

Quelques tours de mathémagie et au-delà...

Michel Rigo, Université de Liège

M.Rigo@ulg.ac.be, <http://www.discmath.ulg.ac.be/mam/>

Printemps des Sciences 2010

Résumé

Nous présentons ici 5 tours de magie ne nécessitant aucune habileté particulière de la part de l'apprenti magicien : des tours de cartes, des tours de divination et le célèbre tour du "barman aveugle avec des gants de boxe". Contrairement au magicien qui ne dévoile jamais ses secrets, ici, nous expliquons que ces tours reposent sur diverses propriétés et constructions mathématiques. Ces dernières débouchent sur de véritables questions de recherche actuelle en théorie des graphes ou en combinatoire des mots et même sur de possibles applications en robotique et automatisation ! Il y en aura donc pour tous les goûts... et tous les niveaux (suivant l'auditoire, l'exposé sera adapté au niveau des élèves de la 4^{ième} à la 6^{ième} secondaire, voire même aux étudiants universitaires). Ce texte présente donc un matériel qui dépassera souvent (et de loin) le "spectacle".

1 Mentalisme, chapelets et mots circulaires

1.1 Le chapelet de Si Stebbins

Le premier tour est issu de [8]. Il utilise la *technique du chapelet*. Il est basé sur une suite prédéterminée de cartes que le magicien doit connaître par coeur (ou être à même de reconstruire facilement). Pour le spectateur, le jeu de cartes paraît, sans inspection minutieuse, avoir été bien mélangé. Le tour de "de Bruijn" présenté plus loin en est une variante plus évoluée.

• Les **préparatifs** du magicien consistent à classer à l'avance les cartes d'un jeu de 52 cartes comme suit : la valeur d'une carte augmente à chaque fois de trois unités. On assigne aux valets, dames et rois respectivement les valeurs 11, 12 et 13. On travaille "modulo 13", cela signifie que $11 + 3 = 1$, $12 + 3 = 2$ et $13 + 3 = 3$. Quand le résultat dépasse 13, on soustrait 13 pour obtenir une valeur toujours comprise entre 1 et 13. Ainsi, on obtient le "cycle" suivant.

$$1 \xrightarrow{+3} 4 \xrightarrow{+3} 7 \xrightarrow{+3} 10 \xrightarrow{+3} R \xrightarrow{+3} 3 \xrightarrow{+3} 6 \xrightarrow{+3} 9 \xrightarrow{+3} D \xrightarrow{+3} 2 \xrightarrow{+3} 5 \xrightarrow{+3} 8 \xrightarrow{+3} V \xrightarrow{+3} \dots$$

On remarque en effet, qu'après un valet (de valeur 11), on a toujours un as (car $11 + 3 = 1 \pmod{13}$). De plus, on ordonne les cartes en variant les couleurs comme suit :

$$\heartsuit \rightarrow \clubsuit \rightarrow \diamondsuit \rightarrow \spadesuit \rightarrow \heartsuit \rightarrow \dots$$

Ainsi, le jeu complet est préparé comme au tableau 1 (d'abord de gauche à droite, puis ligne par ligne). On pourra considérer des variantes : on peut changer

1♥	4♣	7♦	10♠	R♥	3♣	6♦	9♠	D♥	2♣	5♦	8♠	V♥
1♣	4♦	7♠	10♥	R♣	3♦	6♠	9♥	D♣	2♦	5♠	8♥	V♣
1♦	4♠	7♥	10♣	R♦	3♠	6♥	9♣	D♦	2♠	5♥	8♣	V♦
1♠	4♥	7♣	10♦	R♠	3♥	6♣	9♦	D♠	2♥	5♣	8♦	V♠

TAB. 1 – Le chapelet de Si Stebbins.

l'ordre des couleurs et choisir d'ajouter un autre entier que 3 pour passer d'une valeur à la suivante. En effet, modulo 13, ajouter de manière systématique un même entier conduit toujours à un "cycle complet".

- Le **tour** proprement dit. Le magicien montre rapidement le jeu aux spectateurs et demande à l'un d'eux de couper le jeu en deux tas (soient A le tas du "dessus" et B le tas du "dessous"). Une fois le jeu coupé, le spectateur prend la carte se trouvant sur le dessus de B et ne la montre pas. Le magicien la devine facilement ! On pourra même compliquer le tour en devinant les cartes de deux spectateurs qui auront chacun coupé le jeu et pris à chaque fois la carte du dessus. Même si le second spectateur ne coupe pas, le tour fonctionne encore.

- **Pourquoi** cela fonctionne-t-il ? Quand le jeu est coupé, cela ne change en rien la structure de la liste ordonnée des cartes du jeu. On effectue uniquement une permutation circulaire et les valeurs, tout comme les couleurs, sont arrangées de façon cyclique. Une fois la carte prise par le spectateur au sommet de B , en mettant le tas B au dessus du tas A , le magicien s'arrange pour connaître la dernière carte x de A (il s'agit donc, dans la liste ordonnée de cartes, de la carte qui précède la carte à deviner). Le magicien n'a qu'à ajouter 3 à la valeur x . Il connaît aussi l'ordre d'apparition des couleurs. Et le tour est joué.

1.2 Le chapelet de de Bruijn

J'ai vu pour la première fois ce tour en guise d'introduction à un séminaire de recherche en mathématiques donné par Raphaël Jungers (UCL), lui-même le tenait d'un autre mathématicien, Persi Diaconis [7]. Basé sur la technique du chapelet, il s'agit d'une belle application en combinatoire des mots¹.

