang L, pour un entier $L \in \mathbb{N} \setminus \{0\}$, au sens de Cateland [9].

Définition 4.4.1. Soit $(G, +)$ un groupe abélien fini, soit $k \in \mathbb{N} \setminus \{0\}$, et soit $g : \Sigma_k^L \to G$ une fonction satisfaisant $g(0, 0, \ldots, 0) = 0$. On dit que la suite $u = (u_n)_{n\in\mathbb{N}} \in G^{\mathbb{N}}$ est une *suite bloc-additive (de rang L) en base k* de *fonction poids g* si pour chaque entier $n \in \mathbb{N}$, on a

$$u_n = \sum_{i\in\mathbb{N}} g(x_i, x_{i+1}, \ldots, x_{i+L-1}),$$

où $[n]_k = x$.

Soit $(G, +)$ un groupe abélien fini, et soit $k \in \mathbb{N} \setminus \{0\}$. On dit que la fonction $d : \Sigma_k^L \to G$ satisfait la *condition de différence (de rang L)* si :

$$\forall (i, j) \in \Sigma_k \times \Sigma_k \text{ with } i \neq j, \quad \forall (x_2, \ldots, x_{L-1}) \in \Sigma_k^{L-2},$$
$$\forall l \in G, \quad \operatorname{card}\{h \in \Sigma_k : d(i, x_2, \ldots, x_{L-1}, h) - d(j, x_2, \ldots, x_{L-1}, h) = l\} = \frac{k}{|G|}.$$

La condition de différence est une condition suffisante pour les mêmes résultats que dans la Section 4.2.

Exemple 4.4.1. Prenons $k = 2$, $G = \mathbb{Z}_2$, et soit $g : \Sigma_k^3 \to G$ définie par $g(x, y, z) = \begin{cases} 0 \text{ si } x = y = z \\ 1 \text{ sinon.} \end{cases}$.
Cette fonction satisfait la condition de différence. Par conséquent, la suite bloc-additive $u = (u_n)_{n\in\mathbb{N}}$ de fonction poids g, qui est telle que u_n compte (modulo 2) le nombre de blocs différents de 000 et de 111 dans la décomposition binaire de n, a les mêmes corrélations d'ordre 2 qu'une suite binaire choisie uniformément et aléatoirement.

Une autre perspective de recherche possible consiste à essayer de construire des suites bloc-additives pour lesquelles il n'y a pas seulement les corrélations d'ordre 2, mais toutes les corrélations d'ordre

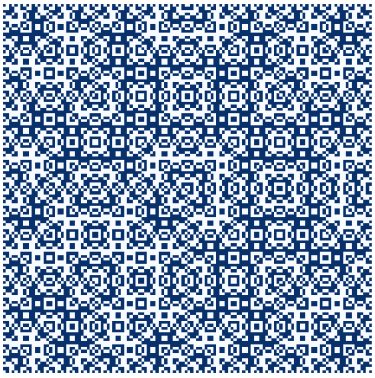
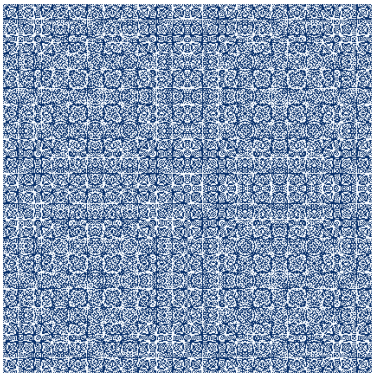
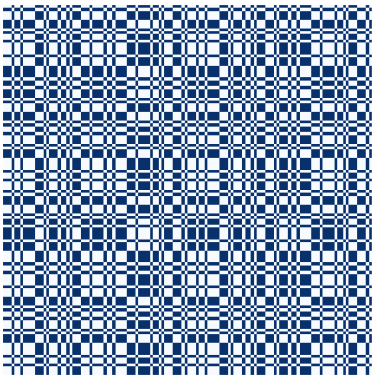
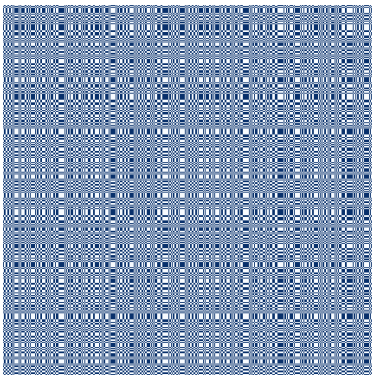
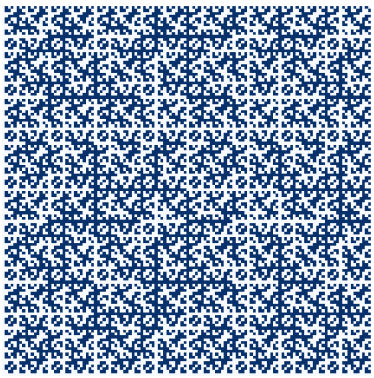
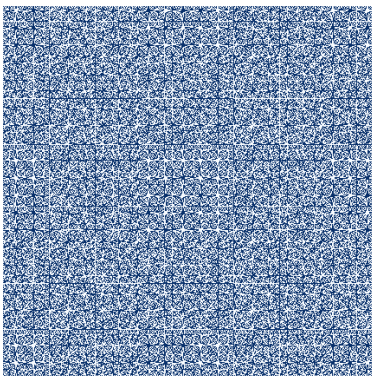
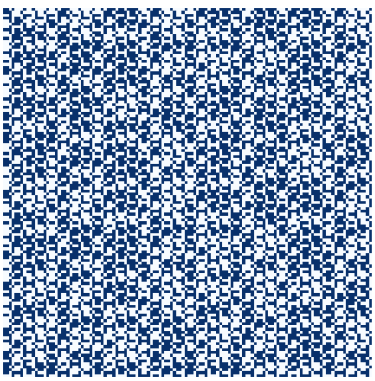
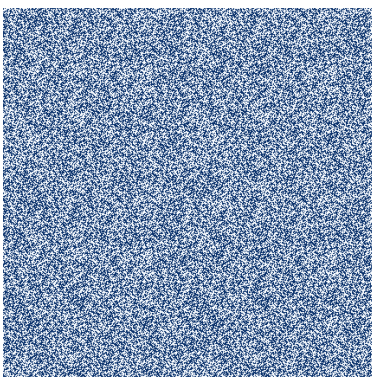
Matrice	Termes dans $[\![0, 2^7 - 1]\!]^2$	Termes dans $[\![0, 2^{10} - 1]\!]^2$
$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$		
$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$		
$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$		
$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$		

