LINGI1101

Logique et Structures Discrètes

Titulaire : Peter Van Roy

2014

Table des matières

Remerciements

Je tiens à remercier les étudiants de LINGI1101 pour avoir pris des notes pendant mon cours, ce qui faisait la base de ce syllabus. Les contributeurs sont : Antoine Walsdorff, Goeric Huybrechts, Romane Schelkens, Nicolas Van Wallendael, Kilian Verhetsel, Cyril de Vogelaere, Jonathan Legat, Siciliano Damiano-Joseph, Aghakhani Ghazaleh, Kühn Alexandre, Maas Dylan, Paulus Aloïs, De Droogh Joachim, André William, Vandeputte Cassandre, Julémont Léonard, Surquin Corentin, Ahad Ivan, Thuin Florian, Malingreau Alexandre, Vaessen Tanguy, De Cocq Aymeric, Powell Jonathan, Pignolet Aurélien, Bollen Thomas, Mondry Laurent, Leurquin Guillaume, Bertaux Jérôme, Palumbo François, Clémenti Florent, Lambin Grégoire, Lambot Sue, de Saint-Hubert Olivier, Istasse Maxime, Sayez Niels, De Grove Gil, De Maeyer Julien, Lepinois Loïc, Vander Schueren Grégory, Van Den Eeckhaut Kim, De Bels Tanguy, Cambier Rodolphe, Demesmaeker Florian, Deplasse Victor, Colard Pierre-Olivier, Sautelet Caroline, Lejoly Florent, Vanden Bulcke Cédric, Demaude Guillaume, Ivinza Mbe Scott, Georges Benjamin, Dizier Romain, Kerger Zacharie, Larigaldie Nathanaël, Russello Helena, Visschers Marie, Grynczel Wojciech, Hauet Alexandre, Jacquet Charles, Lemaire Jérôme, Degryse Baptiste, Moubarak Joey, Wenders Audrey, Vrielynck Nicolas, Henneton Romain, Gusbin Quentin, Gerniers Alexander, Ndizera Eddy, El Jilali Solaiman, Dhillon Sundeep, Rens Maxime, Hardy Maxime, Haven David, Francotte Florian, de Potter d'Indoye Aurian, Dechamps Anthony, Ninane Charles, Mokaddem Sami, Deconinck Guillaume, Dubois Robin, Pierret Alexis, De Mol Maxime, De Ryck Aurélien, Marinx Olivier, Marinx Denis, Candaele Simon, Dagnely Vincent, Dethise Arnaud, Bellenger Jordan, Schmitz Loic, Hofs Sylvian.

Introduction au cours LINGI1101

Le cours "*Logique et Structures discrètes*" a deux buts importants :

— Donner la motivation et l'intuition de la logique, pour que cette matière devienne véritablement utile pour les étudiants.
— Donner les concepts et les formalismes mathématiques nécessaires pour utiliser la logique à bon escient.

L'intuition est donc importante pour ce cours, néanmoins, la connaissance des formalismes mathématiques reste essentielle. Le cours sera coté sur les deux : intuitions (un tiers) et formalismes (deux tiers).

Déroulement du cours

Le cours est composé de deux parties. La première partie, *logique formelle*, représentera deux tiers du cours. La seconde partie, *structures discrètes sur Internet*, comptera quant à elle pour un tiers du cours.

L'évaluation de ce cours se compose de trois parties. Il y aura tout d'abord une interrogation au milieu du quadrimestre portant sur 5 points. Il vous sera également demandé de prendre note pendant une heure de cours par groupe de trois, ceci afin de contribuer au syllabus. Ces notes prises au cours rapporteront au maximum 2 points de la note finale à chacun des participants. L'examen sera divisé en deux parties. La première partie sur 5 points portera sur la matière de l'interrogation. La note retenue sera le maximum entre la note de l'interrogation et celle obtenue à la question de l'examen. La seconde partie de l'examen sera donc cotée sur 13 points et portera sur le reste de la matière.

Afin de suivre ce cours, nous nous baserons sur deux livres de référence

correspondants chacun à une partie du cours :

— Introductory Logic and Sets for Computer Scientists, by *Nimal Nissanke.*
— Networks, Crowds, and Markets : Reasoning About a Highly Connected World, by *David Easley and Jon Kleinberg.* [1]

La première partie sera complétée par des sujets et exercices plus avancés qui approfondissent le traitement du livre.

Plan du cours

Cette partie va parler du rôle des raisonnements et des différentes formes de raisonnement. Nous prendrons en exemple la méthode scientifique.

Logique des propositions

La logique des propositions est un langage formel constitué d'une syntaxe et d'une sémantique. La syntaxe décrit l'ensemble des formules qui appartiennent au langage. La sémantique permet de donner un sens aux formules de langage. C'est une logique très ancienne qui vient de l'antiquité.

Logique des prédicats

C'est une logique beaucoup plus expressive et la plupart des travaux mathématiques peuvent être écrits dans ce langage [2]. Elle est aussi définie comme la logique du premier ordre. [3] En logique des prédicats, les éléments de base du langage ne sont plus des propositions, mais des prédicats.

Interprétations et modèles

La logique a besoin d'un langage, de phrases pour la décrire. Cette section couvrira donc la sémantique à utiliser.

Théorie de la preuve

Nous pouvons manipuler une phrase en logique pour obtenir un résultat. Par exemple, si A et B sont vrais, nous pouvons en déduire que A est vrai. Il y a des règles d'inférences à utiliser pour prendre une phrase en logique et en

1. Quelques chapitres.
2. Elle est un effet un parfait compromis entre expressivité et efficacité.
3. Il existe d'autres formes de logiques plus expressives, mais plus difficiles à utiliser. Exemple : la logique du deuxième ordre.

déduire une autre. Une preuve mathématique est une séquence de phrases liées par des règles d'inférences.

Algorithme de preuve

C'est l'algorithme le plus puissant qui existe en logique des prédicats. Néanmoins, il est inefficace seul. Afin de le rendre efficace, il faut poser des hypothèses. Nous approfondirons ce problème dans le cadre de cette section.

Théorie logique

Il est possible de formaliser tout objet mathématique avec une théorie logique qui lui est propre. En exemple, citons la théorie des ensembles, des fonctions et des ordres partiels.

Programmation logique

Le rêve serait de pouvoir exprimer toute chose logique en langage de programmation efficace. Il s'agira d'appliquer ce principe avec l'algorithme de preuve, sur base d'hypothèses.

Première partie

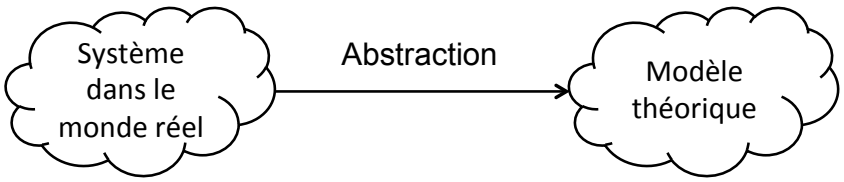
Logique formelle

Chapitre 1

Contexte : la méthode scientifique

1.1 Formalisation d'un système

Comment pouvons-nous formaliser un système dans le monde réel tels que les champs magnétiques ou la gravitation ?

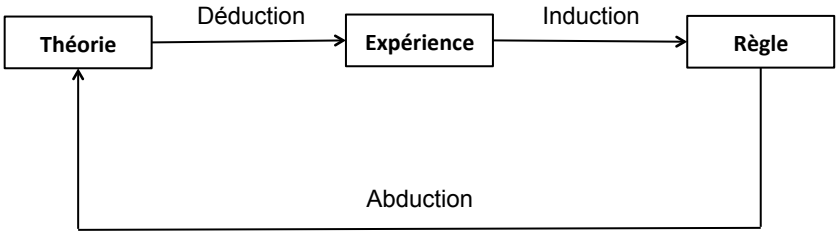


Afin de formaliser un système dans le monde réel, nous devons faire une abstraction vers un modèle théorique. Ce modèle théorique, aussi appelé théorie, est un ensemble de phrases logiques dont il est possible de tirer des prédictions en utilisant le raisonnement déductif. Il n'est intéressant que s'il se comporte comme le vrai système.

Un exemple de cette formalisation pourrait être les équations de Maxwell qui sont le modèle théorique correspondant pour l'électromagnétisme.

1.2 Boucle de raisonnement

Il existe trois formes de raisonnement : la déduction, l'induction et l'abduction. Ces trois formes de raisonnement peuvent être liées dans une boucle de raisonnement de la façon suivante :



1.2.1 Déduction

Il s'agit de faire des calculs et des raisonnements logiques par rapport à une théorie. Avec ces raisonnements, on déduit le résultat qu'une expérience donnerait selon la théorie. Par exemple, en utilisant les équations de Maxwell on peut déduire le trajectoire d'un objet avec une charge électrique dans un champ électromagnétique.

1.2.2 Induction

L'induction est le fait de trouver une règle générale à partir des expériences répétées. On choisit en général une règle moyenne qui deviendra la règle générale. Il faut souligner que les résultats expérimentaux ne sont pas totalement fiables ou complets. Dès lors, la règle trouvée n'est pas nécessairement exacte. Par exemple, si par induction nous avons trouvé la règle, "les oiseaux volent", cela est vrai tant que l'on n'a pas vu un pingouin. Autre exemple, nous pouvons supposer que demain le soleil va se lever comme depuis des milliers d'années, même si rien ne l'assure.

1.2.3 Abduction

On compare la règle générale trouvée lors de l'induction avec la théorie. S'il y a une incohérence entre la règle générale et la théorie qui ne rentre pas dans la marge d'erreur expérimentale, on suppose qu'il y a une erreur dans la théorie. Il faut alors corriger la théorie existante ou en inventer/deviner une nouvelle. Ce type de raisonnement s'appelle l'abduction : trouver une *explication* (= la théorie corrigée) pour une règle ou un fait. On applique l'abduction couramment dans la vie de tous les jours ; par exemple, lorsqu'un élève entre trempé dans la classe, nous supposons qu'il pleut dehors. La pluie est une explication possible pour l'état de l'élève.

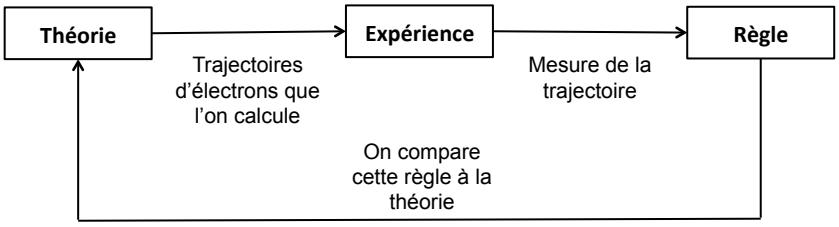
1.2.4 Conclusion

Sur ces trois formes de raisonnement, seule la déduction est un raisonnement sûr. Les deux autres, l'induction et l'abduction, peuvent donner des erreurs. Malgré cela, les trois formes sont tout aussi importantes. Par example, il faut les trois pour expliquer comment marche la méthode scientifique. Dans l'état actuel de la science du raisonnement, nous comprenons beaucoup mieux la déduction que l'induction et l'abduction. Toute la logique mathématique est une approfondissement de la science de la déduction. Nous nous focaliserons dans ce cours uniquement sur la déduction.

1.3 Exemples

1.3.1 Loi de Maxwell

Nous illustrons dès à présent le fonctionnement de la boucle de raisonnement à l'aide de l'exemple cité plus haut, c'est-à-dire les équations de Maxwell :



Par déduction, grâce à la théorie et aux conditions initiales que nous fixons, nous calculons la trajectoire d'un électron. Nous effectuons ensuite des mesures dans le monde réel. Nous allons, par exemple, mesurer la trajectoire plusieurs fois avec des méthodes différentes et, par induction, nous trouvons une règle qui est la loi de comportement de la particule. Nous comparons ensuite cette règle à la théorie, et nous la corrigeons si besoin. La création d'une théorie qui explique la règle trouvée est une abduction.

1.3.2 Sac de billes

Afin d'illustrer les 3 formes de raisonnements de manière plus formelle, considérons un sac de billes pouvant contenir des billes noires ou blanches.

Notons que sac(x) signifie "la bille x est dans le sac" et que blanc(x) signifie "la bille x est blanche".

Déduction

1. Règle : $\forall\ x,\ sac(x) \Rightarrow blanc(x)$
2. Cas : $sac(a),\ sac(b),\ \cdots$

---

3. Résultat : $blanc(a),\ blanc(b),\ \cdots$

Si toutes les billes se trouvant dans le sac sont blanches et que l'on pioche une bille de ce sac, cette bille sera blanche. Cette déduction est forcément correcte.

Induction

1. Cas : $sac(a),\ sac(b),\cdots$
2. Résultat : $blanc(a),\ blanc(b),\ \cdots$

---

3. Règle : $\forall\ x,\ sac(x) \Rightarrow blanc(x)$

Si toutes les billes que l'on pioche du sac sont blanches, alors nous pouvons établir comme règle que toutes les billes dans le sac sont blanches. Cette induction n'est pas forcément correcte.

Abduction

1. Règle : $\forall\ x,\ sac(x) \Rightarrow blanc(x)$
2. Résultat : $blanc(a),\ blanc(b),\ \cdots$

---

3. Cas : $sac(a),\ sac(b),\ \cdots$

Si toutes les billes se trouvant dans le sac sont blanches et que nous trouvons des billes blanches à côté du sac, nous pouvons penser qu'elles viennent du sac. L'explication pour la couleur des billes trouvées est qu'elles viennent du sac. Cette abduction n'est pas forcément correcte.

Chapitre 2

La logique propositionnelle

> « *They don't even need to know what they're talking about.* » — Richard Feynman à propos des mathématiciens.

La logique propositionnelle est la plus simple des formes de logique. Elle permet de formaliser des connexions logiques entre des propositions. Par exemple, prenons les expressions suivantes :

1. « S'il fait beau, alors je vais dehors. »
2. « Cet homme est grand et fort. »
3. « Il fait jour mais pas nuit. »

Dans ces expressions, nous pouvons définir des propositions premières :

1. il fait beau ;
2. je vais dehors ;
3. cet homme est grand ;
4. cet homme est beau ;
5. il fait jour ;
6. il fait nuit.

Le sens de ces propositions en langue naturelle n'a aucune importance dans la logique propositionnelle. C'est pourquoi elles seront remplacées par des lettres majuscules :

1. A = « il fait beau » ;
2. B = « je vais dehors » ;
3. C = « cet homme est grand » ;
4. D = « cet homme est beau » ;

5. E = « il fait jour » ;
6. F = « il fait nuit ».

Une proposition logique est alors :

— soit une des propositions premières ;
— soit une combinaison de propositions logiques connectées par des connecteurs logiques.

Ainsi, les exemples de propositions précédentes peuvent être réécrits comme ceci (la signification précise des différents symboles sera décrite plus loin) :

1. $A \Rightarrow B$;
2. $C \wedge D$;
3. $E \wedge \neg F$.

L'avantage de cette notation par rapport aux phrases en français est qu'elle nous permet d'effectuer des raisonnements formels sur les propositions logiques. En particulier, nous pouvons précisément définir :

1. une *syntaxe* (définie par une grammaire) qui définit ce qui est une proposition logique et ce qui ne l'est pas ;
2. une *sémantique* qui donne un sens à chaque proposition logique ;
3. une *théorie de preuve* permettant, en sachant qu'une proposition est vraie, de trouver d'autres propositions vraies (par exemple à partir de $A \Rightarrow B$ on peut trouver $\neg B \Rightarrow \neg A$).

2.1 La syntaxe

La logique propositionnelle est un *langage formel*. Ce langage peut être défini à l'aide d'une grammaire sur un *alphabet*. L'alphabet est l'ensemble des symboles qui composent une proposition logique, c'est-à-dire :

— les lettres majuscules représentant les différentes propositions premières : A, B, C, etc. ;
— true et false qui représentent des propositions qui sont respectivement toujours vraies et toujours fausses ;
— les différents connecteurs logiques :
  — Conjonction (« et ») : $\wedge$
  — Disjonction (« ou ») : $\vee$
  — Négation : $\neg$
  — Implication : $\Rightarrow$
  — Équivalence : $\Leftrightarrow$

— les caractères de ponctuation « (» et «) ».

Cependant, toutes les séquences composées de ces caractères ne sont pas des phrases propositionnelles. La grammaire suivante permet de donner les règles que les phrases propositionnelles doivent respecter :

$$
\begin{array}{rcl}
\text{<identificateur>} & ::= & A \mid B \mid C \mid D \mid \ldots \\
\text{<proposition>} & ::= & \text{true} \\
& \mid & \text{false} \\
& \mid & \text{<identificateur>} \\
& \mid & (\text{<proposition>}) \\
& \mid & \neg\text{<proposition>} \\
& \mid & \text{<proposition>} \wedge \text{<proposition>} \\
& \mid & \text{<proposition>} \vee \text{<proposition>} \\
& \mid & \text{<proposition>} \Rightarrow \text{<proposition>} \\
& \mid & \text{<proposition>} \Leftrightarrow \text{<proposition>}
\end{array}
$$

Remarquez que seules les séquences de symboles qui respectent cette grammaire sont des phrases propositionnelles. Ainsi, $p \Leftrightarrow q$ n'est *pas* une phrase propositionnelle parce que les propositions premières doivent *toujours* être représentées par des lettres majuscules ; de même les phrases en français — ou en klingon, ou encore dans d'autres formalismes mathématiques – comme « s'il fait beau alors je vais dehors » ne respectent pas la grammaire précédente et ne sont donc pas des phrases propositionnelles.

Métalangage Notez que notre discours (en français et en notation mathématique) à propos des phrases propositionnelles n'est pas une phrase propositionnelle. La grammaire précédente, la description de l'alphabet, et cette explication en français parlent de propositions logiques sans en être, et font donc partie de ce qui est appelé le *métalangage*. Un métalangage est un deuxième langage utilisé pour parler d'un premier langage. Dans notre discours, le premier langage est la logique propositionnelle, et le deuxième langage est le français augmenté avec des notations mathématiques.

Le concept de métalangage est important pour distinguer le raisonnement formel (en utilisant les opérations logiques définies formellement) et le raisonnement informel (typiquement en langage naturel augmenté par des notations mathématiques). Le raisonnement informel reste très important, même si le but ultime est de faire le plus possible en raisonnement formel, parce qu'il est plus facile d'éviter des erreurs de raisonnement dans un raisonnement formel.

2.2 Les tables de vérité

La grammaire définie dans la section précédente permet d'écrire les propositions en logique propositionnelle, mais elle ne leur donne pas un sens, c'est-à-dire de définir quand une proposition est vraie ou fausse. Plus précisément, le sens d'une proposition s'appelle la sémantique de la proposition. Pour savoir si une proposition est vraie ou fausse, il faut commencer par choisir pour chacune de ses propositions premières si elle est vraie ou fausse. Ensuite on peut déterminer si la proposition est vraie ou fausse. Il y a deux approches principales pour faire cela : les *tables de vérité* et les *interprétations*. Dans cette section nous expliquerons les tables de vérité. Dans la section suivante nous expliquerons les interprétations.

Rappelez-vous que la signification des propositions premières n'a aucune importance, le choix de sa véracité est donc complètement arbitraire. Le choix qui décrit au mieux le monde réel n'est qu'un des choix possibles parmi tous les autres. On sait également que les propositions true et false sont, respectivement, toujours vraies et toujours fausses.

Les autres propositions sont construites à partir de propositions plus simples. Leur véracité est fonction de celle des propositions qui les composent. Prenons par exemple $p \wedge q$, où p et q sont d'autres propositions. La véracité de $p \wedge q$ est une fonction de celle de p et de q : $p \wedge q$ est vrai si et seulement si p et q sont vrais aussi ($\wedge$ est un « et » logique). Cette relation peut être exprimée à l'aide de la table de vérité suivante :

p	q	$p \wedge q$
true	true	true
true	false	false
false	true	false
false	false	false

Voici la table de vérité des autres connecteurs logiques :

p	q	$p \vee q$
true	true	true
true	false	true
false	true	true
false	false	false

p	q	$p \Leftrightarrow q$
true	true	true
true	false	false
false	true	false
false	false	true

p	$\neg p$
true	false
false	true

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

Remarquez que le dernier tableau est correct. Il n'est parfois pas intuitif que la proposition $A \Rightarrow B$ (qui pourrait s'exprimer en français par « si A, alors B ») soit toujours vraie quand A est faux, mais c'est pourtant le cas : la proposition dit que quand A est vrai, B doit l'être aussi, mais elle ne donne aucune information sur le cas où A est faux.

Les parenthèses, quant à elles, servent à distinguer des propositions telles que $A \wedge (B \vee C)$ et $(A \wedge B) \vee C$, qui s'écriraient de la même manière sans parenthèses alors qu'elles n'ont pas la même table de vérité :

A	B	C	$A \wedge (B \vee C)$	$(A \wedge B) \vee C$
true	true	true	true	true
true	true	false	true	true
true	false	true	true	true
true	false	false	false	false
false	true	true	false	true
false	true	false	false	false
false	false	true	false	true
false	false	false	false	false

2.3 Les interprétations

Une autre façon de définir si une proposition est vraie ou fausse est d'utiliser une *interprétation*. Si E_P est l'ensemble des propositions premières, alors une interprétation I définit la fonction $\text{val}_I : E_P \to \{\text{true}, \text{false}\}$ qui permet de savoir si ces propositions premières sont vraies ou fausses. [1] Par exemple, on pourrait écrire ceci :

$$\text{val}_I(A) = \text{true}$$
$$\text{val}_I(B) = \text{false}$$
$$\text{val}_I(C) = \text{true}$$

1. La notation $f : A \to B$ signifie que f est une fonction depuis l'ensemble A vers l'ensemble B.

Étant donné la fonction val_I, il est possible de définir la fonction $\text{VAL}_I : P \to \{\text{true}, \text{false}\}$, qui est une extension de val_I à P, l'ensemble de toutes les propositions. L'équivalent des tables de vérité pourrait être des expressions telles que :

$$\forall p \in E_P . \text{VAL}_I(p) = \text{val}_I(p)$$

$$\text{VAL}_I(p \wedge q) = \begin{cases} \text{true si VAL}_I(p) = \text{true et VAL}_I(q) = \text{true} \\ \text{false sinon} \end{cases}$$

$$\text{VAL}_I(p \vee q) = \begin{cases} \text{false si VAL}_I(p) = \text{false et VAL}_I(q) = \text{false} \\ \text{true sinon} \end{cases}$$

$$\text{VAL}_I(\neg p) = \begin{cases} \text{false si VAL}_I(p) = \text{true} \\ \text{true si VAL}_I(p) = \text{false} \end{cases}$$

$$\text{VAL}_I(p \Leftrightarrow q) = \begin{cases} \text{true si VAL}_I(p) = \text{VAL}_I(q) \\ \text{false sinon} \end{cases}$$

$$\text{VAL}_I(p \Rightarrow q) = \begin{cases} \text{false si VAL}_I(q) = \text{false alors que VAL}_I(p) = \text{true} \\ \text{true sinon} \end{cases}$$

Prenons un exemple concret, utilisons une interprétation pour étudier la phrase suivante : « S'il fait beau à midi, j'irai promener le chien ». Nous devons d'abord traduire cette phrase en l'une des propositions du formalisme que nous avons défini, en commençant par identifier les propositions premières :

1. B = « Il fait beau » ;
2. M = « Il est midi » ;
3. P = « Je vais promener le chien » ;

Identifions également les connecteurs à employer : « s'il fait beau $\wedge$ qu'il est midi $\Rightarrow$ j'irai promener le chien ». En combinant ces deux résultats, nous obtenons la phrase propositionnelle $(B \wedge M) \Rightarrow P$.

Interprétons désormais notre proposition à l'aide de l'interprétation suivante :

1. Il fait beau : $\text{val}_I(B) = \text{true}$;

2. Il est midi : $\text{val}_I(M) = \text{true}$;
3. Je n'irai pas promener le chien : $\text{val}_I(P) = \text{false}$.

Nous pouvons alors effectuer le développement suivant :

$$VAL_I((B \wedge M) \implies P) = \begin{cases} false \text{ si } VAL_I(P) = false \text{ alors que } VAL_I(B \wedge M) = true \\ true \text{ sinon} \end{cases}$$

$$VAL_I(B \wedge M) = \begin{cases} true \text{ si } VAL_I(B) = true \text{ et } VAL_I(M) = true \\ false \text{ sinon} \end{cases}$$

Dans notre cas :

$$val_I(B \wedge M) = true \wedge true = true$$

Donc :

$$val_I((B \wedge M) \implies P) = true \implies \text{false} = false$$

Nous pouvons donc en conclure que, dans cette interprétation, la personne ayant fait cette affirmation a menti. Notons néanmoins que notre homme n'aurait pas menti en partant promener le chien alors qu'il pleuvait à midi, rien n'ayant été dit sur ce qu'il ferait dans le cas où il ne ferait pas beau.

2.4 Les modèles logiques

Dans le premier chapitre, nous avons parlés de modèles théoriques (ou théories) d'un système dans le monde réel. Dans le contexte de la méthode scientifique, nous avons fait de la déduction à partir de ces modèles théoriques. Maintenant que nous avons introduit notre première logique et sa sémantique, nous pouvons rendre ces notions plus concrètes.

À partir de la notion d'interprétation, nous pouvons définir ce qu'est un *modèle*. Soit $B = \{b_1, b_2, \ldots, b_n\}$ un ensemble de propositions logiques. Une interprétation I est un modèle de B si et seulement si $\forall b_i \in B.\text{VAL}_I(b_i) = \text{true}$. Autrement dit, I décrit un univers qui respecte toutes les règles se trouvant dans l'ensemble B.

Dans l'exemple de la section précédente, l'interprétation choisie n'est donc pas un modèle de la proposition analysée, celle-ci n'étant pas validée. Par contre, l'interprétation telle que $\text{val}_I(B) = \text{true}$, $\text{val}_I(M) = \text{true}$ et $\text{val}_I(P) = \text{true}$ est bien un modèle de la proposition utilisée comme exemple. Remarquez aussi que cela ne change rien au fait que l'interprétation choisie soit le modèle d'autres propositions que celle étudiée ou non (par exemple $B \wedge M$).

Les tautologies : Pour certaines propositions, toute interprétation est un modèle, c'est-à-dire que ces propositions sont toujours vraies. Par exemple, true est évidemment une tautologie, de même que $A \Rightarrow A$ ou encore $A \vee \neg A$. Le fait qu'une proposition p est une tautologie se note $\vDash p$.

Les contradictions : Pour d'autres propositions, il n'existe aucun modèle, c'est-à-dire qu'elles sont toujours fausses. Par exemple $A \wedge \neg A$ est une contradiction. Le fait qu'une proposition p est une contradiction se note $\nvDash p$.

Les contingences : Toutes les autres propositions sont des contingences. Il existe des interprétations qui sont des modèles et d'autres qui n'en sont pas. Par exemple $A \wedge B$ est vrai pour l'interprétation I telle que $\mathrm{val}_I(A) = \mathrm{val}_I(B) = \mathrm{true}$, mais faux dans tous les autres cas.

2.4.1 Conséquence logique

p est conséquence logique de q si et seulement si $p \Rightarrow q$ est une tautologie. En d'autres termes, si

$p \models q$	q est valide dans tous les modèles de p
alors	
$\models (p \Rightarrow q)$	$p \Rightarrow q$ est une tautologie.
On peut donc écrire	
$p \Rrightarrow q$	p est conséquence logique de q.

Cependant, la conséquence logique ($\Rrightarrow$) n'est pas une proposition logique, mais fait partie du métalangage (cf. syntaxe d'une proposition).