- Les **préparatifs** du magicien consistent à ordonner son chapelet, i.e., à classer à l'avance les cartes d'un jeu de 32 cartes comme à la table 2 en page 3 (d'abord de gauche à droite, puis ligne par ligne).

- Le **tour** proprement dit. On demande à un spectateur (voire plusieurs, cela ne rend le tour que plus spectaculaire) de couper le jeu. Ensuite, six spectateurs prennent chacun une carte, à chaque fois, la première du tas. Les cinq premiers annoncent à haute voix uniquement la couleur (rouge ou noire) de leur carte. Le magicien devine alors la valeur exacte de la sixième carte ! A la lecture du texte ci-dessous, on comprendra que le magicien peut même retrouver la valeur exacte des six cartes.

¹La *combinatoire des mots* est une branche des mathématiques discrètes s'intéressant aux propriétés et arrangements possibles des suites (finies ou infinies) de symboles appartenant à un ensemble fini, appelé alphabet. Elle trouve, entre autres, des applications en bio-informatique ou pour le codage de données.

D♥ (Rouge)	V♦ (Rouge)	7♦ (Rouge)	8♥ (Rouge)	R♦ (Rouge)
7♣ (Noir)	1♠ (Noir)	R♠ (Noir)	1♣ (Noir)	8♠ (Noir)
9♥ (Rouge)	V♠ (Noir)	D♠ (Noir)	10♣ (Noir)	D♦ (Rouge)
7♥ (Rouge)	10♠ (Noir)	V♣ (Noir)	10♥ (Rouge)	9♠ (Noir)
9♦ (Rouge)	R♣ (Noir)	D♣ (Noir)	8♦ (Rouge)	V♥ (Rouge)
1♥ (Rouge)	8♣ (Noir)	10♦ (Rouge)	9♣ (Noir)	R♥ (Rouge)
1♦ (Rouge)	7♠ (Noir)			

TAB. 2 – Le chapelet de de Bruijn.

• **Pourquoi** cela fonctionne-t-il ? Grossièrement parlant (inutile d’être à tout prix formel²), un mot *circulaire* se “referme” sur lui-même. Il n’a ni début, ni fin. De façon imagée, on peut imaginer placer des convives autour d’une table ronde. Chacun a un voisin à sa gauche et à sa droite, mais il n’y a ni premier, ni dernier. La liste des convives placés à table est un mot circulaire. Peu importe de savoir par qui on débute, seul l’ordre des convives a de l’importance. Un *facteur* de longueur n est une suite de n lettres consécutives apparaissant dans le mot. Pour cela, on suppose disposer d’un sens de parcours. Nous fixons ici le sens horloger. Remarquons que travailler avec des mots circulaires est bien commode lorsqu’on décide de couper un jeu de cartes, cela n’affecte pas le mot circulaire correspondant.

Exemple 1. Considérons le mot circulaire “*abbaba*” symbolisé par la figure 1 (ou si vous préférez, le mot “*bbabaa*” etc.). Ses facteurs de longueur 4 sont : *abba*,

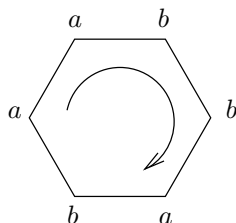


FIG. 1 – Un mot circulaire.

bbab, *baba*, *abaa*, *baab* et *aabb*.

Nicolaas Govert de Bruijn, né en 1918, est professeur émérite à l’Université d’Eindhoven. A la fin des années 1940, il a étudié une famille de mots qui portent à présent son nom.

On fixe tout d’abord un entier $n \geq 2$ et un alphabet de p symboles. Un *mot de de Bruijn* “de type $B(p, n)$ ” est un mot circulaire, le plus court possible (en fait, on peut montrer qu’il est exactement de longueur p^n), contenant tous les p^n facteurs de longueur n sur un alphabet de taille p .

Les premiers travaux sur le sujet remontent à 1894 et de Bruijn lui-même attribue la preuve de l’existence, pour tout entier $n \geq 2$, de tels mots circulaires

²On pourrait facilement, pour un mot circulaire de longueur n , indexer les lettres du mot par les éléments de l’ensemble $\{0, \dots, n-1\}$ et travailler modulo n . Ainsi, la lettre en position $n-1$ a pour voisins directs les lettres en position $n-2$ d’une part et 0 d’autre part. Un facteur est déterminé par les positions appartenant à un intervalle d’entiers consécutifs réduits modulo n .

sur deux lettres, à Camille Flye Sainte-Marie. La généralisation à des alphabets plus grands a été obtenue par de Bruijn avec Tanja van Ardenne-Ehrenfest dans [1]. Une question naturelle est aussi de déterminer le nombre de mots de de Bruijn de type $B(p, n)$ distincts [4].

Théorème 2. *Sur un alphabet de p symboles, il existe pour tout $n \geq 2$, un mot de de Bruijn de type $B(p, n)$ et de longueur p^n .*

Un *graphe (orienté)* et étiqueté par un ensemble fini Σ est la donnée d'un ensemble V de *sommets* et d'un ensemble $E \subseteq V \times \Sigma \times V$ d'*arcs* munis d'un label (ou d'une étiquette) appartenant à Σ et joignant un couple de sommets de V .

Exemple 3. Considérons l'ensemble de sommets $V = \{1, 2, 3\}$, l'alphabet $\Sigma = \{a, b\}$ et l'ensemble d'arcs étiquetés

$$V = \{(1, a, 2), (1, a, 3), (2, b, 3), (3, b, 3)\}.$$

On peut représenter le graphe correspondant comme à la figure 2.