FIGURE 4.1 – Exemples de suites généralisées de Rudin–Shapiro 2-dimensionnelles en base 2.

supérieur qui seraient les mêmes que pour des suites aléatoires tirées de manière uniforme. Précisément, pour des entiers $0 < r_1 < \cdots < r_{\ell-1}$, et pour un choix de vecteur $(i_0, \ldots, i_{\ell-1}) \in G^\ell$, on introduit

$$\delta^r_{i_0,\ldots,i_{\ell-1}}(n) = \begin{cases} 1 & \text{si } (u_n, u_{n+r_1}, \ldots, u_{n+r_{\ell-1}}) = (i_0, \ldots, i_{\ell-1}); \\ 0 & \text{sinon,} \end{cases}$$

et on regarde le comportement asymptotique de $\frac{1}{N}\sum_{n=0}^{N-1} \delta^r_{(i_0,\ldots,i_{\ell-1})}(n)$, quand N tend vers l'infini. On dit qu'une suite a les mêmes corrélations d'ordre ℓ qu'une suite aléatoire tirée uniformément si pour n'importe quel choix de $0 < r_1 < \ldots < r_{\ell-1}$, et pour n'importe quel vecteur $(i_0, \ldots, i_{\ell-1}) \in G^\ell$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \delta^r_{i_0,\ldots,i_{\ell-1}}(n) = \frac{1}{|G|^\ell}.$$

1. Comment peut-on engendrer des fonctions satisfaisant la condition de différence de rang L ? Peut-on avoir une condition plus faible sur la fonction poids pour laquelle les suites bloc-additives obtenues ont les mêmes corrélations d'ordre 2 ?
2. Pour un certain $m \geq 3$, est-il possible de construire une suite bloc-additive ayant les mêmes corrélations d'ordre m qu'une suite aléatoire tirée uniformément ?
3. Pour les suites proposées, le terme d'erreur est-il optimal ?

Notons qu'il n'est pas possible de construire une suite automatique telle que *pour n'importe quel* $\ell \geq 1$, les corrélations d'ordre ℓ serait les mêmes que pour une suite aléatoire tirée uniformément. En effet, cela impliquerait en particulier que la suite serait normale, alors que la complexité d'une suite automatique est au plus linéaire.

Annexe A

Codes SageMath de la Figure 4.3.1

Nous donnons ici les codes SageMath permettant d'obtenir les images de la Figure 4.3.1. On trouvera également des simulations numériques, permettant d'illustrer les résultats sur les corrélations d'ordre 2 des Chapitres 3 et 4.

