Semi-anneaux et algorithmes sur les graphes

P. Simonnet et P. Delfini

Le 13 décembre 2003

Préambule

Le document ci-joint est destiné aux professeurs de Mathématiques du secondaire de l'académie de Corse qui nous ont fait le plaisir d'assister au stage «Semi-anneaux et algorithmes sur les graphes». Le document est une ébauche, relecture et commentaires sont les bienvenus. Ce document a été entièrement tapé en Latex par Pierre Delfini. Le contenu a été enseigné de nombreuses fois par moi même en Licence de Mathématiques, DESS d'informatique, IUP d'informatique, Deug MIAS depuis l'année 1993, date de ma nomination à l'Université de Corse. Les choses racontées ici m'ont été apprises au Laboratoire d'Informatique Théorique et Programmation, Laboratoire des Universités Paris 6 et Paris 7. Faisons un peu de généalogie, Maurice Nivat mon directeur de thèse, fut le directeur du LITP, et le directeur de thèse de Maurice Nivat fut Marcel Paul Schutzenberger grand promoteur en France des automates, des monoïdes, et des semi-anneaux, et plus généralement de l'algébrisation de la combinatoire. Pour l'ex LITP Jacques Sakarovitch la théorie des automates finis est l'algèbre linéaire de l'informatique. Le mémoire suit cette orientation.

Le prétexte à ces journées de formation est le nouveau programme de spécialité Mathématiques des terminales ES. On y introduit, par la pratique, sous forme d'exemples et sans démonstration, des graphes et des algorithmes sur ces graphes. Bref des graphes de manière empirique et concrète. On ne crée rien sans rien, venons en tout de suite aux références. Pour le programme lui même nous avons consulté [9]. Pour ce qui est des graphes une référence classique est le livre de Claude Berge [3], ainsi que [11] écrit par Claude Berge sous un pseudonyme. Pour l'algorithmique nous avons utilisé les trois livres [1, 2, 4], notre chapitre 3 et notre chapitre 4 sont directement issus du chapitre 26 de [4] et du chapitre 4 de [2]. Le document [6] consacré aux graphes et à la complexité est d'une grande clarté. Une très bonne présentation des graphes et des automates a été faite par le groupe IREM d'Aix Marseille [7]. Elle suit à la ligne le programme de spécialité maths d'ES et est bourrée de compléments à destination des professeurs. Notre présentation ici est à l'inverse de celle de Marseille, nous sommes abstraits, nous faisons des preuves et de l'algèbre. Mais nous avons deux guides :

1 Nous appliquons toujours la même formule de récurrence nous changeons juste de semi-anneaux (nous faisons de la programmation dynamique)

2 Nous sommes Fibonaccistes, essayez de repérer les allusions cachées au fil des pages.

Si à la fin de cette journées vous dites : «ces hommes font partie d'une résurgence de la secte pythagoricienne (pentagone, pentagramme, nombre d'or, anthyphérèse, irrationnalité, Hippase de Métaponte)» ou «On a bien vu que ce magicien sortait tous les lapins de sa manche» nous aurons gagné notre pari.

Pour le lecteur curieux d'automates nous lui conseillons la nouvelle bible rédigée par Jacques Sakarovitch [12] récemment parue.

Corte le 2 décembre 2003
Pierre Simonnet

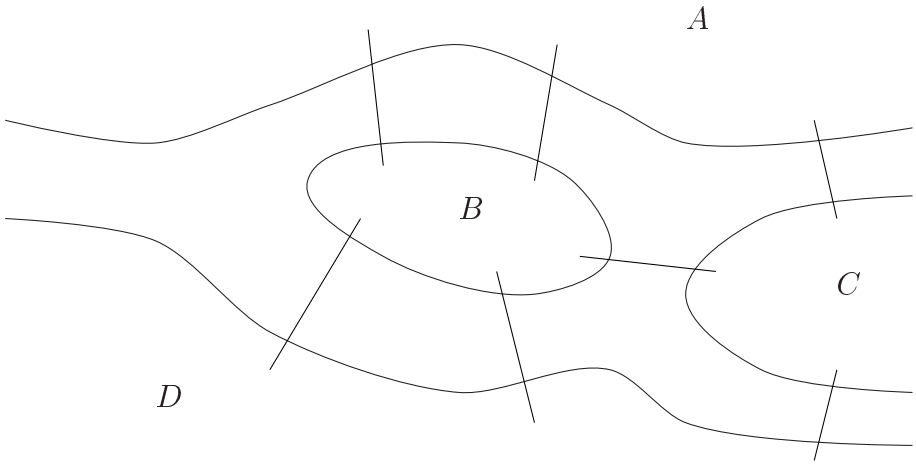
Table des matières

Chapitre 1

Graphes : exemples et notions de base

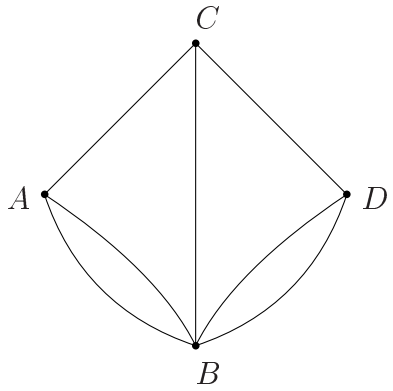
1.1 Introduction

Tous les traités sur la théorie des graphes s'accordent à dire qu'elle a vu le jour en 1736 quand Euler résolut le problème des ponts de Königsberg. Nous ne résisterons pas au plaisir de présenter ce fameux problème. Au dix-huitième siècle donc, les habitants de la ville de Königsberg (alors en Prusse, aujourd'hui Kaliningrad en Russie) aimaient se promener le dimanche sur les bords de la rivière Pregel. Cette rivière entourant deux îles était alors enjambée par sept ponts suivant le schéma ci-dessous.



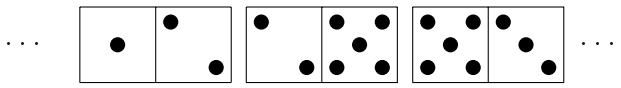
Les promeneurs se demandaient s'il existait un trajet leur permettant d'emprunter les sept ponts une fois et une seule. Le jeu consistait à essayer toutes les possibilités sur les lieux mêmes. Euler démontra qu'un tel circuit est impossible. Sa démonstration se base sur une représentation simplifiée des lieux, un graphe. Les deux îles et les deux rives sont représentées par quatre points ou sommets et les sept ponts sont représentés par des arêtes

suivant le schéma ci-dessous.

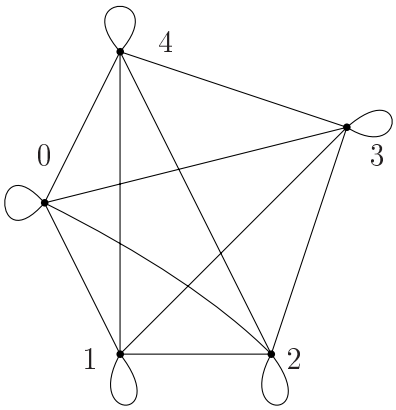


Dans le vocabulaire actuel de la théorie des graphes, le problème revient à rechercher l'existence d'une chaîne eulérienne, c'est à dire un chemin qui passe par tous les sommets en décrivant chaque arête une fois et une seule. Le théorème d'Euler donne une condition nécessaire et suffisante d'existence d'un tel circuit (initialement Euler n'avait donné qu'une condition néc essaire).

Restons dans le domaine des jeux et du divertissement avec le problème suivant. On dispose d'un jeu de dominos contenant une fois et une seule chaque paire de numéros. Peut-on ranger, dans l'ordre usuel de ce jeu, tous les dominos sur une seule ligne?

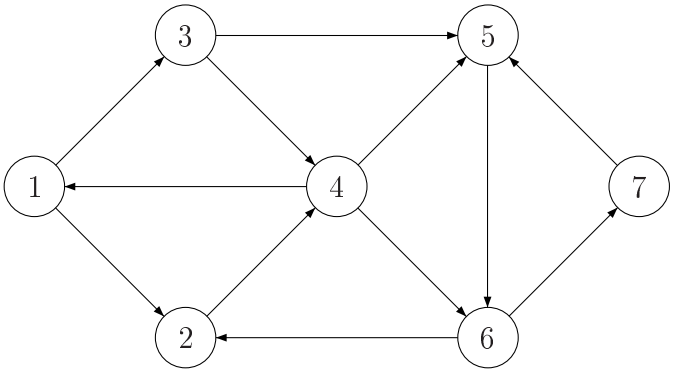


Le graphe qui modélise ce problème est le suivant. Ici on se restreint à un jeu qui ne comporte que $n = 4$ numéros et le blanc, sinon le graphe devient illisible!



Les $n + 1$ sommets représentent les n numéros et le blanc, chaque arête représente un (et un seul) domino. Les boucles représentent les dominos avec deux numéros identiques (on pourrait les supprimer puisqu'ils peuvent toujours s'intercaler). L'existence de solution(s) au problème est encore donnée par le théorème d'Euler, elle dépend de la parité du nombre n de numéros.

Voici maintenant un graphe qui peut représenter le plan d'une ville dans laquelle toutes les rues sont à sens unique. Les arêtes correspondent aux rues et les sommets aux carrefours. Le graphe est évidement orienté par le sens de circulation.



On peut se rendre compte (c'est moins évident quand il y a beaucoup de sommets et d'arêtes) qu'il est possible de relier deux points quelconques par un chemin. On dit que le graphe est connexe. On peut se demander quel est, par exemple, le nombre de chemins pour aller du point 1 au point 7 ou encore quel est le plus court chemin (en nombre d'arêtes) pour aller de 1 à 7.

Si de plus, on associe à chaque arête un nombre qui peut représenter dans notre exemple la distance d'un point à un autre, on peut rechercher la distance minimum entre deux points donnés.

Enfin, si l'on supprime les flèches dans le graphe par exemple en considérant une circulation à double sens, les mêmes types de questions peuvent alors se poser pour ce graphe non orienté.

Reprenons pour finir un exemple proposé par J. Sakarovitch dans [12], exemple que P. Simonnet raconte à ses étudiants de DEUG depuis de nombreuses années : le calcul du reste dans la division euclidienne par 3 d'un entier n écrit en base 2.

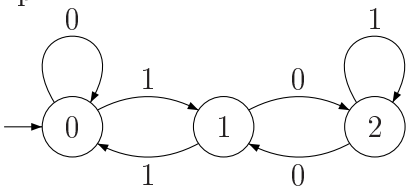
La représentation en base deux d'un entier n est une suite de 0 et de 1, notons la s. Cette suite s s'écrit encore $s = s'c$ où $c = 0$ ou 1 suivant que n est pair ou impair et s' est la suite que l'on devine qui représente l'entier n' tel que $n = 2 \times n' + c$. Si r est le reste de n' dans la division euclidienne par 3, $n' = 3q + r$, alors

$$n = 2 \times n' + c = 2 \times 3q + 2 \times r + c$$

L'entier n a le même reste que $2r + c$. Ainsi

si r vaut :	0	1	2
le reste de n tel que $s = s'0$ *est :*	0	2	1
le reste de n tel que $s = s'1$ *est :*	1	0	2

Ceci nous permet de représenter la «machine à diviser» sous la forme d'un graphe. Les sommets sont les trois restes possibles. L'état initial est le reste nul.



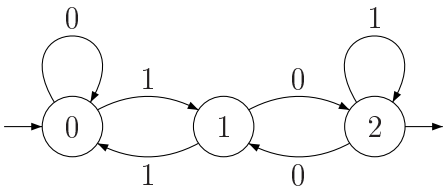
C'est là un cas de graphe étiqueté ou automate que nous allons étudier dans le chapitre 5.

Prenons un nombre entier au hasard $n = 34$, son écriture en base 2 est la suite 10010. Il est alors possible de donner son reste dans la division par 3, c'est le dernier sommet que l'on atteint en parcourant le graphe avec le mot 100010. On lit la suite de la gauche vers la droite. On part de l'état initial 0,

- on lit 1, la flèche étiquetée 1 amène en l'état 1
- on lit 0, la flèche étiquetée 0 fait passer de l'état 1 à l'état 2
- on lit 0, la flèche étiquetée 0 nous conduit de l'état 2 à l'état 1
- on lit 0, la flèche étiquetée 0 nous amène en l'état 2
- on lit 1, la flèche étiquetée 1 nous renvoie sur l'état 2
- on lit 0, la flèche étiquetée 0 va de l'état 2 en l'état 1

Le reste cherché est 1.

Si on fixe un état final, représenté par une flèche sortante, par exemple en 2 comme sur le dessin ci-dessous, on construit ainsi un automate capable de vérifier si un nombre écrit en base 2 est congru à 2 modulo 3.



On parle alors de mots, ou encore de langages reconnus par un automate donné. On généralise ce genre d'exemple à des problèmes de recherche de mots-clefs dans un texte qui trouvent leur utilité dans beaucoup de domaines tels que les traitements de texte (recherche et remplacement de mots), les moteurs de recherche sur internet, etc.

On pourrait continuer longtemps l'énumération de problèmes qui débouchent sur l'étude de graphes et qui restent accessibles à des élèves de terminale ES (option mathématiques). Le site du ministère de l'éducation nationale sur les programmes [10] présente une liste d'où les premiers exemples ci-dessus ont été tirés. Nous nous sommes inspirés aussi d'ouvrages classiques de base sur les graphes [5] et de travaux récents de certains IREM [6], [7] et bien évidement de manuels scolaires comme [9] .

Cette brève introduction historique montre que selon le problème rencontré, on utilise tel ou tel graphe. Une mise au point sur les terminologies s'impose. C'est la première difficulté étant donnée la diversité des types de graphes : graphes orientés, non orientés, simples ou non, pondérés par des nombres entiers ou par des nombres strictements positifs, étiquetés par des lettres et des mots, etc.

1.2 Définitions de base

Commençons par le plus simple: les graphes non orientés. Une première définition raisonnable semble être la suivante :

Définition 1.2.1 *(provisoire) Un graphe non orienté est un couple* (S,A) *où* S *est un ensemble (fini) non vide de points appelés sommets et* A *est un ensemble de parties à deux éléments de* S *appelées arêtes.*

Si s_i et s_j sont deux sommets, l'arête a qui les relie est notée $\{s_i,s_j\}$. On dit que s_i et s_j sont les extrémités de a et qu'ils sont adjacents. On dit que a est incidente à s_i et s_j.

Et nous rencontrons notre premier problème. Cette définition ne peut nous satisfaire entièrement car elle ommet le cas où il existe des arêtes reliant un sommet à lui-même comme dans l'exemple des dominos. De plus, elle ne peut décrire le problème des ponts de Königsberg où l'on trouve plusieurs arêtes entre deux sommets. Il faut la modifier. La définition suivante est extraite de [7].

Définition 1.2.2 *Un graphe non orienté est un couple (S,A) où $S = \{s_1, \ldots, s_n\}$ est un ensemble (fini) non vide de points appelés sommets et $A = \{a_1, \ldots, a_m\}$ est un ensemble dont les éléments sont appelés arêtes, tels qu'à chaque arête a_k sont associés deux éléments s_i et s_j de S, appelés ses extrémités. On note $a_k = [s_i,s_j]_k$.*

Les deux extrémités d'une arête peuvent être confondues, dans ce cas l'arête est appelée boucle. Il peut aussi y avoir plus d'une arête reliant deux sommets, dans ce cas on parle d'un multigraphe. Si le nombre maximal d'arêtes entre deux sommets distincts est 1 (resp : 2,3, ...) on parle d'un 1-graphe (resp : 2-graphe, 3-graphe, ...).

Définition 1.2.3 *Un graphe non orienté est dit simple s'il n'est pas un multigraphe et s'il ne possède pas de boucle.*

En fait dans notre première tentative de définition (1.2.1), nous avions décrit un graphe simple non orienté qui est un cas particulier, mais somme toute assez fréquent de graphe non orienté.

Définition 1.2.4 *Le degré $d(s)$ du sommet s d'un graphe non orienté est le nombre d'arêtes qui lui sont incidentes. Un sommet sera dit pair (resp : impair) si son degré est pair (resp : impair).*

Si le sommet s possède une boucle son degré est augmenté de 2. Le graphe des dominos possède des boucles en chacun de ses sommets.

On peut énoncer un premier résultat simple, appelé théorème des poignées de main.

Théorème 1.2.1 *La somme des degrés de tous les sommets d'un graphe est un nombre pair. Plus précisément, si $G = (S,A)$ avec $S = \{s_1, \ldots, s_n\}$, on a : $\sum_{i=1}^{n} d(s_i) = 2|A|$.*

Preuve Chaque arête est comptée deux fois, puisqu'elle a deux extrémités (quand c'est une boucle, elle est comptée deux fois).CQFD.

Ce théorème a comme conséquence immédiate le

Corollaire 1.2.1 *Le nombre de sommets impairs d'un graphe est toujours pair.*

Preuve Si on suppose que le nombre de sommets de degré impair est impair, on aboutit à une contradiction du théorème précédent. CQFD.

Dans les deux exemples des ponts de Königsberg et des dominos on peut aller d'un sommet à un autre dans les deux sens, par contre dans les deux autres exemples il y a un sens de parcours obligatoire (sens de la circulation dans le troisième exemple et lecture d'une lettre dans le cas du graphe étiqueté). Il faut introduire la notion de graphe orienté.

Définition 1.2.5 *Un graphe simple orienté est un couple (S,A) où S est défini comme précédemment et A est une partie de $S \times S$, c'est à dire un ensemble de couples d'éléments de S appelés arcs.*

Si s_i et s_j sont deux sommets, l'arc $a = (x_i,x_j)$ a pour extrémité initiale ou origine x_i et pour extrémité finale ou destination x_j. Cette définition admet l'existence de boucles, c'est à dire d'arcs reliant des sommets à eux-mêmes, mais elle exclut l'existence de plusieurs arcs reliant un sommet à un autre. Pour évoquer cela il faudrait définir les multigraphes orientés, or nous n'aurons pas besoin de cette notion ici.