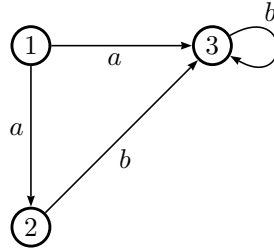


FIG. 2 – Un graphe orienté étiqueté.

Soit un alphabet Σ contenant p symboles. N. G. de Bruijn a défini un graphe (maintenant appelé *graphe de de Bruijn d'ordre n*) dont les p^n sommets sont tous les facteurs de longueur n possibles et dont les arcs sont étiquetés par les éléments de Σ . De chaque sommet est issu un arc par élément de Σ :

$$\forall v \in V, \forall a \in \Sigma, \exists w \in V : (v, a, w) \in E. \quad (1)$$

Si u est un mot de longueur $n - 1$ et si a et b sont deux lettres, alors on a un arc (de label b) entre les sommets au et ub . Par exemple, les 8 facteurs de longueur 3 sur l'alphabet de deux lettres $\{0, 1\}$ sont 000, 001, 011, 111, 110, 101, 010 et 100 et on dispose de l'arc

$$010 \xrightarrow{1} 101.$$

Le graphe d'ordre 3 correspondant est représenté à la figure 3. Il contient 8 sommets et 16 arcs. Il suffit alors de chercher un cycle de longueur minimale passant par *tous les sommets* du graphe pour construire un mot circulaire (fourni par les labels du cycle) contenant *tous les facteurs* de longueur n . Le théorème 2 stipule qu'un tel cycle existe toujours³. Sur notre exemple, le mot circulaire 00011101 contient bien tous les facteurs de longueur 3.

³Le graphe ainsi construit est *hamiltonien* : il existe un cycle passant une et une seule fois par chaque sommet. En particulier, cela entraîne que le mot de de Bruijn correspondant est de longueur p^n et inversement.



0001011001111010

Revenons à notre tour de magie. Pour les facteurs de longueur $n = 5$ sur un alphabet $\{R, N\}$ de taille $p = 2$ (souvenez-vous, cinq spectateurs annoncent chacun une couleur), le mot de longueur $2^5 = 32$

$$RRRRRNNNNRRNNRRNNRRNNRRRRNRNRRN \quad (2)$$

RRRRRNNNNNRNNNRRNNRNRRNNRRRNRRNRN.

⁴On peut montrer que le graphe est aussi *eulérien*, ce qui est ici assez immédiat : chaque sommet a le même demi-degré entrant et sortant valant p .

$$9\spadesuit - 9\diamondsuit - R\clubsuit - D\clubsuit - 8\diamondsuit$$

et dans ce tableau, la carte suivante est le $V\heartsuit$.

Remarque 5. On peut par exemple utiliser les mots de de Bruijn dans des systèmes robotisés. Pour déterminer l'angle fait par un repère fixe et un repère présent sur une roue mécanique utilisée sur une chaîne de montage, il suffit que cette dernière soit marquée par un mot de de Bruijn et que l'on dispose d'un capteur ad hoc pour connaître complètement sa configuration.

Supposons qu'un cadenas électronique fonctionne avec les 4 derniers chiffres entrés sans devoir appuyer sur une touche particulière de validation. Alors, pour trouver le code par essais successifs, un mot de de Bruijn de longueur 10003 consiste en la méthode la plus rapide.

2 Divination et numération

2.1 Un peu d'arithmétique

Ce tour est tiré de [2]. Chacun choisit un nombre de 3 chiffres, comme 712 ou 824. Il faut juste que le chiffre des centaines diffère de celui des unités. Le *miroir* d'un nombre comme 712 est 217. Chacun considère le nombre qu'il a choisi et son miroir. Il soustrait le plus petit du plus grand (pour obtenir un nombre positif). Maintenant, on additionne le résultat avec son miroir (attention, si le résultat n'a que deux chiffres, on suppose avoir un zéro de tête pour en faire un nombre de trois chiffres ; comme $17 = 017$, son miroir est 710) pour obtenir... 1089 !

• **Preuve.** Soit abc une écriture décimale formée de trois chiffres $a, b, c \in \{0, \dots, 9\}$. Supposons $a > c$, la démonstration est analogue dans l'autre cas. La première soustraction donne $(a - c) \times 100 + (c - a)$ mais $c - a$ est négatif. Ce nombre se décompose encore

$$(a - c - 1) \times 100 + 90 + 10 + (c - a)$$

et s'écrit donc en base 10

$$(a - c - 1) \ 9 \ (10 + c - a).$$

Si maintenant, on ajoute à ce dernier son miroir, on obtient :

$$\begin{array}{r} \\ \\ + \\ \hline 1 \end{array}$$

2.2 Le truc de la base 2

Ce tour et le suivant, celui du barman aveugle, m'ont été suggérés par le professeur Fabien Durand de l'Université d'Amiens (lui aussi essaie de promouvoir localement les mathématiques dans les lycées et collèges⁵). Un spectateur choisit un nombre entre 1 et 63. Il l'inscrit sur une feuille de papier qu'il ne montre

⁵Mathématiques pour tou-te-s,

www.mathinfo.u-picardie.fr/schapira/Vulgarisation/propositions_exposes.html

à personne. En posant quelques questions simples, le magicien va découvrir ce nombre. On montre au spectateur six listes de nombres et à chaque fois, il doit dire si oui ou non le nombre qu'il a choisi s'y trouve. Après avoir entendu les six réponses, le magicien est à même de donner le nombre secret.