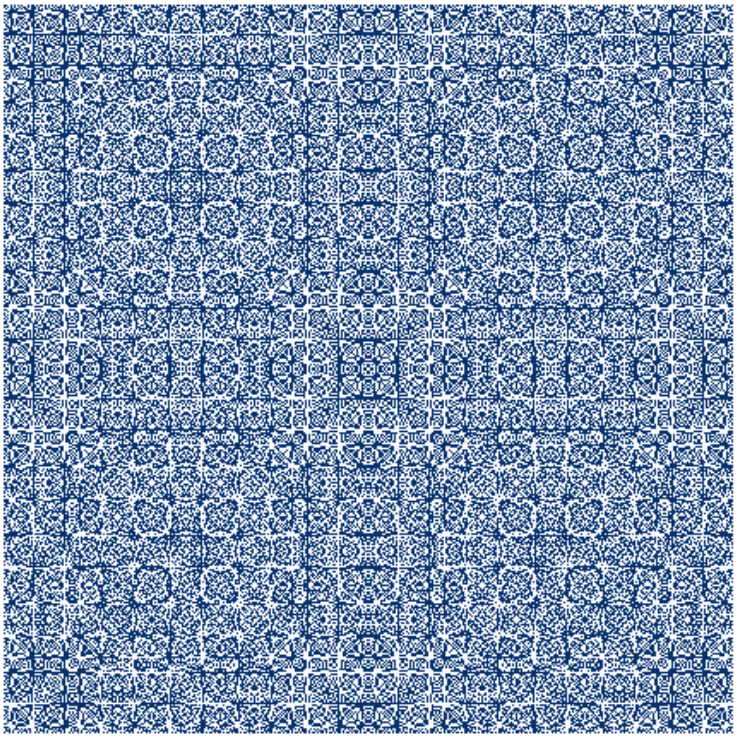
Rudin-Shapiro 2D

```
import numpy

A=Zmod(2)

def SuiteRS2D(n,M):
    R=matrix(A,2*n)
    for i in range(n):
        for j in range(n):
            for k in range(2):
                for l in range(2):

R[2*i+k,2*j+l]=A(R[i,j]+M[2*ZZ(A(i))+ZZ(A(j)),2*k+l])
    return R

def TableauCorrelation(S,n,q,r):
    T=matrix(RR,2)
    for i in range(n):
        for j in range(n):
            T[S[i,j],S[i+q,j+r]]=T[S[i,j],S[i+q,j+r]]+1
    return T/(n^2)
```

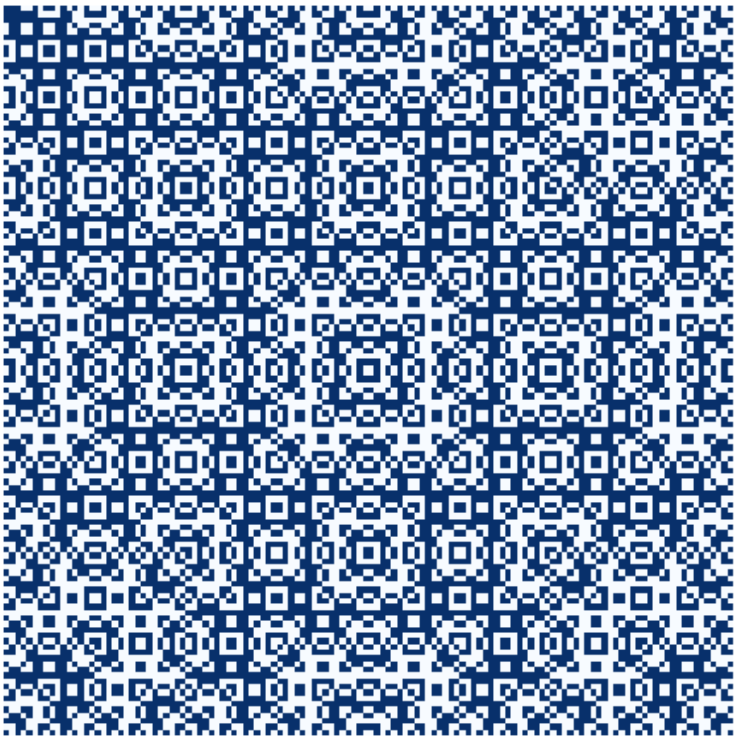
```
M=matrix([[0,1,1,1],[1,0,1,1],[1,1,0,1],[1,1,1,0]])
S=SuiteRS2D(2^9,M)

for i in range(4):
    for j in range(i+1):
        print (i,j)
        print TableauCorrelation(S,2^10-3,i,j)
matrix_plot(S, frame=False, cmap='Blues')
```

```
(0, 0)
[0.498528933531970 0.000000000000000]
[0.000000000000000 0.501471066468030]
(1, 0)
[0.249140239111854 0.249388694420116]
[0.249388694420116 0.252082372047914]
(1, 1)
[0.247580438605158 0.250948494926811]
[0.250947535639907 0.250523530828124]
(2, 0)
[0.248529173353696 0.249999760178274]
[0.250001678752083 0.251469387715947]
(2, 1)
[0.248971404616664 0.249557528915306]
[0.249558488202210 0.251912578265820]
(2, 2)
[0.248531091927505 0.249997841604465]
[0.250000719465178 0.251470347002852]
```

```
(3, 0)
[0.249386775846307 0.249142157685663]
[0.249148872693994 0.252322193774036]
(3, 1)
[0.248112842837149 0.250416090694821]
[0.250420887129344 0.251050179338687]
(3, 2)
[0.248090779238345 0.250438154293624]
[0.250443910015051 0.251027156452979]
(3, 3)
[0.248552196239403 0.249976737292566]
[0.249984411587802 0.251486654880228]
```