Dans un graphe orienté on est amené à définir le demi-degré extérieur d'un sommet x_i, noté $d^+(x_i)$, qui est le nombre d'arc ayant x_i comme origine et le demi-degré intérieur noté $d^-(x_i)$, qui est le nombre d'arc ayant x_i comme extrémité finale. Le degré de x_i étant alors la somme de ces deux demi-degrés. Ces notions ne sont pas utiles ici.

1.3 Connexité

Les problèmes que nous avons vu dans l'introduction nous amènent tout naturellement à parcourir les graphes correspondants, à la recherche de chemins, de parcours, qui fourniront peut-être une solution. Il existe un vocabulaire précis pour décrire ces parcours, vocabulaire qui change suivant qu'on travaille dans un graphe orienté ou non orienté.

Définition 1.3.1 *Une chaîne d'un graphe non orienté est une suite (ordonnée) d'arêtes $(a_1,\ldots,a_n)$ telle que pour tout k, $1 < k < n$ l'arête a_k est reliée à a_{k-1} par une de ses extrémité et à a_{k+1} par son autre extrémité. La chaîne est fermée si son sommet origine et son sommet extrémité sont confondus. Un cycle est une chaîne fermée dont toutes les arêtes sont distinctes.*

On pourra regarder la définition proposée dans [7] afin de lever certaines ambiguïtés. La notion de chaîne sert à décrire la connexité d'un graphe, c'est à dire la possibilité de relier deux sommets quelconques.

Définition 1.3.2 *Un graphe non orienté est dit connexe si deux sommets quelconques peuvent être reliés par une chaîne.*

Un sous-graphe du graphe $G = (S,A)$ est un graphe $G' = (S',A')$ où $S' \subseteq S$ et $A' \subseteq A$ et tel que toutes les extrémités des arêtes de A' soient des éléments de S'.

Définition 1.3.3 *On appelle composante connexe d'un graphe un sous-graphe connexe maximal (qui n'est contenu dans aucun sous-graphe connexe).*

Remarquons que si $G = (S,A)$ est un 1-graphe (non orienté) on peut définir la relation binaire R sur S par :

$x\ R\ y$ si, et seulement si, il existe une chaîne d'extrémités x et y

C'est une relation d'équivalence dont les classes sont les composantes connexes.

On dispose d'un algorithme qui détermine les composantes connexes d'un graphe et qui permet de dire si le graphe est connexe. Il est en $O(n+m)$ où n et m sont respectivement le nombre de sommets et d'arêtes. Voir par exemple [6].

Définition 1.3.4 *On dit qu'une chaîne est eulérienne quand elle contient une fois et une seule chaque arête du graphe. Si de plus cette chaîne est un cycle, on dit que c'est un cycle eulérien.*

Le théorème d'Euler que nous donnons en annexe au chapitre 6 avec sa démonstration fournit une condition nécessaire et suffisante de l'existence d'une chaîne ou d'un cycle eulérien et résoud le problème des ponts de Königsberg ainsi que celui des dominos.

On a le même type de définitions pour les graphes orientés. Il suffit de remplacer «chaîne» par «chemin» et «cycle» par «circuit». Si on peut relier deux sommets quelconques par un chemin on dit que le graphe orienté est fortement connexe.

Chapitre 2

Structures algébriques

La théorie des groupes fut enseignée au Lycée en classe de seconde après la réforme des maths modernes. Un groupe est un ensemble muni d'une loi de composition interne associative possédant un élément neutre et tel que tout élément admet un inverse. Les groupes sont omniprésents en algèbre, notamment en algèbre linéaire ainsi qu'en géométrie. On peut même dire que les groupes sont présents dans toutes les branches des mathématiques. On les trouve aussi en physique et en chimie. Il existe pourtant une structure encore plus simple que la structure de groupe, celle de monoïde utilisée dans certaines branches des mathématiques et de l'informatique fondamentale.

2.1 Monoïdes : définitions et exemples

Définition 2.1.1 *Un ensemble M muni d'une loi de composition interne $*$, associative et possédant un élément neutre noté 1 est appelé monoïde. Le monoïde est dit commutatif si la loi est commutative. On note $< M, * ,1 >$.*

Un groupe est donc un monoïde dans lequel tout élément a un inverse.

Exemple 1 $< \mathbb{N},+,0 >$, $< \mathbb{N},\times,1 >$, $< \mathbb{Z},\times,1 >$ sont des monoïdes infinis, $< \mathbb{Z}/n\mathbb{Z},+,0 >$, $< \mathbb{Z}/n\mathbb{Z}, \times ,1 >$ sont des monoïdes finis.

Exemple 2 Tout groupe est évidemment un monoïde. Exemples : $< \mathbb{Z},+,0 >$, $< \mathbb{Q}^* ,\times,1 >$ etc, mais aussi $< \mathbb{Z}/n\mathbb{Z}, + ,0 >$ et $< (\mathbb{Z}/n\mathbb{Z})^*, \times ,1 >$ le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exemple 3 Si $(A, + ,\times)$ est un anneau unitaire d'élément neutre 1_A, $< A, \times ,1_A >$ est un monoïde.

Exemple 4 Soit E un ensemble non vide, on note $P(E)$ l'ensemble de toutes les parties de E. La réunion, $\cup$, est une loi de composition interne sur $P(E)$, associative et commutative. Pour tout $A \in P(E)$, $A \cup \emptyset = \emptyset \cup A = A$. L'ensemble vide, $\emptyset$, est l'élément neutre de la loi $\cup$. Par conséquent, $< P(E),\cup,\emptyset >$ est un monoïde commutatif. De même, $< P(E),\cap,E >$ est un monoïde commutatif.

Exemple 5 Soit E un ensemble, l'ensemble des applications de E dans E, noté E^E, est un monoïde si on le munit de la loi de composition des applications $\circ$. C'est le monoïde $< E^E, \circ ,1 >$ où 1 désigne l'application identique.

Exemple 6 Soit E un ensemble et F un espace vectoriel, l'ensemble $\mathcal{F}(E,F)$ des applications de E dans F muni de l'addition définie par :

$$\forall f,g \in \mathcal{F}(E,F)\ \forall x \in E \quad (f+g)(x) = f(x) + g(x)$$

est un monoïde. L'élément neutre étant l'application nulle (qui a tout $x \in E$ associe le vecteur nul de F).

Exemple 7 Soit K un corps, on note $M_n(K)$ l'ensemble des matrices carrées $n \times n$ à coefficients dans K, alors $< M_n(K), \times, 1 >$ est un monoïde non commutatif, l'élément neutre 1 étant la matrice identité.

2.2 Le monoïde libre A^*

On appelle «alphabet» un ensemble fini non vide A. Ses éléments sont des «lettres» avec lesquelles nous allons construire des «mots», suites finies de lettres. Le «mot vide» noté ε est le seul mot sans lettre. On note A^* l'ensemble des mots construits sur l'alphabet A. On peut munir A^* d'une loi de composition interne «.», appelée concaténation, de la manière suivante:

$$\forall u,v \in A^*, \quad u.v = uv$$

Si A est l'alphabet classique, si $u = mathé$ et $v = matique$, alors $u.v = uv = mathématique$. La concaténation est clairement associative. Le mot vide ε est l'élément neutre.

Théorème 2.2.1 *$< A^*,.,\varepsilon >$ est un monoïde, non commutatif dès lors que l'alphabet A possède au moins deux lettres. C'est le monoïde libre engendré par A.*

La longueur d'un mot est évidemment le nombre de lettres de la suite qui le compose. On note $|u|$ la longueur de $u \in A^*$. On a clairement :

$$|uv| = |u| + |v| \tag{2.1}$$

On a aussi $|\varepsilon| = 0$

Définition 2.2.1 *On appelle langage sur l'alphabet A tout ensemble de mots écrits avec les lettres de A.*

Un langage L de A est une partie de A^*, $L \subseteq A^*$. C'est un élément de l'ensemble $P(A^*)$, l'ensemble de toutes les parties de A^*.

2.3 Morphismes de monoïdes

Comme pour les groupes, il est utile de définir la notion de morphisme de monoïde et d'isomorphisme de monoïdes. Cette dernière permet en effet d'identifier deux monoïdes dont les éléments n'ont rien de commun mais qui ont la même structure.

Définition 2.3.1 *Soient $< M, *, 1_M >$ et $< N,.,1_N >$, deux monoïdes, une application de M dans N est un morphisme de monoïde si f conserve la loi de monoïde et envoie l'élément neutre sur l'élément neutre, c'est à dire :*
$\forall x,y \in M,\ f(x*y) = f(x).f(y)$ et $f(1_M) = 1_N$.
Si de plus, f est bijective on dit que c'est un isomorphisme de monoïdes ou encore que M et N sont isomorphes.

Un morphisme de groupe est simplement défini par la conservation de la loi de groupe, le fait que l'élément neutre du premier soit envoyé sur le second en découle. Ici par contre, il faut rajouter cette propriété. Cela tient au fait que dans un monoïde la notion de symétrique (ou d'inverse) n'a pas toujours de sens.

Le résultat suivant est un classique. C'est une extension aux monoïdes d'un théorème connu sur les groupes.

Théorème 2.3.1 *Si f est un isomorphisme de monoïdes de M dans N la bijection réciproque f^{-1} est aussi un (iso)morphisme de monoïdes.*

Preuve Comme f est une bijection on a :
$\forall z,t \in N, \quad \exists!\, x,y \in M, tels\ que \quad f(x) = z\ et\ f(y) = t$
c'est à dire :
$x = f^{-1}(z)$ et $y = f^{-1}(t)$.
Alors,

$$\begin{aligned} f^{-1}(z.t) &= f^{-1}(f(x).f(y)) \\ &= f^{-1}(f(x * y)) \quad \text{puisque f est un morphisme} \\ &= (f^{-1} \circ f)(x * y) = x * y \\ &= f^{-1}(z) * f^{-1}(t) \end{aligned}$$

Ceci prouve que f^{-1} est bien un morphisme. CQFD.

Exemple 1 L'application qui a tout mot u d'un alphabet A associe sa longueur $|u|$ est, en vertu de (2.1), un morphisme du monoïde $< A^*,.,\varepsilon >$ sur le monoïde $< \mathbb{N}, +, 0 >$.

Exemple 2 De même, si $|u|_a$ désigne le nombre de a que contient le mot u, l'application $|\ |_a : u \to |u|_a$ est un morphisme de monoïde de $< A^*,.,\varepsilon >$ dans $< \mathbb{N}, +, 0 >$.

Exemple 3 Soit E un ensemble non vide, on rappelle que l'on peut associer à chaque élément A de $P(E)$ un unique élément f_A de $\{0,1\}^E$ (l'ensemble des applications de E dans $\{0,1\}$ noté aussi plus simplement 2^E) qui est la fonction caractéristique de A :

$$\begin{array}{rccc} f_A : & E & \longrightarrow & \{0,1\} \\ & x & \longrightarrow & 1 \text{ si } x \in A \\ & & & 0 \text{ si } x \notin A \end{array}$$

L'application f qui à A associe f_A est une bijection de $P(E)$ dans 2^E. Définissons sur 2^E une loi de composition interne, $+$, en posant :

$$\forall f,g \in 2^E, \forall x \in E, \quad (f + g)(x) = f(x) + g(x)$$

où la somme du second membre est la somme de Boole, c'est à dire vérifie la règle :

$$\begin{array}{l} 0{+}0{=}0 \\ 0{+}1{=}1{+}0{=}1 \\ 1{+}1{=}1 \end{array} \tag{2.2}$$

Cette loi est associative et commutative (car l'addition booléenne l'est) et son élément neutre est 0, l'application qui prend la valeur 0 pour tout $x \in E$ (qui n'est autre que la fonction caractéristique de l'ensemble vide). Alors on a la

Proposition 2.3.1 *Le monoïde $< 2^E, +, 0 >$ est isomorphe à $< P(E), \cup, \emptyset >$. Tous deux sont commutatifs.*

On vérifie aisément que la bijection f est un morphisme de monoïdes. On peut identifier ces deux monoïdes et remplacer le symbole $\cup$ par $+$ comme nous le ferons par la suite. Ainsi nous n'hésiterons pas à parler du monoïde commutatif $< 2^E, \cup, \emptyset >$ ou $< 2^E, +, \emptyset >$.

2.4 Les monoïdes à deux éléments

Nous avons vu plus haut des exemples de monoïdes finis, ici nous allons montrer qu'il n'existe que deux monoïdes à deux éléments, à isomorphisme près. Nous allons illustrer cela par des exemples tirés de la logique mathématique. Une proposition P est vraie ou fausse, de même une proposition Q. On note V pour vrai et F pour faux. On peut définir à partir de cela d'autres propositions qui seront soient vraies soit fausses. La proposition «P ou Q» est vraie dès que P ou Q l'est. Elle n'est fausse que si P et Q sont fausses en même temps. La proposition «P et Q» n'est vraie que si P et Q sont vraies toutes les deux. On peut rajouter le «ou exclusif» qui sera vrai dans le cas où P est vraie et Q fausse et dans le cas où Q est vraie et P fausse. On notera «P ou$_e$ Q». On résume cela dans une table de vérité.

P	Q	V ou F	V et F	P ou$_e$ Q
V	V	V	V	F
V	F	V	F	V
F	V	V	F	V
F	F	F	F	F

Remplaçons V par 1 et F par 0 et modifions la syntaxe suivant les règles communément admises. Le «ou» devient $+$, le «et» devient $.$, le «ou$_e$» devient $\oplus$. On a alors :

$+$	0	1
0	0	1
1	1	1

$.$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

Dans la table du $\oplus$ nous reconnaissons l'unique groupe (unique à isomorphisme près) à deux éléments $(\mathbb{Z}/2\mathbb{Z},+)$. C'est donc à fortiori un monoïde.

Si on note $\mathbb{B} = \{0,1\}$ l'ensemble des booléens, la table du $+$ représente le monoïde $< \mathbb{B}, +, 0 >$, d'élément neutre 0, que nous avons rencontré plus haut en (2.2). Pour démontrer l'associativité de la loi $+$ sur $\mathbb{B}$ on peut compléter le tableau initial avec deux colonnes, l'une pour «(P ou Q) ou R», l'autre pour «P ou (Q ou R)» et voir qu'elles sont identiques. C'est ce que l'on fait ici avec la nouvelle syntaxe.

x	y	z	x+y	(x+y)+z	y+z	x+(y+z)
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	1	1	0	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

En regardant les tables du $\oplus$ et du $+$, il apparaît clairement que les deux monoïdes associés ne sont pas isomorphes. On peut remarquer que dans la table du $+$ 1 n'a pas d'inverse, ou encore que cette table n'est pas un carré latin (1 apparait deux fois sur une même ligne). Donc $< \mathbb{B}, +, 0 >$ n'est pas un groupe alors que la table de $\oplus$ est celle du groupe additif $\mathbb{Z}/2\mathbb{Z}$.

Quant au troisième tableau, celui du ., il représente lui aussi un monoïde, la loi est associative et le 1 est l'élément neutre. Nous aurions pu remarquer que ce n'est rien d'autre que la table de $(\mathbb{Z}/2\mathbb{Z}, \times)$. On le note $< \mathbb{B}, ., 1 >$.

Considérons l'application φ de $< \mathbb{B}, +, 0 >$ dans $< \mathbb{B}, ., 1 >$, telle que $\varphi(0) = 1$ et $\varphi(1) = 0$. De par sa construction, c'est une bijection. Elle est sa propre bijection réciproque : $\forall x \in \mathbb{B}$, $\varphi(\varphi(x)) = x$. De plus, on vérifiera sans difficulté que pour tous $x, y \in \mathbb{B}$,

$$\varphi(x + y) = \varphi(x).\varphi(y) \tag{2.3}$$

C'est un morphisme de monoïde.

Théorème 2.4.1 *Les monoïdes* $< \mathbb{B}, +, 0 >$ *et* $< \mathbb{B}, ., 1 >$ *sont isomorphes.*

Nous avons vu dans le théorème 2.3.1 que l'application réciproque $\varphi^{-1} = \varphi$ est aussi un morphisme de monoïdes. Par conséquent φ vérifie, pour tous $x, y \in \mathbb{B}$,

$$\varphi(x.y) = \varphi(x) + \varphi(y) \tag{2.4}$$

Remarque : Si nous remarquons que φ est la négation, les identités (2.3) et (2.4) ne sont rien d'autre que les lois de De Morgan :

$$\forall\, x, y \in \mathbb{B} \quad \overline{x + y} = \overline{x} \,.\, \overline{y} \qquad \overline{x \,.\, y} = \overline{x} + \overline{y}$$

Proposition 2.4.1 *Il existe, à isomorphisme près, uniquement deux monoïdes à deux éléments;* $< \mathbb{B}, +, 0 >$ *et* $< \mathbb{Z}/2\mathbb{Z}, +, 0 >$. *Ils sont tous les deux commutatifs.*

Preuve. Soit $M = \{e, a\}$ tel que $< M, +, e >$ soit un monoïde. Nous pouvons remplir en partie sa table, en utilisant le fait que e est le neutre.

+	e	a
e	e	a
a	a	?

Forcément le point d'interrogation ne peut prendre que la valeur e ou a, dans le premier cas on retrouve la table du groupe $< \mathbb{Z}/2\mathbb{Z}, +, 0 >$ et dans le second celle de $< \mathbb{B}, +, 0 >$. CQFD.

2.5 Semi-anneaux : définition et exemples

La structure de semi-anneau que nous allons présenter dans ce paragraphe est certainement moins connue que les structures plus classiques d'anneaux et de corps.