1	3	5	7	9	11	13	15
17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47
49	51	53	55	57	59	61	63

2	3	6	7	10	11	14	15
18	19	22	23	26	27	30	31
34	35	38	39	42	43	46	47
50	51	54	55	58	59	62	63

4	5	6	7	12	13	14	15
20	21	22	23	28	29	30	31
36	37	38	39	44	45	46	47
52	53	54	55	60	61	62	63

8	9	10	11	12	13	14	15
24	25	26	27	28	29	30	31
40	41	42	43	44	45	46	47
56	57	58	59	60	61	62	63

16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

• **Pourquoi** cela fonctionne-t-il ? A chaque réponse positive du spectateur, le magicien n'a qu'à additionner le nombre se trouvant dans la première case du tableau considéré. A la fin, il sera en possession du nombre mystère. Le secret réside dans la décomposition des nombres en base 2 (tout entier se décompose comme une somme de puissances de deux). Pour plus de détails sur le système binaire, voir par exemple [14]. Les tableaux ci-dessous contiennent les mêmes entrées mais cette fois, écrite en base 2. Dans le premier tableau, tous les nombres ont un dernier chiffre valant 1. Dans le deuxième tableau, tous les nombres ont un avant-dernier chiffre valant 1, etc. En sommant les entrées positives, on reconstruit en fait la décomposition en base 2 de l'entier choisi secrètement par le spectateur.

1	11	101	111	1001	1011	1101	1111
10001	10011	10101	10111	11001	11011	11101	11111
100001	100011	100101	100111	101001	101011	101101	101111
110001	110011	110101	110111	111001	111011	111101	111111

10	11	110	111	1010	1011	1110	1111
10010	10011	10110	10111	11010	11011	11110	11111
100010	100011	100110	100111	101010	101011	101110	101111
110010	110011	110110	110111	111010	111011	111110	111111

100	101	110	111	1100	1101	1110	1111
10100	10101	10110	10111	11100	11101	11110	11111
100100	100101	100110	100111	101100	101101	101110	101111
110100	110101	110110	110111	111100	111101	111110	111111

1000	1001	1010	1011	1100	1101	1110	1111
11000	11001	11010	11011	11100	11101	11110	11111
101000	101001	101010	101011	101100	101101	101110	101111
111000	111001	111010	111011	111100	111101	111110	111111

10000	10001	10010	10011	10100	10101	10110	10111
11000	11001	11010	11011	11100	11101	11110	11111
110000	110001	110010	110011	110100	110101	110110	110111
111000	111001	111010	111011	111100	111101	111110	111111

100000	100001	100010	100011	100100	100101	100110	100111
101000	101001	101010	101011	101100	101101	101110	101111
110000	110001	110010	110011	110100	110101	110110	110111
111000	111001	111010	111011	111100	111101	111110	111111

Certains spectateurs risquent de reconnaître une certaine régularité dans les tableaux proposés. On pourrait considérer des variantes en se basant sur des systèmes de numération non standards comme celui que l'on peut construire sur la suite de Fibonacci [17].

3 Barman aveugle et synchronisation

- Le **tour** proprement dit. Le magicien se bande les yeux (il peut aussi avoir des gants de boxe pour être certain que le toucher n'a rien à voir dans le tour). Sont disposés face à lui quatre récipients cylindriques avec un marquage bien visible haut/bas, par exemple, des verres, des boîtes de conserve ou des piles électriques avec deux pôles $\oplus$ et $\ominus$ indiscernables. Il est impossible de discerner le haut du récipient de son bas. Quand le magicien a les yeux bandés, un spectateur est invité à placer les récipients comme bon lui semble vers le haut ou vers le bas. Par exemple, deux dans un sens et les deux autres dans l'autre sens. En 7 mouvements maximum (un mouvement revient à retourner un ou deux récipients), le magicien doit être capable de mettre les quatre récipients tous dans le même sens (les quatre vers le haut, ou les quatre vers le bas, peu importe). Puisque le magicien ne voit rien, les spectateurs applaudissent pour lui signaler quand il a réussi son pari.

- **Pourquoi** cela fonctionne-t-il? Le magicien connaît une suite de coups qui, lorsqu'on les applique, permet toujours de passer par la configuration voulue. Les mouvements sont :

“diagonal - vertical - diagonal - un seul - diagonal - vertical - diagonal”.

	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$					
	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$					
$\oplus$ $\ominus$	$\ominus$ $\ominus$	$\ominus$ $\oplus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\ominus$ $\ominus$	$\ominus$ $\oplus$	$\oplus$ $\oplus$					
$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$					
$\oplus$ $\oplus$	$\ominus$ $\oplus$	$\ominus$ $\ominus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$								
$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\oplus$								
$\oplus$ $\oplus$	$\ominus$ $\oplus$	$\ominus$ $\ominus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\ominus$ $\oplus$	$\ominus$ $\ominus$						
$\ominus$ $\oplus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\ominus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\oplus$	$\oplus$ $\oplus$						
$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$	$\oplus$ $\oplus$	$\oplus$ $\oplus$						
$\ominus$ $\ominus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$										
$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\oplus$ $\oplus$										
$\ominus$ $\oplus$	$\oplus$ $\oplus$											
$\oplus$ $\ominus$	$\oplus$ $\oplus$											
$\ominus$ $\oplus$	$\oplus$ $\oplus$	$\oplus$ $\ominus$	$\ominus$ $\ominus$									
$\ominus$ $\oplus$	$\ominus$ $\ominus$	$\ominus$ $\oplus$	$\ominus$ $\ominus$									

[illegible]

9

Une variante consiste à placer les récipients sur un plateau tournant. A chaque nouveau mouvement, un spectateur peut, s'il le souhaite, faire pivoter le plateau. On obtient un modèle semblable à celui de la figure 4 (mais uniquement avec 4 types de configurations) et la même suite de coups fonctionne encore.

