INFORMATIQUE THÉORIQUE ET APPLICATIONS

JEAN MOULIN OLLAGNIER

Sur quelques classes d'applications de N^2 dans les ensembles finis

Informatique théorique et applications, tome 23, n° 4 (1989), p. 461-492

<http://www.numdam.org/item?id=ITA_1989__23_4_461_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 23, n° 4, 1989, p. 461 à 492)

SUR QUELQUES CLASSES D'APPLICATIONS DE N^2 DANS LES ENSEMBLES FINIS (*)

par Jean MOULIN OLLAGNIER (1)

Communiqué par J.-E. PIN

Résumé. – *Cet article poursuit l'étude des treillis d'automates introduits par Culik, Gruska, et Salomaa en résolvant une question qui se posait naturellement à la suite de leurs travaux : les indicatrices des parties rationnelles de N^2 sont à la fois des B-applications sous-markoviennes et des B-applications sous-modulaires pour tous les modules carrés (p, p), où p est un entier positif.*

Abstract. – *We give in this paper a contribution to the study of some classes of networks introduced by Culik, Gruska, and Salomaa by solving a natural question about these objects. The characteristic functions of rational subsets of N^2 are shown to be submarkovian B-mappings and also sub-modular B-mappings for every square modulus (p, p), where p is a positive integer.*

INTRODUCTION

La puissance de calcul des treillis d'automates, introduits par Culik, Gruska, et Salomaa [6] dépend de la manière dont sont répartis les divers types de processeurs dans le réseau N^2.

Le cas le plus simple est celui où tous les processeurs sont identiques. Pour obtenir des résultats plus forts, il faut envisager des réseaux d'automates non-homogènes, mais cependant faciles à décrire.

De manière formelle, la situation est la suivante : chaque site du réseau géométrique N^2 se trouve dans un certain état et le nombre d'états possibles est fini.

(*) Reçu juin 1987, version finale en février 1988.
(1) Département de Mathématiques et Informatique, Université Paris-Nord, avenue J.-B. Clément, 93430 Villetaneuse et Laboratoire Informatique Théorique et Programmation, Université Pierre et Marie Curie, 4, place Jussieu, 75252 Paris Cedex 05.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754 89/04 461 32/$ 5.20/

Le point important est la régularité de la distribution des états aux divers sites de N^2; quelles règles de production faut-il se donner pour pouvoir déduire l'état d'un site de l'état déjà connu de certains autres?

Culik, Gruska, et Salomaa [6] ont introduit ce qu'ils appellent « regular trellises »; ils ont montré que les réseaux reconnaissables appartiennent à cette classe que Korec [11] a d'autre part étudiée en détails.

Récemment, Černy et Gruska [2] ont défini sous le nom de « modular trellises » un nouveau type de réseaux d'automates. Ils ont montré [3] que les deux classes de réseaux n'étaient pas comparables pour l'inclusion.

Les sous-ensembles reconnaissables de N^2 appartiennent aussi à la classe des « modular trellises ».

Il existe une classe strictement plus grande de parties de N^2 (ou d'applications de N^2 dans le semi-anneau de Boole B) que l'on peut utiliser pour construire des réseaux d'automates à deux types de processeurs : les ensembles rationnels.

Une question se pose alors naturellement : les indicatrices des parties rationnelles de N^2 appartiennent-elles à l'une des deux classes de B-applications précédemment citées?

Nous résolvons le problème dans les deux cas.

1. THÉORÈME : *Les indicatrices des parties rationnelles de N^2 sont des B-applications sous-markoviennes (regular trellises).*

2. THÉORÈME : *Pour tous les modules carrés (p, p), les indicatrices des parties rationnelles de N^2 sont des B-applications (p, p)-sous-modulaires [(p, p)-modular trellises].*

Pour montrer que les indicatrices des parties rationnelles sont des B-applications sous-markoviennes, nous introduisons une notion nouvelle, celle d'application markovienne à portée finie; les applications obtenues en composant les applications markoviennes à portée finie avec une fonction terminale sont alors sous-markoviennes dans le premier sens de cette expression. Nous obtenons ainsi une façon très pratique de parler de la dépendance des positions des points dans un ensemble linéaire; c'est un outil décisif pour construire la preuve de ce que les indicatrices des parties rationnelles de N^2 sont des B-applications markoviennes.

Pour prouver que les indicatrices des parties rationnelles sont sous-modulaires dans les bases carrées, nous établissons le résultat suivant.

PROPOSITION : *Le signe d'une forme affine à coefficients dans Z, que l'on définit comme une application de N^2 dans l'ensemble fini $\{-, 0, +\}$, est une*

fonction reconnaissable par un automate lisant de droite à gauche la représentation des éléments de N^2 dans le système de numération à base carrée (p, p).

Nous utilisons ensuite un théorème de structure de nature géométrique pour caractériser les parties rationnelles de N^n :

THÉORÈME : *Les parties rationnelles de N^n sont les réunions finies d'intersections d'une partie reconnaissable de Z^n avec une intersection finie de demi-espaces; un demi-espace est la partie de N^n où une forme affine donnée à coefficients dans Z prend une valeur positive ou nulle.*

Plusieurs lemmes préparant ce théorème se trouvent dans les travaux sur la stabilité de la classe des parties rationnelles de N^n sous l'action des opérations booléennes [8, 9, 10].

Pour ce qui est du théorème de caractérisation ci-dessus, notre remarque originale est la suivante.

PROPOSITION : *Un ensemble linéaire libre de N^n est l'intersection d'une partie reconnaissable de Z^n avec une intersection finie de demi-espaces.*

Ceci achève la démonstration de notre deuxième théorème principal.

Pour compléter la preuve du théorème de caractérisation géométrique, il faut montrer qu'une intersection finie de demi-espaces est une partie rationnelle, résultat qui provient de l'énoncé combinatoire suivant, qui est bien connu :

Un polyèdre borné de Q^n est l'enveloppe convexe de ses points extrémaux, qui sont en nombre fini.

1. APPLICATIONS RECONNAISSABLES

1.1. Reconnaissabilité

Rappelons qu'une partie reconnaissable du monoïde N^2 est l'image réciproque d'une partie P d'un monoïde fini M par un morphisme de N^2 dans ce monoïde. Ainsi, l'indicatrice d'une partie reconnaissable est obtenue par composition d'un morphisme μ de N^2 dans M et d'une application s de M dans $\{ 0, 1 \}$. C'est donc une généralisation minime mais naturelle que de s'intéresser aux applications de N^2 dans les ensembles finis.

Nous utiliserons le nom de F-application lorsque nous souhaiterons insister sur l'ensemble fini F d'arrivée; en particulier, les B-applications sont à valeurs dans le semi-anneau de Boole.

DÉFINITION 1 : *Une application f de N^2 dans un ensemble fini F, ou F-application, est dite reconnaissable si elle peut être factorisée à travers un morphisme μ de N^2 dans un monoïde fini M : $f=\mu \circ s$.*

1.2. Translations d'une F-application

Étant donnée une F-application f définie sur N^2 et un couple (m, n) d'entiers naturels, on appelle translatée de f par le vecteur (m, n) la F-application $f.T^{m,n}$ définie par :

$$\forall (x, y) \in N^2, \quad (x, y).(f.T^{m,n}) = (x+m, y+n).f.$$

PROPOSITION 1 : *Une F-application f est reconnaissable si et seulement si l'ensemble de ses translatées est fini.*

Démonstration : Supposons f reconnaissable; il existe donc un monoïde M, un morphisme μ de N^2 dans M et une application s de M dans F tels que $f=\mu \circ s$.
Alors, pour tout vecteur (m, n),

$$(x, y)(f.T^{m,n}) = (x+m, y+n).(\mu \circ s) = ((x, y).\mu + (m, n).\mu).s.$$

Puisque M est fini, l'image de N^2 par μ l'est aussi et l'application reconnaissable f n'a qu'un nombre fini de translatées.

Réciproquement, soit E l'ensemble des translatées de f; le monoïde N^2 agit sur E et il existe donc un morphisme μ de N^2 dans le monoïde des applications de E dans E. Appelons spécialisation en f et en $(0, 0)$ l'application θ de E^E dans F définie par

$$\varphi.\theta = (0, 0).(f.\varphi).$$

L'application f est alors reconnaissable puisqu'obtenue en composant le morphisme μ avec la spécialisation θ : $f=\mu \circ \theta$.

1.3. Formes extraites

Il est possible de donner une version locale de la proposition précédente, version analogue à ce qui se fait en dimension 1, en introduisant les formes de taille n extraites de la F-application f.

DÉFINITION 2 : *Étant donnée une F-application f, on appelle formes extraites de taille n les traces de f sur les carrés de côté n, c'est-à-dire les applications du carré $[0, n-1] \times [0, n-1]$ dans F obtenues en composant avec f les injections*

$i^n_{p,q}$ *définies par :*

$$(x, y) . i^n_{p,q} = (x+p, y+q).$$

Le nombre des formes de taille n est fini puisqu'il est borné par $| F |^{n^2}$; notons-le $\varphi(n)$. Une application reconnaissable est caractérisée par certaines propriétés de la fonction φ correspondante.