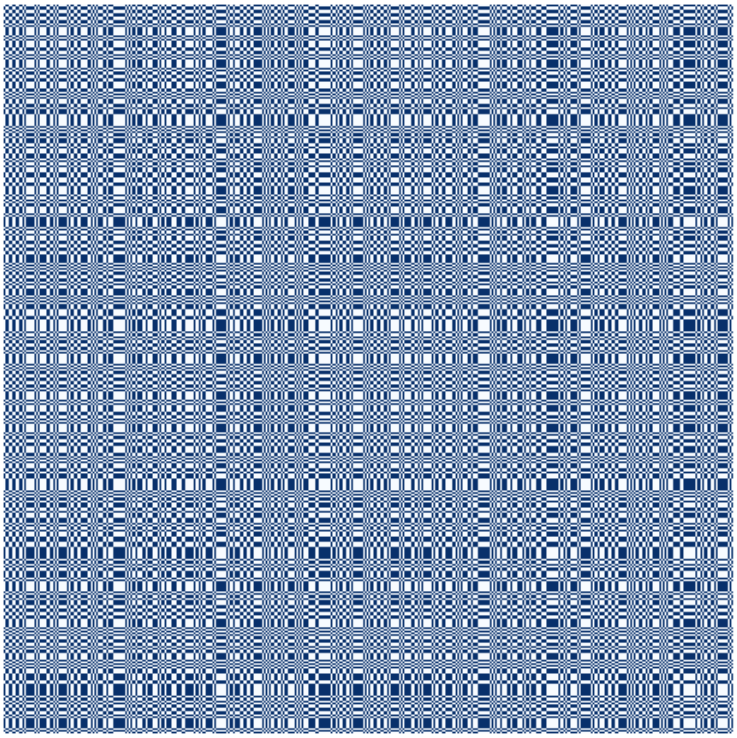
```
M=matrix([[0,1,1,1],[1,0,1,1],[1,1,0,1],[1,1,1,0]])
S=SuiteRS2D(2^6,M)

matrix_plot(S, frame=False, cmap='Blues')
```



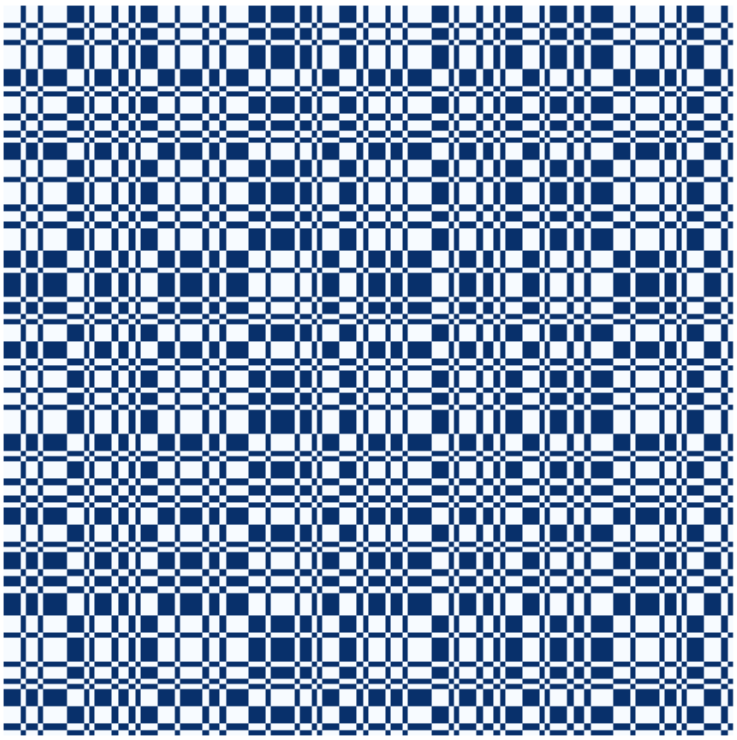
```
M=matrix([[0,0,0,0],[0,1,0,1],[0,0,1,1],[0,1,1,0]])
S=SuiteRS2D(2^9,M)

for i in range(4):
    for j in range(i+1):
        print (i,j)
        print TableauCorrelation(S,2^10-3,i,j)
matrix_plot(S, frame=False, cmap='Blues')
```

```
(0, 0)
[0.500522331719493 0.000000000000000]
[0.000000000000000 0.499477668280507]
(1, 0)
[0.251241077432680 0.249281254286813]
[0.249249597818965 0.250228070461542]
(1, 1)
[0.250493792934085 0.250028538785408]
[0.249967144423521 0.249510523856986]
(2, 0)
[0.250261645503199 0.250260686216294]
[0.250229029748446 0.249248638532061]
(2, 1)
[0.250490915073371 0.250031416646122]
[0.249970022284235 0.249507645996272]
(2, 2)
[0.250491874360276 0.250030457359217]
[0.249969062997330 0.249508605283177]
```

```
(3, 0)
[0.250735533234015 0.249786798485478]
[0.249723485549782 0.249754182730725]
(3, 1)
[0.250477485056708 0.250044846662785]
[0.249953714406859 0.249523953873648]
(3, 2)
[0.250476525769804 0.250045805949689]
[0.249954673693763 0.249522994586744]
(3, 3)
[0.250463095753141 0.250059235966352]
[0.249940284390196 0.249537383890311]
```



