Université Batna 2
Faculté de Mathématiques et de l'informatique
Département de Mathématiques

Logique Mathématiques

Cours et Exercices

L2 Mathématiques

Table des matières

Introduction

La logique mathématique est née à la fin du $19^{ième}$ siècle au sens philosophique du terme ; elle est l'une des pistes explorées par les mathématiciens de cette époque afin de résoudre la crise des fondements provoquée par la complexification des mathématiques et l'apparition des paradoxes. Ses débuts sont marqués par la rencontre entre deux idées nouvelles :

- la volonté chez Frege, Russell, Peano et Hilbert de donner une fondation axiomatique aux mathématiques ;
- la découverte par George Boole de l'existence de structures algébriques permettant de définir un «calcul de vérité».

La logique mathématique se fonde sur les premières tentatives de traitement formel des mathématiques, dues à Leibniz et Lambert (fin $16^{ième}$ siècle - début $17^{ième}$ siècle). Leibniz a en particulier introduit une grande partie de la notation mathématique moderne (usage des quantificateurs, symbole d'intégration, etc.). Toutefois on ne peut parler de logique mathématique qu'à partir du milieu du $19^{ième}$ siècle, avec les travaux de George Boole (et dans une moindre mesure ceux d'Auguste De Morgan) qui introduit un calcul de vérité où les combinaisons logiques comme la conjonction, la disjonction et l'implication, sont des opérations analogues à l'addition ou la multiplication des entiers, mais portant sur les valeurs de vérité faux et vrai (ou 0 et 1) ; ces opérations booléennes se définissent au moyen de tables de vérité.

Le calcul de Boole véhiculait l'idée apparemment paradoxale, mais qui devait s'avérer spectaculaires fructueuse, que le langage logique pouvait se définir mathématiquement et devenir un objet d'étude pour les mathématiciens. Toutefois il ne permettait pas encore de résoudre les problèmes de fondements. Dès lors, nombre de mathématiciens ont cherché à l'étendre au cadre général du raisonnement mathématique et on a vu apparaître les systèmes logiques formalisés ; l'un des premiers est dû à Frege au tournant du $20^{ième}$ siècle.

En 1900 au cours d'une très célèbre conférence au congrès international des mathématiciens à Paris, David Hilbert a proposé une liste des 23 problèmes [5] non résolus les plus importants des mathématiques d'alors. Le deuxième était celui de la cohérence de l'arithmétique, c'est-à-dire de démontrer par des moyens finitistes la non-contradiction des axiomes de l'arithmétique.

Le programme de Hilbert a suscité de nombreux travaux en logique dans le premier quart du siècle, notamment le développement de systèmes d'axiomes pour les mathématiques : les axiomes de Peano pour l'arithmétique, ceux de Zermelo complétés par Skolem et Fraenkel pour la théorie des ensembles et le développement par Whitehead et Russell d'un programme de formalisation des mathématiques. C'est également la période où apparaissent les principes fondateurs de la théorie des modèles : notion de modèle d'une théorie et théorème de Löwenheim-Skolem.

En 1929 Kurt Gödel montre dans sa thèse de doctorat son théorème de complétude qui énonce le succès de l'entreprise de formalisation des mathématiques : tout raisonnement mathématique peut en principe être formalisé dans le calcul des prédicats. Ce théorème a été accueilli comme une avancée notable vers la résolution du programme de Hilbert, mais un an plus tard, Gödel démontrait le théorème d'incomplétude (publié en 1931) qui montrait irréfutablement l'impossibilité de réaliser ce programme.

Ce résultat négatif n'a toutefois pas arrêté l'essor de la logique mathématique. Les années 1930 ont vu arriver une nouvelle génération de logiciens anglais et américains, notamment Alonzo Church, Alan Turing, Stephen Kleene, Haskell Curry et Emil Post, qui ont grandement contribué à la définition de la notion d'algorithme et au développement de la théorie de la complexité algorithmique (théorie de la calculabilité, théorie de la complexité des algorithmes). La théorie de la démonstration de Hilbert a également continué à se développer avec les travaux de Gerhard Gentzen qui a produit la première démonstration de cohérence relative et a initié ainsi un programme de classification des théories axiomatiques.

Le résultat le plus spectaculaire de l'après-guerre est dû à Paul Cohen qui démontre en utilisant la méthode du forcing, l'indépendance de l'hypothèse du continu en théorie des ensembles, résolvant ainsi le 1^{er} problème de Hilbert. Mais la logique mathématique subit également une révolution due à l'apparition de l'informatique ; la découverte de la correspondance de Curry-Howard, qui relie les preuves formelles au lambda-calcul de Church et donne un contenu calculatoire aux démonstrations, va déclencher un vaste programme de recherche.

La logique classique est la première formalisation du langage et du raisonnement mathématique développée à partir de la fin du $19^{ième}$ siècle en logique mathématique. Appelée simplement logique à ses débuts, c'est l'apparition d'autres systèmes logiques formels, notamment pour la logique intuitionniste, qui a suscité l'adjonction de l'adjectif classique au terme logique.

La logique classique est caractérisée par des postulats qui la fondent et la différencient de la logique intuitionniste, exprimés dans le formalisme du calcul des propositions ou du calcul des prédicats .

La logique est utilisée en informatique pour modéliser de manière formelle des "objets" rencontrés par les informaticiens ; par exemple : Bases de données, Bases de connaissances, Pré-post conditions d'une procédure, ... etc. l'informaticien doit être capable de se servir du modèle et raisonner sur celui-ci, comme la validation d'un modèle de données, prise de décision à partir des faits et d'une base de connaissances, preuve de correction d'une procédure/d'un programme.
La logique est à la base de l'étude des raisonnements, c'est-'a-dire des déductions que l'on peut faire sur les modèles formels.

Le but de ce cours est d'étudier en détail les fondements de la logique classique et de donner aux étudiants une formation suffisante pour qu'ils puissent se familiariser avec d'autres logiques (intuitionniste ou floue) qu'ils peuvent rencontrer plus tard. Et également les sensibiliser au fait que la logique peut être très utile pour automatiser/semi-automatiser les tâches de raisonnement rencontrées lors de la construction/l'analyse de modèles et de programmes.

Le premier chapitre de ce document est consacré au calcul des propositions (syntaxe et sémantique), tandis que le deuxième chapitre donne les principes de la théorie de démonstration pour le calcul des propositions (ici, j'ai choisi le système d'Hilbert en cours et proposé une autre système en TD (le système de Lukasiewicz [7])). Le troisième chapitre introduit la notion de calcul des prédicats (syntaxe et sémantique). Bien qu'on a abordé la théorie de la démonstration dans le chapitre2, le chapitre 4 expose un autre moyen de preuve, appelé calcul des séquents. Pour chaque chapitre, il y a une série d'exercices dont la majorité ont été costruit par moi même ainsi que leur corrigés.

Chapitre 1

Le langage du calcul propositionnel

1.1 Introduction

Le calcul des propositions ou calcul propositionnel est une théorie logique ayant pour objet l'étude des relations logiques entre «propositions» et définissant les lois formelles selon lesquelles, au moyen de connecteurs logiques, les propositions se coordonnent et s'enchaînent pour produire des raisonnements valides.

Appelée aussi la logique d'ordre 0, elle est l'un des langages formels privilégiés de la logique mathématique pour la formulation de ses concepts en systèmes formels, en raison de son applicabilité aux fondements des mathématiques et de la richesse de ses propriétés relevant de la théorie de la démonstration.

La notion de proposition a fait l'objet de nombreux débats au cours de l'histoire de la logique ; l'idée consensuelle est qu'une proposition est une construction syntaxique censée avec une valeur de vérité.

En logique mathématique, le calcul des propositions est la première étape dans la définition de la logique et du raisonnement. Il définit les règles de déduction qui relient les propositions entre elles, sans en examiner le contenu ; il est ainsi une première étape dans la construction du calcul des prédicats, qui lui s'intéresse au contenu des propositions et qui est une formalisation achevée du raisonnement mathématique. Le calcul des propositions est parfois appelé logique des propositions, logique propositionnelle ou calcul des énoncés, et parfois théorie des fonctions de vérité.

1.2 Définition

Définition 1.1. (proposition, en anglais : sentense)
On appelle proposition un assemblage de mots d'une langue naturelle vérifiant les trois propriétés suivantes :

1. Il est reconnu syntaxiquement correct ;
2. Il est sémantiquement correct ;
3. Il est possible de lui assigner sans ambiguïté une valeur de vérité (vrai ou faux).

Exemple 1.2.1. Louis 14 est un nombre premier.
Un littéraire attribuera à cette phrase la propriété (1) mais sans doute pas la propriété (2). Ce n'est donc pas une proposition.

Exemple 1.2.2. Dans un triangle rectangle, le carré de l'hypoténuse est égal à la somme des carrés des cotés de l'angle droit.
Les propriétés (1, 2 et 3) sont vérifiées : c'est une proposition (vraie).

Exemple 1.2.3. Le facteur est il arrivé ?
les propriétés (1) et (2) sont vérifiées, mais pas la (3). Ce n'est donc pas une proposition.

1.3 Le langage propositionnel

Le langage propositionnel est composé de formules représentant des propositions. Comme les autres langages, le langage du calcul propositionnel est caractérisé par sa syntaxe et sa sémantique.

1.3.1 La syntaxe du langage propositionnel

La syntaxe d'un langage définit l'alphabet et les règles d'écriture (grammaire) des expressions du langage. Elle ne s'intéresse pas à leurs sens.

L'alphabet

L'alphabet est composé des symboles du langage. Il comporte :
– Un ensemble dénombrable de variables propositionnelles. On convient d'utiliser les lettres de l'alphabet latin (a, b, c ...) éventuellement indicées.

- Des connecteurs logiques ($\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$). Cette liste n'est pas exhaustive, elle peut changer d'un enseignant à un autre ou d'une université à une autre.
- Des symboles auxiliaires.

Les règles d'écriture

Les règles d'écriture précisent la manière dont sont assemblés les symboles de l'alphabet pour former des expressions bien formées (ou formules) du langage propositionnel :

1. Toute variable propositionnelle est une formule ;
2. Si α est une formule, $\neg\alpha$ (ou $\overline{\alpha}$) est une formule ;
3. Si α et β sont des formules, $(\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \Rightarrow \beta)$ et $(\alpha \Leftrightarrow \beta)$ sont des formules ;
4. Une expression n'est une formule que si elle est écrite conformément aux règles 1,2 et 3.

Exemple 1.3.1.
1. p, q, r sont des variables propositionnelles, donc des formules.
2. $p \vee q$ est une formule.
3. $p \Rightarrow (q\neg r)$ n'est pas une formule.

1.3.2 Priorité des connecteurs

Les connecteurs sont appliqués dans l'ordre suivant :

$$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$$

Exemple 1.3.2.
1. $\neg p \wedge q$ se lit $(\neg p) \wedge q$.
2. $p \wedge q \Rightarrow r$ se lit $(p \wedge q) \Rightarrow r$.
3. $p \vee q \wedge r$ se lit $p \vee (q \wedge r)$.
4. $p \vee q \vee r$ se lit $(p \vee q) \vee r$

1.4 Sémantique d'un langage propositionnel

L'étude sémantique d'un langage pour le calcul des propositions a pour but de donner une valeur de vérité aux formules du langage. Elle est aussi appelée la théorie des

modèles.
La sémantique associe une fonction de valuation

$$\mathcal{V} : vp \longrightarrow \{1, 0\},$$

(où vp est l'ensemble des variables propositionnelles, 1 signifie *vrai* et 0 signifie *faux*) unique à chacun des connecteurs logiques.
Cette fonction est décrite par un graphe appelé table de vérité (ou tableau de vérité).
A chaque formule α à n variables propositionnelles correspond une fonction de vérité unique. Le graphe de cette fonction est défini par une table de vérité à 2^n lignes représentant la valeur de vérité de α correspondant à chaque combinaison de valeur de vérité des n variables (appelées aussi distribution de valeurs de vérité des variables).

1. **La négation**
   La négation d'une proposition a notée $\neg a$ ou $\overline{a}$ est définie de la manière suivante :
   Si la proposition a est *vraie* alors $\overline{a}$ est *fausse*.
   Si la proposition a est *fausse* alors $\overline{a}$ est *vraie*.
   En résumé, on a la table de vérité suivante :

a	$\overline{a}$
1	0
0	1

2. **La conjonction**
   La conjonction de deux propositions a et b notée symboliquement par $a \wedge b$ et se lit (a et b) est *vraie* si et seulement si les deux propositions a et b sont *vraies* simultanément. D'où la table de vérité suivante :

a	b	$a \wedge b$
1	1	1
1	0	0
0	1	0
0	0	0

3. **La disjonction**
   La disjonction de deux propositions a et b notée symboliquement par $a \vee b$ et se lit (a ou b) est *fausse* si et seulement si les deux propositions a et b sont *fausses* simultanément. D'où la table de vérité suivante :

a	b	$a \vee b$
1	1	1
1	0	1
0	1	1
0	0	0

4. **L'implication**
   Le connecteur "$\Rightarrow$" est appelé le connecteur d'implication, la proposition $a \Rightarrow b$

est *fausse* dans le cas où a est *vraie* et b est *fausse*. Elle est définie par le tableau suivant :

a	b	$a \Rightarrow b$
1	1	1
1	0	0
0	1	1
0	0	1

Soient a et b deux propositions, dans la formule $a \Rightarrow b$, a est appelée l'hypothèse (ou antécédent) et b la thèse (ou la conséquence).
$(a \Rightarrow b)$ est appelée implication directe.
Les implications apparentes à l'implication directe sont dénommées ainsi :

- $a \Rightarrow b$ implication directe, ici a est une condition suffisante pour b (b si a).
- $b \Rightarrow a$ implication réciproque (converse), ici a est une condition nécessaire de b.
- $\overline{a} \Rightarrow \overline{b}$ implication contraire (inverse).
- $\overline{b} \Rightarrow \overline{a}$ implication contraposée.

5. **L'équivalence** Le connecteur "$\Leftrightarrow$" est appelé le connecteur d'équivalence, la proposition $a \Leftrightarrow b$ est *vraie* dans le cas où a et b ont la même valeur de vérité. Elle est définie par le tableau suivant :

a	b	$a \Leftrightarrow b$
1	1	1
1	0	0
0	1	0
0	0	1

Exemple 1.4.1. Soit α la formule

$$p \vee q \Rightarrow r.$$

Sa table de vérité est :

p	q	r	$p \vee q$	α
1	1	1	1	1
1	1	0	1	0
1	0	1	1	1
1	0	0	1	0
0	1	1	1	1
0	1	0	1	0
0	0	1	0	1
0	0	0	0	1

1.4.1 Satisfiabilité

Une formule α est dite *satisfiable* si et seulement si sa table de vérité contient au moins une ligne où la valeur de vérité de α est *vraie* (ou $\mathcal{V}(\alpha) = 1$).
α est dite *insatisfiable* si elle est *fausse* sur toutes les lignes de sa table de vérité.