PROPOSITION 2 : *Soit φ la fonction de N dans N qui associe à l'entier n le nombre $\varphi(n)$ de formes de taille n extraites d'une F-application f donnée. L'application f est reconnaissable si et seulement si la fonction φ est bornée ; de plus, ce résultat est acquis dès qu'il existe un entier n tel que $\varphi(n+1) = \varphi(n)$.*

Démonstration : Une forme de taille n extraite de f est la restriction au carré d'une application translatée de f ; si f est reconnaissable, le nombre de ses translatées est fini et ce nombre borne tous les $\varphi(n)$.

Réciproquement, la fonction φ est croissante car la restriction fournit une application surjective de l'ensemble des formes de taille $n+1$ sur l'ensemble des formes de taille n. Si $\varphi(n+1) = \varphi(n)$, cette surjection est bijective et les formes de taille n déterminent celles de taille $n+1$; par suite, la translatée $f . T^{p,q}$ de f est entièrement déterminée par la forme extraite de taille n, $i^n_{p,q} . f$. D'où le résultat.

Remarque 1 *: Cet argument de stationnarité est utilisé en dimension* 1 *pour montrer qu'une suite donnée est ultimement périodique : il existe des entiers n tels que le nombre de formes extraites de longueur n soit inférieur ou égal à n.*

On a alors pour le plus petit de ces nombres : $\varphi(n) = \varphi(n+1)$.

2. APPLICATIONS MARKOVIENNES

2.1. Définitions

On dit qu'une F-application f est markovienne si la valeur qu'elle prend au point (m, n) ne dépend que des valeurs aux points qui en sont les antécédents immédiats, $(m-1, n)$ et $(m, n-1)$.

On appelle sous-markovienne une F-application f obtenue par composition d'une F_0-application markovienne et d'une application s de F_0 dans F : $f = f_0 \circ s$.

Les dénominations de l'article de Černy et Gruska sont respectivement « strictly regular trellises » et « regular trellises ».

Il faut bien entendu réserver un sort particulier aux points des bords qui n'ont qu'un seul antécédent dans N^2; on peut unifier les divers cas de figure en ajoutant une lettre n'apparaissant pas dans l'alphabet, notée par exemple « Ω »; une application markovienne est alors la restriction à N^2 d'une application définie sur Z^2, markovienne en tous les points sauf l'origine, et prenant la valeur « Ω » sur $Z^2 \setminus N^2$. Il est clair que les restrictions aux deux bords d'une application markovienne ou sous-markovienne sont des suites markoviennes ou sous-markoviennes; elles sont alors ultimement périodiques.

2.2. Premières propriétés

Donnons sans démonstration quelques propriétés élémentaires des applications markoviennes et sous-markoviennes.

La classe des applications markoviennes (resp. sous-markoviennes) est fermée par produit direct à l'arrivée; cela signifie que si f_1 est une F_1-application markovienne (resp. sous-markovienne) et f_2 une F_2-application markovienne (resp. sous-markovienne), la F-application produit $f=f_1 \times f_2$, à valeurs dans l'ensemble produit $F=F_1 \times F_2$, définie par :

$$\forall (x,y) \in N^2, \quad (x,y).\, f=((x,y).\, f_1, (x,y).\, f_2)$$

est encore markovienne (resp. sous-markovienne).

En utilisant somme, produit et complément comme fonctions terminales, on vérifie que la classe des B-applications sous-markoviennes, où B est le demi-anneau de Boole, est stable par les opérations booléennes.

L'exemple suivant montre qu'il est nécessaire de considérer des applications sous-markoviennes pour assurer la stabilité booléenne de la classe.

Exemple 1: *Considérons les deux B-applications f_1 et f_2 où $B=\{0,1\}$ est le demi-anneau de Boole, nulles à l'origine et dont les prolongements sont définis sur $Z^2 \setminus \{(0,0)\}$ par les transitions suivantes, où la valeur en haut à droite ne dépend que de ses deux antécédents.*

Transitions communes à f_1 et f_2 :

Ω	Ω
.	Ω

0	0
.	Ω

Ω	1
.	0

1	1
.	Ω

Ω	1
.	1

0	1
.	0

1	0
.	1

Les applications f_1 et f_2 se distinguent par les transitions particulières qui sont, pour f_1

0	0
.	1

et

1	0
.	0

et pour f_2

0	1
.	1

et

1	1
.	0

Les traces de f_1 et de f_2 sur $[0, 6]^2$ sont représentées sur la figure suivante où l'on voit que les configurations aux points (2, 1) et (3, 3) de l'application f, produit booléen de f_1 et f_2, sont respectivement

0	1
.	0

et

0	0
.	0

ce qui montre que l'application f n'est pas markovienne.

Voici les traces des deux applications :

1	0	0	1	0	1	0	
1	0	1	0	1	0	1	
1	0	0	1	0	1	0	
1	0	*1*	*0*	1	0	1	
1	0	0	*1*	0	1	0	
1	*0*	*1*	0	1	0	1	
0	0	*0*	0	0	0	0	

l'application f_1

1	0	1	0	1	0	1	
1	1	0	1	0	1	0	
1	0	1	0	1	0	1	
1	1	*0*	*1*	0	1	0	
1	0	1	*0*	1	0	1	
1	*1*	*1*	1	1	1	1	
0	0	*0*	0	0	0	0	

l'application f_2

De même, en faisant le produit « au départ », on peut construire une application markovienne (resp. sous-markovienne) sur N^2 à valeurs dans $F \times G$ comme le produit tensoriel $u \otimes v$ d'une suite markovienne (resp. sous-markovienne) u définie sur N à valeurs dans l'ensemble fini F par la suite markovienne (resp. sous-markovienne) v à valeurs dans l'ensemble fini G :

$$\forall (x, y) \in N^2, \quad (x, y).(u \otimes v) = (x.u, y.v).$$

En particulier, la fonction indicatrice du produit de deux parties reconnaissables de N est une B-application sous-markovienne. Les parties reconnaissables de N^2 sont les réunions finies de tels produits; leurs indicatrices sont donc sous-markoviennes.

2.3. Applications markoviennes de portée k

Le monoïde N^2 n'est pas libre et il existe des parties rationnelles de N^2 qui ne sont pas reconnaissables, la diagonale par exemple. Son indicatrice δ peut être définie comme la trace sur N^2 d'une application de Z^2 dans $B \cup \{\Omega\}$, dont la valeur à l'origine est $(0,0).\delta = 1$, qui prend la valeur Ω sur $Z^2 \setminus N^2$, et qui satisfait en dehors de l'origine la relation

$$(m, n).\delta = (m-1, n-1).\delta.$$

Ceci ne correspond pas à la définition d'une application markovienne car la valeur en un point (m, n) de N^2 dépend des valeurs aux points $(m-x, n-y)$ où (x, y) appartient au triangle :

$$\{0 \leqq x, 0 \leqq y, 1 \leqq x+y \leqq 2\}.$$

Néanmoins, l'indicatrice de la diagonale est une B-application sous-markovienne; par exemple, on peut l'obtenir à partir d'une application markovienne f à valeurs dans $\{0, 1, b\}$ en envoyant b sur 0. L'application f est définie par sa valeur à l'origine, 1, par les transitions sur les deux bords,

$$1 \to b \to 0 \to 0,$$

et par les neuf transitions suivantes :

0	0	0	0	0	b	b	0	b	1	b	1	1	b	1	1	1	1
.	0	.	b	.	1	.	0	.	b	.	1	.	0	.	b	.	1

La définition des trois transitions

b	1	1	1	1	1
.	b	.	b	.	1

est assez formelle puisque l'on ne rencontre jamais les configurations correspondantes :

b	.	1	.	1	.
.	b	.	b	.	1

Introduisons maintenant la notion d'application markovienne de portée k, une application markovienne sans autre précision étant alors de portée 1.

DÉFINITION 3 : *On dit qu'une F-application f est markovienne de portée k, ou plus simplement k-markovienne, si c'est la restriction à N^2 d'une application $\bar{f}$ définie sur Z^2, à valeurs dans l'ensemble $\bar{F} = F \cup \{\Omega\}$, telle que, en tout point (m, n) sauf l'origine, la valeur (m, n). $\bar{f}$ ne dépende que des valeurs $(m-x, n-y)$. $\bar{f}$, où (x, y) appartient au triangle :*

$$\{0 \leqq x, 0 \leqq y, 1 \leqq x+y \leqq k\}.$$

Cette nouvelle notion est purement opératoire comme le montre la proposition suivante; son introduction facilite la démonstration du fait que les indicatrices des parties rationnelles de N^2 sont des B-applications sous-markoviennes.

PROPOSITION 3 : *Une application k-markovienne est sous-markovienne.*

Démonstration : Soit T le triangle suivant :

$$T = \{ 0 \leqq x, 0 \leqq y, 0 \leqq x+y \leqq k \}$$

et soit f une F-application markovienne de portée k.