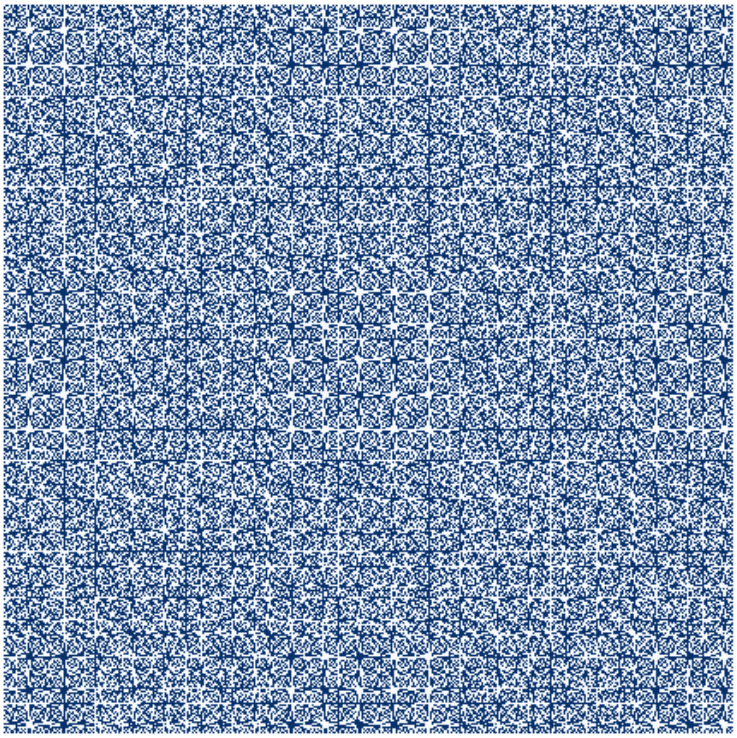
```
M=matrix([[0,0,0,0],[0,1,0,1],[0,0,1,1],[0,1,1,0]])
S=SuiteRS2D(2^6,M)
matrix_plot(S, frame=False, cmap='Blues')
```