Définition 2.5.1 *Un ensemble* K *muni de deux lois de composition internes,* $+$ *et* $\times$, *contenant deux éléments* 0 *et* 1 *vérifiant :*

- $< K, +, 0 >$ *est un monoïde commutatif*
- $< K, \times, 1 >$ *est un monoïde*
- *la multiplication est distributive par rapport à l'addition à droite et à gauche*

– *0 est absorbant pour la multiplication* ($\forall x \in K, x \times 0 = 0 \times x = 0$)

est appelé un semi-anneau. On le note $< K, +, \times, 0, 1 >$. *Si de plus la multiplication est commutative on dit que c'est un semi-anneau commutatif.*

En voici quelques exemples.

Exemple 1 Le semi-anneau des entiers naturels $< \mathbb{N}, +, \times, 0, 1 >$.

Exemple 2 Tout anneau unitaire est évidemment un semi-anneau. Par exemple $(\mathbb{Z}, +, \times)$, l'anneau des entiers avec l'addition et la multiplication usuelles est à fortiori un semi-anneau que nous notons, en respectant la convention ci-dessus, $< \mathbb{Z}, +, \times, 0, 1 >$. De même, l'anneau des entiers modulo 2, $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est le semi-anneau noté $< \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1 >$.

Exemple 3 Le semi-anneau de Boole $< \mathbb{B}, +, ., 0, 1 >$. On vérifie grâce aux tables de vérité la distributivité du . sur le +. Ici la distributivité à gauche puisque le «et» est commutatif.

x	y	z	y+z	x.(y+z)	x . y	x. z	(x. y)+(x. z)
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Exemple 4 Reprenons l'ensemble $M_n(K)$ des matrices carrées à coefficients dans un corps ou dans un semi-anneau K. Alors $< M_n(K), +, \times, 0_n, I_n >$ où 0_n est la matrice nulle et I_n la matrice identité, est un semi-anneau non commutatif.

Exemple 5 Notons $\overline{\mathbb{N}}$ l'ensemble des entiers auquel on a rajouté le point à l'infini; $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$. On définit sur $\overline{\mathbb{N}}$ la loi de composition interne «*min*» par

$$\forall x, y \in \mathbb{N}, \quad min(x,y) = x \Longleftrightarrow x \leq y$$

$$\forall x \in \mathbb{N}, \quad min(x,\infty) = x$$

Cette deuxième propriété signifie que l'élément neutre de *min* est ∞. On étend l'addition des entiers à l'ensemble $\overline{\mathbb{N}}$ en posant, pour tout $x \in \mathbb{N}$,

$$x + \infty = \infty + x = \infty$$

et

$$\infty + \infty = \infty$$

C'est une loi de composition interne. Par suite $< \overline{\mathbb{N}}, min, +, \infty, 0 >$ est un semi-anneau commutatif appelé semi-anneau de Floyd.

Exemple 6 De la même manière que nous venons de définir la loi «*min*» on définit la loi de composition interne «*max*» sur $\overline{\mathbb{N}}$. Son élément neutre est 0. Donc $< \overline{\mathbb{N}}, max, min, 0, \infty >$ est un semi-anneau commutatif.

2.6 Morphismes de semi-anneaux

Il est intéressant de savoir si deux semi-anneaux donnés ont la même structure. Pour cela on définit la notion de morphisme et d'isomorphisme de semi-anneaux comme nous l'avons déjà fait pour les monoïdes. Pour ne pas allonger la liste des symboles, nous avons choisi de noter de la même façon les lois sur les deux semi-anneaux K et L dans la définition ci-dessous.

Définition 2.6.1 *Soient* $< K, +, \times, 0_K, 1_K >$ *et* $< L, +, \times, 0_L, 1_L >$ *deux semi-anneaux et* φ *une application de* K *dans* L. *On dit que* φ *est un morphisme de semi-anneaux si*

- φ *est un morphisme de monoïde de* $< K, +, 0_K >$ *dans* $< L, +, 0_L >$
- φ *est un morphisme de monoïde de* $< K, \times, 1_K >$ *dans* $< L, \times, 1_L >$

Autrement dit, φ vérifie

$\forall x,y \in K, \quad \varphi(x + y) = \varphi(x) + \varphi(y)$

$\varphi(0_K) = 0_L$

$\forall x,y \in K, \quad \varphi(x \times y) = \varphi(x) \times \varphi(y)$

$\varphi(1_K) = 1_L$

Définition 2.6.2 *Si de plus,* φ *est bijective on dit que c'est un isomorphisme de semi-anneaux ou encore que* K *et* L *sont isomorphes.*

Proposition 2.6.1 *Il n'y a que deux semi-anneaux à deux éléments à isomorphisme près. Le corps* $< \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1 >$ *et le semi-anneau de Boole* $< \mathbb{B}, +, ., 0, 1 >$.

Preuve Soit $< K, +, \times, 0, 1 >$ un semi-anneau à deux éléments. Posons $K = \{0,1\}$ où 0 et 1 sont respectivement élément neutre pour l'addition et la multiplication. Utilisons la définition d'un semi-anneau pour construire les tables des deux lois.

$\times$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	?

Comme 0 est absorbant et 1 est élément neutre de la multiplication pour un semi-anneau (par définition), la table de multiplication est entièrement déterminée. Pour la table d'addition nous avons vu plus haut qu'il y a deux possibilités pour $1 + 1$.

Si $1 + 1 = 0$, la table complète est la suivante

$+$	0	1
0	0	1
1	1	0

et on reconnaît le semi-anneau $< \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1 >$.

Si $1 + 1 = 1$, la table complète est la suivante

$+$	0	1
0	0	1
1	1	1

et on reconnaît le semi-anneau de Boole. CQFD.

Chapitre 3

Graphes et semi-anneaux

3.1 Graphe et relation binaire

Soit E un ensemble non vide, une partie R de $E \times E$ définit une relation binaire que nous appellerons aussi R, de la façon suivante :

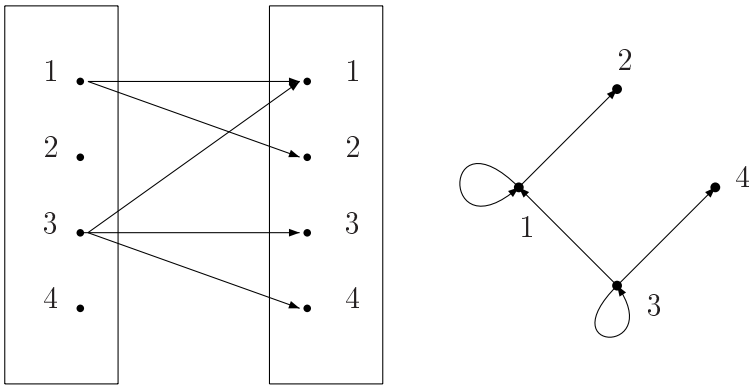
$$\forall x,y \ \in E, \quad xRy \Leftrightarrow (x,y) \in R$$

Définition 3.1.1 *Rappelons que la relation R est :*
réflexive si pour tous $x \in E$, xRx
symétrique si pour tous $x,y \in E$, xRy entraine yRx
transitive si pour tous $x,y,z \in E$, le fait d'avoir xRy et yRz entraine xRz.
Supposons E fini, de cardinal n. Pour simplifier posons $E = \{1,\ldots,n\}$. On peut représenter R soit par un diagramme sagittal, soit par un graphe orienté. Le graphe en question aura éventuellement des boucles en certains sommets, mais entre deux sommets il aura au plus un arc, c'est ce qu'on a appelé un 1-graphe.

Exemple Soit$E = \{1,2,3,4\}$ et R la relation définie par $R \subset E \times E$ tel que

$$R = \{(1,1),(1,2),(3,1),(3,3),(3,4)\}$$

Diagramme sagittal et graphe de R :



3.2 Le semi-anneau $2^{n\times n}$

Dans le chapitre précédent nous avons «assimilé» la partie R de $E \times E$ à un élément de $2^{E\times E}$. Comme $|E| = n$, nous écrirons $2^{n\times n}$ à la place de $2^{E\times E}$. L'ensemble des relations

binaires sur E peut donc s'identifier à $2^{n\times n}$ que nous allons munir de deux lois de composition internes pour en faire un semi-anneau...

Définition 3.2.1 *La somme ou réunion de deux relations binaires R et S sur E, définies par les éléments R et S de $E\times E$ est la relation binaire $T = R+S$ (ou $T = R\cup S$) définie par la partie T de $E\times E$ telle que $T = R\cup S$.*

En d'autres termes :

$$\begin{aligned} xTy &\Leftrightarrow (x,y)\in R\cup S \\ &\Leftrightarrow (x,y)\in R \text{ ou } (x,y)\in S \end{aligned}$$

c'est à dire

$$xTy \Leftrightarrow xRy \text{ ou } xSy \tag{3.1}$$

Nous avons déjà vu plus haut (cf. proposition 2.3.1) que $< 2^{n\times n}, \cup, \emptyset >$ est un monoïde commutatif.

Exemple Soit $E = \{1,2,3,4\}$, R la relation définie dans l'exemple ci-dessus, c'est à dire par $R = \{(1,1),(1,2),(3,1),(3,3),(3,4)\}$ et S la relation définie par $S = \{(1,1),(1,2),(2,1),(2,4),(3,1),(4,1)\}$. La somme est donné par :

$$R+S = \{(1,1),(1,2),(2,1),(2,4),(3,1),(3,3),(3,4),(4,1)\}$$

Définition 3.2.2 *Étant données deux relations R et S sur E, la relation binaire T telle que : $\forall x,y\in E$,*

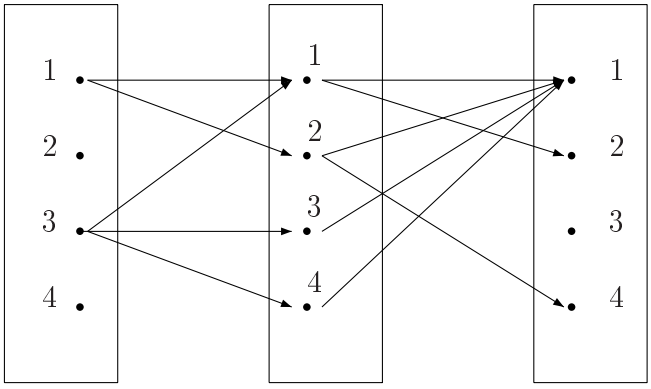
$$xTy \Leftrightarrow \exists z\in E \text{ tel que } xRz \text{ et } zSy$$

est appelée la composée de R par S. On la note $T = S\circ R$ ou encore sous forme multiplicative $T = SR$.

Attention à l'ordre !

Exemple Soient R et S les deux relations de l'exemple précédent. $T = SR$ est caractérisée par la partie

$$T = \{(1,1),(1,2),(1,4),(3,1),(3,2)\}$$



On remarque que la composée $V = R\circ S = RS$ est caractérisée par le sous-ensemble

$$V = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2),(4,1),(4,2)\}$$

de $E\times E$.

On définit ainsi une loi de composition interne sur $2^{n\times n}$. Cette loi est clairement associative, non commutative, et son élément neutre est la relation binaire identité, notée

I qui vérifie: $x\ I\ y$ si, et seulement si, $x = y$. Donc $< 2^{n\times n}, \circ, I >$ est un monoïde non commutatif.

Le lecteur se convaincra que la loi $\circ$ est distributive à droite et à gauche par rapport à $\cup$ et que $\emptyset$ est absorbant pour la loi $\circ$. D'où le théorème :

Théorème 3.2.1 $< 2^{n\times n}, \cup, \circ, \emptyset, I >$ *est un semi-anneau non commutatif.*

3.3 Représentation matricielle

A une relation binaire R sur $E = \{1, \ldots, n\}$ peut être associée une matrice carrée de dimension n que nous noterons $\mathcal{M}(R)$, constituée de 0 et de 1 uniquement.

Définition 3.3.1 *La matrice carrée $\mathcal{M}(R)$ de dimension n, dont les coefficients r_{ij} valent 1 si iRj, i.e. si $(i,j) \in R$, et 0 sinon, est appelée la matrice d'adjacence de la relation binaire R.*

Ainsi le coefficient $r_{i,j}$ vaut 1 quand il existe un arc joignant le sommet i au sommet j (ce sera le seul) dans le graphe de R et il prend la valeur 0 s'il n'y a pas d'arc entre i et j.

Exemple 1 La relation nulle, $\emptyset$, a pour matrice d'adjacence la matrice nulle 0_n puisque tout sommet n'est en relation avec aucun autre et la relation identité, I, a pour matrice I_n, la matrice identité, puisque dans ce cas chaque sommet est uniquement en relation avec lui-même.

Exemple 2 Reprenons les deux relations R et S du paragraphe précédent. Leurs matrices respectives sont

$$\mathcal{M}(R) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathcal{M}(S) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Proposition 3.3.1 *La somme ou réunion de deux relations correspond à la somme des deux matrices d'adjacence correspondantes, où la somme des coefficients est la somme dans $\mathbb{B}$, le semi-anneau de Boole.*

Preuve C'est clair.

Notons $\mathcal{M}$ l'application de $2^{n\times n}$ dans $M_n(\mathbb{B})$ qui à toute relation R associe sa matrice d'adjacence. Cette application vérifie donc :

$$\forall R,S\ \in 2^{n\times n}, \quad \mathcal{M}(R \cup S) = \mathcal{M}(R) + \mathcal{M}(S) \tag{3.2}$$

Dans l'exemple 1 ci-dessus nous avons vu que $\mathcal{M}(\emptyset) = 0_n$. Donc $\mathcal{M}$ est un morphisme de monoïdes, il est clairement bijectif, c'est un isomorphisme du monoïde $< 2^{n\times n}, \cup, \emptyset >$ sur le monoïde $< M_n(\mathbb{B}), +, 0_n >$.

Exemple La matrice d'adjacence de $T = R \cup S$, est donnée par $\mathcal{M}(T) = \mathcal{M}(R) + \mathcal{M}(S)$, soit

$$\mathcal{M}(T) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Proposition 3.3.2 *Soient R et S deux relations de matrices d'adjacence $\mathcal{M}(R)$ et $\mathcal{M}(S)$ respectivement, la relation $T = S \circ R$ a pour matrice d'adjacence $\mathcal{M}(T)$, que l'on obtient en faisant le produit matriciel $\mathcal{M}(R) \times \mathcal{M}(S)$ au sens du semi-anneau de Boole. C'est à dire en suivant les loi d'addition et de multiplication définies dans le semi-anneau de Boole.*

Attention à l'ordre!

Preuve Notons $r_{i,j}$ et $s_{i,j}$ les coefficients des matrices $\mathcal{M}(R)$ et $\mathcal{M}(S)$. Soient i et j deux points de E, si $k \in E$ vérifie iRk et kSj alors, iTj. Nous dirons que cela donne un chemin pour aller de i à j. Cela se traduit pour les coefficients par $r_{i,k} = 1$ et $s_{k,j} = 1$ et donc $r_{i,k} \times s_{k,j} = 1$. Dans le cas contraire, si i n'est pas en relation par R avec k ou si k n'est pas en relation par S avec j, l'un des deux coefficients est nul et le produit $r_{i,k} \times s_{k,j}$ est nul. On reproduit cela pour tous les $k \in E$, i.e. $1 \leq k \leq n$. Puis on fait la somme de tous les produits obtenus, ce qui donne un entier ≥ 0, $n_{i,j}$:

$$n_{i,j} = \sum_{k=1}^{n} r_{i,k} \times s_{k,j}$$

Mais, n'est-ce pas là la formule qui donne le produit matriciel $\mathcal{M}(R) \times \mathcal{M}(S)$? La matrice à coefficients entiers, $N = (n_{i,j})$, vérifie $N = \mathcal{M}(R) \times \mathcal{M}(S)$. Si le coefficient $n_{i,j}$ de N vaut 0 il n'y a aucun chemin qui va de i à j en passant par R puis par S, dans le cas contraire la valeur entière que prend $n_{i,j}$ donne le nombre de chemins qui vont de i à j par R puis S. Si on remplace cet entier par 1 cela donne exactement la matrice d'adjacence de la relation $T = S \circ R$ (on rappelle que pour l'addition booléenne $1 + 1 + \ldots + 1 = 1$). CQFD.

Exemple Pour les relations R et S de notre exemple, on obtient :

$$\mathcal{M}(T) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

alors que pour la relation $V = R \circ S$ on a :

$$\mathcal{M}(V) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

La proposition 3.3.2 signifie que

$$\mathcal{M}(S \circ R) = \mathcal{M}(R) \times \mathcal{M}(S)$$

De plus, dans l'exemple 1 ci-dessus nous avons vu que $\mathcal{M}(I) = I_n$. Par suite, $\mathcal{M}$ est un anti-morphisme bijectif du monoïde $< 2^{n \times n}, \circ, I >$ sur le monoïde $< M_n(\mathbb{B}), \times, I_n >$. Et finalement nous concluons par la

Proposition 3.3.3 *L'application $\mathcal{M}$ est un anti-morphisme bijectif du semi-anneau $< 2^{n \times n}, \cup, \circ, \emptyset, Id >$ sur le semi-anneau $< M_n(\mathbb{B}), +, \times, 0_n, I_n >$ des matrices carrées $n \times n$ à coefficients dans le semi-anneau de Boole.*

Si nous avions choisi la notation Anglo-Saxonne pour la loi de composition, nous aurions pu parler d'isomorphisme de semi-anneaux. En effet, les Anglais écrivent $x(fg)$ et fg quand nous écrivons $(g(f(x))$ et $g \circ f$. Pour cette raison nous identifierons par la suite la relation R et sa matrice d'adjacence, i.e. $\mathcal{M}(R) = R$.

Nous avons démontré au passage, lors de la preuve de la proposition 3.3.2,le résultat suivant :

Proposition 3.3.4 *Si l'on fait le produit matriciel $N = R \times S$ au sens usuel, c'est à dire en considérant les coefficients des matrices dans l'anneau des entiers, alors les coefficients n_{ij} de la matrice N, donnent le nombre de chemins distincts pour aller de i à j dans le diagramme saggital de $S \circ R$.*

En particulier si $R = S$, si l'on fait le produit matriciel $R \times R$ dans l'anneau des entiers on obtient le nombres de chemins de longueur deux dans le graphe de R.