Considérons que f est à valeurs dans $\bar{F} = F \cup \{\Omega\}$ où $\Omega \notin F$, complétons f à Z^2 tout entier en lui donnant la valeur « Ω » en dehors de N^2.

Appelons alors $\bar{f}$ l'application sur Z^2 à valeurs dans $\bar{F}^T$ défini par :

$$\forall (m,n) \in Z^2, \quad (m,n).\bar{f} = \{ (x,y) \to (m-x, n-y).f \}.$$

En tout point de Z^2 où f est markovien de portée k, $\bar{f}$ est markovien de portée 1, sa valeur sur $Z^2 \setminus N^2$ est la fonction constante « Ω ».

La restriction à N^2 de $\bar{f}$ est donc une application markovienne (de portée 1) et la F-application de départ f est obtenue en composant cette application markovienne avec l'application de spécialisation de $\bar{F}^T$ dans $\bar{F}$ qui associe à un élément de $\bar{F}^T$ sa valeur en $(0,0)$. D'où le résultat.

Nous sommes maintenant en mesure de prouver le théorème suivant.

THÉORÈME 1 : *Les indicatrices des parties rationnelles de N^2 sont des B-applications sous-markoviennes.*

Démonstration : Les parties rationnelles de N^2 sont les réunions finies d'ensembles linéaires. La classe des B-applications sous-markoviennes est stable par les opérations booléennes; il suffit donc d'établir que l'indicatrice d'un ensemble linéaire est sous-markovienne.

Pour simplifier, nous procédons en deux temps en montrant d'une part que l'indicatrice de l'étoile d'une partie finie est markovienne d'une cartaine portée et d'autre part que la translatée d'une application sous-markovienne l'est aussi. C'est l'objet des deux lemmes qui suivent.

LEMME 1 : *Soit f une B-application sous-markovienne et (a, b) un élément de N^2. On note g l'application translatée de f par (a, b) définie par :*

$$\forall x \geqq a, \quad \forall y \geqq b, \quad (x, y).g = (x-a, y-b).f$$

et prenant la valeur 0 pour les autres valeurs du couple (x, y). Alors, l'application g est également sous-markovienne.

Démonstration : Par récurrence, il suffit d'établir le résultat pour la translation de vecteur $(0, 1)$ [ou de vecteur $(1, 0)$ par symétrie].

Soit $\bar{f}$ une application markovienne à travers lequel se factorise f et F l'ensemble d'arrivée de $\bar{f}$; ajoutons à F un élément de bordure b qui ne lui

appartienne pas et définissons l'application $\bar{g}$ par :

$$\forall x, \forall y>0,\ (x, y).\bar{g}=(x, y-1).\bar{f}$$
$$\forall x, (x, 0).\bar{g}=b.$$

L'application $\bar{g}$ est markovienne et g s'obtient en identifiant b et 0.

LEMME 2 : *Soit* $E=\{(a_1, b_1), \ldots, (a_l, b_l)\}$ *un ensemble fini d'éléments de* $N^2\setminus\{(0,0)\}$ *et soit* E^* *l'étoile de* E, *c'est-à-dire l'ensemble des sommes d'éléments de* E. *La fonction indicatrice de* E^* *est alors une B-application markovienne de portée* k, *où l'entier* k *est la borne supérieure des sommes* a_i+b_i *pour* i *entre* 1 *et* l.

Démonstration : Soit e la fonction indicatrice de E^*; c'est la trace sur N^2 d'une application sur Z^2 prenant la valeur 1 à l'origine, identiquement égale à « Ω » sur $Z^2\setminus N^2$, markovienne de portée k sauf à l'origine, et où la dépendance markovienne est la suivante

$$\forall (x, y)\in Z^2\setminus\{(0, 0)\},\ (x, y).e=\sup(s_1, s_2).$$

Les valeurs s_1 et s_2 sont ici définies par :

$$s_1=\sup(\{(x-a_i, y-b_i).e\},\ 1\leqq i\leqq l)$$
$$s_2=(\sup(\{(x-a, y-b).e\},\ 1\leqq a+b\leqq k)).z.$$

L'application z de l'ensemble $\{\Omega, 0, 1\}$ dans lui-même envoie Ω sur Ω, 0 et 1 sur 0, cet ensemble étant ordonné par $\Omega<0<1$.

La démonstration de ce lemme achève la preuve du théorème précédent.

Une question naturelle se pose après l'introduction de la portée finie : est-il encore nécessaire de perdre de l'information avec une application non injective ou bien toute application sous-markovienne ne serait-elle pas markovienne d'une portée suffisamment grande? L'exemble suivant montre que l'on ne peut pas se passer de cette projection.

Exemple 2*: Considérons d'abord le triangle de Pascal modulo* 3 :

$$(m, n).p_3=\frac{(m+n)!}{m!\,n!}\bmod 3.$$

C'est une application p_3 *à valeurs dans les entiers modulo* 3 *qui est markovienne (de portée* 1*) comme on peut le vérifier à l'aide de la relation de transition :*

$$m.n>0 \quad\Rightarrow\quad (m, n).p_3\equiv(m-1, n).p_3+(m, n-1).p_3 \pmod 3.$$

Projetons p_3 sur l'ensemble $\{0, 1\}$ en envoyant 0 sur 0, -1 et $+1$ sur 1; l'application p_3 ainsi obtenue est sous-markovienne et c'est l'indicatrice de l'ensemble des couples (m, n) de N^2 pour lesquels le coefficient binomial C_{m+n}^{n} n'est pas divisible par 3.

L'application $\bar{p}_3$ n'est pas markovienne de portée finie; en effet, pour tout entier k, tous les antécédents à une distance inférieure ou égale à 3^k des points $(3^k, 3^k)$ et $(3^k, 2.3^k)$ ayant les mêmes positions relatives ont les mêmes valeurs alors que $(3^k, 3^k).\bar{p}_3 = 1$ et $(3^k, 2.3^k).\bar{p}_3 = 0$.

On a plus précisément :

$$(m+n \geqq 3^k,\ m<3^k,\ n<3^k) \Rightarrow \frac{(m+n)!}{m!\,n!} \equiv 0 \pmod 3$$

$$(m+n \geqq 2.3^k,\ m<3^k,\ n<2.3^k) \Rightarrow \frac{(m+n)!}{m!\,n!} \equiv 0 \pmod 3$$

$$(m=3^k,\ n=2.3^k) \Rightarrow \frac{(m+n)!}{m!\,n!} \equiv 0 \pmod 3$$

$$(n=3^k,\ m<3^k) \Rightarrow \frac{(m+n)}{m!\,n!} \not\equiv 0 \pmod 3$$

$$(n=2.3^k,\ m<3^k) \Rightarrow \frac{(m+n)!}{m!\,n!} \not\equiv 0 \pmod 3.$$

On vérifie tous ces résultats en regardant si la somme suivante, où E désigne la fonction partie entière, est nulle :

$$\sum_{l \geqq 1} \left(E\left(\frac{m+n}{3^l}\right) - E\left(\frac{m}{3^l}\right) - E\left(\frac{n}{3^l}\right) \right).$$

Tous les termes de la somme sont positifs ou nuls et $(m+n)!/m!\,n!$ est divisible par 3 si et seulement si l'un de ces termes est nul. Dans tous les cas où il y a divisibilité, c'est le terme d'indice $l=k$ (ou d'indice $l=k+1$) qui est égal à 1. La non-divisibilité signifie qu'il n'y a pas de retenue dans l'addition en base 3 des nombres m et n; c'est ce qui se passe dans les cas indiqués.

L'exemple suivant montre qu'il existe des B-applications sous-markoviennes qui ne sont pas des indicatrices de parties rationnelles de N^2.

Exemple 3 : Considérons le triangle de Pascal modulo 2; cette application p_2 est markovienne. Ce n'est cependant pas l'indicatrice d'une partie rationnelle de N^2.

En effet, si la partie correspondante de N^2 était rationnelle, son intersection avec l'ensemble linéaire $(0,1)+N.(1,1)$ le serait aussi d'après le théorème de Ginsburg et Spanier [8, 9]. *La projection de cette intersection sur la première coordonnée serait alors une partie rationnelle de N et serait donc ultimement périodique.*

Cette projection A est exactement :

$$A=\left\{n\in N\,|\,\frac{(2n+1)!}{n!(n+1)!}\equiv 1 \bmod 2\right\}.$$

A l'aide de remarques semblables à celles de l'exemple précédent, on montre que n appartient à l'ensemble A si et seulement si il n'y a pas de retenue dans l'addition en base 2 des nombres n et $n+1$.

L'ensemble A est donc l'ensemble des nombres de la forme 2^n-1; il n'est pas ultimement périodique.

2.4. Suites définies par substitution

Černy et Gruska [3] ont énoncé la propriété suivante.

Pour toute suite infinie de lettres d'un alphabet E obtenue comme la limite de substitutions de lettres par des mots de longueur éventuellement non constante, il est possible de construire une application markovienne avec les propriétés suivantes.