Exemple 1.4.2. La formule α de l'exemple précédent est *satisfiable*.

Exemple 1.4.3. Soit β la formule $(p \wedge q) \wedge \overline{(p \Leftrightarrow q)}$,

p	q	$p \wedge q$	$\overline{(p \Leftrightarrow q)}$	β
1	1	1	0	0
1	0	0	1	0
0	1	0	1	0
0	0	0	0	0

D'où β est insatisfiable (contradiction ou antilogie).

1.4.2 Satisfiabilité d'un ensemble de formules

On généralise la notion de *satisfiabilité* à un ensemble de formules :
Soit $\Gamma = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ un ensemble de formules. Γ est dit *satisfiable* si et seulement si étant donné la table de vérité de toutes les formules $\alpha_1, \alpha_2, \ldots, \alpha_n$, il existe au moins une lignes où toutes ces formules sont vraies simultanément.
La satisfiabilité d'un ensemble de formules est assimilée à la conjonction de toutes ses formules.

Exemple 1.4.4.
1. L'ensemble $\{p \wedge q, p \vee q, p \Rightarrow q\}$ est satisfiable.
2. L'ensemble $\{p \wedge q, p \vee q, \overline{p}\}$ est insatisfiable.

1.4.3 Tautologie

Une formule α est une *tautologie* (on note $\models \alpha$), si et seulement si α est vraie sur toutes les lignes de sa table de vérité.

Exemple 1.4.5. la formule $a \wedge b \Rightarrow b$ est une tautologie.

a	b	$a \wedge b$	$a \wedge b \Rightarrow b$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

Remarque 1.4.1. – Si $\models \alpha \Rightarrow \beta$, on dit que α implique logiquement β.

– Si $\models \alpha \Leftrightarrow \beta$, on dit que α est logiquement équivalente à β et on note $\alpha \equiv \beta$.

Lemme 1.4.1. *Une formule α est une tautologie si et seulement si $\overline{\alpha}$ est insatisfiable.*

Démonstration.
1. Supposons que $\models \alpha$ mais $\overline{\alpha}$ est satisfiable. Donc, il existe au moins une ligne de la table de vérité où $\overline{\alpha}$ est vraie. Pour cette ligne, α est fausse mais $\models \alpha$. Alors $\overline{\alpha}$ est insatisfiable.
2. Supposons maintenant que $\overline{\alpha}$ est insatisfiable mais α n'est pas une tautologie. Donc, il existe au moins une ligne de la table de vérité où α est fausse. Pour cette ligne, $\overline{\alpha}$ doit être vraie ce qui contredit le fait que $\overline{\alpha}$ est insatisfiable.

□

Théorème 1.4.1. *Si $\models \alpha$ et $\models \alpha \Rightarrow \beta$, alors $\models \beta$.*

Démonstration. Procédons par absurde.
Supposons que $\models \alpha$ et $\models \alpha \Rightarrow \beta$, mais $\not\models \beta$. Donc, il existe au moins une ligne où β est fausse. Pour cette ligne, $\alpha \Rightarrow \beta$ est fausse car $\models \alpha$. Contradiction avec le fait que $\models \alpha \Rightarrow \beta$. □

1.4.4 Conséquence logique

En langage propositionnel, une formule β est conséquence logique d'une formule α (et on note $\alpha \models \beta$), si et seulement si étant donné la table de vérité de α et β, la valeur de vérité de β est vraie sur toutes les lignes où la valeur de vérité de α est vraie.
De manière générale, une formule β est conséquence logique d'un ensemble de formules $\Gamma = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ (et on note $\Gamma \models \beta$ ou encore $\alpha_1, \alpha_2, \ldots, \alpha_n \models \beta$) si et seulement si étant donné la table de vérité des formules $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta$, la valeur de vérité de β est vraie sur toutes les lignes où les formules $\alpha_1 \alpha_2 \ldots \alpha_n$ sont vraie simultanément.

Exemple 1.4.6. $p \Rightarrow q, \overline{q} \models \overline{p}$

p	q	$p \Rightarrow q$	$\overline{q}$	$\overline{p}$
1	1	1	0	0
1	0	0	1	0
0	1	1	0	1
0	0	**1**	**1**	**1**

Remarque 1.4.2.
1. $\{\alpha_1, ..., \alpha_n\} \models a$ si et seulement si $\models \alpha_1 \wedge ... \wedge \alpha_n \Rightarrow \alpha$.
2. Soit E un ensemble de formules et $A \subseteq E$. Alors, si E est satisfiable, A est satisfiable.

3. L'ensemble vide est satisfiable.
4. L'ensemble de toutes les formules est insatisfiable.
5. Soit E un ensemble de formules et $A \subseteq E$. Alors, si A est insatisfiable alors E est insatisfiable.
6. Toute formule est conséquense logique d'un ensemble insatisfiable.
7. Toute tautologie est conséquense logique d'un ensemble quelconque de formules, en particulier de l'ensemble vide.

1.4.5 Théorème de substitution

Soit β une formule où figure la variable propositionnelle x, et soit β' la formule obtenue à partir de β en substituant à x, en toutes ses occurrences, une formule α.

$$\text{Si} \quad \models \beta, \qquad \text{alors} \quad \models \beta'.$$

Exemple 1.4.7. Soit $\beta \equiv x \Rightarrow ((y \Rightarrow z) \Rightarrow x)$. On peut vérifier que $\models \beta$.
Et soit $\beta' \equiv (a \wedge b) \Rightarrow ((y \Rightarrow z) \Rightarrow (a \wedge b))$ obtenue en substituant dans β, $(a \wedge b)$ à x.
Alors, $\models \beta'$.

1.4.6 Théorème de remplacement

Soit α une formule dans laquelle apparaît en une ou plusieurs occurrences la formule β, et soit α' la formule obtenue à partir de α en remplaçant β en une ou plusieurs de ses occurrences par la formule β'.

$$\text{Si} \quad \beta \equiv \beta', \qquad \text{alors} \quad \alpha \equiv \alpha'.$$

Exemple 1.4.8. Soit $\alpha \equiv x \vee (x \Rightarrow y) \Leftrightarrow (z \vee (z \Rightarrow y)$. On peut vérifier que $z \Rightarrow y \equiv \overline{z} \vee y$.
Soit α' la formule obtenue à partir de α en remplaçant $z \Rightarrow y$ par $\overline{z} \vee y$.
$\alpha' \equiv x \vee (x \Rightarrow y) \Leftrightarrow (z \vee (\overline{z} \vee y))$. On peut aisément vérifier que $\alpha \equiv \alpha'$.

1.5 Système complet de connecteurs

Un ensemble Γ de connecteurs est dit complet, si étant donné une formule quelconque α du calcul propositionnel, on peut trouver une formule α' dans laquelle n'interviennent que les éléments de Γ et telle que $\alpha \equiv \alpha'$.

Exemple 1.5.1. L'ensemble $\{\neg, \vee\}$ est complet.

1.6 Forme normale

Définition 1.2. **(atome, littéral, clause, forme normale conjonctive)**.

- Un atome ou formule atomique est une formule ne comportant qu'une variable propositionnelle (pas de connecteurs).
- Un littéral est une formule atomique ou la négation d'une formule atomique.
- Un monôme conjonctif est une conjonction de littéraux.
- Une clause est une disjonction de littéraux.
- Une formule est en forme normale conjonctive si elle est une conjonction de clauses.
- Une formule est en forme normale disjonctive si elle est une disjonction de monômes.

1.6.1 Obtention de Forme normale disjonctive (FND)

Il est nécessaire d'avoir un moyen algorithmique pour obtenir la (FND) à partir de la table de vérité.
Soit α une formule du calcul propositionnel ayant n variables $x_1, x_2, \ldots, x_n$. Supposons que A est la table de vérité de α. La FND de α est obtenue de la manière suivante :

- Soit p le nombre de lignes de A telles que $V(\alpha) = 1$.
- Pour chaque ligne i, $i = 1, \ldots, p$ où $V(\alpha) = 1$, soit M_i le monôme conjonctif correspondant.

$$M_i = \bigwedge_{k=1}^{n} a_{ik}, \quad \text{avec } a_{ik} = \begin{cases} x_k, \text{ si } V(x_k) = 1; \\ \overline{x_k}, \text{ si } V(x) = 0. \end{cases}$$

- La FND de α est alors :

$$\alpha \equiv \bigvee_{i=1}^{p} M_i.$$

1.6.2 Forme normale conjonctive (FNC)

D'une manière analogue, on obtient la FNC d'une formule α. Soit α une formule du calcul propositionnel ayant n variables $x_1, x_2, \ldots, x_n$. Supposons que A est la table de vérité de α. La FNC de α est obtenue de la manière suivante :

- Soit q le nombre de lignes de A, telles que $V(\alpha) = 0$.

– Pour chaque ligne $i,\ i = 1, \ldots, q$ où $V(\alpha) = 0$, soit C_i la clause correspondante.

$$C_i = \bigvee_{k=1}^{n} l_{ik}, \quad \text{avec } l_{ik} = \begin{cases} x_k, \text{ si } V(x_k) = 0; \\ \overline{x_k}, \text{ si } V(x) = 1. \end{cases}$$

– La FNC de α est alors :

$$\alpha \equiv \bigwedge_{i=1}^{p} M_i.$$

Remarque 1.6.1. 1.

$$FND(\alpha) \equiv FNC(\alpha).$$

2. Par convention, si $\models \alpha$, alors $FND(\alpha) \equiv 1$;
3. Si α est une contradiction (antilogie ou formule insatisfiable) alors, $FNC(\alpha) \equiv 0$.

1.7 Conclusion

Enormément de problèmes peuvent être formulés en logique des propositions, mais quand le nombre de variables est important ou inconnu, l'utilisation des tables de vérité devient difficile et parfois impossible. Dans le chapitre 2, nous allons présenter une méthode formelle (qui ne fait pas appel aux tables de vérité) pour montrer que les formules sont des tautologies ou des conséquences logiques d'autres formules : la théorie de la démonstration.

Le calcul propositionnel a de bonnes propriétés (on peut décider si une formule est valide ou satisfiable), mais manque d'expressivité surtout quand il faut modéliser des espaces infinis comme les entiers. On pourrait utiliser une infinité de variables propositionnelles et une infinité d'hypothèses, mais ce n'est pas facile à manipuler pour des humains et encore moins pour des machines. Il peut être utile d'avoir des descriptions finies qui rendent compte de situations potentiellement infinies. Cette notion est le calcul des prédicats. Nous allons donner une présentation du calcul des prédicats du premier ordre dans le chapitre 3.

1.8 Exercices

Exercice 1.1. Traduire en langage propositionnelle les phrases suivantes :

1. Une relation est une relation d'équivalence si et si et seulement si elle est reflexive, symétrique et transitive.
2. Si Said est fatigué, il se reposera, et s'il ne l'est pas, il terminera son travail.
3. Si Ali prend le bus et celui ci est en retard, alors Ali n'arrivera pas à l'heure à son rendez vous.

Exercice 1.2. "Si je ne peins pas mon portail en fer, il va rouiller". Peut-on en déduire que si je le peins, il ne rouillera pas ?

Exercice 1.3. Lors d'élections, un candidat énonce : " si vous votez pour mon adversaire, les impôts vont augmenter". Cela présente-t-il un intérêt pour le contribuable de voter pour ce candidat ?

Exercice 1.4. Soit f une formule logique à 4 variables logiques, telle que $f = 1$ si et seulement le nombre de variables de f qui sont vraies est supérieur ou égale à 2.

1. Etablir le tableau de vérité de f.
2. Donner la forme normale disjonctive et la forme normale conjonctive de f

Exercice 1.5. Soient α une antilogie et β une formule quelquonque. Montrer que $\alpha \Rightarrow \beta$ est une tautologie.

Exercice 1.6. On considère la proposition (0) si les hirondelles se rassemblent, elles commencent leur migration. Parmi les propositions suivantes, dites lesquelles sont logiquement équivalentes à (0), lesquelles sont en contradiction avec (0), lesquelles sont sa réciproque.

1. Si les hirondelles ne commencent pas leur migration, alors elles ne se rassemblent pas.
2. Il suffit que les hirondelles se rassemblent pour qu'elles commencent leur migration.
3. Les hirondelles se rassemblent si elles commencent leur migration.
4. Les hirondelles commencent leur migration.
5. Les hirondelles se rassemblent et elles ne commencent pas leur migration.

6. Il suffit que les hirondelles commencent leur migration pour qu'elles se rassemblent.
7. Il est nécessaire que les hirondelles se rassemblent pour qu'elles commencent leur migration.
8. Si les hirondelles ne se rassemblent pas, alors elles ne commencent pas leur migration.
9. Les hirondelles ne se rassemblent pas ou elles commencent leur migration.
10. Il faut que les hirondelles se rassemblent pour qu'elles commencent leur migration.
11. Aprés le rassemblement des hirondelles, c'est l'hiver.
12. Les hirondelles se rassemblent

Exercice 1.7. Que peut-on dire des formules suivantes ? Sont-elles satisfaisables ? tautologies ? Insatisfaisables ? Utiliser pour chacune les tables de vérité.

1. $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$
2. $((p \Rightarrow q) \wedge (s \Rightarrow m)) \Rightarrow ((p \vee s) \Rightarrow q)$
3. $p \Rightarrow q \wedge p \wedge \neg q$
4. $(p \wedge \neg p) \Rightarrow q$

Exercice 1.8. Montrer que :

1. p implique logiquement p
2. p implique logiquement $(p \Rightarrow p)$
3. $\models (q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$
4. $(\overline{(p \vee \overline{q})} \Rightarrow (q \Rightarrow r) \equiv q \Rightarrow (p \vee r)$

Exercice 1.9. Etant donnée deux propositions P et Q, on définit la proposition $(P \triangle Q)$ qui est logiquement équivalente à $(\overline{P} \wedge \overline{Q})$.
Exprimer, à l'aide du seul symbole $\triangle$ les propositions $\overline{P}$, P, $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$.

Exercice 1.10.
- Donner une formule logiquement équivalente à $p \Leftrightarrow \neg q$ et ne contenant ni le symbole $\Leftrightarrow$ ni le symbole $\Rightarrow$.
- Déterminer si la formule suivante est une tautologie : $\neg p \Rightarrow (p \Rightarrow q)$
- Si $(A \wedge B) \equiv (A \wedge C)$, peut-on en conclure que $B \equiv C$?