2.4.2 Équivalence logique

Par le raisonnement ci-dessus, on peut dire que p est logiquement équivalent à q si et seulement si

$p \models q$	q est valide dans tous les modèles de p
$q \models p$	p est valide dans tous les modèles de q
et donc	
$\models (p \Rightarrow q)$	$p \Rightarrow q$ est une tautologie et
$\models (q \Rightarrow p)$	$q \Rightarrow p$ est une tautologie.
On peut donc écrire	
$p \Lleftarrow\Rrightarrow q$	p sont logiquement équivalents q.

L'équivalence logique n'est pas non plus une proposition logique.

Il ne faut pas non plus oublier la différence entre phrase propositionnelle (p, q, s,...) et propositions premières (P, Q, S,...) (cf. syntaxe d'une proposition) :

	$p \Rightarrow q$	n'est pas une proposition
mais		
	$P \wedge Q \Rightarrow R \wedge \neg S$	en est bien une.

Chapitre 3

Preuves en logique propositionnelle

Une preuve est un raisonnement déductif qui démontre si une proposition est vraie ou fausse. On distingue des preuves informelles et des preuves formelles. Une preuve informelle est un raisonnement en langage naturel, parfois augmenté avec des notations mathématiques. Une preuve formelle est un objet mathématique qui formalise le raisonnement déductif. Un des buts de la logique mathématique est de prouver le plus possibles des résultats mathématiques avec des preuves formelles.

Au 20ème siècle les mathématiciens sont arrivés à prouver la plupart des mathématiques classiques (telles qu'utilisées par des ingénieurs) avec des preuves formelles. Un des résultats les plus célèbres est la preuve formelle du théorème des quatre couleurs, fait par Georges Gonthier et Benjamin Werner avec l'assistant de preuve Coq (un logiciel qui automatise la plupart des manipulations formelles nécessaires). Ce théorème dit que toute carte découpée en régions connexes peut être colorée avec seulement quatre couleurs, de sorte que deux régions adjacentes ont toujours des couleurs distinctes.

Dans ce chapitre nous allons définir des preuves formelles pour la logique propositionnelle. Nous présenterons trois approches :

— Table de vérité
— Preuve transformationnelle
— Preuve déductive (la plus générale)

3.1 Preuve avec table de vérité

La preuve formelle la plus simple est une table de vérité. Prouvons que $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$ est vrai :

P	Q	$\neg P$	$\neg Q$	$(\neg P \vee \neg Q)$	$P \wedge Q$	$(\neg P \vee \neg Q)$
F	F	T	T	***T***	F	***T***
T	F	F	T	***T***	F	***T***
F	T	T	F	***T***	F	***T***
T	T	F	F	***F***	T	***F***

On peut constater que le vecteur de vérité de $\neg(P \wedge Q)$ est équivalent à celui de $(\neg P \vee \neg Q)$. La preuve a donc vérifié la véracité de la proposition. Notez qu'une table de vérité est un objet mathématique en métalangage parce qu'elle n'est pas une proposition.

L'inconvénient de cette méthode de preuve est qu'elle devient rapidement très lourde quand le nombre de propositions premières augmente. Il faut en effet 2^n lignes dans la table pour n propositions.

3.2 Preuve transformationnelle

Une preuve transformationnelle est une séquence de transformations $p_1 \Lleftrightarrow p_2 \Lleftrightarrow \cdots \Lleftrightarrow p_n$, dans laquelle on a toujours $p_i \Lleftrightarrow p_{i+1}$ (équivalence logique entre éléments adjacents dans la séquence). Une preuve transformationnelle est aussi un objet mathématique en métalangage. Pour faciliter la création d'une preuve transformationnelle, on utilise des "Lois", c'est-à-dire des équivalences connues.

$p \Lleftrightarrow p \vee p$	Idempotence
$p \vee q \Lleftrightarrow q \vee p$	Commutativité
$(p \vee q) \vee r \Lleftrightarrow p \vee (q \vee r)$	Associativité
$\neg\neg p \Lleftrightarrow p$	Double Négation
$p \Rightarrow q \Lleftrightarrow \neg p \vee q$	Implication
$\neg(p \wedge q) \Lleftrightarrow \neg p \vee \neg q$	1^{ere} loi de De Morgan
$p \Leftrightarrow q \Lleftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$	Équivalence

On ajoute deux règles supplémentaires : la transitivité et la substitution.

Transitivité de l'équivalence

Si $p \Lleftrightarrow q$ et $q \Lleftrightarrow r$, alors $p \Lleftrightarrow r$.

Substitution

Il est autorisé de remplacer une formule par une formule équivalente à l'intérieur d'une autre formule. Autrement dit :

Soit p,q,r des formules propositionnelles.

Si $p \Leftrightarrow q$ et $r(p)$, alors $r(p) \Longleftrightarrow r(q)$.
On peut remplacer p par q car elles sont équivalentes.

Exemple

On veut prouver : $p \wedge (q \wedge r) \Longleftrightarrow (p \wedge q) \wedge r$

$$
\begin{array}{ll}
p \wedge (q \wedge r) & \Longleftrightarrow p \wedge \neg\neg(q \wedge r) \\
& \Longleftrightarrow p \wedge \neg(\neg q \vee \neg r) \\
& \Longleftrightarrow \neg\neg(p \wedge \neg(\neg q \vee \neg r)) \\
& \Longleftrightarrow \neg(\neg p \vee \neg\neg(\neg q \vee \neg r)) \\
& \Longleftrightarrow \neg(\neg p \vee (\neg q \vee \neg r)) \\
& \Longleftrightarrow \neg((\neg p \vee \neg q) \vee \neg r) \\
& \vdots \\
& \text{effectuer les mêmes lois dans le sens contraire} \\
& \vdots \\
& \Longleftrightarrow (p \wedge q) \wedge r
\end{array}
$$

Le problème de cette méthode de preuve est qu'elle requiert de l'intuition, de la créativité. Elle n'est donc pas forcément plus efficace que les tables de vérité, surtout si "l'astuce" est difficile à trouver.

3.3 Preuve déductive

Une preuve déductive est un objet mathématique qui formalise une séquence de pas de raisonnement simples. Chaque pas doit être justifié avec le nom de la règle ou la loi qui est utilisée. Les pas utilisent trois techniques de raisonnement différentes : les équivalences logiques, les règles d'inférence et les schémas de preuve. Avec ces techniques, une preuve déductive est beaucoup plus expressive qu'une preuve transformationnelle.

3.3.1 Equivalences logiques

$p \Longleftrightarrow p \vee p$	Idempotence de $\vee$
$p \vee q \Longleftrightarrow q \vee p$	Commutativité de $\vee$
$(p \vee q) \vee r \Longleftrightarrow p \vee (q \vee r)$	Associativité de $\vee$
$\neg\neg p \Longleftrightarrow p$	Double Négation
$p \Rightarrow q \Longleftrightarrow \neg p \vee q$	Implication
$\neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q$	1^{ere} loi de De Morgan
$\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q$	2^{eme} loi de De Morgan
$(p \wedge q) \vee r \Longleftrightarrow (p \vee r) \wedge (q \vee r)$	Distributivité de $\vee$

À ces équivalence nous ajoutons aussi l'idempotence, la commutativité, l'associativité et la distributivité de $\wedge$.

3.3.2 Règles d'inférence

À la différence de la preuve transformationnelle, les règles d'inférences ont une direction : elles commencent par les prémisses et se terminent par la conclusion. Pour chaque règle, si les prémisses sont vraies, alors la conclusion est vraie. Nous utilisons un raisonnement informel pour justifier chaque règle.

Conjonction :

p	prémisse
q	prémisse
$p \wedge q$	Conclusion

Simplification : $\dfrac{p \wedge q}{p}$

Addition : $\dfrac{p}{p \vee q}$

Contradiction : $\dfrac{p \quad \neg p}{q}$

Double Négation : $\dfrac{\neg\neg p}{p}$

Transitivité de l'équivalence : $\dfrac{p \Leftrightarrow q \quad q \Leftrightarrow r}{p \Leftrightarrow r}$

Modus Ponens : $\dfrac{p \Rightarrow q \quad p}{q}$

Modus Tollens : $\dfrac{p \Rightarrow q \quad \neg q}{\neg p}$

Loi d'équivalence : $\dfrac{p \Leftrightarrow q}{q \Leftrightarrow p}$

3.3.3 Schémas de preuve

En plus des équivalences logiques et des règles d'inférence, nous ajoutons deux schémas de preuve qui formalisent des techniques de raisonnement plus abstraites : le théorème de déduction et la démonstration par l'absurde. Ces schémas donnent à l'approche de preuve déductive une grande expressivité, beaucoup plus qu'une preuve transformationnelle.

Théorème de déduction (preuve conditionnelle)

Pour prouver la proposition $s \Rightarrow t$, on suppose s vrai. La proposition s s'ajoute donc aux prémisses utilisées dans la preuve. Ensuite, on fait une preuve de t : on peut construire une preuve (objet mathématique) de t en commençant de s. On note ce théorème $s \vdash t$. On écrit ce schéma un peu comme une règle d'inférence :

$$\frac{p, ..., r, s \vdash t}{p, ..., r \vdash s \Rightarrow t}$$

On déduit t et donc on sait que l'hypothèse $s \Rightarrow t$ est vraie et on l'évacue.

Remarque : Il ne faut pas confondre les deux notations $p \models t$ et $p \vdash t$.

— $p \models t$ est une notion de vérité (tout modèle de p est un modèle de t), et donc de sémantique ;

— $p \vdash t$ est une notion syntaxique (en commençant de p on peut construire une preuve de t), car une preuve est une séquence de manipulations syntaxiques.

Démonstration par l'absurde (preuve par contradiction)

On suppose que les prémisses $p, ..., q$ n'ont pas de problème, c'est-à-dire qu'on ne peut pas prouver une contradiction à partir de ces propositions. Ensuite, on ajoute r aux prémisses. S'il est possible de prouver s et aussi de prouver $\neg s$, cela signifie qu'il y a une erreur dans les prémisses. On suppose que c'est l'ajout r qui est fautif. On justifie qu'il n'y a aucune contradiction dans $p, ..., q$ car on part du principe qu'il existe un modèle de $p, ...q$. On écrit ce schéma ainsi :

$$\frac{\begin{array}{c} p, ..., q, r \vdash s \\ p, ..., q, r \vdash \neg s \end{array}}{p, ..., q \vdash \neg r}$$

3.4 Exemple de preuve déductive

Nous donnons un premier exemple de preuve déductive. Voici les propositions premières :

A = "tu manges bien"

B = "ton système digestif est en bonne santé"

C = "tu pratiques une activité physique régulière"

D = "tu es en bonne forme physique"

E = "tu vis longtemps"

On peut maintenant établir une théorie, c'est-à-dire, un ensemble de propositions, dont on espère qu'elle aura un modèle.

Théorie

1. $A \implies B$
2. $C \implies D$
3. $B \vee D \implies E$
4. $\neg E$

À prouver $\neg A \wedge \neg C$

Preuve Voici la preuve déductive. Nous la mettons dans un cadre pour souligner qu'elle est un objet mathématique. Chaque ligne est où une prémisse, où un pas de raisonnement (une équivalence ou une règle d'inférence). Pour chaque ligne il faut donner le nom de la règle qui est appliquée, cela s'appelle la *justification* et c'est une partie importante de la preuve. Les deux schémas se présentent avec des indentations ; la partie indentée d'une preuve contient une prémisse en plus (s pour la preuve conditionnelle, r pour la preuve indirecte).

1. A⇒B	prémisse
2. C⇒D	prémisse
3. B∨D ⇒E	prémisse
4. ¬E	prémisse
5. A	hypothèse
6. B	modus ponens (1)
7. B∨D	addition (6)
8. E	modus ponens (7)
9. ¬A	preuve indirecte
10. C	hypothèse
11. D	modus ponens (2)
12. D∨B	addition (11)
13. B∨D	commutativité (12)
14. E	modus ponens (9)
15. ¬C	preuve indirecte
16. ¬A ∧ ¬C	conjonction (9,15)

Les quatre premières lignes introduisent les prémisses (les propositions de la théorie). La ligne 5 commence une première preuve indirecte : on fait l'hypothèse A et ensuite on déduit E (sur la ligne 8). C'est une contradiction avec la prémisse ¬E et donc on vient de prouver ¬A (sur la ligne 9). La ligne 10 commence une deuxième preuve indirecte : on fait l'hypothèse C et

ensuite on déduit E (sur la ligne 14). De nouveau, c'est une contradiction (avec la prémisse ¬E) et donc on vient de prouver ¬C (sur la ligne 15). Les justifications pour les lignes 9 et 15 sont *preuve indirecte*.

Avec cette preuve déductive, nous avons pu prouver que tu ne manges pas bien et que tu ne pratiques pas d'activité physique régulière.

3.5 Exemples de l'utilisation des schémas

Pour illustrer l'utilisation des deux schémas, la preuve conditionnelle et la preuve par contradiction, nous allons prouver la même conclusion en trois manières, avec chaque schéma et sans schéma.

— Prémisse : $(p \wedge q) \vee r$
— Conclusion : $\neg$ p $\Rightarrow$ r

3.5.1 Exemple sans schéma

1. $(p \wedge q) \vee r$	*Prémisse*
2. $r \vee (p \wedge q)$	*Commutativité en 1*
3. $(r \vee p) \wedge (r \vee q)$	*Associativité en 2*
4. $(r \vee p)$	*Simplification en 3*
5. $(p \vee r)$	*Commutativité en 4*
6. $\neg\neg p \vee r$	*Loi de la négation en 5*
7. $\neg p \Rightarrow r$	*Implication en 6*

3.5.2 Exemple de preuve conditionnelle

1. $(p \wedge q) \vee r$	*Prémisse*
2. $\neg\neg(p \wedge q) \vee r$	*Double négation en 1*
3. $\neg(\neg p \vee \neg q) \vee r$	*Loi De Morgan en 2*
4. $\neg p \vee \neg q \Rightarrow r$	*Implication en 3*
5. $\neg p$	*Hypothèse*
6. $\neg p \vee \neg q$	*Addition sur 5*
7. r	*Modus Ponens sur 4 et 6*
8. $\neg p \Rightarrow r$	*Evacuation de l'hypothèse*

3.5.3 Exemple de preuve par contradiction

1. $(p \wedge q) \vee r$	*Prémisse*
2. $(p \vee r) \wedge (q \vee r)$	*Distributivité sur 1*
3. $(p \vee r)$	*Simplification en 2*
4. $\neg(\neg p \Rightarrow r)$	*Hypothèse*
5. $\neg(\neg\neg p \vee r)$	*Implication en 4*
6. $\neg(p \vee r)$	*Négation en 5*
7. $\neg\neg(\neg p \Rightarrow r)$	*Preuve par contradiction*
8. $\neg p \Rightarrow r$	*Négation en 7*

3.6 Quelques concepts supplémentaires

3.6.1 Principe de dualité

Dans les formules sans $\rightarrow$:

$$\wedge \leftrightarrow \vee$$
$$true \leftrightarrow false$$

$$\models \neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$$
$$\models \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$$

Formule quelconque :

$$\wedge \leftrightarrow \vee$$
$$true \leftrightarrow false$$
$$p \leftrightarrow \neg p$$

Justification en raisonnant sur les modèles :

$$(p_1, ..., p_n) \models q \qquad ssi \models (p_1 \wedge ... \wedge p_n \wedge q) \leftrightarrow false$$
$$ssi \models (\neg p_1 \vee ... \vee \neg p_n \vee q) \leftrightarrow true$$

3.6.2 Algorithme de normalisation

Une formule quelconque peut être transformée en une formule équivalente de forme normale.

Forme Normale

— Conjonctive : $(p \vee q) \wedge (q \vee a) \wedge (s \vee r)$
— Disjonctive : $(p \wedge q) \vee (q \wedge a) \vee (s \wedge r)$

Terminologie

— Littéral : $P \vee \neg P \approxeq L$
— Clause : $\vee L_i = (L_1 \vee L_2 \vee L_3 \vee ... \vee L_i)$

Algorithme de normalisation

1. Eliminer les $\rightarrow$ et $\leftrightarrow$
2. Déplacer les négations vers l'intérieur (dans les propositions premières) De Morgan
3. Déplacer les disjonctions ($\vee$) vers l'intérieur
4. Simplifier $(P \vee \neg P)$

Exemple de normalisation

$(p \rightarrow (Q \rightarrow R)) \rightarrow ((P \wedge S) \rightarrow R)$
$\neg(...) \vee (...)$
$\neg(\neg P \vee (\neg Q \vee R)) \vee (\neg(P \wedge S) \vee R)$
$(\neg\neg P \wedge \neg(\neg Q \vee R)) \vee ((\neg P \vee \neg S) \vee R)$
$(P \wedge (Q \wedge \neg R)) \vee (\neg P \vee \neg S \vee R)$
$(P \vee \neg P \vee \neg S \vee R) \wedge (Q \vee \neg P \vee \neg S \vee R) \wedge (\neg R \vee \neg P \vee \neg S \vee R)$
$(Q \vee \neg P \vee \neg S \vee R)$

3.7 Algorithme de preuve

Nous allons maintenant introduire un algorithme qui permet de trouver une preuve en logique propositionnelle. Cet algorithme est une automatisation de la *démonstration par l'absurde* qui est basé sur une seule règle d'inférence, la *résolution*.

3.7.1 La résolution

On veut quelque chose de simple, sans toutes les règles que nous avons vues auparavant, mais le plus puissant possible. Nous n'utiliserons qu'une seule règle : la **résolution**. On peut faire des résolutions de preuves propositionnelles rien qu'en ayant cette règle. Cette règle utilise la forme normale conjonctive. On utilise les preuves indirectes (preuves par l'absurde), car c'est le plus simple.
Commençons par un exemple de résolution.

Exemple de résolution

Prenons comme propositions premières :

P_1 : il neige
P_2 : la route est dangereuse
P_3 : on prend des risques
P_4 : on va vite
P_5 : on va lentement
P_6 : on prend le train

$$\left.\begin{array}{l} 1.\ P_1 \Rightarrow P_2 \\ 2.\ P_2 \Rightarrow \neg P_3 \\ 3.\ P_4 \Rightarrow P_3 \vee P_6 \\ 4.\ P_4 \vee P_5 \\ 5.\ P_1 \end{array}\right\} \text{B : notre théorie}$$

On va utiliser B + modus ponens + résolution..

1. $P_1 \Rightarrow P_2$	
2. $P_2 \Rightarrow \neg P_3$	
3. $P_4 \Rightarrow P_3 \vee P_6$	1-5 : B : notre théorie que l'on utilise comme prémisse
4. $P_4 \vee P_5$	
5. P_1	
3'. $\neg P_3 \Rightarrow \neg P_4 \vee P_6$	réécriture de 3
6. P_2	modus ponens (1,5)
7. $\neg P_3$	modus ponens (6,2)
8. $\neg P_4 \vee P_6$	modus ponens (7,3')
9. $P_5 \vee P_6$	résolution (4,8)

La ligne 3 n'étant pas symétrique, nous pouvons la transformer pour obtenir une proposition symétrique et donc choisir le membre qui est à gauche de l'implication. Pour rappel, $P_4 \Rightarrow P_3 \vee P_6$ peut être réécrit : $\neg P_4 \vee P_3 \vee P_6$ (loi de l'implication), qui est logiquement équivalent à $\neg P_3 \Rightarrow \neg P_4 \vee P_6$ (loi de l'implication). C'est de cette manière que nous avons obtenu la ligne 3'.

On peut fusionner les lignes 4 et 8 grâce à la résolution. La **résolution** est une règle qui prend deux disjonctions avec une proposition première et sa négation, et qui les fusionne en retirant cette proposition première. On peut prouver que cela fonctionne de plusieurs manières.
Par exemple : si P_4 est vrai, P_6 doit être vrai. Si P_4 est faux, P_5 doit être vrai. Donc on sait que P_5 ou P_6 doit être vrai car on sait que dans tous les cas de figure, c'est soit l'un soit l'autre qui doit être vrai.

Principe de résolution

$p_1 \vee q$
$p_2 \vee \neg q$

$p_1 \vee p_2$

Cette règle représente la base de l'algorithme de résolution. On peut la vérifier en utilisant le métalangage. De plus, cette règle est aussi utilisée dans la logique des prédicats.

La résolution préserve les modèles

Tout ce qui est modèle des deux premières disjonctions sera aussi modèle de la résultante.

$p : \bigwedge_{1 \leq i \leq n} C_i$ $\quad$ C_i : disjonction : $\bigvee_{1 \leq j \leq n} L_j$ $\quad$ $\{C_1, ..., C_n\}$

C_1, C_2 = deux disjonctions

On doit prouver : $\{C_1, ..., C_n\} \models r$ avec $r = C_1$ - $\{P\} \vee C_2$ - $\{\neg P\}$. r est une nouvelle disjonction à partir de deux autres disjonctions. On doit prouver que r est toujours vrai.

On considère que P est dans C_1 et que $\neg$P est dans C_2.

Pour prouver cela, on utilise la sémantique. On fait une preuve en métalangage, ce n'est pas formalisé.
$\text{Val}_I(P) = \begin{cases} T \\ F \end{cases}$

Dans les deux cas de figure, on doit démontrer que quand on a un modèle, une interprétation qui rend vrai p, le r sera vrai aussi. Si P est vrai alors $\neg$P est faux, donc C_2 sera vrai et donc r sera vrai. Quand P est faux, le C_1 doit être vrai, donc r est vrai. r est donc vrai dans les deux cas.

3.7.2 Algorithme

C_i : clause $\bigvee_i L_i$
L_i : P ou $\neg$P
$\{C_i,...,C_n\} \models C$
s.s.i
$\{C_i,...,C_n,\neg C\} \models$ false
C_i : axiomes
C : candidat théorème
Ce que nous voulons prouver : $\{C_i,...,C_n\} \vdash C$
Il existe une preuve avec les règles d'inférence $\{C_i,...,C_n\}$ tel qu'on obtient C.
$S = \{C_i,...,C_n,\neg C\}$
But : Déterminer si S est inconsistant. On veut faire des déductions jusqu'à arriver sur false.

Pseudocode

while $false \notin S$ *et* $\exists$ *? clauses résolvables non résolues* **do**
| — choisir $C_1, C_2 \in S$ tel que $\exists P \in C_1, \neg P \in C_2$
| — calculer r :=$C_1 - \{P\} \wedge C_2 - \{\neg P\}$
| — calculer S := $S \cup \{r\}$
end
if $false \in S$ **then**
| C est prouvé
else
| C n'est pas prouvé
end

La subtilité de cet algorithme est de choisir correctement les clauses C_1 et C_2 car l'efficacité de l'algorithme en dépend.

3.7.3 Exemples

Exemple 1

C_1 : P $\vee$ Q
C_2 : P $\vee$ R
C_3 : $\neg$Q $\vee$ $\neg$R
C : P $\{C_1, C_2, C_3, \neg C\}$

Quelques pas de résolution :

C_1 + $\neg$C $\rightarrow$ Q (C_5)
C_2 + $\neg$C $\rightarrow$ R (C_6)
C_3 + C_5 $\rightarrow$ $\neg$R (C_7)
C_6 + C_7 $\rightarrow$ <u>false</u> ($\in$ S donc C est prouvé)

Exemple 2

p_1 : Mal de tête $\wedge$ Fièvre $\Rightarrow$ Grippe
p_2 : Gorge blanche $\wedge$ Fièvre $\Rightarrow$ Angine
p_3 : Mal de tête
p_4 : Fièvre

<u>Algorithme</u>
— Normalisation en forme normale
— Pseudocode avec résolution
Question : Grippe ?

3.7.4 Conclusion

Nous pouvons tirer des conclusions sur la logique des propositions et sur notre algorithme.

Pour toute théorie $B = \{c_1, \ldots, c_n\}$ et p,
— si $B \vdash p$ alors $B \models p$ (Adéquat - *Soundness*) ;
— si $B \models p$ alors $B \vdash p$ (Complet - *Completeness*) ;
— $\forall\ B, p$, l'exécution de l'algorithme se termine après un nombre fini d'étapes. (Décidable - *Decidable*)

Cet algorithme est très puissant mais n'est pas toujours très efficace. Par contre, quoi qu'il arrive, on peut au moins être sûr qu'il s'arrêtera toujours à un moment.

La logique des propositions n'est malheureusement pas très expressive. Elle ne permet pas de relations entre les propositions. Nous allons essayer d'appliquer la même démarche mais avec une logique plus puissante : la logique des prédicats. Il n'est par contre pas possible d'arriver à un algorithme aussi puissant avec la logique des prédicats, la logique étant trop forte.

Chapitre 4

La logique des prédicats

4.1 Introduction

Nous allons maintenant étudier une logique beaucoup plus expressive que la logique propositionnelle, la logique des prédicats, qui est aussi appelée la logique de premier ordre. [1] Voici un premier tableau qui montre les différences entre la logique propositionnelle vue jusqu'à présent et la logique des prédicats que nous allons étudier.

Logique Propositionnelle	Logique des prédicats
Propositions premières P, Q, R ↪ Pas de Relations	Prédicats P(x,y) Quantifieurs : ∃x, ∀y ↪ Relation

On note P(x,y) dans la logique des prédicats avec x,y, les arguments du prédicat P qui sont des variables. Dans la logique propositionnelle, chaque proposition est isolée/indépendante alors que dans les prédicats on peut lier plusieurs prédicats ensemble.

Exemple	Logique propositionnelle	Logique des prédicats
Socrate est un philosophe	P	Phil(Socrate)
Platon est un philosophe	Q	Phil(Platon)

En logique propositionnelle il n'y a aucunes relations entre P et Q, alors qu'en logique des prédicats on peut lier Socrate et Platon avec le prédicat Philosophe qui prend en argument le nom du philosophe (Socrate ou Platon dans ce cas). Phil(Socrate) est donc vrai. On peut donc dire grâce aux

1. Il existe des logiques d'ordres supérieures, mais elles ne feront pas l'objet de ce cours.

prédicats que Socrate et Platon sont "la même chose", des philosophes.

Un autre exemple de prédicat :

$$\forall \alpha \ \text{Phil}(\alpha) \Rightarrow \text{Savant}(\alpha)$$

$\hookrightarrow$ *... cette formulation permet de résumer un très grand nombre de faits. L'ensemble des arguments α peut être infini*

Comme Socrate est un philosophe, on peut déduire que Socrate est un savant aussi !

Dire la même chose en logique propositionnelle serait beaucoup plus compliqué :

"Socrate est un savant" Proposition "R"
"Platon est un savant" Proposition "S"

On va donc noter en logique propositionnelle

$$(\text{P} \Rightarrow \text{R}) \cup (\text{Q} \Rightarrow \text{S}) \cup ...(\textit{potentiellement infini})$$

On doit tout énumérer car il n'y a aucune relation entre les différentes propositions. S'il y a un nombre infini, ça ne marche pas. Il y a donc de grandes limitations dans la logique propositionnelle.

Néanmoins parfois la logique propositionnelle peut être utile. Il existe des outils informatiques qui utilisent la logique propositionnelle. On peut prendre l'exemple de "SAT solver" à qui on donne des équations booléennes très compliquées et qui va trouver les valeurs des propositions primitives qui rendent vraie cette proposition. C'est donc assez utilisé ! La logique propositionnelle est utile, mais si l'on veut faire du raisonnement sur plus que "vrai" et "faux" avec des relations entre des propositions, la logique propositionnelle ne marche pas. Si on veut faire un logiciel qui montre une certaine intelligence, il faut utiliser la logique des prédicats.

Autre exemple :

Exemple	Logique propositionnelle	Logique des prédicats
Tout adulte peut voter	P	$\forall$x adulte(x) $\Rightarrow$ voter(x)
John est un adulte	Q	adulte(John)
———	—	———
John peut voter	?R ?	voter(John)

Ce genre de raisonnement est très difficile à faire en logique propositionnelle alors qu'en logique des prédicats c'est beaucoup plus simple ! Le John

en ligne 3 et en ligne 4 correspond à la même personne, ou de manière plus général à la même variable ! Ceci montre donc bien qu'il nous faut la logique des prédicats pour faire des relations de ce type.