L'ensemble d'arrivée de l'application contient l'alphabet E et il est muni d'une involution dont les éléments invariants sont ceux de E; la suite est la trace de l'application sur la diagonale de N^2 et, de plus, l'application est presque symétrique par rapport à la diagonale, en ce sens que la symétrique de l'application par rapport à la diagonale est obtenue en effectuant l'involution sur l'ensemble d'arrivée.

Ils ont donné une esquisse de preuve dans leur article [3]. Nous présentons dans cette section une démonstration complète de ce résultat, démonstration qui est malheureusement un peu technique; la justification de ces efforts est le fait que cette construction permet d'exhiber des applications markoviennes qui ne soient pas modulaires (*cf.* section suivante). Commençons par préciser quelques définitions.

DÉFINITION 4 : *Étant donné un ensemble fini E, une substitution σ sur l'alphabet E est un morphisme de monoïdes de E^* dans lui-même, morphisme qui est donc entièrement déterminé par les images $x.\sigma$ des lettres de E.*

On suppose qu'il existe une lettre a de E telle que le mot-image $a.\sigma$ *commence par a. Alors, pour tout entier n, le mot* $a.\sigma^n$ *est facteur gauche du mot* $a.\sigma^{n+1}$, *ce qui permet, par passage à la limite de définir une suite infinie u d'éléments de E.*

Remarquons que cette suite infinie n'est rien d'autre qu'un mot infini engendré par un DOL-langage [1].

Il est bien entendu que l'image $x.\sigma$ *d'une lettre de E n'est jamais le mot vide et que celle de a est au moins de longueur 2; ceci assure la croissance stricte de la suite des* $a.\sigma^n$ *et la définition de la suite infinie u.*

DÉFINITION 5 : *La suite infinie u définie à partir de la substitution* σ *et de la lettre a n'est que la partie visible d'un triplet* (m, p, u) *de fonctions sur N, défini par récurrence.*

La fonction m associe à l'entier n son ancêtre et la fonction p la place (qui commence à 0) de la lettre $n.u$ *dans le mot* $((n.m).u).\sigma$.

La description intuitive est la suivante. A la position repérée par l'entier n se trouve une lettre d'un mot qui est l'image par σ *d'une lettre se trouvant à une position repérée par l'ancêtre de n; de plus, cette lettre image a une certaine place dans le mot en question, qui définit la place de n.*

Ce triplet de fonctions est entièrement défini par sa valeur initiale

$$0.(m, p, u)=(0, 0, a)$$

et par la formule de récurrence :

$$n.p<|((n.m).u).\sigma|-1 \quad \Rightarrow \quad \{(n+1).m=n.m;\ (n+1).p=n.p+1\}$$

$$n.p=|((n.m).u).\sigma|-1 \quad \Rightarrow \quad \{(n+1).m=n.m+1;\ (n+1).p=0\}$$

$$(n+1).u=\text{la lettre de place } (n+1).p \text{ dans le mot } (((n+1).m).u).\sigma$$

Remarquons que cette dernière propriété est encore vraie pour $n=0$.

La définition par récurrence est possible car les conditions rappelées plus haut impliquent que, pour tout n différent de 0, l'ancêtre $n.m$ est strictement inférieur à n et que l'on fait donc appel à des valeurs déjà calculées. On cherche à construire une application markovienne sur N^2 à valeurs dans un ensemble fini F contenant E dont la suite u soit la trace sur la diagonale :

$$\forall n \geqq 0,\ (n, n).f=n.u.$$

On souhaite de plus que la symétrie par rapport à la diagonale corresponde à une involution : ce problème sera résolu dans un second temps.

DÉFINITION 6 : *L'ensemble F est la réunion disjointe de l'ensemble E, de l'ensemble E^2 des couples (x, y) de lettres de E, de l'ensemble fini des couples (x, k) de $E \times N$ tels que $0 \leqq k < |x.\sigma|$, d'un catalyseur noté « \$ »,* et du symbole *« − » destiné à être la valeur de l'application que nous voulons construire pour les points de N^2 situés sous la diagonale.*

Pour décrire plus facilement les transitions générales, introduisons trois fonctions sur *F*, définies sauf pour « \$ » et « − », l'élévateur *l*, le premier élément *g*, le second élément *d*.

DÉFINITION 7 : *La fonction partielle l, à valeurs dans F, est ainsi définie pour un élément α de F :*

si $\alpha \in E$ *alors* $\alpha.l = (\alpha, 0)$

si $\alpha = (x, y) \in E^2$ *alors* $\alpha.l = (x, 0)$

si $\alpha = (x, k) \in E \times N$ *et* $0 \leqq k < |x.\sigma| - 1$ *alors* $\alpha.l = (x, k+1)$

si $\alpha = (x, k) \in E \times N$ *et* $k = |x.\sigma| - 1$ *alors* $\alpha.l =$ « \$ ».

DÉFINITION 8 : *La fonction partielle g, à valeurs dans E, est ainsi définie pour un élément α de F :*

si $\alpha \in E$ *alors* $\alpha.g = \alpha$

si $\alpha = (x, y) \in E^2$ *alors* $\alpha.g = x$

si $\alpha = (x, k) \in E \times N$ *alors* $\alpha.g = x$.

DÉFINITION 9 : *La fonction partielle d, à valeurs dans E, est ainsi définie pour un élément α de F :*

si $\alpha \in E$ *alors* $\alpha.d =$ « − »

si $\alpha = (x, y) \in E^2$ *alors* $\alpha.d = y$

si $\alpha = (x, k) \in E \times N$ *alors* $\alpha.d$ *est la lettre de place k dans le mot* $x.\sigma$.

Passons maintenant à la définition de l'application *f*.

DÉFINITION 10 : *La F-application markovienne f est ainsi définie. Sa valeur initiale est a; sur l'axe des abscisses, la succession des symboles est la suivante :*

$$a \to - \to -$$

et sur celui des ordonnées, on a la suite ultimement périodique

$$a \to (a, 1) \to (a, 2) \to \ldots \to (a, |a.\sigma| - 1) \to \$ \to \$$$

Les transitions générales sont d'une part

\$	\$	\$	$\alpha.l$	α	$(\beta.g, \alpha.d)$	α	$\alpha.d$	—	—
.	\$	.	α	.	β	.	—	.	—

et d'autre part

α	?	—	?	—	?	\$	?
.	\$	.	\$	.	α	.	—

où α désigne un élément de F différent des deux symboles spéciaux; la valeur notée « ? » est arbitraire car les conditions de bord sur f interdisent en fait ces configurations.

En effet, on s'assure facilement en partant des bords et par récurrence sur la somme $m+n$ qu'à gauche ou au-dessus d'un « \$ », il ne peut y avoir qu'un « \$ », et qu'à droite ou en dessous d'un « — », il ne peut y avoir qu'un « — ». L'impossibilité de la dernière des quatre configurations citées résulte de ce que la case marquée d'un point ne pourrait être occupée que par une lettre simple pour que l'on puisse trouver un « — » à sa droite; mais le « \$ » au-dessus ne peut provenir que d'une élévation. L'élévation d'une lettre simple ne donnant jamais le signe « \$ », ces conclusions sont contradictoires.

La F-application f possède les propriétés suivantes, dont la démonstration se fait par récurrence sur $m+n$.

Les valeurs prises sur la diagonale de N^2 sont des lettres simples, ce qui permet de définir une suite u' à valeurs dans E.

Les valeurs prises au-dessus de la diagonale sont, soit des couples, soit le symbole « \$ ».

Au-dessous de la diagonale n'apparaît que le symbole « — ».

Il reste à établir la propriété annoncée : la trace de f sur la diagonale est la suite u.

PROPOSITION 4 : *Considérons le triplet (m', p', u') de fonctions sur N définies à partir de l'application f de la façon suivante.*

Tout d'abord, u' est la restriction à la diagonale de l'application f :

$$\forall n \in N, \quad n.u' = (n, n).f.$$

La ligne d'ordonnée n commence par un certain nombre de « $ »; la position de la première valeur différente de « $ » est (k, n) *où* $k \leqq n$ *et cette valeur est un couple* (x, t).

On pose alors : $n.m' = k$; $n.p' = t$.

Dans le cas particulier (qui ne se produit pas si la substitution vérifie les conditions raisonnables permettant la définition de la suite infinie u) de la lettre a, on poserait $n.p' = 0$.

Le triplet (m', p', u') *ainsi défini vérifie la même condition initiale et les mêmes hypothèses de récurrence que* (m, p, u).

Ces deux triplets de fonctions sur N coïncident donc; en particulier, la suite diagonale u' de f est la suite u définie par la substitution σ.

Démonstration : Le fait que la première valeur autre que « $ » soit un couple du type (x, k) provient de ce que ce couple résulte d'une élévation. De même, c'est de la définition de la fonction l avec ses divers cas de figure que résultent les relations de récurrence.