Exemple Effectuons le produit $R \times S$ de notre exemple en nous plaçant cette fois dans l'anneau des entiers relatifs (en fait dans le semi-anneau $< \mathbb{N}, +, \times, 0, 1 >$). Cela donne la matrice

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

On peut vérifier sur la figure de la page 17 qu'il y a effectivement deux chemins qui mènent de 1 à 1, qu'il n'existe aucun chemin reliant 2 à 1, qu'il existe trois chemins qui vont de 3 à 1, etc.

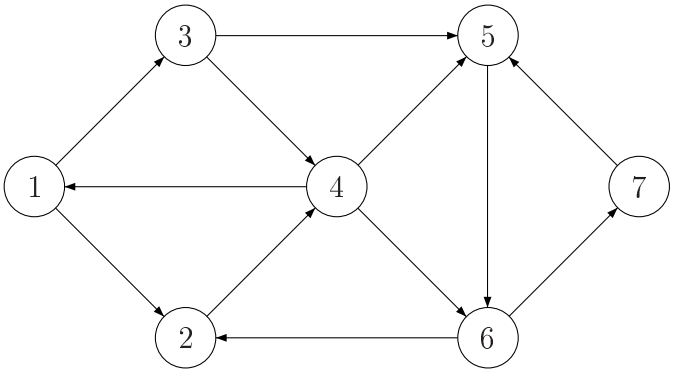
Remarque En pratique, on fera le produit matriciel dans l'anneau des entiers puis on remplacera les coefficients différents de 0 par 1 pour obtenir la matrice d'adjacence.

Corollaire 3.3.1 *Si G est un graphe de matrice d'adjacence R, la matrice produit R^n au sens usuel compte les chemins de longueur n alors que la matrice R^n pour le produit dans le semi-anneau de Boole, est la matrice d'adjacence des chemins de longueur n.*

Preuve On reprend la démonstration de la proposition 3.3.2 avec $R = S$. On obtient la matrice R^2. On fait ensuite le produit $R \times R^2$, etc. CQFD.

Exemple Elaboration de circuits touristiques (voir [10]). Pour traverser une chaîne de montagnes, il faut passer par plusieurs sommets, reliés entre eux par des cols que l'on ne peut franchir que dans un seul sens. Le graphe associé est celui que nous avons rencontré

au chapitre 1.



L'office de tourisme peut rechercher toutes les traversées qui partent d'un point donné et arrivent à un autre en trois, cinq ou huit étapes. La matrice d'adjacence de ce graphe étant donnée par :

$$R = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

il suffit de calculer R^3, R^5 et R^8.

$$R^3 = \begin{pmatrix} 2 & 0 & 0 & 0 & 2 & 3 & 0 \\ 0 & 2 & 1 & 0 & 0 & 1 & 1 \\ 0 & 3 & 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 3 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad R^5 = \begin{pmatrix} 0 & 2 & 0 & 7 & 5 & 0 & 2 \\ 3 & 0 & 0 & 1 & 4 & 5 & 0 \\ 4 & 0 & 0 & 1 & 5 & 7 & 0 \\ 1 & 8 & 3 & 0 & 1 & 5 & 5 \\ 0 & 3 & 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 4 & 3 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 2 & 0 \end{pmatrix}$$

$$R^8 = \begin{pmatrix} 0 & 13 & 2 & 26 & 19 & 2 & 11 \\ 11 & 1 & 0 & 7 & 17 & 19 & 1 \\ 15 & 1 & 0 & 8 & 22 & 26 & 1 \\ 7 & 30 & 11 & 1 & 8 & 24 & 19 \\ 1 & 11 & 4 & 0 & 1 & 6 & 7 \\ 0 & 7 & 1 & 15 & 11 & 1 & 6 \\ 4 & 0 & 0 & 1 & 5 & 7 & 0 \end{pmatrix}$$

Ainsi, sur la première ligne de chacune de ces matrices on lit le nombre de parcours possibles pour aller du point 1 aux autres points, en trois, cinq ou huit étapes. On peut vérifier rapidement les résultats sur le graphe (pour la puissance trois), mais pour les puissances supérieures cela devient plus difficile.

Chapitre 4

Algorithmes sur les graphes

Dans tout ce chapitre E est un ensemble fini non vide, $E = \{1, \ldots, n\}$ et R une relation binaire sur E. Cette relation est définie par une partie, notée aussi R, de l'ensemble produit cartésien $E \times E$. En d'autres termes, elle peut être représentée par un 1-graphe orienté $G = (E,R)$.

Nous allons présenter trois problèmes de la théorie des graphes qui peuvent être résolus par la même formule de récurrence (4.2). C'est l'algorithme de Roy-Warshall que l'on appliquera à chaque fois dans un semi-anneau différent en fonction du problème. Ce chapitre est essentiellement extrait de [2] et [4](qui renvoient eux même à un livre de Aho Hopcroft et Hullman de 1974, c'est dire que c'est pas tout jeune tout ça). La formule de récurrence utilisée ici est une version simplifiée de celle utilisée au chapitre suivant dans l'étude des automates, tout cela est bien mis en évidence dans [2], ce qui est normal J.Berstel a longuement travaillé avec M.P. Schutzenberger. M.P. Schutzenberger, rappelons le, est le grand promoteur en France des automates, des monoïdes, et des semi-anneaux, et plus généralement de l'algébrisation de la combinatoire.

4.1 Problème d'accessibilité, clôture transitive

Le problème que l'on aborde ici est un problème d'accessibilité. Etant donné deux sommets i et j du graphe G, existe-t-il un chemin de longueur finie partant de i et arrivant en j?

On peut éventuellement répondre à cette question en regardant le graphe G quand il y a un nombre raisonnable de sommets et d'arcs, mais dès que les sommets et les arcs deviennent trop nombreux (et cela arrive très vite) il faut envisager une autre méthode. Dans cette section nous allons définir une relation particulière à partir de R, la clôture transitive R^+ de R. Nous verrons alors que (par construction) la matrice d'adjacence de R^+ donne la réponse au problème d'accessibilité : si le coefficient $r^+_{i,j}$ vaut 0, il n'y a pas de chemin qui va de i à j et s'il vaut 1, il existe un chemin fini allant de i à j.

Convention Pour les commodités de l'écriture nous désignons par R à la fois la relation binaire R, le sous-ensemble de $E \times E$ qui lui est associé et la matrice d'adjacence.

Étant donnée une relation R, existe-t-il une relation binaire transitive contenant R qui soit minimale pour l'inclusion? C'est à dire, existe-t-il une relation binaire S telle que:

– S est transitive

- $S \supseteq R$, c'est à dire : $\forall x,y \in E$, $xRy \Rightarrow xSy$ ou en d'autres termes, toute arête de R est une arête de S
- Toute relation transitive contenant R contient S, c'est à dire: $\forall T \subset E \times E$, T transitive et $T \supseteq R$, alors $T \supseteq S$.

Définition 4.1.1 *Une telle relation S est appelée clôture transitive de R.*

Nous allons montrer qu'elle existe. Construisons par récurrence les relations R^k, $k \in \mathbb{N}$. Par convention

$R^0 = Id$

puis, pour tout $k \in \mathbb{N}$,

$R^{k+1} = R^k \circ R = R \circ R^k$

Posons ensuite

$$R^+ = \sum_{k=1}^{\infty} R^k = R + R^2 + \ldots + R^k + \ldots$$

Les loi $\circ$ et $+$ sont respectivement la loi de composition des relations et l'addition des relations vues au chapitre précédent. On peut donc interpréter cela en terme de parties de $E \times E$ ou en terme de matrices à coefficients dans le semi-anneau de Boole.

Proposition 4.1.1 *R^+ est la clôture transitive de R.*

Preuve Il est clair que R^+ contient R puisque $R^+ = R + R^2 + \ldots$.

Montrons que R^+ est transitive. Soient $x,y,z \in E$, tels que xR^+y et yR^+z. Cela signifie qu'il existe $p,q \in \mathbb{N}^*$ tels que xR^py et yR^qz. Il existe un chemin de longueur p pour aller de x à y et un chemin de longueur q qui va de y à z. Par conséquent, en reliant ces deux chemins, on obtient un chemin de longueur $p+q$ qui va de x à y, i.e. $xR^{p+q}z$ et par suite xR^+z.

Montrons que toute relation transitive T contenant R contient forcément R^+. Soient $x,y \in E$, xR^2y signifie qu'il existe $z \in E$ tel que xRz et zRy, et comme $R \subset T$, xTz et zTy d'où, par transitivité de T, xTy. Cela montre que $R^2 \subset T$. Par récurrence sur k, nous montrons que $\forall k \in \mathbb{N}$, $R^k \subset T$. Et par suite,

$$R^+ = \sum_{k=1}^{\infty} R^k \subset T$$

CQFD.

Le calcul de la clôture transitive R^+ se fait de la façon suivante :

$$\begin{aligned} &S_0 = R \\ &S_1 = S_0 \times R + R = R + R^2 \\ &S_2 = S_1 \times R + R = R + R^2 + R^3 \\ &\ldots \\ &S_{k+1} = S_k \times R + R = R + R^2 + \ldots + R^{k+2} \\ &\ldots \end{aligned} \tag{4.1}$$

Comme E est fini, $E = \{1, \ldots, n\}$, $E \times E$ est fini. Il y a donc un nombre fini de relations sur E. La suite croissante $(S_k)_{k \in \mathbb{N}}$ devient donc stationnaire au bout d'un nombre fini d'opérations.

Que signifie iR^+j? Cela veut dire qu'il existe un entier $m \geq 1$ pour lequel iR^mj, il existe un chemin de longueur m allant de i à j. On peut dire que iR^+j s'il existe un chemin de longueur non nulle de i vers j.

Proposition 4.1.2 *La relation R^+ est définie par: $\forall i,j \in E$, iR^+j si, et seulement si, il existe un chemin allant de i vers j.*

Remarquons encore que s'il y a un chemin pour aller du sommet i au sommet j, alors il y a forcément un chemin sans répétition de sommets, donc de longueur $\leq n-1$ pour aller de i à j (au plus, n sommets distincts sont reliés par $n-1$ arêtes).

En effet, soit un chemin de longueur supérieure à n, reliant i à j en passant deux fois par un même sommet k

$$i \to \ldots \to k \to \ldots \to k \to \ldots \to j$$

Supprimons le chemin intermédiaire entre les deux sommets k, le chemin restant

$$i \to \ldots \to k \to \ldots \to j$$

est un chemin joignant toujours i à j. En répétant cette opération chaque fois que l'on rencontre au moins deux fois le même sommet entre i et j, on obtient un chemin sans répétition de sommets, donc passant par au plus n sommets.

L'algorithme (4.1) ci-dessus dont l'entrée est la matrice R et qui donne en sortie la matrice $S = R^+$ de la clôture transitive, s'arrête au bout de $n-1$ itérations. Chaque itération effectue un produit matriciel dont la complexité est en $O(n^3)$, par suite l'algorithme est en $O(n^4)$.

4.2 Algorithme de Roy Warshall

Cet algorithme permet lui aussi de calculer la clôture transitive de la relation R, mais il est bien plus avantageux que le précédent puisqu'il est en $O(n^3)$.

Définition 4.2.1 *Pour $k \in \mathbb{N}$, $S^{(k)}$ est la relation binaire sur E définie par:*
$iS^{(k)}j$ si, et seulement si, il existe un chemin de i vers j passant uniquement par des sommets intermédiaires $\leq k$. On note $S^{(k)}$ les matrices Booléennes associées, i.e. telles que $S^{(k)}_{ij} = 1$ si $iS^{(k)}j$, $S^{(k)}_{ij} = 0$ sinon.

L'origine et l'extrémité du chemin ne sont pas considérés comme des sommets intermédiaires. On commence au rang 0:

Proposition 4.2.1 $S^{(0)} = R$.

Preuve Selon la définition $S^{(0)}_{ij} = 1$ si, et seulement si, il existe un chemin allant de i vers j ne passant que par des sommets intermédiaires ≤ 0, en d'autres termes, ne passant par aucun point intermédiaire. Donc $S^{(0)}_{ij} = 1$ si, et seulement si, il existe un chemin direct allant de i vers j, un arc, i.e. iRj. CQFD.

Proposition 4.2.2 *Les coefficients $S^{(k)}_{ij}$ de la matrice $S^{(k)}$ sont donnés par la relation de récurrence:*

$$S^{(k)}_{ij} \quad = \quad S^{(k-1)}_{ij} \quad + \quad \left(S^{(k-1)}_{ik} \quad \times \quad S^{(k-1)}_{kj} \right) \tag{4.2}$$

où les opérations $+$ et $\times$ sont les opérations Booléennes.

Preuve Il faut montrer que les deux quantités de part et d'autre de l'égalité prennent la valeur 1 en même temps (et donc la valeur 0 en même temps).

Supposons que le membre de droite de (4.2) est égal à 1. C'est une somme de deux booléens, or une telle somme ne vaut 1 que si ses deux membres valent 1 ou si l'un des deux vaut 1. Si $S_{ij}^{(k-1)} = 1$, i.e. s'il existe un chemin allant de i à j en passant par des sommets $\leq k-1$, schématisé par

$$i \underset{\leq k-1}{\longrightarrow} j$$

ce chemin est à fortiori un chemin qui joint i à j en ne passant que par des sommets $\leq k$. Donc $S_{ij}^{(k)} = 1$. Si $S_{ik}^{(k-1)} \times S_{kj}^{(k-1)} = 1$, cela ne peut se réaliser que si $S_{ik}^{(k-1)} = 1$ et $S_{kj}^{(k-1)} = 1$, i.e. s'il existe un chemin allant de i à k et un chemin allant de k à j, tous deux passant par des sommets $\leq k-1$, alors le chemin obtenu en les mettant bout à bout

$$i \underset{\leq k-1}{\longrightarrow} k \underset{\leq k-1}{\longrightarrow} j$$

va de i à j en passant par des sommets $\leq k$. Donc là encore $S_{ij}^{(k)} = 1$.

Réciproquement, supposons que le membre de gauche de (4.2) est égal à 1, $S_{ij}^{(k)} = 1$, i.e. il existe un chemin de i à j passant par des sommets $\leq k$. Deux cas de figure sont possibles. Soit aucun sommet intermédiaire ne dépasse $k-1$ et dans ce cas, $iS^{(k-1)}j$ ou encore $S_{ij}^{(k-1)} = 1$. Dans ce cas le membre de droite vaut 1. Soit l'un au moins des sommets intermédiaires vaut k. On peut schématiser cela de la manière suivante

$$i \underset{\leq k-1}{\longrightarrow} k \underset{\leq k-1}{\longrightarrow} k \longrightarrow \ldots \longrightarrow k \underset{\leq k-1}{\longrightarrow} k \underset{\leq k-1}{\longrightarrow} j$$

On peut faire sauter le chemin intermédiaire qui va du premier k au dernier k, cette boucle supprimée, il reste le chemin

$$i \underset{\leq k-1}{\longrightarrow} k \underset{\leq k-1}{\longrightarrow} j$$

La première partie

$$i \underset{\leq k-1}{\longrightarrow} k$$

signifie que $S_{ik}^{(k-1)} = 1$, la deuxième partie

$$k \underset{\leq k-1}{\longrightarrow} j$$

signifie que $S_{kj}^{(k-1)} = 1$. Par suite $S_{ik}^{(k-1)} \times S_{kj}^{(k-1)} = 1$ et le membre de droite vaut 1. Et ceci termine la démonstration. CQFD.

Il est clair que la suite $(S^{(k)})_{k\in\mathbb{N}}$ est stationnaire à partir du rang n puisque les sommets intermédiaires sont pris dans l'ensemble $\{1,\ldots,n\}$. Il s'en suit que :

Proposition 4.2.3 *La matrice $S^{(n)}$ est la matrice de la clôture transitive R^+ de R.*

Ajoutons le résultat suivant sur les coefficients. Il nous sera utile plus loin.

Lemme 4.2.1 *Pour tous $i,j,k \in E = [1,n]$, on a : $S_{ik}^{(k)} = S_{ik}^{(k-1)}$ et $S_{kj}^{(k)} = S_{kj}^{(k-1)}$*

Preuve Elle est évidente... Il suffit de reprendre la démonstration de la proposition précédente avec les schémas. CQFD.

La procédure Roy Warchall induite par la formule de récurrence (4.2) donnant $S_{ij}^{(k)}$ est la suivante :

début
$S := R$
pour $k = 1$ à n faire
pour $i = 1$ à n faire
pour $j = 1$ à n faire

$$S_{ij} := S_{ij} + S_{ik} \times S_{kj} \tag{4.3}$$

fin

On en déduit le résultat suivant, moins trivial qu'il n'y paraît car il faut vérifier que cette procédure donne en sortie la matrice $S = R^+$.

Proposition 4.2.4 *La procédure Roy Warshall calcule la matrice R^+ de la clôture transitive de R en $O(n^3)$ opérations élémentaires.*

Preuve On initialise : $S = R$. Puis on fait tourner l'algorithme. Supposons qu'on l'ai fait tourner avec succès jusqu'aux pas k, i, j, et donc que le terme $S_{i,j}$ de la formule (4.3), représentant le coefficient $S_{ij}^{(k)}$, soit le prochain terme à calculer. Il faut vérifier que l'on obtiendra la formule (4.2).

Dans (4.3), $S_{i,j}$ à initialement la valeur $S_{ij}^{(k-1)}$ calculée au pas précédent. Par contre, il y a deux possibilités pour le terme S_{ik}. En effet,

- si $j < k$, S_{ik} a la valeur $S_{ik}^{(k-1)}$ car il n'a pas encore été calculé au pas k
- si $j > k$, le terme S_{ik} a été calculé au pas k, il vaut donc $S_{ik}^{(k)}$

De même, il y a deux possibilités pour le terme S_{kj}.

