Notes de Cours :
LOGIQUE MATHÉMATIQUE

Par
Pr. Mohamed MEZGHICHE

Table des matières

Première partie

LOGIQUE

CHAPITRE 1

Rappels mathématiques

1. Les entiers naturels

Souvent on écrit l'ensemble des entiers naturels $\{1, 2, 3 \ldots, \}$ en utilisant les trois points $(\ldots)$ pour exprimer que l'ensemble des entiers est un ensemble qui possède une infinité d'éléments. Cette définition est intuitive et facilement acceptée. Mais elle ne suffit pas pour utiliser le concept de nombres entiers dans plusieurs domaines des mathématiques. Ceci revient au fait d'écrire trois points $(\ldots)$, pour exprimer la notion d'infini, qui n'est pas, en soit, un concept mathématique.

Il est donc nécessaire de donner une définition des entiers naturels adaptée à de nombreuses applications en mathématiques et aussi en logique.

Dans la nouvelle définition des entiers on prend chaque entier comme un objet mathématique construit à partir de l'entier 0 (zero) et l'application S dite fonction successeur : $(\forall n \in N) S : n \to n+1$. Ainsi on peut construire tous les entiers naturels comme suit :

$$1 = S(0), 2 = S(1), 3 = S(2), \ldots, n+1 = f(n), \ldots$$

Cette manière de construire les entiers naturels amène à proposer une nouvelle définition des entiers naturels

Définition 1.1. (1) *0 est un entier naturel*

(2) *Si n est un entier naturel alors $S(n) = (n+1)$ est un entier naturel.*

(3) *L'ensemble des entiers naturels est défini par les clauses (1) et (2).*

Cette définition est un exemple de définition par induction. La clause (1) est appelée règle de base, la clause (2) qui permet de construire un nouveau élément est appelée règle de génération. La dernière clause est appelée règle de fermeture, elle signifie que la définition des entiers est déterminée par les clauses (1) et (2).

1.1. Induction mathématique. Le principe d'induction mathématique est très utilisé pour démontrer des proptiétés sur les ensembles des entiers ou sur tout autre ensemble dont les éléments sont des objets mathéamtiques et qui est isomorphe à un sous ensemble de l'ensemble des entiers naturels. Il serait très utile de rappeler de façon simple le principe d'induction. Supposons que l'on souhaite démontrer une propriété $P(n)$ pour tout $n \in N$. Pour utiliser le principe d'induction dans notre démonstration nous devons suivre les étapes suivantes :

(1) Montrer que la propriété $P(n)$ est vérifiée pour $n = 0$.

(2) Montrer que $P(n+1)$ est vérifiée si l'on admet que $P(n)$ est vérifiée.

(3) On déclare que $(\forall n \in N)P(n)$ est démontrée si nous avons montré les étapes 1) et 2).

Accepter le principe de l'induction mathématique, très utilisé en mathématique, devient immédiat si on prend en considération la définition inductive des entiers naturels. Soulignons que le principe d'induction n'est pas seulement utilisé pour démontrer des propriétés des entiers naturels mais concerne aussi les proriétés sur des ensembles dénombrables. Le principe d'induction est aussi très utilisé dans les preuves des propriétés et théorèmes en logique où souvent les définitions sont données sous la forme de définition inductive. Généralement la preuve par induction d'une propiété $P(n)$ sur un ensemble dénombrable E est constituée de trois étapes :

(1) Montrer que le plus petit élément de E, soit n_0 vérifie la propriété P. Ceci signifie que $P(n_0)$ est vérifiée. $P(n_0)$ est la base d'induction.

(2) On suppose que $P(n)$ est vérifiée, c'est l'hypothèse d'induction.

(3) A partir de l'hypothèse d'induction on montre que $P(n+1)$ est vérifiée. Dans le cas où cela est montré on peut dire que : $(\forall n \in E)P(n)$ est vérifiée.

On trouve souvent dans certaines démonstrations mathématiques l'utilisation du principe d'induction sous une autre forme légèrement différente de celle décrite ci-dessus. L'hypthèse d'induction est donnée sous la forme $P(m)$ est vérifiée pout tout $(m < n)$. Il est facile de voir que c'est une généralisation du principe d'induction décrit plus haut.

Exemple 1.1. *Montrer par induction que la somme des entiers* $1, 3, 5, \ldots, 2n-1$ *est égale à* n^2.

Tout d'abord on peut réecrire cette question sous une forme qui correspond à la définition du principe d'induction. Soit $P(n) = 1 + 2 + \ldots + 2n - 1 = n^2$. *Le domaine de définition de* P *est* $E = \{1, 3, 5, \ldots, 2n-1, \ldots\}$. *Appliquer le principe d'induction pour montrer cette propriété nous amène à :*

(1) *S'assurer que la base d'induction est vérifiée, cest à dire que* $P(1)$ *est vraie. Ceci donne* $P(1) = 1 = 1^2$.

(2) *Supposer que* $P(n)$ *est vraie. Ceci sgnifie que* $P(n) = 1+3+5+\ldots+2n-1 = n^2$.

(3) *Montrer que* $P(n+1) = 1+3+5+\ldots+2n+1 = (n+1)^2$.

Pour démontrer ce résultat on part de l'hypothèse $P(n) = 1+3+5+\ldots+2n-1 = n^2$, *on ajoute aux deux membres cette égalité, le nombre* $2n+1$. *Ceci donne :*
$1+3+5+\ldots+2n-1+2n+1 = n^2+2n+1$
On obtient :
$1+3+5+\ldots+2n-1+2n+1 = n^2+2n+1 = (n+1)^2$.
et donc :
$P(n+1) = (n+1)^2$.

2. Démonstration par contraposition

La démonstration par contraposition est basée sur le principe suivant :

Démontrer que la négation d'une proposition est fausse prouve que cette proposition est vraie. Nous verrons dans le reste de ce cours la justification de ce principe. Nous allons maintenant, à l'aide d'un exemple, montrer son utilisation dans la déduction mathématique.

Supposons que que l'on pose cette question : l'ensemble des entiers naturels premiers est-il fini ? Les entiers premiers sont les entiers dont l'ensemble des diviseurs se réduit à 1 et l'entier lui même. Les entiers $2, 3, 7, 11, 13, \ldots$ sont des premiers.

Pour répondre à cette question nous allons appliquer le raisonnement par contraposition. Partant de notre intuition que l'ensemble des entiers premiers est un ensemble infini, on supposera que cet ensemble est fini et on démontrera que cette hypothèse est fausse.

Si notre hypothèse était vraie alors l'ensemble des entiers premiers s'écrirait :

$$\{2, 3, 7, 11, 13, 17, \ldots, p\}.$$

Ici p est le plus grand entiers premiers.

Soit $Q = (2*3*7*11*13*17*\ldots*p)+1$. Q est plus grand que p et par hypothèse Q n'est pas premier puisque p est le plus grand entier premier. Mais observons que le reste de la division de Q par tout entier premier est égal à 1. Alors Q est premier. Ceci Nouscontredit l'hypothèse qui dit que l'ensemble des entiers premiers est fini.

3. Démonstration par contradition

Le principe du raisonnement par contradition est basé sur le principe suivant :

Si nous arrivons à déduire une contradiction en partant d'une hypothèse donnée alors nous concluons que cette hypothèse est fausse. Plus loin, nous présenterons la justification d'un tel principe. Donnons un exemple d'application de ce principe pour montrer son utilisation dans les preuves mathématiques. Problème : Trouver l'ensemble des nombres entiers écrits à l'aide des chiffres $0, 1, \ldots, 9$ en utilisant une seule fois chacun de ces chiffres et dont la somme est égale à 100. Une première tentative nous permet de donner l'ensemble $\{4, 5, 6, 730, 28, 19\}$. Cet ensemble possède la seconde condition mais pas la première puisque $4+5+6+7+30+28+19 = 99$. Une deuxième tentative nous amène à constater que l'ensemble des nombres $\{4, 5, 6, 7, 31, 28, 19\}$ vérifie la première condition puisque $4+5+6+7+31+28+19 = 100$; mais ne vérifie pas la deuxième condition. Le chiffre 1 apparait dans 19 et 31.

Après d'autres tentatives infructieuses, le lecteur se convaint facilement qu'il n'existe aucun ensemble de nombres vérifiant les conditions de ce problème. Alors, on se trouve devant la situation de croire qu'un tel ensemble n'existe pas. Cette idée sur la solution du problème est dictée par l'expérience et l'intuition développées après plusieurs essais.

Pour justifier cette nouvelle idée qu'aucune solution ne vérifie les conditions du problème, on supposera qu'une telle solution existe et on déduira une contradition. Supposons que la somme de certains nombres, vérifiant les conditions du problème, est égale à 100. Ces nombres constituent dix (10) formes différentes puisque $0, 1, 2, 3, \ldots, 9$ sont utlisés une seule fois pour écrire ces nombres. Nous avons :

$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$

Chacune de ces formes représente, dans notre ensemble de nombres, solution du problème, soit une dizaine ou soit une unité. Considérons que T est la somme des formes représentant les dizaines. La somme des formes restantes est $45 - T$.

La somme des nombres, solution du problème, est donc $10T + (45 - T) = 100$. Ceci donne $T = 55/9$. T n'est donc pas un entier naturel et ceci est contradictoire avec le fait que T est la somme de nombres entiers. Ceci contredit l'hypothèse qu'il existe une suite de nombres vérifiant les conditions posées plus haut, c'est à dire, dont la somme est égale à 100.

CHAPITRE 2

Calcul propositionnel

1. Préliminaires

Dans la logique propositionnelle, on trouve des *énoncés* simples dits atomes ou variables propositionnelles. On trouve aussi des énoncés composés complexes construits é partir des atomes ou des variables propositionnelles en utilisant des connecteurs. Par exemple pour construire l'énoncé mathématique :

$$(1) \qquad (x > 2) \quad \textbf{et} \quad (x^2 - 1/2 \leq 1).$$

Nous avons utilisé le connecteur **"et"** pour reliér les deux plus simples énoncés "$x > 2$" et "$x^2 - 1/2 \leq 1.$". De même l'énoncé $P \to Q$ est formé à l'aide des deux énoncés plus simples P, Q et du connecteur "$\to$".

Ils existent plusieurs autres connecteurs utilisés fréquement :"équivaut", "ou" et le "non".

Donnons maintenant la notation symbolique et la définition des différents connecteurs les plus utilisés.

Connecteur	Forme symbolique
non A	$\neg$ A
A et B	A $\wedge$ B
A ou B	A $\vee$ B
A implique B	A $\to$ B
A équivalent à B	A $\leftrightarrow$ B

A et B dénotent des énoncés quelconques .

Avant de donner la définition et pour mieux expliciter le sens de certains connecteurs, considérons les exemples suivants :

(1) Si la terre est plate alors Alger est une ville propre.

(2) Alger est une ville propre.

(3) La terre n'est pas plate.

Si nous convenons de noter par A et B l'énoncé "`La terre est plate`" et l'énoncé " Alger est une ville calme" respectivement ; la formule $A \to B$ dénotera l'énoncé " `Si` `la terre est plate alors Alger est une ville propre`” . L’énoncé “`La terre n’est pas plate`" se notera $\neg A$.

1.1. Les connecteurs $\rightarrow$, $\neg$, $\wedge$ et $\vee$. Explicitons maintenant les définitions de ces différents connecteurs :

($\neg$): **Négation.**

La négation d’un énoncé A est notée ¬A et elle est définie par : Si l’énoncé A est vrai alors la négation de l’énoncé A est fausse et si l’énoncé A est faux alors l’énoncé ¬A est vrai. Ceci est rendu plus comprhensible grâce au tableau :

A	¬A
V	F
F	V

Exemple 1.1. *L’énoncé “la terre est plate" est la négation de l’énoncé "la terre est sphérique". l’énoncé “$x = 2$” est la négation de l’énoncé “$x = 0$”.*

($\wedge$): **Conjonction.**

La conjonction de deux énoncés A, B est notée symboliquement par A ∧ B. Le connecteur de conjonction “et" noté par le symbole ∧ est défini par la table suivante :

A	B	A∧B
F	F	F
F	V	F
V	F	F
V	V	V

Ceci signifie que, l’énoncé A ∧ B est vrai, que dans le cas où les deux énoncés A et B sont vrais. L’énoncé A ∧ B est faux dans tous les autres cas.

($\vee$): **Disjonction.**

La disjonction de deux énoncés A, B est notée A ∨ B ; ceci se traduit dans le langage naturel par la phrase “l’énoncé A est vrai ou bien l’énoncé B est vrai”.

Habituellement dans le langage parlé le connecteur “ou bien " est entendu dans le sens exclusif, c’est dire nous ne pouvons pas avoir les deux énoncés A, B vrais simultanément. Un tel connecteur “ou" est dit exclusif. Ce que nous considérerons dans toute la suite sera le connecteur “ou" dit inclusif qui signifie que l’énoncé “A ou B" exprime que nous avons soit l’énoncé A vrai, soit l’énoncé B vrai, soit l’énoncé A et l’énoncé B sont vrais. La définition du connecteur est donne par la table suivante :

A	B	A $\vee$ B
F	F	F
F	V	V
V	F	V
V	V	V

($\rightarrow$): **Implication.**

Le connecteur $\rightarrow$ appelé le connecteur d’implication est souvent le seul qui pose quelques difficultés pour son utilisation. L’attribution d’une valeur de vérité à certains énoncés de la forme : A $\rightarrow$ B, dans certains cas, met en défaut notre “bon sens". L’exemple suivant nous donne une idée sur ce problème : Soit l’énoncé A “la terre est plate" et l’énoncé B “les enseignants sont milliardaires" . L’énoncé A $\rightarrow$ B exprimera : ”Si la terre est plate alors les enseignants sont milliardaires“. Le bon sens acceptera difficilement qu’un tel énoncé est vrai. La difficulté vient certainement du fait que dans le langage naturel nous ne rencontrons pas de tels type d’énoncés, mais il est fréquent de les trouver dans les langages artificiels (le langage mathématique, langage de programmation ...). Ces difficultés sont écartées en définissant le connecteur d’implication par la table suivante :

A	B	A$\rightarrow$B
F	F	V
F	V	V
V	F	F
V	V	V

Remarquons que le seul cas où l’nonc A $\rightarrow$ B est faux est lorsque l’énoncé A est vrai et l’énoncé B est faux. Ce qui traduit qu’un énoncé vrai ne peut pas impliquer un énoncé faux.

($\leftrightarrow$): **Equivalence.**

Le connecteur $\leftrightarrow$ d’équivalence liant deux énoncés A et B peut être défini par : A est vrai si B est vrai et B est vrai si A est vrai. La table suivante donne la définition du connecteur $\leftrightarrow$.

A	B	A↔B
F	F	V
F	V	F
V	F	F
V	V	V

2. Syntaxe de la logique propositionnelle

Les formules propositionnelles sont les énoncés considérés comme correctement écrits dans le langage de la logique propositionnelle. La définition des formules propositionnelles est donnée d'une manière inductive par la définition suivante :

DÉFINITION 2.1.
(1) *Les variables propositionnelles p, q, u, v, … sont des formules propositionnelles*
(2) *Si A est une forme propositionnelle alors* $\neg A$ *est une formule propositionnelle*
(3) *Si A, B sont des formules propositionnelles alors* $(A \wedge B)$, $(A \vee B)$ *et* $(A \rightarrow B)$ *sont des formules propositionnelles.*
(4) *Les formules propositionnelles sont définies par les clauses 1), 2) et 3).*

EXEMPLE 2.1. *$((p \wedge q) \rightarrow (\neg(p \vee q)))$ est une formule propositionnelle à partir du fait que les variables p et q sont des variables propositionnelles. On déduit par les clauses 1) et 2) que $p \wedge q$ et $\neg(p \vee q)$ sont des formules propositionnelles et finalement $((p \wedge q) \rightarrow (\neg(p \vee q)))$ est une formule propositionnelle par la clause 3).*

3. Sémantique de la logique propositionnelle

Nous nous intérressons maintenant aux formules propositionnelles qui ont toujours la valeur de vrité "vrai" à cause de leur structure syntaxique sans aucune réfrence au sens des variables propositionnelles.