Pour passer maintenant à une version presque symétrique de l'application f, on définit un nouvel alphabet G en enlevant « − » de F, en notant $(\$, +)$, $(x, y, +)$ et $(x, k, +)$ les éléments de F qui ne sont pas dans E. On donne à ces éléments des symétriques notés $(\$, -)$, $(x, y, -)$ et $(x, k, -)$, les éléments de E étant leurs propres symétriques.

L'involution i consiste à échanger les signes « + » et « − » et la nouvelle application f' est défini à partir de la trace de f sur la diagonale et la sur-diagonale :

$$\forall (m, n) \in N^2, \quad m \leqq n \quad \Rightarrow \quad (m, n).f' = (m, n).f$$

$$\forall (m, n) \in N^2, \quad m > n \quad \Rightarrow \quad (m, n).f' = ((n, m).f).i.$$

C'est une application markovienne dont il est inutile de préciser plus les transitions et sa trace sur la diagonale est toujours la suite u.

Considérons, par exemple, la substitution suivante :

$$a \to abc,\ b \to ca,\ c \to b.$$

Voici le résultat de la construction avant la symétrisation :

\$	\$	\$	\$	$(a,0)$	(b,a)	(b,a)	a
\$	\$	\$	$(c,0)$	(a,b)	(b,b)	b	–
\$	\$	$(c,0)$	(c,b)	(a,b)	b	–	–
\$	$(b,1)$	(c,a)	(c,a)	a	–	–	–
\$	$(b,0)$	(c,c)	c	–	–	–	–
$(a,2)$	(b,c)	c	–	–	–	–	–
$(a,1)$	b	–	–	–	–	–	–
a	–	–	–	–	–	–	–

Après symétrisation, on obtient le tableau suivant :

$(\$,+)$	$(\$,+)$	$(\$,+)$	$(\$,+)$	$(a,0,+)$	$(b,a,+)$	$(b,a,+)$
$(\$,+)$	$(\$,+)$	$(\$,+)$	$(c,0,+)$	$(a,b,+)$	$(b,b,+)$	b
$(\$,+)$	$(\$,+)$	$(c,0,+)$	$(c,b,+)$	$(a,b,+)$	b	$(b,b,-)$
$(\$,+)$	$(b,1,+)$	$(c,a,+)$	$(c,a,+)$	a	$(a,b,-)$	$(a,b,-)$
$(\$,+)$	$(b,0,+)$	$(c,c,+)$	c	$(c,a,-)$	$(c,b,-)$	$(c,0,-)$
$(a,2,+)$	$(b,c,+)$	c	$(c,c,-)$	$(c,a,-)$	$(c,0,-)$	$(\$,-)$
$(a,1,+)$	b	$(b,c,-)$	$(b,0,-)$	$(b,1,-)$	$(\$,-)$	$(\$,-)$
a	$(a,1,-)$	$(a,2,-)$	$(\$,-)$	$(\$,-)$	$(\$,-)$	$(\$,-)$

3. APPLICATIONS MODULAIRES SUR N^2

3.1. Substitutions de module constant

Černy et Gruska introduisent sous le nom de « strictly modular trellises » l'équivalent pour la dimension 2 des suites définies par des substitutions de longueur constante; nous qualifierons ces applications de modulaires.

En composant avec une application de l'alphabet F dans un alphabet G on obtient les applications sous-modulaires (modular trellises). Pour pouvoir définir les applications modulaires, il faut préciser ce qu'est, en dimension 2, l'équivalent des substitutions de longueur constante.

DÉFINITION 11 : *Étant donné un alphabet fini F et deux entiers non nuls p et q, une substitution de module (p, q) est une application σ de F dans $F^{[p\,;\,q]}$ où*

$[p; q]$ désigne la partie finie rectangulaire de N^2 :

$$[p; q] = \{(x, y) \mid 0 \leqq x < p,\ 0 \leqq y < q\}$$

DÉFINITION 12 : *Une substitution σ de module (p, q) sur un alphabet F permet de construire une application T_σ de l'ensemble des F-applications dans lui-même. La notation E désignant ici la fonction partie entière, l'image d'une F-application f est donnée par :*

$$(x, y).(f.T_\sigma) = (x \bmod p,\ y \bmod q).(((E(x/p),\ E(y/q)).f).\sigma)$$

On appelle (p, q)-morphisme une telle application T_σ.

Une F-application modulaire est un point fixe d'un (p, q)-morphisme T_σ défini sur l'alphabet F; il est entièrement déterminé par la substitution σ et par sa valeur initiale

$$(0, 0).f = a$$

qui doit vérifier $(0, 0).(a.\sigma) = a$.

Si p et q sont supérieurs à 1, on peut également envisager cette définition de manière plus constructive.

DÉFINITION 13 : *Étant donnée une lettre a de l'alphabet F comme point de départ, on construit par récurrence une suite $\{f_n\}$ d'applications à valeurs dans F; f_0 est définie sur le rectangle à un point $\{(0, 0)\}$ sur lequel elle prend la valeur a; f_n est définie sur le rectangle $[p^n; q^n]$ à partir de l'application f_{n-1} par*

$$(x, y).f_n = (x \bmod p,\ y \bmod q).(((E(x/p),\ E(y/q)).f_{n-1}).\sigma).$$

Si la lettre a satisfait la condition $(0, 0).(a.\sigma) = a$, les diverses applications de la suite $\{f_n\}$ se prolongent les unes les autres. Leur limite f est une F-application définie sur N^2 tout entier qui est un point fixe du (p, q)-morphisme T_σ.

DÉFINITION 14 : *On dit qu'une F-application f est sous-modulaire de module (p, q) s'il existe un alphabet fini $\bar{F}$, une application φ de $\bar{F}$ dans F, et une $\bar{F}$-application modulaire de module (p, q) tels que :*

$$\forall (x, y) \in N^2, \quad (x, y).f = ((x, y).\bar{f}).\varphi.$$

3.2. Premières propriétés

Les restrictions d'une application modulaire ou sous-modulaire de module (p, q) aux deux bords sont des suites modulaires ou sous-modulaires pour des substitutions de longueur p et q.

Lorsque le module de la substitution est carré ($p=q$), la trace diagonale d'une application modulaire (resp. sous-modulaire) de module (p, q) est une suite modulaire (resp. sous-modulaire) pour une substitution de longueur p.

Pour chaque valeur du module (p, q), la classe des applications modulaires (resp. sous-modulaires) de module (p, q) est stable par produit à l'arrivée. Cela signifie que si f_1 est une F_1-application modulaire (resp. sous-modulaire) et f_2 une F_2-application modulaire (resp. sous-modulaire) de module (p, q), l'application produit $f=f_1 \times f_2$ à valeurs dans l'ensemble produit $F=F_1 \times F_2$ défini par :

$$\forall (x, y) \in N^2, \quad (x, y).f=((x, y).f_1, (x, y).f_2)$$

est une F-application modulaire (resp. sous-modulaire) de module (p, q).

On vérifie ainsi la stabilité de la classe des B-applications sous-modulaires de module (p, q) sous l'action des opérations booléennes.

De même, on peut construire une application modulaire ou sous-modulaire de module (p, q) sur N^2 à valeurs dans le produit $F \times G$ comme le produit tensoriel $u \otimes v$ d'une suite u définie sur N par une substitution de longueur p à valeurs dans l'ensemble fini F par la suite v définie sur N par une substitution de longueur q à valeurs dans l'ensemble fini G :

$$\forall (x, y) \in N^2, \quad (x, y).(u \otimes v)=(x.u, y.v).$$

En particulier, pour tout module (p, q), l'indicatrice du produit de deux parties reconnaissables de N est une B-application sous-modulaire.

On en déduit le résultat suivant.

PROPOSITION 5 : *Les indicatrices des parties reconnaissables de N^2 sont des B-applications sous-modulaires pour tout module (p, q).*

3.3. Comparaison des deux classes d'applications

Nous exposons maintenant un résultat de Černy et Gruska [3] : les deux classes d'applications de N^2 dans les ensembles finis que nous avons présentées, celle des applications sous-markoviennes et celle des applications sous-modulaires, sont incomparables pour l'inclusion.

Nous détaillons pour cela un certain nombre de lemmes, qui ne figurent pas tous explicitement dans leur travail. De plus, nos démonstrations n'utilisent pas la caractérisation des applications modulaires à l'aide des automates.

PROPOSITION 6 : *Soit t l'application modulaire de module $(2, 2)$ sur N^2 et à valeurs dans $\{0, 1\}$ définie par sa valeur initiale $(0, 0).t = 0$ et par la substitution :*

$$0 \to \begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array} \qquad 1 \to \begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array}$$

Cette application n'est pas sous-markovienne.

Démonstration : Les suites marginales de t sont des suites de Morse-Thue. Si t était sous-markovienne, elles seraient sous-markoviennes, donc ultimement périodiques. Or, la suite de Thue-Morse est connue pour ne pas l'être.