- si $i < k$, S_{kj} prend la valeur $S_{kj}^{(k-1)}$
- si $i > k$, le terme S_{ik} a été calculé au pas k, il vaut donc $S_{kj}^{(k)}$

Mais, le lemme ci-dessus permet de conclure en retrouvant la formule (4.2). CQFD.

4.3 Problème de plus court chemin

Dans les cours d'informatique, le problème de plus court chemin (ou de coût minimal) est présenté de manière concrète à l'aide d'un réseau routier reliant des villes entres elles. Les villes sont les sommets d'un graphe et les routes reliant directement deux villes sont les arcs (ou des arêtes si on peut les parcourir dans les deux sens) du graphe. Ces arcs (arêtes) sont pondérés ou valués par des nombres positifs (éventuellement nuls) représentant par exemple une distance dans le cas du réseau routier. On exclue toute boucle sur un sommet (on pourrait éventuellement les accepter, elles seraient munies d'un poids >0 et par suite on les éviterait systématiquement puisqu'elles ne feraient que rallonger tout chemin les empruntant). De même, il n'existe qu'un arc (ou qu'une arête) pour relier deux sommets. Les graphes qui décrivent ce genre de situations sont donc des 1-graphes sans boucle d'après la terminologie donnée au chapitre 1.

Le problème est le suivant : étant données deux villes i et j, quelle est la distance minimale qui les sépare dans le réseau routier? On essayera aussi de déterminer un chemin (il se peut qu'il y en ait plusieurs) qui donne cette distance. La méthode proposée ici calcule la matrice coût minimum grâce à une formule de récurrence du type Roy-Warshall, c'est une matrice à coefficients dans le semi-anneau des entiers positifs. Il existe d'autres

méthodes, l'une des plus connues est l'algorithme de Dijkstra. Nous la présentons dans le dernier chapitre.

On définit une matrice coût L, à coefficients dans le semi-anneau $< \overline{\mathbb{N}}, min, +, \infty, 0 >$ vu au paragraphe 2.5 (exemple 4), en associant un coût à chaque arc. S'il existe une route directe pour aller de i à j, c'est à dire un arc (i,j), sa longueur (en Km) donne le coefficient $l_{i,j} \in \mathbb{N}$. S'il est impossible d'aller de i à j directement, c'est à dire s'il n'y a pas d'arc (i,j), on dit que le coût pour aller de i à j est infini, on pose $l_{i,j} = \infty$. Le coût pour aller de i à i est nul, $l_{i,i} = 0$.

Construisons par récurrence une matrice $S^{(k)}$, pour $k = 0, \ldots, n$, dont les coefficients $S_{ij}^{(k)}$ représentent le coût minimal pour aller de i à j en passant uniquement par des sommets intermédiaires $\leq k$.

$$S^{(0)} = L$$

La formule de récurrence qui permet de calculer les coefficients est :

$$S_{ij}^{(k)} = min\left(S_{ij}^{(k-1)}, S_{ik}^{(k-1)} + S_{kj}^{(k-1)}\right) \tag{4.4}$$

En effet, parmi les chemins allant de i à j, il y a ceux qui ne passent que par des sommets $\leq k-1$ dont l'un (ou plus) donne un coût minimum $S_{ij}^{(k-1)}$, puis il y a les chemins qui passent (sans répétition) par le sommet k et qui donnent un coût minimum $S_{ik}^{(k-1)} + S_{kj}^{(k-1)}$. Le minimum de ces deux quantités donne $S_{ij}^{(k)}$. L'algorithme prend fin au rang n puisqu'il n'y a qu'un nombre n de villes, par conséquent, la matrice $S^{(n)}$ est la matrice coût minimum. On peut donc écrire la procédure donnant le coût minimum :

début
$S := L$
pour $k = 1$ à n faire
pour $i = 1$ à n faire
pour $j = 1$ à n faire

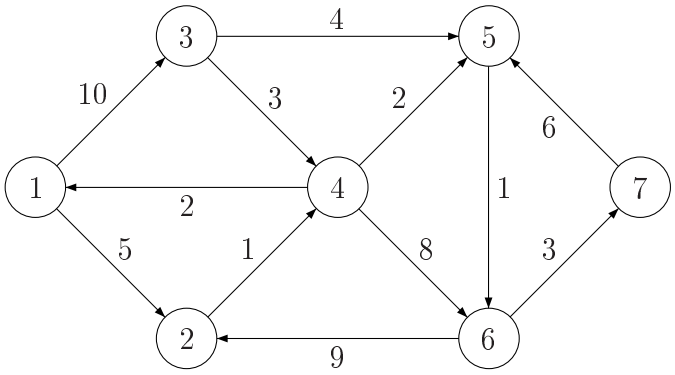
$$S_{ij} := min\left(S_{ij}\ ,\ S_{ik} + S_{kj}\right) \tag{4.5}$$

fin

Cet algorithme donne en sortie, pour tous i, j, le coût minimal pour aller du sommet i au sommet j, mais il ne donne pas le chemin correspondant. Il faut le coupler avec un autre algorithme, mais cela est un autre problème.

Exemple Traitons le cas du réseau routier déjà rencontré dans l'introduction en rajoutant pour chaque arc (arête) une valeur positive représentant une distance (ou coût). On peut

considérer le cas orienté et le cas non orienté.



La matrice coût pour le graphe orienté est la matrice carrée 7×7, L ci-dessous. Pour obtenir la matrice L' du même graphe non orienté il suffit de reproduire les valeurs $\neq \infty$ par symétrie par rapport à la diagonale principale.

$$S^{(0)} = L = \begin{pmatrix} 0 & 5 & 10 & \infty & \infty & \infty & \infty \\ \infty & 0 & \infty & 1 & \infty & \infty & \infty \\ \infty & \infty & 0 & 3 & 4 & \infty & \infty \\ 2 & \infty & \infty & 0 & 2 & 8 & \infty \\ \infty & \infty & \infty & \infty & 0 & 1 & \infty \\ \infty & 9 & \infty & \infty & \infty & 0 & 3 \\ \infty & \infty & \infty & \infty & 6 & \infty & 0 \end{pmatrix}$$

Un logiciel de calcul formel tel que Maple permet d'effectuer les itérations successives de cette matrice. On obtient au final :

$$S^{(7)} = \begin{pmatrix} 0 & 5 & 10 & 6 & 8 & 9 & 12 \\ 3 & 0 & 13 & 1 & 3 & 4 & 7 \\ 5 & 10 & 0 & 3 & 4 & 5 & 8 \\ 2 & 7 & 12 & 0 & 2 & 3 & 6 \\ 13 & 10 & 23 & 11 & 0 & 1 & 4 \\ 12 & 9 & 22 & 10 & 9 & 0 & 3 \\ 19 & 16 & 29 & 17 & 6 & 7 & 0 \end{pmatrix}$$

Dans le cas du graphe non orienté, la matrice initiale et la matrice de coût minimal sont données par :

$$S^{(0)} = L' = \begin{pmatrix} 0 & 5 & 10 & 2 & \infty & \infty & \infty \\ 5 & 0 & \infty & 1 & \infty & 9 & \infty \\ 10 & \infty & 0 & 3 & 4 & \infty & \infty \\ 2 & 1 & 3 & 0 & 2 & 8 & \infty \\ \infty & \infty & 4 & 2 & 0 & 1 & 6 \\ \infty & 9 & \infty & 8 & 1 & 0 & 3 \\ \infty & \infty & \infty & \infty & 6 & 3 & 0 \end{pmatrix} \quad S^{(7)} = \begin{pmatrix} 0 & 3 & 5 & 2 & 4 & 5 & 8 \\ 3 & 0 & 4 & 1 & 3 & 4 & 7 \\ 5 & 4 & 0 & 3 & 4 & 5 & 8 \\ 2 & 1 & 3 & 0 & 2 & 3 & 6 \\ 4 & 3 & 4 & 2 & 0 & 1 & 4 \\ 5 & 4 & 5 & 3 & 1 & 0 & 3 \\ 8 & 7 & 8 & 6 & 4 & 3 & 0 \end{pmatrix}$$

4.4 Un problème de hauteurs maximales de camions

On considère maintenant un réseau de villes reliées par des routes surmontées de ponts qui interdisent le passage à des camions dépassant une certaine hauteur. Le problème

consiste ici à rechercher la hauteur maximale autorisée pour aller d'une ville i à une ville j.

On définit une suite de matrices $(S^{(k)})_{k\in\mathbb{N}}$, à coefficients dans le semi-anneau $< \overline{\mathbb{N}}, max, min, 0, \infty >$ vu au paragraphe 2.5 (exemple 5). Les coefficients $S_{ij}^{(k)}$ donnent la hauteur maximale d'un camion pour aller de i à j en passant uniquement par des sommets intermédiaires $\leq k$.

Notons H la matrice initiale. S'il existe une route directe pour aller de i à j, c'est à dire un arc (i,j), le coefficient $h_{i,j} \in \mathbb{N}$ est la hauteur maximale autorisée (en m), c'est à dire la hauteur du pont le plus bas sur cet arc, s'il n'y a pas de pont traversant cette route, $h_{i,j} = \infty$. S'il est impossible d'aller de i à j directement, c'est à dire s'il n'y a pas d'arc (i,j), $h_{i,j} = 0$. On a donc $S^{(0)} = H$. Puis on a la formule de récurrence suivante :

$$S_{ij}^{(k)} = max\left(S_{ij}^{(k-1)}, min\left(S_{ik}^{(k-1)}, S_{kj}^{(k-1)}\right)\right) \tag{4.6}$$

En effet, parmi les chemins allant de i à j, il y a ceux qui ne passent que par des sommets $\leq k-1$ dont l'un (ou plus) donne une hauteur maximale de camion $S_{ij}^{(k-1)}$, puis il y a les chemins qui passent (sans répétition) par le sommet k et qui donnent aussi une hauteur maximale de camion $min\left(S_{ik}^{(k-1)}, S_{kj}^{(k-1)}\right)$. Entre ces deux hauteurs possibles on choisit la plus grande, puisque le but est de faire passer de i à j le camion le plus haut. L'algorithme prend fin au rang n puisqu'il n'y a qu'un nombre n de villes, donc de sommets intermédiaires. La matrice $S^{(n)}$ est la matrice qui donne pour chaque couple de sommets (i,j) la hauteur maximale autorisée. On peut donc écrire la procédure :

début
  $S := H$
  pour $k = 1$ à n faire
  pour $i = 1$ à n faire
  pour $j = 1$ à n faire

$$S_{ij} := max\left(S_{ij}\ ,\ min\left(S_{ik}, S_{kj}\right)\right) \tag{4.7}$$

fin

Chapitre 5

Automates finis. Théorème de Kleene

5.1 Définitions de base

Un automate est le terme usuel pour désigner un graphe étiqueté. C'est à dire un graphe orienté dont on décrit les arcs en lisant une lettre ou une suite de lettres (un mot) d'un alphabet donné. Nous en avons vu un exemple dans l'introduction, la division euclidienne par 3. Voici une définition mathématique rigoureuse d'un automate.

Deux ensembles (non vides) sont nécessaires pour construire un automate. Il faut un «alphabet», c'est à dire un ensemble fini dont les éléments seront appelés «lettres». On le note généralement A. On a besoin aussi d'un autre ensemble dont les éléments sont des «états», on le note Q. L'automate est une machine qui permet de passer d'un état à un autre état quand on lit une lettre de l'alphabet A.

Définition 5.1.1 *Un automate $\mathcal{A}$ est la donnée d'un quintuplet*

$$\mathcal{A} = < A, Q, I, T, F >$$

où A est un alphabet fini, Q est un ensemble d'états, $I \subset Q$ est l'ensemble des états initiaux et $F \subset Q$ celui des états finaux, quant à $T \subset Q \times A \times Q$ c'est l'ensemble des transitions.

Il y a un sens de lecture. On part d'un état appartenant à l'ensemble I et on sort uniquement si on aboutit à un état final, c'est à dire appartenant à l'ensemble F. Chaque passage d'un état à un autre, c'est à dire chaque arc du graphe, est décrit par un triplet $t = (p,a,q)$ de $Q \times A \times Q$ qui donne l'origine p de l'arc, son extrémité q et la lettre a qui permet de passer de l'un à l'autre.

Définition 5.1.2 *Quand l'ensemble Q des états est fini, on parle d'automate fini.*
Dans ce travail on ne rencontrera que des automates finis.

Exemple 1 Etant donné un alphabet à deux lettres $A = \{a,b\}$ et un ensemble d'états $Q = \{1,2,3\}$, on définit un automate en posant :

- $I = \{1\}$
- $F = \{1,2\}$
- $T = \{(1,a,1),(1,b,2),(2,a,1),(2,b,3),(3,a,3),(3,b,3)\}$

Exemple 2 Etant donné l'alphabet $A = \{z\}$ et l'ensemble des états $Q = \{1,2\}$, on définit

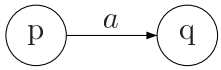
un automate en posant :

- $I = \{1\}$
- $F = \{1\}$
- $T = \{(1,z,1),(1,z,2),(2,z,1)\}$

Il est clair que même dans des cas très simples une telle représentation des automates n'est guère lisible, et encore moins exploitable pour élaborer une théorie. On utilise donc des figures régies par des conventions adoptées par l'ensemble de la communauté mathématique et informatique. Dans ces figures les états sont représentés par des ronds :

$q \in Q$ 

les transitions par des flèches :

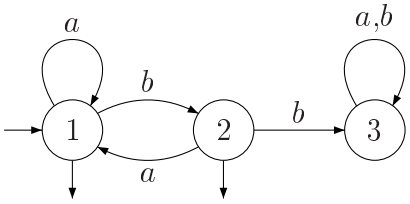
$t = (p,a,q) \in T$ 

Un état initial se distingue par une flèche rentrante et un état final par une flèche sortante :

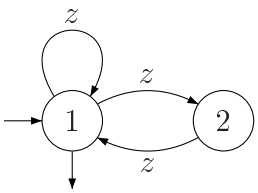
$i \in I$ $f \in F$

Quelques exemples : Les deux premières figures ci-dessous représentent les automates de nos exemples!

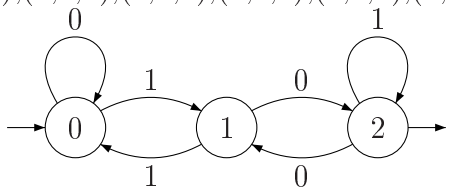
Exemple 1



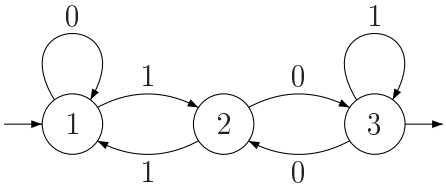
Exemple 2



Exemple 3 L'automate de la division euclidienne par 3 vu au chapitre 1, avec en état final, le reste 2. $\mathcal{A} = \{(0,0,0),(0,1,1),(1,0,2),(1,1,0),(2,0,1),(2,1,2)\}$



Remarque. Si l'on modifie la valeurs des états en prenant $Q = \{1,2,3\}$ au lieu de $Q = \{0,1,2\}$, l'automate devient



On peut y discerner une représentation du groupe symétrique S_3 constitué de l'identité, des trois transpositions (1,2), (2,3), (1,3) et des deux 3-cycles (1,2,3) et (1,3,2). Ces éléments correspondent respectivement à la lecture des mots 00, 1, 0, 101, 01, 10. Par exemple, en lisant le mot 10, on passe de l'état 1 à l'état 3 (en passant par l'état 2), de l'état 3 à l'état 2 (en bouclant sur l'état 3) et de l'état 2 à l'état 1 (en bouclant sur l'état 1); le mot 10 corespond bien à la bijection de $\{1,2,3\}$ sur lui-même qui envoie 1 sur 3, 3 sur 2 et 2 sur 1, c'est le cycle noté (1,3,2). Il suffisait par ailleurs de remarquer que les mots 0 et 1 donnent les transpositions (2,3) et (1,2) qui engendrent le groupe S_3.

On définit trois applications o,E,e.

– L'application origine o :

$$\begin{array}{rccc} o: & T & \longrightarrow & Q \\ & t=(p,a,q) & \longrightarrow & o(t)=p \end{array}$$

– L'application extrémité e :

$$\begin{array}{rccc} e: & T & \longrightarrow & Q \\ & t=(p,a,q) & \longrightarrow & e(t)=q \end{array}$$

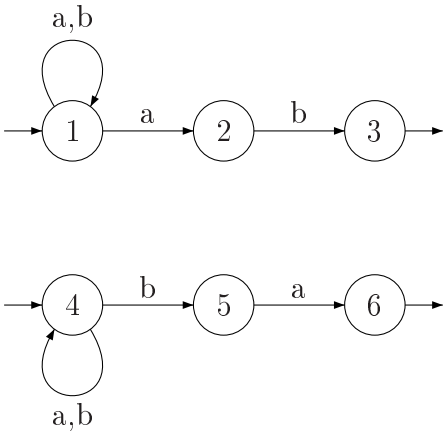
– L'application étiquette E :

$$\begin{array}{rccc} E: & T & \longrightarrow & A \\ & t=(p,a,q) & \longrightarrow & E(t)=a \end{array}$$

On dit que deux transitions $t_1 = (p_1,a_1x,q_1)$ et $t_2 = (p_2,a_2,q_2)$ sont consécutives si $e(t_1) = o(t_2)$, c'est à dire si $q_1 = p_2$.