DÉFINITION 3.1. *Une valuation Booléenne est une application v de l'ensemble des formules propositionnelles vers l'ensemble {V,F} vérifiant les conditions :*
(1) $v(\neg X) = \neg v(X)$
(2) $v(X \wedge Y) = v(X) \wedge v(Y)$; $v(X \wedge Y) = v(X) \vee v(Y)$; $v(X \rightarrow Y) = v(X) \rightarrow v(Y)$.

EXEMPLE 3.1. *Considérons la valuation Booléenne v telle que $v(p) = V$ et $v(q) = F$. La formule propositionnelle $((\neg\, p) \vee q)$ a pour valuation Booléenne :*

$$\begin{aligned} v((\neg p) \vee q) &\equiv v(\neg p) \vee v(q) \\ &\equiv \neg v(p) \vee v(q) \\ &\equiv \neg(V) \vee F \\ &\equiv F \vee F = F \end{aligned}.$$

Notation : A partir de maintenant nous adopterons la convention suivante : Noter F (faux) par 0 et V (vrai) par 1.

DÉFINITION 3.2. (1) *Une formule propositionnelle est une tautologie si elle prend une valeur de vérité 1 (vraie) pour toutes les valeurs prises par les variables contenues dans cette formule propositionnelle.*

(2) *Une formule propositionnelle est une contradiction si elle prend une valeur 0 (Fausse) pour toutes les valeurs prises par les variables contenues dans cette formule propositionnelle.*

EXEMPLE 3.2. *$(a \vee \neg a)$ est une tautologie. $(a \wedge \neg a)$ est une contradiction. $(a \rightarrow (b \rightarrow a))$ est une tautologie.*

Il est aisé de voir qu'une formule propositionnelle est une tautologie ou une contradiction ; il suffit de construire la table de vérité correspondante.

DÉFINITION 3.3. *Si A et B sont des formules propositionnelles, on dira que A implique logiquement B si $(A \rightarrow B)$ est une tautologie et on dira que, A est logiquement équivalent à B si $A \leftrightarrow B$ est une tautologie.*

EXEMPLE 3.3. *$p \wedge q$ implique logiquement p. $\neg(p \wedge q)$ est logiquement équivalant à $(\neg\, p \vee \neg q)$. On peut vérifier facilement que le connecteur d'équivalence $\leftrightarrow$ peut être défini par :*

$$A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A).$$

4. Théorème de remplacement

Nous pouvons voir à l'aide des tables de vérité que l'énoncé $(p \rightarrow p)$ est une tautologie. Si nous substituons la formule propositionnelle $((r \wedge s) \rightarrow t)$ à la variable propositionnelle p, nous obtenons $((r \wedge s) \rightarrow t) \rightarrow ((r \wedge s) \rightarrow t)$ qui est aussi une tautologie. Il revient à dire que si nous remplaçons toutes les occurrences d'une variable propositionnelle dans une tautologie par une formule propositionnelle quelconque ; la formule propositionnelle obtenue est aussi une tautologie. Ce résultat est donné par le thorème suivant :

THÉORÈME 4.1. *Soit A une formule propositionnelle contenant les variables p_1 , p_2 , ..., p_n et soient A_1 , A_2 , ..., A_n des formules propositionnelles quelconques. Si A est une tautologie alors la formule propositionnelle B obtenue en remplaçant dans A les occurrences des variables p_i $(i \leq n)$ par les A_i respectivement, est aussi une tautologie.*

DÉMONSTRATION. Soient A une tautologie et p_1, p_2,..., p_n des variables propositionnelles contenues dans A et A_1, A_2,..., A_n des formules propositionnelles. Soit B la formule obtenue en substituant dans A les formules A_i $(1 \leq i \leq n)$ respectivement aux variables propositionnelles p_i. Quelque soit la valeur de vérité prise par A_1, A_2, ..., A_n , B prend la même valeur de vérité que A quand ces mêmes valeurs de vérités des A_i $(1 \leq i \leq n$) sont prises respectivement par p_1, p_2, ..., p_n . Donc B est aussi une tautologie. □

EXEMPLE 4.1. *Soit A la formule propositionnelle* $(a \to ((b \wedge c) \to a)$*. On peut vérifier facilement que A est une tautologie. Soit B la formule propositionnelle obtenue en remplaçant dans A les variables b et c par les deux formules propositionnelles*

$$A_1 \equiv (\neg x \to y) \text{ et}$$
$$A_2 \equiv (y \to x).$$
$$B \equiv [A_1/b]\ [A_2/c]A \equiv (a \to (((\neg x \to y) \wedge (y \to x)) \to a)$$

B est aussi une tautologie.

PROPOSITION 4.1. *Soit A une formule propositionnelle contenant seulement les connecteurs* $\neg$, $\wedge$, *et* $\vee$. *Soit A* la formule propositionnelle obtenue en interchangeant les connecteurs* $\wedge$ *et* $\vee$ *et en remplaçant chaque variable p par sa ngation* $(\neg p)$ *dans A. Alors A* est logiquement équivalent à* $\neg A$.

DÉMONSTRATION. La démonstration se fait par induction sur le nombre n de connecteurs qui sont contenus dans A.

`Base d'induction(n = 0)`

A ne contient aucun connecteur. Dans ce cas A est une variable propositionnelle p, A* est donc $(\neg p)$. Il est évident que A* est logiquement équivalent à $(\neg p)$.

`Hypothèse d'induction :`

Supposons que A contient k connecteurs $(k \leq n)$ et supposons que chaque énoncé avec moins de k connecteurs vérifie la propréité. Alors, il existe 3 cas à considrer :

(1) A est de la forme $(\neg B)$
(2) A est de la forme $(B \vee C)$
(3) A est de la forme $(B \wedge C)$.

Cas 1 : B a $k-1$ connecteurs. Par hypothèse d'induction B* est logiquement équivalent à $(\neg B)$, mais A est $(\neg B)$. Donc A* est logiquement équivalent à $\neg(B^*)$ et comme B* est logiquement équivalent à $\neg B$; alors A* est logiquement équivalent à $\neg\neg B$; c'està dire à $\neg A$.

Cas 2 : B et C contiennent chacun moins de k connecteurs et donc B* et C* sont logiquement équivalents à (¬B) et (¬C) respectivement. A* est (B* ∧ C*) et il est logiquement équivalent à (¬B ∧ ¬C) et donc ¬A.

Cas 3 : B* et C* sont logiquement équivalentà (¬B) et (¬C) respectivement. A* est (B* ∨ C*) qui est logiquement équivalent à (¬B) ∨ (¬C) et donc ¬(B ∧ C) c'est à dire ¬A.

□

COROLLAIRE 4.1. *Si p_1, p_2,..., p_n sont des variables propositionnelles alors :* *$(\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_n)$ est logiquement équivalent à $\neg(p_1 \wedge p_2 \wedge \ldots \wedge p_n)$.*

DÉMONSTRATION. C'est un cas particulier de la proposition précédente dans laquelle A est la formule propositionnelle ($\mathrm{p}_1 \wedge \mathrm{p}_2 \wedge \ldots \wedge \mathrm{p}_n$) Utiliser la proposition précédente pour montrer que $((\neg p_1) \wedge (\neg p_2) \wedge \ldots \wedge (\neg p_{n_1}) \wedge (\neg p_n))$ est logiquement équivalent à $\neg(p_1 \vee p_2 \vee \ldots \vee p_n)$. □

PROPOSITION 4.2. *(Les lois de Morgan).*
Soient A_1 , A_2 , ..., A_n des formules propositionnelles quelconques alors :

(1) *L'énoncé $((\neg A_1) \vee (\neg A_2) \vee \ldots (\neg A_n))$ est logiquement équivalent à* $\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n)$
(2) *L'énoncé $(\neg A_1 \wedge \neg A_2 \wedge \ldots \wedge \neg An_1 \wedge \neg A_n$) est logiquement équivalent à* $\neg(A_1 \vee A_2 \vee \ldots \vee A_n)$.

DÉMONSTRATION. La démonstration de cette proposition découle des résultats précédents et elle est suggére comme exercice. □

5. Forme normale conjonctive d'un énoncé

Nous allons maintenant écrire les formules propositionnelles en utilisant seulement les connecteurs ∧, ∨ et ¬. L'objectif, comme nous le verrons plus loin, est de pouvoir donner une méthode directe qui permet de vérifier si une formule est une tautologie ou une contradiction sans passer par sa table de vérité.

DÉFINITION 5.1. *Soient $X_1, X_2, \ldots, X_n$ une liste de formules propositionnelles. On introduit la notation suivante :*

$[X_1, X_2, \ldots, X_n]$ dénote la disjonction $X_1 \vee X_2 \vee \ldots \vee X_n$.

$< X_1, X_2, \ldots, X_n >$ dénote la conjonction $X_1 \wedge X_2 \wedge \ldots \wedge X_n$.

Si v est une validation booléenne nous avons : $v([X_1, X_2, \ldots, X_n]) = t$ si $v(X_i) = t$ pour un certain X_i et $v([X_1, X_2, \ldots, X_n]) = f$ sinon.

$v(< X_1, X_2, \ldots, X_n) = t$ si $v(X_i) = t$ pour tout X_i et $v(< X_1, X_2, \ldots, X_n >) = f$ sinon.

DÉFINITION 5.2. *Un litéral est une variable propositionnelle ou la négation d'une variable propositionnelle.*

DÉFINITION 5.3. *Une* **clause** *est une disjonction $X_1 \vee X_2 \vee \ldots \vee X_n$ note $[X_1, X_2, \ldots, X_n]$ ou chaque lment est un litéral. Une formule propositionnelle est dite sous* **forme normale conjonctive** *ou sous* **forme clausale** *si c'est une conjonction $C_1 \wedge C_2 \wedge \ldots \wedge C_n$ note $< C_1, C_2, \ldots, C_n >$ où chaque C_i est une clause.*

THÉORÈME 5.1. *Il existe un algorithme qui transforme une formule propositionnelle ordinaire en forme clausale.*

Avant de décrire l'algorithme définissons les notions de α-formule et β-formule.

α-formule (conjonction)	α_1	α_2	β-formule (disjonction)	β_1	β_2
$X \wedge Y$	X	Y	$\neg(X \wedge Y)$	$\neg X$	$\neg Y$
$\neg(X \vee Y)$	$\neg X$	$\neg Y$	$X \vee Y$	X	Y
$\neg(X \rightarrow Y)$	X	$\neg Y$	$X \rightarrow Y$	$\neg X$	Y

Description de l'algorithme

Etape 1. On commence avec $< [X] >$. Après avoir excuté l'étape n en produisant $< D_1, D_2, \ldots, D_n >$ où les éléments D_i sont des disjonctions et si nous n'avons pas encore la forme clausale aller à l'tape suivante :

Etape n+1. Choisir un élément D_i qui contient certains non litéraux, soit N par exemple.

(a) Si N est $\neg\neg Z$ remplacer N par Z.

(b) Si N est une β-formule remplacer N par la suite des deux formules β_1, β_2.

(c) Si N est est une α-formule remplacer la disjonction D_i par les deux disjonctions $[\alpha_1/\alpha]D_i$ et $[\alpha_2/\alpha]D_i$.

EXEMPLE 5.1. *Donnons la forme clausale de la formule :*
$(a \rightarrow (b \rightarrow c)) \rightarrow ((a \rightarrow b) \rightarrow (a \rightarrow c))$

(1) $< a \rightarrow (b \rightarrow c)) \rightarrow ((a \rightarrow b) \rightarrow (a \rightarrow c))] >$

(2) $< [\neg(a \rightarrow (b \rightarrow c)), (a \rightarrow b) \rightarrow (a \rightarrow c))] >$

(3) $< [\neg(a \rightarrow (b \rightarrow c)), \neg(a \rightarrow b), (a \rightarrow c)] >$

(4) $< [a, \neg(a \rightarrow b), (a \rightarrow c]], [\neg(b \rightarrow c), \neg(a \rightarrow b), (a \rightarrow c] >$

(5) $< [a, a, a \rightarrow c], [a, \neg b, \neg a, c], [b, a, \neg a, c], [b, \neg b, \neg a, c], [\neg c, a, \neg a, c], [\neg b, \neg c, \neg a, c] >$

(6) $< [a, a, \neg a, c], [a, \neg b, \neg a, c], [b, a, \neg a, c], [b, \neg b, \neg a, c], [\neg c, a, \neg a, c], [\neg b, \neg c, \neg a, c] >$

La forme normale conjonctive est :
$(a \vee \neg a \vee c) \wedge (a \vee \neg b \vee \neg a \vee c) \wedge (b \vee \neg a \vee a \vee c) \wedge (b \vee \neg b \vee \neg a \vee c) \wedge (\neg c \vee a \neg a \vee c) \wedge (\neg b \vee \neg c \vee \neg a \vee c)$

6. Ensemble complet de connecteurs

DÉFINITION 6.1. *Un ensemble complet de connecteurs est un ensemble qui est tel que à toute formule F correspond une formule proposionnelle G logiquement équivalente à F contenant que les connecteurs de cet ensemble.*

Nous pouvons montrer maintenant le résultat suivant.

PROPOSITION 6.1. *Les ensembles $\{\neg, \rightarrow\}$, $\{\neg, \vee\}$ et $\{\neg, \wedge\}$ sont des ensembles complets de connecteurs.*

DÉMONSTRATION. On peut observer que l'ensemble $\{\neg, \wedge, \vee\}$ est un ensemble complet de connecteurs puisque, comme on vient de le voir, on peut à toute formule F trouver une formule équivalente G contenant seulement les connecteurs de l'ensemble $\{\neg, \wedge\}$. Pour montrer, par exemple, que l'ensemble $\{\neg, \wedge\}$ est un ensemble complet il suffit de montrer que le connecteur $\vee$ s'exprime en fonction de $\wedge$ et $\neg$. En utilisera le fait que $A \vee B$ est logiquement équivalent à $\neg(\neg A \wedge \neg B)$. □

DÉFINITION 6.2. *Soient les connecteurs $|$ et $\downarrow$ définis par :*

p	q	$p \downarrow q$	$p \mid q$
0	0	1	1
0	1	0	1
1	0	0	1
1	1	0	0

PROPOSITION 6.2. $\{|\}$ *et* $\{\downarrow\}$ *dont des ensembles complets de connecteurs.*

DÉMONSTRATION. Exprimons $\neg$ et $\wedge$ ou $\neg$ et $\vee$ dans $\{|\}$ et $\{\downarrow\}$.
nous avons :

$$\begin{aligned} \neg \mathrm{p} &\equiv \mathrm{p} \downarrow \mathrm{p} \\ \mathrm{p} \wedge \mathrm{q} &\equiv (\mathrm{p} \downarrow \mathrm{p}) \downarrow (\mathrm{q} \downarrow \mathrm{q}) \\ \neg \mathrm{p} &\equiv \mathrm{p} \mid \mathrm{p} \\ \mathrm{p} \vee \mathrm{q} &\equiv (\mathrm{p} \mid \mathrm{p}) \mid (\mathrm{q} \mid \mathrm{q}) \end{aligned}$$

□

PROPOSITION 6.3. *Les seuls connecteurs qui forment à eux seuls un ensemble de connecteurs complet sont $|$ et $\downarrow$.*

DÉMONSTRATION. Supposons qu'il existe un autre connecteur que nous noterons $\star$. La table de vérité définissant ce connecteur aura la forme :

A	B	A$\star$B
0	0	?
0	1	?
1	0	?
1	1	?

Si la valeur de la dernière ligne est 1 alors toute formule construite en utilisant le seul connecteur $\star$ doit prendre la valeur 1 si les variables propositionnelles composant cette formule prennent la valeur 1. Donc, aucune combinaison ne peut exprimer la négation d'un énoncé A. La valeur de cette dernière ligne du tableau doit être 0. De la même façon la valeur de la première ligne doit être 1. Alors nous avons :

A	B	A$\star$B
0	0	1
0	1	?
1	0	?
1	1	0

Si les valeurs de la 2^{eme} ligne et 3^{eme} ligne sont identiques à 0 le connecteur $\star$ sera identique à $|$. Si les valeurs de la 2^{eme} ligne et 3^{eme} ligne sont identiques à 1 le connecteur $\star$ sera identique à $\downarrow$.