Pour montrer l'existence d'applications sous-markoviennes qui ne soient modulaires pour aucun module, il faut faire appel à une caractérisation nouvelle des applications sous-modulaires. Avec cette caractérisation, l'application markovienne involutive construit dans la section précédente pour avoir une trace diagonale égale à une suite donnée définie par substitution ne peut être sous-modulaire que pour des modules carrés (p, p).

La suite définie par substitution serait alors définie par une substitution de longueur constante. Or, les travaux de Cobham [5] montrent l'existence de suites définies par substitution qui ne peuvent être définies par aucune substitution de longueur constante.

Décrivons donc cette nouvelle caractérisation, et montrons le résultat annoncé sur les applications spéciales construites sur les suites définies par substitution.

DÉFINITION 15 : *Étant donné un ensemble fini F une substitution de module $((a, b), (c, d))$ est une application σ de $F^{[a;\,b]}$ dans $F^{[c;\,d]}$ où $[a; b]$ et $[c; d]$ désignent les parties rectangulaires de N^2 définies plus haut.*

DÉFINITION 16 : *On associe à une substitution σ de module $((a, b), (c, d))$ une application T_σ de l'ensemble des F-applications dans lui-même, application que l'on appelle un $((a, b), (c, d))$-morphisme.*

Ce morphisme est ainsi défini. L'ensemble N^2 est découpé régulièrement en rectangles contigus de taille (a, b), chacune des fonctions sur (a, b) définies par les traces d'une F-application f donnée est remplacée par son image par σ, puis

les rectangles de taille (c, d) *sont recollés, ce qui donne une application définie sur* N^2, *qui est par définition l'image de* f *par le morphisme. Plus formellement, on a :*

$$\forall (x, y) \in N^2, \quad (x, y).(f.T_\sigma) = (x \bmod c, y \bmod d).((\beta_{E(x/c),\, E(y/d)}).\sigma).$$

où $\beta_{z,\,t}$ *désigne le bloc, élément de* $F^{[a,\,b]}$, *que voici*

$$\forall (x, y) \in [a; b], \quad (x, y).\beta_{z,\,t} = (x + a.z, y + b.t).f.$$

PROPOSITION 7 : *Une application* f *est sous-modulaire de module* (p, q) *si et seulement si c'est un point fixe d'un* $((a, b), (a.p^m, b.q^m))$*-morphisme, où les entiers* a, b *et* m *sont supérieurs ou égaux à* 1.

Démonstration : La preuve repose sur les trois lemmes suivants dont elle se déduit simplement.

LEMME 3 : *Soit* f *une F-application sous-modulaire de module* (p, q) ; *il existe deux entiers* a *et* b, *où* a *est inférieur à* b *et une substitution de module* $((p^a, q^a), (p^b, q^b))$ *sur l'alphabet* F *tels que* f *soit un point fixe du morphisme correspondant.*

La démonstration se trouve dans [2].

LEMME 4 : *Si la F-application* f *est un point fixe d'un* $((a, b), (a.p, b.q))$*-morphisme, elle est sous-modulaire de module* (p, q).

Démonstration : Soit G l'ensemble fini $F^{[a,\,b]} \times [a; b]$. On définit une G-application $\bar{f}$ à partir de f en associant au point (x, y) de N^2 le couple constitué du bloc $\beta_{E(x/a),\,E(y/b)}$ et de la position $(x \bmod a, y \bmod b)$ du point dans le découpage de N^2 en rectangles de taille $[a; b]$.

Cette application $\bar{f}$ est modulaire de module (p, q), puisque f est point fixe d'un $((a, b), (a.p, b.q))$-morphisme et f est obtenue en composant $\bar{f}$ avec l'application naturelle de G dans F qui associe au couple (bloc, position) la valeur prise par le bloc à cette position.

LEMME 5 : *Soit* m *un entier supérieur ou égal à* 1. *Une F-application* f, *modulaire de module* (p^m, q^m), *est sous-modulaire de module* (p, q).

Démonstration : Ici encore nous définissons un nouvel alphabet G à partir de F et une application $\bar{f}$ à valeurs dans G dont f soit un quotient.

L'ensemble G est celui des m-uplets $(c_i,\ 0 \leqq i < m)$, où c_i est un couple $(a_i, (x_i, y_i))$, a_i étant une lettre de l'alphabet F et (x_i, y_i) un élément du rectangle $[p^i; q^i]$.

La valeur en un point (x, y) de l'application $\bar{f}$ est donnée par la liste de ses coordonnées, chacune étant ainsi définie:

$$((x, y).\bar{f})_i = \left(\left(E\left(\frac{x}{p^i}\right), E\left(\frac{y}{q^i}\right)\right).f, (x \bmod p^i, y \bmod q^i)\right).$$

La substitution de module (p, q) pour $\bar{f}$ se déduit de la substitution de module (p^m, q^m) de f et $\bar{f}$ est une application modulaire de module (p, q).

Précisément, si $((a_i, (x_i, y_i)), 0 \leqq i < m)$ est la valeur prise par $\bar{f}$ au point $(E(x/p), E(y/q))$, f a pour valeur en (x, y) le m-uplet $(c_0, \ldots, c_{m-1})$:

$$0 < i < m \quad \Rightarrow \quad ((x, y).\bar{f})_i = (a_{i-1}, (p.x_{i-1} + x \bmod p,\ q.y_{i-1} + y \bmod q))$$

et $((x, y).\bar{f})_0$ se réduit à un couple, couple qui est la valeur prise au point $(p.x_{m-1} + x \bmod p,\ q.y_{m-1} + y \bmod q)$ par le bloc, image de la lettre a_{m-1} par la substitution de module (p^m, q^m) définissant f.

L'application f se déduit de $\bar{f}$ en envoyant un couple élément de G sur sa première coordonnée, qui se réduit à une lettre de F. Elle est donc sous-modulaire de module (p, q).

Il s'agit maintenant d'utiliser la proposition précédente dans le cas de l'application spéciale construite sur une suite diagonale définie par substitution. Nous aurons alors, d'après les remarques précédentes, montré l'existence d'applications markoviennes qui ne sont sous-modulaires pour aucun module.

PROPOSITION 8 : *Soit u une suite définie par une substitution σ sur un alphabet F et soit f l'application markovienne sur N^2 construite à la fin de la section 2 pour être symétrique par rapport à la diagonale et avoir u comme trace diagonale. Si f est sous-modulaire de module (p, q), elle est sous-modulaire pour le module carré (pq, pq).*

Démonstration : Il est clair que f est également sous-modulaire de module (q, p) à cause de la symétrie par rapport à la diagonale.

Puisque f est sous-modulaire de module (p, q), il existe trois entiers a, b et m tels que f soit un point fixe d'un $((a, b), (ap^m, bq^m))$-morphisme T_σ; puisque f est aussi sous-modulaire de module (q, p), il existe trois entiers c, d et n tels que f soit un point fixe d'un $((c, d), \{cq^n, dp^n\})$-morphisme T_τ. L'application f est alors un point fixe de la transformation $T_\sigma^n \circ T_\tau^m$, qui est un $((e, f), (e(pq)^{mn}, f(pq)^{mn}))$-morphisme.

D'après la proposition précédente, l'application f est donc sous-modulaire de module (pq, pq).

Remarque 2: *Il est assez facile de voir que l'indicatrice de la diagonale, qui est une partie rationnelle non reconnaissable de* N^2, *est une B-application modulaire pour tout module carré* (p, p) *et, en utilisant le résultat de Cobham* [4], *qu'elle ne l'est pas pour les modules* (p, q) *où les deux nombres sont multiplicativement indépendants.*

La fin de ce travail est consacrée à la démonstration du second de nos résultats principaux:

Les indicatrices de toutes les parties rationnelles de N^2 sont des B-applications sous-modulaires pour tous les modules carrés.

La remarque précédente montre que l'on ne peut pas espérer grand chose de plus dans cette voie.

3.4. Numérations sur N^2, fonctions automatiques

Černy et Gruska utilisent pour l'étude des applications modulaires la représentation des éléments de N^2 par des mots sur un alphabet de chiffres, représentation analogue à la numération habituelle.

Ceci leur permet de se servir d'automates généralisés pour obtenir des démonstrations concernant la classe des applications sous-modulaires.

En effet, une application sous-modulaire de module (p, q) est une fonction que l'on peut obtenir à l'aide d'un automate lisant de gauche à droite la représentation d'un élément de N^2 en base (p, q).

En fait, l'automate n'est qu'une paraphase de la définition d'une application modulaire de module (p, q): c'est pourquoi nous n'en avons pas eu besoin dans les démonstrations de la sous-section précédente.

Mais, comme nous le montrons plus loin, si une fonction est réalisée par un automate lisant de gauche à droite, elle peut l'être aussi par un automate lisant de droite à gauche.

Dans les bases carrées (p, p), le signe d'une forme affine est une fonction que l'on peut naturellement calculer à l'aide d'un automate lisant de droite à gauche la représentation des éléments de N^2 en base (p, p).