Exercice 1.11. Soient les formules suivantes :

$$\alpha_1 : (x \vee y) \Rightarrow (x \wedge y)$$

$$\alpha_2 : (x \wedge z) \Rightarrow (x \Rightarrow y)$$

$$\alpha : (x \vee z) \Rightarrow (x \Rightarrow y)$$

Montrer que $\alpha_1, \alpha_2 \models \alpha$

Chapitre 2

Théorie de la démonstration pour le calcul propositionnel

2.1 Introduction

La théorie de la démonstration, aussi connue sous le nom de théorie de la preuve (de l'anglais proof theory), est une branche de la logique mathématique. Elle a été fondée par David Hilbert au début du 20^{me} siècle.
Hilbert a proposé cette nouvelle discipline mathématique lors de son célèbre exposé au 2^{me} congrès international des mathématiciens en 1900 avec pour objectif de démontrer la cohérence des mathématiques.
Après une période de calme, qui a tout de même permis d'établir un certain nombre d'autres résultats de cohérence relative et d'esquisser une classification des théories axiomatiques, la théorie de la démonstration a connu une renaissance spectaculaire au cours des années 1960 avec la découverte de la correspondance de Curry-Howard qui a exhibé un lien structurel nouveau et profond entre logique et informatique.
En logique, les systèmes à la Hilbert servent à définir les déductions formelles en suivant un modèle proposé par David Hilbert au début du 20^{me} siècle : un grand nombre d'axiomes logiques exprimant les principales propriétés de la logique que l'on combine au moyen de quelques règles, notamment la règle de Modus Ponens, pour dériver de nouveaux théorèmes. Les systèmes à la Hilbert héritent du système défini par Gottlob Frege et constituent les premiers systèmes déductifs, avant l'apparition de la déduction naturelle ou du calcul des séquents, appelés parfois par opposition systèmes à la Gentzen.

Définition 2.1.1. 1. Une théorie formelle T est définie par :

(a) L'alphabet ;

(b) Les formules de T ;

(c) Un sous ensemble de formules formant les axiomes ;

(d) Une ou plusieurs règles d'inférence.

2. Une preuve dans T est une séquence de formules $\alpha_1, \alpha_2, \ldots, \alpha_n$, telles que chaque α_i est soit un axiome, soit un théorème déjà démontré, soit obtenue à partir de l'application d'une des règles d'inférence.
3. Si une formule α admet une preuve, on dit que α est démontrable ou α est un théorème et on note $\vdash \alpha$.
4. Une déduction (ou démonstration) d'une formule α à partir d'un certain ensemble de formules Γ est une séquence de formules $\alpha_1, \alpha_2, \ldots, \alpha_n$ telles que $\alpha_n = \alpha$ et chaque α_i est soit un axiome, soit un théorème déjà démontré, soit une formule de Γ, soit obtenue à partir de l'application d'une des règles d'inférence. Et on note $\Gamma \vdash \alpha$.

Dans le cadre de notre cours, on convient de considérer l'alphabet et les formules du calcul propositionnel.

2.2 Liste des axiomes

La liste des axiomes peut varier d'un auteur à un autre ou d'une institution à une autre. Les axiomes sont des formules dont on admet qu'elles sont des théorèmes sans pouvoir leur donner une démonstration formelle.
Nous donnons ici la liste des axiomes de Hilbert-Ackerman (H.A) ; et on considère le système complet de connecteurs $\{\neg, \vee\}$.

Définition 2.1. L'expression $x \Rightarrow y$ n'est qu'une abréviation de l'écriture $\overline{x} \vee y$.

Les axiomes d'H. A sont :

1. $(H.A)_1$ $\quad (x \vee x) \Rightarrow x$;
2. $(H.A)_2$ $\quad x \Rightarrow x \vee y$;
3. $(H.A)_3$ $\quad x \vee y \Rightarrow y \vee x$;
4. $(H.A)_4$ $\quad (x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$.

2.3 Les règles ou schémas de déduction

Les règles de déduction ont pour objet la déduction de nouveaux théorèmes à partir de théorèmes connus. Une règle de déduction n'est pas un axiome mais en quelque sorte un procédé permettant d'obtenir de nouveaux théorèmes.

2.3.1 Règle de détachement (ou Modus Ponens)

Contrairement à la liste des axiomes et les autres règles de déduction, la règle du Modus Ponens est commune à toutes les théorie. Le terme Modus Ponens (ou plus exactement Modus Ponendo Ponens) vient de ce que l'on pose α (Ponens est le participe présent de verbe latin Ponere, poser) afin d'en tirer la conclusion. Elle est donnée comme suit :

$$\text{De} \quad \vdash \alpha, \quad \vdash \alpha \Rightarrow \beta, \quad \text{on déduit} \quad \vdash \beta.$$

cette règle peut être formulée ainsi : soient deux formules α et β, telles que α et $\alpha \Rightarrow \beta$ sont des théorèmes, alors β est un théorème.

On peut utiliser un schéma pour illustrer cette règle : $\dfrac{\vdash \alpha \quad \vdash \alpha \Rightarrow \beta}{\vdash \beta}$

Cette figure fait bien apparaître pourquoi la règle s'appelle *règle de détachement* : elle permet de détacher le conséquent β de l'antécédent α dans l'implication $\alpha \Rightarrow \beta$, pourvu que $\vdash \alpha$ et $\vdash \alpha \Rightarrow \beta$.

2.3.2 Règle de substitution

Cette règle est indispensable pour les théorie où les axiomes sont donnés avec des variables propositionnelles (comme le cas de la théorie d'H.A.).
Soit α un théorème dans lequel figure la variable propositionnelle x, alors pour toute formule β (où β n'est pas nécessairement un théorème), la substitution de β à x en chacune de ses occurrences engendre un théorème.
Autrement dit :

$$\text{De} \quad \vdash \alpha, \quad \text{on déduit} \quad \vdash \alpha(x := \beta)$$

Exemple 2.3.1. Montrons le théorème $\vdash \overline{x} \vee x$.

Démonstration. Nous proposons la preuve suivante :

(1) $(x \vee x) \Rightarrow x$	$(H.A)_1$
(2) $x \Rightarrow x \vee y$	$(H.A)_2$
(3) $x \Rightarrow x \vee x$	sub $y := x$ dans (2)
(4) $(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(5) $(x \vee x \Rightarrow y) \Rightarrow (z \vee (x \vee x) \Rightarrow z \vee y)$	sub $x := x \vee x$ dans (4)
(6) $(x \vee x \Rightarrow x) \Rightarrow (z \vee (x \vee x) \Rightarrow z \vee x)$	sub $y := x$ dans (5)
(7) $(z \vee (x \vee x) \Rightarrow z \vee x)$	Modus Ponens (1,6)
(8) $(\overline{z} \vee (x \vee x) \Rightarrow \overline{z} \vee x)$	sub $z := \overline{z}$ dans (7)
(9) $(z \Rightarrow (x \vee x)) \Rightarrow (z \Rightarrow x)$	abréviation
(10) $(x \Rightarrow (x \vee x)) \Rightarrow (x \Rightarrow x)$	sub $z := x$ dans (9)
(11) $x \Rightarrow x$	Modus Ponens (3,10)
(12) $\overline{x} \vee x$	Définition de $\Rightarrow$.

□

Les démonstrations donnent rapidement lieu à des textes de longueur démesurée. On peut arriver plus vite au but en prenant des raccourcis qui consistent à adopter des *Règles dérivées*.

2.3.3 Règle S

Soient α, β, γ des formules. Alors

$$\text{de } \vdash \alpha \Rightarrow \beta \text{ et } \vdash \beta \Rightarrow \gamma \text{ on déduit } \vdash \alpha \Rightarrow \gamma$$

Démonstration. La preuve de cette règle est :

(1) $\alpha \Rightarrow \beta$	Hypothèse
(2) $\beta \Rightarrow \gamma$	Hypothèse
(3) $(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$	$(H.A)_4$
(4) $(\beta \Rightarrow \gamma) \Rightarrow (\overline{\alpha} \vee \beta \Rightarrow \overline{\alpha} \vee \gamma)$	sub $(x := \beta,\ y := \gamma,\ z := \overline{\alpha})$
(5) $(\beta \Rightarrow \gamma) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$	Abréviation
(6) $(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)$	Modus Ponens $(5, 2)$
(7) $\alpha \Rightarrow \gamma$	Modus Ponens $(6, 1)$.

□

2.3.4 Règles I

$$\text{De } \vdash \alpha \vee \alpha \text{ on déduit } \vdash \alpha.$$

Démonstration. La preuve de cette règle est :

(1) $(x \vee x) \Rightarrow x$ $(H.A)_1$
(2) $(\alpha \vee \alpha) \Rightarrow \alpha$ sub $(x := \alpha)$
(3) $\alpha \vee \alpha$ Hypothèse
(4) α Modus Ponens $(2, 3)$.

□

2.3.5 Règles II

De $\vdash \alpha$ on déduit $\vdash \alpha \vee \beta$.

Démonstration. La preuve de la règle II est :
(1) $x \Rightarrow x \vee y$ $(H.A)_2$
(2) $\alpha \Rightarrow \alpha \vee \beta$ sub $(x := \alpha,\ y := \beta)$
(3) α Hypothèse
(4) $\alpha \vee \beta$ Modus Ponens $(2, 3)$.

□

2.3.6 Règles III

De $\vdash \alpha \vee \beta$ on déduit $\vdash \beta \vee \alpha$.

Démonstration. La preuve de la règle III est :
(1) $x \vee y \Rightarrow y \vee 3$ $(H.A)_3$
(2) $\alpha \vee \beta \Rightarrow \beta \vee \alpha$ sub $(x := \alpha,\ y := \beta)$
(3) $\alpha \vee \beta$ Hypothèse
(4) $\beta \vee \alpha$ Modus Ponens $(2, 3)$.

□

2.3.7 Règles IV

De $\vdash \alpha \Rightarrow \beta$ on déduit $\vdash \gamma \vee \alpha \Rightarrow \gamma \vee \beta$.

Démonstration. La preuve de la règle IV est :
(1) $(x \Rightarrow y) \Rightarrow (z \vee x \Rightarrow z \vee y)$ $(H.A)_4$
(2) $(\alpha \Rightarrow \beta) \Rightarrow (\gamma \vee \alpha \Rightarrow \gamma \vee \beta)$ sub $(x := \alpha,\ y := \beta,\ z := \gamma)$
(3) $\alpha \Rightarrow \beta$ Hypothèse
(4) $\gamma \vee \alpha \Rightarrow \gamma \vee \beta$ Modus Ponens $(2, 3)$.

□

Définition 2.2. L'expression $x \wedge y$ est une abréviation permettant d'écrire $\overline{\overline{x} \vee \overline{y}}$.

2.3.8 Règles V

De $\vdash \alpha$ et $\vdash \beta$ on déduit $\vdash \alpha \wedge \beta$ et réciproquement.

Démonstration. La démonstration de cette règle se fait en trois partie. D'abord, on démontre que

De $\vdash \alpha$ et $\vdash \beta$ on déduit $\vdash \alpha \wedge \beta$.

Pour ce faire, on procède comme suit :

1. On démontre le théorème $x \Rightarrow (y \Rightarrow (x \wedge y))$;
2. Faire les substitutions adéquates ;
3. Obtenir le résultat en utilisant le Modus Ponens.

Ensuite, on démontre la réciproque
De $\vdash \alpha \wedge \beta$ on déduit $\vdash \alpha$ et de même, on déduit $\vdash \beta$. On procède de la manière suivante :

1. On démontre le théorème $(x \Rightarrow y) \Rightarrow (y \Rightarrow x)$;
2. On utilise $(H.A)_2$;
3. Quelques substitutions et abréviations, on obtient le résultats.

□

Définition 2.3. L'expression $x \Leftrightarrow y$ est une abréviation permettant d'écrire la formule $(x \Rightarrow y) \wedge (y \Rightarrow x)$.

Il est impossible de donner une liste complète des théorèmes du calculs des propositions car elle est infinie. Néanmoins, on peut donner les plus utilisés.
Ces théorèmes, combinés avec les règles de déduction ainsi que les règles dérivées, permettent de démontrer les autres théorèmes du calcul des propositions.

2.4 Liste des théorèmes

Les théorèmes les plus connus sont :

(1) $x \vee x \Leftrightarrow x$, $x \Leftrightarrow x \vee x$	Lois de *tautologie* ;
(2) $x \Leftrightarrow \overline{\overline{x}}$	Loi de la double négation ;
(3) $\overline{x} \vee x$	Loi du tiers exclu ;
(4) $x \vee \overline{x}$	Loi du tiers exclu (autre forme) ;
(5) $(x \Rightarrow y) \Leftrightarrow (\overline{y} \Rightarrow \overline{x})$	Loi de contraposition ;
(6) $x \vee (y \vee z) \Leftrightarrow (x \vee y) \vee z$	Associativité de $\vee$;
(7) $x \wedge (y \wedge z) \Leftrightarrow (x \wedge y) \wedge z$	Associativité de $\wedge$;
(8) $\overline{x \wedge y} \Leftrightarrow \overline{x} \vee \overline{y}$	Loi de De Morgan ;
(9) $\overline{x \vee y} \Leftrightarrow \overline{x} \wedge \overline{y}$	Loi de De Morgan (autre forme) ;
(10) $x \Rightarrow (y \Rightarrow (x \wedge y))$;	
(11) $x \wedge (y \vee z) \Leftrightarrow (x \wedge y) \vee (x \wedge z)$	Distribution de $\wedge$ sur $\vee$;
(12) $x \vee (y \wedge z) \Leftrightarrow (x \vee y) \wedge (x \vee z)$	Distribution de $\vee$ sur $\wedge$;
(13) $x \vee y \Leftrightarrow y \vee x$	Commutativité de $\vee$;
(14) $x \wedge y \Leftrightarrow y \wedge x$	Commutativité de $\wedge$;
(15) $x \wedge y \Rightarrow x$;	
(16) $x \Rightarrow x \vee y$;	
(17) $(x \Rightarrow y) \Rightarrow ((z \Rightarrow x) \Rightarrow (z \Rightarrow y))$;	
(18) $(x \Rightarrow y) \Rightarrow ((y \Rightarrow z) \Rightarrow (x \Rightarrow z))$.	

Dans ce qui suit, nous donnons quelques définitions nécessaires à la présentation et à la démonstration du plus important résultat du calcul des propositions qui est le théorème fondamental.

Définition 2.4. Deux formules α et β sont dites équivalentes si $\vdash \alpha \Leftrightarrow \beta$.

Exemple 2.4.1. Les deux formules $x \Rightarrow y$ et $\overline{y} \Rightarrow \overline{x}$ sont équivalentes.

Définition 2.5. On appelle *monôme disjonctif* par rapport aux variables $x, y, z, \ldots$, une formule présentant les caractéristiques suivantes :

- Chaque variable présente exactement une occurrence. Cette variable peut être surmontée d'une barre.
- Outre les variables, le monôme disjonctif ne comporte que le connecteur $\vee$.