4.2 Quantificateurs

Les expressions "pour tout x" ($\forall x$) et "il existe x tel que" ($\exists x$) sont appelés des quantificateurs en logique des prédicats. Les quantificateurs permettent d'instancier les variables dans une formule. La notion de portée d'un quantificateur est un concept très important auquel il faut faire très attention, car il peut changer complètement le sens d'une formulation.

$\forall x$ (enfants(x) $\wedge$ intelligents(x) $\Rightarrow$ $\exists y$ aime(x,y))

$\forall x$ (enfants(x) $\wedge$ intelligents(x)) $\Rightarrow$ $\exists y$ aime(x,y)

Ces deux formules peuvent paraître équivalentes, mais en réalité elles ont un sens tout à fait différent. En effet, dans le deuxième cas on remarque que le quantificateur $\forall x$ ne porte pas sur la dernière variable x qui est en argument du prédicat aime(x,y).

Il faut donc faire bien attention à quel quantificateur une variable s'identifie lorsqu'on manipule des formules.

- $\forall x$ P(x) $\wedge$ $\exists x$ Q(x) : contient deux variables différentes
- $\forall x$ $\exists x$ P(x) $\wedge$ Q(x) : est une forme incorrecte, conflit des noms de variables

Pour résoudre ces conflits, on fait appel à une nouvelle opération, le renommage. Cette opération permet de changer le nom des variables tout en conservant le sens de la formule. Ainsi on obtient :

$\forall x$ $\exists z$ P(x) $\wedge$ Q(z) *renommage (2)*

Le concept de variables, de leurs portées ainsi que d'opérateurs en logique des prédicats fait fortement penser au langage de programmation

Une comparaison entre un code et une formule est tout à fait envisageable. Prenons un code tout à fait banal comprenant des variables différentes avec des portées différentes qui ont le même identificateur ainsi qu'une

formule correspondante.

```
1.  begin {
2.      var x,y: int;
3.      x := 4;
4.      y := 2;
5.
6.      begin {
7.          var x: int;
8.          x := 5;
9.          x := x*y;
10.     end }
11.     x := x*y;
12. end }
```

$\forall x \ \forall y$ p(x) $\wedge$ ($\exists x$ q(x,y) $\vee$ r(x,y))

En analysant morceau par morceau de la formule :

- " $\forall x \ \forall y$ p(x) $\wedge$ " correspond aux points $\{2, 3, 4\}$ du code
- " $\exists x$ q(x,y) $\vee$ " correspond aux points $\{7, 8, 9\}$
- " r(x,y)) " correspond au point $\{11\}$

Cet exemple illustre parfaitement la ressemblance et le lien entre le monde de la programmation et celui de la logique des prédicats

4.3 Syntaxe

Symboles logiques	quantificateurs connecteurs logiques parenthèses variables true, false	$\forall \ \exists$ $\wedge \ \vee \ \neg \ \Rightarrow \ \Leftrightarrow$ ( ) x, y, z
Symboles non logiques	symboles de prédicats symboles de fonction	$P \ \varphi \ R$ + arguments ≥ 0 + $arguments \geq 0$

4.4 Grammaire

4.4.1 Règles de formation

$$
\begin{aligned}
< formule >::= \quad & < formule\ atomique > \\
& | \neg < formule > \\
& | < formule > < connecteur > < formule > \\
& | \forall < var > . < formule > \\
& | \exists < var > . < formule > \\
< formule\ atomique >::= \quad & \text{true, false} \\
& | < predicat > (< terme > *) \\
< terme >::= \quad & < constante > \\
& | < var > \\
& | < fonction > (< terme > *) \\
< connecteur\ binaire >::= \quad & \wedge | \vee | \Rightarrow | \Leftrightarrow
\end{aligned}
$$

4.5 Exemple de sémantique

Dans la logique des prédicats, nous gardons les notions de modèle et d'interprétation déjà définis dans la logique propositionnelle. Même si la logique des prédicats est beaucoup plus puissante, sa sémantique reste similaire à la logique propositionnelle. Comme pour la logique propositionnelle, une interprétation peut avoir une valeur (true, false).

Illustrons par un exemple :

$$p : P(b, f(b)) \Rightarrow \exists y P(a, y)$$

On suppose que le a et le b sont des constantes et que le f est une fonction. Il faut donner un sens à cette formule et pour cela il faut donner un sens à :

- P : $val_I(P) = \geq$ (*considéré comme un vrai prédicat*)
- a : $val_I(a) = 2$
- b : $val_I(b) = \pi$
- f : $val_I(f) = f_i \quad f_i = \Re \to \Re : d \to \dfrac{d}{2}$

Avec ces éléments, on peut donc trouver l'interprétation :

$$Si\ \pi \geq \frac{\pi}{2},\ alors\ \exists\ d \in \Re\ tel\ que\ \sqrt{2} \geq d$$

Cette phrase n'est pas très utile, mais avec cette interprétation, la phrase logique donne ce sens. Une autre interprétation donnerait un sens totalement différent à la phrase logique. Voici une autre interprétation totalement différente :

- a : $val_I(a)$ = "Barack Obama"
- b : $val_I(b)$ = "Vladimir Putin"
- f : $val_I(f) = f_i$ $\quad f_i \rightarrow$ père(d)
- P : $val_I(P) = P_I$ $\quad d_1$ est enfant de d_2

Avec ce nouveau sens, on trouve l'interprétation suivante :

Si Vladimir Putin est l'enfant du père de Vladimir Putin alors $\exists$ *une personne telle que Barack Obama est l'enfant de cette personne.*

La seconde interprétation est très différente de la première malgré le fait que ce soit la même formule à l'origine ! La connexion entre une formule et son sens permet de garder une certaine souplesse dans le sens où l'on peut choisir ça. C'est un peu comme dans la logique propositionnelle, mais avec encore plus de souplesse.

On peut se demander si ces deux interprétations sont des modèles de la formule ?
La première interprétation est un modèle de la formule, car le sens de la formule est vrai dans l'interprétation. En effet, $\pi \geq \frac{\pi}{2}$ et $\exists\ d \in \Re$ tel que $\sqrt{2} \geq d$. On voit donc que le modèle est vrai.

La deuxième interprétation est aussi un modèle de la formule, car l'interprétation trouvée est vraie aussi. Cela peut paraître bizarre, mais c'est correct.

4.6 Détails techniques

La première question que l'on se pose est : comment faire des preuves en logique des prédicats ? Il faut noter que les quantificateurs $\forall$ et $\exists$ rendent le raisonnement plus subtil. Il faudra des règles pour pouvoir raisonner sur ces quantificateurs.

4.6.1 Sémantique

La sémantique en logique des prédicats est très proche de celle en logique propositionnelle. Cependant, l'interprétation, I, est plus précise qu'en logique propositionnelle et est également plus compliquée à utiliser à cause des variables et des symboles de fonction. Cette interprétation peut être décrite comme une paire : $I = pair(D_I, val_I)$ avec D le domaine de discours I et la fonction val qui est l'interprétation de tous les symboles. $D_I \neq \emptyset$ $\forall s \in S$ avec s soit un symbole de prédicat soit une fonction. $val_I(S) = P_I$ une fonction $P_I : D_I^n \rightarrow (True, False)$ avec S symbole d'une fonction. Il

existe aussi une vraie fonction $f_I : D_I^n \rightarrow D_I$ avec n le nombre d'arguments tel que $val_I(S) = f_I$. Cela implique que dans le domaine de discours chaque fonction correspond à une vraie fonction et chaque prédicat correspond à un vrai prédicat.

Si l'on rajoute une variable, x par exemple, l'expression devient : $(var, x) \rightarrow val_I(x) = x_I \in D_I$. L'interprétation d'une variable, x_I est un élément (n'importe lequel en fonction de l'interprétation) de D_I. La fonction VAL_I est la même fonction, mais pour les formules et pas uniquement pour les symboles comme avant. Néanmoins, on ne doit pas redéfinir , VAL_I car elle existe à partir du moment ou val_I et D_I existent. Définition : $VAL_I : TERM \cup PRED \rightarrow D_I \cup (True, False)$ avec TERM l'ensemble des termes et PRED l'ensemble des prédicats (toutes les formules en logique des prédicats). Les termes peuvent être définis comme $t \rightarrow VAL_I(t)$ et les prédicats comme $P \rightarrow VAL_I(P)$ avec P une formule. Il y a une forte relation entre val_I et VAL_I : $val_I((P(T_1, ..., T_n)) = P_I(VAL_I(t_1), ..., VAL_I(t_n))$ avec $P_I = VAL_I(P)$ La première partie de l'égalité est un prédicat avec des arguments tandis que la seconde est formée de plusieurs prédicats avec un argument.

Définissons d'autres formules : $VAL_I(P \wedge Q)$ est true si $VAL_I(P) = True$ et $VAL_I(Q) = True$. false sinon. Donc il faut $VAL_I(\forall x.P) = True$ avec P une formule pouvant dépendre de x (il faut remplacer toutes les occurrences de x dans P et la formule doit rester vraie. Si pour chaque d $\in D_I$ $I' = I \cup (x \leftarrow d)$ et $val_I(x) = d$ alors l'interprétation de x doit être : $VAL'_I(P) = True$. Pour $VAL_I(\exists x.P) = True$ le raisonnement est identique en remplaçant $\forall$ par $\exists$.

4.7 Différence avec la logique des propositions

Les trois différences entre les deux logiques sont :

1. les variables,
2. les quantificateurs,
3. les symboles de fonction (moins important).

Imaginons un modèle $B : \{ P_1, ...P_n \}$ Si nous utilisons une interprétation I pour B cela donne : $\forall P_I \in B : VAL_I(P_I) = True$ qui est très générale, car P_I peut avoir des variables, des quantificateurs ...

4.8 Preuves avec règles

Il est possible de faire des preuves avec des règles de preuve. Une preuve est une simple manipulation de symboles qui sont des règles. Mais il faut

justifier ces règles pour obtenir des résultats vrais. Elles sont justifiées en raisonnant sur les interprétations pour vérifier si elles sont correctes ou non. Tout cela est la sémantique. C'est la base pour pouvoir faire des preuves.

Beaucoup de choses restent les mêmes que dans la logique des propositions. La preuve est toujours un objet mathématique, une séquence avec des formules, des justifications, une application des règles. Elle commence avec des prémisses et finit par une conclusion. Il est possible de faire des preuves manuelles, mais aussi des preuves automatisées. C'est une généralisation de l'approche de la logique des propositions.

Il y a toujours :

— Une règle de résolution pour les preuves automatisées, mais celle-ci est plus générale. Elle va utiliser un concept appelé "unification". Ce nouveau concept est introduit à cause des variables. En effet, celles-ci peuvent être différentes, il faut donc trouver un nouveau moyen de les fusionner.

— Une forme normale, qui est plus compliquée à cause des quantificateurs et des symboles de fonctions, mais qu'il est encore possible de l'obtenir.

— un algorithme avec ses propriétés. Mais il est moins fort/complet que l'algorithme développé pour la logique des propositions. Il ne sera plus décidable, mais seulement semi-décidable. C'est-à-dire que parfois il tournera en boucle. Cela est dû aux variables et aux quantificateurs. La logique des prédicats est beaucoup plus riche que la logique des propositions, mais en contrepartie l'algorithme arrive à prouver moins de choses. Cependant, l'algorithme sera toujours adéquat, mais pas forcément complet. Il ne sera pas toujours possible de trouver une preuve, même quand elle existe parce qu'elle sera trop compliquée.

Qu'est il possible de faire avec ce genre d'algorithme moins fort ?

Il y a deux possibilités :

— Un assistant de preuve

C'est un outil qui aide les gens à faire des preuves formelles. Deux exemples d'assistants de preuves sont Coq et Isabelle. C'est un outil très sophistiqué, mais qui a permis de prouver des choses de manière totalement formelle, alors qu'avant des preuves prenaient des dizaines voire des centaines de pages de preuves mathématiques. Mais cet assistant ne fait pas tout parce que l'algorithme est moins bon. Cependant, il aide beaucoup. C'est à l'être humain de lui donner des coups de pouce sous forme de lemmes, hypothèses, chemins, stratégies ... Ensuite, l'algorithme s'occupe de la manipulation des symboles.

Un exemple très célèbre est le théorème de la coloration d'une carte. La question est : est-il toujours possible de colorier chaque pays avec une couleur, de façon à ce que deux pays limitrophes n'aient pas la

même couleur et en utilisant un certain nombre de couleurs différentes ? Ce n'est pas évident à prouver et ça a demandé beaucoup de travail aux mathématiciens. Mais récemment, Georges Gonthier (un informaticien) a réussi à formuler ce problème avec l'assistant de preuves. Ce fut un tour de force. Désormais, il existe une preuve complètement formalisée, sans erreur pour ce théorème.

— L'utiliser dans les langages de programmation
L'algorithme peut être considéré comme le moteur d'un programme. C'est ce qu'on appelle maintenant la programmation logique. Elle consiste à utiliser la logique dans un programme. Le langage le plus célèbre qui a suivi cette approche est Prolog. Ce fut un énorme succès, car les gens ne croyaient pas que c'était possible de faire un programme en logique qui pouvait tourner. Cela a donné naissance à la programmation par contraintes (une contrainte est une relation logique). Cette discipline est très utile pour les optimisations, par exemple dans le cas du "voyageur de commerce".

La logique des prédicats n'est donc pas quelque chose de seulement théorique, destiné uniquement aux mathématiciens. Les gens ont vraiment essayé avec succès d'utiliser la logique dans l'exécution des programmes.

Chapitre 5

Preuves en logique des prédicats

On va généraliser l'approche de la logique propositionnelle, car comme vu précédemment le langage des prédicats est beaucoup plus riche. Il ajoute entre autres :

— Des variables
— Des constantes
— Des fonctions (détaillé plus tard)
— Des prédicats
— Des quantificateurs

Les preuves en logique des prédicats ressemblent très fort aux preuves en logique propositionnelle. Il y a encore des prémisses, des formules avec leurs justificatifs et une conclusion. On peut aussi utiliser des preuves indirectes et des preuves conditionnelles. Cela reste un objet formel.

1.	...	*Prémisses*
2.	Formule, regle	$Justification$
...	...	...
n.	Conclusion	$Justification$

5.1 Exemple

La méthode pour passer de $\forall x \cdot P(x) \wedge Q(x)$ (prémisse) à $\forall x \cdot P(x) \wedge (\forall x \cdot Q(x))$ (conclusion) est la suivante :

1. Enlever les quantificateurs pour avoir des variables libres
2. Raisonner sur l'intérieur
3. Remettre les quantificateurs

Les étapes difficiles à réaliser correctement sont les étapes 1 et 3. Voici la preuve en "français" :

En retirant les quantificateurs des prémisses, cela donne : "Comme $P(x) \wedge Q(x)$ est vrai pour tout x, alors $P(x)$ est vrai pour tout x". De là, on peut remettre les quantificateurs pour obtenir $\forall x \cdot P(x)$. De façon similaire, on obtient $\forall x \cdot Q(x)$. Et on conclut en remettant les quantificateurs : $\forall x \cdot P(x) \wedge \forall x \cdot Q(x)$, en utilisant la conjonction.

En preuve formelle, cela donne :

1.	$\forall x \cdot P(x) \wedge Q(x)$	Prémisses
2.	$P(x) \wedge Q(x)$	Élimination de $\forall$
3.	$P(x)$	Simplification
4.	$\forall x \cdot P(x)$	Introduction de $\forall$
5.	$Q(x)$	Simplification $\forall$
6.	$\forall x \cdot Q(x)$	Introduction de $\forall$
7.	$\forall x \cdot P(x) \wedge \forall x \cdot Q(x)$	Conjonction

On a donc utilisé 4 règles en plus par rapport aux preuves formelles en logique propositionnelle (les règles de la logique propositionnelle restent valables en logique des prédicats) :

— Élimination de $\forall$
— Introduction de $\forall$
— Élimination de $\exists$
— Introduction de $\exists$

Certaines de ces règles sont simples d'utilisation, d'autres sont plus difficiles. Il est également possible d'utiliser d'autres règles (certaines plus générales que d'autres [1]).

Note :

Il est possible d'utiliser les quantificateurs dans les formules mathématiques. Typiquement, on ne les note pas, car ils sont présents de manière implicite. Par exemple :

— $\forall x \cdot \sin(2x) = 2 \cdot \sin(x) \cdot \cos(x)$
— $\forall x \cdot x + x = 2x$
— $\exists x \cdot \sin(x) + \cos(x) = 0,5$
— $\exists x \cdot x + 5 = 9$

On peut remarquer que pour les deux premiers cas, x est une véritable variable, on peut donc ajouter un quantificateur universel $\forall$.

1. Voir "Inference logic" ou "Predicate logic"

Pour les deux cas suivants, on remarque que x est une inconnue, car il y a une équation à résoudre et une solution à trouver, on peut donc ajouter un quantificateur existentiel $\exists$.

Dans certains cas, les quantificateurs existentiels et universels sont utilisés au sein de la même formule mathématique.

$\forall a \cdot \forall b \cdot \forall c \cdot \exists x \cdot ax^2 + bx + c = 0$

Dans l'exemple ci-dessus, nous avons 4 variables : a, b, c, x. Les 3 premières sont des véritables variables, on peut les affecter à n'importe quelle valeur, tandis que la dernière est une inconnue, c'est la solution à trouver. Il faut donc trouver x pour toutes les valeurs possibles de a, b, c.

5.2 Règles en logique des prédicats

En logique des prédicats, pour trouver une preuve, on va faire des manipulations de formules.

5.2.1 La substitution

Une manipulation fréquente en logique des prédicats est la **substitution**. Elle consiste à prendre une formule et remplacer une partie par une autre.

Si on a une formule $p[x/t]$ (où p veut dire "toutes les formules"). On va remplacer toutes les occurrences libres de x par t.
On peut aussi écrire cela de la manière suivante :
$p[x/t]$ possède deux portées :

La première se note $p[x]$ et correspond à une partie de la règle.
La seconde se note $p[t]$ et correspond à l'autre partie de la règle.

Exemple :

1.	$P(x) \to \forall y \cdot (P(x) \land R(y))$	$[x/y]$ veut dire qu'on va remplacer toutes les occurrences libres de x par y.
2.	$P(y) \to \forall y \cdot (P(y) \land R(y))$	En remplaçant x par y, on a changé le sens de la formule, car avant, x n'était pas dans la portée du quantificateur alors que maintenant il l'est. Ce changement de sens s'appelle une **capture de variable**, car la variable y est capturée par le quantificateur. Pour résoudre ce problème, on va effectuer un **renommage**.
3.	$P(y) \to \forall z \cdot (P(y) \land R(z))$	Résultat après renommage (pour éviter la capture de variable).

5.3 Élimination de ∀

∀x•P(x) → P(a) a est une constante
→ P(y) y est une variable ($P_I(y_I)$ est vrai $y_I \in P_I$)
∀ = pour tout $x_I \in P_I$: $P_I(x_I)$ est vrai

Règle :

$$\frac{\forall x{:}p}{p[x/t]}$$

Substitution : t remplace x

⚠Il est parfois nécessaire d'effectuer un renommmge

Exemple :

1. ∀x • ∀y • P(x,y) Prémisse
2. ∀y • P(x,y) Élimination de ∀
3. P(x,x) Élimination de ∀ → Pas de renommage, car pas de capture
4. ∀x • P(x,x) Introduction de ∀

5.4 Élimination de ∃

∃x • P(x) → P(a) a = nouvelle constante qui apparaît nulle part ailleurs ($val_I(a) = x_I$)
Il existe un $x_I \in D_I$ avec $P_I(x_I)$ est vrai
↛ P(y) y = variable qui existe déjà dans la preuve
→ P(z) z = nouvelle variable dans la preuve $val_I(z) = x_I$

Exemple 1 :

1. ∃x • chef(x) Prémisse
2. ∃x • voleur(x) Prémisse
3. chef(y) Élimination de ∃
4. ~~voleur(y)~~ Élimination de ∃ y n'est pas une nouvelle variable dans la preuve
5. chef(y) ∧ voleur(y) Conjonction
6. ~~∃y • chef(y) ∧ voleur(y)~~ Introduction de ∃ FAUX

Exemple 2 :

1. $\exists$x • chef(x) Prémisse
2. $\exists$x • voleur (x) Prémisse
3. chef(y) Élimination de $\exists$
4. voleur (z) Élimination de $\exists$
5. chef(y) $\wedge$ voleur(z) Conjonction
6. $\exists$y $\exists$z chef(y) $\wedge$ voleur(z) Introduction de $\exists$

5.5 Introduction de $\exists$

Règle :

$$\frac{p[t]}{\exists x \bullet p[x]}$$

Il y a une substitution p[x/t]

Exemple :

P(y,y)
$\exists$x • P(x,x)

~~P(y,x)~~
~~$\exists$x • P(x,x)~~

Ceci n'est pas correct !

$\Rightarrow$ Il doit être possible de retrouver la formule originale en remplaçant.

5.6 Introduction de $\forall$

Règle :

$$\frac{p}{\forall x \bullet p}$$

— Si p n'a pas d'occurrence libre de x alors c'est OK
— Si p contient une occurrence libre de x : on doit s'assurer que la preuve jusqu'à cet endroit marchera pour toutes valeurs affectées à x
↪ Aucune formule dans la preuve jusqu'à cet endroit ne doit mettre une contrainte sur x !

Deux conditions :

- x n'est pas libre dans une formule dans la preuve jusqu'à cet endroit obtenu par élimination de $\exists$
- x n'est pas libre dans une prémisse (x est déjà connu au début donc il possède déjà une valeur)

Exemple :

1. $\forall x\ \exists y$ parent(y,x) Prémisse
2. $\exists y$ parent(y,x) Élimination de $\forall$
3. parent(y,x) Élimination de $\exists$ $\rightarrow$ N'est valable que pour ce y et ce x, pas pour tous
4. ~~$\forall x$ parent(y,x)~~ Introduction de $\forall$ $\rightarrow$ On ne peut pas faire ça, car il y a une contrainte sur x. Là on dit que ce y est parent de tous !

Terminons par un exemple un peu plus conséquent d'une preuve manuelle en logique des prédicats avant d'introduire l'algorithme permettant d'effectuer des preuves de manière automatisée.

5.6.1 Exemple de preuve manuelle

Il est important de pouvoir faire des preuves manuellement, car cela permet de bien comprendre toutes les étapes de raisonnement d'une preuve, même si par la suite on utilise un algorithme plutôt que de faire les preuves à la main.

L'exemple suivant est inspiré de l'Empire romain :

Prémisses

— Les maîtres et esclaves sont tous des hommes adultes
— toutes les personnes ne sont pas des hommes adultes

Note : on voit dans les prémisses qu'il y a des quantificateurs : tous, toutes.

A prouver

— il existe des personnes qui ne sont pas des maîtres

Preuve

1. $\forall x\ (maitre(x) \vee esclave(x) \implies adulte(x) \wedge homme(x))$ prémisse
2. $\neg\forall x\ (adulte(x) \wedge homme(x))$ prémisse
3. $\exists x\ \neg(adulte(x) \wedge homme(x))$ théorème négation
   S' il n'est pas vrai que toutes les personnes sont des hommes adultes alors il existe une personne qui n'est pas un homme adulte
4. $\neg(adulte(x) \wedge homme(x))$ $\exists$ elim
   On élimine le quantificateur existentiel : on peut le faire, car on introduit une variable x qu'on choisit comme étant une personne rendant vraie la proposition.
5. $(maitre(x) \vee esclave(x) \implies adulte(x) \wedge homme(x))$ $\forall$ elim
   On peut retirer le $\forall$ en réduisant le champ de x aux x rendant vraie la proposition.
6. $\neg(maitre(x) \vee esclave(x))$ modus tollens
7. $\neg maitre(x) \wedge \neg esclave(x)$ De Morgan
8. $\neg maitre(x)$ simplification

9. $\exists y\ \neg maitre(y)$ $\exists$ intro
   Comme dans l'interprétation, x est une personne qui rend valable cette proposition, on peut dire qu'il existe une personne rendant valable cette proposition et réintroduire le quantificateur $\exists$

C'était un exemple très simple ne faisant que quelques pas, mais la logique est assez expressive pour permettre des preuves plus complexes(par exemple, formaliser les mathématiques), le nombre de pas serait alors beaucoup plus important.

Instant Histoire :

A la fin du 19ème siècle, début du 20ème :

- création de la logique de 1er ordre (Gottlob Frege)
- Deux personnes ont essayé de formaliser toutes les mathématiques. Principa Mathématica (Alfred Whitehead, Bertrand Russell)

Lors que l'arrivée des ordinateurs, fin du 20ème siècle(années 50-60 et fin du siècle) on a essayé de formaliser la logique via des algorithmes :

- Création de l'Algorithme de Preuves (1965) :
  - Alan Robinson crée La Règle de Résolution (qui va être expliquée au chapitre suivant)
  - Création de prouveurs (assistants de preuve) par exemple Coq et Isabelle en 1972
  - Création de la logique de programmation qui aide à l'élaboration de la programmation par contraintes : Prolog (1972)
- Création de la sémantique Web : OWL (Web Ontology Langage)

Chapitre 6

Algorithme de preuve pour la logique des prédicats

— Cet algorithme s'inspire de l'algorithme de réfutation de la logique des propositions [résolution forme clausale]
— Pour la logique des prédicats, c'est un peu plus complique, mais ça marche !

On peut le faire marcher malgré la complexité des variables et des quantificateurs ce qui est assez étonnant, car c'est une logique très expressive. Arriver à trouver un algorithme permettant de traiter la logique des prédicats était une sorte de Graal au 20ème siècle.

6.1 3 transformations

On va commencer par faire les transformations de normalisation. Il y a 3 transformations à effectuer :

1. formule → forme prénexe :

$$(\dots\forall\dots\exists\dots\forall) \implies \forall\exists\forall(\dots)$$

   Tous les quantificateurs sont mis en tête de la formule. Les quantificateurs étant très compliqués à gérer, on transforme la formule pour les extraire de celle-ci.
   Les modèles sont conservés durant cette transformation.

2. forme prénexe → forme Skolem (élimination des $\exists$) :

$$\forall\exists\forall(\dots) \implies \forall\forall\forall(\dots)$$

   Les quantificateurs existentiels sont très embêtants, car ils sont restrictifs. Ils disent qu'il existe des éléments, mais ne précisent pas

lesquels, on va donc les éliminer.
Cette transformation préserve l'existence des modèles, mais pas les modèles eux-mêmes. Ils doivent être modifiés pour conserver la même signification.

3. forme Skolem → forme normale conjonctive :

$$\forall \ldots \forall \wedge_i (\vee_j L_{ij})$$

Cette transformation est la même que celle effectuée dans la logique des propositions.
Les modèles sont préservés lors de cette transformation.

6.2 Résolution

En logique des propositions :

$$\frac{L \vee C_1, \neg L \vee C_2}{C_1 \vee C_2}$$

Cette technique fonctionne en logique des propositions, car il n'y a pas de variables, mais ici, on peut avoir $L_1 \vee C_1 \quad \neg L_2 \vee C_2$ avec L_1 et L_2 qui ont des variables différentes. Par exemple P(x,a) et P(y,z).
Pour pouvoir faire la résolution, il va falloir en quelque sorte les rendre identiques.
On va donc dire : ce ne sont peut-être pas toujours les mêmes, mais, pour certaines valeurs, ils sont identiques. Si x=y et a=z alors on peut faire la résolution.