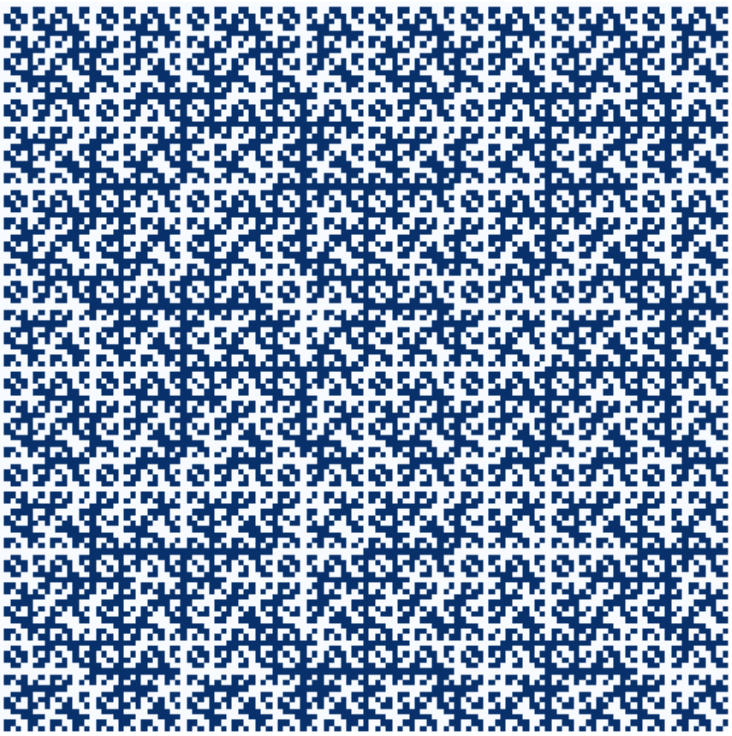
```
M=matrix([[0,0,0,0],[0,0,1,1],[0,1,0,1],[0,1,1,0]])
S=SuiteRS2D(2^9,M)

for i in range(4):
    for j in range(i+1):
        print (i,j)
        print TableauCorrelation(S,2^10-3,i,j)
matrix_plot(S, frame=False, cmap='Blues')
```

```
(0, 0)
[0.500493553112358 0.000000000000000]
[0.000000000000000 0.499506446887642]
(1, 0)
[0.250370044923406 0.250123508188953]
[0.249632353293855 0.249874093593786]
(1, 1)
[0.250002638038987 0.250490915073371]
[0.249508605283177 0.249997841604465]
(2, 0)
[0.250246296912727 0.250247256199631]
[0.249755142017630 0.249751304870012]
(2, 1)
[0.249999760178274 0.250493792934085]
[0.249510523856986 0.249995923030656]
(2, 2)
[0.250002638038987 0.250490915073371]
[0.249508605283177 0.249997841604465]
```

```
(3, 0)
[0.250610825936432 0.249882727175926]
[0.249390612993925 0.250115833893717]
(3, 1)
[0.250003597325892 0.250489955786467]
[0.249506686709368 0.249999760178274]
(3, 2)
[0.250001678752083 0.250491874360276]
[0.249509564570081 0.249996882317560]
(3, 3)
[0.250004556612796 0.250488996499562]
[0.249506686709368 0.249999760178274]
```



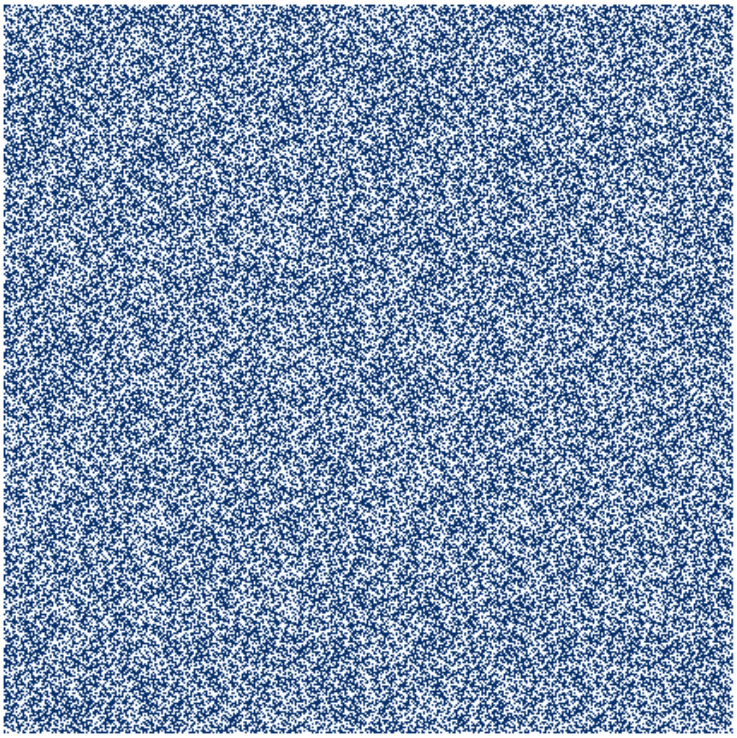
```
M=matrix([[0,0,0,0],[0,0,1,1],[0,1,0,1],[0,1,1,0]])
S=SuiteRS2D(2^6,M)
matrix_plot(S, frame=False, cmap='Blues')
```