Ceci laisse deux autres possibilités :

(1) la valeur de la 2^{eme} ligne est 1 et la valeur de la 3^{eme} ligne est 0
(2) la valeur de la 2^{eme} ligne est 0 et la valeur de la 3^{eme} ligne est 1.

Dans le premier cas nous avons A $\star$ B = $\neg$A Dans le second cas nous avons A $\star$ B = $\neg$B Dans chacun des cas $\star$ pourrait ëtre dfini en termes de $\neg$. Mais le connecteur $\neg$ (ngation) ne peut former seul un ensemble complet. Les seuls fonctions à un argument que l'on peut exprimer en fonction de $\neg$ sont la négation et l'identité. A partir d'une formule A nous pouvons obtenir que :

$$\neg A$$
$$\neg\neg A$$
$$\neg\neg\neg A$$
$$\dots$$

$\square$

En conclusion il n'existe aucun autre connecteur formant un ensemble complet.

7. Exercices.

(1) Démontrer par induction que $n^2 \geq 2n+3$ pour $n \geq 3$.

(2) Démontrer par induction sur n que pour tout $n \geq 1$.

$$1 + 3 + 5 \ldots + (2n - 1) = n^2.$$

(3) Démontrer par induction sur n que $n^3 + 2n$ est divisible par 3 pour tout $n \geq 1$.

(4) Soient A, B et C trois ensembles avec $A \cup B = A \cup C$. Est-il vrai que $B = C$?

(5) Donner la table de vérit ? du **ou** exclusif.

(6) Donner les tables de vérité des énoncés $p \vee p$, $p \wedge p$, $p \vee 0$ et $p \vee 1$.

(7) Donner la forme propositionnelle des phrases suivantes :

  (a) Il est habile et intelligent.

  (b) Il est habile mais pas intelligent.

  (c) Il doit travailler dur, sinon il choue.

  (d) Il n'a pas écrit la lettre ou il l'a perdue.

  (e) La somme de deux nombres est pair si les deux nombres sont pair ou les deux nombres sont impairs.

(8) Une association est régie par le règlement intérieur suivant :

  art1. Les membres de la direction financière doivent être choisis parmi ceux de la direction générale.

  art2. Nul ne peut être à la fois membre de la direction générale et de la direction de la bibliothèque s'il n'est pas membre de la direction financère.

  art.3 Aucun membre de la direction de la bibliothèque ne peut être membre de la direction financière.

  On dsigne par f,g,b les propositions atomiques "être membre de la direction financière" [resp. générale], [resp.de la bibliothèque].

  (a) Ecrire sous forme de clauses l'ensemble des 3 articles du règlement.

  (b) Montrer que l'ensemble précédent est logiquement équivalent à l'ensemble des deux propositions suivantes $\{ f \rightarrow g,\ g \rightarrow \neg b \}$. Rédiger un règlement équivalent plus simple.

(9) Montrer que

  (a) $A \vee B$ peut être exprimé en fonction de $\rightarrow$ seulement.

  (b) $A \wedge B$ ne peut pas être exprimé en fonction de $\rightarrow$ seulement.

(10) Combien de fonctions booléennes à une variable, deux variables, n variales peut-on définiré

(11) Montrer que la fonction définie par $h(a, b, c) = (a \vee b) \rightarrow \neg c$ engendre toutes les fonctions de vérité.

(12) Donner la forme normale conjonctive des formules :

(a) $(a \rightarrow b) \rightarrow ((b \rightarrow c) \rightarrow (a \rightarrow c))$

(b) $((a \rightarrow (b \rightarrow c)) \rightarrow ((b \rightarrow (a \rightarrow c))))$

(c) $(\neg a \rightarrow (a \rightarrow b)) \vee c$

(13) Former la conjonction des négations des propositions : $x > 3$ et $x < 3$. Quels nombres satisfont à cette conjonction.

(14) Traduire les expressions suivantes dans le langage du calcul propositionnel :

(a) Si non p ou non q alors ce n'est pas le cas que p ou q.

(b) Si p implique que q implique r, alors p et q ensemble implique r.

(15) Vérifier par la méthode des tables de vérité que les propositions suivantes sont des tautologies :

(a) $\neg\neg p \equiv p$

(b) $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$

(c) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(16) Un énoncé A est satisfiable s'il existe une validation v telle que v(A) $= 1$.

(a) Montrer que A est satisfiable si et seulement si $\neg A$ n'est pas une contradiction.

(b) Soit $D = L_1 \vee L_2 \vee \ldots \vee L_n$ $(n \geq 4)$ et soient c_1, c_2, ..., c_{n-2} des variables propositionnelles qui n'occure pas dans D. On construit E tel que :

$$E = (L_1 \vee L_2 \vee c_1) \wedge (\neg c_1 \vee L_3 \vee c_2) \wedge (\neg c_2 \vee L_4 \vee c_3) \wedge \ldots \wedge (\neg c_{n-3} \vee L_{n-1} \vee c_{n-2} \wedge (\neg c_{n-2} \vee L_n \vee c_1)$$

Montrer que toute validation qui satisfait D peut être tendue pour satisfaire E et réciproquement.

CHAPITRE 3

CALCUL PROPOSITIONNEL FORMEL

1. Système déductif pour le calcul propositionnel

Les tables de vérité (approche sémantique) permettent de décider si un énoncé est une tautologie, une contradiction ou ni l'une ni l'autre. Mais, une bonne partie de la logique que nous verrons par la suite, une telle méthode, ne peut pas lui être appliquée. En conséquence une autre approche,dite déductive, basée sur la formalisation de la théorie est proposée. Cette méthode d'axiomatisation souvent aussi appellée de formalisation prend une place importante dans l'étude de la logique, plus particulièrement en mathématiques et aujourd'hui en informatique. Il serait intéressant d'appliquer cette méthode au calcul propositionnel, partie simple de la logique, pour introduire la notion de déduction.

Pour spécifier notre système du calcul propositionnel formel nous avons besoin d'avoir :

(1) Un alphabet (l'ensemble des symboles utilisés)
(2) Un ensemble de suites finies de ces symboles qui sont appelées formules bien formées. Ce sont les phrases du langage formel.
(3) Un ensemble fini de formules appelées axiomes
(4) Un ensemble fini de règles : les règles de déduction".

DÉFINITION 1.1. *Le systéme formel du calcul proposionnel (CPF) est défini par :*

(1) *L'alphabet est composé de :*
    (a) *a, b, ... z : variables propositionnelles*
    (b) $\neg$, $\rightarrow$ *: symboles primitifs.*
    (c) *(,) : parenthèses.*
(2) *L'ensemble des formules bien formées est défini par induction comme suit :*
    (a) *Chaque variable proposionnelle est une formule bien formée.*
    (b) *Si A et B sont des formules bien formées alors, $A \rightarrow B$ et $\neg B$ sont des formules bien formées.*

(c) *L'ensemble des formules bien formées est engendré par les clauses a) et b) ci-dessus.*

(3) *Axiomes. Pour toutes formules bien formées (fbfs) A, B et C les formules suivantes sont des axiomes du systéme formel CPF.*
- (ax_1) $(A \to (B \to A))$
- (ax_2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- (ax_3) $(\neg B \to \neg A) \to (A \to B)$

(4) *Règles d'inférence appelée modus ponens (MP)*

$$\frac{A, A \to B}{B}\ (MP)$$

En d'autres termes cette règle signifie : B est une conséquence directe de A et $(A \to B)$ où A et B sont des formules bien formées (fbfs).

(5) *Règle de substitution.*

$$\frac{B}{[A/p]B}\ (Sub)$$

La règle de substitution signifie que à partir d'une formule B contenant une variable p, on peut déduire la formule [A/p]B obtenu en remplaçant toutes les occurences de p dans B par une formule A.

Remarquons aussi que les deux symboles $\neg$ et $\to$ ont été introduits sans aucune définition. Ici ils n'ont aucun sens précis. Ce sont de simples marques (des symboles primitifs) intervenant dans la construction des formules. La règle Modus Ponens est la seule règle du système qui nous permet d'obtenir, à partir des axiomes, d'autres formules appelées conclusion de déduction. Cette règle peut être acceptée sans difficultés car elle correspond à quelques détails prés au mode de raisonnement (de déduction) de tous les jours. Les axiomes, au contraire, ne semblent pas intuitifs. Ce sont la partie la moins évidente du système formel. Le choix de l'ensemble des axiomes définit le système formel et détermine souvent les propriétés de ce dernier. Il existe plusieurs systèmes formels du calcul proposionnel. Le système que nous utiliserons ici est parmi les plus étudiés et les plus simples.

Donnons maintenant quelques définitions de nature à préciser ce qu'est un système de déduction formel.

Définition 1.2. *Une démonstration dans le calcul proposionnel est une suite de formules bien formées A_1, A_2, ..., A_n telle que A_i est soit un axiome ou soit A_i se déduit à partir de deux éléments précédants A_j et A_k avec ($j \leq i$) de la suite comme conséquence directe en utilisant la règle de déduction MP ou soit A_i se déduit par application de la règle de substitution à partir d'un élément p pr'ecédent de la suite.*

On dit que la suite A_1, A_2, ..., A_n est une démonstration de A_n. La formule A_n est appelée théorème.

Remarque 1.1. *a) Dans la définition ci-dessus, notons que A_j et A_k doivent nécessairement être de la forme B et (B → A_k) respectivement.*
b) Si A_1, A_2, ..., A_n est une démonstration dans le calcul proposionnel et k<n alors A_1, A_2, ..., A_k est aussi une démonstration. A_k est un théorème.

Exemple 1.1. *Soit la suite :*

1)	$(a \to (b \to a))$	(axiome 1)
2)	$(a \to (b \to a)) \to ((a \to b) \to (a \to a))$	(axiome 2) + (Sub)
3)	$(a \to b) \to (a \to a)$	1) + 2) + MP

Cette suite est une démonstration dans CPF et la formule $(a \to b)) \to (a \to a))$ est un théorème.

Définition 1.3. *Considérons* F *un ensemble de fbfs. La suite A_1, A_2, ..., A_n de formules bien formées est une F-déduction si pour tout i ($1 \leq i \leq n$) nous avons l'un des cas suivants :*

(1) *A_i est un axiome de CPF*

(2) *A_i est un élément de* F

(3) *A_i est déduit à partir des éléments précédants de la suite comme conséquence directe de l'application de la régle MP ou de substitution.*

Une F-déduction est comme une démonstration dans laquelle les éléments de F sont considérés temporairement comme axiomes. Le dernier élément A_n de la suite est déductible de F. Nous le noterons : $F \vdash A_n$

Remarque 1.2. *L'écriture $\vdash A$ signifie que A est un théorème. L'écriture $F \vdash A$. signifie que A est déductible de l'ensemble F.*

Exemple 1.2. *Montrons que $\{A, (B \to (A \to C))\} \vdash (B \to C)$ est une déduction. Ici $\Gamma = \{A, (B \to (B \to C))\}$*

1	$\vdash A$	élément de Γ.
2	$\vdash (B \to (A \to C))$	élément de Γ.
3	$\vdash A \to (B \to A)$	Axiome 1.
4	$\vdash (B \to A)$	1,2 + MP.
5	$\vdash (B \to (A \to C)) \to ((B \to A) \to (B \to C))$	Axiome 2.
6	$\vdash ((B \to A) \to (B \to C))$	2,5 + MP.
7	$\vdash (B \to C)$	2,6+ MP.

EXEMPLE 1.3. *Montrons que les deux formules* $(A \to A)$ *et* $(\neg B \to (\neg B \to (B \to A)))$ *sont des théorèmes.*

Donnons la démonstration que $(A \to A)$ *est un théorème.*

1	$\vdash (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	*Axiome2.*
2	$\vdash (A \to ((A \to A) \to A))$	*Axiome1.*
3	$\vdash (A \to (A \to A)) \to (A \to A)$	*1,2 + MP.*
4	$\vdash (A \to (A \to A))$	*Axiome 1.*
5	$\vdash (A \to A)$	*3,4 + MP.*

La démonstration que la formule $(\neg B \to (\neg B \to (B \to A))$ *est un théorème est proposée au lecteur comme exercice.*

PROPOSITION 1.1. *(Théorème de déduction).*
Si $\Gamma \cup A \vdash B$ *alors* $\Gamma \vdash A \to B$. Γ *est un ensemble de formules qui peut être vide. A est une formule quelconque.*

DÉMONSTRATION. La démonstration se fait par induction sur le nombre de formules dans la suite qui forme la déduction de B à partir de $\Gamma \cup$ A.

cas 1: B est axiome. On déduit $A \to B$ à partir de Γ comme suit.

(1) $\vdash B$ axiome.

(2) $\vdash (B \to (A \to B))$ Axiome1.

(3) $\vdash (A \to B)$ 1,2 + MP.

D'où $\Gamma \vdash (A \to B)$.

cas 2: B $\in \Gamma$; ce qui suit est une déduction de $\Gamma \vdash$ (A $\to$ B).

1	$\vdash$ B	élément de Γ
2	$\vdash$ (B $\to$ (A $\to$ B))	Axiome 1.
3	$\vdash$ (A $\to$ B)	1, 2 + MP.

cas 3: B $\equiv$ A. Nous avons vu que (A $\to$ A) est un théorème. La démonstration dans CPF de (A $\to$ A) servira de déduction de (A $\to$ A) à partir de Γ. Ceci termine la démonstration de la base d'induction.

Supposons maintenant que la déduction de B à partir de $\Gamma \cup$ A est une suite avec n éléments (n>1) et que la proposition est vérifiée pour toute formule déduite de $\Gamma \cup$ A dont la démonstration est une suite de formules ayant moins de n éléments : C'est l'hypothèse d'induction.

cas 1: B est un axiome de CPF. Ce cas est identique au cas 1 de la base d'induction.

cas 2: B $\in \Gamma$, $\Gamma \vdash$ (A $\to$ B). C'est le même cas que le cas 2 précédant.

cas 3: B est identique à A. C'est le même cas que le cas 3 précédant.

cas 4: B est obtenue à partir de deux précédantes fbfs et par application de la règle de déduction MP. Ces deux fbfs doivent avoir la forme C et C $\rightarrow$ B et chacune d'elle est déduite à partir de $\Gamma \cup$ A et chacune de leur démonstration contient moins de n éléments. Par hypothèse d'induction nous avons :
$\Gamma \vdash$ (A $\rightarrow$ C) et $\Gamma \vdash$ (A $\rightarrow$ (C $\rightarrow$ B)).

La déduction de (A $\rightarrow$ B) à partir de Γ peut être donnée comme suit :
(1)
$\vdots$
(k) (A $\rightarrow$ C)
$\vdots$
(l) (A $\rightarrow$ (C $\rightarrow$ B))
(l+1) (A $\rightarrow$ (C $\rightarrow$ B)) $\rightarrow$ ((A $\rightarrow$ C) $\rightarrow$ (A $\rightarrow$ B)) Axiome 2.
(l+2) (A $\rightarrow$ C) $\rightarrow$ (A $\rightarrow$ B) 1, l+1 + MP.
(l+3) (A $\rightarrow$ B) k, l+2 + MP.

□

PROPOSITION 1.2. *(réciproque du théorème de déduction.)*
Si $\Gamma \vdash$ *(A* $\rightarrow$ *B) alors* $\Gamma \cup A \vdash$ *B.*

DÉMONSTRATION. Soit une déduction de (A $\rightarrow$ B) à partir de Γ. Notre objectif est de construire une démonstration de B à partir de $\Gamma \cup A$.
(1)
$\vdots$
(k) (A $\rightarrow$ B) □
(k+1) A élément de $\Gamma \cup$ A.
(k+2) B k, k+1 + MP.