6.2.1 Unification

L1 : P(x,a)
L2 : P(y,z)

Pour que L_1 et L_2 soient identiques, on va restreindre les variables et faire une substitution.

$$(a : constante,\ x, yz : variables)$$

$$\sigma = \{(x, y), (z, a)\}$$

$$P(x, a) \rightarrow P(y, a)$$

$$P(y, z) \rightarrow P(y, a)$$

Cette résolution marche pour toutes les valeurs qui sont limitées par la substitution. Le résultat ne sera donc pas général. Cette opération s'appelle l'unification et utilise la substitution σ (sigma). On peut maintenant faire la résolution en appliquant le même algorithme de réfutation que pour la logique des prédicats :

$$\frac{L_1 C_1, \neg L_2 \vee C_2}{(C_1 \vee C_2)\sigma}$$

6.3 Propriétés de cet algorithme

— Cet algorithme est moins fort que pour la logique des propositions, car la logique des prédicats est beaucoup plus expressive.
— adéquat : Si $B \vdash T \rightarrow B \models T$
si l'on trouve une preuve de T avec les axiomes B alors T sera vrai dans tous les modèles de B
— complet : Si $B \models T \rightarrow B \vdash T$
Si quelque chose est vrai dans tous les modèles alors on va trouver une preuve
— L'algorithme possède les propriétés d'un algorithme semi-décidable :
  — Si $B \vdash T \rightarrow$ l'algorithme trouve une preuve.
  — Si $B \nvdash T \rightarrow$ il peut tourner en rond indéfiniment.
  Si ce qu'on tente de prouver est vrai dans tous les modèles, l'algorithme va finir par trouver une preuve, mais si ce n'est pas vrai, l'algorithme va tourner en rond et ne jamais se terminer. Le problème est donc que quand l'algorithme prend trop de temps à trouver une preuve, on doit l'arrêter et l'on n'est jamais certain du résultat. On ne peut jamais être sûr que l'algorithme n'aurait pas trouvé une preuve si on l'avait laissé tourner plus longtemps. Il est donc semi-décidable, car ses résultats ne sont totalement fiables que dans le cas ou une preuve est trouvée.

6.4 Transformation de la formule de base vers la forme prénexe

Etapes de la transformation en formule logiquement équivalente :

1. Éliminer $\Leftrightarrow$ et $\Longrightarrow$
2. Renommer les variables.
   — Chaque quantificateur ne porte que sur une variable, il faudra en créer de nouvelles si besoin en prenant soin de conserver l'équivalence de la formule .
   — Attention : ne jamais garder le même nom de variable pour une variable libre et une variable liée.
   — Supprimer les quantificateurs si possible.

3. Migrer les négations ($\neg$) vers l'intérieur, vers les prédicats. On peut faire cela, car $\neg\exists$ peut être transformé en $\forall\neg$ et vice versa.

4. On peut mettre tous les quantificateurs de la logique des prédicats à l'avant de la formule.

6.4.1 Exemple d'une transformation en forme prénexe

1. $\forall x[p(x) \wedge \neg(\exists y)\forall x(\neg q(x,y)) => \forall z \exists v \bullet p(a,x,y,v))]$
   Expression de base
2. $\forall x[p(x) \wedge \neg(\exists y)(\forall x)(\neg \neg q(x,y) \vee \forall z \exists v \bullet r(a,x,y,v)]$
   Suppression des $\Longrightarrow$
3. $\forall x[p(x) \wedge \neg(\exists y)(\forall u)(\neg\neg q(u,y) \vee \not\forall z \exists v \bullet r(a,u,y,v)]$
   Renommage des variables et suppression des quantificateurs inutiles
4. $\forall x[p(x) \wedge \forall y \neg (\forall u)(\not\neg q(u,y) \vee \exists v \bullet r(a,u,y,v)]$
   $\neg\exists y$ *devient* $\forall\ y\ \neg$ *et simplification des* $\neg$
5. $\forall x[p(x) \wedge \forall y\ \exists u \neg (q(u,y) \vee \exists v \bullet r(a,u,y,v)]$
   $\neg\forall u$ *devient* $\exists\ u\ \neg$
6. $\forall x[p(x) \wedge \forall y \exists u\ (\neg q(u,y) \wedge \neg(\exists v) \bullet r(a,u,y,v))]$
   Distribution des $\neg$*(De Morgan)*
7. $\forall x[p(x) \wedge \forall y \exists u(\neg q(u,y) \wedge (\forall v) \bullet \neg r(a,u,y,v))]$
   $\neg\exists y$ *devient* $\forall\ y\ \neg$
8. $\forall x\ \forall y \exists u \forall v \bullet [p(x) \wedge (\neg q(u,y) \wedge \neg r(a,u,y,v))]$
   Extraction des quantificateurs.

6.5 Transformation en forme Skolem

6.5.1 Intuition

Cette transformation consiste à éliminer toutes les occurences de quantificateurs existentiels.

$(\forall x)(\forall y)(\exists u)(\forall v)\big[P(x) \wedge \neg Q(u,y) \wedge \neg R(a,u,y,v)\big]$

Dans ce cas-ci, la valeur de u dépend des valeurs de x et y. Lorsqu'on a choisi x et y, on est alors libre de choisir u. On peut donc supposer qu'une fonction $g(x,y)$ fournit cet élément de façon à conserver la satisfaisabilité de la formule tout en supprimant $(\exists u)$.

$(\forall x)(\forall y)(\forall v)\big[P(x) \wedge \neg Q(\mathbf{g(x,y)},y) \wedge \neg R(a,\mathbf{g(x,y)},y,v)\big]$

Après la transformation, l'existence des modèles est préservée.

6.5.2 Règle

Pour chaque élimination d'un quantificateur existentiel $(\exists x)$, on remplace sa variable quantifiée par une fonction $f(x_1,...,x_n)$ dont les arguments sont les variables des quantificateurs universels dont x est dans la portée.

Justification par un exemple :

$p : \forall x \forall y \exists z\big[\neg P(x,y) \vee Q(x,z)\big]$

$p_s : \forall x \forall y\big[\neg P(x,y) \vee Q(x,\mathbf{f(x,y)})\big]$

Les modèles de p $\neq$ modèles p_s.

Pour p
— Interprétation I
— D_I = Professeur $\cup$ Université
— $Val_I(P) = P_i$ = "a enseigné à l'université"
— $Val_I(Q) = Q_i$ = "est diplômé de l'université"
— $Val_I(f)$ n'existe pas.

Pour p_s
— Étendre I
— $I' = \{F \vdash F_i\} \circ I$
— $f(a,b)$ = "l'université ayant dû diplômer a pour que a puisse enseigner à b"

p admet un modèle (I) si et seulement si p_s admet un modèle (I').

Que ça ne soit exactement le même modèle ne pose pas de problème

pour notre algorithme. L'algorithme par réfutation continue à itérer jusqu'à trouver une contradiction ($false$). S'il n'y a pas de modèle pour p_s, il n'y a pas de modèle pour p et ça suffit.

6.6 Transformation en forme normale conjonctive

Mêmes manipulations qu'en logique des propositions.

6.7 La règle de résolution

$$\frac{L_1 \vee C_1, \neg L_2 \vee C_2}{(C_1 \vee C_2)\sigma}$$

Cette règle de résolution ne fonctionne que si L_1 et L_2 sont identiques.

— $L_1 = P_1(a, y, z)$
— $L_2 = P_1(x, b, z)$

Dans un modèle il y a un prédicat qui correspond au symbole P_1 et il y a un ensemble de triplets qui rendent vrai P_1.

L'unification de L_1 et L_2 donne L qui représente l'intersection des deux ensembles. On écrit :

— $L_1\sigma = L$
— $L_2\sigma = L$

L_1 et L_2 sont unifiables s'il existe une substitution σ telle que $L_1\sigma = L_2\sigma$.

— $\sigma = \{(x, a), (y, b)\}$
— $L_1\sigma = P(a, b, z)$
— $L_2\sigma = P(a, b, z)$

Exemple :

— $L_1 = P_1(a, x)$
— $L_2 = P_2(b, x)$

Il n'y pas de substitution qui existe, car on a deux constantes différentes, l'intersection des deux ensembles est vide.

Exemple 2 :

— $L_1 = P(f(x), z)$
— $L_2 = P(y, a)$

Dans ce cas-ci, il y a beaucoup de substitutions possibles telles que :

— $\sigma_1 : \{(y, f(a)), (x, a), (z, a)\} => L_1\sigma_1 = L_2\sigma_1 = p(f(x), a)$
— $\sigma_2 : \{(y, f(x)), (z, a)\} => L_1\sigma_2 = L_2\sigma_2 = p(f(x), a)$

Dans ce cas-ci, σ_2 est plus général.

— On préfère alors la substitution σ la plus générale.
— On peut démontrer qu'il existe un unificateur plus général U.P.G.
— U.P.G. est calculable.

Règle de résolution :
— p_1, p_2 clauses
— $p_1 = L^+ \vee C_1$
— $p_2 = \neg L^- \vee C_2$
— L^+ et L^- ont les mêmes symboles de prédicat.
— $\{L^+, L^-\}$ unifiable par σ U.P.G.
Alors

$$\frac{L^+ \vee C_1, \neg L^- \vee C_2}{(C_1 \vee C_2)\sigma}$$

6.8 Algorithme

Input: $S := \{\Delta x_1, ..., \Delta x_i, \neg Th\}$ dont chaque formule est en forme normale conjonctive (FNC).
while *$false \notin S$ et il existe une paire de clauses résolvables et non résolues.* **do**
| Choisir p_i, p_j dans S et L tel que :
| — L^+ dans p_i
| — L^- dans p_j
| — $\{L^+, L^-\}$ unifiable par σ U.P.G.
| Calculer :
| — $r := (p_i - [L^+] \vee p_j - [\neg L^-])\sigma$
| — $S_i = S \cup \{r\}$
end
if $false \in S$ **then**
| Th prouvé.
else
| Th non prouvé.
end

6.9 Exemple

— $(\forall x) homme(x) \wedge fume(x) \Rightarrow mortel(x)$
— $(\forall x) animal(x) \Rightarrow mortel(x)$

— $homme(Ginzburg)$
— $fume(Ginzburg)$
— **Candidat-théorème :** $mortel(Ginzburg)$

6.9.1 Initialisation de S

— P1 : $(\forall x) homme(x) \wedge fume(x) \Rightarrow mortel(x)$
— P2 : $(\forall x) animal(x) \Rightarrow mortel(x)$
— P3 : $homme(Ginzburg)$
— P4 : $fume(Ginzburg)$
— P5 : $\neg mortel(Ginzburg)$

6.9.2 Itérations

A
— P1 + P5
— $\sigma = \{(x, Ginzburg)\}$
— $r = P6 = \neg homme(Ginzburg) \vee \neg fume(Ginzburg)$
B
— P3 + P6
— $\sigma = \{\}$
— $r = P7 = \neg fume(Ginzburg)$
C
— P4 + P7
— $\sigma = \{\}$
— $r = false$. Inconsistence donc le candidat théorème est prouvé.

6.9.3 Non-déterminisme

Importance des choix qu'on fait.

A
— P2 + P5
— $\sigma = \{(x, Ginzburg)\}$
— $r = \neg animal(Ginzburg)$
Si on avait fait ce choix-ci pour la première itération, l'algorithme ne peut plus continuer et on doit faire marche arrière.

6.10 Stratégies

— Quelles paires p_i, p_j choisir ?
— Quelles L^+, L^- choisir ?

Les assistants de preuves utilisent des stratégies existantes, avec l'input de l'humain.

Le langage **Prolog**, inventé en 1972 par Alain Colmerauer et Robert Kowalski, utilise volontairement des stratégies naïves qui permettent de rendre l'algorithme prévisible. Les axiomes deviennent un programme, c'est la programmation logique. Un exemple de stratégie naïve est la stratégie LUSH qui choisi de haut vers le bas les paires p_i, p_j, et de gauche à droite dans p_i.

Chapitre 7

Théorie logique

7.1 Étude des structures discrètes

Exemples de structures discrètes : entiers positifs, chaînes, arbres, ensembles, relations, fonctions ...

On peut définir ces structures avec la logique des prédicats et faire des raisonnements sur celles-ci en utilisant des règles d'inférence.

Utilisation :

- On peut programmer avec ces structures. *Prolog* permet d'écrire les axiomes directement. Il faut cependant faire attention de bien les choisir ;
- On peut les utiliser dans les assistants de preuve (exemples d'assistants de preuve : *Coq, Isabelle*)

7.2 Théorie du premier ordre

Intuition : définition logique d'une structure mathématique

7.2.1 Définition d'une théorie

- Sous-langage de la logique du premier ordre
  - **vocabulaire** : constantes, fonctions, prédicats ;
  - règles syntaxiques et sémantiques sur ce vocabulaire ;
- Ensemble d'axiomes (formules fermées, c'est-à-dire formules ne contenant pas de variables libres) ;

— Ensemble de règles d'inférence.

7.2.2 Exemple : théorie des liens familiaux (fam)

1. Vocabulaire :
   — 2 symboles de fonctions : $p/1$, $m/1$
   — 3 symboles de prédicats : $P/2$, $GM/2$, $GP/2$

   On peut interpréter les fonctions p et m comme "père de" et "mère de", et les prédicats P, GM et GP comme "parent de", "grand-mère de" et "grand-père de". On donnera plus de précisions sur cette interprétation par la suite.

2. Axiomes :

   $(\forall x)\,(P(x, p(x)))$ (père)
   $(\forall x)\,(P(x, m(x)))$ (mère)
   $(\forall x)(\forall y)\,(P(x, y) \Rightarrow GP(x, p(y)))$
   $(\forall x)(\forall y)\,(P(x, y) \Rightarrow GM(x, m(y)))$

3. Règles :
   Les règles sont uniquement celles de la logique des prédicats.

Première interprétation

D_I : personnes

$\text{val}_I(p)$ = "père de"	père de : Pers $\to$ Pers : $d \to$ "père de" d
$\text{val}_I(m)$ = "mère de"	mère de : Pers $\to$ Pers : $d \to$ "mère de" d
$\text{val}_I(P)$ = "Parent"	Parent$(d_1, d_2) = T$ ssi d_2 est un parent de d_1
$\text{val}_I(GP)$ = "Grand-père"	Grand-père$(d_1, d_2) = T$ ssi d_2 est un grand-père de d_1
$\text{val}_I(GM)$ = "Grand-mère"	Grand-mère$(d_1, d_2) = T$ ssi d_2 est une grand-mère de d_1

Cette interprétation est un modèle de FAM car les axiomes sont tous vérifiés.
On remarque la ressemblance avec une théorie scientique, où les axiomes correspondent à la théorie et l'interprétation à ce que celle-ci signifie dans le monde réel.
Une théorie peut avoir plusieurs modèles.

Seconde interprétation

Cette interprétation est également un modèle de FAM.

$D_J : \mathbb{N}$	
$\text{val}_J(p) = "p_J"$	$p_J : \mathbb{N} \to \mathbb{N} : d \to 2d$
$\text{val}_J(m) = "m_J"$	$m_J : \mathbb{N} \to \mathbb{N} : d \to 3d$
$\text{val}_J(P) = "P_J"$	$P_J(d_1, d_2)$ ssi $d_2 = 2d_1$ ou $d_2 = 3d_1$
$\text{val}_J(GP) = "GP_J"$	$GP_J(d_1, d_2)$ ssi $d_2 = 4d_1$ ou $d_2 = 6d_1$
$\text{val}_J(GM) = "GM_J"$	$GM_J(d_1, d_2)$ ssi $d_2 = 6d_1$ ou $d_2 = 9d_1$

7.3 Propriétés des théories

— Une formule fermée p est **valide** dans la théorie Th si elle est vraie dans chaque modèle de Th. On écrit :

$$\vDash_{Th} p$$

Soit l'ensemble des axiomes $Ax = \{Ax_1, \ldots, Ax_n\}$. On a bien que $\vDash_{Th} Ax_i$.

— q est une **conséquence logique** de p dans la théorie Th si q est vraie dans tous les modèles de Th qui rendent p vraie. On écrit :

$$p \vDash_{Th} q$$

— Une théorie est **consistante** si elle a au moins un modèle (> 0 modèles).
— Une théorie est **inconsistante** si elle n'a pas de modèle (0 modèles).

Comment peut-on faire pour établir $\vDash_{Th} p$? Il y a deux approches différentes :

1. **l'approche sémantique** : on prend un modèle quelconque de Th et on évalue $\text{VAL}_I(p)$ en utilisant le fait que $\text{VAL}_I(Ax_i) = T$;
2. **l'approche syntaxique** : théorie de preuve : on essaye de construire une preuve de p à partir des axiomes, en appliquant les règles de Th.

En pratique, la deuxième approche est beaucoup plus souvent utilisée.

Preuve (esquisse)

La preuve qui suit est une esquisse. Il manque plusieurs étapes.
On veut montrer :

$$\vDash_{\text{FAM}} (\forall x)(\exists z) GM(x, z)$$

$(\forall x)(\forall y)\,(P(x,y) \Rightarrow GM(x,m(y)))$	(Ax)
$(\forall x)\,(P(x,p(x)) \Rightarrow GM(x,m(p(x))))$	(Elimination de $\forall y$ et substitution $y/p(x)$)
$(\forall x\ P(x,p(x))) \Rightarrow \forall x\ GM(x,m(p(x)))$	(Distribution $\forall/\Rightarrow$)
$\forall x\ GM(x,m(p(x)))$	(Modus ponens)
$\forall x\ \exists y\ GM(x,y)$	(Introduction de $\exists$)

7.4 Qualité d'une théorie

Certaines qualités sont directement issues de la logique :

1. **consistante** : il est impossible de déduire p et $\neg p$ de la même théorie.
2. **minimale** : les axiomes sont indépendants : $\{Ax_1, \ldots, Ax_n\} \not\models Ax_k$
   Vérification : Construction d'interprétations.
   $\mathrm{VAL}_J(Ax_k) = False$
   $\mathrm{VAL}_J(Ax_i) = True$ pour $i \neq k$
3. **complète** : les axiomes suffisent pour prouver la propriété d'intérêt. Sinon il faut en ajouter.

7.4.1 Exemple : qualité de deux théories

1. **Système de Copernic** : Chaque axiome de chaque planète est indépendant, car elles tournent toutes autour du soleil.
2. **Système de Ptolémée** : Les axiomes de chaque planète dépendent de ceux de la Terre, car elle représente le centre de l'univers, mais elle est également une planète et dispose donc d'axiomes.

7.5 Extension d'une théorie

Lorsqu'on a une théorie déjà existante, on souhaite parfois l'étendre afin de la rendre plus complète. Pour ce faire, on ajoute des axiomes et on étend le vocabulaire. Voici deux exemples d'extension de théorie pour mieux comprendre comment effectuer cette opération. Ils étendent tous les deux la théorie des liens familiaux (FAM) décrite dans la section précédente.

Exemple 1

Considérons le nouvel axiome suivant, que nous noterons Ax.

$$(\forall x)\neg P(x,x)$$

La nouvelle théorie ainsi étendue que nous noterons FAM* possède un axiome de plus : Ax. Cette théorie FAM* est **consistante**, c'est-à-dire qu'il existe au moins un modèle qui valide cette théorie. Pour s'en convaincre, il suffit de considérer la première interprétation de la théorie FAM de la section précédente, qui utilise les liens familiaux.

En revanche, si on considère la deuxième interprétation (deuxième modèle, noté J) de FAM qui associe les symboles p et m aux fonctions mathématiques $p_J : \mathbb{N} \to \mathbb{N} : d \to 2d$ et $m_J : \mathbb{N} \to \mathbb{N} : d \to 3d$, on observe une contradiction. En effet, dans le modèle J on a la définition suivante du prédicat P :

$$P_J(d_1, d_2) \text{ ssi } d_2 = 2d_1 \text{ ou } d_2 = 3d_1$$

Il suffit de choisir $x = 0$ dans notre nouvel axiome Ax pour constater que le modèle J ne valide pas la théorie étendue FAM*. De manière générale, l'extension d'une théorie peut donc réduire l'ensemble des modèles de celle-ci.

Exemple 2

Considérons à présent le nouvel axiome suivant, que nous noterons Adam.

$$(\forall y)\neg P(a,y)$$

où a est une constante arbitraire. Notons la théorie étendue FAM' = FAM + Adam. Dans cet exemple, on peut observer que FAM' est **inconsistante,** car aucun modèle ne peut valider cette théorie. En effet, en partant du premier axiome de FAM (appelé "père"), nous effectuons quelques étapes

pour obtenir une contradiction.

$$\begin{aligned} & (\forall x)P(x, p(x)) & \\ \iff & P(a, p(a)) & \text{Elimination } \forall \\ \iff & (\exists y)P(a, y) & \text{Intro } \exists \end{aligned}$$

Ci-dessus, le premier axiome de FAM reformulé (père), qui est en contradiction avec le nouvel axiome (Adam), que nous reformulons ci-dessous.

$$\begin{aligned} & (\forall y)\neg P(a, y) \\ \iff & \neg(\exists y)P(a, y) \end{aligned}$$

Par la règle de preuve par contradiction, on démontre qu'aucun modèle n'est possible pour la théorie étendue FAM'. Étendre une théorie équivaut à faire de la manipulation syntaxique. Il est important de bien vérifier ce que notre modification a comme conséquence sur le nombre de modèles que la théorie accepte.

7.6 Liens entre théories

Dans cette section, nous abordons la comparaison de différentes théories : inclusion, équivalence et quelques corollaires ainsi que la théorie des ordres partiels stricts. Dans ce qui suit, on note Th_1 et Th_2 deux théories.

Inclusion

On dit que Th_1 est **contenue** dans Th_2 si
- Le vocabulaire de Th_1 est inclus dans le vocabulaire de Th_2.
- Toute formule valide dans Th_1 l'est aussi dans Th_2.

Attention, on peut donc avoir deux théories qui "parlent de la même chose" mais qui possèdent des axiomes totalement différents. TODO : expliquer pourquoi / Ajouter un exemple

Équivalence

On dit que Th_1 et Th_2 sont **équivalentes** si elles sont contenues l'une dans l'autre. Cela signifie que les deux théories "disent la même chose" et que tout modèle d'une des théories est également modèle de l'autre.

Il est important de bien faire la différence entre les **liens** entre les théories et l'**extension** d'une théorie. Le premier concept exprime ce que modélisent les théories tandis que le deuxième n'est que de la manipulation syntaxique.

Corolaires

On note respectivement V_i, M_i et Ax le vocabulaire, les modèles et les axiomes d'une théorie i.

Si $V_{Th_1} \subseteq V_{Th_2}$ et $M_{Th_2} \subseteq M_{Th_1}$ alors Th_1 est contenue dans Th_2.

Si $V_{Th_1} \subseteq V_{Th_2}$ et tout axiome de Th_1 est aussi axiome de Th_2 alors Th_1 est contenue dans Th_2.

Si $V_{Th_1} = V_{Th_2}$ et $\forall i, j \quad \vDash_{Th_2} Ax_{i,1}$ et $\vDash_{Th_1} Ax_{j,2}$ alors Th_1 et Th_2 sont équivalentes.

Si p une formule fermée telle que $\vDash_{Th_1} p$ et $Th_2 = Th_1 \bigcup \{p\}$ alors Th_1 et Th_2 sont équivalentes.

7.7 Théorie des ordres partiels stricts

Nous allons donner un autre exemple de théorie ainsi que deux interprétations différentes de cette théorie.

Vocabulaire

- Le symbole P

Axiomes

- $(\forall x)\neg P(x, x)$ (irréflexivité) (OPS1)
- $(\forall x)(\forall y)(\forall z)(P(x, y) \wedge P(y, z) \Rightarrow P(x, z))$ (transitivité) (OPS2)

Première interprétation

Soit l'interprétation I de cette théorie. On a :

- $D_I = \mathbb{Z}$
- $val_I(P) =$ " $<$ "

Lorsque l'on écrit $val_I(<) =$ " $<$ ", le premier symbole $<$ est un mot de vocabulaire dans la théorie tandis que le deuxième est une fonction. Cette fonction confère un sens au symbole. On remarque que cette interprétation est un modèle de notre théorie. En effet, la fonction $<$ sur les entiers est

irréflexive et transitive. Si on a $x < y$ et $y < z$, on peut en déduire que $x < z$.

Deuxième interprétation

Soit l'interprétation J de cette théorie. On a :

- $D_J = \mathbb{Z}$
- $val_J(P) = " \neq "$

Ici on change le sens du symbole $<$:

$$val_J(<) = " \neq "$$

Cette interprétation n'est pas un modèle. En effet, par exemple, pour $x = 5, y = 3, z = 5$, on a :

$$5 < 3 \wedge 3 < 5 \nRightarrow 5 < 5$$

Ceci est un contre-exemple, car 5 n'est pas différent de 5 (irréflexivité), et donc cette interprétation ne vérifie pas l'axiome sur la transitivité !

7.8 Théorie de l'égalité (EG)

Il existe différents symboles pour représenter l'égalité :
— E(x,y)
— $x = y$
— $x == y$
Nous allons utiliser $'=='$ dans la suite de ce cours pour représenter l'égalité.

7.8.1 Axiomes

Pour définir ce qu'est une égalité, nous avons d'abord besoin de définir 3 axiomes et 2 schémas d'axiomes :

1. Réflexivité
   $\forall x, x == x$
2. Symétrie
   $\forall x, \forall y, x == y \Rightarrow y == x$
3. Transitivité
   $\forall x, \forall y, \forall z, (x == y \wedge y == z) \Rightarrow x == z$
4. Substituabilité dans les fonctions
   $\forall x_1, ..., x, ..x_n \ , \ x_i == x \Rightarrow f(x_1, ..., x_i, ..x_n) == f(x_1, ..., x, ..x_n)$
5. Substituabilité dans les prédicats
   $\forall x_1, ..., x, ..x_n \ , \ x_i == x \Rightarrow P(x_1, ..., x_i, ..x_n) == P(x_1, ..., x, ..x_n)$

7.8.2 Règles d'inférences

En plus de ces 5 axiomes, il nous faut aussi définir deux règles d'inférences.

Substituabilité fonctionnelle

$$\frac{s_1 == t_1 \wedge s_2 == t_2 \wedge ... \wedge s_n == t_n}{f(s_1, s_2, ..., s_n) == f(t_1, t_2, ..., t_n)}$$

Substituabilité prédicative

$$\frac{s_1 == t_1 \wedge s_2 == t_2 \wedge ... \wedge s_n == t_n}{P(s_1, s_2, ..., s_n) == P(t_1, t_2, ..., t_n)}$$

Grâce aux règles sémantiques de l'égalité, on peut raisonner sur des formules, mais aussi bien sur une interprétation.
Si $VAL_I(t_1) == VAL_I(t_2)$ alors $VAL_I(t_1 == t_2) = true$

Preuve (Métalangage)

Soit I, un modèle de EG ($'=='$) pour t_1 et t_2.
$VAL_I(t_1 == t_2) = VAL_I(==)(VAL_I(t_1), VAL_I(t_2))$
On pose $VAL_I(==) = E_I$ et $VAL_I(t_1) = e$ et $VAL_I(t_2) = e$
Donc $VAL_I(t_1 == t_2) = E_I(e, e)$
$\Rightarrow$ preuve en regardant les axiomes
$VAL_I(\forall x, x == x) = true$ (réflexivité)
On cherche le $\forall x$ dans la sémantique :
On sait que pour tout d $\in$ Domaine de I, $VAL_I(d == d) = true$,
Si $d = e$
alors $E_I(e, e) = true$

7.8.3 Remarque

La théorie de l'égalité a une utilité très limitée, elle doit être étendue pour pouvoir servir à quelque chose. On appelle une telle théorie un template.

7.9 Théorie de l'ordre partiel (OP)

On ajoute un deuxième symbole dans le langage en plus du symbole d'égalité.

— $==$
— $\leq$

7.9.1 Axiomes

Aux axiomes et schémas d'axiomes de la théorie de l'égalité, on rajoute de nouveaux axiomes

1. Réflexivité
   $\forall x$, $x \leq x$
2. Anti-symétrie
   $\forall x$, $\forall y$, $x \leq y \wedge y \leq x \Rightarrow y == x$
3. Transitivité
   $\forall x$, $\forall y$, $\forall z$, $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$
4. Substituabilité à gauche
   $\forall x_1$, $\forall x_2$, $\forall x$, $x_1 == x \Rightarrow x_1 \leq x_2 \Leftrightarrow x \leq x_2$
5. Substituabilité à droite
   $\forall x_1$, $\forall x_2$, $\forall x$, $x_2 == x \Rightarrow x_1 \leq x_2 \Leftrightarrow x_1 \leq x$

Théorème : $\models \forall x, \forall y, [x == y \Leftrightarrow (x \leq y) \wedge (y \leq x)]$

7.9.2 Preuve

La preuve va être démontrée en partie en métalangage et en partie en preuve formelle.