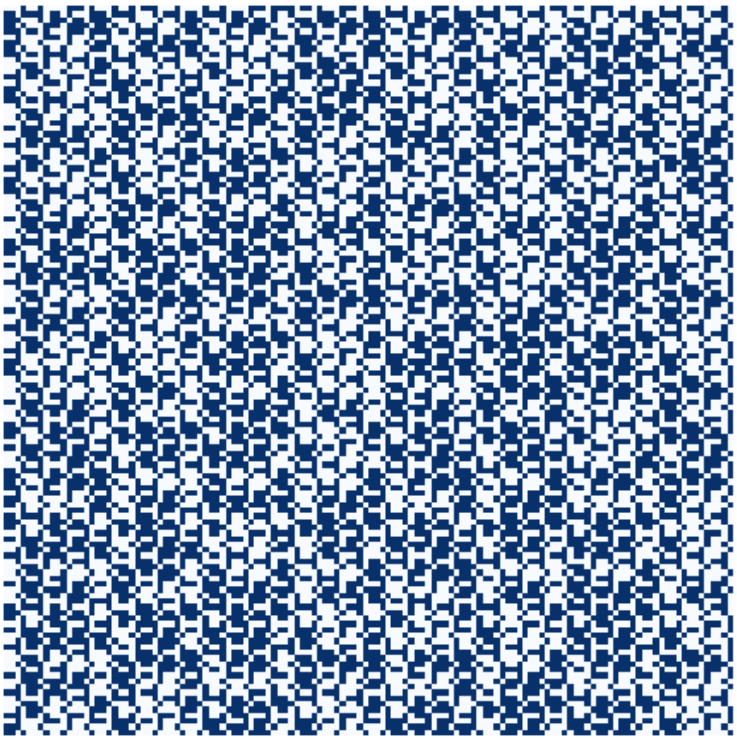
```
M=matrix([[0,0,1,1],[0,1,0,1],[0,0,0,0],[0,1,1,0]])
S=SuiteRS2D(2^9,M)

for i in range(4):
    for j in range(i+1):
        print (i,j)
        print TableauCorrelation(S,2^10-3,i,j)
matrix_plot(S, frame=False, cmap='Blues')
```

```
(0, 0)
[0.500492593825454 0.000000000000000]
[0.000000000000000 0.499507406174546]
(1, 0)
[0.250491874360276 0.250000719465178]
[0.249999760178274 0.249507645996272]
(1, 1)
[0.250445828588860 0.250046765236594]
[0.250075543843728 0.249431862330818]
(2, 0)
[0.250492833647180 0.249999760178274]
[0.249998800891369 0.249508605283177]
(2, 1)
[0.250446787875765 0.250045805949689]
[0.250074584556824 0.249432821617722]
(2, 2)
[0.250520652967410 0.249971940858044]
[0.250029498072313 0.249477908102233]
```

```
(3, 0)
[0.250491874360276 0.250000719465178]
[0.249998800891369 0.249508605283177]
(3, 1)
[0.250507222950747 0.249985370874707]
[0.250014149481841 0.249493256692705]
(3, 2)
[0.250520652967410 0.249971940858044]
[0.250029498072313 0.249477908102233]
(3, 3)
[0.250507222950747 0.249985370874707]
[0.250014149481841 0.249493256692705]
```



```
M=matrix([[0,0,1,1],[0,1,0,1],[0,0,0,0],[0,1,1,0]])
S=SuiteRS2D(2^6,M)
matrix_plot(S, frame=False, cmap='Blues')
```



Bibliographie

[1] J.-P. Allouche, *On a Golay–Shapiro–like sequence*, Unif. Distrib. Theory **11** (2016), 205–210.

[2] J.-P. Allouche and M. Bousquet-Mélou, *Facteurs des suites de Rudin–Shapiro généralisées*, Bull. Belg. Math. Soc. Simon Stevin **1** (1994), 145–164.

[3] J.-P. Allouche and M. Mendès France, *Automata and automatic sequences*, Beyond quasicrystals (Berlin, Heidelberg), Springer, 1995, pp. 293–367.

[4] J.-P. Allouche and P. Liardet, *Generalized Rudin–Shapiro sequences*, Acta Arith. **60** (1991), 1–27.

[5] J.-P. Allouche and J. Shallit, *The Ubiquitous Prouhet-Thue-Morse Sequence*, Sequences and their Applications (London) (C. Ding, T. Helleseth, and H. Niederreiter, eds.), Discrete Mathematics and Theoretical Computer Science, Springer, 1999, pp. 1–16.

[6] ———, *Automatic Sequences : Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.

[7] S. R. Blackburn, *Non-Overlapping Codes*, IEEE Trans. Inform. Theory **61** (2015), 4890–4894.

[8] J. Brillhart and L. Carlitz, *Note on the Shapiro polynomials*, Proc. Amer. Math. Soc. **25** (1970), 114–118.

[9] E. Cateland, *Digital sequences and k-regular sequences*, Thèses, Université Sciences et Technologies - Bordeaux I, June 1992.

[10] Y. M. Chee, H. M. Kiah, P. Purkayastha, and C. Wang, *Cross-Bifix-Free Codes Within a Constant Factor of Optimality*, IEEE Trans. Inform. Theory **59** (2013), 4668–4674.

[11] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, *Suites algébriques, automates et substitutions*, Bul. Soc. Math. France **79** (1980), 401–419.

[12] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192.

[13] M. Delacourt, V. Poupet, M. Sablik, and G. Theyssier, *Directional Dynamics along Arbitrary Curves in Cellular Automata*, Theoret. Comput. Sci. **412** (2011), 3800–3821.