COROLLAIRE 1.1. *Pour toutes fbfs. A, B et C nous avons :*
(A $\rightarrow$ *B), (B* $\rightarrow$ *C)* $\vdash$ *(A* $\rightarrow$ *C). C'est le syllogisme hypothétique.*

DÉMONSTRATION. La preuve est comme suit :

(1)	$\vdash$ (A $\rightarrow$ B)	hypothèse
(2)	$\vdash$ (B $\rightarrow$ C)	hypothèse
(3)	$\vdash$ A	hypothèse
(4)	$\vdash$ B	1, 3 + MP.
(5)	$\vdash$ C	2,4 + MP.

Nous avons démontré (A $\rightarrow$ B), (B $\rightarrow$ C), A $\vdash$ C
En appliquant le théorème de déduction (TD) nous obtenons :

$(\mathrm{A} \rightarrow \mathrm{B}), (\mathrm{B} \rightarrow \mathrm{C}) \vdash (\mathrm{A} \rightarrow \mathrm{C})$

□

EXEMPLE 1.4. *Soit à démontrer que les deux formules :*

(1) $(\neg B \rightarrow (B \rightarrow A))$

(2) $((\neg A \rightarrow A) \rightarrow A)$

La démonstration de (1) est :

(1) $\vdash$	$(\neg B \rightarrow (\neg A \rightarrow \neg B))$	*Axiome 1.*
(2) $\vdash$	$((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A))$	*Axiome 3.*
(3) $\vdash (\neg B \rightarrow (B \rightarrow A))$	*1,2 + SH.*	

La démonstration de (2) est :

(1) $(\neg A \rightarrow (\neg\neg(\neg A \rightarrow A) \rightarrow \neg A))$ *par l'axiome 1.*

(2) $(\neg\neg(\neg A \rightarrow A) \rightarrow \neg A) \rightarrow (A \rightarrow \neg(\neg A \rightarrow A))$ *Axiome 3.*

(3) $(\neg A \rightarrow (A \rightarrow \neg(\neg A \rightarrow A)))$ *par 1, 2 + SH.*

(4) $(\neg A \rightarrow (A \rightarrow \neg(\neg A \rightarrow A))) \rightarrow (\neg A \rightarrow A) \rightarrow (\neg A \rightarrow \neg(\neg A \rightarrow A))))$ *Axiome 2*

(5) $(\neg A \rightarrow A) \rightarrow (\neg A \rightarrow \neg(\neg A \rightarrow A))))$ *par 3, 4 +MP.*

(6) $(\neg A \rightarrow \neg(\neg A \rightarrow A))$ *par 1, 5+ MP.*

(7) $(\neg A \rightarrow \neg(\neg A \rightarrow A)) \rightarrow ((\neg A \rightarrow A) \rightarrow A)$ *Axiome 3.*

(8) $((\neg A \rightarrow A) \rightarrow A)$ *par 6,7 + MP.*

2. Adéquation et complétude du CPF.

Nous allons établir un lien entre la méthode des tables de vérité et la méthode axiomatique, appliquée au calcul propositionnel. Nous tirerons profit des liens entre ces deux approches pour montrer la consistance du calcul proposionnel formel.

DÉFINITION 2.1. *Une valuation de CPF est une fonction v dont le domaine de définition est l'ensemble des fbfs. et l'ensemble des valeurs est {T, F }. Elle est définie par :*

(1) $v(A) \not\models v(\neg A)$

(2)

$$v(A \rightarrow B) = \begin{cases} F & \text{ssi } v(A) = T \text{ et } v(B) = F \\ T & \text{sinon} \end{cases}$$

DÉFINITION 2.2. *Une fbf A du CPF est une tautologie si pour chaque valuation v,* $v(A) = T$.

REMARQUE 2.1. *Nous pouvons constater aisement que la définition de la notion de tautologie à l'aide des valuations est exactement la même que celle donnée à l'aide des tables de vérité. Les tables de vérité sont construites à partir des définitions des connecteurs. Les valuations sont définies en attribuant un "sens" ou une valeur aux marques (* $\neg$ *et* $\rightarrow$*) utilisées dans le CPF. C'est là toute la différence.*

Ennonçons maintenant le théorème d'adequation qui permet de montrer que tous les théorèmes du CPF sont des tautologies. Cela signifie que les formules démontrées à partir des axiomes en utilisant la règle de Modus ponens sont des formules toujours vraies dans le sens, où elles sont considérées comme des énoncés du calcul proposionnel, elles prennent la valeur vraie.

THÉORÈME 2.1. *Tout théorème du CPF est une tautologie.*

DÉMONSTRATION. La démonstration se fait par induction sur la longueur de la démonstration du théorème. Il s'agit de vérifier que tous les axiomes sont des tautologies et montrer ensuite que dans une démonstration chaque formule intermédiaire est une tautologie. □

La réciproque de ce théorème est le théorème de complètude qui répond à la question : Toute formule vraie du CP est-elle un théorème ?

THÉORÈME 2.2. *(complétude). Toute tautologie du Calcul Proposionnel est un théorème.*

Avant de démontrer ce théorème nous avons besoin de démontrer les résultats suivants.

LEMME 2.1. *Soit A une formule du CPF et* p_1, p_2, p_3, ..., p_k *des formules atomiques dans A et soient*

$$p_i' = \begin{cases} p_i & \textit{si } p_i = \textit{1} \\ \neg p_i & \textit{si } p_i = \textit{0} \end{cases}$$

et

$$A_i' = \begin{cases} A_i & \textit{si } A_i = \textit{1} \\ \neg A_i & \textit{si } A_i = \textit{0} \end{cases}$$

Alors nous avons : p'$_1$, *p'*$_2$, ..., *p'*$_k$ $\vdash$ *A'.*

DÉMONSTRATION. La démonstration se fait par induction sur le nombre d'occurences des symboles logiques $\neg$ et $\rightarrow$ contenus dans A. Si n=0 alors A est p et on a bien $\mathrm{p}_1 \vdash \mathrm{p}_1$ et $\neg\mathrm{p}_1 \vdash \neg\mathrm{p}_1$.

cas 1: Si A est ¬B alors B a moins de n occurences de symboles logiques. Si B prend la valeur 1 pour l'ensemble des valeurs attribuées à $p_1,\ldots,p_k$ alors A prend la valeur 0. Donc B' est B et A' est ¬A. Par hypothèse d'induction nous avons : $p'_1,\ldots p'_k \vdash$ B ou encore $p'_1,\ldots p'_k \vdash \neg\neg$B. Mais ¬¬B est A' et donc $p'_1,\ldots p'_k \vdash$ A'. Si B prend la valeur 0 alors B' est ¬B et A' est A. Nous avons dans ce cas $p'_1,\ldots p'_k \vdash \neg$B et donc $p'_1,\ldots p'_k \vdash$ A'.

cas 2: A est (B → C). B et C contiennent moins de symboles logiques que A. $p'_1,\ldots p'_k \vdash$ B' et $p'_1,\ldots p'_k \vdash$ C' découlent par hypothèse d'induction.
a) B prend la valeur 0, A prend la valeur 1. B' est ¬B et A' est A. $p'_1,\ldots p'_k \vdash \neg$B. En utilisant le théorème $\vdash (\neg B \to (B \to C))$ et $p'_1,\ldots p'_k \vdash \neg$B et la règle MP. on obtient : $p'_1,\ldots p'_k \vdash (B \to C)$. Mais comme $(B \to C)$ est A' alors $p'_1,\ldots p'_k \vdash$ A'.
b) C prend la valeur 1 alors A prend la valeur 1, C est C' est A' est A. $p'_1,\ldots p'_k \vdash$ C ou $p'_1,\ldots p'_k \vdash$ C'. En utilisant le théorème $\vdash (C \to (B \to C))$, $p'_1,\ldots p'_k \vdash$ C et MP on obtient : $p'_1,\ldots p'_k \vdash (B \to C)$.

cas 3: B prend la valeur 1 et C prend la valeur 0. A prend la valeur 0, B' est B, C' est ¬C et A' est ¬A. $p'_1,\ldots p'_k \vdash$ B et $p'_1,\ldots p'_k \vdash \neg$C. D'aprés le théorème : $\vdash B \to (\neg C \to \neg(B \to C))$.
nous avons $p'_1,\ldots p'_k \vdash \neg(B \to C)$. Mais $(B \to C)$ est A, A' est donc $\neg(B \to C)$. Finalement nous avons montré : $p'_1,\ldots p'_k \vdash$ A'.

□

Démonstration du théorème. Soit A une tautologie et soient $p_1,\ldots p_k$ les formules atomiques de A. D'aprés le lemme précédant et le fait que A' ≡ A nous avons $p'_1,\ldots p'_k \vdash$ A. Si p_k prend la valeur 1 alors $p'_1,\ldots, p'_{k-1}\ p_k \vdash$ A et si p_k prend la valeur 0 alors $p'_1,\ldots,p'_{k-1}, \neg p_k \vdash$ A. En appliquant le théorème de déduction on peut écrire : $p'_1,\ldots p'_{k-1} \vdash (p_k \to A)$ et $p'_1,\ldots p'_{k-1} \vdash (\neg p_k \to A)$. Nous obtenons en appliquant la règle MP et le théorème $\vdash (p_k \to A) \to (\neg p_k \to A) \to A)$ la déduction $p'_1,\ldots p'_{k-1} \vdash$ A. On peut refaire le même raisonnement avec p'_{k-1} et l'éliminer et puis recommencer avec p'_{k-2} et ainsi de suite jusqu'à obtenir ⊢ A.

Corollaire 2.1. *Le système CPF est consistant : Il n'existe aucune formule A telle que ¬A et A sont des théorèmes.*

Démonstration. Nous avons montré que tout théorème de CPF est une tautologie. La négation d'une tautologie n'est pas une tautologie. A et ¬A ne peuvent être toutes les deux des théorèmes. □

3. Méthode de Davis Putnam pour le calcul propositionnel.

Le problème qui nous intéresse içi est la validité de la déduction $\mathbf{H} \models$ A qui signifie que A découle de l'hypothèse H et où **H** est un ensemble de propositions et A une proposition. Nous pouvons aisement voir d'après les résultats des chapitres précédents que ceci revient á prouver que l'ensemble des propositions $\mathbf{F} = \mathbf{H} \cup \{\neg \mathrm{A}\}$ est contradictoire (c.à.d un sous ensemble fini de propositions de **F** est contradictoire).

Les tables de vérité offrent, en principe, une méthode pour décider de la valdité ou de la contradiction d'un ensemble de propositions. Mais, nous savons que l'utilisation d'une telle méthode est trés lourde si le nombre de variables propositionnelles intevenant dans la formule **F** est très grand.

La méthode de démonstration du calcul propositionnel formel est difficile à mettre en oeuvre algorithmiquement. Ceci est essentiellement dû à l'existence d'une infinité de schémas d'axiomes et à la nature de la règle d'inférence Modus Ponens.

La méthode définie par Davis Putnam, que nous introduirons ici, est destinée à prouver des théorèmes à l'aide de procédure que l'on peut programmer. Sa généralisation au calcul des prédicats constitue aujourd'hui le fondement de la programmation logique et la base de la démonstration automatique de théorèmes.

Considérons **P** l'ensemble des variables propositionnelles, un **littéral** est une proposition qui se présente sous la forme p_i ou $\neg \mathrm{p}_i$ avec $\mathrm{p}_i \in \mathbf{P}$. Une proposition C est dite une **clause** si **C** est une disjonction de littéraux :

$$\mathrm{C} = \mathrm{p}_1 \vee \mathrm{p}_2 \vee \ldots \vee \mathrm{p}_i \vee \mathrm{p}_{i+1} \vee \ldots \vee \mathrm{p}_n$$

avec pour tout i $\leq$n, p_i est un littéral. Si n=0 , **C** est la clause vide qui sera notée $\mathbf{C} = \epsilon$ (= faux). On admettera que dans une clause il n'y a pas de répétition d'un même littéral. Les littéraux p et $\neg$p sont dits opposés. Une paire {p,p'} de littéraux est dite opposée si p et p' sont opposés.

Remarque 3.1. *Notons que les propositions sont ici écrites seulement à l'aide des deux connecteurs $\neg$ et $\vee$. Ces deux connecteurs forment un ensemble $\{\neg, \vee\}$ complet de connecteurs.*

La méthode de Davis Putnam pour décider si une conjonction

$$S = G_1 \wedge G_2 \wedge \ldots \wedge G_n$$

de clauses G_i est un insatisfaite consiste à appliquer autant de fois qu'il est possible les règles citées ci-dessous. Dans chaque étape la conjonction S est tranformée en une nouvelle conjonction S' telle que S est insatisfaite si et seulement si S' est insatisfaite ou transformée en une nouvelle paire de conjonction S' et S'' telle que S est insatisfaite si et seulement si S' et S'' sont insatisfaites.

(1) **Règles pour clauses à un litéral.**
   (a) Si les deux clauses à un litéral $G_i = l$ et $G_j = \neg l$ occurent dans la clause S alors S est insatisfaite.
   (b) Si la règle (a) ne s'applique pas et S contient une clause à un litéral $G_i = l$, S' est obtenu à partir de S en supprimant toute les clauses dans S contenant l (G_i incluse) et en supprimant les occurences des litéraux opposés $\neg l$ des clauses restantes. Si S' est vide, S est satisfaite.

(2) **Règle d''élimination.** Si la règle (1) ne s'applique pas et un litéral l occure dans S alors que son opposé ($\neg l$) n'occure pas dans S, alors supprimer toute les clauses G_i contenant l. La clause S' ainsi obtenue est insatisfaite si et seulement si S est insatisfaite. Si S' est vide alors S est satisfaite.

(3) **Règle de consensus.** Supposant que les deux règles (1) et(2) ne s'appliquent pas. Il existe donc un litéral l et son opposé $\neg l$ qui occurent dans S. Alors S peut se mettre sous la forme :

$$\begin{gathered}(A_1 \vee l) \wedge \ldots \wedge (A_n \vee l) \wedge \\ (B_1 \vee \neg l) \wedge \ldots \wedge (B_m \vee \neg l) \wedge \\ R_1 \wedge \ldots \wedge R_p\end{gathered}$$

Les clauses A_i, B_i et R_i ne contiennent ni l et ni $\neg l$. Alors nous avons les conjonctions $S' = (A_1 \wedge \ldots \wedge A_n) \wedge R_1 \wedge \ldots \wedge R_p$ et $S'' = (B_1 \wedge \ldots \wedge B_m) \wedge R_1 \wedge \ldots \wedge R_p$. alors, S est insatisfaite si et seulement si $(S' \vee S'')$ est insatisfaite.

Exemple 3.1. *Soit la formule :*

$$S = (p_1(a) \vee p_2(b)) \wedge \neg p_2(b) \wedge (\neg p_1(a) \vee p_2(b) \vee \neg p_3(a))$$

En appliquant la règle 1b sur $\neg p_2(b)$ *on obtient :*

$$p_1(a) \wedge (\neg p_1(a) \vee \neg p_3(a))$$

En appliquant la règle 1b sur $p_1(a)$ *on obtient :*

$$\neg p_3(a)$$

Finalement en appliquant la règle 1b sur $\neg p_3(a)$ on obtient la clause vide, ce qui implique que S est satisfaite.

Exemple 3.2. *Soit la formule :*

$$(a \vee b) \wedge (a \vee \neg c) \wedge (\neg a \vee c) \wedge (\neg a \vee \neg b) \wedge (c \vee \neg b) \wedge (\neg c \vee b)$$

Par r ?gle du consensus sur a

$b \wedge \neg c \wedge (c \vee \neg b) \wedge (\neg c \vee b)$	$c \wedge \neg b \wedge (c \vee \neg b) \wedge (\neg c \vee b)$
$\neg c \wedge c$ *(par 1b sur b)*	$\neg b \wedge b$ *(par 1b sur c)*
contradiction (par 1a)	*contradiction (par 1a)*

4. 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 $\Gamma = \{A_1, A_2, \ldots, A_n\}$ et Δ= $\{B_1, \ldots, B_k\}$ alors le séquent $\{A_1, \ldots, A_n\} \vdash \{B_1, \ldots, B_k\}$ sera écrit simplement :

$$A_1, \ldots, A_n \vdash B_1, \ldots, B_k$$

.