$\Leftrightarrow$ equivant à : $\Leftarrow \wedge \Rightarrow$

$\Leftarrow$: est démontré par l'axiome antisymétrique

$\Rightarrow \models_{op} \forall x, \forall y, [x \leq y \wedge y \leq x]$

preuve formelle :

1. $\forall x, \forall y, x == y \Rightarrow x \leq x \Leftrightarrow y \leq x$ — substituabilité à gauche
2. $\forall x, \forall y, x == y \Rightarrow x \leq x \Leftrightarrow x \leq y$ — substituabilité à droite
3. $x == y \Rightarrow x \leq x \Leftrightarrow y \leq x$ — $\forall$ élimination
4. $x == y \Rightarrow x \leq x \Leftrightarrow x \leq y$ — $\forall$ élimination

preuve conditionnelle :

5. $x == y$ — supposition
6. $y \leq x$ — modus ponens (1,4)
7. $x \leq y$ — modus ponens (2,4)
8. $y \leq x \wedge x \leq y$ — conjonction (6,7)
9. $x == y \Rightarrow x \leq x \Leftrightarrow y \leq x \wedge x \leq y$
10. $\forall x, \forall y, x == y \Rightarrow x \leq x \Leftrightarrow y \leq x \wedge x \leq y$ — $\forall$ Introduction

7.9.3 Exemples de modèles d'OP

— $\underline{I_1} : D_{I_1} = \mathbb{Z}$
$val_{I_1}(==) = '='$: égalité d'entiers
$val_{I_1}(\leq) = '\leq'$: plus petit ou égal pour les entiers
cette interprétation va satisfaire tous les entiers.

— $\underline{I_2} : D_{I_2} = P(E)$ ensemble des sous-ensembles de E
$val_{I_2}(==) = '='$: égalité d'ensemble
$val_{I_2}(\leq) = '\subseteq'$: inclusion d'ensemble

— $\underline{I_3} : D_{I_3} = ALPH^2 = (l_1, l_2), ..$ doublons de lettres de l'alphabet
$val_{I_3}(==)$ = égalité des paires
$val_{I_3}(\leq)$ = suivant ordre lexicographique
exemple : $(l_i, l_j) \leq (l_p, l_q)$ si $l_i < l_p$ ou $l_i = l_p$ et $l_j < l_q$ ou $l_j = l_q$

— $\underline{I_3} : D_{I_4}$ = ensemble de listes
$val_{I_4}(==) = =$ égalité de liste (si elles possèdent les mêmes composants à la même position)
$val_{I_3}(\leq)$ = "suffixe de"

exemple : l_1 est suffixe de l_2
l_1 = [d, e, f, g, h] et l_2 = [a, b, c, d, e, f, g, h, i]

— $\underline{I_5}$: Soit D_{I_5} l'ensemble des formules en logique des propositions. On commence à utiliser la logique pour parler d'elle-même :
$VAL_{I_5}(==)$ = "<≡>" → L'égalité est synonyme d'équivalence en logique des propositions $VAL_{I_5}(\leq)$ = "⊨" → Le signe d'inclusion entre les ensembles de modèles. Maintenant qu'on a défini la sémantique de l'ordre partiel en utilisant la notion de modèles, on peut prendre quelques exemples en raisonnant sur la logique :
p $\leq_{I_5}$ q p $\models_{I_5}$ q $\models$ p ⇒ q

— $\underline{I_6}$: D_{I_6} = l'ensemble des unificateurs d'un ensemble S de termes ou de formules $VAL_{I_6}(==)$ = égalité entre substitutions { (x_i,t_i)... } : un ensemble de paires avec une variable et un terme $VAL_{I_6}(\leq)$ = "moins général que"

Exemple : P(x,f(y)) $\underbrace{P(x,z)}_{\sigma}$

σ' = $\sigma \cup$ {(z, f(y)} donc $\sigma' \leq \sigma$

Ces exemples montrent qu'on peut raisonner sur tout, y compris sur la logique et les algorithmes eux-mêmes, à partir du moment où on respecte les axiomes.

7.10 Théorie des ensembles

Elle sera utilisée pour la spécification des systèmes $\mathbb{Z}$.

Ensemble : on peut définir les ensembles de façon informelle (c'est-à-dire sans les axiomes) :

- Un ensemble peut être défini comme une énumération d'éléments
  Ex : {0,20,40,60,80,100 } ou {Mercure, Vénus, terre ..., Neptune}
- Il peut également être défini comme le prédicat d'un argument qui est vrai pour les membres. On appelle cette définition informelle "compréhension)". Certains langages comme Python possèdent des syntaxes particulières dédiées à la création de listes remplies par des compréhensions
  Ex. : $\{ n \mid n \in \mathbb{N} \land \exists k, k \in \mathbb{N} \land 20k = n \land 0 \leq n \leq 100 \}$

La définition formelle des ensembles passe par 8 axiomes :
Axiomes

- **Égalité** (1 ère définition)
  $A = B \Leftrightarrow (\forall x)\ (x \in A \Leftrightarrow x \in B)$

- **Ensemble vide** (sans éléments)
  $\emptyset = \{x \mid x \neq x\}$

- **Ensemble universel** (tous les éléments du domaine)
  $\mathcal{U}$ (par exemple : $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Z}$)

- **Sous-ensemble**
  $A \subseteq B \Leftrightarrow (\forall x)\ (x \in A \Rightarrow x \in B)$
  $A \nsubseteq B \Leftrightarrow \neg(A \subseteq B)$
  $A \subset B \Leftrightarrow A \subseteq B \land A \neq B$

- **Construction de sous ensemble**
  $A \subseteq B \Leftrightarrow (x \in A \Leftrightarrow x \in B \land \varphi(x))$
  On va ici prendre des éléments de B tels que $\varphi(x)$ est vrai, et les mettre dans A. C'est un peu une formulation de la notion de compréhension.

- **Propriétés**
  $\emptyset \subseteq A$
  $A \subseteq A$
  $A \subseteq B \land B \subseteq C \Rightarrow A \subseteq C$

— **Égalité** (2e définition)
(A = B) ⇔ (A ⊆ B) ∧ (B ⊆ A)

— **Taille d'un ensemble**
  — Prédicat à 2 arguments
  #(A,n)
  #∅ = 0 → #(∅, 0)
  — ℙA = {a | a ⊆ A} (prédicat à 2 arguments)
  #ℙA = $2^{\#A}$

Spécification formelle des systèmes avec l'approche ℤ

Cette approche est "Orientée modèle" : On ne donne pas que des équations, mais aussi des structures

Deux concepts en ℤ :

Types :

— Types génériques (ensembles) : par exemple : Book, Location
— Types énumérés : par exemple :

Statuts := $\underbrace{In}_{\textit{Dans la bibliothèque, disponible}} \mid \overbrace{Out}^{\textit{Prêté}} \mid \underbrace{Ref}_{\textit{Livre de référence}}$

Schémas :

— État du système : → logique des prédicats
— Comportement actions : préconditions et posconditions → également logique des prédicats

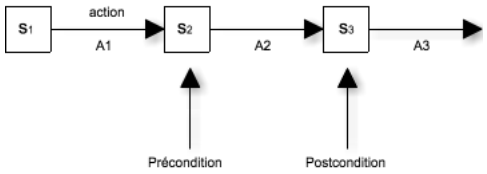
Exemple d'un état

nom	LIB_STOCK
signature	stock on_loan on_shelf ref_coll : ℙ Book
prédicat	stock = on_loan ∪ on_shelf on_loan ∩ on_shelf = ∅ ret_call ⊆ on_shelf

$\mathbb{F}$ Book représente un sous-ensemble fini de l'ensemble Book.

Exemple du comportement

— Il y a un "avant" et un "après"
Les variables "avant", on les écrit normalement (sans rien changer) alors qu'on ajoute une apostrophe aux variables "après" pour pouvoir les distinguer. Ex. : Stock et Stock'
— Une exécution est une séquence d'états



— Notation $\mathbb{Z}$
Δ Lib_Stock $\triangleq$ Lib_Stock $\wedge$ Lib_Stock'
$\equiv$ Lib_Stock $\triangleq$ Lib_Stock $\wedge$ (Lib_Stock' | Lib_Stock = Lib_Stock')
Cette deuxième ligne d'exemple veut dire la même chose, mais dans la condition où Lib_stock n'a pas changé.

nom	ADD_STOCKo
signature	Δ lib_stock new ? : $\mathbb{F}$ Book
prédicat	new ? $\neq \emptyset \rightarrow$ précondition new ? $\wedge$ stock $= \emptyset \rightarrow$ précondition stock' = stock $\cup$ new ? $\rightarrow$ postcondition on_loan' = on_loan $\rightarrow$ postcondition

Le " ?" signifie qu'il s'agit d'une entrée.
On peut déduire de ces prédicats que new ? sera dans on_shelf.
— Si la ou les préconditions ne sont pas satisfaites, on aura des erreurs que l'on devra corriger via la gestion d'erreurs. Si les préconditions n'échouent jamais, on a affaire à une opération totale.

Exemple d'opération totale :

ADD_STCK = AdDD_STCKo $\cup$ ERRONEOUS_NEW_STOCK

nom	ERRONEOUS_NEW_STOCK
signature	$\equiv$ lib_stock new ? : # Book rep ! : Report
prédicat	(new ? $= \emptyset \cup$ new ? $\cap$ stock $\wedge \emptyset$) ... $\rightarrow$ préconditions rep ! = "Attention stock problem"

Le " !" signifie qu'il s'agit d'une sortie.

7.11 Introduction à la programmation logique

7.11.1 Introduction à la programmation logique

Prolog est l'un des principaux langages de programmation logique. Il est à la base de nombreux fondements.

La programmation logique fait de la déduction sur les axiomes. On utilise la logique comme un langage de programmation : on va adapter l'algorithme de réfutation vu précédemment

Le programme (ressemble à une théorie) :
— Axiomes en logique des prédicats
— Une requête, un but (=goal)→ le but du système est d'apporter une preuve
— Un prouveur de théorème → attention : il faut des conditions sur le prouveur car il faut être capable de prévoir le temps et l'espace utilisé par le programme.

Exécuter un programme = faire des déductions en essayant de prouver le but. Mais est-ce que cette idée peut donner un système de programmation pratique ?

Il y a un compromis entre expressivité et efficacité : si c'est trop expressif, ça devient moins efficace, par contre si c'est trop peu expressif, on ne peut rien programmer, ça ne sert à rien non plus. Il faut donc être expressif tout en restant efficace. Le Prolog offre un bon équilibre entre expressivité et efficacité.

Mais pour arriver à cela, il y a quelques problèmes à surmonter :

a. un prouveur est limité :
vérité = $p \models q$ (= q est vrai dans tous les modèles de p)
preuve = $p \vdash q$
$p \models q \Rightarrow p \vdash q$ (= Si c'est vrai dans tous les modèles, on peut trouver une preuve)
Si $p \models q$ alors l'algorithme se terminera. Cependant, on ne peut pas trouver les preuves que pour des choses vraies dans tous les modèles. (Comme c'est impossible, on ne prend qu'une partie des modèles ce qui limite le programme).
b. Même si l'on peut trouver une preuve, le prouveur est peut-être inefficace (utilise trop de temps ou de mémoire) ou imprévisible. → On ne peut pas raisonner sur l'efficacité du prouveur.
c. La déduction faite par le prouveur doit être constructive

Si le prouveur affirme : $(\exists X)P(X)$ alors le prouveur doit donner une valeur de x (c'est quoi x).

Il faut construire un résultat.

Pour résoudre ces problèmes...

1. Restrictions sur la forme des axiomes.
   typiquement :

$$(\forall X_1)...(\forall X_n)A_1 \wedge A_2 \wedge ... \wedge A_n \Rightarrow A \tag{7.1}$$

$$C_i = \neg A_1 \vee \neg A_2 \vee ... \vee \neg A_n \vee A \tag{7.2}$$

   Il n'y a qu'un seul littéral sans négation. (Pour prouver A, il faut prouver A_1 ; A_2, ..., A_n).
   C_i est une clause. Le programme tout entier est une série de clauses :

$$C_1 \wedge C_2 \wedge ... \wedge C_k \tag{7.3}$$

2. Le programmeur va aider le prouveur. Par exemple : il faut commencer par prouver A_1 puis A_2... dans cet ordre là.
   $\rightarrow$ Le programmeur donnera des heuristiques. Attention : ces heuristiques ne changent pas la sémantique logique du programme. Elles ont seulement un effet sur l'efficacité !

$$\text{ordre des axiomes} \begin{cases} C_1 = \neg A_1 \vee \neg A_2 \vee ... \vee A_n \vee A \\ C_2 = \underbrace{\neg B_1 \vee \neg B_2 \vee ... \vee B_k \vee A}_{\text{ordre des littéraux dans un axiome}} \end{cases} \tag{7.4}$$

Le langage Prolog utilise ces 2 ordres.

Bref historique :

1. 1965 : La règle de résolution a été inventée par A. Robinson
2. 1972 : Invention du langage Prolog / premier interprète (de Prolog) par A. Calmerauer, R. Kowalski et Ph. Roussel. Ils voulaient faire un langage de programmation logique, et connaissaient les différentes formes de logique ainsi que la résolution. Ils ont donc inventé un langage très simple qu'ils ont appelé Prolog (pour Programmation Logique). Il s'avère que ce langage a un compromis très intéressant par rapport à la tension entre efficacité et expressivité. Aujourd'hui, on peut faire une implémentation extrêmement efficace de Prolog. Il est extrêmement expressif, ce qui permet de faire des programmes complexes. C'est un langage à part entière.

7.11.2 Introduction à Prolog

En Prolog, on a des clauses (règles) :

$$A1 \leftarrow B1, \ldots, Bn \tag{7.5}$$

(On peut prouver A en prouvant $B1$ jusqu'à Bn. Remarque :←ou :-)

$$\neg(B_1 \wedge ... \wedge B_n) \vee A_1 \tag{7.6}$$

$$(\neg B_1 \vee \neg B_2 \vee ... \vee \neg B_n \vee A_1) \tag{7.7}$$

Programme = ensemble de clauses.

Exemple d'un petit programme en Prolog : (extrait du livre « The Art of Prolog » par L. Sterling et E. Shapine)

Règle : $grandpere(x, z) \leftarrow pere(x, y), pere(y, z)$. ($x$, y,... sont des variables. En Prolog, elles sont souvent en majuscule)

Faits : $pere(terach, abraham)$ (terach, abraham,... sont des constantes)
$pere(abraham, isaac)$
$pere(haram, lot)$
...

→ Syntaxe clausale : $pere(terach, abraham) \wedge pere(abraham, isaac) \wedge pere(haram, lot) \wedge (\neg pere(x, y) \vee \neg pere(y, z) \vee grandpere(x, z))$

Il existe une corrélation évidente entre Prolog et les bases de données. Elles ont été inventées quasi au même moment et aujourd'hui Prolog est utilisé comme une sémantique pour les bases de données déductibles. Ici, on peut avoir une relation avec deux colonnes qui auraient l'argument père. le grand-père serait une combinaison de ces deux relations.

Prolog peut être vu comme une sorte de base de données relationnelle mais beaucoup plus puissante : on peut faire des programmes qui sont plus que des simples requêtes, avec des calculs beaucoup plus complexes.

7.11.3 Algorithme d'exécution de Prolog

Dans la version de l'algorithme de preuve par résolution, l'ensemble S grandit (ce qui n'est pas très efficace).

L'idée :

— On commence par mettre le but (G) que l'on veut prouver dans r (sans négation).

— Ensuite, jusqu'à ce que r soit vide, on prend le premier littéral dans $r(A_1)$.
— Puis, on parcourt un à un les axiomes de P (P est le programme, la base de faits) pour trouver une clause Ax_i unifiable avec A_1 au moyen de $\sigma(u.p.g)$
  — Si on trouve une telle clause, on ajoute à r les littéraux de Ax_i après unification avec A_1 (et on recommence au début).
  — Si on ne trouve pas de clause unifiable, on revient sur le dernier choix (Par exemple, pour un A_1 qui aurait plusieurs clauses unifiables, on a dû en choisir une. Et bien, on retourne en arrière pour en choisir une autre, sans oublier de modifier r. (En effet, il faut éliminer les résultats de toutes les unifications qui ont été réalisées entre le moment où le point de choix a été mémorisé et le moment du retour en arrière.))
  — Si on épuise tous les choix sans que r soit vide alors nous sommes en cas d'échec.
— Lorsque le programme s'arrête, si r est vide, on a un résultat.

Programme : $P = Ax_1, ..., Ax_n$

Un « but » (un goal, une « requête ») G ($\simeq$ théorie)

$r :=< G > \ldots$ résolvante (une séquence de littéraux $\rightarrow$
$r =< A_1, A_2, ..., A_m >$ Il n'y a qu'un seul r.)

while *r est non vide* **do**
  — Choisir un littéral A_1 dans r (on prend le premier littéral)
  — Choisir une clause $Ax_1 = (A \leftarrow B_1, ..., B_k)$ dans P. (d'abord on prend la première clause, puis la suivante jusqu'à ce qu'on trouve une clause unifiable avec A_1. Si aucune clause n'est unifiable on revient sur le dernier choix (backtrack))
  — Nouvelle résolvante $:=< B_1, ..., B_k, A_2, ..., A_m > \sigma$
  — $G' = G\sigma$
end
if *r est vide* **then**
  le résultat est le dernier G'
end
if *on épuise les choix sans que r soit vide* **then**
  le résultat est NON. (On n'a pas prouvé G). (Attention : G est peut-être vrai, mais les heuristiques ne suffisent pas pour le prouver.)
end

On peut également avoir une boucle infinie (l'algorithme est non déterministe).

7.12 Exemples de programmes Prolog

Programme (code Prolog)

Ce petit programme permet de calculer la factorielle d'un nombre. Il s'agit de clauses exprimant des faits, des règles et des questions. Le code commence par un fait : 0 !==1. Ensuite, il définit une clause pour les factorielles de façon généralisée. Attention, les virgules et les points sont importants. Les virgules sont les séparateurs entre les littéraux dits négatifs tandis que le point marque la fermeture de la clause.

```
fact(0,1)
fact(N,F) :- N>0,
 N1 is N-1
 fact(N1,F1),
 F is N* F1 .
```

Requête

Nous allons maintenant exécuter le programme fact afin de trouver la factorielle de 5 et stocker la réponse dans la variable F. Le prompt Prolog est représenté par " | ?- " et la sortie standard par "->". Les commentaires sont après les "%" ou entre "/* */". Il ne faut pas oublier le point à la fin de la requête.

```
|?- fact (5,F). %requête
-> F=120 % réponse
```

Forme clausale

Le programme réécrit sous forme clausale.

$$
\begin{aligned}
& fact(0,1) \\
& \quad \wedge \\
& \quad (\neg n > 0 \\
& \quad \vee \neg minus(n1, n, 1) \\
& \quad \vee \neg fact(n1, f1) \\
& \quad \vee \neg times(f, n, f1) \\
& \quad \vee fact(n, f))
\end{aligned}
$$

Exécution

Le but de l'exécution est de prouver que $G \equiv fact(5, r)$. Pour y arriver, Prolog va faire une suite de substitutions σ afin de vérifier les affirmations contenues dans r. La substitution finale contiendra le résultat final.

$G \equiv fact(5, r)$
$r =< fact(5, r) >$
%(1)
$\sigma = \{(n, 5), (f, r)\}$
$r =< (5 > 0), minus(n1, 5, 1), fact(n1, f1), times(r, 5, f1) > \sigma$
%(2)
$r =< minus(n1, 5, 1), fact(n1, f1), times(r, 5, f1) >$
$\sigma' = \{(n1, 4) \cup \sigma\}$
$r =< fact(4, f1), times(r, 5, f1) >$
[...]
$\sigma_{res} = \{(r, 120), ...\}$

(1) avec clause 2
(2) a>b existe dans le système prédéfini -> true

Exemple 2

Le but de cet exemple est de faire un "append" de deux listes :
append(L1, L2, L2)

Prolog :
- append ([] , L , L)
- append ([X|L1], L2, [X|L3]) :- append (L1,L2,L3)

Clausal Le programme réécrit sous forme clausale.
append(nil,l',l')
$\wedge$
($\neg$append(l_1, l_2, l_3) $\wedge$ append (cons(x, l_1), l_2, cons(x,l_3))

Execution Attention, l'exécution du programme est une preuve en soi.
G = append (cons(1,nil), cons(2, nil), l)

1. r= < append (cons(1,nil), cons(2,nil, l)> et σ_1 = (x,1), (l_1,nil), (l_2, cons(2,nil)), (cons(x,l_3),l)
2. r=< append(nil,cons(2,nil),l_3)> et σ_2 = (l', cons(2, nil), (l_3,l')
3. r=<>

Résultat l = con (1, l_3) l_3 = l' l' = cons(2,nil) l=con(1,cons(1,nil))

Exemple 3

Intéressons-nous à la manière dont prolog exécute la requête **|?- append (L1,L2,[1])** en nous basant sur la syntaxe définie lors de l'exemple 2.
Pour information, la fonction cons prend comme premier argument une valeur et comme second argument une liste. Elle place le premier argument en tête du second argument.

Requête

```
|?- append (L_{1},L_{2},[1]). %requête
-> r = <append (l_{1}',l_{2}',cons(1,nil))> % réponse

L_{1} = [],
L_{2} = [1]. %clause 1
ou
L_{1} = [1],
L_{2} = []. %clause 2
```

Forme clausale Le programme réécrit sous forme clausale.
append(nil,l',l')
$\wedge$
($\neg$append(l_1, l_2, l_3) $\vee$ append (cons(x, l_1), l_2, cons(x,l_3))

Exécution Dans cet exemple, il y a plusieurs chemins pour arriver au résultat

Si l'on choisit la clause 1 :

$$\sigma = (l'_1, nil), (l'_2, l'), (l', cons(1, nil))$$
$$r = <>$$
$$l'_1 = nil$$
$$l'_2 = cons(1, nil)$$

Si l'on choisit la clause 2 :

$$\sigma = (l'_1, cons(x, l_1)), (l'_2, l_2), (x, 1), (l_3, nil)$$
$$r =< append(l_1, l'_2, nil) >$$
$$\sigma = (l_1, nil), (l_2, l'_2), (nil, l_3)$$
$$r =<>$$
$$l'_1 = nil$$
$$l'_2 = cons(1, nil)$$

Il existe deux manières de percevoir une exécution Prolog.

1 Approche "impérative" : l'exécution est vue comme une séquence de calculs
2 Approche logique : l'exécution est vue comme une preuve. Cette approche n'existe pas dans les langages classiques, c'est ce qui fait la force de Prolog.

Prolog est présent dans beaucoup de domaines de programmation :

— Dans la gestion de base de données avec Datalog
— Dans la sémantique web
— Dans la programmation par contrainte. Les substitutions sont remplacées par des relations quelconques.

Deuxième partie

Structures discrètes sur Internet

Chapitre 8

Structures discrètes sur l'Internet

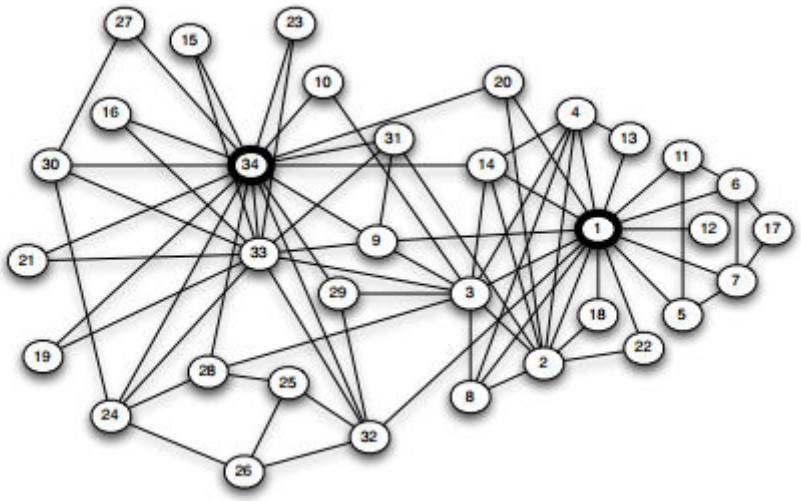
8.1 Ressources

Livre : sur iCampus
- Chapitre 1-5 (Graphe = modèle des réseaux) définitions, concepts (liens forts et faibles), contexte des réseaux, relations positives et négatives
- Chapitre 13 (Structure du web)
- Chapitre 14 (Analyse des liens sur le web)
- Chapitre 18 (Lois de puissances)
- Chapitre 20 (Les phénomènes de petit monde)

8.2 Exemple et analyse de graphes

Voici quelques commentaires réalisés sur les figures du 1^{er} chapitre :
- **Figure 1.1** (ci-dessous : Figure 8.2 Illustration des relations amicales entre 34 personnes dans un club de karaté. Chaque nœud représente une personne et chaque lien, un lien d'amitié entre ces personnes. On constate que tout le monde n'est pas ami avec tout le monde. Grâce à cette structure, on peut déduire certaines choses, par exemple : deux personnes ont beaucoup de liens d'amitié avec d'autres personnes, mais pas entre eux.

- **Figure 1.2** Des employés dans un laboratoire de recherche (nœud) ont des liens entre eux : Lignes claires = communication e-mail. Lignes foncées = hiérarchie, organisation du laboratoire. On voit que la communication entre les gens suit relativement bien la structure



Graphique 8.1 – Relations amicales dans un club de karaté

hiérarchique, mais pas complètement. On peut voir comment les gens collaborent, leurs degrés de collaboration, etc.

— **Figure 1.3** On constate que dans cette illustration, il y a beaucoup plus de nœuds. Chaque nœud est une institution financière (banque par exemple). Chaque nœud a un chemin vers un autre nœud (il y a des liens entre toutes les banques). Le centre est très dense, ça montre une faiblesse du système financier : si une banque dans le centre fait faillite par exemple, toutes les autres banques liées à elle sont également mises en danger . Donc si le noyau central est trop grand, c'est une faiblesse. En regardant cette structure, on peut trouver les faiblesses et les comprendre. Ça peut être très important.

— **Figure 1.4** Un nœud représente un blog politique et un lien, une référence vers un autre blog. Nous avons deux partis qui représentent chacun un noyau : les démocrates et les républicains. On constate qu'il y a moins de connexions entre les deux noyaux qu'à l'intérieur de ceux-ci. On peut visualiser cette structure et se poser des questions : est-ce que ce monde bipolaire est un problème ?

Ce sont divers exemples que nous allons essayer d'analyser. Sur Internet, il y a beaucoup de nœuds avec de grandes capacités de calcul et de stockage. On peut maintenant regarder ces structures (pas avant).

8.3 Introduction

- Structure des réseaux (Facebook, Twitter, réseau économique,...).
- Comportement des participants (interactions : chaque nœud sera un participant et va interagir).En principe, chaque nœud ne voit que son voisinage et interagit en conséquence.
  - Interactions LOCALES avec conséquence GLOBALES. Il faut faire le lien entre ces deux choses.
  - Effets non attendus. Ex : réseaux routiers (nœud = automobilistes, lien = routes) :
    S'il y a des bouchons, on augmente la capacité du réseau (ajouter une voie par exemple) Le résultat peut être non intuitif, ça peut être :
    - Une réduction des transferts.
    - Une augmentation du trafic. (résultat opposé à celui attendu)
  - Le **Paradoxe de Braess** nous dit que l'ajout d'une nouvelle capacité à un réseau peut réduire la performance globale (effet non attendu). Il faut donc comprendre comment le réseau fonctionne au lieu de faire n'importe quoi et avoir des effets non attendus.