Exemple 2.4.2. x, $\overline{x}$, $x \vee \overline{y}$, $x \vee y \vee \overline{z}$.

Définition 2.6. Une formule α qui se présente sous la forme $\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n$ où $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont des monômes disjonctifs, est dite formule sous *forme normale conjonctive*.

2.5 Exercices

Exercice 2.1. Dans le système d'axiomes d'H.A., montrer les règles de déduction suivantes :

1. $\alpha \Rightarrow \gamma, \beta \Rightarrow \sigma, \overline{\gamma} \vee \overline{\sigma} \vdash \overline{\alpha} \vee \overline{\beta}$.
2. $\alpha \Rightarrow \beta, \gamma \Rightarrow \sigma, \vdash \alpha \wedge \gamma \Rightarrow \beta \vee \sigma$.

Exercice 2.2. Montrer que les formules suivantes sont des théorèmes :

1. $\overline{\overline{\beta}} \Rightarrow \beta$;
2. $\beta \Rightarrow \overline{\overline{\beta}}$;
3. $\overline{\alpha} \Rightarrow (\alpha \Rightarrow \beta)$;
4. $(\overline{\beta} \rightarrow \overline{\alpha} \Rightarrow ((\overline{\beta} \Rightarrow \alpha)) \Rightarrow \beta)$;
5. $(\alpha \Rightarrow \beta) \Rightarrow (\overline{\beta} \Rightarrow \overline{\alpha})$;
6. $\alpha \Rightarrow (\overline{\beta} \Rightarrow \overline{(\alpha \Rightarrow \beta)})$;
7. $(\alpha \Rightarrow \beta) \Rightarrow ((\overline{\alpha} \Rightarrow \beta) \Rightarrow \beta)$.

Exercice 2.3. Soit le système d'axiomes suivant :
$A1 : \alpha \Rightarrow (\beta \Rightarrow \alpha)$;
$A2 : (\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$;
$A3 : (\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow (\alpha \Rightarrow \beta)$.
et la règle du Modus Ponens Si $\vdash \alpha$ et $\vdash \alpha \Rightarrow \beta$, alors $\vdash \beta$.
Montrer que l'on a :
de $\vdash \alpha$, on déduit $\vdash \beta \Rightarrow \alpha$;
De $\vdash (\alpha \Rightarrow \beta)$, et $(\beta \Rightarrow \gamma)$ on déduit $(\alpha \Rightarrow \gamma)$;
de $\alpha \Rightarrow (\beta \Rightarrow \gamma)$ on déduit $\beta \Rightarrow (\alpha \Rightarrow \gamma)$.

Exercice 2.4. En utilisant éventuellement les résultats de l'exercice précédent, montrer formellement que les formules suivantes sont des théorèmes du calcul propositionnel :

1. $(q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$;
2. $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$.

2.6 Corrigés des exercices

Corrigé de l'exercice 2.1. 1. Montrons que : $\alpha \Rightarrow \gamma, \beta \Rightarrow \sigma, \overline{\gamma} \vee \overline{\sigma} \Rightarrow \overline{\alpha} \vee \overline{\beta}$.

Preuve :

(1) $\alpha \Rightarrow \gamma$	Hypothèse 1 ;
(2) $\beta \Rightarrow \sigma$	Hypothèse 2 ;
(3) $\overline{\gamma} \vee \overline{\sigma}$	Hypothèse 3 ;
(4) $\overline{\sigma} \vee \overline{\gamma}$	Règle III sur (3) ;
(5) $\sigma \Rightarrow \overline{\gamma}$	Abréviation $\Rightarrow$;
(6) $\beta \Rightarrow \overline{\gamma}$	Règle S (2, 5) ;
(7) $\overline{\beta} \vee \overline{\gamma}$	Définition $\Rightarrow$;
(8) $\overline{\gamma} \vee \overline{\beta}$	Règle III sur (7) ;
(9) $\gamma \Rightarrow \overline{\beta}$	Abréviation $\Rightarrow$;
(10) $\alpha \Rightarrow \overline{\beta}$	Règle S (1, 9) ;
(11) $\overline{\alpha} \vee \overline{\beta}$	Définition $\Rightarrow$.

□

2. Montrons que : $\alpha \Rightarrow \beta, \gamma \Rightarrow \sigma \vdash \alpha \wedge \gamma \Rightarrow \beta \vee \sigma$.

Preuve :

(1) $\alpha \Rightarrow \beta$	Hypothèse 1 ;
(2) $\gamma \Rightarrow \sigma$	Hypothèse 2 ;
(3) $x \Rightarrow (x \vee y)$	$(H.A)_2$;
(4) $\beta \Rightarrow \beta \vee \sigma$	Substitution $(x := \beta, y := \sigma)$ dans (3) ;
(5) $\alpha \Rightarrow \beta \vee \sigma$	Règle S (1, 4) ;
(6) $(x \wedge y) \Rightarrow x$	Théorème 15.
(7) $(\alpha \wedge \gamma) \Rightarrow \alpha$	Substitution $(x := \alpha, y := \gamma)$ dans (6) ;
(8) $(\alpha \wedge \gamma) \Rightarrow \beta \vee \sigma$	Règle S (7, 5).

□

Corrigé de l'exercice 2.2. 1. Montrons que : $\vdash \overline{\overline{\beta}} \Rightarrow \beta$.

Preuve :

Remarque 2.6.1. Nous allons démontrer la condition suffisante de ce théorème. Donc, on peut supposer que la condition nécessaire est démontrée et l'utiliser mais on ne peut pas utiliser le théorème en entier directement.

(1) $x \Rightarrow \overline{\overline{x}}$	Théorème 2 ;
(2) $\overline{x} \vee \overline{\overline{x}}$	Définition de $\Rightarrow$;
(3) $\overline{\overline{x}} \vee \overline{\overline{\overline{x}}}$	Substitution $(x := \overline{x})$ dans (2) ;
(4) $\overline{x} \Rightarrow \overline{\overline{\overline{x}}}$	Abréviation de $\Rightarrow$;
(5) $x \vee \overline{x} \Rightarrow x \vee \overline{\overline{\overline{x}}}$	Règle IV ;
(6) $x \vee \overline{x}$	Théorème 4 ;
(7) $x \vee \overline{\overline{\overline{x}}}$	Modus Ponens (6, 5) ;
(8) $\beta \vee \overline{\overline{\beta}}$	Substitution $(x := \beta)$;
(9) $\overline{\overline{\beta}} \vee \beta$	Règle III ;
(10) $\overline{\overline{\beta}} \Rightarrow \beta$	Abréviation $\Rightarrow$.

□

2. Montrons que : $\vdash \beta \Rightarrow \overline{\overline{\beta}}$.

Preuve :

(1) $x \vee \overline{x}$	Théorème 4 ;
(2) $\overline{\beta} \vee \overline{\overline{\beta}}$	Substitution $(x := \overline{\beta})$ dans (1) ;
(3) $\beta \Rightarrow \overline{\overline{\beta}}$	Abréviation $\Rightarrow$.

□

3. Montrons que : $\vdash \overline{\alpha} \Rightarrow (\alpha \Rightarrow \beta)$.

Preuve :

(1)] $x \Rightarrow (x \vee y)$	$(H.A)_2$;
(2)] $\overline{\alpha} \Rightarrow (\overline{\alpha} \vee \beta)$	Substitution $(x := \overline{\alpha}, y := \beta)$ dans (1) ;
(3)] $\overline{\alpha} \Rightarrow (\alpha \Rightarrow \beta)$	Abréviation $\Rightarrow$.

□

4. Montrons que : $\vdash (\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow [(\overline{\beta} \Rightarrow \alpha) \Rightarrow \beta]$.

Preuve :

(1) $(x \Rightarrow y) \Rightarrow [(z \vee x) \Rightarrow (z \vee y)]$	$(H.A)_4$;
(2) $(\alpha \Rightarrow \beta) \Rightarrow [(\beta \vee \alpha) \Rightarrow (\beta \vee \beta)]$	Substitution $(x := \alpha, y := \beta, z := \beta)$;
(3) $(x \Rightarrow y) \Leftrightarrow (\overline{y} \Rightarrow \overline{x})$	Théorème 5 ;
(4) $\Big[(x \Rightarrow y) \Rightarrow (\overline{y} \Rightarrow \overline{x})\Big] \wedge \Big[(\overline{y} \Rightarrow \overline{x}) \Rightarrow (x \Rightarrow y)\Big]$	Définition $\Leftrightarrow$;
(5) $\Big[(\overline{y} \Rightarrow \overline{x}) \Rightarrow (x \Rightarrow y)\Big]$	Règle V ;
(6) $(\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow (\alpha \Rightarrow \beta)$	Substitution $(x := \alpha, y := \beta)$;
(7) $(\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow \Big[(\beta \vee \alpha) \Rightarrow (\beta \vee \beta)\Big]$	Règle S (2, 6) ;
(8) $(x \vee x) \Rightarrow x$	$(H.A)_1$;
(9) $(\beta \vee \beta) \Rightarrow \beta$	Substitution $(x := \beta)$ dans (8) ;
(10) $\Big[\overline{(\beta \vee \alpha)} \vee (\beta \vee \beta)\Big] \Rightarrow \Big[\overline{(\beta \vee \alpha)} \vee \beta\Big]$	Règle IV ;
(11) $\Big[(\beta \vee \alpha) \Rightarrow (\beta \vee \beta)\Big] \Rightarrow \Big[(\beta \vee \alpha) \Rightarrow \beta\Big]$	Abréviation $\Rightarrow$;
(12) $(\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow \Big[(\beta \vee \alpha) \Rightarrow \beta\Big]$	Règle S(7, 11) ;
(13) $(\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow \Big[(\overline{\beta} \Rightarrow \alpha) \Rightarrow \beta\Big]$	Abréviation $\Rightarrow$.

□

5. Montrons que : $\vdash (\alpha \Rightarrow \beta) \Rightarrow (\overline{\beta} \Rightarrow \overline{\alpha})$.

Preuve :

(1) $(x \vee y) \Rightarrow (y \vee x)]$	Théorème 13 ;
(2) $(\overline{\alpha} \vee \beta) \Rightarrow (\beta \vee \overline{\alpha})]$	Substitution $(x := \overline{\alpha}, y := \beta)$;
(2) $(\alpha \Rightarrow \beta) \Rightarrow (\overline{\beta} \Rightarrow \overline{\alpha})$	Abréviation $\Rightarrow$.

□

6. Montrons que : $\vdash \alpha \Rightarrow \Big[\overline{\beta} \Rightarrow \overline{(\alpha \Rightarrow \beta)}\Big]$.

Preuve :

(1) $x \vee (y \vee z) \Leftrightarrow (x \vee y) \vee z$	Théorème 6 ;
(2) $\Big[x \vee (y \vee z) \Rightarrow (x \vee y) \vee z\Big] \wedge \Big[(x \vee y) \vee z \Rightarrow x \vee (y \vee z)\Big]$	Définition $\Leftrightarrow$;
(3) $\Big[(x \vee y) \vee z \Rightarrow x \vee (y \vee z)\Big]$	Règle V ;
(4) $\Big[(\overline{\alpha} \vee \overline{\overline{\beta}}) \vee \overline{(\overline{\alpha} \vee \beta)}\Big] \Rightarrow \overline{\alpha} \vee (\overline{\overline{\beta}} \vee \overline{(\overline{\alpha} \vee \beta)})$	Substitution $(x := \overline{\alpha}, y := \overline{\overline{\beta}}, z := \overline{(\overline{\alpha} \vee \beta)})$.

(5) $\beta \Rightarrow \overline{\overline{\beta}}$	Théorème de la question 2 ;
(6) $(\overline{\alpha} \vee \beta) \Rightarrow (\overline{\alpha} \vee \overline{\overline{\beta}})$	Règle IV ;
(7) $\overline{(\overline{\alpha} \vee \beta)} \vee (\overline{\alpha} \vee \overline{\overline{\beta}})$	Définition $\Rightarrow$;
(8) $(\overline{\alpha} \vee \overline{\overline{\beta}}) \vee \overline{(\overline{\alpha} \vee \beta)}$	Règle III ;
(9) $\overline{\alpha} \vee \Big[\overline{\overline{\beta}} \vee \overline{(\overline{\alpha} \vee \beta)}\Big]$	Modus Ponen (8, 4) ;
(10) $\alpha \Rightarrow \Big[\overline{\overline{\beta}} \vee \overline{(\overline{\alpha} \vee \beta)}\Big]$	Définition de $\Rightarrow$;
(11) $\alpha \Rightarrow \Big[\overline{\beta} \Rightarrow \overline{(\overline{\alpha} \vee \beta)}\Big]$	Définition de $\Rightarrow$;
(12) $\alpha \Rightarrow \Big[\overline{\beta} \Rightarrow \overline{(\alpha \Rightarrow \beta)}\Big]$	Définition de $\Rightarrow$.

□

7. Montrons que : $\vdash (\alpha \Rightarrow \beta) \Rightarrow \Big[(\overline{\alpha} \Rightarrow \beta) \Rightarrow \beta\Big]$.