Définition 5.1.3 *Un chemin (souvent on dit calcul) dans l'automate $\mathcal{A}$ est une suite finie t_1,...,t_n de transitions consécutives. Soit $c = t_1$,...t_n un tel chemin, son origine est $o(c) = o(t_1)$, son extrémité est $e(c) = e(t_n)$. Si pour $i = 1,\ldots,n$, $t_i = (p_i,a_i,q_i)$, l'étiquette de c est la concaténation des étiquettes des transitions qui le composent : $E(c) = a_1a_2\ldots a_n$.*

Exemple 4



Dans ce cas, $A = \{a,b\}$, $Q = \{1,2,3,4,5,6\}$, $I = \{1,4\}$, $F = \{3,6\}$. La suite $(1,a,1),(1,b,1),(1,a,2),(2,b,3)$ constitue un chemin c d'origine $o(c) = 1$, d'extrémité $e(c) = 3$ et d'étiquette $E(c) = abab$. On note aussi

$$1 \xrightarrow{a} 1 \xrightarrow{b} 1 \xrightarrow{a} 2 \xrightarrow{b} 3$$

ou encore

$$1 \xrightarrow{abab} 3$$

Convention : On considère que $\forall p \in Q$ il existe un chemin de longueur 0, d'origine p d'étiquette ε et d'extrémité p.

5.2 Langages reconnaissables

Dans ce paragraphe, A est un alphabet, Q un ensemble d'états et $\mathcal{A}$ est l'automate $\mathcal{A} =< A,Q,I,T,F >$.

Définition 5.2.1 *Un mot $u \in A^*$ est reconnu (accepté) par l'automate $\mathcal{A}$ s'il existe un chemin d'étiquette u, dont l'origine est un état initial et l'extrémité un état final.*

Définition 5.2.2 *L'ensemble des mots reconnus par l'automate $\mathcal{A}$ est un sous-ensemble de A^*, c'est donc un élément de $P(A^*)$. On le note $L(\mathcal{A})$, on l'appelle le langage reconnu par $\mathcal{A}$.*

En d'autres termes

$$L(\mathcal{A}) = \{u \in A^*; \quad \exists\, c \text{ chemin } o(c) \in I, E(c) = u, e(c) \in F\} \tag{5.1}$$

Reprenons nos exemples d'automates et déterminons les langages qu'ils reconnaissent.

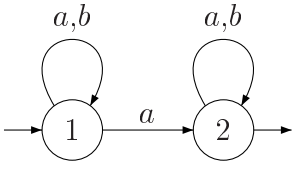
Exemple 1 Ici, $L(\mathcal{A})$ = n'est autre que l'ensemble des mots qui n'ont pas deux b consécutifs.

Exemple 2 Dans ce cas, $L(\mathcal{A}) = \{z\}^*$

Exemple 3 Dans le cas de la division euclidienne par 3 en base 2, le langage reconnu par l'automate ayant 2 en état final est l'ensemble des mots qui sont l'écriture en base 2 des entiers congrus à 2 modulo 3.

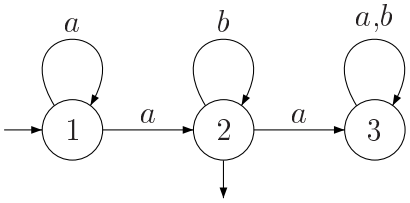
Exemple 4 Ici, $L(\mathcal{A}) = \{uab \,/\, u \in A^*\} \bigcup \{uba \,/\, u \in A^*\}$. $L(\mathcal{A})$ est l'ensemble des mots qui se terminent par ab ou ba.

Exemple 5



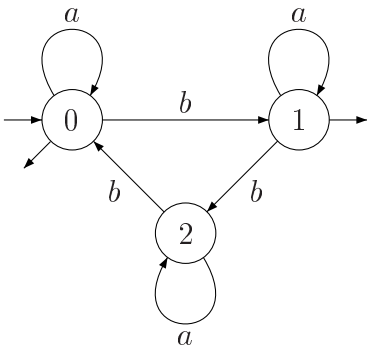
Le langage reconnu par cet automate est $L(\mathcal{A}) = \{u \in A^* \ / \ |u|_a \geq 1\}$ où $|u|_a$ représente le nombre de a dans le mot u.

Exemple 6



Si un mot contient deux fois la lettre a, le premier a fait passer de l'état initial à l'état 2 et le deuxième envoie de l'état 2 sur l'état 3 dont on ne peut plus sortir (c'est un état poubelle). Cet automate $\mathcal{A}$ reconnait $L(\mathcal{A}) = \{u \in A* \ / \ |u|_a = 1\}$

Exemple 7



$L(\mathcal{A}) = \{u \in A* \ / \ |u|_b \equiv 0 \ mod \ 3 \ ou \ |u|_b = 1 \ mod \ 3\}$

Définition 5.2.3 *On note $Rec(A^*)$ l'ensemble de tous les langages reconnaissables par automates finis sur l'alphabet A.*

$Rec(A^*) = \{L(\mathcal{A}) \ / \ \mathcal{A} \ automate \ fini \ sur \ \mathrm{A}\}$

5.3 Langages rationnels

Nous avons vu que les sous-ensembles de A^* sont appelés langages. On définit sur ces langages l'opération d'union :

$$L_1 \cup L_2 = \{u \in A^* / u \in L_1 \ ou \ u \in L_2\}$$

et l'opération de concaténation dérivée de l'opération de concaténation sur les mots :

$$L_1.L_2 = L_1L_2 = \{uv \in A^* / u \in L_1 \ et \ v \in L_2\}$$

On a alors le

Théorème 5.3.1 $< P(A^*), \cup, ., \emptyset, \{\varepsilon\} >$ *est un semi-anneau (non commutatif)*

Preuve Voir le théorème 2.2.1 et l'exemple 7 page 9. CQFD.

On peut définir par récurrence, pour tout entier naturel n, le langage L^n.
Par convention le langage L^0 désigne le langage réduit au mot vide :

$$L^0 = \{\varepsilon\}$$

Pour tout $n \in \mathbb{N}$, on pose :

$$L^{n+1} = L^n.L = L.L^n$$

D'où l'on déduit pour tous m,$n \in \mathbb{N}$

$$L^m L^n = L^{m+n}$$

et par suite la formule suivante utile par la suite :

$$L^m L^n = L^n L^m \tag{5.2}$$

Grâce à ces deux opérations élémentaires, nous pouvons définir, à partir du langage L, deux nouveaux langages, L^* et L^+.
(i) Opération * : (monoïde engendré)

$$L^* = \{\varepsilon\} \cup L \cup L^2 \cup \ldots \cup L^n \cup \ldots = \bigcup_{n \geq 0} L^n$$

Si nous remplaçons le symbole union par $+$, le langage L^* s'écrit sous forme d'une série géométrique :

$$L^* = \sum_{n \geq 0} L^n$$

(ii) Opération $^+$:

$$L^+ = L \cup L^2 \cup \ldots \cup L^n \cup \ldots = \bigcup_{n \geq 1} L^n$$

qui s'écrit aussi sous la forme d'une somme

$$L^+ = \sum_{n \geq 1} L^n$$

Pour la commodité de l'écriture on a tendance à identifier le langage constitué du seul mot vide $\{\varepsilon\}$ et le mot vide lui-même ε. On peut alors donner les relations suivantes :

- $L^* = \varepsilon + L^+$ i.e. $L^* = \{\varepsilon\} \cup L^+$.
- $L^+ = LL^* = L^*L$

Théorème 5.3.2 *L^* est le plus petit monoïde contenant L.*

Preuve Le langage L^* contient ε et L. Pour tous u,$v \in L^*$, il existe par définition m,$n \in \mathbb{N}$ tels que $u \in L^m$ et $v \in L^n$. Par conséquent, $uv \in L^m L^n$, et en vertu de (5.2) $uv \in L^{m+n}$ et donc $uv \in L^*$. Ceci prouve que le langage L^* est stable par concaténation. D'autre part, la concaténation est associative sur A^* donc sur L^* ce qui finit de prouver que $< L^*,.,\varepsilon >$ est un monoïde. Montrons que L^* est le plus petit monoïde contenant L.

Pour cela, considérons un monoïde M, i.e. $< M,.,\varepsilon >$, contenant L. Il contient ε et L, il contient donc L^2, et par récurrence ; $\forall n$, il contient L^n. M contient donc L^*. CQFD.

Nous allons maintenant définir une classe de langages par récurrence à partir d'une base constituée des langages élémentaires, à savoir : le langage vide, le langage réduit au mot vide, les langages constitués d'une unique lettre de l'alphabet A.

Définition 5.3.1 *: récursive des langages rationnels*
Etant donné un alphabet A.
Base :

- $\emptyset$ *est un langage rationnel*
- $\{\varepsilon\}$ *est un langage rationnel*
- $\forall a \in A$, $\{a\}$ *est un langage rationnel*

Récurrence :

- *Si* L *est rationnel* L^* *l'est aussi*
- *Si* L_1 *et* L_2 *sont rationnels,* $L_1 \cup L_2$ *l'est aussi*
- *Si* L_1 *et* L_2 *sont rationnels,* $L_1.L_2$ *l'est aussi*

Un langage est donc rationnel s'il s'obtient à partir des parties finies de A^* en utilisant un nombre fini de fois les opérations union, concaténation et étoile. On peut dire encore que la famille des langages rationnels est la plus petite famille de langages contenant les parties finies de A^* et close par les opérations union, concaténation et étoile.

Les langages rationnels se représentent par des expressions rationnelles. Il s'agit simplement d'une écriture «allégée», on enlève les accolades ensemblistes pour les singletons et l'on substitue l'opération $+$ à $\cup$.

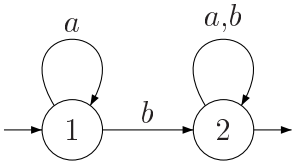
Définition 5.3.2 *: récursive des expressions rationnelles.*
Base :

- *0 est l'expression rationnelle représentant* $\emptyset$
- ε *est l'expression rationnelle pour* $\{\varepsilon\}$
- a *est l'expression rationnelle pour* $\{a\}$

Récurrence :

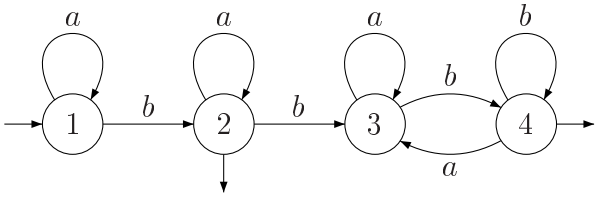
- *Si* e *est l'expression rationnelle pour le langage rationnel* L *alors* e^* *est l'expression rationnelle pour le langage rationnel* L^*
- *Si* e_1 *(resp :* e_2*) est l'expression rationnelle pour le langage rationnel* L_1 *(resp :* L_2*), alors* $e_1 + e_2$ *est l'expression rationnelle pour le langage rationnel* $L_1 + L_2$
- e_1e_2 *est l'expression rationnelle pour le langage rationnel* L_1L_2

Exemple 1



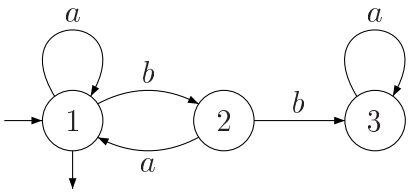
L'expression rationnelle du langage reconnu par cet automate est :
$L(\mathcal{A}) = (a+b)^*b(a+b)^* = a^*b(a+b)^*$

Exemple 2



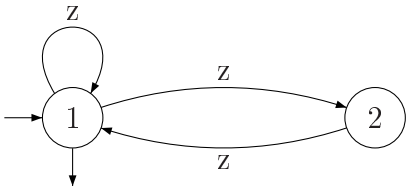
Ici nous avons $L(\mathcal{A}) = a^*ba^* + a^*ba^*b(a+b)^*b$.

Exemple 3



Pour cet automate, $L(\mathcal{A}) = (a + ba)^*$.

Exemple 4



Ici, $L(\mathcal{A}) = (z + z^2)^*$.

Définition 5.3.3 *On note $Rat(A^*)$ l'ensemble des langages rationnels sur l'alphabet A.*

5.4 Théorème de Kleene

Dans les deux paragraphes précédents nous avons défini deux familles de langages sur un alphabet donné A

- la famille des langages reconnaissables par automates finis sur A, que nous avons notée $Rec(A^*)$,
- la famille des langages rationnels sur A, construite de manière algébrique par quelques opérations sur les éléments de $P(A^*)$, notée $Rat(A^*)$.

L'un des résultats fondamentaux de la théorie des automates est que ces deux familles coïncident. C'est le fameux :

Théorème 5.4.1 *(de Kleene, 1956)* $Rec(A^*) = Rat(A^*)$.

L'inclusion $Rat(A^*) \subset Rec(A^*)$ se montre par récurrence sur les expressions rationnelles.

Pour montrer l'inclusion $Rec(A^*) \subset Rat(A^*)$ nous utiliserons l'algorithme de **Mac Naughton Yamada** qui permet de passer d'un automate à une expression rationnelle.

Cet algorithme est du même type que l'algorithme de Roy Warshall, c'est pourquoi nous le présentons dans ce travail.

Soit $Q = \{1, \ldots, n\}$ l'ensemble des états. Etant donnés deux états p,$q \in Q$ on définit pour tout $k \in \mathbb{N}$

- le langage X_{pq} comme l'ensemble des mots qui sont étiquettes de chemins allant de l'état p à l'état q.

$$X_{pq} = \{u \in A^* \ / \ \exists\, c \ chemin, \ tel \ que \ o(c) = p, \ e(c) = q, \ E(c) = u\}$$

- le langage $X_{pq}^{(k)}$ constitué des mots qui sont étiquettes de chemins partant de l'état p pour arriver à l'état q en ne passant que par des états intermédiaires (distincts de p et q) inférieurs ou égaux à k.

$$X_{pq}^{(k)} = \{u \in A^* \ / \ \exists\, c = t_1 \ldots t_s \ chemin, \ tel \ que \ o(c) = p, \ e(c) = q,$$

$$E(c) = u \ avec \ \forall j, \ 1 \leq j < s, \ e(t_j) \leq k\}$$

S'il existe un chemin d'étiquette u allant de p à q en ne passant que par des états intermédiaires $\leq k$, on note

$$p \xrightarrow[\leq\, k]{u} q$$

Si $p \neq q$,

$$X_{p,q}^0 = \{a \ / \ (p,a,q) \in T\} \tag{5.3}$$

Si $q = p$,

$$X_{p,p}^0 = \{a \ / \ (p,a,p) \in T\} \cup \{\varepsilon\} \tag{5.4}$$

Le résultat suivant nous donne les langages $X_{p,q}^{(k)}$ par récurrence.

Lemme 5.4.1 *Si $p \neq k$ et $q \neq k$,* $\quad X_{p,q}^{(k)} = X_{p,q}^{(k-1)} + X_{p,k}^{(k-1)} (X_{k,k}^{(k-1)})^* X_{k,q}^{k-1}$

Preuve L'inclusion $\supseteq$ étant évidente, démontrons l'inclusion $\subseteq$. Si $u \in X_{p,q}^{(k)}$, i.e.,

$$p \xrightarrow[\leq k]{u} q$$

il existe deux possibilités. Soit sur ce chemin on ne rencontre pas k comme sommet intermédiaire, i.e. u est l'étiquette d'un chemin ne passant que par des sommets intermédiaires strictement inférieurs à k

$$p \xrightarrow[\leq k-1]{u} q$$

et dans ce cas $u \in X_{p,q}^{(k-1)}$. Soit k est un sommet intermédiaire sur ce chemin que l'on peut donc décomposer de la manière suivante :

$$p \xrightarrow[\leq k-1]{} k \xrightarrow[\leq k-1]{} k \ldots k \ldots k \xrightarrow[\leq k-1]{} k \xrightarrow[\leq k-1]{} p$$

puisque pour aller de p jusqu'à la première occurence de k les sommets intermédiaires sont forcément inférieurs à $k-1$, qu'entre deux occurences consécutives de k les sommets intermédiaires sont forcément inférieurs à $k-1$, et que pour aller de la dernière occurence de k jusqu'à q les sommets intermédiaires sont forcément inférieurs à $k-1$. L'étiquette

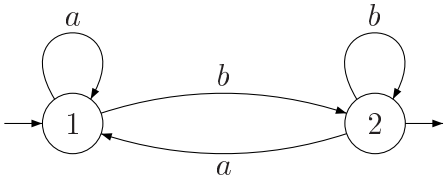
du chemin allant de p au premier k appartient à $X_{p,k}^{(k-1)}$, l'étiquette d'un chemin reliant deux occurences consécutives de k appartient à $X_{k,k}^{(k-1)}$ et l'étiquette du chemin qui va du dernier k à l'état q appartient à $X_{k,q}^{(k-1)}$. Donc $u \in X_{p,k}^{(k-1)}(X_{k,k}^{(k-1)})^* X_{k,q}^{k-1}$. Ceci termine la démonstration. CQFD.