8.4 Nouvelle discipline

Les graphes et leurs propriétés évoluent avec le temps, ce n'est pas statique.
⇒Nouvelles disciplines pour analyser des graphes YouTube, Flicker, etc.
Synthèse de 3 disciplines :

1. La théorie des graphes => mathématique
2. La théorie des jeux => mathématique Exemple : YouTube impose ses règles et ceux qui utilisent YouTube sont des joueurs.
3. La sociologie (étude des groupes sociaux) : les participants sont humains ou guidés par un humain. Il n'est pas uniquement question de mathématiques, il faut aussi comprendre les humains.

Dans ce cours, nous nous concentrerons principalement sur la théorie des graphes. La théorie des jeux sera très intuitive, et nous parlerons un peu de la sociologie.

8.4.1 Théorie des jeux

On a un ensemble de participants qui jouent à "un jeu" (un ensemble de règles suivies par tous les participants). Chaque participant doit agir :

— Simple à spécifier (comme les échecs : 2 participants et 1 action en alternance).
— Compliqué : pas d'alternance, tout le monde agit en même temps. C'est un système concurrent.

Exemple d'action simple : la vente aux enchères : n participants, règles simples (différentes techniques)

On va rester intuitif sur ce sujet, mais si on veut être plus précis, il y a des mathématiques pour ça.

— **Figure 1.8** Réseau d'interaction économique entre pays. Structure de l'économie mondiale : Hong Kong a un gros avantage, il a une porte d'entrée vers la Chine (à l'époque). Certains pays sont des partenaires privilégie des États-Unis...
— **Figure 1.9** Chemins de commerces médiévaux en Europe. L'endroit comporte des avantages : la position dans le graphe. On a toute une série d'avantages qui viennent de la structure du réseau (le comportement d'un participant peut dépendre de la structure). Si on est malin et qu'on comprend le réseau dans lequel on est, on peut essayer de se mettre dans une structure ou on a plus de pouvoir.

Si on connaît la structure, une petite action peut suffire pour arrêter une épidémie.

Chapitre 9

Théorie des Graphes

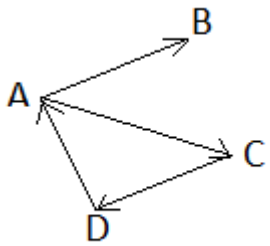
9.1 Définitions

Graphe G = ensemble de liens et de nœuds. Un lien est une paire de deux nœuds.

G = (N,E)
N = nœud
E = edge (lien, arête)

Deux types de graphes :

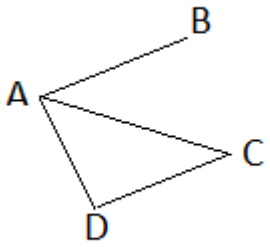
— **Les graphes orientés** (avec flèches et principe de direction). Une arête/lien est une paire de nœuds. L'ordre a de l'importance. Dans cet exemple, les paires de nœuds sont : (A,B), (A,C), (D,A) et (C,D).



Graphique 9.1 – Graphe orienté

— **Les graphes non orientés** (sans flèche, sans direction). Une arête est un ensemble de deux nœuds. On ne parle pas de "paire" vu que

l'ordre des nœuds n'a pas d'importance. Ici, parler de l'arête (A,B) ou (B,A) revient à la même chose.



Graphique 9.2 – Graphe non orienté

Dans le cours, on aura surtout affaire à des graphes non orientés.

9.2 Chemins et connectivité

Nous allons commencer par rappeler la notion de chemin :

Chaine : Dans un graphe non orienté, une chaîne reliant une somme x à un sommet y est une suite finie d'arêtes consécutives, reliant x à y

Chemin : c'est une séquence de nœuds dont chaque paire consécutive est relié par une arrête.

Chemin simple : c'est un chemin dont chaque nœud se trouve au maximum une fois dans la séquence de nœuds.

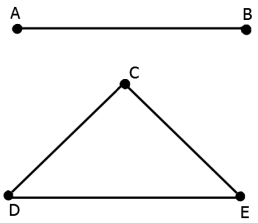
Cycle : c'est un chemin dont le premier et le dernier nœud sont les mêmes. Un cycle possède au moins 3 liens (arêtes).

Maintenant, nous allons définir la notion de connectivité d'un graphe.

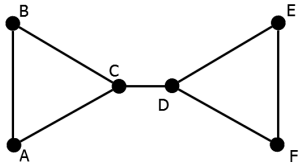
Connectivité : un graphe est dit connexe si pour toutes paires de nœuds A et B, il existe au moins un chemin de A vers B.

Tous les graphes ne sont en effet pas connexes. La figure 9.3 montre un exemple de graphe non connexe. Ce graphe possède deux composants, AB et CDE. Ces composants (qui sont maximaux) sont les parties connexes du graphe. On a les définitions suivantes :

Composant d'un graphe : c'est un sous-graphe (partie de graphe) qui est connexe. Il est maximal s'il ne fait pas partie d'un composant plus grand.



Graphique 9.3 – Graphe non connexe



Graphique 9.4 – Graphe connexe

Composant géant : il s'agit d'un composant qui contient une fraction significative de l'ensemble des nœuds contenus dans le graphe.

Par exemple, le graphe des amitiés mondiales n'est sûrement pas connexe. En effet, il peut y avoir des habitants d'une île reculée qui se connaissent entre eux, mais qui n'ont pas de connexion avec le reste du monde. Cependant, la majorité du monde est connectée ; on a donc un énorme composant géant.

C'est une propriété générale des grands graphes complexes : il est rare qu'ils soient connexes, mais ils ont très souvent un composant géant. Avoir plusieurs composants géants est instable : il arrive vite qu'un lien se forme entre les deux composants, formant ainsi un seul composant géant. Si avant le XV$^{\text{ème}}$ siècle, il y avait un composant géant eurasien et un autre Américain, il n'a fallu qu'un lien (la découverte de l'Amérique par Christophe Colomb) pour assembler les deux composants, avec toutes les conséquences que cela a entraîné (maladies, exploitation, etc.).

Avec les éléments que nous venons de définir, on est en mesure d'analyser tout un graphe. On peut le partitionner en composants et regarder la structure interne de chacun d'entre eux. Par exemple, dans la figure 9.4, on peut partitionner en deux composantes, ABC et DEF. On constate que le lien CD est un lien spécial, car si on l'enlève, il déconnecte de graphe.

9.3 Distance entre nœuds

Nous allons maintenant définir la longueur d'un chemin ainsi que la distance entre deux nœuds :

Longueur d'un chemin : le nombre d'arêtes consécutives sur ce chemin.

Distance entre 2 nœuds : le chemin le plus court entre ces deux nœuds.

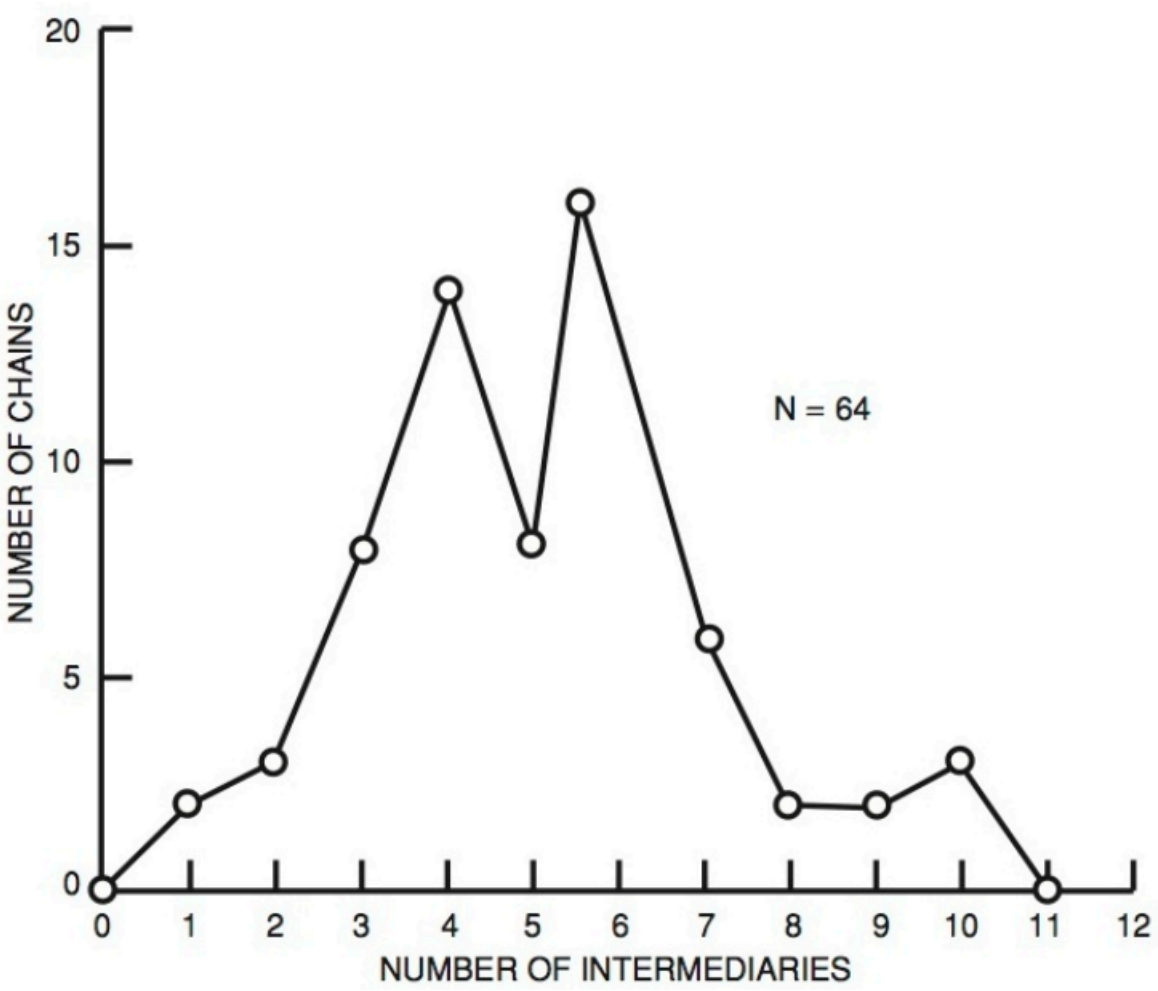
La méthode de calcul de distance entre deux nœuds est la traversée en largeur d'abord (*breadth-first traversal*). Cela consiste à débuter par un nœud, puis à regarder tous les nœuds qui sont à une distance de 1 du nœud de départ. À partir de tous ceux-là, on regarde les nœuds qui sont à une distance 1, et donc à une distance 2 du nœud de départ. On continue jusqu'à arriver au nœud d'arrivée. On a donc, à chaque étape, constitué des couches de nœuds se trouvant à une certaine distance. Cet algorithme sera expliqué plus en détail par après.

9.4 Phénomène du petit monde

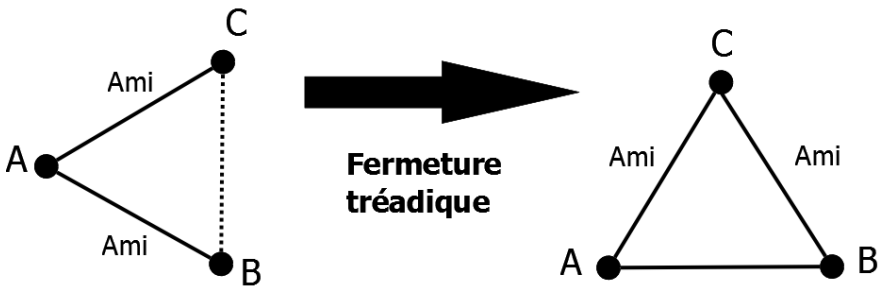
Le « phénomène du petit monde », aussi connu sous le vocable « paradoxe de Milgram » (du nom du psychosociologue *Stanley Milgram*), est l'hypothèse que chacun puisse être relié à n'importe quel autre individu par une courte chaîne de relations sociales. La figure 9.5 montre la probabilité qu'ont deux personnes d'être reliés par x intermédiaires. Cette courte chaîne de relations sociales a été approfondie par la théorie des « six degrés de séparation » affirmant qu'en prenant deux personnes, il est possible de trouver une chaîne d'amis entre eux de taille maximum 6. Différents types de distances entre des personnes existent, comme :

- Le nombre d'Erdos est la distance de collaboration avec le célèbre mathématicien *Paul Erdös* qui a réalisé de très nombreuses co-publications. Avoir réalisé une publication en collaboration avec Erdös correspond au nombre d'Erdös 1. Avoir écrit une publication avec quelqu'un qui a co publié avec Erdös équivaut au nombre 2, etc.
- Le nombre de Bacon est la distance de collaboration dans un film avec l'acteur *Kevin Bacon*.

Ce phénomène de petit monde est particulièrement vrai pour les réseaux créés dynamiquement. Nous expliquerons plus en détail pourquoi cette affirmation est vraie dans la suite du cours.



Graphique 9.5 – Statistiques du phénomène du petit monde



Graphique 9.6 – Exemple de fermeture triadique

9.5 Liens forts et faibles

Un réseau peut évoluer de différentes manières et selon différents mécanismes. Considérons un exemple où chaque nœud correspond à une personne et les arcs correspondent à un lien d'amitié (figure 9.6). Dans cet exemple, on voit que A est ami à la fois avec B et avec C. Dans cette condition, il est fort probable que B et C deviennent eux-mêmes amis. C'est ce qu'on appelle la fermeture triadique.

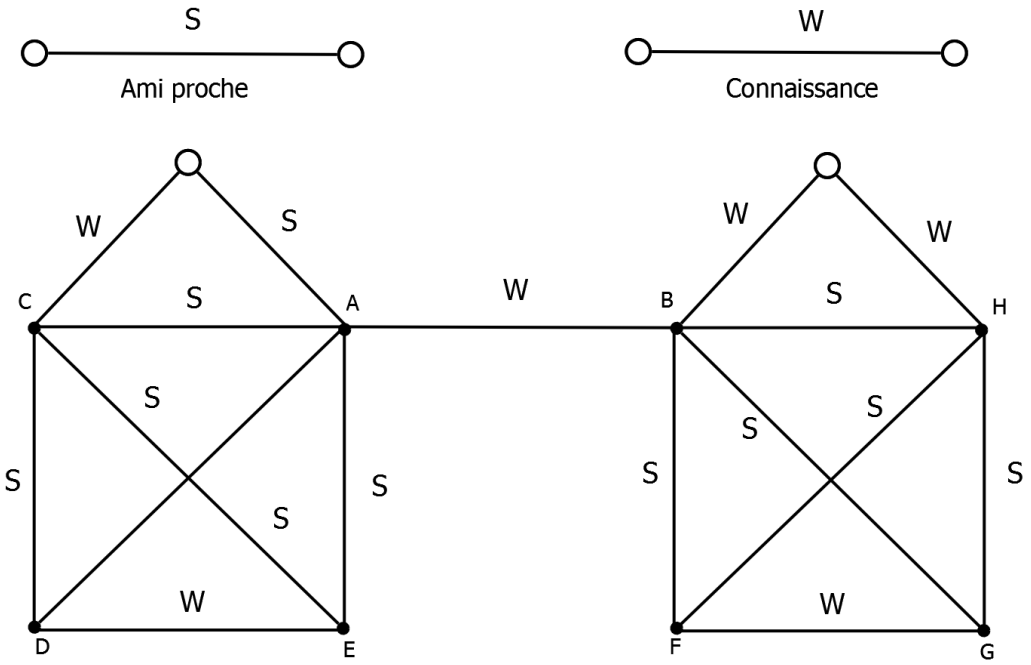
Cette situation nous amène à nous intéresser à la notion de coefficient de regroupement qui reflète la probabilité qu'un arc se crée entre deux nœuds dans un graphe dynamique. Dans l'exemple ci-dessus, cela correspondrait au fait que C et B deviennent amis. On peut démontrer qu'au plus on fait de fermetures triadiques, au plus le coefficient de regroupement est élevé.

Exemple

Une étude a été faite dans les années 1960, par le sociologue américain *Mark Granovetter*, dans laquelle il s'est intéressé aux personnes qui changent de travail et plus particulièrement à la manière dont ils trouvent un nouveau travail. Il a remarqué que les personnes trouvent du travail plutôt via des connaissances que via des amis. Cela s'explique par la structure des graphes des amis et nous amène à définir les notions de **liens forts** et de **liens faibles** (figure 9.7). La suite de cet exemple sera expliquée plus tard.

9.6 Ponts

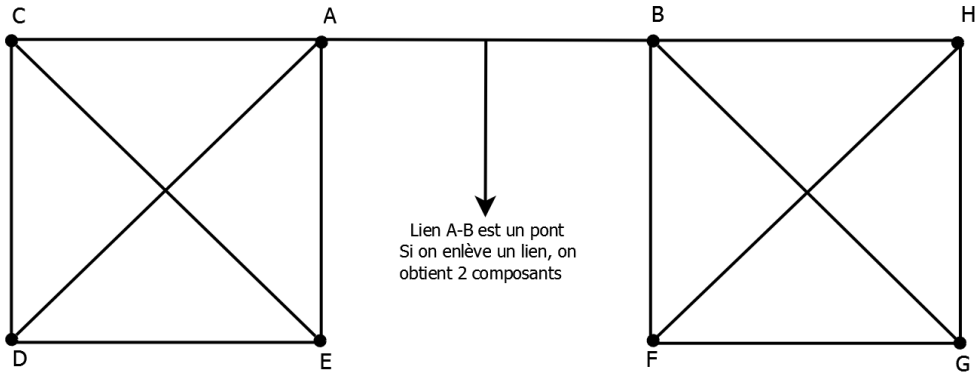
Pour expliquer l'exemple précédent, nous avons besoin de la notion de pont (figures 9.8 et 9.9).



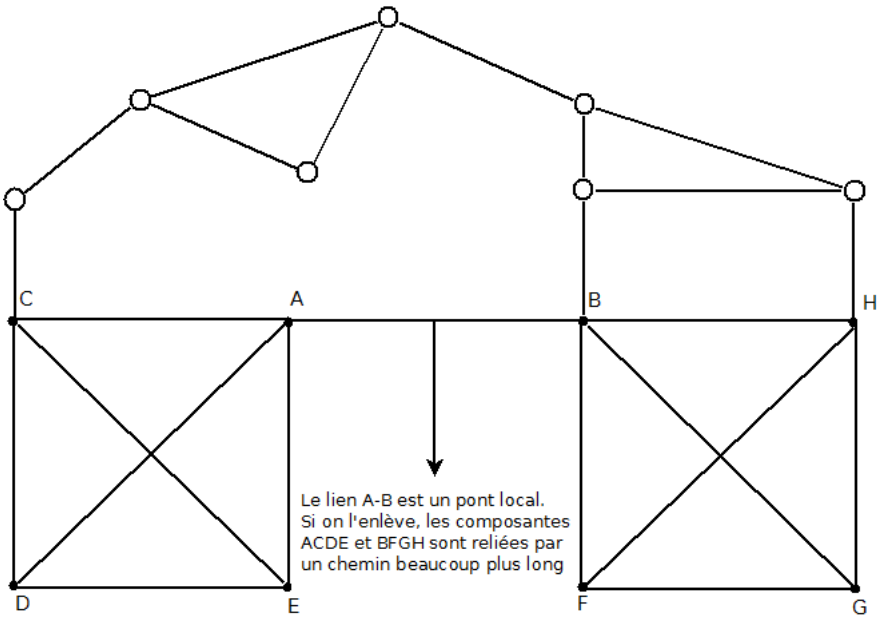
Graphique 9.7 – Liens forts et faibles

Pont Un lien entre A et B est un pont si l'enlèvement de ce lien aboutit à la séparation du graphe en deux composants disjoints.

Pont local Un lien entre A et B est un pont local si l'enlèvement de ce lien aboutit au fait que deux composantes sont reliées par un chemin significativement plus long.



Graphique 9.8 – Pont



Graphique 9.9 – Pont local

Reprenons l'exemple de la section 31.4, si l'on s'intéresse à la personne A, on sait que s' il cherche du travail c'est fort probable que ce soit via B qu'il en trouve (B est une connaissance de A).Socialement, on sait que si deux amis ont un ami en commun, il y a des chances qu'ils deviennent ami aussi ou tout du moins connaissance (propriété de fermeture triadique forte).On peut donc en déduire que chaque pont local tel que celui entre A et B dans la figure 8 sera un lien faible (conséquence de la propriété de fermeture triadique forte).En effet si le lien entre A et B était fort, la propriété de fermeture triadique forte nous dirait que d'autres liens se formeraient. Par exemple, entre E et B et entre A et F ce qui aurait pour conséquence que le lien A-B ne serait plus un pont.B fourni donc de nouvelles informations à A via le pont local.

9.7 Force d'un lien dans un grand réseau

Pour caractériser la force d'un lien dans un grand réseau, il va falloir généraliser les concepts relatifs aux liens forts et faibles vus précédemment. La force d'un lien sera caractérisée en y attribuant une quantité numérique, on va utiliser la notion de chevauchement de voisinage (neighbourhood overlapping) pour ça. Chevauchement de voisinage = (Nombre de noeuds voisins de A et B)/(Nombre de noeuds voisins de A ou B) La quantité numérique augmentera en fonction de ce chevauchement. Plus cette valeur de chevauchement de voisinage tendra vers 0, plus ce lien deviendra un pont local.

9.8 Force des liens en pratique dans un réseau téléphonique

Une étude portée sur les conversations cellulaires nous prouve que plus les liens entre des individus sont fort, plus ces personnes passeront du temps au téléphone à communiquer. Effectivement, on remarque que la durée augmente au fur et à mesure que le chevauchement de voisinage augmente.

9.9 Force des liens en pratique sur Facebook

Facebook est un réseau social développé sur internet permettant à des individus de communiquer avec des personnes de leur entourage. Les liens

entre individus sur Facebook sont nommés les liens d'amitié. Facebook est ainsi notamment un bon exemple où la force des liens est utilisée au maximum. D'après une étude réalisée sur une période d'un mois, on trouve trois catégories de liens sur Facebook, caractérisant soit : - une communication réciproque ; - une communication orientée ; - une relation maintenue.

On peut faire une comparaison avec la force d'un lien, le nombre de personnes ayant un lien d'amitié avec quelqu'un augmente en fonction de la taille du voisinage. On remarque également que la propagation d'informations est plus rapide avec la 3e catégorie de lien.

9.10 Twitter

Twitter est un microblog qui permet de partager de petits messages (140 caractères au maximum). Il est basé sur une relation de Followers à Followees. Force du lien : - Faible si on est follower - Forte si on envoie un message ciblé Si on "suit" plus de personnes, on a plus d'amis (jusqu'à un certain point, c'est une fonction logarithmique). Effectivement, cela s'explique par le fait que pour entretenir des liens forts, ceci demande un effort conditionnel. Il y a une limite physique aux nombres de liens forts que l'on peut posséder. A contrario, il ne demande pas de temps ou d'effort pour 'suivre' quelqu'un. Il y a moins de contraintes, c'est un engagement passif et c'est ce qui est prôné sur Twitter.

9.11 Notion de trou structurel et capital social

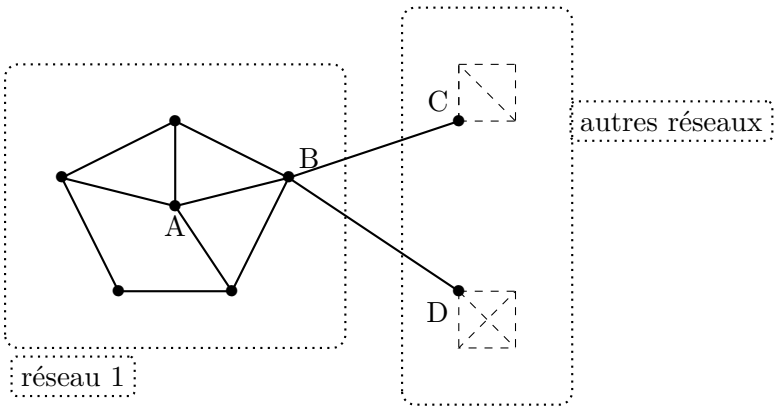
Comme nous l'avons vu précédemment, il existe deux types différents de liens. Les liens faibles et les liens forts, ces derniers étant beaucoup moins nombreux que les faibles.

Or lorsque l'on regarde un réseau, les noeuds ont aussi une grande importance. En fonction de la structure ou de l'organisation du graphe, certains noeuds posséderont quelques avantages et inconvénients. Par la suite, nous allons montrer que cette propriété propre aux noeuds est de posséder un "pouvoir".

9.11.1 L'enchâssement d'un lien (embaddness)

Attardons-nous tout d'abord à l'enchâssement d'un lien, c'est-à-dire le nombre de voisins commun entre les deux noeuds de ce lien. Par ailleurs, on peut observer que ce nombre est équivalent au dénominateur du chevauchement. On peut dire qu'un lien est plus fortement incrusté dans le réseau si les 2 noeuds du lien possèdent un grand nombre de voisins.

Considérons le graphe 9.10 à la page 100. On peut remarquer que le noeud **A** admet quelques fermetures triadiques parmi ses voisins tandis que le noeud **B** permet au **réseau 1** de rejoindre les deux autres.



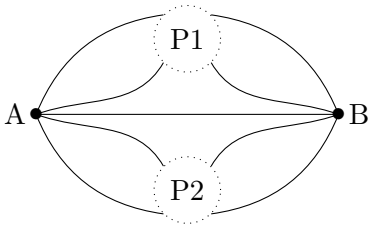
Graphique 9.10 – Un réseau central lié à deux autres sous-réseaux

On peut aussi apercevoir que le noeud **A** est localisé là où le coefficient de regroupement [1] est assez élevé contrairement à **B** qui est dans une zone à faible densité . On dit que les liens de **A** sont 'incrustés', ils ont un enchâssement significatif.

Deux individus connectés par un lien possédant un grand enchâssement

1. Un exemple de ce concept peut être trouvé en annexe.

auront une plus grande confiance mutuelle. En plus de la simple force du lien, c'est également la structure du réseau qui va augmenter la confiance entre deux noeuds. Il y aura une observation mutuelle. Une représentation de ce concept est donnée dans le graphe 9.11. Dans cette figure, une observation mutuelle entre **A** et **B** est de mise.



Graphique 9.11 – Deux noeuds possédant un enchâssement significatif

En effet, imaginons que le noeud **A** effectue une action quelconque, tous les autres noeuds (par exemple, ceux de *P1* et *P2*) peuvent voir cette action. Ainsi, deux noeuds possédant un enchâssement suffisamment conséquent ont une certaine confiance mutuelle.

On peut donc en tirer la propriété suivante provenant directement de la structure du graphe :

Plus l'enchâssement augmente, plus la confiance mutuelle est grande.

Revenons maintenant au graphique 9.10. Bien que le lien **A** possède un grand enchâssement, il n'en est pas de même pour **B** avec **C** et **D**. En effet, ils ne peuvent pas avoir une confiance mutuelle, car les autres noeuds de leur réseau respectif ne peuvent plus les "observer".

Bien que d'un certain point de vue, **A** pourrait posséder plus d'avantages que **B** grâce à ses fermetures et son voisinage, ce n'est pas tout à fait exact. Le noeud **B** possède lui aussi des avantages aussi fondamentaux que **A**.

— **B** est au bord d'un pont local. Il joue le rôle d'intermédiaire entre plusieurs réseaux.
— **B** s'étend sur un trou structurel, il remplit le vide entre plusieurs ensembles de noeuds.
— **B** est le seul lien pour communiquer avec certains ensembles. Tous les chemins entre ces deux communautés passent par **B**. Il est donc incontournable.
— Il a des informations dispersées auxquelles les autres n'ont pas accès. Il va donc pouvoir amplifier sa créativité en observant les informations

ou en en faisant passer certaines pour siennes.
— Il joue le rôle de gardiennage social, il peut réguler l'accès de l'extérieur.