Preuve :

(1) $(\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow \Big[(\overline{\beta} \Rightarrow \alpha) \Rightarrow \beta\Big]$	Théorème démontré dans la question 4 ;
(2) $(\alpha \Rightarrow \beta) \Rightarrow (\overline{\beta} \Rightarrow \overline{\alpha})$	Théorème démontré dans la question 5 ;
(3) $(\alpha \Rightarrow \beta) \Rightarrow \big[(\overline{\beta} \Rightarrow \alpha) \Rightarrow \beta\big]$	Règle S(1,2) ;
(4) $(\overline{y} \Rightarrow \overline{x}) \Rightarrow (x \Rightarrow y)$	Théorème 5 ;
(5) $(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow (\overline{\beta} \Rightarrow \alpha)$	Substitution $x := \overline{\beta}, y := \alpha$;
(6) $(\beta \Rightarrow \overline{\overline{\beta}})$	Théorème de la question 2 ;
(7) $(\overline{\overline{\alpha}} \vee \beta) \Rightarrow (\overline{\overline{\alpha}} \vee \overline{\overline{\beta}})$	Règle IV ;
(8) $(\overline{\alpha} \Rightarrow \beta) \Rightarrow (\overline{\alpha} \Rightarrow \overline{\overline{\beta}})$	Abréviation de $\Rightarrow$;
(9) $(x \Rightarrow y) \Rightarrow (\overline{y} \Rightarrow \overline{x})$	Théorème 5 ;
(10) $\big[\overline{(\overline{\alpha} \Rightarrow \beta)} \Rightarrow (\overline{\alpha} \Rightarrow \overline{\overline{\beta}})\big] \Rightarrow \big[\overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})} \Rightarrow \overline{(\overline{\alpha} \Rightarrow \beta)}\big]$	sub $x := (\overline{\alpha} \Rightarrow \beta); y := (\overline{\alpha} \Rightarrow \overline{\overline{\beta}})$;
(11) $(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow \overline{(\overline{\alpha} \Rightarrow \beta)}$	Modus Ponens (8,10) ;
(12) $\big[\beta \vee \overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})}\big] \Rightarrow \big[\beta \vee \overline{(\overline{\alpha} \Rightarrow \beta)}\big]$	Règle IV ;
(13) $(x \vee y) \Rightarrow (y \vee x)$	$(H.A.)_3$;
(14) $\big[\overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})} \vee \beta\big] \Rightarrow \big[\beta \vee \overline{(\overline{\alpha} \vee \overline{\overline{\beta}})}\big]$	Sub $x := (\overline{\alpha} \Rightarrow \overline{\overline{\beta}}); y := \beta$;
(15) $\big[\overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})} \vee \beta\big] \Rightarrow \big[\beta \vee \overline{(\overline{\alpha} \Rightarrow \beta)}\big]$	Règle S(14, 12) ;
(16) $\big[(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow \beta\big] \Rightarrow \big[\beta \vee \overline{(\overline{\alpha} \Rightarrow \beta)}\big]$	Abréviation $\Rightarrow$.
(17) $\big[\beta \vee \overline{(\overline{\alpha} \Rightarrow \beta)}\big] \Rightarrow \big[\overline{(\overline{\alpha} \Rightarrow \beta)} \vee \beta\big]$	Sub $(x := \beta; y := \overline{(\overline{\alpha} \Rightarrow \beta)})$ dans $(H.A.)_3$;
(18) $\big[(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow \beta\big] \Rightarrow \big[\overline{(\overline{\alpha} \Rightarrow \beta)} \vee \beta\big]$	Règle S(16, 17) ;
(19) $\big[(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow \beta\big] \Rightarrow \big[(\overline{\alpha} \Rightarrow \beta) \Rightarrow \beta\big]$	Abréviation $\Rightarrow$;
(20) $\big[(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow (\overline{\beta} \Rightarrow \alpha)\big] \Rightarrow \big[\overline{(\overline{\beta} \Rightarrow \alpha)} \Rightarrow (\overline{\alpha} \Rightarrow \overline{\overline{\beta}})\big]$	Sub $(x := (\overline{\alpha} \Rightarrow \overline{\overline{\beta}}), y := (\overline{\beta} \Rightarrow \alpha)$;

(21) $\left[\overline{(\overline{\beta} \Rightarrow \alpha)} \Rightarrow \overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})}\right]$	Modus Ponens (5, 20) ;
(22) $\left[\beta \vee \overline{(\overline{\beta} \Rightarrow \alpha)}\right] \Rightarrow \left[\beta \vee \overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})}\right]$	Règle IV ;
(23) $\left[\overline{(\overline{\beta} \Rightarrow \alpha)} \vee \beta\right] \Rightarrow \left[\beta \vee \overline{(\overline{\beta} \Rightarrow \alpha)}\right]$	Sub $(x := \overline{(\overline{\beta} \Rightarrow \alpha)}; y := \beta)$ dans $(H.A.)_3$;
(24) $\left[\overline{(\overline{\beta} \Rightarrow \alpha)} \vee \beta\right] \Rightarrow \left[\beta \vee \overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})}\right]$	Règle S(22, 23) ;
(25) $\left[\beta \vee \overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})}\right] \Rightarrow \left[\overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})} \vee \beta\right]$	Substitution $(x := \beta; y := \overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})})$ dans $(H.A.)_3$;
(26) $\left[\overline{(\overline{\beta} \Rightarrow \alpha)} \vee \beta\right] \Rightarrow \left[\overline{(\overline{\alpha} \Rightarrow \overline{\overline{\beta}})} \vee \beta\right]$	Règle S(24, 25) ;
(27) $\left[(\overline{\beta} \Rightarrow \alpha) \Rightarrow \beta\right] \Rightarrow \left[(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow \beta\right]$	Abréviation $\Rightarrow$;
(28) $(\alpha \Rightarrow \beta) \Rightarrow \left[(\overline{\alpha} \Rightarrow \overline{\overline{\beta}}) \Rightarrow \beta\right]$	Règle S(3, 27) ;
(29) $(\alpha \Rightarrow \beta) \Rightarrow \left[(\overline{\alpha} \Rightarrow \beta) \Rightarrow \beta\right]$	Règle S(28, 19).

□

Corrigé de l'exercice 2.3. On a le système d'axiomes suivant :

$$\begin{cases} A_1 : \alpha \Rightarrow (\beta \Rightarrow \alpha); \\ A_2 : \Big[\alpha \Rightarrow (\beta \Rightarrow \gamma)\Big] \Rightarrow \Big[(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)\Big]; \\ A_3 : (\overline{\beta} \Rightarrow \overline{\alpha}) \Rightarrow (\alpha \Rightarrow \beta); \\ \text{Modus Ponens} : \vdash \alpha \text{ et } \vdash \alpha \Rightarrow \beta \text{ alors, } \vdash \beta. \end{cases}$$

1. Montrons que : $\vdash \alpha$, on déduit $\vdash (\beta \Rightarrow \alpha)$ (qu'on nommera après $\mathcal{R}_1$).

Preuve :

(1) $\vdash \alpha$	Hypothèse ;
(2) $\alpha \Rightarrow (\beta \Rightarrow \alpha)$	A_1 ;
(3) $(\beta \Rightarrow \alpha)$	Modus Ponens (1, 2).

□

2. Montrons que de $\vdash (\alpha \Rightarrow \beta)$, et $\vdash (\beta \Rightarrow \gamma)$, on déduit $\vdash (\alpha \Rightarrow \gamma)$ (qu'on nommera après $\mathcal{R}_2$).

Preuve :

(1) $(\beta \Rightarrow \gamma)$	Hypothèse ;
(2) $\Big[\alpha \Rightarrow (\beta \Rightarrow \gamma)\Big]$	Application du résultat de la question 1 du même exercice ($\mathcal{R}_1$) ;
(3) $\Big[\alpha \Rightarrow (\beta \Rightarrow \gamma)\Big] \Rightarrow \Big[(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)\Big]$	A_2 ;
(4) $(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)$	Modus Ponens (3, 2) ;
(5) $\alpha \Rightarrow \beta$	Hypothèse ;
(6) $\alpha \Rightarrow \gamma$	Modus Ponens (4, 3).

□

3. Montrons que de $\vdash \Big[\alpha \Rightarrow (\beta \Rightarrow \gamma)\Big]$, on déduit $\vdash \beta \Rightarrow (\alpha \Rightarrow \gamma)$ (qu'on nommera après $\mathcal{R}_3$).

Preuve :

(1)]	$\Big[\alpha \Rightarrow (\beta \Rightarrow \gamma)\Big]$	Hypothèse ;
(2)]	$\Big[\alpha \Rightarrow (\beta \Rightarrow \gamma)\Big] \Rightarrow \Big[(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)\Big]$	A_2 ;
(3)]	$\Big[(\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)\Big]$	Modus Ponens (1, 2) ;
(4)]	$\beta \Rightarrow (\alpha \Rightarrow \beta)$	A_1.
(5)]	$\beta \Rightarrow (\alpha \Rightarrow \gamma)$	$\mathcal{R}_2$ appliquée à (4) et (3).

□

Corrigé de l'exercice 2.4. Démontrons en utilisant les résultats de l'exercice précédent les théorèmes suivants :

1. $(q \Rightarrow r) \Rightarrow \Big[(p \Rightarrow q) \Rightarrow (p \Rightarrow r)\Big]$. C'est le théorème 17 (de la liste des théorèmes) qu'on va démontrer avec les axiomes de l'exercice 3.

Preuve :

(1)	$\Big[p \Rightarrow (q \Rightarrow r)\Big] \Rightarrow \Big[(p \Rightarrow q) \Rightarrow (p \Rightarrow r)\Big]$	Substitution $(\alpha := p, \beta := q, \gamma := r)$ dans A_2 ;
(2)	$(q \Rightarrow r) \Rightarrow \Big[p \Rightarrow (q \Rightarrow r)\Big]$	Substitution $(\alpha := (q \Rightarrow r), \beta := p$ dans A_1 ;
(3)	$(q \Rightarrow r) \Rightarrow \Big[(p \Rightarrow q) \Rightarrow (p \Rightarrow r)\Big]$	$\mathcal{R}_2$ appliquée à (2) et (1).

□

2. $(p \Rightarrow q) \Rightarrow \Big[(q \Rightarrow r) \Rightarrow (p \Rightarrow r)\Big]$. C'est le théorème 16 (de la liste des théorèmes) qu'on va démontrer avec les axiomes de l'exercice 3.

Preuve :

(1)	$(q \Rightarrow r) \Rightarrow \Big[(p \Rightarrow q) \Rightarrow (p \Rightarrow r)\Big]$	Théorème démontré précédemment dans la question 1 ;
(2)	$(p \Rightarrow q) \Rightarrow \Big[(q \Rightarrow r) \Rightarrow (p \Rightarrow r)\Big]$	$\mathcal{R}_3$ appliquée à (1).

□

Chapitre 3

Le langage du calcul des prédicats du premier ordre

3.1 Introduction

Le calcul propositionnel reste très limité, et ne permet essentiellement que d'exprimer des opérations booléennes sur des propositions. Si l'on veut pouvoir raisonner sur des assertions mathématiques, il nous faut autoriser des constructions plus riches.
Ainsi la formule $\forall x \in \mathbb{N}, x \leq x2$ représente toutes les formules $0 \leq 0$, $1 \leq 1$, $2 \leq 4$, $3 \leq 9$,...

Un tel énoncé n'est pas capturé par la logique propositionnelle. Tout d'abord par ce qu'il utilise des prédicats comme $x \in \mathbb{N}$ dont la valeur de vérité dépend d'une variable x, ce qui n'est pas possible en logique propositionnelle. Par ailleurs, on utilise ici des quantificateurs comme $\forall, \exists$ qui ne sont pas présents en logique propositionnelle.

L'énoncé précédent est un exemple de formule du calcul des prédicats du *premier ordre*. Dans ce cours, on ne parlera que de logique du *premier ordre*. La terminologie *premier ordre* fait référence au fait que les quantifications existentielles et universelles ne sont autorisées que sur les variables.

Un énoncé du *second ordre*, on parle plus généralement d'*ordre supérieur*, serait un énoncé où l'on autoriserait les quantifications sur les fonctions ou des relations : par exemple, on peut écrire $\neg\forall f(\exists x(f(x) > f(x+1)))$ pour signifier qu'il n'existe pas de suite infiniment décroissante. On ne cherchera pas à comprendre la théorie derrière ce type d'énoncé, car on le verra, les problèmes et les difficultés avec le premier ordre sont déjà suffisamment nombreux.

L'objectif de ce chapitre est alors de définir la logique du premier ordre. Comme pour la logique propositionnelle, on va le faire en parlant d'abord de la syntaxe, c'est-à-dire comment écrire les formules, puis de leur sémantique.

Le calcul des prédicats, reste le formalisme le plus courant pour exprimer des propriétés mathématiques. C'est aussi un formalisme très utilisé en informatique pour décrire les objets.

3.2 Définitions

Définition 3.1. 1. En littérature, un prédicat est ce qui est affirmé d'un sujet ou est dit lui appartenir. (Sagesse/sage est prédicat dans La sagesse appartient à Socrate ou dans Socrate est sage.)
2. En logique mathématique, un prédicat est un moule à propositions. C'est un énoncé qui est syntaxiquement correct, il est sémantiquement correct mais sa valeur de vérité dépend de l'objet. Ainsi, le prédicat "x est premier" dépend de la valeur de l'entier x.
3. On peut avoir un prédicat à une variable $P(x)$ (dans ce cas, on parle d'une propriété de l'objet x), un prédicat à deux variables (ex : $x > y$, dans ce cas, c'est une relation entre l'objet x et l'objet y) ou encore un prédicat à n variables (On dit alors un prédicat n-aire).

3.3 Le langage des prédicats du premier ordre

3.3.1 Alphabet

Il est formé :
- Des connecteurs logiques : $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$;
- Des quantificateurs : $\forall, \exists$;
- D'un ensemble dénombrable de symboles de variables : $x, y, z, \ldots$;
- D'un ensemble dénombrable éventuellement vide de symboles de constantes : $a, b, e, \ldots$;
- D'un ensemble dénombrable éventuellement vide de symboles de fonctions : $f_0, f_1, \ldots$;
- D'un ensemble dénombrable de symboles de prédicats : $P_1, P_2, Q, \ldots$;
- Des symboles auxiliaires : $(,)$.

3.3.2 Les expressions du langage

– **Les termes**

1. Toute constante est un terme ;
2. Toute variable est un terme ;
3. Si f est un symbole de fonction à n arguments et $t_1, t_2, \ldots, t_n$ sont des termes, alors $f(t_1, t_2, \ldots, t_n)$ est un terme ;
4. Rien d'autres n'est un terme, s'il n'est pas obtenu en vertus des règles 1, 2 et 3.

– **Les formules**

1. Une variable propositionnelle est une formule ;
2. Si $t_1, t_2, \ldots, t_n$ sont des termes et P un prédicat à n variables, alors $P(t_1, t_2, \ldots, t_n)$ est une formule ;
3. Si α et β sont des formules, alors $\neg\alpha, \alpha \wedge \beta, \alpha \vee \beta, \alpha \Rightarrow \beta, \alpha \Leftrightarrow \beta$ sont aussi des formules ;
4. Si α est une formule et x une variable, alors $\forall x\alpha$ et $\exists x\alpha$ sont des formules ;
5. Rien n'est une formule, s'il n'est pas obtenu en vertus des règles 1, 2,3 et 4.

3.3.3 Priorité des connecteurs

Les connecteurs et les quantificateurs sont appliqués dans l'ordre suivant :

$$\neg, \wedge, \vee, \forall, \exists, \Rightarrow, \Leftrightarrow$$

Exemple 3.3.1.

$$\forall x\ P(x) \vee \exists y Q(y) \wedge P(x)$$

se lit

$$\forall x\ \ (P(x) \vee \exists y\ (Q(y) \wedge P(x)))$$

3.3.4 Champ d'un quantificateur

Le Champ d'un quantificateur est la partie de la formule couverte par un quantificateur.