Soit X une formule, Γ et Δ deux ensembles de formules nous écrirons :

$$\Gamma,\ X \vdash \Delta \text{ au lieu de } \Gamma \cup \{X\} \vdash \Delta.$$

$$\vdash \Delta \text{ au lieu de } \emptyset \vdash \Delta.$$

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 :*

$$v(\Gamma \vdash \Delta) = 1 \textit{ si } v(X) = 0 \textit{ pour un certain } X \in \Gamma \textit{ ou } v(Y) = 1 \textit{ pour un certain } Y \in \Delta.$$

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

$$(A_1 \wedge \ldots \wedge A_n) \vdash (B_1 \vee \ldots \vee B_k).$$

Définition 4.3. *Les axiomes et les règles d'inférence du calcul des séquents sont :*
(Axiome) $X \vdash X$.

$$\frac{\Gamma \vdash \Delta, X}{\Gamma, \neg X \vdash \Delta}\ (\neg - gauche) \qquad \frac{\Gamma, X \vdash \Delta}{\Gamma \vdash \Delta, \neg X}\ (\neg - droit)$$

$$\frac{\Gamma, X, Y \vdash \Delta}{\Gamma, X \wedge Y \vdash \Delta}\ (\wedge - gauche) \qquad \frac{\Gamma \vdash \Delta, X \quad \Gamma \vdash \Delta, Y}{\Gamma, \vdash \Delta, X \wedge Y}\ (\wedge - droit)$$

$$\frac{\Gamma, X \vdash \Delta \quad \Gamma, Y \vdash \Delta}{\Gamma, X \vee Y \vdash \Delta}\ (\vee - gauche) \qquad \frac{\Gamma \vdash \Delta, X, Y}{\Gamma \vdash \Delta, X \vee Y}\ (\vee - droit)$$

$$\frac{\Gamma \vdash \Delta, X \qquad \Gamma, Y \vdash \Delta}{\Gamma, X \rightarrow Y \vdash \Delta}\ (\rightarrow -gauche) \qquad \frac{\Gamma, X \vdash \Delta, Y}{\Gamma \vdash \Delta, X \rightarrow Y}\ (\rightarrow -droit)$$

Dans un règle, par exemple $(\rightarrow\ -droit)$, le séquent $\Gamma, X \vdash \Delta, Y$ est appellé prémisse de la règle et le séquent $\Gamma \vdash \Delta, X \rightarrow Y$ la conclusion de la règle.

Exemple 4.1. *Soit la formule* $\neg(P \wedge Q) \vdash (\neg P \vee \neg Q)$. *Sa preuve dans le calcul des séquents est la suivante :*

1. $P \vdash P$ *2.* $Q \vdash Q$.

3. $P, Q \vdash P$ *4.* $P, Q \vdash Q$

5. $P, Q \vdash P \wedge Q$

6. $Q \vdash P \wedge Q, \neg P$

7. $\vdash P \wedge Q, \neg P, \neg Q$

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

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

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

Sous forme d'arbre la preuve sera présentée par :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P \vdash P \qquad Q \vdash Q}{P, Q \vdash P, \qquad P, Q \vdash Q}\ (Axiome)}{Q \vdash P \wedge Q, \neg P}\ (\wedge - droit)}{\vdash P \wedge Q, \neg P, \neg Q}\ (\neg - droit)}{\neg(P \wedge Q) \vdash \neg P, \neg Q}\ (\neg - gauche)}{\neg(P \wedge Q) \vdash \neg P \vee \neg Q}\ (\vee - droit)$$

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

LEMME 4.2. *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 admetterons ici les deux lemmes sans les démontrer.

Une preuve en calcul des séquents se présente comme un arbre dont les feuilles sont étiquetées par des axiomes, la racine est étiquetée par le séquent é prouver, et les noeuds internes sont étiquétés par le séquent inférieur obtenu par applicalication d'une règle d'introduction. Pour démontrer une proposition F, il suffit de montrer le séquent $\vdash F$. Un séquent $\Gamma \vdash \Delta$ est valide si et seulement si il posséde une preuve dans le calcul des séquents ci-dessus.

Nous admetterons, aussi, sans démonstration les deux théorèmes suivants :

THÉORÈME 4.1. *Si X est un théorème du calcul des séquents alors X est une tautologie.*

THÉORÈME 4.2. *Si X est une tautologie alors X est un théorème du calcul des séquents.*

5. Exercices.

I. Montrer que les formules suivantes sont des théorèmes :

(1) $(\mathrm{A} \rightarrow \mathrm{B}) \rightarrow ((\neg \mathrm{A} \rightarrow \mathrm{B}) \rightarrow \mathrm{B})$.
(2) $(\mathrm{A} \rightarrow (\neg \mathrm{B} \rightarrow \neg(\mathrm{A} \rightarrow \mathrm{B}))$.
(3) $\neg \mathrm{B} \rightarrow (\mathrm{B} \rightarrow \mathrm{A})$

II. Soit CPF^+ une extension de CPF obtenue en ajoutant un quatrième axiome :

$$((\neg \mathrm{A} \rightarrow \mathrm{B}\ ) \rightarrow (\mathrm{A} \rightarrow \neg \mathrm{B})).$$

Montrer que CPF^+ est inconsistant.

III. Montrer que si B est une contradiction alors B n'est théorème d'aucune extension consistante de CPF.

IV. Montrer en utilisant la procédure de Davis-Putnam que les formules suivantes sont des tautologies.

(1) $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$
(2) $((P \rightarrow Q) \rightarrow (P \rightarrow R)) \rightarrow (P \rightarrow (Q \rightarrow R))$
(3) $(P \rightarrow Q) \vee (Q \rightarrow R)$

V. Impl ?menter la proc ?dure de Davis-Putnam en Lisp ou caml.

VI. Donner les preuves dans le calcul des s ?quents des formules :

(1) $X \supset (Y \supset X)$
(2) $(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))$
(3) $(\neg X \supset \neg Y) \supset ((\neg X \supset Y) \supset X)$
(4) $((X \supset Y) \supset X) \supset X$
(5) $(\neg B \supset \neg A) \supset (A \supset B)$

VII. Montrer que si $\Gamma \rightarrow \Delta, \neg X$ est un th ?or ?me dans le calcul des s ?quents alors $\Gamma, X \rightarrow \Delta$ est aussi un th ?or ?me.

VIII.

(1) Appliquer la méthode de Davis-Putnam pour montrer que la formule suivante est valide : $((p \wedge q) \wedge (q \wedge r)) \rightarrow (p \rightarrow (q \wedge r))$
(2) Appliquer le calcul des séquents pour montrer que la formule suivante est valide :

$$(p \supset (q \wedge (r \vee s)) \wedge (\neg q \vee \neg r)) \supset (p \supset s)$$

CHAPITRE 4

Calcul des Prédicalts du premier ordre.

1. Langage du calcul des prédicats.

Le calcul des prédicats est considéré comme une extension du calcul propositionnel qui offre la possibilité d'introduire en même temps que les variables propositionnelles d'autres variables appartenant à un domaine arbitraire (ensemble d'entiers, de réels ou d'objets quelconques). Cette extension est obtenue grâce à l'introduction des deux quantificateurs $\exists$ et $\forall$.

La formule $\exists x P(x)$ se lit : Il existe x $\in$ D tel que $P(x)$ est vraie et, la formule $\forall x P(x)$ se lit : Pour tout x $\in$ D, $P(x)$ est vraie. L'ensemble D est ici le domaine de définition du prédicat P.

Avant de définir le langage du calcul des prédicats i.e l'ensemble des formules bien formées (correctement ï£¡crites) nous allons d'abord préciser :

(1) **L'alphabet** du langage du calcul des prédicats est composé de :

x_1,x_2, $\ldots$	les variables
a_1,a_2, $\ldots$	les constantes
P_1,P_2, $\ldots$	les prédicats
f_1,f_2, $\ldots$	les fonctions
$\neg$, $\rightarrow$	les connecteurs
$\exists$, $\forall$	les quantificateurs

(2) **Les termes**. Les termes du calcul des prédicats (`CP.`) sont définis comme suit :

(a) Les variables et les constantes sont des termes.

(b) Si f_i est une fonction à n arguments du `CP`. et t_1, t_2, $\ldots$, t_n sont des termes alors $\mathrm{f}_i(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_n)$ est un terme du `CP`.

(c) L'ensemble des termes est engendré par les clauses (a) et (b).

Exemple 1.1. *x_i, $f_1(x_i)$, $g_2(x,f_1(x_i))$ sont des termes.*

Définition 1.1. **(formule atomique)**.

Une formule atomique du CP. *est définie par :*
Si P_i *est un prédicat i.e une fonction définie d'un domaine D vers l'ensemble* $\{0,1\}$ *et* t_1, t_2, ..., t_n *sont des termes alors* $P_i(t_1, t_2, \ldots, t_n)$ *est une formule atomique.*

DÉFINITION 1.2. **(formules bien formées).** *Les formules bien formées (ou formule tout simplement) sont définies par :*

(1) *Chaque formule atomique est une formule bien formée.*
(2) *Si A, B sont des formules bien formées du* CP. *alors* $\neg A$, $(A \to B)$, $(\forall x)A$, *et* $(\exists x)A$ *sont des formules bien formées.*
(3) *L'ensemble de toutes les formules bien formées est engendré par les clauses (1) et (2).*

EXEMPLE 1.2. *Les formules suivantes sont des formules bien formées :*

(1) $F \equiv \forall x A(x) \to (\forall y((P(f(x),0) \to (P(g(y),b)))$
(2) $G \equiv (P(f(a),b)) \to \forall x\,((\neg P(x,0)) \wedge P(f(x), g(x, f(x))))$

2. Notion de variables libres et de variables liées

Dans la formule ∀xA la formule A est dite champ du quantificateur ∀. La variable x est dite variable quantifiée par le quantificateur universel ∀. Les positions occupées par la variable x dans la formule A sont appelées occurences de x. Dans la formule précédante F la variable x possède deux occurences.

DÉFINITION 2.1. *Une occurence d'une variable x dans une formule est dite liée si elle possède une occurrence dans le champ d'un quantificateur ∀ (ou ∃) dans cette formule. Si une occurrence d'une variable n'est pas liée, elle est libre.*

EXEMPLE 2.1. $F \equiv \forall x A(\underline{x}) \to \big(\forall y((P(f(\underline{\underline{x}}),0) \to (P(g(y),b))\big)$
La première occurence de la variable x est liée par le quantificateur ∀x, mais la deuxième occurence de la variable x est libre.

DÉFINITION 2.2. *Soit A une formule du calcul des prédicats. Un terme t est libre pour la variable x dans A si aucune occurence libre de x dans A n'appartient à un champ d'un quantificateur (∀y) où y est une variable dans t.*

EXEMPLE 2.2. *le terme f(x,v) n'est pas libre pour y dans la formule :*

$$\forall x P(x,y) \to \forall z Q(z,x).$$

Le terme g(w,z) est libre pour y dans la formule $\forall x P(x,y) \to \forall z Q(z,x)$.

3. Interprétation

On attribue un "sens" (une valeur de vérité !) à chacune des formules en "interprétant" les différents symboles (fonctions, prédicats), les constantes et les variables. Ainsi, pour une formule particulière, nous pouvons obtenir plusieurs interprétations dépendant du sens que l'on donnera aux symboles de cette formule. Considérons par exemple la formule $\forall x \exists y P(x,y)$. Plaçons nous dans l'ensemble des entiers naturels (c.a.d x, y $\in \mathtt{N}$) et interprétons P(x,y) comme étant la relation " x $\leq$ y". Pour cette interprétation la formule devient $\forall x \exists y (x \leq y)$. Remarquons qu'il est aisé, dans ce cas, de voir si cette formule est une proposition vraie ou une proposition fausse.

Définition 3.1. *Soit une formule F du* CP *telle que :*
– *$\{P_1, \ldots P_n\ \}$ sont les prédicats contenus dans F.*
– *$\{F_1, \ldots F_k\ \}$ sont les symboles de fonctions contenus dans F.*
– *$\{a_1, \ldots a_m\ \}$ sont les constantes contenues dans F.*
Une interprétation I *de F consiste en la donnée :*

(1) *d'un ensemble non vide $\mathtt{D}_I$ appellé le domaine de l'interprétation* I.
(2) *d'une assignation $d_j \in \mathtt{D}_I$ à chaque constante a_j.*
(3) *d'une assignation d'une relation n-aire R_i à chaque prédicat n-aire P_i.*
(4) *d'une assignation d'une fonction n-aire f_i à chaque symbole de fonction n-aire F_i.*

Exemple 3.1. *Soit la formule (∀x)(∀y)(∃z)P(f(x,y), z). Pour l'interpréter cette formule nous devons spécifier chacun des éléments du quadruplet caractérisant la définition d'une interprétation. Soit par exemple :*

(1) $\mathtt{D}_I \equiv \mathtt{N}$ *l'ensemble des entiers naturels.*

(2) *Assigner àă la fonction f, la fonction $f : \mathtt{N} \times \mathtt{N} \to \mathtt{N}$ definie par f(x,y) = x + y,*
(3) *Assigner au prédicat P, la relation suivante :*
$R : \mathtt{N} \times \mathtt{N} \to \mathtt{N}$ *definie par* $R(x,y) =$ "$x = y''$.

4. Satisfaction, Valeurs de vérité

La formule précédante (∀x)(∀y)(∃z)P(f(x,y), z) interprétée dans I de l'exemple précédent donne la formule : $(\forall x)(\forall y)(\exists z)(x + y = z)$.

Nous remarquons qu'il nous est plus facile de dire si cette dernière formule prend toujours la valeur vraie ou la valeur fausse ou bien ni l'une ni l'autre. Pour pouvoir, dans le cas général, décider de la valeur de vérité d'une formule nous introduisons les notions de valeur d'une formule dans une interprétation I.

DÉFINITION 4.1. *Soit A une formule du calcul des prédicats et soit* I *une interprétation. Une valeur v(A) dans* I *est définie d'abord en remplaçant chaque constante* a_i *de A par un élément* d_i *de I et par induction sur la structure de A : comme suit :*

(1) *Si* $A = P(t_1, \ldots, t_n)$ *alors* $v(A) = T$ *ssi* $R_v(v(t_1, \ldots, v(t_n))$ *est vraie dans* $\mathtt{D}_{\mathtt{I}}$.
(2) *Si* $A = (\neg\ B)$ *alors* $v(A) = \neg v(B)$.
(3) *Si* $A = B \rightarrow C)$ *alors* $v(A) = \neg v(B)$ *ou bien* $v(A)= v(C)$.
(4) $A = (\forall x)B$ *alors* $v(A) = T$ *ssi pour tout* $c \in \mathtt{D}_{\mathtt{I}}\ = T$.

EXEMPLE 4.1. *Soit la formule* $G : \forall y\ P(y) \rightarrow (a = y)$. *Soit* N*, l'ensemble des entiers naturels, le domaine d'interprétation. Soit v une validation quelconque sur* N *telle que* $v(P(y)) = P_v(v(y))$. *Il y'a deux cas à distinguer :*

(1) *Si* $v(P(y))= F$ *alors* $v(\neg P(y))=T$ *et donc* $v(G) = T$.
(2) *Si* $v(P(y))=T$ *alors* $v(y = a)= T$ *où a est la valeur de y pour laquelle* $v(P(y))=T$.

DÉFINITION 4.2. *Une formule A est vraie dans une interprétation* I *si* $v(A) = T$ *dans* I. *Une formule A est dite satisfaite s'il existe une interprétation I telle que A est vraie dans I. Une formule du calcul des prédicats est dite valide si elle est vraie pour toute interprétation. Elle est dite non valide s'il existe au moins une interprétation pour laquelle la formule n'est pas vraie (fausse) ou possède un contr-modèle. Une formule du calcul des prédicats est dite insatisfaisable si elle est fausse pour toute interprétation.*

Notation. $\mathtt{I} \models$ A signifie A est vraie dans I. Il existe une relation importante entre modèle et contre-modèle qui sera exploitée plus loin.