3.1 Graphes synchronisants

On peut reconsidérer le thème introduit par le tour du barman aveugle mais avec une contrainte plus forte. Soient $\Sigma = \{\sigma_1, \dots, \sigma_k\}$ un ensemble de k labels ou “couleurs” et $\mathcal{A} = (Q, \Sigma, \delta)$ un *graphe de transitions*⁶ (fini). Cela signifie que de tout sommet q de l'ensemble Q des sommets sont issus exactement k arcs, un par couleur. Le codage de ces arcs est donné par $\delta : Q \times \Sigma \rightarrow Q$; $\delta(q, \sigma) = r$ signifie que depuis l'état q , il est possible de parcourir un arc de couleur σ pour aboutir dans l'état r . De manière raccourcie, on écrira simplement $q.\sigma = r$.

Exemple 6. Voici deux graphes de transitions. Tous deux ont des arcs colorés par deux couleurs a et b . Le premier a $\{1, 2, 3\}$ pour ensemble de sommets et le second $\{4, 5, 6\}$. Ces deux graphes ont la même “structure” mais pas les mêmes coloriages d'arcs. On peut vérifier que depuis chaque sommet sont issus deux arcs, un de label a et un de label b .

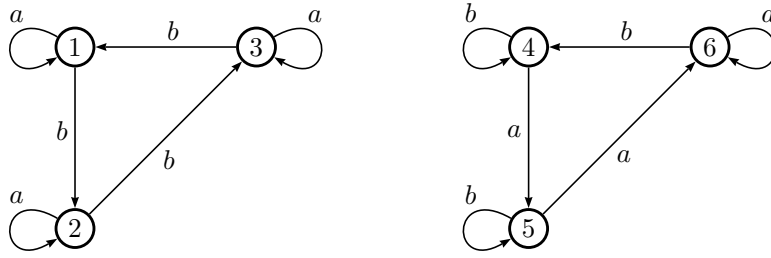


FIG. 5 – Deux graphes de transitions avec $\Sigma = \{a, b\}$.

Une suite ordonnée $m = m_1 \dots m_\ell$ de ℓ couleurs (ou simplement un mot) est *synchronisante* s'il existe un sommet $p \in Q$ tel que pour tout sommet $q \in Q$, $q.m = p$. Cela signifie que suivre, depuis tout sommet q , des arcs colorés dans l'ordre prescrit par m aboutit toujours dans le sommet p ,

$$(\dots((q.m_1).m_2)\dots.m_\ell) = p$$

Exemple 7. Poursuivons l'exemple 6, et considérons la suite de couleurs $abba$ dans le graphe de transitions de gauche de la figure 5. Celle-ci nous donne $1.baab = 3$, $2.baab = 1$ et $3.baab = 2$. Le mot $baab$ n'est donc pas synchronisant. Par contre, si on considère ce même mot $baab$ dans le graphe de transitions de droite, on a $4.baab = 4$, $5.baab = 4$ et $6.baab = 4$. Ce mot est donc synchronisant pour le graphe de droite. On peut même assez facilement se convaincre que,

⁶Il s'agit d'un graphe orienté et étiqueté semblable aux graphes de de Bruijn introduits précédemment. Il vérifie la condition (1). Le lecteur connaissant la théorie des automates pourra remarquer qu'il s'agit en fait d'un automate fini déterministe pour lequel on ne spécifie pas l'état initial et l'ensemble des états finals. C'est d'ailleurs dans le langage de la théorie des automates que s'exprime le plus souvent les résultats décrits ici.

contrairement au graphe de droite, le graphe de transitions de gauche ne possède aucun mot synchronisant. Pour une preuve rigoureuse, on pourra utiliser les résultats de la section 3.4 ou le théorème 10.

3.2 Conjecture de Černý

Un graphe de transitions est *synchronisant* s'il admet un mot synchronisant. La conjecture de Černý⁷ affirme que si un graphe de transitions à n sommets est synchronisant, alors il admet un mot synchronisant de longueur au plus $(n-1)^2$.

Exemple 8. Dans cet exemple, on considère le graphe de transitions à 4 sommets repris à la figure 6. On vérifie que le mot $abbbabbba$ est une suite de couleurs de longueur $9 = (4-1)^2$ synchronisante (on aboutit toujours dans le sommet 3). On peut vérifier (simplement en passant en revue toutes les suites de longueur inférieure) qu'il n'existe aucune suite synchronisante plus courte. Cet exemple

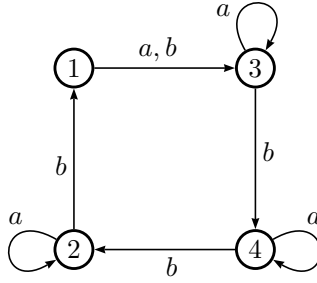


FIG. 6 – Un graphe de transitions synchronisant.

montre donc que, si la conjecture s'avère vraie, alors la borne $(n-1)^2$ ne peut pas être améliorée.