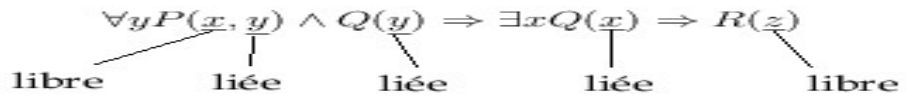
$$\begin{array}{ll} \forall x\ \underline{\alpha \wedge \beta} & \exists x\ \underline{\alpha \wedge \beta} \\ \forall x\ \underline{\alpha \vee \beta} & \exists x\ \underline{\alpha \vee \beta} \\ \forall x\ \underline{\alpha} \Rightarrow \beta & \exists x\ \underline{\alpha} \Rightarrow \beta \\ \forall x\ \underline{(\alpha \Rightarrow \beta)} & \exists x\ \underline{(\alpha \Rightarrow \beta)} \end{array}$$

3.3.5 Variable libre et variable liée

- Dans une formule α, l'occurrence d'une variable x est liée si elle se trouve dans le champ d'un quantificateur Qx ; sinon elle est libre.
- Une variable x est libre dans une formule α s'il existe dans α une occurrence libre de x.
- Une variable x est liée dans une formule α s'il existe dans α une occurrence liée de x.

Exemple 3.3.2. Soit α la formule suivante

$$\forall y P(x, y) \wedge Q(y) \Rightarrow \exists x Q(x) \Rightarrow R(z)$$



3.3.6 Formule close (fermée

Une formule α est dite close (ou fermée), si et seulement si, α ne possède pas de variables libres.

3.4 Sémantique de la logique des prédicats du premier ordre

En calcul propositionnel, il existe des moyens algorithmiques relativement efficaces pour déterminer si une formule est satisfiable ou est une tautologie. En calcul des prédicats, nous ne pouvons pas dire d'une formule qu'elle est vraie ou fausse si nous ne connaissons pas la signification de chacun des symboles qui apparaissent dans la formule.

3.4.1 Interprétation

Etant donné un langage $\mathfrak{L}$ du premier ordre, une interprétation I sur ce langage, est une fonction de domaine D non vide qui assigne :

- à chaque symbole de prédicat n-aire P, une relation n-aire

$$I(P) : D^n \rightarrow \{0, 1\};$$

– à chaque symbole de fonction f à n arguments $(n > 0)$, une opération sur les éléments du domaine de l'interprétation

$$I(f) : D^n \to D;$$

– à chaque symbole de constante a_i un élément

$$I(a_i) = d_i,\ d_i \in D.$$

3.4.2 Valuation

Etant donné un langage $\mathfrak{L}$ du premier ordre et une interprétation I de domaine D sur ce langage, une valuation est une fonction qui associe à chaque variable un élément de D.

3.4.3 Interprétation d'un terme

On désigne par $I(t)_v$ l'élément de D associé au terme t par l'interprétation I de domaine D et la valuation V sur ce domaine. Cet élément est défini comme suit :

– Si $t = c$, alors $I(t)_v = I(c)_v = I(c)$, (c est une constante) ;
– Si $t = x_i$, alors $I(t)_v = I(x_i)_v = V(x_i)$, ($x_i$ est une variable) ;
– Si $t = f(t_1, t_2, \ldots, t_n)$, alors $I(t)_v = I(f)(I(t_1)_v, I(t_2)_v, \ldots, I(t_n)_v)$, ($f$ est un symbole de fonction et $t_1, t_2, \ldots, t_n$ des termes).

3.4.4 Interprétation d'une formule

Etant donné un langage $\mathfrak{L}$ du premier ordre et une interprétation I de domaine D et une valuation V sur ce domaine. $I(\alpha)_v$ d'une formule α du premier ordre est définie comme suit :

1. Si α est une formule atomique, alors :

$$I(\alpha)_v = I(P(t_1, t_2, \ldots, t_n))_v = I(P)(I(t_1)_v, I(t_2)_v, \ldots, I(t_n)_v);$$

2. Si $\alpha = \overline{\beta}$, alors :

$$I(\alpha)_v = I(\overline{\beta})_v = \overline{I(\beta)_v};$$

3. Si $\alpha = \beta_1 \star \beta_2$ avec $\star \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, alors :

$$I(\alpha)_v = I(\beta_1)_v \star I(\beta_2)_v.$$

3.4.5 Satisfiablité d'une formule

Etant donnés un langage $\mathfrak{L}$ et une interprétation I. Une valuation V satisfait une formule α, si et seulement si, après substitution de l'élément du domaine de I associé par V à chaque variable libre de α, on obtient une proposition vraie pour l'interprétation considérée. Et on note

$$I \models \alpha_v.$$

Exemple 3.4.1. Soit la formule

$$\beta \equiv P\left(f(x,y),y\right).$$

On se donne l'interprétation I de domaine $D = \mathbb{N}$, telle que $I(P) = " > "$, $I(f) = " - "$, et la valuation V telle que $V(x) = 4$ et $V(y) = 1$ qui satisfait β pour I. Donc :

$$I \models \beta_v.$$

Alors que la valuation V' telle que $V'(x) = 4$ et $V'(y) = 3$, ne satisfait pas la formule β pour I.

$$I \not\models \beta_v.$$

Définition 3.4.1. Une formule α est *satisfiable*, si et seulement si, il existe une interprétation I pour laquelle il existe au moins une valuation qui satisfait α.

Exemple 3.4.2. La formule β ci-dessus est satisfiable.

3.4.6 Modèle d'une formule

Définition 3.4.2. Une formule α est vraie pour une interprétation I et on note $I \models \alpha$, si et seulement si, toute valuation satisfait α pour l'interprétation I. Dans ce cas, I est appelée *modèle* de α. Autrement dit :

$$I \models \alpha \Leftrightarrow (\text{quel que soit } V,\ I \models \alpha_v).$$

Exemple 3.4.3. Soit α la formule

$$P\left(f(x,y),x\right).$$

L'interprétation I de domaine $D = \mathbb{N}$, $I(P) = " > "$, $I(f) =$ "le est successeur de x" est un modèle de α. Donc $I \models \alpha$.

Définition 3.4.3. Une formule α est fausse pour une interprétation I si et seulement si, aucune valuation de I ne satisfait α.

Exemple 3.4.4. Soit α la formule

$$P\left(f(x,y),x\right).$$

Et soit l'interprétation I de domaine $D = \mathbb{N}$, $I(P) = " < "$, $I(f) = " + "$. Aucune valuation de D ne satisfait α pour I. Donc α est fausse pour I.

3.4.7 Formule valide

Une formule α est *valide* et on note $\models \alpha$, si et seulement si, α est vraie pour toutes les interprétations. Toute interprétation est modèle pour α. Autrement dit

$$\models \alpha \Leftrightarrow (\text{quel que soit } I, \text{quel que soit } V, I \models \alpha_v).$$

Pour montrer qu'une formule α est valide, on procède généralement par l'absurde. On suppose l'existence d'une interprétation I et d'une valuation v, telles que $I \not\models \alpha_v$ et on arrive à une contradiction.

Exemple 3.4.5. Montrons que $\models \overline{P(x)} \vee P(x)$.
Supposons le contraire, i.e. qu'il existe une interprétation I et une valuation V telles que $I \not\models \left(\overline{P(x)} \vee P(x)\right)_v$
i.e $\exists I, \exists V \ / I \models \overline{\left(\overline{P(x)} \vee P(x)\right)_v}$;
$\exists I, \exists V \ / I \models \left(P(x) \wedge \overline{P(x)}\right)_v$;
$\exists I, \exists V \ / I \models (P(x))_v$ et $I \models \left(\overline{P(x)}\right)_v$;
$\exists I, \exists V \ / I \models (P(x))_v$ et $I \not\models (P(x))_v$ d'où une contradiction.
Donc, on a bien $\models \overline{P(x)} \vee P(x)$.

Remarque 3.4.1. Pour montrer qu'une formule n'est pas valide, il suffit de trouver un contre exemple.

3.4.8 Satisfiabilité d'un ensemble de formules

Un ensemble de formules $\Gamma = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ est satisfiable, si et seulement si, il existe une interprétation I et une valuation V, telles que $I \models (\alpha_1)_v, I \models (\alpha_2)_v, \ldots, I \models (\alpha_n)_v$.

Exemple 3.4.6. $\Gamma = \{P(x,y), M(x,y), E(x,y)\}$.
Soit I l'interprétation de domaine $D = \{1,2,6\}$, telles que $I(P) =$ ".est diviseur de.", $I(M) =$ ". est multiple de." et $I(E) =$ ".est égal à.". Pour la valuation $V(x) = V(y) = 1$ l'ensemble Γ est satisfiable.

3.4.9 Modèle d'un ensemble de formules

Une interprétation I est un modèle d'un ensemble de formules Γ, si et seulement si, I est un modèle de chacune des formules de Γ.

3.4.10 Conséquence logique

Une formule β est une conséquence logique d'un ensemble de formules Γ (et on note $(\Gamma \models \beta)$), si et seulement si, pour toute interprétation, toute valuation qui satisfait chacune des formule de Γ, satisfait aussi β. Tout modèle de Γ est aussi un modèle de β.

3.4.11 Renommage

Soit α une formule du calcul des prédicats du premier ordre. Et soit y une variable n'apparaissant pas dans α.
Soit x une variable liée de α. Le remplacement de x par y dans α est appelé renommage. L'opération est faite pour distinguer les variables libres des variables liées et faire en sorte qu'une variable ne soit concernée que par un seul cuantificateur.

Exemple 3.4.7. Soit la formule

$$\alpha_1 \equiv (\forall x \exists y P(x,y) \Rightarrow P(x,z)) \vee (\exists x R(x)) \wedge (\forall y P(x,y)).$$

Après renommage on aura la formule

$$\alpha_2 \equiv (\forall u \exists y P(u,y) \Rightarrow P(x,z)) \vee (\exists v R(v)) \wedge (\forall t P(x,t)).$$

On a

$$\alpha_1 \equiv \alpha_2.$$

Propriété 3.4.1.

$$\forall x \alpha \equiv \alpha, \text{ si } x \text{ n'apparaît pas libre dans } \alpha.$$

$$\exists x \alpha \equiv \alpha, \text{ si } x \text{ n'apparaît pas libre dans } \alpha.$$

3.5 Normalisation

Les formes normales (conjonctives et disjonctives) permettent de simplifier l'étude de la satisfiabilité et la validité en calcul propositionnel. En calcul des prédicats, cette mise en forme se fait en quatres étapes :

1. Mise sous forme prénexe (déplacement de tous les quantificateurs au début de la formule) ;
2. Skolemisation (suppression des $\exists$) ;
3. Mise en forme normale conjonctive ;
4. Mise en forme clausale (suppression des $\forall$) ;

3.5.1 Forme prénexe

Une formule est dite en forme prénexe si tous ses quantificateurs apparaissent au début. Ainsi, la formule est composée de deux parties, la partie quantificateur (au début) et la matrice. Il est toujours possible de transformer une formule en une formule équivalente sous forme prénexe. Pour cela, on applique autant de fois que nécessaire les équivalences suivantes :

$$\overline{\forall x \alpha} \equiv \exists x \overline{\alpha};$$

$$\overline{\exists x \alpha} \equiv \forall x \overline{\alpha};$$

$$(\forall x \alpha) \wedge \beta \equiv \forall x (\alpha \wedge \beta) \ x \text{ n'apparaît pas libre dans } \beta;$$

$$(\forall x \alpha) \vee \beta \equiv \forall x (\alpha \vee \beta) \ x \text{ n'apparaît pas libre dans } \beta;$$

$$(\exists x \alpha) \wedge \beta \equiv \exists x (\alpha \wedge \beta) \ x \text{ n'apparaît pas libre dans } \beta;$$

$$(\exists x \alpha) \vee \beta \equiv \exists x (\alpha \vee \beta) \ x \text{ n'apparaît pas libre dans } \beta;$$

$$\alpha \wedge (\forall x \beta) \equiv \forall x (\alpha \wedge \beta) \ x \text{ n'apparaît pas libre dans } \alpha;$$

$$\alpha \vee (\forall x \beta) \equiv \forall x (\alpha \vee \beta) \ x \text{ n'apparaît pas libre dans } \alpha;$$

$$\alpha \wedge (\exists x \beta) \equiv \exists (\alpha \wedge \beta) \ x \text{ n'apparaît pas libre dans } \alpha;$$

$$\alpha \vee (\exists x \beta) \equiv \exists x (\alpha \vee \beta) \ x \text{ n'apparaît pas libre dans } \alpha;$$

$$\forall x \alpha \Rightarrow \beta \equiv \exists x (\alpha \Rightarrow \beta) \ x \text{ n'apparaît pas libre dans } \beta;$$

$$\exists x \alpha \Rightarrow \beta \equiv \forall x (\alpha \Rightarrow \beta) \ x \text{ n'apparaît pas libre dans } \beta;$$

$$\alpha \Rightarrow \forall x\beta \equiv \forall x(\alpha \Rightarrow \beta) \; x \text{ n'apparaît pas libre dans } \alpha;$$
$$\alpha \Rightarrow \exists\beta \equiv \exists(\alpha \Rightarrow \beta) \; x \text{ n'apparaît pas libre dans } \alpha.$$

Exemple 3.5.1. Soit la formule

$$\alpha \equiv \forall x \forall y E(x,y) \Rightarrow \exists z A(x,z).$$
$$\alpha \equiv \forall t \forall y E(t,y) \Rightarrow \exists z A(x,z);$$
$$\alpha \equiv \exists t \exists y \left(E(t,y) \Rightarrow \exists z A(x,z)\right);$$
$$\alpha \equiv \exists t \exists y \exists z \left(E(t,y) \Rightarrow A(x,z)\right).$$

3.5.2 Forme de Skolem (Skolemisation)

Soit α une formule ayant la forme prénexe. Transformons α ainsi :
On remplace chaque variable, quantifiée par un existentiel, par une fonction des variables quantifiées universellement avant, et on supprime les quantificateurs existentiels. On convient de n'introduire que des fonctions nouvelles et différentes. La formule obtenue est la *skolémisée* de α, elle notée α^{sko}.

La skolémisée d'une formule ne lui est pas en général équivalente, néanmoins :
- tout modèle de la formule skolémisée est modèle de la formule initiale.
- tout modèle de la formule initiale peut être étendu en un modèle de la formule skolémisée, obtenu en conservant les interprétations des symboles de la formule initiale, et en interprétant correctement les nouveaux symboles de fonction introduits pas la skolemisation.
- une formule close et sa forme de Skolem sont dites équisatisfaisables : si l'une possède un modèle, l'autre également et réciproquement.

Exemple 3.5.2. Reprenons la formule précédente (sous forme prénexe) $\alpha \equiv \exists t \exists y \exists z \left(E(t,y) \Rightarrow A(x,z)\right)$, alors $\alpha^{sko} \equiv E(a,b) \Rightarrow A(x,c)$ où a, b, c sont des constantes.