PROPOSITION 4.1. *Si les deux formules A et* $(A \rightarrow B)$ *sont vraies alors la formule B est vraie.*

DÉMONSTRATION. Soit l'interprétation I. v(A) = T et v(A → B) = T. Par définition v(¬A) = T ou v(B) = T Or v(¬A) ≠ T car v(A) = T. Donc v(B) = T. □

PROPOSITION 4.2. *Soit A une formule et* I *une interprétation, alors* $\mathtt{I} \models A \leftrightarrow \forall x A$ *où x est une variable quelconque.*

DÉMONSTRATION. Supposons que nous avons $\mathtt{I} \models$ A et v(A) =T dans $\mathtt{I}$. Soit x une constante occurnant dans A. Donc v et chaque validation v' x-équivalente à v satisfait aussi A car toute validation satisfait A dans $\mathtt{I}$. Donc v ([d/x]A) = T pour tout d $\in D_I$ et par définition v($\forall$ x A) = T. D'où $\mathtt{I} \models \forall$xA. La réciproque $\mathtt{I} \models \forall$xA $\rightarrow \mathtt{I} \models$ A est immédiate. □

LEMME 4.1. *Une formule A est valide ssi $\neg A$ est insatisfaisable.*

La démonstration de ce lemme est immédiate et elle est laissée comme exercice au lecteur.

EXEMPLE 4.2. *Montrons que la formule*

$$\forall x \forall y \, [(x \neq y) \vee P(x,y) \vee \neg P(y,x))]$$

est valide. Il y'a deux cas à distinguer quelque soit l'interprétation $\mathtt{I}$ *considérée :*

(1) $x = y$.

P(x,y) $\vee$ $\neg$P(y,x) devient P(x,x) $\vee$ $\neg$P(x,x) et donne toujours la valeur vraie à la formule.

(2) $x \neq y$.

Dans ce cas $x \neq y$ donne toujours la valeur vraie à la formule considérée.

5. Exercices.

(1) Soient les phrases suivantes :
   (a) Tout étudiant qui travaille réussit.
   (b) Tout étudiant qui comprend et qui est intelligent réussit ses examens.
   (c) A est un étudiant qui travaille.
   (d) A est intelligent.

   Utiliser le langage des prédicats du premier ordre pour symboliser chacune des phrases précédantes.
(2) Montrer que les formules suivantes sont valides :
   (a) $\forall x(p(x) \vee q(x)) \rightarrow (\forall x p(x) \vee \forall x q(x))$
   (b) $(\exists x p(x) \wedge \exists x q(x)) \rightarrow \exists x(p(x) \wedge q(x))$
   (c) $\forall x A(x) \rightarrow \exists x A(x)$.
   (d) $(\exists x A(x) \rightarrow \forall x B(x)) \rightarrow \forall x(A(x) \rightarrow B(x))$
(3) Étudier la validité des formules suivantes :
   (a) $\forall x(\neg A(x) \rightarrow (A(x) \rightarrow (A(x) \rightarrow \neg A(x))))$

(b) $\forall x \exists y P(x,y) \rightarrow \exists y P(y,y)$

(c) $P(x,x) \rightarrow \exists y P(y,y)$

(d) $\forall y P(x,y) \rightarrow P(y,y)$

(4) A l'aide de l'interprétation suivante : $D = \{a, b\}$ et

P(a,a)	P(a,b)	P(b,a)	P(b,b)
T	F	F	T

Déterminer les valeurs de vérité des formules suivantes :

(a) $\exists y \neg P(x,x)$

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

(c) $\forall x \exists y P(x,y)$

(d) $\exists y \forall y (P(x,y) \rightarrow P(y,x))$

6. Calcul des prédicats formalisé

Les symboles du calcul des prédicats peuvent être interprétés de différentes manières. Mais dans ce qui suit , nous nous intéresserons seulement aux aspects formels du langage contrairement à ce qui a été fait précédement concernant les propriétés dépendant d'interprétations particulières. Dans le système formel que nous allons définir, nous montrerons des propriétés importantes telles que la consistance et le théorème de complétude.

Définition 6.1. *Soient A,B,et C des formules d'un langage du premier ordre. Les axiomes du calcul des prédicats formel sont :*

(ax1) $A \rightarrow (B \rightarrow A)$

(ax2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

(ax3) $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$

(ax4) $\forall x A \rightarrow A$ *si x n'est pas libre dans A.*

(ax5) $\forall x A(x) \rightarrow A(t)$ *si le terme t est libre pour x dans A(x).*

(ax6) $\forall x(A \rightarrow B) \rightarrow (A \rightarrow \forall x B)$ *si x n'est pas libre dans A.*

Les rg̀les de déductions sont :

(Modus Ponens) $A,\ A \rightarrow B \vdash B$

(Généralisation) $A \vdash \forall x A$ *où x est une variable quelconque.*

Remarquons que les axiomes du calcul des prédicats ci-dessus sont des axiomes schemas. Chacun d'eux remplace une infinité de formules appelées instances.

Exemple 6.1. *Les formules* $(p \rightarrow r) \rightarrow ((p \rightarrow p) \rightarrow (p \rightarrow r))$ *et* $(a \rightarrow ((b \rightarrow c) \rightarrow a))$ *sont des instances de l'axiome (ax1).*

Remarquons aussi que l'ensemble des axiomes du calcul des prédicats inclut l'ensemble des axiomes du calcul propositionnel. Les nouveaux axiomes introduits concernent les propriétés immédiates du quantificateur $\forall$ que l'on utilise pour dériver (démontrer) certaines formules à partir d'autres. La définition de la notion de démonstration dans le calcul des prédicats `CP` étend celle donnée dans le chapitre qui concerne le calcul propositionnel.

DÉFINITION 6.2. *Une démonstration dans le calcul des prédicats formel est une suite de formules A_1, A_2, ..., A_n telle que :*

(1) *A_i est un axiome ou*
(2) *A_i se déduit à partir des éléments précédents de la suite par l'application de le règle Modus Ponens où de la règle de généralisation .*

Si Γ est un ensemble de formules, une déduction à partir de Γ est une suite de formules P_1, P_2, ... P_n telle que :

(1) *P_i est un axiome ou un élément de Γ ou*
(2) *P_i se déduit à partir des éléments précédents de la suite par l'application de la règle Modus Ponens ou de la règle de généralisation.*

Une formule du calcul des prédicats est dite théorème si elle est la dernière formule d'une certaine suite de formules qui forme une démonstration.

Notation. "$\vdash$ A" exprime que A est un théorème. "$\Gamma \vdash$ A" exprime que A se déduit à partir de Γ (Ici A n'est pas un théorème, la formule A se déduit de l'ensemble des formules de Γ).

DÉFINITION 6.3. *Une formule A du calcul des prédicats est une tautologie s'il existe une formule A_0 du calcul propositionnel telle que A est obtenue à partir de A_0 par substitution de certaines variables propositionnelles par des formules du* `CP` *et A_0 est une tautologie.*

EXEMPLE 6.2. *Soit la formule $\forall x A(x) \to (\exists y B(y) \to \forall x A(x))$. On voit bien que cette peut être obtenue en substituant dans la tautologie $a \to (b \to a)$ a par $\forall x A(x)$ et b par $\exists y B(y)$. La formule est donc une tautologie.*

PROPOSITION 6.1. *Si A est une tautologie alors, A est un théorème du calcul des prédicats.*

DÉMONSTRATION. A est une tautologie du calcul des prédicats alors, il existe une formule A_0 tautologie du calcul propositionnel telle que A est obtenue par substitution des variables propositionnelles de A_0 par des formules. La démonstration de A_0 dans le calcul propositionnel formel peut être transformée en une démonstration de A dans le calcul des prédicats formel. On observera que les axiomes schemas (ax1), (ax2) et (ax3) sont communs aux deux systèmes qui posèdent la même règle de déduction MP (Modus Ponens). □

PROPOSITION 6.2. *Toutes les instances des axiomes schemas (ax4), (ax5) et (ax6) sont logiquement valides.*

DÉMONSTRATION. .

Pour l'axiome (ax4), considérons une validation v d'une interprétation `I` du `CP`. Supposons que v satisfait $\forall$xA, alors par définition toute validation v' x-équivalenteà v satisfait A. C'est à dire toute validation v' telle que v(y) = v'(y) pour tout y différent de x satisfait A. Pour toute valeur de x, v satisfait A. Donc, chaque validation v satisfait ($\forall$xA $\rightarrow$ A) qui est donc logiquement valide. Pour l'axiome (ax5) considérons un terme t tel que x $\notin$ t et une validation v. Il suffit de démontrer que si v satisfait $\forall$xA(x) alors, v satisfait A(t).

□

PROPOSITION 6.3. *Pour toute formule A du calcul des prédicats ; si $\vdash$ A alors, A est logiquement valide.*

DÉMONSTRATION. La démonstration se fait par induction sur le nombre n de pas dans la démonstration de A.
Base d'induction. Si n = 1 alors A est un axiome du `CP`. et donc, A est logiquement valide par la proposition précédante.
Hypothèse d'induction. Supposons que A a une démonstration de n étapes (n>1) et que tous les théorèmes ayant une démonstration de n-1 étapes sont logiquement valides. La formule A apparaît dans la démonstration, soit comme axiome, ou soit comme conséquence des précédantes formules dans la démonstration de l'application de la règle MP et/ou de la règle de généralisation. Si A se déduità partir de B et (B $\rightarrow$ A) et que chacune de ces deux formules est logiquement valide par hypothèse d'induction. Il découle immédiatement que A est aussi logiquement valide. Si A se déduit par application de la règle de généralisation à partir d'une formule C qui est logiquement valide par hypothèse d'induction. A identique à $\forall$xC est aussi logiquement valide. □

COROLLAIRE 6.1. *Le Calcul des prédicats du premier ordre est consistant.*

DÉMONSTRATION. Supposons que l'on a : $\vdash$ A et $\vdash \neg$ A. Alors A et $\neg$A sont logiquement valides, ceci découle de la proposition précédante. A et $\neg$A ne peuvent être valides ensemble par la définition même de la négation. Notre hypothèse est contradictoire et nous n'aurons jamais $\vdash\neg$A et $\vdash$A. $\square$

Maintenant, nous souhaitons montrer dans le calcul des prédicats, l'analogue du théorème de déduction que nous avons rencontré dans le chapitre consacré au calcul propositionnel. Mais, nous remarquerons déjà que le théorème de déduction dans `CP` ne peut être montré sans certaines restrictions. Par exemple nous avons :

$$\begin{array}{lll} A & \vdash & \forall xA. \text{ (règle de généralisation)} \\ & \vdash & A \to \forall xA \text{ (en appliquant l'analogue du théorème de déduction.)} \end{array}$$

Cette démonstration donne la formule A $\to \forall$xA comme un nouveau théorème. Mais remarquons que si x $\in$ FV(A) alors, la formule A $\to \forall$xA n'est pas valide.

THÉORÈME 6.1. **(Théorème de déduction)**. *Soient A, B deux formules et* Γ *un ensemble de formules du calcul des prédicats. Si* $\Gamma \cup \{A\} \vdash B$ *et la démonstration ne contient aucune application de la règle de généralisation sur une variable libre de A alors,* $\Gamma \vdash A \to B$.

DÉMONSTRATION. La démonstration se fait par induction sur le nombre n des formules dans la déduction de B à partir de $\Gamma \cup \{A\}$.

Base d'induction. n = 1, B est un axiome ou B $\equiv$ A ou B $\in \Gamma$.
Nous déduisons $\Gamma \vdash$ (A $\to$ B) exactement de la même manière que pour la démonstration correspondante dans le calcul propositionnel.
Hypothèse d'induction. $n > 1$. Supposons que si F est formule déduite de $\Gamma \cup \{A\}$ sans utiliser la règle de générarlisation sur une variable libre dans A dans la déduction contenant moins de n formules alors $\Gamma \vdash$ A $\to$ B.
Cas 1. B se déduit à partir des formules précédantes par la règle MP. La démonstration est la même que celle donnée dans le cas du calcul propositionnel.
Cas 2. B est un axiome ou B $\equiv$ A ou B $\in \Gamma$. La démonstration est la même que celle donnée dans le cas du calcul propositionnel. **Cas 3.** B se déduit à partir d'une formule précédante par généralisation. Donc B est $\forall$xC où C apparaît dans la déduction $\Gamma \cup \{A\} \vdash$ (A $\to$ C). Par hypoyhèse d'induction $\Gamma \vdash$ A $\to$ C puisque il n'y a aucune application de la règle de généralisation sur une variable libre de A. Aussi x ne paut être libre dans A car, l'application de la règle de généralisation dans la déduction de B à partir de $\Gamma \cup \{A\}$ se fait sur la variable x. La déduction de (A $\to$ B) à partir est comme suit :

$$\left.\begin{array}{ll} 1 & \\ \vdots & \\ (k) & (A \to C) \end{array}\right\}. \text{ déduction de } (\mathrm{A} \to \mathrm{C}) \text{ à partir de } \Gamma$$

(k+1) $\quad \forall$x(A $\to$ C) $\quad$ (k) + règle de généralisation.
(k+2) $\quad \forall$x(A $\to$ C)$\to$ (A$\to \forall$xC $\quad$ (ax6).
(k+3) $\quad$ A $\to \forall$xC. $\quad$ (k+1),(k+2) + MP.

Nous avons donc $\Gamma \vdash (\mathrm{A} \to \mathrm{B})$.

□

Corollaire 6.2. *Si $\Gamma \cup \{A\} \vdash B$ et si A est fermée alors, $\Gamma \vdash (A \to B)$*

La preuve de ce corollaire est à faire comme exercice.

Corollaire 6.3. *Soient A, B deux formules, Γ un ensemble de formules du calcul des prédicats. Si $\Gamma \vdash (A \to B)$ alors $\Gamma \cup \{A\} \vdash B$.*

Démonstration. Il suffit d'adapter celle décrite dans le cas du calcul propositionnel. □

Exemple 6.3. *Cet exemple donne la démonstration des deux théorèmes $(A \to \forall xB) \to \forall x(A \to B)$si $x \notin FV(A)$ et $\forall x(A \to B) \to (\exists xA \to \exists xB)$.*

(1) *Si $x \notin FV(A)$ alors $\vdash (A \to \forall xB) \to \forall x(A \to B)$.*

1-$\vdash (A \to \forall x\ B)$	*hypothèse*
2-$\vdash \forall xB \to B$	*(axiome 4)*
3-$\vdash (A \to B)$	*1+2 +SH*
4-$\vdash \forall x\ (A \to B)$	*3+généralisation*
5-$\vdash (A \to \forall xB) \to \forall x(A \to B)$	*1,3+Théorème de déduction.*

(2) $\vdash \forall x(A \to B) \to (\exists xA \to \exists xB)$.

a) $\vdash \forall x\ (A \to B)$	*hypothèse*
b) $\vdash \forall x\ \neg B$	*hypothèse*
c) $\vdash \forall x\ (A \to B) \to (A \to B)$	*(axiome 4)*
d) $\vdash (A \to B)$	*a+c+MP*
e) $\vdash (A \to B) \to (\neg B \to \neg A)$	*tautologie.*
f) $\vdash (\neg B \to \neg A\ )$	*d+e+MP*
g) $\vdash (\forall x\ \neg B)\to (\neg B)$	*(axiome 4)*
h) $\vdash \neg B$	*b,g + MP*
i) $\vdash \neg A$	*f,h + MP*
j) $\vdash \forall x \neg A$	*a + i +généralisation*

Ceci démontre $\{\forall x(A \to B), \forall x\neg B\} \vdash (\forall x\, \neg A)$. *Par application du théorème de déduction nous obtenons :*
11-$\forall x(A\to B) \vdash (\forall x\, \neg B) \to (\forall x\, \neg A)$ *car* $x \notin FV(\forall x\neg B)$.
12-$\vdash ((\forall x\neg B)\to \forall x\neg A) \to (\neg(\forall x\neg A)\to \neg(\forall x\neg A))$ *tautologie.*
13- $\forall x(A \to B) \vdash (\neg(\forall x\neg A)\to \neg(\forall x\neg A))$ *11+12+MP.*

Et finalement : $\vdash \forall x(A \to B) \to (\exists xA \to \exists xB)$.