Proposition 9. *Un graphe de transitions est synchronisant si et seulement si pour tous $p, q \in Q$, il existe un mot m tel que $p.m = q.m$.*

La conjecture de Černý n'est toujours ni démontrée, ni réfutée. On ne connaît d'ailleurs que peu de graphes synchronisants à n sommets dont un mot synchronisant le plus court, comme dans l'exemple 8, est de longueur $(n-1)^2$. Le plus souvent, on dispose d'un mot synchronisant de longueur $< (n-1)^2$.

Assez facilement⁸, on peut se convaincre de l'existence d'une borne exponentielle guère satisfaisante : si un graphe de transitions à n sommets est synchronisant, alors il admet un mot synchronisant de longueur au plus k^n . Cependant, à ce jour, on dispose du résultat suivant généralement attribué à Jean-Eric Pin [12]. Pour les détails complets, on lira l'excellent survol [16].

Théorème 10. *Si un graphe de transitions à n sommets est synchronisant, alors il admet un mot synchronisant de longueur au plus $(n^3 - n)/6$.*

Pour des cas particuliers de familles de graphes de transitions, i.e., en imposant des hypothèses plus fortes, on connaît de meilleures bornes, cf. par exemple la remarque 18.

⁷Jan Černý, informaticien slovaque, introduisit en 1964 la notion d'automate synchronisant.

⁸Si on pense à la construction par sous-ensembles d'états, classique en théorie des automates.

3.3 Application

La notion de graphe synchronisant trouve par exemple des applications dans les chaînes de montage automatisées devant assembler diverses pièces. En effectuant une suite finie de mouvements, des bras robotisés amènent une pièce dans une configuration déterminée et ce, quelle que soit l'orientation qu'avait la pièce sur le tapis roulant de la chaîne de montage. Ainsi, le robot peut poursuivre le montage, la pièce étant, à coup sûr, dans le bon sens et on évite ainsi l'emploi de senseurs coûteux.

Cette notion est aussi utile pour des machines à relais ou des systèmes discrets, lorsqu'on ne sait pas dans quel état se trouve la machine (on observe uniquement les sorties produites) ; imposer la lecture d'un mot synchronisant permet de ré-initialiser le système.

3.4 Calcul matriciel

Définition 11. A un graphe de transitions $\mathcal{A} = (Q, \Sigma, \delta)$ ayant n sommets, on associe une matrice $n \times n$ pour chaque couleur $\sigma \in \Sigma$. Soit M_σ la matrice dont l'élément $M_{i,j}$ vaut 1 si et seulement si il existe un arc de couleur σ joignant i à j .

Pour le graphe de gauche à la figure 5, on dispose des matrices

$$M_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } M_b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Pour “ceux qui savent”, il s'agit en fait des matrices d'adjacence des graphes repris à la figure 7 et obtenus en ne considérant respectivement que les arcs de label a ou b .

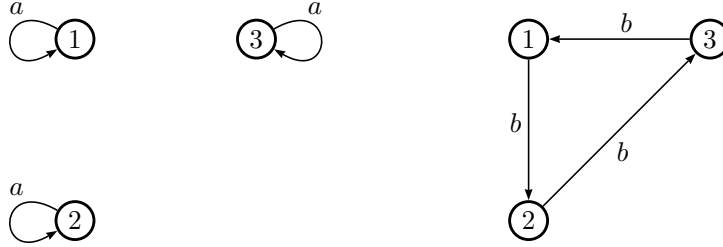


FIG. 7 – On ne considère que les arcs de label a (resp. b).

Pour le graphe de droite à la figure 5, on dispose des matrices

$$N_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } N_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Proposition 12. Soient $\mathcal{A}$ un graphe de transitions ayant Σ pour ensemble de couleurs et pour tout $\sigma \in \Sigma$, on considère la matrice M_σ de la définition 11. Soit $m = \sigma_1 \sigma_2 \cdots \sigma_t$ un mot sur Σ . L'élément i, j de la matrice

$$M_{\sigma_1} M_{\sigma_2} \cdots M_{\sigma_t}$$

vaut 1 si et seulement si partant de i , on aboutit en j en suivant le chemin prescrit par $\sigma_1\sigma_2\cdots\sigma_t$. En particulier, m est synchronisant si $M_{\sigma_1}M_{\sigma_2}\cdots M_{\sigma_t}$ contient une colonne formée exclusivement de 1.

Pour le graphe de droite de la figure 5, le calcul

$$N_b N_a N_a N_b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

montre que le mot $baab$ est un mot synchronisant. Pour le graphe de gauche de la figure 5, on calcule

$$M_b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad M_b^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{et} \quad M_b^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Puisque M_a est la matrice identité, on en conclut qu'un produit quelconque (mais fini) de facteurs M_a et M_b est égal à l'une des matrices M_a , M_b ou M_b^2 . Ceci prouve donc que le graphe en question n'est pas synchronisant.

En utilisant le théorème 10, on dispose d'un algorithme, i.e., d'une méthode "automatique" (mais fastidieuse), permettant de décider si un graphe arbitraire est ou non synchronisant. Soit un graphe de transitions à n sommets et k couleurs d'arcs. On passe en revue tous les mots de longueur au plus $N = (n^3 - n)/6$. Il y en a

$$k^{N(N+1)/2}.$$

Si on détecte que l'un de ces mots est synchronisant, la procédure s'achève : le graphe est évidemment synchronisant. Si par contre, après avoir réalisé chacun des produits, il s'avère qu'aucun mot n'est synchronisant, on peut, en considérant la contraposée du théorème 10, conclure que le graphe en question n'est pas synchronisant : si aucun mot de longueur au plus N n'est synchronisant, alors le graphe de transitions n'est pas synchronisant.