Exemple 3.5.3. Soit

$$\beta \equiv \forall x \exists u \forall y \exists z \left(P(x,u) \Rightarrow (Q(u,y) \wedge R(y,z))\right).$$

On a

$$\beta^{sko} \equiv \forall x \forall y \left(P(x,f(x)) \Rightarrow (Q(f(x),y) \wedge R(y,g(x,y)))\right.$$

Théorème 3.5.1. *Une formule α est satisfiable si et seulement si α^{sko} est satisfiable.*

3.5.3 Forme clausale

Une fois que la formule a été skolémisée, il ne reste que des variables quantifiées universellement. On peut donc se passer de l'écriture explicite des quantificateurs. La formule restante est composée d'atomes et de connecteurs logiques. On peut alors appliquer la même technique qu'en logique propositionnelle pour la mettre en forme normale conjonctive, puis sous forme d'un ensemble de clauses.

Losqu'une formule est sous forme clausale, on peut ensuite la décomposer en appliquant la règle $\forall x(\alpha \wedge \beta) \equiv (\forall x\alpha) \wedge (\forall x\beta)$

Exemple 3.5.4. Si on repart de la formule skolémisée

$$\beta^{sko} \equiv \forall x \forall y \left(P(x, f(x)) \Rightarrow (Q(f(x), y) \wedge R(y, g(x, y)))\right),$$

l'élimination des quantificateurs universels donne

$$\left(P(x, f(x)) \Rightarrow (Q(f(x), y) \wedge R(y, g(x, y)))\right).$$

En appliquant la transformation de $\Rightarrow$ vers $\{\neg, \vee\}$ on obtient :

$$\left(\overline{P(x, f(x))} \vee (Q(f(x), y) \wedge R(y, g(x, y))\right),$$

Puis, par distributivité, on aura :

$$\left(\overline{P(x, f(x))} \vee Q(f(x), y)\right) \wedge \left(\overline{P(x, f(x))} \vee R(y, g(x, y))\right).$$

Et donc on a deux clauses :

1. $\left(\overline{P(x, f(x))} \vee Q(f(x), y)\right)$;
2. $\left(\overline{P(x, f(x))} \vee R(y, g(x, y))\right)$.

Définition 3.2. **(Forme clausale)**
Une formule est sous forme clausale si elle est sous forme de Skolem et si sa matrice est sous forme normale conjonctive.

Théorème 3.5.2. *Soit S un ensemble de clauses résultant de la mise sous forme clausale d'une formule α. Alors, α est insatisfiable si et seulement si S est insatisfiable.*

Ce théorème forme la base de nombreux démonstrateurs automatiques utilisant une représentation des formules sous forme de clauses. Il établit que la recherche de l'insatisfiabilité d'une formule α est équivalente à la recherche d'insatisfiabilité de sa représentation sous forme clausale S. Cependant, α et S ne sont pas logiquement équivalentes : seule la satisfiabilité est préservée.

3.6 Complétude et décidabilité

Théorème 3.6.1. ***(Théorème de complétude de Gödel)*** *Le calcul des prédicats est complet : on peut donner un nombre fini de principes (axiomes logiques, schémas d'axiomes logiques et règles de déduction) qui suffisent pour déduire de façon mécanique toutes les formules universellement valide de la logique du premier ordre.*

Théorème 3.6.2. *La logique du premier ordre n'est pas décidable, mais elle est semi-décidable.*

3.7 Conclusion

Bien qu'il existe un système de preuve correct et complet, le calcul des prédicats n'est pas décidable. Si par exemple on considère le calcul des séquents, on ne va pas pouvoir déterminer qu'une formule n'est pas universellement valide car il y a un nombre non borné d'explorations possibles.

Toutefois, puisqu'une preuve est un objets finis et que tous les objets considérés sont dénombrables, et donc énumérables, il est possible d'énumérer toutes les preuves, et donc tous les théorèmes. Le calcul des prédicats est donc semi-décidable : si on veut déterminer si une formule α est universellement valide, il suffit de la comparer avec chacun des théorèmes : le calcul se terminera si α est effectivement un théorème (mais dans un temps non borné), le calcul peut ne pas se terminer mais dans ce cas, on n'a pas la certitude que α n'est pas un théorème. En effet, on ne sait pas si le calcul des théorèmes n'a pas été mené assez loin pour identifier α comme théorème ou si ce calcul ne se terminera pas parce que α n'est pas un théorème.

3.8 Exercices

Exercice 3.1. Traduire les phrases suivantes dans le langage des prédicats du premier ordre :

(a) Tous les chats sont gris ;

(b) Aucun chat n'est gris ;

(c) Les éléphants sont grands et forts ;

(d) Il n'y a pas d'éléphant méchant ;

(e) Certains oiseaux sont des mammifères ;

(f) Il y a des poissons dangereux ;

(g) Il existe des hommes riches comme il existe des hommes pauvres ;

(h) Il sont tous blancs ou tous noirs ;

(i) Un nombre entier est ou pair ou impair ;

(j) Tout flatteur dépend de celui qui l'écoute.

(h) Mon père est mon ami.

Exercice 3.2. Determiner les occurences libres et liées dans les formules suivantes :

1. $\forall z\left((\forall x\alpha(x,y)) \Rightarrow \alpha(z,x)\right)$;
2. $\forall y\alpha(z,y) \Rightarrow \forall z\alpha(z,y)$;
3. $(\forall y\exists x\exists z\beta\left(x,y,f(x,y)\right)) \vee \left(\overline{\forall x\alpha\left(y,g(x)\right)}\right)$.

Pour chaque formule, donner l'ensemble des variables libres et l'ensemble des variables liées.

Exercice 3.3. Soit $L = P, R, f, g, c$ où les symboles de relation sont P unaire et R binaire et les symboles de fonction sont f unaire, g binaire et c symbole de constante. Pour chacune des expressions suivantes, déterminez s'il s'agit d'une formule de L ; ou pas et dans ce cas justifiez.
(1) $\forall(x,y)$, (2) $\alpha(x,y)$, (3) $g(x,y)$, (4) $R(g(x,y))$, (5) $P(R(x,y))$, (6) $x = g(x,y)$, (7) $R(f(x),g(y,c))$, (8) $\forall xR(x,x)$, (9) $\forall x\exists yR(x,x)$, (10) $\exists y(y = c \wedge P(y))$, (11) $\exists x(P(f(x)) \wedge \forall yR(x,y))$, (12) $(\exists xP(f(x)) \wedge \forall yR(x,y))$, (13) $\forall x\forall xP(g(f(x),x))$, (14) $\forall x(P(x) \Rightarrow \exists yR(x,y))$.

Exercice 3.4. Soit E l'ensemble des formules $\{\alpha_1, \alpha_2, \alpha_3\}$ où
$\alpha_1 :$ $\forall x \exists y P(x, y)$;
$\alpha_2 :$ $\forall x P(x, y)$;
$\alpha_3 :$ $\exists y P(x, y)$;
et F la formule $\forall x P(x, y) \wedge \forall y \overline{P(x, y)}$.

1. Montrer que $\alpha_1, \alpha_2, \alpha_3$ sont satisfiables.
2. Pour chacune des formules $\alpha_1, \alpha_2, \alpha_3$, trouver un modèle.
3. Montrer que E est satisfiable.
4. Montrer que $E \nvDash F$.

Exercice 3.5. Soit F la formule :

$$\exists x \forall y R(x) \Rightarrow R(y).$$

1. Trouver un modèle pour$F$.
2. F est-elle valide ?
3. Donner la forme prénexe de F.
4. Donner la forme prénexe de $\overline{F}$
5. Donner la forme Skolem de F.

3.9 Corrigés des exercices

Corrigé de l'exercice 3.1. Le premier élément dans une traduction en logique des prédicats est l'nseble de base. Il spécifie la nature des objets manipulés. Selon l'ensemble de base choisi, l'expression peut changer.
Ainsi la traduction de la phrase "Tous les chats sont gris" sera :

1. $D = \{\text{les chats}\}$, soit le prédicat $G(x)$: "x est gris". On aura la formule $\forall x G(x)$;
2. $D = \{\text{les animaux}\}$, soient les prédicats $C(x)$: "x est un chat" et $G(x)$: "x est gris". On aura la formule $\forall x\,(C(x) \Rightarrow G(x))$;

Corrigé de l'exercice 3.2. Déterminons les occurrences libres et liées des trois formules données :
1 : Pour la formule $\forall \mathbf{z}((\forall \underbrace{x\alpha(x,y)}) \Rightarrow \alpha(\mathbf{z},\mathbf{x}))$, le champs du quantificateur universel relatif à la variable x, $(\forall x)$ est indiqué par une sous-accolade et le champs du quantificateur universel relatif à la variable z, $(\forall z)$ est souligné et il n'y a pas de quantificateur relatif à la variable y, ainsi on constate que :

- la variable x à gauche du connecteur $\Rightarrow$ est liée et celle à droite est libre.
- la variable z est liée tout le temps.
- la variable y est libre,

2 : Pour la formule $\underline{\forall \mathbf{y}\alpha(\mathbf{z},\mathbf{y})} \Rightarrow \underline{\underline{\forall \mathbf{z}\alpha(\mathbf{z},\mathbf{x})}}$, le champs du quantificateur universel relatif à la variable y est souligné par une seule ligne el le champs du quantificateur universel relatif à la variable z est souligné par deux lignes, ainsi on constate que :

- la variable y à gauche du connecteur $\Rightarrow$ est liée et celle à droite est libre.
- la variable z à gauche du connecteur $\Rightarrow$ est libre et celle à droite est liée.

3 : Pour la formule $(\forall \mathbf{y}\exists \underbrace{x\exists z\beta(x,y,f(x,y))}) \vee \overline{\underline{\underline{(\forall \mathbf{x}\alpha(\mathbf{y},\mathbf{g}(\mathbf{x}))}}}$, le champs du quantificateur universel relatif à la variable y est souligné par une seule ligne, le champs du quantificateur existentiel relatif à la variable x à gauche du connecteur $\vee$ est indiqué par une sous-accolade et le champs du quantificateur universel relatif à la variable x à droite du connecteur $\vee$ est souligné par deux lignes, ainsi on constate que :

- la variable y est liée dans toutes ses occurrences.
- la variable x à gauche du connecteur $\vee$ est liée au quantificateur existentiel $(\exists y)$ et la variable x à droite du connecteur $\vee$ est liée au quantificateur universel $(\forall x)$.

- la variable y est libre,

- il n'y a pas de variable z dans la formule donc le quantificateur relatif à cette variable z peut être exclu de cette formule. Ainsi, elle sera équivalente à la formule : $(\forall \mathbf{y} \exists \underbrace{x\beta(x, y, f(x, y))}) \vee (\overline{\underline{\forall \mathbf{x} \alpha(\mathbf{y}, \mathbf{g}(\mathbf{x}))}})$

Corrigé de l'exercice 3.3. Le langage donné est le suivant $L = P, R, f, g, c$ où les symboles des relations (prédicats) sont P unaire et R binaire. Les symboles de fonctions sont f unaire et g unaire. Le symbole c est un symbole de constante.
Pour chacune des expressions données de 1 jusqu'à 14, on déterminera s'il s'agit d'une formule du langage L donné. Si ce n'est pas le cas, justifier pourquoi :

1) $\forall(x, y)$ cette formule n'est pas une formule du langage donné, car il n'y a pas de prédicat dedans alors que le langage donné est un langage d'ordre 1.
2) $\alpha(x, y)$ cette formule n'est pas une formule du langage donné, car il n'y a pas de prédicat dedans alors que le langage donné est un langage d'ordre 1.
3) $g(x, y)$ cette formule n'est pas une formule du langage donné, car il n'y a pas de prédicat dedans alors que le langage donné est un langage d'ordre 1.
4) $R(g(x, y))$ cette formule n'est pas une formule du langage donné car la fonction g est binaire et dans cette formule on lui a associé deux arguments.
5) $P(R(x, y))$ cette formule n'est pas une formule du langage donné, car le langage des prédicats du premier ordre n'autorise pas la composition des prédicats.
6) $x = g(x, y)$ cette formule n'est pas une formule du langage donné car elle contient le connecteur égalité "=" qui n'a aucun sens dans ce langage d'ordre 1.
7) $R(f(x), g(x, c))$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.
8) $\forall x R(x, x)$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.
9) $\forall x \exists y R(x, x)$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.
10) $\exists y(y = c \wedge P(y))$ cette formule n'est pas une formule du langage donné car elle contient le connecteur égalité "=" qui n'a aucun sens dans un langage de premier ordre.
11) $\exists x(P(f(x) \wedge \forall y R(x, y))$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.

12) $(\exists x P(f(x)) \wedge \forall y R(x,y))$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.

13) $\forall x \forall x P(g(f(x),x))$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.

14) $\forall x(P(x) \Rightarrow \exists y R(x,y))$ cette formule est une formule du langage donné, elle vérifie toutes les conditions exigées.

Corrigé de l'exercice 3.4. On a $E = \{\alpha_1, \alpha_2, \alpha_3\}$ avec :

$$\begin{cases} \alpha_1 : \forall x \exists y P(x,y); x \text{ est lée et } y \text{ est liée.} \\ \alpha_2 : \forall x P(x,y); x \text{ est liée et } y \text{ est libre.} \\ \alpha_3 : \exists y P(x,y); x \text{ est libre et } y \text{ est liée.} \end{cases}$$

Soit la formule $F \equiv \forall x P(x,y) \wedge \forall y \overline{P(x,y)}$.

I.) Montrons que $\alpha_1, \alpha_2, \alpha_3$ sont satisfiables :

Pour montrer qu'une formule est satisfiable, il suffit de trouver une interprétation et une valuation pour lesquelles cette formule est vraie.

Remarque : comme solution, Nous allons donner des interprétation et des valuations telles que $\alpha_1, \alpha_2, \alpha_3$ soient satisfiables. Cependant, ces interprétations ne sont pas uniques et vous pouvez trouver d'autres interprétations.

Pour α_1 : Nous proposons l'interprétation I_1 de domaine de base $D_1 = \mathbb{N}$, et on définit le prédicat P : " $\leq$ ". Avec cette interprétation, on a : $\alpha_1 \equiv \forall x \exists y \ (x \leq y)$. On a les deux variables x et y sont liées.

On constate que α_1 est satisfaite tout le temps car pour tout entier, on peut lui trouver un entier qui lui soit supérieur, c'est à dire α_1 est satisfaite pour toutes les valuations de I_1, ainsi I_1 est un modèle, (i.e. $I \models \alpha_1$).