Il est utile, dans la pratique, d'introduire le connecteur d'équivalence $\leftrightarrow$. Il sera défini par : A $\leftrightarrow$ B est identique à $\neg((A \to B) \to \neg(B \to A))$.

Proposition 6.4. *Soient A et B deux formules bien formées du calcul des prédicats,* $\vdash A \leftrightarrow B$ *est équivalent à* $\vdash (A \to B)$ *et* $\vdash (B \to A)$.

Démonstration.

1) $\vdash \neg((A \to B) \to \neg(B \to A))$	Par hypothèse
2) $\vdash \neg((A \to B) \to \neg(B \to A)) \to (A \to B)$	Tautologie
3) $\vdash \neg((A \to B) \to \neg(B \to A)) \to (B \to A)$	Tautologie
4) $\vdash (A \to B)$	1+2 + MP
5) $\vdash (B \to A)$	1+3 + MP

Pour montrer la reciproque ($\Leftarrow$) il suffit de vérifier que :

$(A \to B) \to ((B \to A) \to \neg\, ((A \to B) \to \neg(B \to A)))$
est une tautologie. □

Définition 6.4. *Si A, B sont des formules du calcul des prédicats et* $\vdash A \leftrightarrow B$ *alors, A et B sont dit équivalents.*

Proposition 6.5. *Si A, B et C sont des formules du calcul des prédicats et si A et B sont équivalents et B et C sont équivalents alors, A et C sont équivalents.*

Cette dernière proposition sera trés utile dans le cas où nous aurons besoin de montrer que deux formules sont équivalentes. Nous aurons à étudier aussi quelles parties d'une formule peuvent être substituées et de quelles manières interchanger les noms de variables.

Proposition 6.6. *Si* x_i *est libre dans* $A(x_i)$ *et* x_j *est une variable qui n'a aucune occurence libre ou liée dans* $A(x_i)$ *alors* $\vdash \forall x_i\ A(x_i) \leftrightarrow \forall x_j\ A(x_j)$

DÉMONSTRATION. x_i est libre pour x_j dans $A(x_j)$ et x_j est libre pour x_i dans $A(x_i)$.

1) $\vdash \forall x_i\ A(x_i)$	Hypothèse
2) $\vdash \forall x_i\ A(x_i) \rightarrow A(x_j)$	Axiome 5
3) $\vdash A(x_j)$	1 + 2 + MP
4) $\vdash \forall x_j\ A(x_j)$	3 + règle de généralisation
5) $\vdash \forall x_i\ A(x_i) \rightarrow \forall x_j\ A(x_j)$	puisque x_j n'est pas libre dans $\forall x_i\ A(x_i)$

Et de la même manière nous obtenons :

$\vdash \forall x_j\ A(x_j) \rightarrow \forall x_i\ A(x_i)$

et donc : $\vdash \forall x_i\ A(x_i) \leftrightarrow \forall x_i\ A(x_i)$

□

Cette proposition montre que l'on peut changer le nom des variables liées dans une formule et obtenir une autre formule équivalente à la première formule. L'utilité de cette proposition, nous la verrons dans la suite.

PROPOSITION 6.7. *Soient A une formule et y_1, ..., y_n les seules variables libres de A. Alors $\vdash A$ si et seulement si $\vdash \forall y_1,...\forall y_n A$.*

DÉMONSTRATION. ($\Rightarrow$) La démonstration est par induction sur le nombre des variables libres dans A.
Base de l'induction : $n = 1$. Nous avons $\vdash$A alors par application de la règle de généralisation nous obtenons $\vdash \forall y_1 A(y_1)$.

Hypothèse d'induction : $n > 1$. Supposons la proposition est vraie pour toute formule avec $n-1$ variables libres. Considérons la formule $(\forall y_n)A$ qui a $n-1$ variables libres. Nous avons :
$\vdash$ A par la règle de généralisation et
$\vdash \forall y_1 \ldots \forall y_{n-1} \forall y_n A$ par hypothèse d'induction.

Réciproquement supposons que $\vdash \forall y_1 \ldots \forall y_{n-1} \forall y_n A$ et montrons que $\vdash$ A. La démonstration est immédiate par induction sur le nombre n des variables y_i ($1 \leq i \leq n$) et par application de l'axiome 5.

□

DÉFINITION 6.5. *Si A est une formule contenant les seules variables libres y_1, ..., y_n alors, la formule $\forall y_1 \ldots \forall y_{n-1} \forall y_n A$ est appelée la fermeture universelle de A.*

7. Forme normale prénexe d'une formule

Nous allons décrire maintenant comment transformer les formules sous des formes spéciales appelées forme normale prénexe conjonctive et forme normale prénexe disjonctive. L'utilité de ces formes normales réside dans le fait qu'elles permettent de mettre en évidence certaines relations logiques qui ne sont pas évidentes à voir sous les formes habituelles des formules.

DÉFINITION 7.1. *Une formule est dite sous forme normale prénexe conjonctive si elle est de la forme :*
$(Qv_1)(Qv_2)\ \ldots\ (Qv_n)\{[A_{11} \vee A_{12} \ldots \vee A_{1n}] \wedge \ldots \wedge [A_{m1} \vee A_{m2} \vee \ldots \vee A_{mq}]\}$

où Q est soit le quantificateur $\exists$ ou soit le quantificateur $\forall$, les v_i sont des variables distinctes qui ont une occurence libre dans les A_{ij}. Chaque A_{ij} est une formule atomique ou une négation d'une formule atomique.

EXEMPLE 7.1. *La formule :* $\forall x \exists y\, \{[\neg p(x) \vee p(x)] \wedge [g(y) \vee p(a)]\}$ *est sous forme normale prénexe conjonctive.*

THÉORÈME 7.1. *Toute formule du calcul des prédicats peut être transformée en une formule équivalente sous forme normale prénexe conjonctive.*

DÉMONSTRATION. Soit F une formule quelconque. Nous allons construire une formule F' sous forme normale prénexe conjonctive en remplaçant successivement des parties de F par des formules équivalentes. La construction de F' se fait en plusieurs étapes.

(1) Eliminer dans F tous les quantificateurs redondants ; c.a.d éliminer les quantificateurs ∀v ou ∃v si aucune occurence libre de v n'apparait dans leur champ.
(2) Changer le nom des variables liées. Prendre la partie la plus à gauche de la formule F sous la forme ∀vB(v) ou ∃vB(v) telle que v a une occurence dans une autre partie de formule F (libre ou liée). Remplacer ∃vB(v) ou ∀vB(v) par $\exists \mathrm{v}_1\mathrm{B(v)}$ ou $\forall \mathrm{v}_1\mathrm{B(v)}$. La variable v_1 est une nouvelle variable.
(3) Eliminer les connecteurs autre que ∨, ∧ et ¬. Remplacer A → B par ¬A ∨ B et A ↔ B par (¬A ∨ B) ∧ (¬ B ∨ A).
(4) Déplacer les connecteurs à l'exterieur de la formule. Remplacer :

∃vA(v) ∨ B	par	∃v $[A(v) \vee B]$
B ∨ ∃vA(v)	par	∃v $[B \vee A(v)]$
B ∨ ∀vA(v)	par	∀v $[B \vee A(v)]$
∃vA(v) ∧ B	par	∃v $[A(v) \wedge B]$
B ∧ ∃vA(v)	par	∃v $[B \wedge A(v)]$
∃vA(v) ∨ B(v)	par	∃v $[A(v) \vee B(v)]$
∀vA(v) ∧ ∀vB(v)	par	∀v $[A(v) \vee B(v)]$

(5) Appliquer la distributivité de ∧ par rapportà ∨ ; remplacer

(A ∧ B) ∨ C	par	(A ∨ C) ∧ (B ∨ C)
A ∨ (B ∧ C)	par	(A ∨ B) ∧ (B ∨ C)

La formule ainsi obtenue est la formule F' recherchée. □

Exemple 7.2. *Soit la formule F :*
$\forall x\,[(\forall y p(x) \vee \forall z q(z,y)) \rightarrow \neg \forall y r(x,y)]$. *Sa forme normale prénexe conjonctive est obtenue en appliquant la procédure précédante :*

(1) *Eliminer le quantificateur redondant* $\forall y$ *:*

$$(\forall x)\,[(p(x) \vee (\forall z) q(z,y)) \rightarrow \neg(\forall y) r(x,y)]$$

(2) *Renommer la variable y :*

$$\forall x\,[(p(x) \vee (\forall z) q(z,y)) \rightarrow \neg \forall y_1 r(x,y_1)]$$

(3) *Eliminer le quantificateur* $\rightarrow$ *:*

$$\forall x\,[\neg(p(x) \wedge \exists z \neg q(z,y)) \vee \exists y_1 \neg r(x,y_1)]$$

(4) *Déplacer à gauche le quantificateur* $\exists$ *:*

$$\forall x \exists z \exists y_1\,[\neg(p(x) \wedge \neg q(z,y)) \vee \neg r(x,y_1)]$$

(5) *Distribuer* $\wedge$ *par rapportà* $\vee$ *:*

$\forall x \exists z \exists y_1\,[\neg(p(x) \vee \neg r(x,y_1)) \wedge (\neg q(z,y) \vee \neg r(x,y_1)]$ *: C'est la formule recherchée.*

8. Exercices

(1) Démontrer les théorèmes suivants :

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

(b) $\forall x(P(x) \to Q(x)) \to (\forall x P(x) \to \forall x Q(x))$

(c) $\forall x(P(x) \to Q(x)) \to (\exists x P(x) \to \exists x Q(x))$

(d) $\exists x(P(x) \to Q(x)) \to (\forall x P(x) \to \exists x Q(x))$

(2) Trouver les formes prenexes des formules suivantes :

(a) $\forall x(P(x) \to Q(x,y)) \to (\exists y P(y) \to \exists z Q(y;z))$

(b) $\forall x(P(x) \to \forall y(Q(x,y) \to \neg\forall z R(y,z)))$

(c) $\forall x(P(x) \to Q(x)) \to (\forall x P(x) \to \forall x Q(x))$

9. Solémisation, Résolution

Cette section se veut une introduction trés brève à la méthode de résolution de Robinson, appliquée au calcul des prédicats, dont l'impact en informatique a été trés important. La méthode de Résolution, généralisation de la méthode de Davis Putnam, a été l'une des premières à être utilisée pour la démonstration automatique de théorèmes. C'est aussi, rappelons le, l'origine du développement du langage de programmation Prolog, trés utilisé pour l'écriture de programme en intelligence artificielle.

On peut considérer que la méthode de résolution est basée sur le principe de démonstration par réfutation. Les travaux de Skolem et de Herbrand, aux environs de 1930, ont ouvert la voie. J.A. Robinson a défini en 1965 une méthode appelée résolution, trés performente, permettant de montrer qu'un ensemble de formules est contradictoire. Nous en donnerons dans ce qui suit les étapes essentielles.

9.1. Forme clausales, Skolémisation. Dans le calcul des prédicats, un littéral est défini comme étant une formule atomique ou une négation d'une formule atomique. Une clause est une disjonction de plusieurs littéraux. Une formule du calcul des prédicats est dite sous forme clausale si elle est sous la forme :

$$\forall \mathrm{x}_1 \ldots \forall \mathrm{x}_n(\mathrm{C}_1 \wedge \mathrm{C}_2 \wedge \ldots \wedge \mathrm{C}_k)$$

Où C_i $(0 < i < k+1)$ est une clause et les x_i ($\mathrm{i} \leq \mathrm{n}$) sont des variables telles que $\mathrm{x}_i \neq \mathrm{x}_j$ si $i \neq j$.

Par exemple, P(f(x), a) et ¬q(y) sont deux littéraux. La formule :

$$\mathrm{P(f(x),a)} \vee \neg \mathrm{q(y)} \vee \neg \mathrm{p(a,y)}.$$

est une clause.

On appelle forme de Skolem d'une formule D, la formule D_s , sous forme clausale, obtenue en éliminant tous les quantificateurs existentiels, telle que D satisfaisable équivaut D_s satisfaisable.

THÉORÈME 9.1. *(Skolémisation). Chaque formule D peut être transformée en une formule D_s sous forme clausale telle que D est satisfaisable si et seulement si D_s est satisfaisable.*

DÉMONSTRATION. La transformation de D se fait par la construction de la suite D_1, D_2, ... D_n , telle que $D = D_1, D_n = D_s$ et D_i satisfaisable $\Leftrightarrow$ D_{i+1} satisfaisable. La procédure de construction est comme suit :

(1) Prendre la fermeture existentielle de D (c.à.d quantifier les variables libres de D par le quantificateur $\exists$).
(2) Eliminer dans D tous les quantificateurs redondants.
(3) Renommer chaque variable quantifiée dans D plus d'une fois.
(4) Eliminer les occurences des connecteurs autres que $\neg$, $\vee$ et $\wedge$.
(5) Pousser à droite tous les connecteurs en remplaçant :
   (a) $\neg(\forall \mathrm{x} \mathrm{A})$ par $\exists \mathrm{x}(\neg \mathrm{A})$
   (b) $\neg(\exists x A)$ par $\forall x(\neg A)$
   (c) $\neg(A \vee B)$ par $\neg A \wedge \neg B$
   (d) $\neg(A \wedge B)$ par $\neg A \vee \neg B$
   (e) $\neg(\neg A)$ par A.

   jusqu'à ce que toutes les occurences de $\neg$ précède immédiatemment une formule atomique.
(6) Pousser les quantificateurs à droite en remplçant :
   (a)
$$\exists x(A \vee B) par \begin{cases} A \vee \exists x B & \text{si x n'est pas libre dans A} \\ \exists x A \vee B & \text{si x n'est pas libre dans B} \end{cases}$$
   (b)
$$\exists x(A \wedge B) par \begin{cases} A \wedge \exists x B & \text{si x n'est pas libre dans A} \\ \exists x A \wedge B & \text{si x n'est pas libre dans B} \end{cases}$$
   (c)
$$\forall x(A \vee B) par \begin{cases} A \vee \forall x B & \text{si x n'est pas libre dans A} \\ \forall x A \vee B & \text{si x n'est pas libre dans B} \end{cases}$$
   (d)
$$\forall x(A \wedge B) par \begin{cases} A \wedge \forall x B & \text{si x n'est pas libre dans A} \\ \forall x A \wedge B & \text{si x n'est pas libre dans B} \end{cases}$$

(7) Eliminer les quantificateurs existentiels. Prendre la formule la plus à gauche de la forme $\exists$yB(y) et la remplaçer par B(f(x_1,…,x_n)) où
   (a) x_1,…,x_n sont des variables distinctes de $\exists$yB(y) quantifiées universellement à gauche de $\exists$yB(y).
   (b) f est fonction à n arguments qui n'occure pas dans la formule. Répéter ce processus jusqu'à l'élimination complète des tous les quantificateurs existensionnels. Dans le cas perticulier $n = 0$, remplacer $\exists$yB(y) par B(a) où a est une nouvelle constante qui n'occure pas dans la formule.
(8) Déplacer les quantificateurs $\forall$ à gauche.
(9) Distribuer $\wedge$ et $\vee$.
(10) Simplifier en utilisant les règles préservant la satisfaction.

$\square$

Nous proposons au lecteur de vérifier que toutes ces transformations conservent la satisfaction de la formule D.