On démontre de manière analogue les formules suivantes :

Lemme 5.4.2 $\forall p,q,k \in Q,\ k > 0$ *:*

- *Si* $p \neq k$, $\quad X_{p,k}^{(k)} = X_{p,k}^{(k-1)}(X_{k,k}^{(k-1)})^*$
- *Si* $q \neq k$, $\quad X_{k,q}^{(k)} = (X_{k,k}^{(k-1)})^* X_{k,q}^{(k-1)}$
- $X_{k,k}^{(k)} = (X_{k,k}^{(k-1)})^*$

Exemple 1



$X_{p,\ q}^{(0)}\ p/q$	1	2
1	$\varepsilon + a$	b
2	a	$\varepsilon + b$

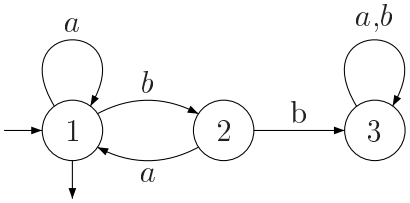
$X_{p,q}^{(1)}\ p/q$	1	2
1	a^*	a^*b
2	$aa^* = a^+$	$aa^*b = a^+b$

On a :

$$X_{1,2} = \{u \ / \ 1 \xrightarrow{u} 3\}$$

$$X_{1,2} = X_{1,2}^{(2)} = X_{1,2}^{(1)}(X_{2,2}^{(1)})^* = a^*b(a^*b)^*$$

Exemple 2



$X_{p,\ q}^{(0)}\ p/q$	1	2	3
1	$\varepsilon + a$	b	0
2	a	ε	b
3	0	0	$\varepsilon + a + b$

$$X^{(1)}_{1,\,1} = \left(X^{(0)}_{1,\,1}\right)^* = (\varepsilon + a)^* = a^*$$

$$X^{(1)}_{1,2} = (X^{(0)}_{1,1})^* X^{(0)}_{1,2} = a^* b$$

$$X^{(1)}_{2,1} = X^{(0)}_{2,1}(X^{(0)}_{1,1})^* = aa^* = a^+$$

$$X^{(1)}_{2,2} = X^{(0)}_{2,\,2} + X^{(0)}_{2,\,1}\left(X^{(0)}_{1,\,1}\right)^* X^{(0)}_{1,\,2} = \varepsilon + aa^*b = \varepsilon + a^*b$$

$X^{(1)}_{p,\,q}$ p/q	1	2	3
1	a^*	a^*b	
2	a^+	$\varepsilon + a^+b$	
3			

On a $L(A) = X_{1,1} = X^{(3)}_{1,1}$ puisque $Q = \{1,2,3\}$. Remarquons que l'on ne peut pas aller de l'état 3 à l'état 1. Autrement dit $X^{(3)}_{1,1} = X^{(2)}_{1,1}$. D'où

$$X^{(2)}_{1,\,1} = X^{(1)}_{1,\,1} + X^{(1)}_{1,\,2}\left(X^{(1)}_{2,\,2}\right)^* X^{(1)}_{2,\,1} = a^* + a^*b(\varepsilon + a^+b)^*a^+ = a^* + a^*b(a^+b)^*a^+$$

Remarquons que l'on peut aussi décrire le langage $L(A)$ par l'expression rationnelle $(a + ba)^*$.

Preuve (du théorème de Kleene) L'algorithme de Mac Naughton Yamada donne une preuve effective de l'inclusion $Rec(A^*) \subseteq Rat(A^*)$. Puisqu'il y a un nombre fini d'états $Q = \{1, \ldots, n\}$, on a

$$X_{p,q} = X^{(n)}_{p,q}$$

Or, $X^{(0)}_{p,q}$ est rationnel puisque l'on n'utilise que le mot vide et des lettres. Et, en utilisant les formules de récurrence des lemmes ci-dessus, on montre par récurrence sur k, que $X^{(k)}_{p,q}$ est rationnel. Par conséquent $X_{p,q}$ est rationnel.

Enfin, nous pouvons écrire que le langage reconnu par l'automate est la réunion de tous les langages qui relient un état initial i à un état final j :

$$L(\mathcal{A}) = \sum_{i \in I,\ f \in F} X_{i,f}$$

et une somme finie (i.e. une réunion) de langages rationnels est un langage rationnel. Nous venons de montrer que tout langage reconnu par l'automate est rationnel. CQFD.

Chapitre 6

Annexe

Dans cette dernière partie nous avons simplement voulu rappeler les définitions des principales structures algébriques, celles que rencontre tout étudiant d'un DEUG scientifique, à savoir les groupes anneaux et corps. De plus, nous donnons la démonstration du théorème d'Euler qui est, d'un point de vue historique, à la base de la théorie des graphes. Nous présentons aussi l'algorithme de Dijkstra puisque c'est un classique pour la recherche des chemins de coût minimal.

6.1 Groupes, anneaux et corps

Soit G un ensemble, une loi de composition interne (on notera **l.c.i.**) sur G est une application de $G \times G$ dans G, c'est à dire une loi qui à tout couple d'éléments de G associe un unique élément de G.

Exemple 1. Pour $G = \mathbb{R}$, l'application $(x,y) \to x + y$ où $+$ est l'addition usuelle définit une **l.c.i.**. Cette même addition définit des **l.c.i**. sur les ensembles $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, ou encore $\mathbb{N}$.

Exemple 2. Si G est l'ensemble des parties d'un ensemble E, on peut définir une **l.c.i**. par l'application $(A,B) \to A \cup B$.

Exemple 3. Soit X un ensemble et $E = X^X$ l'ensemble des applications de X dans lui-même, on définit une **l.c.i.** sur E en considérant l'application $(f,g) \to f \circ g$. L'application composée $f \circ g$ est l'application de X dans X définie par :

$$\forall x \in X, \quad (f \circ g)(x) = f(g(x))$$

Cela suit le schéma

$$\begin{array}{ccccc} X & \xrightarrow{g} & X & \xrightarrow{f} & X \\ x & \to & g(x) & \to & f(g(x)) \end{array}$$

On prend l'image de x par g, puis l'image du point obtenu $g(x)$ par f. Attention : l'ordre de lecture et l'ordre dans lequel on fait agir les deux applications sont inversés. Nous noterons dorénavant (pour la commodité de l'écriture) fg au lieu de $f \circ g$.

Définition 6.1.1 *Un groupe est un ensemble muni d'une loi de composition interne $(x,y) \to x.y$ qui vérifie les propriétés suivantes :*

- *elle est associative :* $\forall\ x,y,z \in G,\ (x.y).z = x.(y.z)$
- *il existe dans G un élément neutre, noté e :* $\forall\ x \in G,\ e.x = x.e = x$
- *tout élément est inversible :* $\forall\ x \in G,\ \exists\ y \in G$ *tel que* $x.y = y.x = e$. *On dit que y est l'inverse de x, on le note* $y = x^{-1}$.

Quand un ensemble est simplement muni d'une loi de composition interne associative on dit que c'est un semi-groupe. Si de plus il possède un élément e vérifiant $e.x = x.e = x$ pour tout x on dit que c'est un monoïde.

En fait, le terme de groupe s'applique au couple $(G,.)$ constitué de l'ensemble G et de la loi ., mais s'il n'y a pas de risque de confusion sur la loi en question on se contente de parler simplement du groupe G.

Quand la loi est commutative ($\forall\ x,y \in G,\ x.y = y.x$) on dit que le groupe G est **commutatif** ou **abélien**.

Si le cardinal de G, noté $|G|$ ou $o(G)$, est fini, on dit que G est un groupe fini et $|G|$ est appelé l'**ordre** de G.

La nécessité de l'existence d'un élément neutre fait que l'ensemble vide, $\emptyset$, n'est pas un groupe.

L'associativité permet de passer du produit de 2 éléments au produit de 3, puis au produit d'un nombre fini d'éléments. Etant donnés $x,y,z \in G$, le produit de ces trois éléments est $x.y.z = (x.y).z = x.(y.z)$. Etc.

Dans la suite on se contentera de noter xy pour le produit $x.y$.

Quand la loi du groupe est de type addition (addition de nombres ou d'applications quand c'est possible), on parle du symétrique et non de l'inverse d'un élément x, on le note $-x$.

Exemple 1. Les ensembles $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ munis de l'addition usuelle sont des groupes commutatifs. L'ensemble $\mathbb{N}$ muni de l'addition n'est pas un groupe, puisque, excepté 0, aucun élément n'admet de symétrique. La loi + étant une loi de composition interne associative sur $\mathbb{N}$, on dit que $\mathbb{N}$ est un semi-groupe. En plus de cela $0 \in \mathbb{N}$ et vérifie : $\forall\ x \in \mathbb{N},\ x + 0 = 0 + x = x$. $\mathbb{N}$ est un monoïde.

Exemple 2. Les ensembles $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*$ (i.e. $\mathbb{Q},\mathbb{R},\mathbb{C}$ privés de 0) munis de la multiplication usuelle sont des groupes commutatifs. L'ensemble $\mathbb{Z}^*$ n'est pas un groupe pour la multiplication, puisque, excepté ± 1, aucun élément n'admet d'inverse dans $\mathbb{Z}^*$. C'est un monoïde.

Exemple 3. L'ensemble $\mathcal{U} = \{z \in \mathbb{C} \quad / \quad |z| = 1\}$ muni de la multiplication est un groupe commutatif. En effet, la multiplication est une **l.c.i.** $\forall\ z,z' \in \mathcal{U},\ |zz'| = |z|\,|z'| = 1$ soit $zz' \in \mathcal{U}$, 1 est l'élément neutre, l'inverse $1/z$ de tout élément z de $\mathcal{U}$ est de module 1, $|1/z| = 1/|z| = 1$, et pour conclure la commutativité et l'associativité dans $\mathbb{C}$ induisent la commutativité et l'associativité dans $\mathcal{U}$.

Exemple 4. L'ensemble $\mathcal{U}_n = \{z \in \mathbb{C} \quad / \quad z^n = 1\}$ muni de la multiplication est un groupe commutatif appelé groupe des racines n-ièmes de l'unité. Il suffit de remarquer que $\forall\ z,z' \in \mathcal{U}_n,\ (zz')^n = z^n(z')^n = 1$ et $(1/z)^n = 1/z^n = 1$. Quand on résout l'équation $z^n = 1$ on obtient les solutions ω^m, $m \in \mathbb{Z}$, où $\omega = \exp(\frac{2i\pi}{n})$. La division euclidienne par n permet d'écrire, $\forall m \in \mathbb{N}$: $\exists!(q,r) \in \mathbb{N}$ tels que $m = nq + r \quad$ avec $\quad 0 \leq r \leq n-1$
d'où

$$\omega^m = \omega^{nq+r} = (\omega^n)^q\omega^r = 1^q\omega^r = \omega^r$$

Par conséquent, $\mathcal{U}_n$ est un groupe fini d'ordre n, dont tous les éléments sont des puissances de ω.

$$\mathcal{U}_n = \{1,\omega,...,\omega^{n-1}\} = \{\omega^k \ / \ 0 \leq k \leq n-1\}$$

L'inverse de ω^k n'est autre que ω^{n-k}. C'est à dire :

$$(\omega^k)^{-1} = \omega^{-k} = \omega^{n-k}$$

Exemple 5. Soit X un ensemble non vide quelconque, l'ensemble $E = X^X$ muni de la loi de composition des applications définie plus haut n'est pas un groupe. E admet un élément neutre, l'application identique Id_E. La loi de composition des applications est associative. E est un monoïde. L'inverse d'une application $f : X \to X$ serait une application $g : X \to X$ telle que $f \circ g = g \circ f = Id_X$, or un tel g n'existe pas en général, sauf si f est bijective, et dans ce cas g est sa bijection réciproque.

Par contre si on se restreint à l'ensemble des bijections de X dans X on obtient un groupe pour la loi de composition des applications, appelé **groupe symétrique de** X. On le note $\mathfrak{S}_X$ ou S_X.

Il n'est pas commutatif dès que X contient au moins trois éléments. En effet, si a,b,c sont trois éléments distincts de X, on peut toujours construire deux bijections de X,σ et σ', telles que $\sigma(a) = b$,$\sigma(b) = a$,$\sigma(c) = c$ et $\sigma'(a) = a$,$\sigma'(b) = c$,$\sigma'(c) = b$. Elles vérifient $\sigma(\sigma'(a)) = \sigma(a) = b$ et $\sigma'(\sigma(a)) = \sigma'(b) = c$, c'est à dire $\sigma \circ \sigma' \neq \sigma' \circ \sigma$.

Soit A un ensemble muni de deux lois de composition internes, que nous noterons de manière classique $+$ et $\times$.

Définition 6.1.2 *L'ensemble A muni de ces deux lois est un anneau s'il vérifie les propriétés suivantes :*

- $(A,+)$ *est un groupe commutatif*
- *la loi* $\times$ *est associative :* $\forall\ x,y,z \in A,\ (x \times y) \times z = x \times (y \times z)$
- *La loi* $\times$ *est distributive à droite et à gauche par rapport à la loi* $+$ *:* $\forall\ x,y,z \in A,$ $x \times (y + z) = (x \times y) + (x \times z)$ *et* $(y + z) \times x = (y \times x) + (z \times x)$

Si la loi $\times$ est commutative, on dit que l'anneau est commutatif. S'il existe un élément neutre pour la multiplication, on dit que l'anneau est unitaire. Cet élément est noté 1_A ou tout simplement 1, on l'appelle l'élément unité de A. A ce sujet, il y a divergence entre mathématiciens et informaticiens. Pour ces derniers un anneau est toujours unitaire. Et notamment, un morphisme d'anneau envoie toujours l'élément unité sur l'élément unité. On note $(A, +, \times)$. On note 0_A ou tout simplement 0 l'élément neutre du groupe $(A,+)$.

Définition 6.1.3 *Si tout élément non nul (différent de 0) admet un inverse pour la loi* $\times$ *;* $\forall x \in A,\ \exists y \in A$ *tel que* $x \times y = y \times x = 1$*, on dit que* $(A, +, \times)$ *ou que A est un corps.*

En d'autres termes, A est un corps si $(A,+)$ est un groupe commutatif et $(A\backslash 0,\times)$ est un groupe.

Exemple 1 $(\mathbb{Z}, +, \times)$ est un anneau, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.

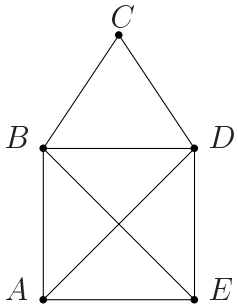
Exemple 2 Soit K un corps commutatif ($K = \mathbb{R}$ ou $K = \mathbb{C}$), l'ensemble des polynômes à coefficients dans K est un anneau commutatif si on le munit de l'addition et de la multiplication des polynômes.

Exemple 3 Soient E un espace vectoriel sur un corps commutatif K, l'ensemble des applications linéaires de E dans E (on les appelle endomorphismes de E) muni de l'addition et de la loi de composition des applications est un anneau non commutatif, noté $(End(E), +, \circ)$.

Exemple 4 Si K est un corps commutatif, on sait définir sur l'ensemble $\mathcal{M}(n,K)$ des matrices $n \times n$, à n lignes et n colonnes, à coefficients dans K, une addition et une multiplication telles que $(\mathcal{M}(n,K), +, \times)$ est un anneau non commutatif (isomorphe à l'anneau $(End(E), +, \circ)$.

6.2 Le théorème d'Euler

Tous les écoliers savent tracer la maison ci-dessous sans lever le crayon et sans passer deux fois sur une arête. Ils savent donc trouver une chaîne eulérienne.



Le théorème d'Euler donne une démonstration de cette propriété, de même qu'il résoud le problème des ponts de Königsberg et celui des dominos.

Théorème 6.2.1 *Un graphe non orienté (éventuellement un multigraphe) connexe admet une chaîne eulérienne si, et seulement si, il possède* 0 *ou* 2 *sommets impairs. Il admet un cycle eulérien si, et seulement si tous ses sommets sont pairs.*

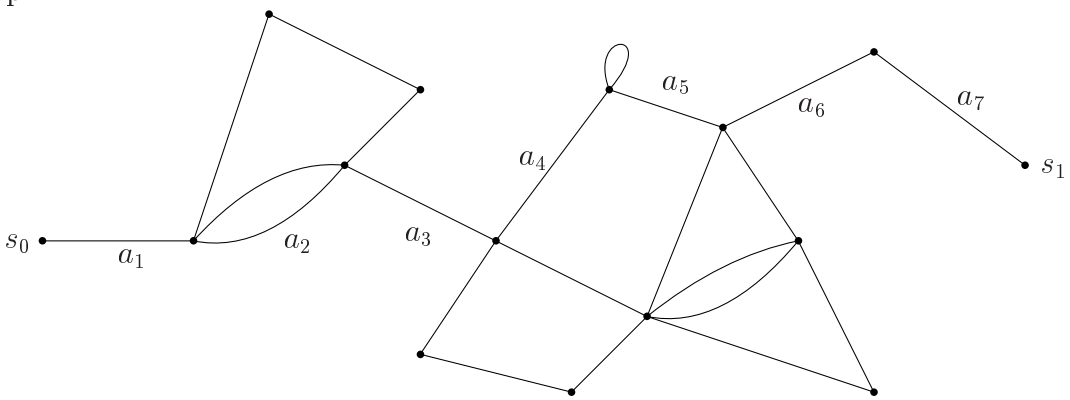
Preuve La condition est nécessaire. Soit $G = (S,A)$ un graphe admettant une chaîne eulérienne. Comme le graphe est connexe, en chaque sommet s arrive une arête et repart une autre arête de cette chaîne, sauf pour le sommet initial et le sommet terminal de la chaîne si celle-ci n'est pas fermée. Par conséquent, si la chaîne est un cycle eulérien tout sommet s est de degré pair : $d(s) = 2k$ si k est le nombre d'arêtes arrivant en s. Si la chaîne n'est pas fermée tous les sommets sont de degré pair sauf l'origine et l'extrémité qui sont impairs.

La condition est suffisante. Cela se démontre par récurrence sur le nombre n d'arêtes du graphe. Pour tout $n \geq 1$, montrons la propriété $P(n)$: « tout graphe $G = (S,A)$ avec $|A| = n$, et tel que, pour tous les sommets s (resp : pour tous les sommets s sauf deux), $d(s) \equiv 0$ (2), admet un cycle eulérien (resp : une chaîne eulérienne).

Cela est évident pour $n = 1$. Il faut montrer que, pour tout $n \geq 2$, $P(n-1)$ vraie entraine $P(n)$ vraie.

Premier cas : $G = (S,A)$ est un graphe connexe constitué de n arêtes et tel que tous ses sommets soient pairs sauf deux s_0 et s_1. Le graphe étant connexe, il existe (au moins) une chaîne, que nous notons C, qui va du sommet s_0 au sommet s_1.