Pour α_2 : Nous proposons l'interprétation I_2 de domaine de base $D_2 = \mathbb{N}^*$, et on définit le prédicat $P(x,y)$: x multiple de y. Avec cette interprétation, on a : $\alpha_2 \equiv \forall x, x$ est un multiple de y. On a la variable x est liée et la variable y est libre. Soit alors valuation $v(y) = 1$, pour cette valuation α_2 est satisfaite car tout entier non nul est un multiple de 1, donc $I_2 \models (\alpha_2)_{v(y=1}$. Cependant, I_2 n'est pas un modèle de α_2. En effet, α_2 n'est pas satisfiable pour toutes les valuations de I_2. Par exemple, la valuation $v(y) = c$ avec $c \neq 1$, α_2 n'est pas satisfaite, i.e. $I_2 \not\models \alpha_2$.

Pour α_3 : Nous proposons l'interprétation I_3 de domaine de base $D_3 = \{2,4,6,8\}$, et on définit le prédicat $P(x,y)$: "x diviseur de y". Donc, pour cette interprétation on

a : $\alpha_3 \equiv \exists y,\ x$ est un diviseur de y. On a la variable x est libre et la variable y est liée. Pour la valuation $v(x) = 2$, on a $I_3(\alpha_3) : \exists y/2$ est un diviseur de y est satisfaite donc $I_3 \models (\alpha_3)_{v(x)=2}$. On constate que pour toutes les valuations possibles de x, la formule α_3 est satisfiable, donc I_3 est un modèle de α_3 (i.e. $I_3 \models \alpha_3$).

II.) Précédemment on a trouvé une interprétation I_1 qui est un modèle pour la formule α_1 et une interprétation I_3 qui est un modèle pour la formule α_3 Maintenant, on propose une interprétation qui soit un modèle pour l'ensemble des trois formules données $E = \{\alpha_1, \alpha_2, \alpha_3\}$.

Soit l'interprétation I' de domaine de base $D' = \{1\}$ et telle que $P(x, y) : "x \leq y"$. avec $v(x) = v(y) = 1$. Pour cette interprétation il est facile de vérifier que : $I' \models \alpha_1,\ I' \models \alpha_2$ et $I' \models \alpha_3$, donc E est satisfiable et même plus I' est un modèle pour E (i.e. $I' \models E$).

III.) Montrons que F n'est pas une conséquence logique de E.

On a : $F \equiv \forall x P(x, y) \wedge \forall y \overline{P(x, y)}$, on constate que y est libre dans la partie gauche de $\wedge$ et x est liée.

On reprend l'interprétation I' considérée précédemment (bien sûr on aurait pu choisir une autre interprétation), pour cette interprétation I', on a montrer que :

$$I' \models E, \tag{3.1}$$

On a : $I'(F) : \underbrace{\underbrace{\forall x(x \leq 1)}_{vraie} \wedge \underbrace{\forall y, x > y}_{fausse}}_{fausse}$, donc :

$$I' \not\models F, \tag{3.2}$$

Alors, de (3.1) et (3.2) on conclut que F n'est pas une conséquence logique de E, i.e. $E \not\models F$.

Corrigé de l'exercice 3.5. On a : $F \equiv \exists x \forall y R(x) \Rightarrow R(y)$. on a la variable x est liée et la variable y est libre.

1. On va trouver un modèle pour la formule F. Soit alors l'interprétation I de domaine de base $D = \{2, 6, 20, 40\}$ et $R(x) : "x$ est pair$"$. Pour toutes les valuations possibles $\{v(y) = 2, v(y) = 6, v(y) = 20, v(y) = 40\}$ de la variable libre y, on constate que F est vraie, car :

$$\underbrace{\underbrace{\exists x R(x)}_{vraie} \Rightarrow R(y)}_{vraie}.$$

Donc I' est un modèle de F (i.e. $I' \models F$).
2. La forme prénexe de F est la suivante :

$$\begin{aligned} F &\equiv \exists x R(x) \Rightarrow R(y); \\ &\equiv \forall x \left(R(x) \Rightarrow R(y)\right). \end{aligned}$$

Remarque : on a enlevé le quantificateur de y car la variable y est libre, elle n'est pas dans le champs de ce quantificateur donc ça ne sert à rien de garder ce quantificateur.
3. La forme prénexe de la négation de la formule F c'est exactement la négation de la forme prénexe de F, c'est à dire :

$$\begin{aligned} \overline{F} &\equiv \overline{\forall x[R(x) \Rightarrow R(y)]}, \\ &\equiv \exists x[R(x) \Rightarrow R(y)]. \end{aligned}$$

Remarque : il faut réviser les identités données en cours qui sont nécessaires pour trouver une forme prénexe.)
4. La forme skolem de F est exactement la forme prénexe de F car il n'y a pas de quantificateur existentiel dans la forme prénexe de F, donc :

$$F^{sko} \equiv \forall x \left(R(x) \Rightarrow R(y)\right).$$

Chapitre 4

Le calcul des séquents

4.1 Introduction

En logique mathématique et plus précisément en théorie de la démonstration, le calcul des séquents est un système de déduction créé par Gerhard Gentzen. Le nom de ce formalisme fait référence à un style particulier de déduction ; le système original a été adapté à diverses logiques, telles que la logique classique, la logique intuitionniste et la logique linéaire.

Un séquent est une suite d'hypothèses suivie d'une suite de conclusions, les deux suites étant usuellement séparées par le symbole $\vdash$ ou $\rightarrow$ dans l'œuvre originale de Gentzen. Un séquent représente une étape d'une démonstration, le calcul des séquents explicitant les opérations possibles sur ce séquent en vue d'obtenir une démonstration complète et correcte.

Le calcul des séquents, contrairement aux systèmes à la Hilbert ou à la déduction naturelle, n'a pas été créé pour être un formalisme intuitif qui refléterait une forme naturelle de raisonnement, car le propos de Gentzen était de résoudre certains problèmes techniques rencontrés en déduction naturelle lors de la démonstration de la cohérence de l'arithmétique. C'est pourquoi le calcul des séquents doit se penser comme un formalisme pour raisonner sur les preuves formelles plutôt que pour rédiger des preuves formelles, ce à quoi la déduction naturelle est plus adaptée. On peut toutefois facilement montrer que toute formule prouvable dans l'un des systèmes l'est également dans l'autre.

L'intérêt du calcul des séquents est de rendre explicite un grand nombre de propriétés de la logique :

– la dualité hypothèse/conclusion exprimée par la symétrie parfaite entre la droite

et la gauche dans les séquents ;
- la symétrie de la logique classique exprimée par le partitionnement des règles en gauche et droite ;
- les propriétés structurelles (commutativité, idempotence) exprimées par les règles du groupe structurel.

Dans ce chapitre, nous allons donner une introduction au calcul des séquents.

Définition 4.1. Un séquent est une paire $< \Gamma, \Delta >$ d'ensembles finis de formules.

Habituellement, un séquent $< \Gamma, \Delta >$ est écrit $\Gamma \vdash \Delta$. Si $\Gamma = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ et $\Delta = \{\beta_1, \beta_2, \ldots, \beta_m\}$ alors le séquent $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \vdash \{\beta_1, \beta_2, \ldots, \beta_m\}$ sera simplement écrit

$$\alpha_1, \alpha_2, \ldots, \alpha_n \vdash \beta_1, \beta_2, \ldots, \beta_m$$

Soit α une formule, Γ, Δ deux ensembles de formules nous notons : Γ, α au lieu de $\Gamma \cup \alpha$, et $\vdash \Delta$ au lieu de $\emptyset \vdash \Delta$.
La sémantique d'un séquent est donnée par la définition suivante :

Définition 4.2. Soit V une validation définie de l'ensemble des séquents vers l'ensemble $\{0, 1\}$ des valeurs de vérité. Alors, nous avons :
$v(\Gamma \vdash \Delta) = 1$ si $v(\alpha) = 0$ pour un certain $\alpha \in \Gamma$ ou $v(\beta) = 1$ pour un certain $\beta \in \Delta$.

Ceci revient à considérer que le séquent $\Gamma \vdash \Delta$ est interprété par la formule :

$$(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \vdash (\beta_1 \vee \beta_2 \vee \ldots \vee \beta_m).$$

Définition 4.3. Les axiomes et les règles d'inférence du calcul des séquents sont :
Axiomes
$\alpha \vdash \alpha$ (*axiome*)
Règles structurelles

$$\frac{\Gamma \vdash \Delta}{\Gamma, \alpha \vdash \Delta}(\text{aff}_g) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \alpha, \Delta}(\text{aff}_d)$$

$$\frac{\Gamma, \alpha, \alpha \vdash \Delta}{\Gamma, \alpha \vdash \Delta}(\text{contr}_g) \qquad \frac{\Gamma \vdash \alpha, \alpha, \Delta}{\Gamma \vdash \alpha, \Delta}(\text{contr}_d)$$

Règles des connecteurs logiques

$$\frac{\Gamma, \alpha, \beta \vdash \Delta}{\Gamma, \alpha \wedge \beta \vdash \Delta}(\wedge_g) \qquad \frac{\Gamma \vdash \alpha, \Delta \quad \Gamma \vdash \beta, \Delta}{\Gamma \vdash \alpha \wedge \beta, \Delta}(\wedge_d)$$

$$\frac{\Gamma, \alpha \vdash \Delta \quad \Gamma, \beta \vdash \Delta}{\Gamma, \alpha \vee \beta \vdash \Delta}(\vee_g) \qquad \frac{\Gamma \vdash \alpha, \beta, \Delta}{\Gamma \vdash \alpha \vee \beta, \Delta}(\vee_d)$$

$$\frac{\Gamma \vdash \alpha, \Delta \quad \Gamma, \beta \vdash \Delta}{\Gamma, \alpha \Rightarrow \beta \vdash \Delta}(\Rightarrow_g) \qquad \frac{\Gamma, \alpha \vdash \beta, \Delta}{\Gamma \vdash \alpha \Rightarrow \beta, \Delta}(\Rightarrow_d)$$

$$\frac{\Gamma \vdash \alpha, \Delta}{\Gamma, \overline{\alpha} \vdash \Delta}(\neg_g) \qquad \frac{\Gamma, \alpha \vdash \Delta}{\Gamma \vdash \overline{\alpha}, \Delta}(\neg_d)$$

Règles des quantificateurs

$$\frac{\Gamma, \alpha[x := t] \vdash \Delta}{\Gamma, \forall x\ \alpha \vdash \Delta}(\forall_g) \qquad \frac{\Gamma \vdash \alpha, \Delta \quad x \text{ n'est pas libre dans } \Gamma, \Delta}{\Gamma \vdash \forall x\ \alpha, \Delta}(\forall_d)$$

$$\frac{\Gamma, \alpha \vdash \Delta \quad x \text{ n'est pas libre dans } \Gamma, \Delta}{\Gamma, \exists x\ \alpha \vdash \Delta}(\exists_g) \qquad \frac{\Gamma \vdash \alpha[x := t], \Delta}{\Gamma \vdash \exists x\ \alpha, \Delta}(\exists_d)$$

Règle de coupure

$$\frac{\Gamma \vdash \alpha, \Delta \quad \Gamma', \alpha \vdash \Delta'}{\Gamma, \Gamma' \vdash, \Delta', \Delta}(\text{coupure})$$

Remarque 4.1.1. Les expressions *aff* et *contr* signifient respectivement affaiblissement et contraction.

Exemple 4.1.1. Soit à montrer la règle

$$\neg(P \wedge Q) \vdash (\neg P \vee \neg Q)$$

Sa preuve dans le calcul des séquents est la suivante

(1) $P \vdash P$ (axiome)

(2) $Q \vdash Q$ (axiome)

(3) $P, Q \vdash P$ (aff$_g$)

(4) $P, Q \vdash Q$ (aff$_g$)

(5) $P, Q \vdash P \wedge Q$ ($\wedge_d$)

(6) $Q \vdash P \wedge Q, \neg P$ ($\neg_d$)

(7) $\vdash P \wedge Q, \neg P, \neg Q$ ($\neg_d$)

(8) $P \wedge Q \vdash \neg P, \neg Q$ ($\neg_g$)

(9) $P \wedge Q \vdash \neg P \vee \neg Q$ ($\vee_d$)

Les règles du calcul des séquents sont appelées introductions quand elles sont utilisées de haut en bas, et éliminations quand elles sont utilisées de bas en haut.

On dira qu'une règle est correcte si elle ne change pas la validité des formules . Plus précisement, si les séquents de départ sont valides, alors les séquents d'arrivée sont valides. Nous allons maintenant énoncer les deux lemmes suivants :

Lemme 4.1.1. *Les règles d'introduction du calcul des séquents sont correctes.*

Lemme 4.1.2. *Les règles d'éliminations du calcul des séquents sont correctes.*

Ceci se traduit par l'équivalence des séquents inférieurs et des séquents supérieurs des règles ci-dessus. Nous admettrons ici les deux lemmes sans les démontrer.

4.2 Exercices

Exercice 4.1. Montrer les axiomes d'Hilbert Ackerman en utilisant le calcul des séquents.

Exercice 4.2. Montrer que les formules suivantes sont des théorèmes :

1. $\overline{\overline{\alpha}} \Rightarrow \alpha$;
2. $\alpha \Rightarrow \overline{\overline{\alpha}}$;
3. $\overline{\alpha} \Rightarrow (\alpha \Rightarrow \beta)$;
4. $(\overline{B} \rightarrow \overline{\alpha} \Rightarrow ((\overline{\beta} \Rightarrow \alpha)) \Rightarrow \beta)$;
5. $(\alpha \Rightarrow \beta) \Rightarrow (\overline{\alpha} \Rightarrow \overline{\beta})$;
6. $\alpha \Rightarrow (\overline{\beta} \Rightarrow \overline{(\alpha \Rightarrow \beta)})$;
7. $(\alpha \Rightarrow \beta) \Rightarrow ((\overline{\alpha} \Rightarrow \beta) \Rightarrow \beta)$.

Exercice 4.3. Montrer $\vdash \exists x \forall y \, (R(y) \Rightarrow R(x))$

Bibliographie

[1] A. Church, (1936). *An Unsolvable Problem of Elementary Number Theory*, American Journal of Mathematics, vol. 58,245–63.

[2] A. Church, (1936). *A Note on the Entscheidungsproblem* , Journal of Symbolic Logic, vol. 1,40-41, correction p. 101-102.

[3] R. Cori, and D. Lascar, (1993). *Logique mathématique*. Volume I. Mason.

[4] R. David, K. Nour et C. Raffalli, (2001). *Introduction à la logique. Théorie de la démonstration*. Cours et exercices corrigés. Dunod.

[5] D. Hilbert, (1900). *Les 23 problèmes de Hilbert*, congrès international des mathématiciens, Paris, France.

[6] A. Turing, (1937). *On Computable Numbers, with an Application to the Entscheidungsproblem* , Proc. London Math. Soc., vol. 42, 230-265.

[7] J. Wolenski and J. Lukasiewicz, (1994). *On the Liar Paradox, Logical Consequence, Truth and Induction*, Modern Logic 4 (1994), 394-400.