Un théorème de caractérisation géométrique des rationnelles de N^n, dont nous donnons les grandes lignes de la démonstration, permet alors la conclusion annoncée dans l'introduction: les indicatrices des parties rationnelles de N^2 sont des B-applications sous-modulaires pour tout module carré (p, p).

Définissons les numérations sur N^2.

DÉFINITION 17 : *Étant donnés deux entiers p et q supérieurs à* 1, *on représente un élément de* N^2 *en base* (p, q) *en superposant une représentation de la première*

coordonnée avec p comme base de numération et une représentation en base q de la seconde; on aligne à droite ces deux représentations que l'on complète ensuite à gauche par des zéros en nombre arbitraire mais de telle façon que les deux mots soient de même longueur.

Autrement dit, on choisit comme alphabet, ou ensemble de chiffres, le rectangle $C=[p; q]$, *et on associe à un mot de* C^* *l'élément de* N^2 *dont ce mot fournit une écriture en base p de la première coordonnée et une écriture en base q de la seconde, le nombre de chiffres* (0, 0) *à gauche ne changeant pas le résultat.*

Nous rappellerons automates tout court ce que Černy et Gruska appellent «sorting automata» et qui sont connus dans la littérature sous le nom de machines de Moore; il s'agit de prendre en compte le fait que l'ensemble fini d'arrivée peut être autre chose que le demi-anneau de Boole. Donnons-en une définition un peu formelle.

DÉFINITION 18 : *Une application f du monoïde* C^* *dans un ensemble fini* Γ *est dite réalisée par un automate (lisant de gauche à droite) s'il existe un ensemble fini* Σ, *une application s de* Σ *dans* Γ, *un morphisme* μ *de* C^* *dans le monoïde* Σ^Σ *des applications de* Σ *dans lui-même et un élément i de* Σ *tels que*

$$\forall w \in C^*,\ w.f=(i.\ (w.\mu)).s.$$

On appelle automate le quadruplet (Σ, i, μ, s).

C'est une généralisation de la notion d'automate déterministe complet: l'automate passe d'un état à un autre au fur et à mesure que les lettres du mot sont lues de gauche à droite et, la lecture achevée, on prend l'image par s de l'état où l'on est arrivé comme valeur de f pour le mot d'entrée.

La proposition suivante [3] précise le lien entre applications sous-modulaires et fonctions réalisées par automates.

PROPOSITION 9 : *Étant donné une application sous-modulaire* $\bar{f}$ *de module* (p, q), *il existe une application f réalisée par un automate sur le monoïde libre* C^*, *où C est l'ensemble des chiffres en base de numération* (p, q), *telle que la valeur de* $\bar{f}$ *en un point de* N^2 *soit égale à la valeur de f pour une représentation de ce point en base* (p, q). *De plus, l'état initial de l'automate est stable à la lecture du chiffre* (0, 0).

Réciproquement, si une application f sur C^* *est réalisée par un automate* (Σ, i, μ, s) *tel que* $i.((0, 0).\mu)=i$, *sa valeur ne dépend pas du nombre de chiffres* (0, 0) *en tête de la représentation d'un élément de* N^2; *elle définit ainsi*

une application de N^2 dans l'ensemble d'arrivée de s. Cette application est sous-modulaire de module (p, q).

Démonstration : Traitons le cas d'une application modulaire $\bar{f}$ prenant ses valeurs dans F. Elle est entièrement déterminée par sa valeur initiale a et par la substitution σ qui est une application de F dans $F^{[p;q]}$.

Décrivons l'automate. On choisit comme ensemble d'états l'ensemble F, comme état initial a et le morphisme μ est défini à partir de la substitution σ par

$$\forall (x, y) \in C, \quad \forall_e \in F, \quad e.((x, y).\mu) = (x, y).(e.\sigma)$$

la fonction s étant l'identité de F.

Le fait que a soit valeur initiale de $a.\sigma$ et que l'on puisse donc construire f implique que $a.(0, 0) = a$ et donc que la valeur de f ne dépend pas des zéros en tête du mot.

Dans le cas d'une application sous-modulaire, la fonction terminale s est celle qui permet de construire l'application à partir d'une application modulaire.

Pour établir la réciproque, il suffit de choisir Σ comme alphabet et de définir la substitution σ de module (p, q), qui est une application de Σ dans $\Sigma^{[p;q]}$, par

$$\forall (x, y) \in [p; q], \quad \forall a \in \Sigma, \quad (x, y).(e.\sigma) = e.((x, y).\mu).$$

On choisit évidemment l'état initial de l'automate comme point de départ de la construction de la fonction modulaire par itération de la substitution σ.

Dans le cas sous-modulaire, on prend pour fonction terminale la fonction terminale de l'automate.

Passons maintenant à la lecture de droite à gauche.

DÉFINITION 19 : *On dit qu'une fonction f définie sur C^* et à valeurs dans un ensemble fini Γ est réalisée par un automate lisant de droite à gauche si la fonction $\bar{f}$ définie par*

$$\forall w \in C^*, \quad w.\bar{f} = \bar{w}.f$$

où l'on désigne par $\bar{w}$ l'image miroir du mot w, est réalisée par un automate lisant de gauche à droite.

Lorsque Γ n'a que deux éléments, on est ramené à la notion classique de langage reconnu par un automate et le résultat suivant est donc naturel.

PROPOSITION 10 : *Soit f une fonction réalisée par un automate (lisant de gauche à droite) sur C^*. La fonction $\bar{f}$ définie plus haut l'est aussi, ce qui signifie que f est réalisée par un automate lisant de droite à gauche.*

Démonstration : Soit Γ l'ensemble des valeurs de f et (Σ, i, μ, s) un automate réalisant f.

Prenons comme ensemble d'états $\bar{\Sigma}=\Gamma^{\Sigma}$ au lieu de 2^{Σ} dans le cas usuel, posons $\bar{i}=s$ (c'est un élément de $\bar{\Sigma}$), et définissons l'application $\bar{s}$ de $\bar{\Sigma}$ dans Γ comme la spécialisation en i.

$$\forall \alpha \in \bar{\Sigma}, \quad \alpha . \bar{s} = i . \alpha .$$

Soit d l'application de dualité de Σ^{Σ} dans $\bar{\Sigma}^{\bar{\Sigma}}$ définie par

$$\forall e \in \Sigma^{\Sigma}, \quad \forall \alpha \in \bar{\Sigma}, \quad \alpha . (e . d) = e \circ \alpha .$$

Cette dualité d est un antihomomorphisme de monoïdes et l'application $\nu = \mu \circ d$ est aussi un antihomomorphisme de C^* dans $\bar{\Sigma}^{\bar{\Sigma}}$.

On définit alors le morphisme $\bar{\mu}$ de C^* dans $\bar{\Sigma}^{\bar{\Sigma}}$ en posant

$$\forall w \in C^*, \quad w . \bar{\mu} = \bar{w} . \nu$$

Pour prouver le résultat annoncé, montrons que l'automate $(\bar{\Sigma}, \bar{i}, \bar{\mu}, \bar{s})$ ainsi construit réalise la fonction $\bar{f}$ en vérifiant l'identité

$$w . \bar{f} = (\bar{i} . (w . \bar{\mu})) . \bar{s}$$

Calculons

$$(\bar{i} . (w . \bar{\mu})) . \bar{s} = i . (\bar{i} . (w . \bar{\mu}))$$

$$(\bar{i} . (w . \bar{\mu})) . \bar{s} = i . (\bar{i} . ((\bar{w} . \mu) . d))$$

$$(\bar{i} . (w . \bar{\mu})) . \bar{s} = i . ((\bar{w} . \mu) \circ \bar{i})$$

$$(\bar{i} . (w . \bar{\mu})) . \bar{s} = (i . (\bar{w} . \mu)) . \bar{i}$$

$$(\bar{i} . (w . \bar{\mu})) . \bar{s} = (i . (\bar{w} . \mu)) . s = \bar{w} . f .$$

Ceci achève la preuve de la proposition.

Pour pouvoir utiliser cette équivalence dans le cas de fonctions réalisées par automate qui correspondent à des fonctions sous-modulaires sur N^2, remarquons que la condition sur le premier automate qui exige que son état initial soit stable à la lecture du chiffre (0, 0) est équivalente au fait de

demander que la fonction terminale du second automate vérifie

$$\forall e \in \bar{\Sigma}, \quad e.\bar{s} = (e.((0, 0).\bar{\mu})).\bar{s}$$

3.5. Parties rationnelles de N^2

L'outil décisif pour prouver que les parties rationnelles de N^2 sont (p, p)-sous-modulaires est la reconnaissabilité du signe des formes affines par un automate.

DÉFINITION 20 : *Une forme affine sur N^2 est ici une forme affine à coefficients dans Z, c'es-à-dire une application de la forme*

$$(x, y) \to ax + by + c$$

où (a, b, c) est un triplet fixé de Z^3.

Le signe de cette forme affine est l'application composée à valeurs dans l'ensemble $\{-, =, +\}$ où le signe d'un entier relatif est « − », « = » ou « + » selon que cet entier est négatif, nul ou positif.