[14] M. Drmota, P. J. Grabner, and P. Liardet, *Block additive functions on the Gaussian integers*, Acta Arith. **135** (2008), no. 4, 299–332. MR 2465714

[15] P. C. Fischer, *Generation of Primes by a One-Dimensional Real-Time Iterative Array*, J. Assoc. Comput. Mach. **12** (1965), 388–394.

[16] H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra **7** (1967), 271–277.

[17] G. Ge, *On* $(g, 4; 1)$*-difference matrices*, Discrete Math. **301** (2005), 164–174.

[18] E. N. Gilbert, *Synchronization of Binary Messages*, IRE Trans. IT **6** (1960), 470–477.

[19] M. J. E. Golay, *Statistic multislit spectrometry and its application to the panoramic display of infrared spectra*, J. Optical Soc. America **41** (1951), 468–472.

[20] E. Grant, J. Shallit, and T. Stoll, *Bounds for the discrete correlation of infinite sequences on k symbols and generalized Rudin–Shapiro sequences*, Acta Arith. **140** (2009), 345–368.

[21] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays*, Springer, New York, NY, 1999.

[22] G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375.

[23] I. Korec, *Real-Time Generation of Primes by a One-Dimensional Cellular Automaton with 11 States*, Mathematical Foundations of Computer Science 1997, vol. 1295, Springer, Berlin, Heidelberg, 1997, pp. 358–367.

[24] P. H. J. Lampio, *Classification of difference matrices and complex Hadamard matrices*, Ph.D. thesis, Aalto University, 2015.

[25] P. H. J. Lampio and P. R. J. Östergård, *Classification of difference matrices over cyclic groups*, J. Statist. Plann. Inference **141** (2011), 1194–1207.

[26] V. I. Levenshtein, *The maximal number of words in codes without overlap*, Problemy Peredachi Informatsii **6** (1970), 88–90.

[27] B. Litow and Ph. Dumas, *Additive Cellular Automata and Algebraic Series*, Theoret. Comput. Sci. **119** (1993), 345–354.

[28] I. Marcovici, T. Stoll, and P.-A. Tahay, *Construction of Some Nonautomatic Sequences by Cellular Automata*, Lecture Notes in Comput. Sci. **10875** (2018), 113–126.

[29] ———, *Discrete correlations of order 2 of generalised Rudin-Shapiro sequences : a combinatorial approach*, arXiv :2006.13162 [cs, math] (2020).

[30] C. Mauduit and J. Rivat, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc. **17** (2015), 2595–2642.

[31] ———, *Rudin–Shapiro sequences along squares*, Trans. Amer. Math. Soc. **370** (2018), 7899–7921.

[32] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I : Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.

[33] ———, *On finite pseudorandom binary sequences*, J. Number Theory **73** (1998), 256–276.

[34] J. Mazoyer and V. Terrier, *Signals in One-Dimensional Cellular Automata*, Theoret. Comput. Sci. **217** (1999), 53–80.

[35] M. Minsky and S. Papert, *Unrecognizable Sets of Numbers*, J. Assoc. Comput. Mach. **13** (1966), 281–286.

[36] A. M. Montgomery, *Asymptotic Enumeration of Difference Matrices over Cyclic Groups*, Combin. Probab. Comput. **27** (2018), 84–109.

[37] C. Müllner, *The Rudin-Shapiro sequence and similar sequences are normal along squares*, Canad. J. Math. **70** (2018), 1096–1129.

[38] M. Queffélec, *Une nouvelle propriété des suites de Rudin–Shapiro*, Ann. Inst. Fourier (Grenoble) **37** (1987), 115–138.

[39] P. Rendell, *Turing Machine Universality of the Game of Life*, Emergence, Complexity and Computation, Springer International Publishing, 2016.

[40] D. Rider, *Transformations of Fourier coefficients*, Pacific J. Math. **19** (1966), 347–355.

[41] E. Rowland and R. Yassawi, *A Characterization of p-Automatic Sequences as Columns of Linear Cellular Automata*, Adv. in Appl. Math. **63** (2015), 68–89.

[42] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959), 855–859.

[43] H. S. Shapiro, *Extremal problems for polynomials and power series*, Ph.D. thesis, MIT, 1951.

[44] P.-A. Tahay, *Discrete correlation of order 2 of generalized Rudin–Shapiro sequences on alphabets of arbitrary size*, Unif. Distrib. Theory **15** (2020), 1–26.

[45] J. von Neumann, *The theory of self reproducing automata*, University of Illinois Press, Cambridge, 1966.

[46] S. Wolfram, *A New Kind of Science*, Wolfram Media, Inc., Champaign, IL, 2002.