3.5 The Road Coloring Problem

Si l'on dispose d'un graphe (fini) orienté k -régulier, c'est-à-dire où chaque sommet possède le même demi-degré sortant k (on a un même nombre k d'arcs issus de chaque sommet du graphe), alors on peut se poser la question suivante : *est-il possible de colorer les arcs du graphe de façon à le rendre synchronisant ?* Ainsi, au départ, on dispose d'un graphe sans étiquette et il faut, si possible, déterminer un étiquetage permettant la synchronisation.

Exemple 13. Si on considère le graphe 2-régulier repris à la figure 8, nous savons qu'on peut le rendre synchronisant. Il suffit de considérer le coloriage des arcs du graphe de transitions de droite à la figure 5.

Avant d'énoncer un résultat (dont il aura fallu attendre près de trente ans pour en obtenir la preuve), deux définitions sont nécessaires.

Définition 14. Un graphe orienté est *fortement connexe* si pour tout couple (p, q) de sommets, il existe une suite d'arcs allant de p à q . Autrement dit, pour tout sommet d'origine et pour tout sommet d'arrivée, il existe un chemin les joignant.

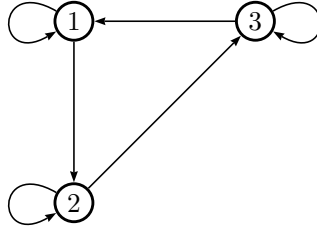


FIG. 8 – Un graphe orienté 2-régulier.

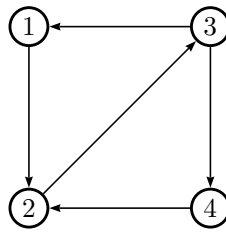


FIG. 9 – Un graphe orienté fortement connexe.

Le graphe de la figure 10 n'est pas fortement connexe. Il n'existe aucune suite d'arcs joignant 4 à 1.

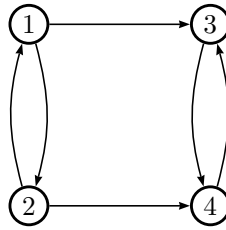


FIG. 10 – Un graphe orienté non fortement connexe.

Définition 15. Un graphe fortement connexe est *apériodique* si le plus grand commun diviseur des longueurs de ses cycles vaut 1.

Par exemple, on remarque que les cycles du graphe de la figure 11 sont tous de longueur paire : $1 \rightarrow 3 \rightarrow 4 \rightarrow 2 \rightarrow 1$, $3 \rightarrow 4 \rightarrow 3$ et $1 \rightarrow 3 \rightarrow 4 \rightarrow 3 \rightarrow 4 \rightarrow 2 \rightarrow 1$ sont des cycles de longueurs respectives 4, 2 et 6...

Par contre, le graphe de la figure 12 est apériodique car on dispose des cycles $1 \rightarrow 3 \rightarrow 4 \rightarrow 2 \rightarrow 1$ et $3 \rightarrow 4 \rightarrow 5 \rightarrow 3$ de longueurs respectives 3 et 4. Par conséquent, le plus grand commun diviseur des longueurs des cycles ne peut être que 1 (le pgcd de 3 et 4).

On peut montrer qu'un graphe de transitions synchronisant, fortement connexe et k -régulier est toujours apériodique⁹. Le résultat suivant a été conjecturé

⁹Dans un graphe fortement connexe non apériodique, les longueurs des chemins joignant

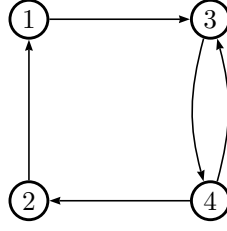


FIG. 11 – Un graphe orienté non apériodique.

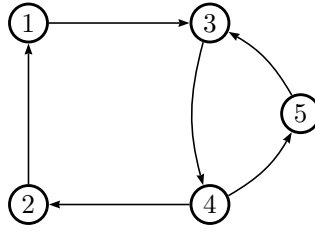


FIG. 12 – Un graphe orienté apériodique.

par Adler, Goodwin et Weiss en 1977 [3] et prouvé en 2007 par Avraham Trahtman.

Théorème 16 (Trahtman [15]). *Tout graphe fini orienté k -régulier, fortement connexe et apériodique possède un coloriage de ses arcs qui en fait un graphe de transitions synchronisant.*

Exemple 17. La figure 13 présente un graphe fini orienté 2-régulier fortement connexe et apériodique. La figure 14 fournit un coloriage des arcs et on peut vérifier que *bbabbabba* et *baabaabaa* sont deux mots synchronisants.

Remarque 18. Sous les hypothèses du théorème de Trahtman, la conjecture de Černý est vérifiée : un graphe à n sommets dispose toujours d'un coloriage avec un mot synchronisant de longueur au plus $n(n-1)/2$ et cette borne est bien inférieure à $(n-1)^2$, pour tout n .