THÉORÈME 2 : *Étant donnés trois entiers relatifs a, b et c et un entier p supérieur à 1, la fonction de N^2 dans $\{-, =, +\}$ qui associe à un élément (x, y) de N^2 le signe de $ax + by + c$ est réalisée par un automate lisant de droite à gauche (et donc aussi par un automate lisant de gauche à droite) dans la base de numération (p, p).*

Démonstration : L'ensemble Σ des états est le produit par l'ensemble $\{=, +\}$ d'un intervalle de Z que l'on déterminera *a posteriori.*

L'état initial est le couple $(c, =)$ et la transition est définie de la manière suivante. On est dans l'état (d, σ) et on lit le chiffre (x, y); on calcule la somme $s = a.x + b.y + d$, le quotient entier de s par p fournit la partie scalaire de l'état suivant; le signe de l'état suivant est « + » si le reste de la division de s par p n'est pas nul et sinon, on garde l'ancien signe σ.

La fonction terminale est la suivante: le signe d'un état (d, σ) est celui de d si d n'est pas nul et sinon, c'est σ.

Cet automate fait ce que l'on attend de lui; à chaque étape en effet, la valeur de la forme affine est le multiple par une certaine puissance de p de la somme $a\bar{x} + b\bar{y} + d + \varepsilon$, où $\bar{x}$ et $\bar{y}$ sont les coordonnées du nombre qui reste à lire, où d est la partie scalaire de l'état où l'on est, et où ε est un rationnel nul si le signe de l'état est « = », strictement compris entre 0 et 1 si ce signe est « + ».

Pour être complet, il faut s'assurer que la partie scalaire de l'état reste dans un intervalle de Z quoi qu'il arrive. En fait, sa valeur absolue reste toujours inférieure ou égale à la somme des valeurs absolues de a, b et c.

Appelons demi-espace la partie de N^2 où une forme affine est positive ou nulle; le complémentaire d'un demi-espace est encore un demi-espace (la forme opposée est supérieure ou égale à 1).

La classe des B-applications sous-modulaires de module (p, p) contient les indicatrices des parties reconnaissables et elle est stable par les opérations booléennes.

Le théorème suivant caractérise géométriquement les parties rationnelles de N^n et permet de conclure que les indicatrices des parties rationnelles de N^2 sont des B-applications sous-modulaires de module (p, p) pour toute valeur de la base p.

THÉORÈME 3 : *Les parties rationnelles de N^n sont les réunions finies d'ensembles dont chacun est l'intersection d'une partie reconnaissable et d'un certain nombre de demi-espaces.*

Cette caractérisation a pour corollaire le résultat de Ginsburg et Spanier [8,9] montrant que les opérations booléennes laissent stable la classe des parties rationnelles du monoïde abélien libre.

La démonstration de ce théorème commence par deux lemmes dont on trouve la preuve dans le travail de Ginsburg et Spanier.

LEMME 6 : *Les parties rationnelles de N^n sont les réunions finies d'ensembles linéaires.*

LEMME 7 : *Un ensemble linéaire de N^n est une réunion finie d'ensembles linéaires libres.*

Notre approche s'écarte de la démonstration classique avec la remarque suivante.

PROPOSITION 11 : *Un ensemble linéaire libre est l'intersection d'une partie reconnaissable et d'un certain nombre de demi-espaces.*

Démonstration : Considérons un ensemble linéaire libre E dans N^n d'origine V_0 et de base $\{V_1, \ldots, V_k\}$; c'est l'ensemble des éléments V de N^n qui

s'écrivent (et d'une manière unique)

$$V = V_0 + \sum_{i=1}^{i=k} \lambda_i V_i$$

où les λ_i sont des entiers naturels.

Complétons éventuellement (si $k < n$) le système libre $\{V_1, \ldots, V_k\}$ par $\{V_{k+1}, \ldots, V_n\}$ pour obtenir une base $\{V_1, \ldots, V_n\}$ du Q-espace vectoriel Q^n constituée d'éléments de Z^n. Soit alors $\{p_1, \ldots, p_n\}$ la base duale de la base $\{V_1, \ldots, V_n\}$.

Un vecteur V de N^n appartient à l'ensemble linéaire E si et seulement si les conditions suivantes sont simultanément réalisées:

Le vecteur $V - V_0$ appartient au réseau R engendré dans Z^n par $\{V_1, \ldots, V_n\}$.

Pour tout i compris entre 1 et k, la projection $p_i(V - V_0)$ est positive ou nulle.

Pour tout i compris entre $k+1$ et n, la projection $p_i(V - V_0)$ est positive ou nulle.

Pour tout i compris entre $k+1$ et n, la projection $p_i(V_0 - V)$ est positive ou nulle.

Un élément V de E est donc caractérisé par le signe d'un certain nombre de formes affines (on peut multiplier les p_i par des entiers positifs pour en faire des formes affines à coefficients entiers sans changer leur signe) et par le fait que l'image de V dans le quotient de Z^n par le réseau R est la même que celle de V_0.

Puisque R est un réseau, ce quotient est un groupe fini, et l'ensemble des éléments de N^n congrus à V_0 modulo R une partie reconnaissable.

Ainsi, les parties rationnelles sont du type indiqué, ce qui suffit pour obtenir le théorème suivant.

THÉORÈME 4 : *Les indicatrices des parties rationnelles de N^2 sont des B-applications (p, p)-sous-modulaires pour tous les modules carrés.*

Réciproquement, pour achever la preuve du théorème de caractérisation géométrique des parties rationnelles de N^n, il reste à établir qu'une intersection de demi-espaces est une partie rationnelle, l'intersection avec une partie reconnaissable lui conservant ce caractère.

On déduit cette propriété d'un résultat analogue sur les parties convexes d'un espace vectoriel de dimension finie sur le corps des rationnels, résultat qui fait l'objet du lemme suivant.

LEMME 8 : *La partie convexe de Q^n, correspondant à l'intersection d'un certain nombre de demi-espaces, est la somme d'une partie bornée et du cône engendré par un nombre fini de vecteurs à coordonnées positives (dont on peut alors choisir les coordonnées entières).*

En rendant le problème projectif, ceci résulte de l'énoncé suivant, dont on peut donner une démonstration constructive et laborieuse :

Une partie convexe bornée de Q^n, intersection d'un nombre fini de demi-espaces, est l'enveloppe convexe de ses points extrémaux, qui sont en nombre fini.

On pourrait aussi déduire ce résultat du théorème de Krein-Milman en analyse réelle.

CONCLUSION

Nous avons présenté deux théorèmes nouveaux relatifs aux classes d'applications de N^2 dans les ensembles finis (trellises) introduites par Culik, Gruska et Salomaa, et par Černy et Gruska.

Premièrement, les indicatrices des parties rationnelles de N^2 sont des B-applications sous-markoviennes.

Deuxièmement, pour tous les modules carrés (p, p), les indicatrices des parties rationnelles de N^2 sont des B-applications (p, p)-sous-modulaires.

REMERCIEMENTS

C'est un grand plaisir pour moi de remercier Jacques Sakarovitch pour ses encouragements et ses précieux conseils. Je voudrais aussi exprimer au rapporteur mes vifs remerciements pour son aimable vigilance.

BIBLIOGRAPHIE

1 J. BERSTEL, *Every Iterated Morphism Yields a co-CFL*, Inform. Processing Letters, vol. 22, 1986, p. 7-9.

2 A. CERNY et J. GRUSKA, *Modular Trellis Automata*, preprint 1986, Fundamenta Informaticae (à paraître).

3 A. CERNY et J. GRUSKA, *Modular Trellises*, preprint 1986.

4 A. COBHAM, *On the Base-Dependence of Sets of Numbers Recognizable by Finite Automata*, Math. Systems Theory, vol. 3, 1969, p. 186-192.

5 A. COBHAM, *Uniform Tag Sequences*, Math. Systems Theory, vol. 6, 1972, p. 164-192.

6 K. CULIK, J. GRUSKA et A. SALOMAA, *Systolic Trellis Automata: Stability, Decidability and Complexity*, Res. Report CS-82-04, Univ. of Waterloo, 1982.

7 K. CULIK, J. GRUSKA et A. SALOMAA, *Systolic Trellis Automata,* Intern. Jour. Computer Math., vol. 15, 1984, p. 195-212 et vol. 16, 1984, p. 3-22.

8 S. EILENBERG et M. P. SCHUTZENBERGER, *Rational Sets in Commutative Monoids,* Journal of Algebra, vol. 13, 1969, p. 173-191.

9 S. GINSBURG et E. H. SPANIER, *Bounded ALGOL-like Languages,* Trans. Amer. Math. Soc., vol. 113, 1964, p. 333-368.

10 R. ITO, *Every semilinear Set is a Finite Union of Disjoint linear Sets,* J.C.S.S., vol. 8, 1969, p. 221-231.

11 I. KOREC, *Generalized Pascal Triangles: Decidability results,* Acta Math. Univ. Comen., Bratislava, 1985 (à paraître).