Par ailleurs, ces quelques derniers avantages peuvent engendrer un conflit d'intérêts entre **B** et ses sous-ensembles. Par exemple, dans le cas où **B** voudrait laisser deux réseaux scindés alors que ceux-ci désireraient s'assembler.

⇒ On fait donc appel à des notions de *pouvoir* ou d'*avantage*.

Ces notions sont aussi appelées *capital social* ou capacité à se procurer des avantages grâce à l'appartenance à une structure sociale.

9.11.2 Notion de capital social

Le capital social est la capacité à se procurer des avantages grâce à l'appartenance à une structure sociale. C'est une forme de capital, car elle représente une capacité que l'on possède et que l'on peut utiliser. Il existe d'autres notions de capitaux :

— Capital physique (exemple : technologie)
— Capital humain (exemple : expertise des personnes)
— Capital économique (exemple : monétaire)
— Capital culturel (exemple : les ressources accumulées dans une culture, les connaissances communes)

9.12 Similitude des noeuds

Après nous être intéressés aux liens entre les noeuds, nous allons nous concentrer sur les similitudes entre ces noeuds.

9.12.1 Principe de similitude

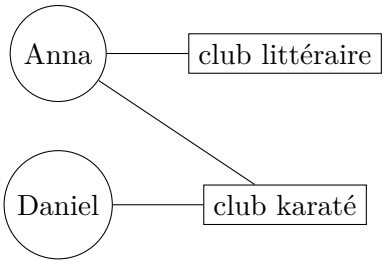
(Notion sociologique) On augmente le nombre de liens entre les noeuds. Exemple : Les étudiants de l'UCL présentent une similitude par le fait qu'ils font partie de la même université.

Ce principe implique de nouveaux mécanismes dans la manière où nous allons représenter les graphes :

Sélection	$\longrightarrow$	`local:` Chacun choisi ses amis
Influence sociale	$\longrightarrow$	`global/extérieur:` induite par les gens que l'on fréquente.

Exemple de cette dernière propriété :
Le fait d'être dans le même auditoire qu'un autre individu peut-être représenté.

Bien que la sociologie est un concept difficile à formaliser. Une idée pourrait être d'inclure les facteurs de similitudes dans le graphe.



Graphique 9.12 – Exemple d'un graphe personnes-intérêts

Les graphes sont maintenant constitués à partir de deux types de noeuds :
— noeud Individu : représente une personne physique.
— noeud Activité ou point d'intérêt.

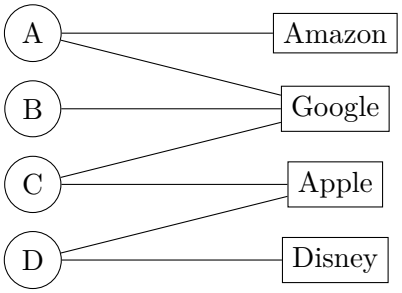
Mais aussi de deux types de liens :
— liens Personnes - Personnes
— liens Personnes - Focus
Ces graphes aussi appelés réseau d'affiliations ont une caractéristique bien particulière, ils sont toujours bipartis.

Définition *graphe biparti* : Soit un graphe G=G(V,E) et V_1, V_2 deux ensembles de noeuds et $V_1 \cup V_2 = V$, un graphe est dit biparti s'il n'existe pas d'arête interne dans ces deux sous-ensembles. $\forall e = (u, v) \in E, u \in V_1$ et $v \in V_2$.

Comme on peut le voir ci-dessous (graphe 9.13), il peut y avoir un conflit d'intérêts, par exemple entre Google et Apple.

Par ailleurs, ces graphes bipartis ne sont pas statiques. En effet, ils peuvent subir des évolutions dans le temps comme des ajouts de noeuds, points d'intérêts, nouveaux liens ...

Ainsi, ces graphes nous fournissent plus de précisions que les précédents. Grâce à ce concept, on peut voir plus efficacement les changements et trans-

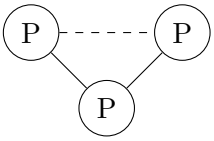


Graphique 9.13 – Exemple d'un graphe représentant un conseil d'administration

formations lors d'évolutions.

9.12.2 Nouveaux mécanismes de fermeture

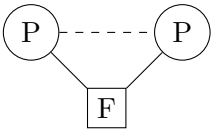
Nous avons déjà vu précédemment le principe de fermeture triadique.



Graphique 9.14 – Rappel de fermeture triadique

Grâce à la prise en compte des points d'intérêts (focus), deux nouveaux principes de fermeture peuvent être considérés :

Fermeture focale

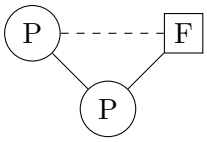


Graphique 9.15 – Exemple de fermeture focale

Comme on peut le voir sur le graphique 9.15, deux personnes ayant des similitudes ou mêmes centres d'intérêts, peuvent devenir amis.

Fermeture d'adhésion

De la même manière, une personne ayant une activité peut convertir son ami.

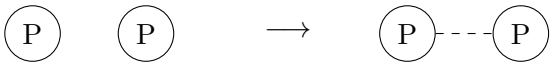


Graphique 9.16 – Exemple de fermeture d'adhésion

Ces deux nouveaux mécanismes de fermeture permettent de raisonner beaucoup plus fort sur ces graphes. Ils sont même essentiels ! Si on ne les prenait pas en compte, on ne pourrait jamais comprendre pourquoi un lien apparaît spontanément.

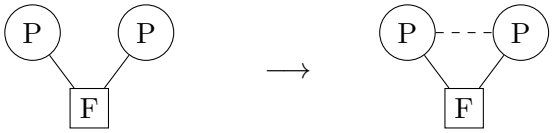
Ci-dessous, un exemple illustrant cette propriété :

Sans les concepts introduits dans cette partie, voici ce que l'on observerait :



Graphique 9.17 – Apparition spontanée d'un lien

Heureusement avec la propriété de fermeture focale, on peut raisonner sur la raison de cette apparition.



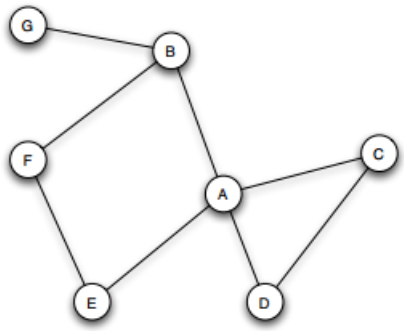
Graphique 9.18 – Apparition du lien dû au focus en commun

Coefficient de regroupement

Le coefficient de regroupement ou en anglais, *The Clustering Coefficient*, représente la probabilité pour un noeud **A** que deux amis de celui-ci choisi aléatoirement, soit amis entre eux.

$$\text{Clustering coefficient} = \frac{\text{\# d'arêtes existantes reliant les amis de } \mathbf{A}}{\text{\# total d'arêtes possible reliant les amis de } \mathbf{A}}$$

Un exemple de ce concept est donné pour la figure suivante.

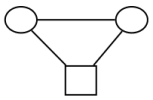


Graphique 9.19 – Graphe simple

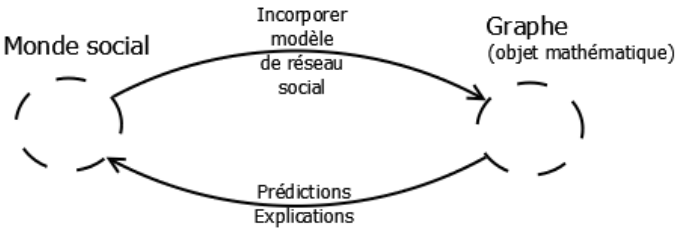
Considérons la figure 9.19. Le coefficient de regroupement pour le noeud **A** est , $\frac{1}{6}$ car il n'y a qu'une seule arête **C-D** parmi les six autres paires (**B-C**, **B-D**, **B-E**, **C-D**, **C-E**, et **D-E**) reliées entre elles.

9.12.3 Réseaux dans leurs contextes

— réseau social : similitude entre amis (on voudrait mettre ces similitudes dans le réseau)

— réseau d'affiliation - social  <- explication d'une similitude
- personnes
- points d'intérêts

Idée générale



9.12.4 Exemples

Il y a trois formes de fermeture

1. Fermeture triadique 
2. Fermeture focale 
3. Fermeture d'adhésion 

9.13 La formation des liens (selon les 3 approches)

— On a des données réelles -> réseaux sociaux
On a plus facilement un accès direct au graphes qu'avant.
— mesurer empiriquement le taux de création des liens en fonction du nombres d'amis communs.

9.13.1 Algorithme

1. Capture à deux instants différents le réseau (appelons ces deux graphes (1) et (2))
2. Pour chaque entier "k" plus grand ou égal à 0 :
   — On identifie les paires de noeuds qui ont "k" amis en communs dans (1)

3. On regarde dans (2) si pour chaque paire un lien s'est formé

=> On calcule T(k) = fraction des paires qui ont formé un lien

9.13.2 Modèle pour expliquer ce résultat (fermeture triadique)

Si on prend deux personnes : s'il y a 1 ami en commun, il y a une probabilité "p" qu'un lien se forme.
Quelle est la probabilité pour "k" amis en commun ?
=> On calcule la probabilité de "aucun lien se forme".

La probabilité qu'aucun lien se forme quand il y a un ami en commun est de $(1-p)$.
On en déduit que pour "k" amis en commun, la probabilité est de $(1-p)^k$
Dès lors, la probabilité qu'au moins 1 lien se forme pour k amis en commun est de $1-(1-p)^k$. C'est ce qui est égal à T(k).

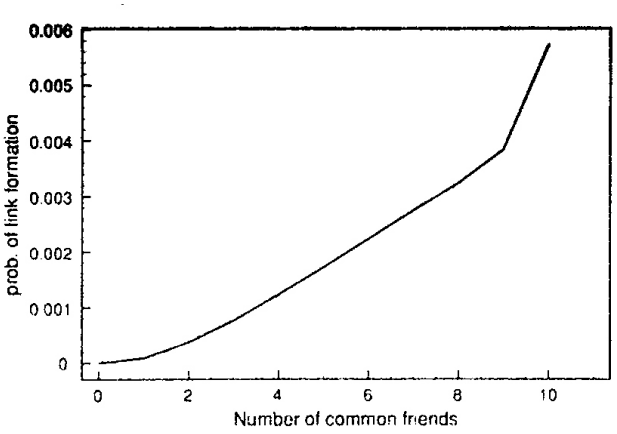


Figure 4.9. Quantifying the effects of triadic closure in an e-mail data set [259]. The curve determined from the data is shown in the solid black line; the dotted curves show a comparison to probabilities computed according to two simple baseline models in which common friends provide independent probabilities of link formation. (Image from the American Association for the Advancement of Science.)

On voit sur la figure 4.9 (fermeture triadique) que la probabilité qu'un lien se forme augmente exponentiellement avec le nombre d'amis en commun.

Attention ! Le comportement et donc les calculs sont différents pour la fermeture focale et d'adhésion !

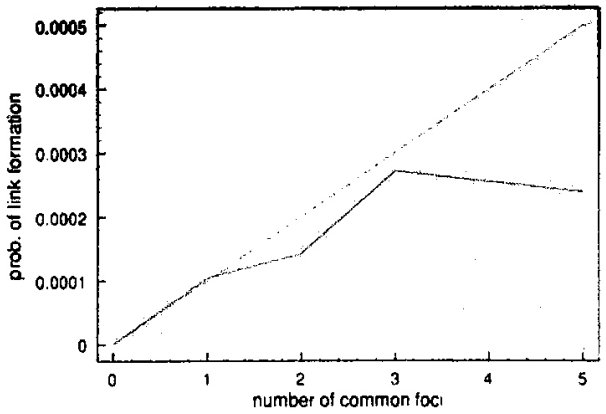
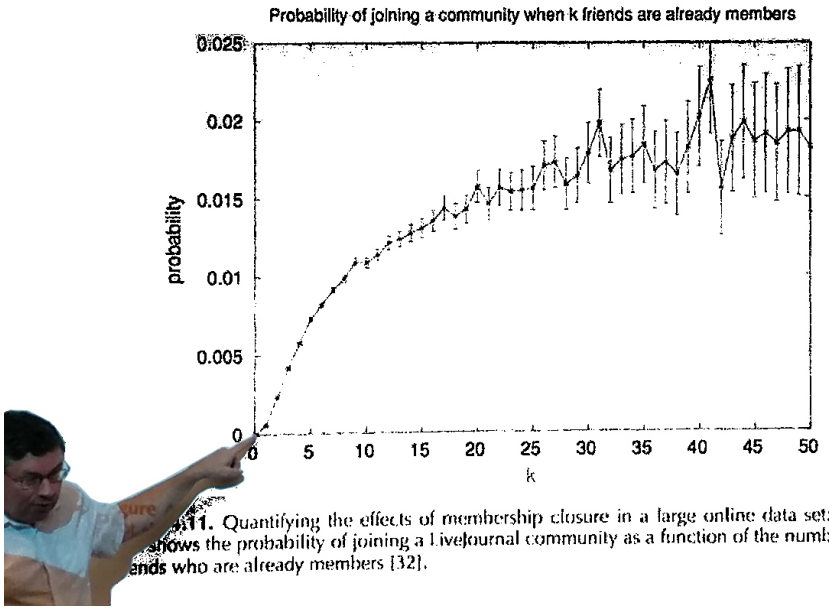


Figure 4.10. Quantifying the effects of focal closure in an e-mail data set [259]. Again, the curve determined from the data is shown as the solid black line, while the dotted curve provides a comparison to a simple baseline. (Image from the American Association for the Advancement of Science.)

La figure 4.10 (fermeture focale) nous montre que dans le cas où l'on considère le nombre d'intérêts en commun (ici, des cours), on arrive à un certains moment à saturation. Augmenter le nombre de points d'intérêts communs n'augmente plus la probabilité de création d'un lien à partir d'un certain point (ici 3 cours en communs).



11. Quantifying the effects of membership closure in a large online data set: The shows the probability of joining a LiveJournal community as a function of the number of nds who are already members [32].

Enfin, la figure 4.11 (fermeture d'adhésion) présente aussi un saturation à partir d'un certains nombre d'amis qui ont le même point d'intérêt.

9.14 Quantifier les rôles relatifs de sélection d'influence sociale

Les mécanismes de similitude :
— La sélection (intérieur, c'est nous qui faisons le choix)
— L'influence sociale (extérieur, c'est les autres qui nous influencent)

9.14.1 Comment quantifier cela ?

Par exemple wikipédia Il peut exister une similitude de comportement entre rédacteurs. Par exemple les articles sur lesquels ils travaillent.
Raisonnement :
— On a des rédacteurs
— Un lien entre deux rédacteurs : ils communiquent par la "Talk page" (chaque article a une "Talk page"). Autrement dit, si un rédacteur B communique sur la page de A, alors il y a un lien.
— Les "points d'intérêts" ici sont les articles.
— Quantification de la similitude $= \frac{\text{nombre d'articles rédigés par A ET B}}{\text{nombre d'articles rédigés par A OU B}}$
Notons dès lors que la similitude ne peut pas être plus petit que 0 ni plus grand que 1. $0 \leq sim \leq 1$
— La rupture se fait quand le lien est créé.
— On compare la similitude avant et après cette rupture (figure 4.13). C'est surtout la sélection qui joue avant, et l'influence sociale rentre en jeu après.

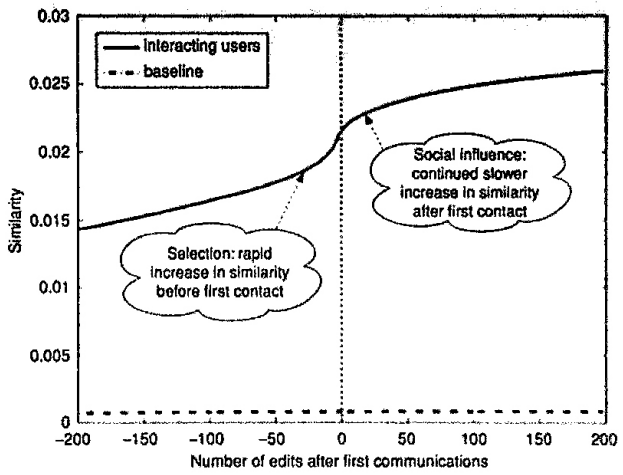
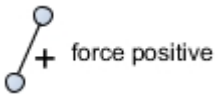


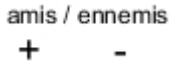
Figure 4.13. The average similarity of two editors on Wikipedia, relative to the time (0) at which they first communicated [122]. Time, on the x-axis, is measured in discrete units, where each unit corresponds to a single Wikipedia action taken by either of the two editors. The curve increases both before and after the first contact at time 0, indicating that both selection and social influence play a role; the increase in similarity is steepest just before time 0.

9.15 Les relations positives et négatives

Précédemment, les relations étudiées étaient considérées comme uniquement positives (on ne peut se faire que des amis).



Dans ce chapitre, nous allons étudier les graphes comportant également des relations positives et des relations négatives (on peut se faire des amis et des ennemis).

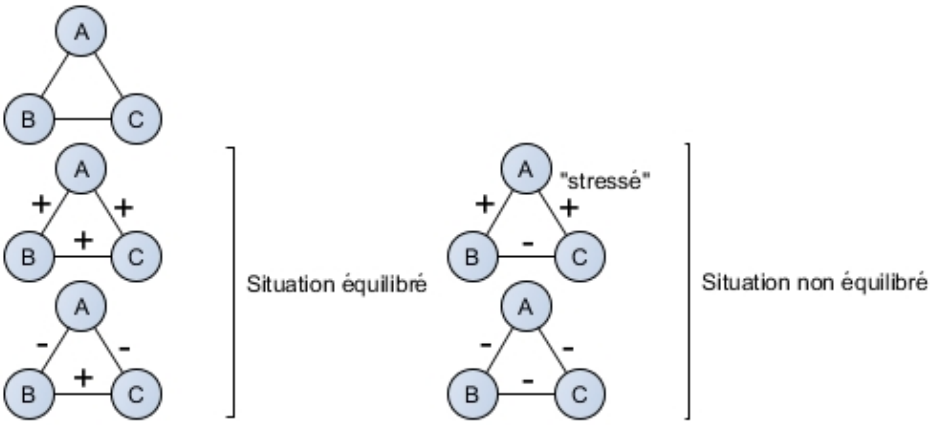


9.15.1 Théorie de l'équilibre de structure (Equilibre structurel fort)

L'équilibre dans une structure va nous permettre d'identifier les situations stables et celles qui sont instables. Cette étude se fera dans un graphe complet (un graphe dont chaque paire a un lien et dont chaque lien peut être de type "+" ou "-").

L'idée cruciale est d'identifier dans le graphe les situations équilibrées et les situations qui ne le sont pas et qui engendrent un stress entre les nœuds.

Graphique 9.20 – Relations équilibrées et non équilibrées

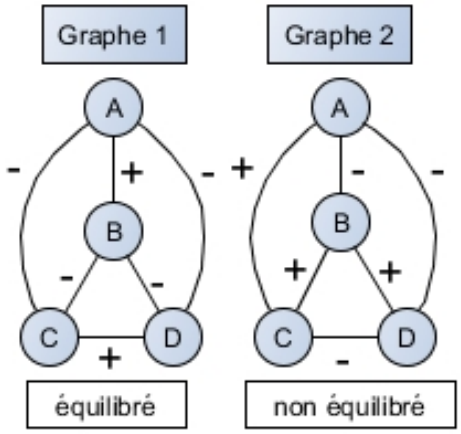


Dans la figure 9.15.1, les schémas de gauche sont considérés comme équilibrés. En effet, soit A, B et C sont tous amis et il n'y aucun conflit entre eux, soit B et C sont amis, mais sont en confit avec A.

Par contre, les schémas de droite sont des situations non équilibrées. Dans la 3, B et C sont amis avec A mais ennemis entre eux, on peut supposer que A doive alors choisir un camp. La 4 indique que tous sont ennemis, mais il est fort probable que le graphe évolue vers une situation où deux nœuds se liguent contre le troisième.

On peut maintenant généraliser cela pour un nombre quelconque de nœuds. Ainsi un graphe complet sera équilibré si chaque ensemble de 3 nœuds est équilibré et donc possède des liens de type $+++$ ou $+--$.

Graphique 9.21 – Généralisation des relations équilibrées et non équilibrées



Si un graphe n'est pas équilibré, il a tendance à s'équilibrer.

9.15.2 Caractérisation de l'équilibre structurel

Dans le point précédent, nous avons réalisé une définition avec des conditions locales, mais il est difficile de comprendre ce que cela fait pour tout le graphe. Ainsi nous voudrions une définition globale (une caractérisation) sur l'ensemble du graphe.

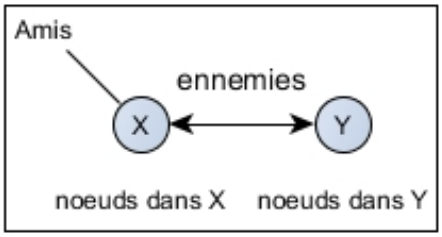
Preuve :

Pour prouver qu'un graphe est bien équilibré, il faut pouvoir démontrer dans les deux sens :

1. $\Rightarrow$ la structure est équilibrée $\rightarrow$ direction facile à déterminer
2. $\Leftarrow$ équilibrée est la structure $\rightarrow$ direction plus complexe à déterminer

9.15.3 Théorème d'équilibre : [Frank Harary 1953]

Graphique 9.22 – 2 groupes d'amis qui sont ennemis entre eux.



Si un graphe complet est équilibré, alors :

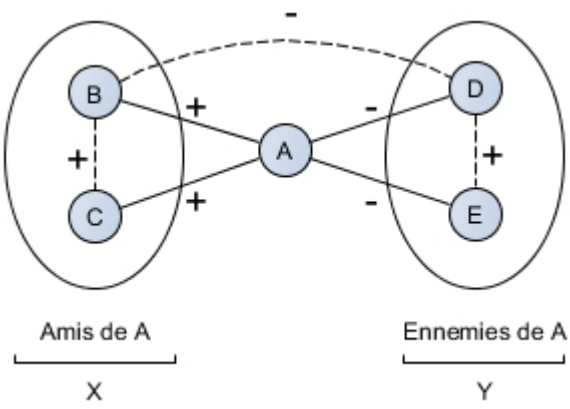
1. toutes les paires sont amies
2. on peut diviser les nœuds en deux groupes X et Y, tel que X et Y chacun contient des amis mutuels et chaque membre de X est ennemi de chaque membre de Y comme représenté à la figure : 9.15.3.

Preuve :

- graphe complet, annoté $+, -$
- graphe équilibré
  1. si aucun lien négatif : (1)
  2. sinon il existe un lien négatif
- prenons un nœud A quelconque
- Définissons :
  1. $X = A+$ tous ses amis
  2. $Y =$ les ennemis de A
- Est-ce que X et Y satisfont la condition du théorème ?

A démontrer :

1. chaque paire dans X = amis
2. chaque paire dans Y = amis
3. chaque nœud de X est ennemi de chaque nœud de Y

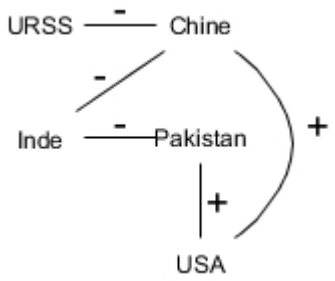


Exemple 1

On peut retrouver ce type de comportement de graphe dans les relations internationales : lors de la séparation du Bangladesh au Pakistan en 1972, on a assisté à un surprenant soutien des États-Unis pour le Pakistan alors que celui-ci n'était pas un allié des Américains.

Explication Comme indiqué dans la figure 9.15.3, les USA désiraient se rapprocher de la Chine, pour y arriver, ils ont analysé les relations des différents pays de la région. Ils ont ainsi constaté que la Chine avait des ennemis communs avec le Pakistan. Un rapprochement avec le Pakistan lui permettait de rentrer dans le groupe des amis de la Chine.

Graphique 9.23 – Relation lors de l'indépendance du Bangladesh



Une autre approche de ce conflit peut être réalisée d'un point de vue de la Chine :

— Vietnam du Nord $\overset{+}{\longleftrightarrow}$ Inde
— Pakistan $\overset{-}{\longleftrightarrow}$ pays du bloc EST
— Chine : vote l'abolition du Bangladesh à l'ONU

Exemple 2

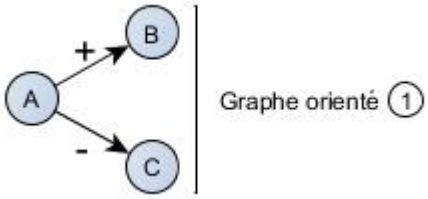
Un autre exemple de ce jeu diplomatique est donné à la figure 55 du livre de référence et représente le jeu des alliances des grandes puissances européennes à la veille de la Première Guerre mondiale.

On assiste à un équilibrage du graphe des relations avec des pays qui changent continuellement d'alliés jusqu'au moment de la triple entente et de la triple alliance qui sépara tous les pays d'Europe en deux camps ennemis.

Exemple 3

Dans ce troisième exemple, on touche directement les réseaux sociaux tel que Facebook et Twitter où il existe des relations *Like ou Trust* et *Dislike ou Distrust* dont les utilisateurs peuvent se servir pour juger le contenu des autres.

Le classement de produits y est libre : un utilisateur est libre d'avoir des opinions positives (+) ou négatives (-) sur les autres



Transitivité

Il est intéressant de savoir si les relations sont transitives ou non, autrement dit si A croit en B et que B croit en C, A croira-t-il en C ?

$$A \overset{trust}{\longrightarrow} B \overset{trust}{\longrightarrow} C \overset{?}{\longrightarrow} A \overset{trust}{\longrightarrow} C$$

Ou alors, si A n'a pas confiance en B et que B n'a pas confiance en C, est-ce que A aura alors confiance en C ou non ?

$$A \overset{distrust}{\longrightarrow} B \overset{distrust}{\longrightarrow} C \overset{?}{\longrightarrow} A \overset{trust}{\longrightarrow} C$$
$$A \overset{distrust}{\longrightarrow} C$$

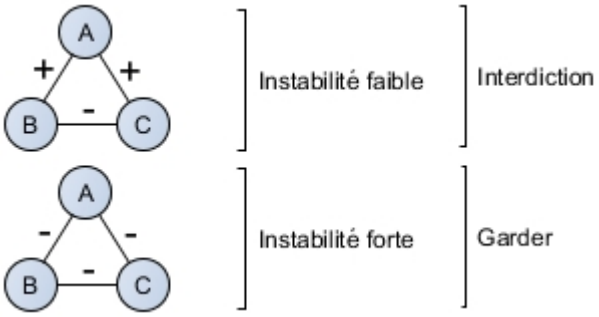
Finalement, tout est possible selon le cas rencontré :

— Si le trust signifie une relation d'amitié, la transitivité sera respectée.
— Si le trust indique une confiance sur l'opinion, la transitivité ne peut être respectée.
— Si par contre trust en une proximité dans les opinions politiques, un rapprochement de A et C est probable.

Conclusion : La théorie de l'équilibre structurel sera gérée selon le cas

9.15.4 Équilibre structurel faible

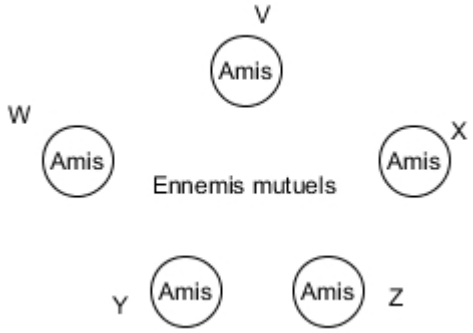
L'équilibre structurel faible, à l'instar de l'équilibre structurel fort, se base sur la notion de stabilité des triangles du graphe. Mais contrairement à l'équilibre fort, on ajoute deux cas instables



Un graphe complet annoté est faiblement équilibré si :
— aucun triplet n'est $++-$;
— tous les triplets sont de type $+++, +--, ---$.