4 Conclusion

Nous avons rencontré deux types de propriétés de localisation. Imaginons un agent parcourant un graphe orienté et étiqueté. Par exemple, dans un graphe de de Bruijn, connaître un nombre suffisant de labels du chemin suivi par l'agent fournit avec précision sa position dans le graphe. D'autre part, dans le cas des

deux sommets peuvent être décrites précisément en fonction du pgcd des longueurs des cycles, appelé *période du graphe*. Par exemple, si on considère le graphe de la figure 11, les chemins joignant 1 à 2 sont de longueur $3 + 2n$, $n \in \mathbb{N}$. Par contre, les chemins joignant 3 à 2 sont de longueur $2 + 2m$, $m \in \mathbb{N}$. Par conséquent, 2 ne sera un sommet où peut se faire la synchronisation puisqu'il ne peut pas être atteint par un même mot depuis 1 et 3. On peut, par le même raisonnement, montrer qu'un phénomène analogue se produit pour chaque sommet.

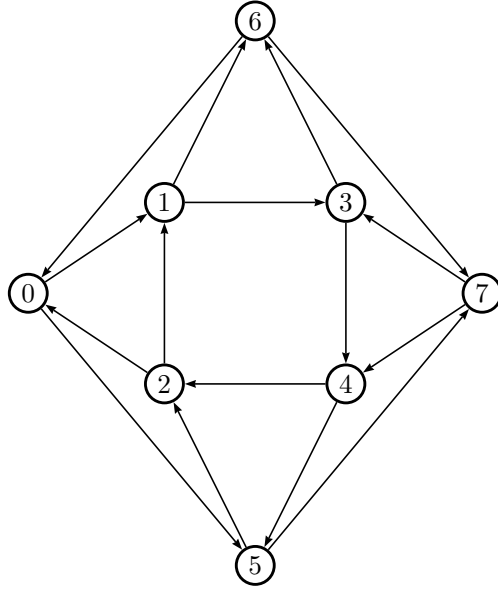


FIG. 13 – Un graphe orienté.

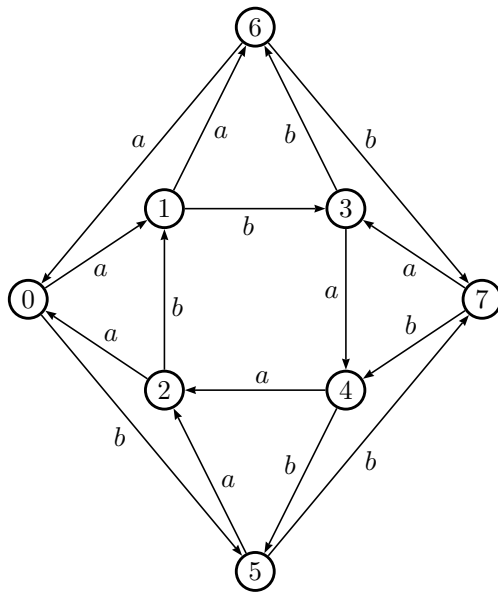


FIG. 14 – Un graphe de transitions synchronisant.

graphes synchronisants, imposer à un agent de suivre un chemin prescrit par une suite de labels amène inévitablement l'agent dans une position unique.

Références

- [1] T. van Aardenne-Ehrenfest, N. G. de Bruijn, Circuits and trees in oriented linear graphs, *Simon Stevin* **28** (1951), 203–217.
- [2] D. Acheson, *1089 and all that*, Oxford University Press (2002).
- [3] R. L. Adler, L. W. Goodwyn, B. Weiss, Equivalence of topological Markov shifts, *Israel J. Math.* **27** (1977), 49–63.
- [4] N. G. de Bruijn, A combinatorial problem, *Nederl. Akad. Wetensch., Proc.* **49** (1946), 758–764, *Indagationes Math.* **8** (1946), 461–467.
- [5] J. Černý, Poznámka k. homogénnym experimentom s konečnými automatmi. *Matematicko-fyzikálny Casopis SAV* **14** (1964), 208–215.
- [6] J. Černý, A. Pirická, B. Rosenauerova, On directable automata, *Kybernetika* **7** (1971), 289–298.
- [7] P. Diaconis, Mathematics and Magic Tricks, Clay public lecture, http://www.claymath.org/public_lectures/diaconis.php
- [8] Hiéronymus, *Nouveaux tours extraordinaires de mathémagique*, Ellipses, Paris, (2009).
- [9] E. Moreno, On the theorem of Fredricksen and Maiorana about de Bruijn sequences, *Advances in Applied Math.* **33** (2004), 413–415.
- [10] D. Perrin, *Voyage au pays des automates : le coloriage des routes*, Collège de France, Cours informatique et sciences numériques, Gérard Berry, décembre 2009.
- [11] J.-E. Pin, Sur un cas particulier de la conjecture de Černý, *ICALP, Lect. Notes Comput. Sci.* **62**, 345–352, Springer, Berlin, (1978).
- [12] J.-E. Pin, On two combinatorial problems arising from automata theory, *Ann. Disc. Math.* **17** (1983), 535–548.
- [13] A. Ralston, de Bruijn sequences—a model example of the interaction of discrete mathematics and computer science, *Math. Mag.* **55** (1982), 131–143.
- [14] M. Rigo, les codes correcteurs, Printemps des Sciences 2009, version disponible sur <http://www.discmath.ulg.ac.be/mam/>
- [15] A. Trahtman, The road coloring problem, à paraître dans *Israel J. Math.*
- [16] M. Volkov, Synchronizing automata and the Černý's conjecture, in *Language and Automata Theory and Applications Second International Conference, LATA 2008, Tarragona, Spain*, *Lect. Notes Comp. Sci.* **5196** (2008), 11–27.
- [17] E. Zeckendorf, Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombre de Lucas, *Bull. Soc. Roy. Sci. Liège* **41** (1972), 179–182.