Exemple :



$C = (a_1,a_2,a_3,a_4,a_5,a_6,a_7)$

Considérons le sous-graphe $G' = (S',A')$ où A' est l'ensemble des arêtes qui n'appartiennent pas à C. On a,

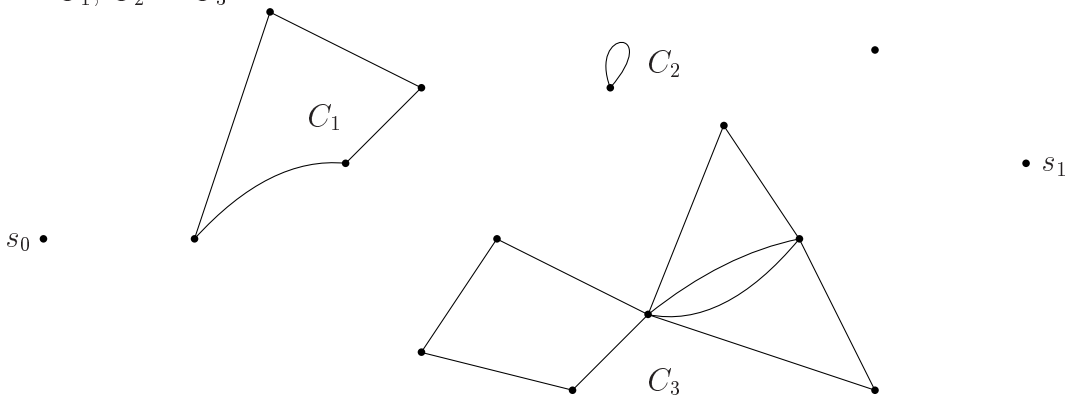
$$\forall s \in S', d(s) \equiv 0\ (2)$$

On pourrait alors conclure en utilisant l'hypothèse de récurrence si G' était connexe. Or ce n'est pas forcément le cas (cf figure ci-après). On surmonte cette difficulté en considérant les composantes connexes de G'. Supposons que G' soit la «réunion» des graphes connexes $G_1,\ldots,G_p$ où $G_i = (S_i,A_i)$ pour $i = 1,\ldots,p$. On a, pour tout $i = 1,\ldots,p$:

- $\forall s \in S_i, d(s) \equiv 0\ (2)$
- G_i est connexe (c'est fait pour!)
- $|A_i| \leq n-1$

On peut cette fois appliquer l'hypothèse de récurrence. Il existe pour chaque composante connexe G_i un cycle eulérien que nous noterons C_i. Et comme G est connexe, la chaîne C rencontre chaque C_i en au moins un de ses sommets.

Exemple (suite) : on a isolé les trois composantes connexes qui génèrent trois cycles eulériens C_1, C_2 et C_3.



En conclusion, la chaîne C complétée par les cycles C_i fournit une chaîne eulérienne qui va de s_0 à s_1.

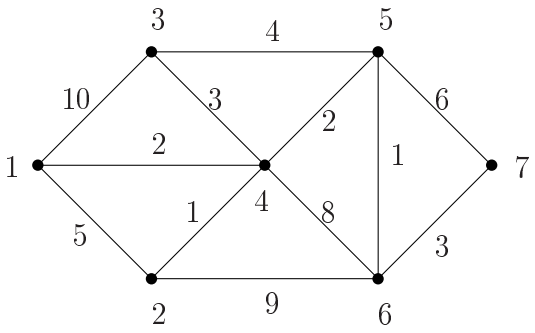
Deuxième cas : $G = (S,A)$ est un graphe connexe constitué de n arêtes et dont tous les sommets sont pairs. Si l'on enlève une arête du graphe, on se retrouve dans le cas précédent. Il existe donc une chaîne eulérienne. On rajoute alors l'arête enlevée précédement, on obtient un cycle eulérien. CQFD.

Applications

- Dans le cas des ponts de Königsberg, tous les sommets sont impairs, il n'y a ni cycle ni chaîne eulériens. Les habitants de la ville ne pouvaient pas effectuer une promenade empruntant les sept ponts une fois et une seule.
- Par contre dans le problème des dominos, tous les sommets du graphe sont pairs (que ce soit pour des dominos de six chiffres (plus blanc) ou comme dans notre schéma des dominos de quatres chiffres (plus blanc)), il existe donc un cycle eulérien et la construction demandée est possible. Si les dominos ont un nombre impair de chiffres et le blanc, les sommets sont tous impairs et dans ce cas le théorème d'Euler permet de conclure qu'il n'existe ni chaîne, ni cycle eulériens.
- Quant à la maison de la page 44, elle a exactement deux sommets impairs A et E. Elle admet une chaîne eulérienne qui va de A à E (ou l'inverse).

6.3 Algorithme de Dijkstra

On pourra consulter le chapitre 5 de [5] ou le chapitre 25 de [4] ou encore [6] dont nous nous sommes largement inspirés. Nous présenterons l'algorithme de Dijkstra pour des graphes simples non orientés, c'est à dire des 1-graphes sans boucle. Nous pourrons comparer le résultat avec celui de l'algorithme de Floyd sur l'exemple ci-dessous.



Soit $G = (S,A)$ un graphe pondéré, sa matrice coût notée L, donne la longueur $l_{i,j}$ de l'arête $\{i,j\}$. Le problème rappelons-le, consiste à déterminer pour chaque paire $\{i,j\}$ de sommets, le plus court chemin de i à j, ou pour être plus précis, le coût du chemin minimal de i à j. Ici, nous n'allons pas résoudre le problème d'un seul coup, pour toutes les paires $\{i,j\}$. On calcule dans un premier temps le coût minimal d'un sommet donné à tous les sommets du graphe. Il faut donc ensuite reproduire cette opération pour chaque sommet, c'est à dire n fois.

Plutôt que de calculer le coût minimal d'un sommet i à tous les sommets du graphe, nous calculerons le coût minimal du sommet 1 à tous les sommets du graphe. Il n'y aura ensuite qu'à reproduire le modèle pour les sommets $2,\ldots,n$.

Le coût minimal pour aller de 1 à chacun des n sommets j du graphe sera calculé dans la j-ème composante $v(j)$ du vecteur

$$V = (v(1),\ldots,v(n)).$$

Partant d'une valeur initiale de V, on modifie à chaque étape de l'algorithme une partie de ses composantes et l'une d'entre elle, représentant un coût minimal, sera conservée pour la suite (elle sera soulignée). En même temps, le sommet correspondant ira rejoindre les sommets sélectionnés aux étapes précédentes dans un sous-ensemble T de S. L'algorithme prend fin quand $T = S$, ce qui arrive au bout des $n-1$ étapes qui suivent l'initialisation.

Initialisation Au départ, les composantes $v(j)$ sont les valeurs des arêtes $\{1,j\}$, V n'est autre que la première ligne de la matrice L :

$$V = (l_{1,1} = 0,\ldots,l_{1,j},\ldots,l_{1,n})$$

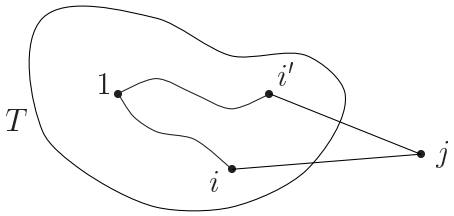
Le coût minimal pour aller de 1 à 1 est 0, tout autre chemin serait d'un coût > 0. La composante $v(1) = 0$ de V est définitive, c'est pourquoi elle sera soulignée. On commence donc toujours par le vecteur $V = (\underline{0},l_{1,2},\ldots,l_{1,n})$ et l'on pose $T = \{1\}$.

Itération Le théorème suivant montre comment l'on passe d'une étape à la suivante.

Théorème 6.3.1 *Soit $G = (S,A)$ un graphe simple non orienté de matrice coût L.*
Soit T une partie non vide de S pour laquelle on a:
$\forall i \in T$, *$v(i)$ est le coût minimal de* 1 *à i et le chemin correspondant est entièrement dans T.*
On définit, pour tout $k \in S \setminus T$:
$v(k) = min\{v(i) + l_{i,k} \ / \ i \in T\}$
Si $j \in S \setminus T$ est un sommet qui réalise le minimum des $v(k)$, c'est à dire :
$v(j) = min\{v(k) \ / \ k \in S \setminus T\}$,
(il en existe toujours un, il n'est pas forcément unique), alors $v(j)$ donne le coût minimal pour aller de 1 *à j et le chemin correspondant est entièrement dans T, hormis le sommet j.*

Preuve Pour montrer que $v(j)$ donne bien la longueur d'un chemin minimal C pour aller de 1 à j raisonnons par l'absurde.

Supposons qu'il existe un chemin C' de 1 à j de longueur l' strictement inférieure à $l = v(j)$. Il passe nécessairement par au moins un sommet n'appartenant pas à T. En effet, supposons que C' passe uniquement par des sommets de T, comme sur la figure ci-dessous :



On additionne la longueur du chemin $(1,\ldots,i')$ et celle de l'arête $\{i',j\}$ pour obtenir l'. L'arête est de longueur $l_{i',j}$. Comme i' appartient à T, le chemin $(1,\ldots,i')$ est de longueur $\geq v(i')$. Par suite,

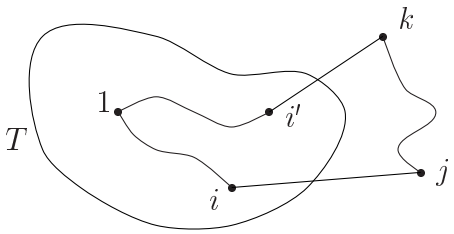
$$l' \geq v(i') + l_{i',j}$$

De plus, par définition de $v(j)$,

$$v(i') + l_{i',j} \geq v(j)$$

d'où $l' \geq v(j)$. Contradiction.

Soit k le premier sommet de $C' \in S \setminus T$.



La longueur l' de C' s'obtient en faisant la somme des longueurs de $(1,\ldots,i')$, de l'arête $\{i',k\}$ et de $(k,\ldots,j)$. Comme $i' \in T$ la longueur du chemin $(1,\ldots,i')$ est $\geq v(i')$. La longueur de $(k,\ldots,j)$ est ≥ 0. Donc,

$$l' \geq v(i') + l_{i',k}$$

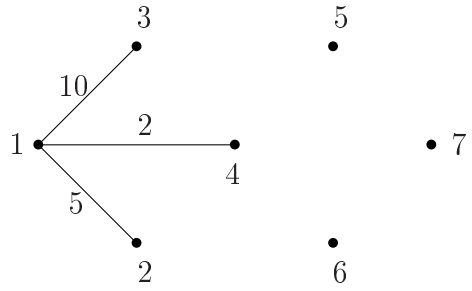
Mais, par définition,

$$v(i') + l_{i',k} \geq v(k)$$

Il s'en suit que $l' \geq v(k) \geq v(j)$. Cela est en contradiction avec l'hypothèse initiale $l' < v(j)$. CQFD.

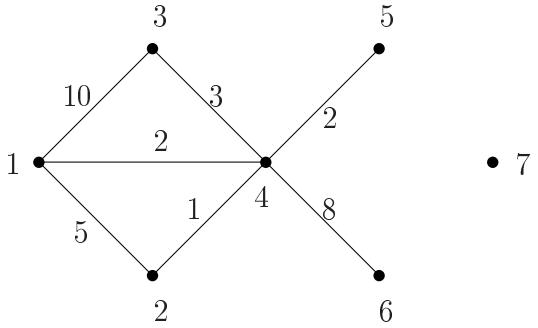
Reprenons notre exemple.

- Initialisation : $V = (\underline{0},5,10,2,\infty,\infty,\infty)$ et $T = \{1\}$.
- Etape 1 : La valeur minimale des composantes de V est 2, qui est le coût de l'arête $\{1,4\}$.



C'est le chemin de coût minimal allant de 1 à 4 puisque tout autre chemin serait indirect et passerait par un sommet distinct de 4 donc de coût ≥ 2. Le sommet 4 rejoint le sommet 1 dans l'ensemble $T = \{1,4\}$ et l'on sélectionne définitivement la composante $v(4) = 2$ dans le nouveau vecteur V. $V = (\underline{0},5,10,\underline{2},\infty,\infty,\infty)$ et $T = \{1,4\}$.

- Etape 2 : Pour tous les sommets $j \in S \setminus T = \{2,3,5,6,7\}$ on regarde $v(j) = min\ \{v(1) + l_{1,j},\ v(4) + l_{4,j}\}$, c'est à dire $v(j) = min\ \{0 + l_{1,j} = l_{1,j},\ 2 + l_{4,j}\}$.



Cela donne

- $v(2) = min\ \{0 + 5 = 5,\ 2 + 1 = 3\} = 3$,
- $v(3) = min\ \{0 + 10 = 10,\ 2 + 3 = 5\} = 5$,

- $v(5) = min\ \{0 + \infty = \infty,\ 2 + 2 = 4\} = 4$,
- $v(6) = min\ \{0 + \infty = \infty,\ 2 + 8 = 10\} = 10$
- $v(7) = min\ \{0 + \infty = \infty,\ 2 + \infty = \infty\} = \infty$.

On prend alors la valeur minimale de tous ces $v(j)$, soit $v(2) = 3$. $V = (\underline{0},\underline{3},5,\underline{2},4,10,\infty)$ et $T = \{1,2,4\}$.

- Etape 3 : Pour tous les sommets $j \in S \setminus T = \{3,5,6,7\}$ calculons $v(j) = min\ \{v(1) + l_{1,j},\ v(2) + l_{2,j},\ v(4) + l_{4,j}\}$, soit $v(j) = min\ \{0 + l_{1,j},\ 3 + l_{2,j},\ 2 + l_{4,j}\}$. On a :
  - $v(3) = min\ \{0 + 10 = 10,\ 3 + \infty = \infty,\ 2 + 3 = 5\} = 5$,
  - $v(5) = min\ \{0 + \infty = \infty,\ 3 + \infty = \infty,\ 2 + l_{4,5} = 2 + 2 = 4\} = 4$,
  - $v(6) = min\ \{0 + \infty = \infty,\ 3 + 9 = 12,\ 2 + l_{4,6} = 2 + 8 = 10\} = 10$
  - $v(7) = min\ \{0 + \infty = \infty,\ 3 + \infty = \infty,\ 2 + l_{4,7} = 2 + \infty = \infty\} = \infty$.

  Par suite, $min\ \{v(3),v(5),v(6),v(7)\} = v(5) = 4$. $V = (\underline{0},\underline{3},5,\underline{2},\underline{4},10,\infty)$ et $T = \{1,2,4,5\}$.
- Etape 4 : Pour tous les sommets $j \in S \setminus T = \{3,6,7\}$ calculons $v(j) = min\ \{v(1) + l_{1,j},\ v(2) + l_{2,j},\ v(4) + l_{4,j},\ v(5) + l_{5,j}\}$, soit $v(j) = min\ \{0 + l_{1,j},\ 3 + l_{2,j},\ 2 + l_{4,j},\ 4 + l_{5,j}\}$. Cela donne
  - $v(3) = min\ \{0 + 10 = 10,\ 3 + \infty = \infty,\ 2 + 3 = 5,\ 4 + 4 = 8\} = 5$,
  - $v(6) = min\ \{0 + \infty = \infty,\ 3 + 9 = 12,\ 2 + 8 = 10,\ 4 + 1 = 5\} = 5$
  - $v(7) = min\ \{0 + \infty = \infty,\ 3 + \infty = \infty,\ 2 + \infty = \infty,,\ 4 + 6 = 10\} = 10$.

  Alors $min\ \{v(3),v(6),v(7)\} = v(3) = v(6) = 5$. $V = (\underline{0},\underline{3},\underline{5},\underline{2},\underline{4},\underline{5},10)$ et $T = \{1,2,3,4,5,6\}$. Ici on a traité deux sommets à la fois, ce qui fait que l'on saute une étape (l'étape 5).
- Etape 6 : Pour le sommet restant 7 on a : $v(7) = min\ \{v(i) + l_{i,7},\ i = 1,\ldots,6\}$, soit $v(7) = min\ \{0 + l_{1,7},\ 3 + l_{2,7},\ 5 + l_{3,7}\ 2 + l_{4,7},\ 4 + l_{5,7},\ 5 + l_{6,7}\}$. Ce qui donne $v(7) = min\ \{0 + \infty = \infty,\ 3 + \infty = \infty,\ 5 + \infty = \infty,\ 2 + \infty = \infty,\ 4 + 6 = 10,\ 5 + 3 = 8\} = 8$. Par conséquent, $V = (\underline{0},\underline{3},\underline{5},\underline{2},\underline{4},\underline{5},\underline{8})$ et $T = \{1,2,3,4,5,6,7\} = S$. Ce qui met fin à l'algorithme.

On vérifiera sans peine que le coût minimum pour aller de 1 à 7 est égal à 8, cela correspond au chemin (1,4,5,6,7). En général, on range les calculs intermédiaires dans un tableau... Nous renvoyons les lecteurs désireux d'approfondir la question à des ouvrages de base sur les graphes.

Bibliographie

[1] A. AHO, JEFFREY ULLMAN, Concepts fondamentaux de l'informatique, DUNOD, 1993.

[2] D.BEAUQUIER, J.BERSTEL, P.CHRETIENNE, Eléments d'algorithmique, MASSON, 1992.

[3] C.BERGE, Graphes et hypergraphes , DUNOD, 1983.

[4] T. CORMEN, C. LEISERSON, R. RIVEST, Introduction à l'algorithmique, DUNOD,1994.

[5] F. DROESBEKE, M. HALLIN, CI. LEFEVRE, Les graphes par l'exemple, Ellipse, 1987.

[6] J.L. FOUQUET, J.M. VANHERPE, Université du Maine, Quelques éléments de théorie des graphes, (Polycopié IREM).

[7] Groupes de travail «liaison Lycées-Université» et «Informatique» de l'IREM d'Aix-Marseille, Graphes pour la spécialité de terminale E.S., Faculté des sciences de Luminy - IREM d'Aix-Marseille, 2002.

[8] A. S. KECHRIS, Classical Descriptive Set Theory, Springer-Verlag. New York 1995.

[9] Mathématiques Terminale ES, Enseignement obligatoire et de spécialité, par une équipe de l'IREM de Poitiers, Bréal, 2002.

[10] Ministère de l'Education Nationale, www.eduscol.education.fr/index.php?./D0015/graphes.htm

[11] Aimé Sache, La théorie des graphes, Que sais-je 1954, 1974.

[12] J. SAKAROVITCH, Eléments de théorie des automates, Vuibert, 2003.