L'équilibre faible permet une structure **multipolaire**.

Graphique 9.24 – Structure multipolaire



Théorème d'équilibre pour l'équilibre faible

Si graphe complet annoté est faiblement équilibré, alors on peut diviser ses nœuds en groupes :

— dans un groupe : amis
— autre groupe : ennemis

Preuve : *(analogue à la preuve sur l'équilibre structurel)*

1. Nœud A + tous ses amis appartiennent au groupe X
   → amis mutuels, car $(+ + +)$.
2. A + ses amis sont ennemis avec tous les autres.
3. Enlever A + ses amis : nouveau graphe.
   → raisonnement récursif

Chapitre 10

Structure du Web

10.1 Mémoire associative - Hypertexte

Liens hypertextes : chaque élément a des liens vers et depuis d'autres éléments. Un contenu hypertexte est un contenu auquel il est fait référence dans un document.

Deux exemples de contenus hypertextes :

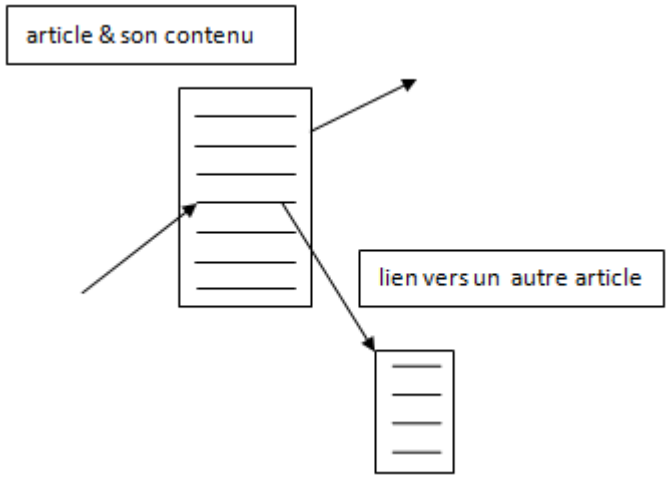
- **Graphe de citations**
  Précurseur du web : nœuds indépendants, liens strictement vers le passé
- **Encyclopédie**
  Les articles renvoient vers d'autres articles
  (Wikipédia)

} Réseaux d'informations

Problème de cohérence

- Web : Cohérence *"a posteriori"*
  Le web n'ayant pas d'organisation, on va devoir en trouver une : un index ou un moteur de recherche
- Wikipedia : Cohérence *"a priori"*
  Une structure existe déjà, définie par les rédacteurs, les modérateurs et les règles de structure.

Le succès du Web réside dans la possibilité de trouver une structure à ce dernier, notamment grâce à l'algorithme PageRank. Altavista, Google, Lycos, ... proposent tous leur version de moteur de recherche. C'est grâce à l'efficacité de PageRank que Google s'est imposé largement comme moteur de recherche dominant.



Graphique 10.1 – Hypertexte -liens vers des articles

10.2 Le Web est un graphe orienté

— Chemin dans un graphe orienté : $A - \rightarrow B$

Séquence de nœuds qui commence avec A et termine avec B et où chaque paire consécutive correspond à un lien orienté.

— Connectivité :

Un graphe orienté est connexe s'il existe un chemin orienté entre chaque paire de nœuds.

10.3 Composant fortement connexe (CFC) *Strongly Connected Component (SCC)*

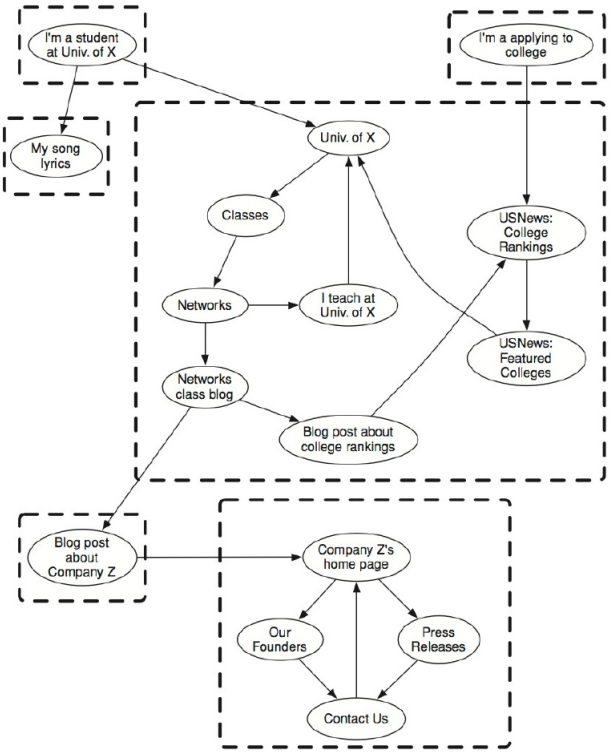
À l'intérieur d'un graphe orienté, un composant fortement connexe est :

— Un ensemble de nœuds tel qu'il existe un chemin orienté entre chaque paire.

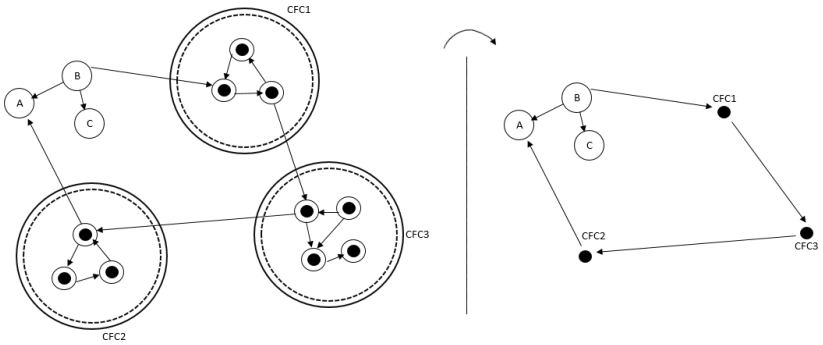
— L'ensemble ne fait pas partie d'un plus grand environnement qui à la même propriété.

Les CFCs forment un genre de *"super noeud"*. Pour la connectivité, on peut ignorer la structure interne des CFCs.

On peut donc transformer le graphe en un graphe réduit : le CFC devient un unique nœud. Pour trouver un chemin dans le graphe original, il suffit de trouver un chemin dans le graphe réduit. Un exemple de transformation de ce type est illustré sur la figure 10.3.



Graphique 10.2 – Un graphe dirigé avec ses CFCs identifiés

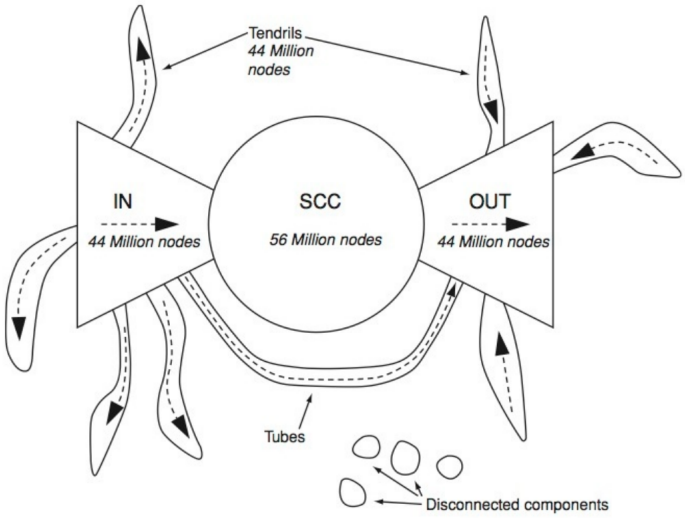


Graphique 10.3 – Exemple de transformation du graphe

10.4 Nœud papillon (≈ *années 2000*)

Maintenant, à quoi ressemble le graphe réduit du web ? Autour des années 2000, sa structure était proche de celle d'un nœud papillon, tel que celui représenté sur la figure 10.4.

On repère trois composants principaux :
— Un composant "in", qui contient des liens hypertextes sortants.



Graphique 10.4 – Structure en nœud papillon du web

— Un composant fortement connecté principal, qui forme un "noyau".
— Un composant "out", qui contient beaucoup de liens hypertextes entrants.

10.5 Émergence du Web 2.0 ($\geq$ *années 2000*)

L'émergence du Web 2.0 se déroule entre 2000 et 2010. Il s'agit en fait d'un changement d'attitude général des certains acteurs importants du web conduisant à une structuration de la toile basée sur trois grands principes.

1. Création collaborative de contenu plutôt que des pages personnelles.
2. Services vers lesquels sont transférés les données personnelles. Au lieu de publier du contenu sur des sites personnels, les gens se tournent vers des services pour publier leur contenu (par exemple YouTube, Flicker, Github...)
3. Personnes au lieu des documents. On n'identifie plus un document en fonction de son contenu, mais en fonction de son auteur ou de la personne qui en est le sujet.

Technologies utilisées :
— Blogs (Skyblog), ensuite détrônés par les réseaux sociaux (Facebook, Twitter, MySpace, Friendster...)
— Deep Web : création de page à la demande (créer un nouveau profil, une page Wikipédia, un groupe d'intérêt...)

— Cloud : regroupement et partage de ressources "à la demande", permet plus d'élasticité (adaptation en fonction des besoins)

Un petit bout d'histoire

Quelques précurseurs :

— 1945 - Vannevar Bush : Conseiller du président des États-Unis, Roosevelt
Il a écrit un article intitulé "As We May Think" dans lequel il explique son appareil électronique relié à une bibliothèque et capable d'afficher des livres et de projeter des films appelé "Memex".

— 1934 - Paul Otlet : Documentaliste
Il avait imaginé un système où l'on pourrait faire des recherches et consulter le résultat de ces recherches sur un écran. Cette intuition d'un pré internet est à l'origine d'une structuration des ressources des bibliothèques. Il est aussi un pionnier des microfiches, des fiches indépendantes qui stockent des informations, ayant une ressemblance non négligeable avec les pages web d'aujourd'hui.

— 1990 - Tim Berners-Lee et Robert Cailliau - CERN : Inventeur du World Wide Web
Ils se sont inspirés des écrits de Vannevar Bush pour inventer le WWW, avec sa structure de pages indépendantes reliées par des liens hypertextes.

Chapitre 11

Recherche dans le Web

Comment trouver une information ?

1960 : Concept de mot-clé → Limitations fortes

— Limitations dues au concept de mot
  — Synonymie : plusieurs mots pour le même concept.
  — Polysémie : un mot pour plusieurs concepts.
    Par exemple les noms propres peuvent référer à plusieurs personnes, des lieux et des organisations.

  Autrement dit, il n'y a pas de bijection entre les mots et les concepts.
— Limitations dues à l'abondance d'informations.
  — Avant : Les informations sur le web étaient rares.
  — Maintenant : Il y a beaucoup trop d'informations.

  } Plus grand problème du web

Pour résoudre le problème de surabondance d'informations, il faut trouver une façon de savoir quelle page est la meilleure. Comment faire ce choix ?

La meilleure solution est d'utiliser l'information contenue dans la structure du réseau.

11.1 L'Analyse des liens

— Concentrateurs (Hubs)
— Autorités (Authorities)
— Comment trouver la meilleure page ? (Voir 11.1)

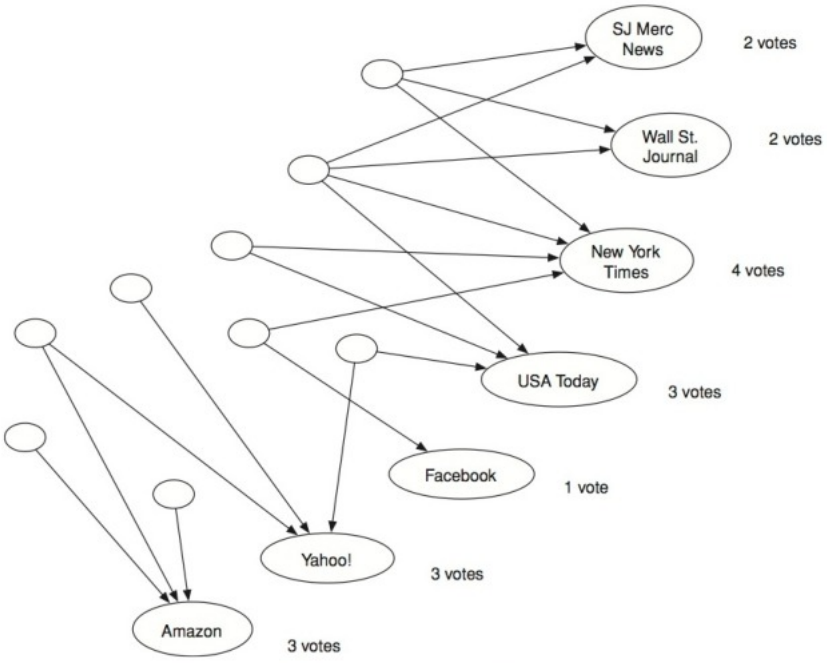


Figure 14.1. Counting in-links to pages for the query "newspapers."

Graphique 11.1 – Counting in-links to pages for the query "newspapers. "

11.1.1 Requête News Papers

Pourquoi Facebook, Yahoo, Amazon, se retrouvent-ils dans la requette News Papers ? Car beaucoup d'utilisateurs ont des pages concentrées sur ces sites et comme dans cet exemple on utilise un algorithme qui n'est pas très sophistiqué, elles apparaissent.

Comment trouver la meilleure page ?

1. Liens entrants → votes
2. Liens sortants calcul du→ poids
3. Mise à jour des liens entrants

4. Mise à jour des liens sortants

Algorithme

— Pages autorité (liens entrants) → auto (p)
— Pages concentrateurs (liens sortants) → conc (p)
— Mises à jour des liens entrants :

$$auto'(p) = \sum_{p' \to p} conc(p') \quad \textit{avec } p' \to p \textit{ les pages p' qui ont un lien vers P}$$

— Mises à jour des liens sortants :

$$conc'(p) = \sum_{p \to p'} auto(p') \quad \textit{avec } p \to p' \textit{ les pages p' qui sont référencées à partir de p}$$

Itération

$$\forall p(page) : \begin{cases} auto(p) = 1 \\ conc(p) = 1 \end{cases} \tag{11.1}$$

Mise à jour, normalisation :

$$auto'(p) = \frac{auto(p)}{\sum auto(p')}$$

$$conc'(p) = \frac{conc(p)}{\sum conc(p)}$$

Cet algorithme converge

En appliquant maintenant cet algorithme, la Requête News Papers nous donnerait les résultats suivants (11.2 et 11.3) :

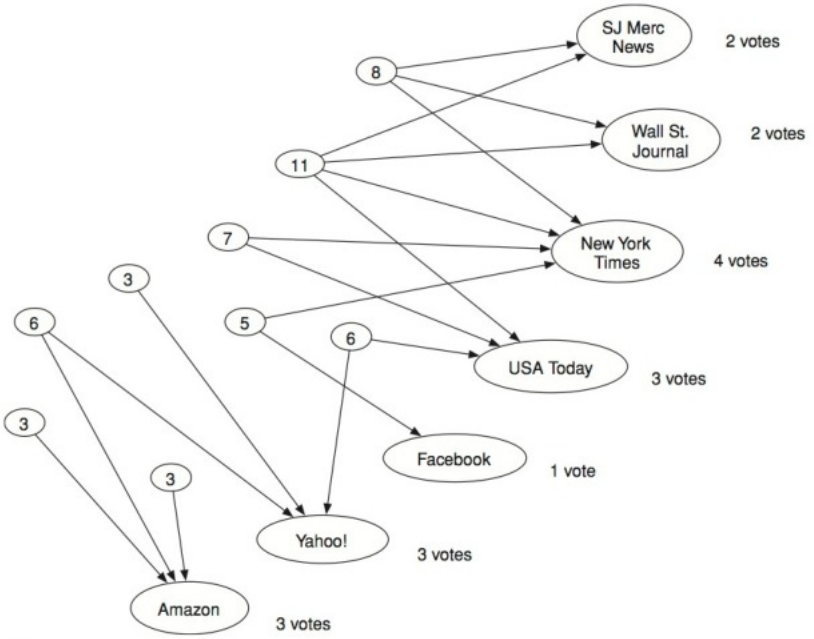


Figure 14.2. Finding good lists for the query "newspapers": each page's value as a list is written as a number inside it.

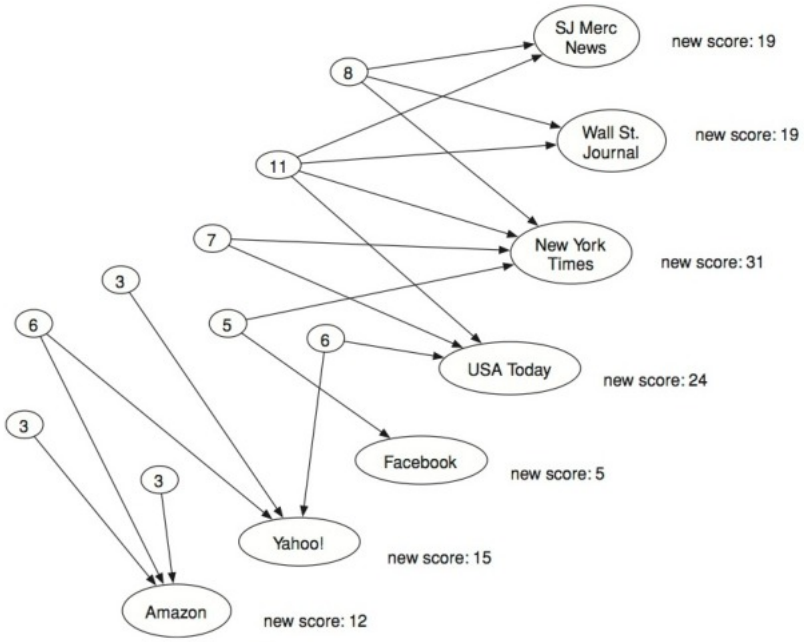


Figure 14.3. Reweighting votes for the query "newspapers": each labeled page's new score is equal to the sum of the values of all lists that point to it.

Graphique 11.2 – Page Rank

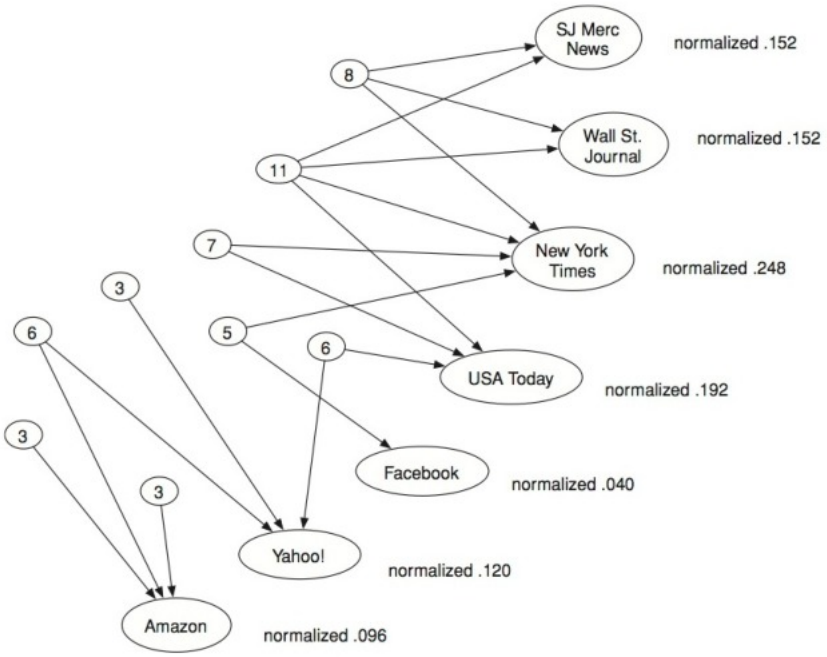


Figure 14.4. Reweighting votes after normalizing for the query "newspapers."

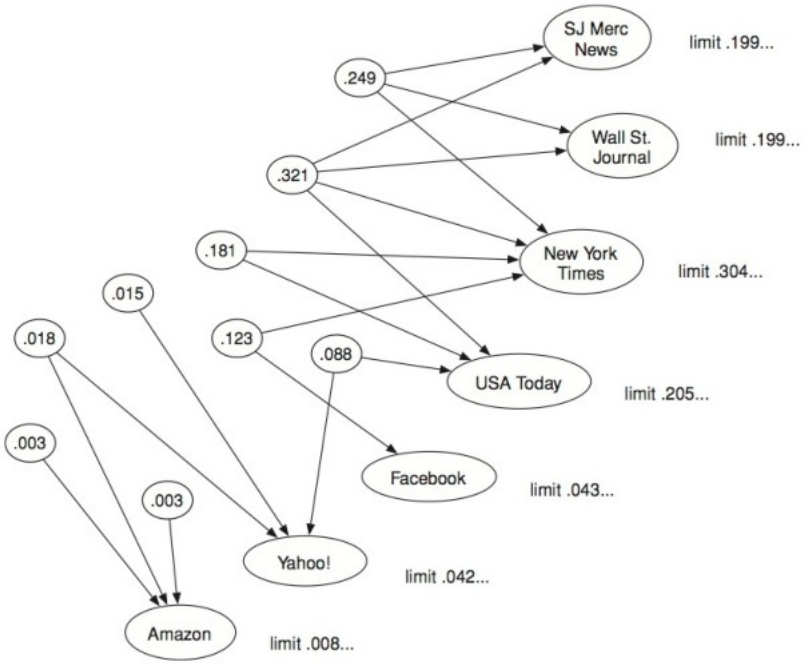


Figure 14.5. Limiting hub and authority values for the query "newspapers."

Graphique 11.3 – Page Rank

Comme nous pouvons voir, l'algorithme compte le nombre de liens entrants pour attribuer un poids à chaque place. Puis on normalise les valeurs trouvées, ce qui correspond au poids de la page. Au plus grand est le poids d'une page au plus son autorité sera grande.

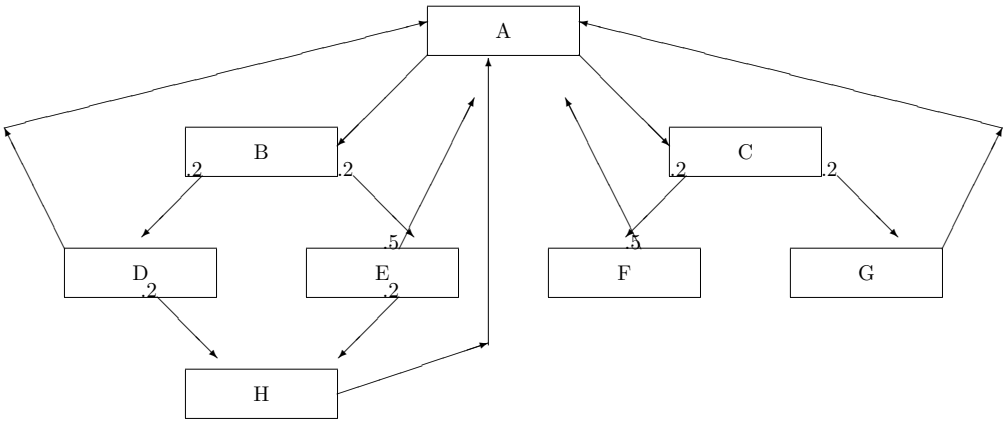
11.2 PageRank

— Consolider autorités et concentrateurs.
— Une valeur par noeud → son "PageRank" que nous allons calculer.
— Intuition : Un "fluide" qui circule dans le réseau.

Algorithme PageRank :

1. N noeuds (chaque noeud représentant une page) : Initialisation Pr(p) $= \frac{1}{n}$
2. Choisir un nombre de pas k
3. K mises à jour :
   Pr(p) = $\sum_{p'} \frac{Pr(p')}{n(p')}$ avec n(p') le nombre de liens sortant de p' et Pr(p') le poids (ou PageRank de p') à la $k^{ème}$ itération.

Exemple de PageRank :



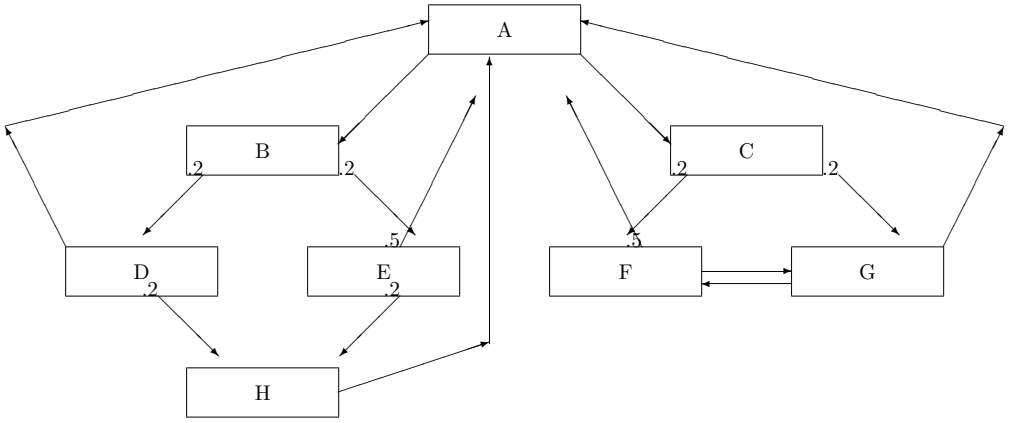
Noeuds/Itérations	0	1	2
A	1/8	1/2	5/16
B	1/8	1/16	1/4
C	1/8	1/16	1/4
D	1/8	1/16	1/32
E	1/8	1/16	1/32
F	1/8	1/16	1/32
G	1/8	1/16	1/32
H	1/8	1/8	1/16
$\sum$	1	1	1

Si nous continuons à laisser travailler l'algorithme, pour un nombre n fini d'itérations telles que k=n, il y aura convergence de l'algorithme. Dans cet exemple-ci, nous aurons :

$$Pr(A) = 4/13; Pr(B) = 2/13; Pr(C) = 2/13; Pr(Autres) = 1/13$$

Et la condition $\sum Pr(p) = 1$ est toujours vérifiée.

L'équilibre est vérifié si le graphe est connexe,par contre si il ne l'est pas un problème se pose : Le fluide peut arriver au mauvais noeud (analogie réseau d'eau) :



Solution du problème

— Fermer la boucle
— Créer des cycles
— Analogie : Circulation d'eau dans l'atmosphère

La solution est de réinjecter un peu de fluide partout à chaque itération pour éviter que le fluide se concentre dans les noeuds qui n'ont que des liens entrants et pas de liens sortant.

Ancienne règle de mise à jour :

$$Pr(p) = \sum_{p'} \frac{Pr(p')}{n(p')}$$

Nouvelle règle de mise à jour :

$$Pr(p) = Sx(Pr(p) + (1 - S) \times \frac{1}{n})$$

Ou S est un paramètre : $0 \leq S \leq 1$

Une autre manière de voir l'algorithme :

Marche aléatoire d'un utilisateur sur le web :

— Probabilité de S : Suivre un lien dans la page web ou l'on se trouve

— (1-S) : Choisi un nœud au hasard, par exemple, taper une adresse URL et accéder directement à un site

— → La même valeur pour Pr(p)

PageRank : (début 1990)
- Abandon partiel en 2003/2004 à cause des SEO : Search engine optimisation (Tricheurs)

Bibliographie

[Nis] Nimal Nissanke. *Introductory Logic and Sets for Computer Scientists.*

[LPP] David Easley and Jon Kleinberg. *Networks, Crowds, and Markets : Reasoning About a Highly Connected World.*