Exemple 9.1. *Considérons la formule D suivante :*

$$\forall x(p(x) \rightarrow \exists z(\neg\forall y(q(x,y) \rightarrow p(f(t))) \wedge \forall y(q(x,y) \rightarrow p(x))))$$

(1) *Prendre la fermeture existentielle de D et éliminer le quntificateur redondant $\exists z$.*

$$\exists t\forall x(p(x) \rightarrow (\neg\forall y(q(x,y) \rightarrow p(f(t))) \wedge \forall y(q(x,y) \rightarrow p(x))))$$

(2) *Renommer la variable y, elle est quantifiée deux fois.*

$$\exists t\forall x(p(x) \rightarrow (\neg\forall y(q(x,y) \rightarrow p(f(t))) \wedge \forall z(q(x,z) \rightarrow p(x))))$$

(3) *Eliminer toutes les occurences de $\rightarrow$*

$$\exists t\forall x(\neg p(x) \vee (\neg\forall y(\neg q(x,y) \vee p(f(t))) \wedge \forall z(\neg q(x,z) \vee p(x))))$$

(4) *Déplacer $\neg$*

$$\exists t\forall x(\neg p(x) \vee (\exists y(q(x,y) \wedge \neg p(f(t))) \wedge \forall z(\neg q(x,z) \vee p(x))))$$

(5) *Pousser les quantificateurs $\exists y$ et $\forall z$ à droite*

$$\exists t\forall x(\neg p(x) \vee ((\exists y q(x,y) \wedge \neg p(f(t))) \wedge (\ \forall z(\neg q(x,z)) \vee p(x))))$$

(6) *Eliminer les quantificateurs $\exists t$ et $\exists y$.*

$$\forall x(\neg p(x) \vee ((q(x,g(x)) \wedge \neg p(f(a))) \wedge (\ \forall z(\neg q(x,z)) \vee p(x))))$$

(7) *Déplacer le quatificateur $\forall$ à gauche*

$$\forall x\forall z(\neg p(x) \vee ((q(x,g(x)) \wedge \neg p(f(a))) \wedge ((\neg q(x,z)) \vee p(x))))$$

(8) *Aprés distribution de $\vee$ et $\wedge$ et simplification :*

$$\forall x\ \{(\neg p(x) \vee q(x,g(x))) \wedge \neg p(f(a))\}.$$

9.2. Procédure de Herbrand. La procédure de Herbrand joue un rôle important dans la démonstration automatique de théorèmes. Elle permet, en effet, de ramener le problème de l'existence d'un modèle pour un ensemble fini de clauses à un problème de la satisfaisabilité d'un ensemble de propositions.

Par définition un ensemble de clauses S est insatisfaisable si et seulemnet si il est contradictoire pour toutes les interprétations. Comme il est difficile de considérer toutes les interprétations (infinies), il serait plus pratique de se fixer sur une seule interprétation I_H telle que S est insatisfaisable dans I_H équivaut que S est contradictoire.

DÉFINITION 9.1. *Soit S un ensemble de clauses. Soit H_0 l'ensemble des constantes de S. Si aucune constante n'occure dans S alors $H_0 = \{a\}$, où a est une constante arbitraire. $H_{i+1} = H_i \cup \{f(t_1, \ldots, t_j),$ tel que $t_1, \ldots, t_j \in H_i\}$. H_∞ est appelé univers de Herbrand.*

EXEMPLE 9.2. *Soit S = {P(a), ¬P(x) ∨ P(f(x)) }. Nous avons $H_0 = \{a\}$, $H_1 = \{a, f(a)\}$ et $H_\infty = \{a, f(a), f(f(a)), f(f(f(a))), \ldots\}$.*

DÉFINITION 9.2. *Soit S un ensemble de clauses. Une clause instance C d'une clause A de l'ensemble S est une clause obtenue en remplaçant les variables dans A par les éléments de l'univers de Herbrand. On appelle déploiement de Herbrand de A l'ensemble de toutes les clauses issues de chaque A ∈ S. Cet ensemble est noté H(S).*

Le théorème de Herbrand s'énnonce comme suit :

THÉORÈME 9.2. *L'ensemble fini de clauses S admet un modèle équivaut à H(S) est satisfaisable.*

COROLLAIRE 9.1. *L'ensemble fini de clauses S est contradictoire si et seulement si l'ensemble H(S) est contradictoire.*

Le théorème de Herbrand et son corollaire suggèrent une procédure pour démontrer l'insatifaisabilité des formules sous formes clausales. Pour une formule F sous forme clausale, nous engendrons successivement les instances de clauses G_i des clauses de F et tester si leur conjonction est contradictoire. Cette procédure permet de détecter si F est insatisfaisable aprés un nombre fini d'étapes. Dans le cas contraire si F est satisfaisable la procédure peut ne pas se terminer. C'est une procédure de déçision partielle.

Donnons un exemple. Soit la formule :

$$\exists \mathrm{y} \forall \mathrm{z}(\mathrm{p}(\mathrm{x},\mathrm{y}) \Leftrightarrow \neg \exists \mathrm{x}(\mathrm{p}(\mathrm{z},\mathrm{x}) \wedge \mathrm{p}(\mathrm{x},\mathrm{z}))).$$

La forme prénnexe conjonctive de cette formule est :

$\exists y \forall z \exists u \forall x$ {($\neg$p(z,y) $\vee$ $\neg$p(z,x) $\vee$ $\neg$p(x,z)) $\wedge$ (p(z,y) $\vee$ p(z,u)) $\wedge$ (p(z,y) $\vee$ p(u,z)) }

Aprés Skolémisation (en prenant y = a, u = f(z)) on obtient les clauses :

c_1 $\neg$p(z,a) $\vee$ $\neg$p(z,x) $\vee$ $\neg$p(x,z)

c_2 p(z,a)$\vee$ p(z,f(z))

c_3 p(z,a) $\vee$ p(f(z),z)

L'ensemble S(F) contient :

i $\neg$p(a,a) On remplace dans (c_1) x,z par a et on simplifie.

ii p(a,a)$\vee$ p(f(a),a) Dans (c_2) on remplace z par a.

iii $\neg$p(f(a),a) $\vee$ $\neg$p(a,f(a)) Dans (c_1) on remplace z par f(a) et x par a.

En notant A = p(a,a), B = p(a,f(a)) et C = p(f(a),a), le sous ensemble ci-dessus n'est autre que : { $\neg$A, A $\vee$ B, A $\vee$ C, $\neg$B $\vee$ $\neg$C }. On peut vérifier aisement que cet ensemble est contradictoire. La formule F est donc valide.

9.3. Méthode de résolution, unification. La méthode de résolution consiste une seule règle d'inférence, appelée règle de résolution. La règle de résolution peut être énoncée comme suit :

Pour deux clause C et D quelconques contenant un litéral l et son opposé $\neg$l, respectivement, on construit une nouvelle clause G, appelée le résolvant de C et D, en éliminant toutes les occurences de l et $\neg$l, respectivement, G est alors l'union des clauses C' et D' ainsi obtenues. Eliminer les occurences des litéraux dupliqués dans G, et ajouter G à la liste des clauses. Le cas particulier est l'existence de deux clauses l et $\neg$l, alors leur résolvant est la clause vide $\emptyset$.

Le résultat principal de cette méthode est qu'une conjonction d'un ensemble fini S de clauses est insatisfaisable si et seulemnet si la clause vide $\emptyset$ peut être engendrée à partir de S en répètant l'application de la règle de résolution. Il est clair que ce processus se termine vu que nous partons d'un ensemble fini de clauses et que nous pouvons construire qu'un ensemble fini de clauses à partir de S. L'idée de cette méthode se résume à S = $F_1 \wedge F_2 \wedge \ldots F_n$ est insatisfaisable si et seulement si S' = $F_1 \wedge F_2 \wedge \ldots F_n \wedge F_{n+1}$ est insatisfaisable, où F_{n+1} est le résolvant de F_i et F_j.

Considérons l'exemple suivant qui montre que la conjonction des clauses c_1, c_2 et c_3 est contradictoire :

c_1 $\neg$p(z,a) $\vee$ $\neg$p(z,x) $\vee$ $\neg$p(x,z)

c_2 p(z,a)$\vee$ p(z,f(z))

c_3 p(z,a) $\vee$ p(f(z),z)

On obtient :

c_4 $\neg$p(a,a) z = a dans C_1

c_5 p(a,f(a)) résolution de c_2 et c_4.

c_6 p(f(a),a) résolution de c_3 et c_4.
c_7 $\neg$p(f(a),a) $\vee$ $\neg$p(a,f(a)) résolution de c_6 et c_1.
c_8 p(z,a)$\vee$ p(z,f(z)) résolution de c_6 et c_7.
c_9 $\emptyset$ résolution cd c_5 et c_8.

L'inconvénient de cette méthode, sur le plan pratique, est que l'ensemble des clauses engendrées, pour la pluspart des formules, est trés grand. Ce qui demenadera pour leur traitement un espace mémoire à l'ordinateur et un temps de calcul inacceptable. Pour surmonter ces difficultés Robinson introduit une nouvelle méthode de résolution générale en généralisant la règle de résolution décrite précédement.

Pour pouvoir décrire cette méthode générale de résolution il est nécessaire d'introduire quelques définitions.

Définition 9.3. *Une substitution est un ensemble fini (peut être vide) de couple de la forme :*

$$\alpha = \{ (v_1,\ t_1),(v_2,\ t_2),\ldots\ (v_n,\ t_n)\}$$

les variables v_i sont distinctes deux à deux et sont toutes différents des termes t_i. Pour tout littŕal L, L' = Lα est un littéral obtenu à partir de L en remplaçant simultanement les variables vi_i $1 \leq i \leq n$ par les termes t_i dans L. L' est appelé instance de L.

Définition 9.4. *L'ensemble de consensus d'une disjoncion de formules atomiques :*

$$p(t^1_1,\ldots,t^1_n) \vee p(t^2_1,\ldots,t^2_n) \vee \ldots \vee p(t^k_1,\ldots,t^k_n)$$

est l'ensemble des sous-termes $\{\tau^1,\tau^2,\ldots,\tau^k\}$ obtenu comme suit : On considère chacune des formules atomiques comme une suite de symboles et on répère la position du premier symbole qui n'occupe pas la même position dans toutes les formules atomiques. Alors, pour chaque i $(1 \leq i \leq k)$ on considŕe τ^i le sous-terme de $p(t^i_1,\ldots,t^i_n)$ qui commence par cette position du symbole.

Exemple 9.3. *L'ensemble de consensus de la formule :*

$$p(x,g(\underline{f(y,z)},x),y) \vee p(x,g(\underline{a},b),b) \vee p(x,g(\underline{g(h(x),a)},y),h'x))$$

est l'ensemble des sous-termes {f(y,z), a, g(h(x),a) }.

Une substitution α est dite un unificateur de la disjonction des formules atomiques $A_1 \vee A_2 \vee \ldots \vee A_n$ si $A_1\alpha = A_2\alpha = \ldots = A_n\alpha$. Dans le cas où il existe un unificateur pour une disjonction de formules on dit que cette disjonction est unifiable. Un unificateur β d'une disjonction $A_1 \vee A_2 \vee \ldots \vee A_n$ est un unificateur le plus général si pour chaque unificateur α pour cette disjonction $A_i\alpha$ est une instance de $A_i\beta$ (pour $1\leq$ i $\leq$ n). La formule atomique B telle que B = $A_i\alpha$ = ... = $A_n\alpha$ obtenu par un unificateur le plus général β , appelée facteur de $A_1 \vee A_2 \vee \ldots \vee A_n$, est unique.

EXEMPLE 9.4. *L'unificateur le plus général de la disjonction :*

$$p(a,x,f(g(y))) \vee p(z,h(z,w),f(w))$$

$\alpha = \{(z,a),\ (x,h(a,g(y))),\ (w,g(w))\ \}$.

La partie principale de la méthode de résolution est l'application de l'algorithme d'unification qui trouve l'unificateur le plus général α pour une certaine disjonction $A_1 \vee A_2 \vee \ldots \vee A_n$ unifiable. Il renvoit une erreur si cette disjonction n'est pas unifiable.

DÉFINITION 9.5. **Algorithme d'unification**

(1) *Début : L'algorithme commence avec un substitution $\alpha_0 = \{\}$ vide et construit pas à pas l'unificateur le plus général β.*
(2) *Etape k+1 ($k \geq 0$) : Supposons quà l'étape k la substitution produite est α_k. Si toutes les formules atomiques $A_i\alpha_k$ sont identiques, alors $\beta = \alpha_k$ est l'unificateur les plus général de la disjonction $A_1 \vee A_2 \vee \ldots \vee A_n$ et le processus se termine, sinon déterminer en premier l'ensemble D_k de consensus de $A_1\alpha_k \vee A_2\alpha_k \vee \ldots \vee A_n\alpha_k$. L'algorithme, ensuite, modifie la substitution α_k (pour obtenier α_{k+1}) de telle manière à rendre égaux deux éléments de l'ensemble de consensus. Ceci n'est possible que si l'ensemble de consensus contient comme élément une variable v_k et un certain terme t_k tel que $v_k \notin t_k$. Si de tels éléments n'existent pas dans D_k une erreur est renvoyée : la disjonction $A_1 \vee A_2 \vee \ldots \vee A_n$ n'est pas unifiable. La substitution α_{k+1} est calculée comme suit :*

$$\alpha_{k+1} = \{(v_1,[t_k/v_k]\ t_1),\ (v_2,[t_k/v_k]\ t_2),\ldots\ (v_n,[t_k/v_k]\ t_n)\} \cup \{(v_k,t_k)\}.$$

(3) *Incrémente k ; k = k+1 et aller à (2).*

Donnons maintenant la règle de r'esolution sous forme d'une procédure.

Entrée : Une paire de clauses C_1, C_2
Sortie : Un résolvant C_3 de C_1 et C_2 s'il existe

(1) Si, C_1 et C_2 contiennent respectivement les littéraux l_1 et l_2, $l_1 = p(x_1,\ldots,x_n)$ et $l_2 = \neg p(y_1,\ldots,y_n)$.
   (a) Si $x_i = y_i$ $(1 \leq i \leq n)$ alors le résolvant de C_1 et C_2 est calculé comme suit :

$$C_3 = (\ C_1 \text{ -} l_1) \vee (\ C_2 \text{ - } l_2)$$

(b) Sinon On applique l'algorithme d'unification
   (i) Si l'unificateur le plus général, soit β de l_1 et l_2 existe alors
      (A) Construire les facteurs $(C_1)\beta$ et $(C_2)\beta$.
      (B) Le résolvant C_3 est calculé comme suit

$$C_3 = ((C_1)\beta - (l_1)\beta) \vee ((C_2)\beta - (l_2)\beta)$$

   (ii) Sinon, le résolvant de C_1 et C_2 n'existe pas
(2) Sinon, Les deux clauses n'ont pas de résolvant.

Exemple 9.5. *Soit la disjonction :*

$$p(a,x,f(g(y))) \vee p(z,h(z,w),f(w))$$

pour trouver l'unificateur le plus général nous commençons par poser :

$$\alpha_0 = \{\ \}$$

L'ensemble de consensus de $p(a,x,f(g(y))) \vee p(z,h(z,w),f(w))$ est $\{a,z\}$. Nous avons donc

$$\alpha_1 = \{(z,a)\}$$

le facteur de la disjonction précédante obtenu l'unificateur le plus gńéral α_1 est :

$$p(a,x,f(g(y))) \vee p(a,h(a,w),f(w))$$

L'ensemble de consensus de $p(a,x,f(g(y))) \vee p(a,h(a,w),f(w))$ est $\{x,h(a,w)\}$. Nous avons :

$$\alpha_2 = \{(z,a),(x,h(a,w))\}$$

le facteur de la disjonction précédante obtenu l'unificateur le plus gńéral α_2 est :

$$p(a,h(a,w),f(g(y))) \vee p(a,h(a,w),f(w))$$

L'ensemble de consensus de $p(a,h(a,w),f(g(y))) \vee p(a,h(a,w),f(w))$ est $\{g(y),w\}$. Nous avons :

$$\alpha_3 = \{(z,a),(x,h(a,w)),\ (w,g(y)\}$$

α_3 est l'unificateur le plus général puisque $(\ p(a,h(a,w),f(g(y))))\alpha_3 = (\ p(a,h(a,w),f(w)))\alpha_3$.

La méthode générale de résolution, pour démontrer l'instisfaisabilité d'une formule F sous forme clausale, est basée sur l'application répetée de la règle de résolution. On commence par appliquer la règle de résolution à une paire de clauses C_1 et C_2 de F pour obtenir un résolvant C_3 de C_1 et C_2. Cette nouvelle clause C_3 est ajoutée à l'ensemble de clauses de F. La règle de résolution est encore appliquée jusqu'à ce que la clause vide est engendrée.

Exemple 9.6. *Montrons que la formule suivante est valide :*

$$F : \exists x \exists y \forall z \ \{(p(x,y) \rightarrow (p(y,z) \wedge p(z,z)))wedge\ ((p(x,y) \wedge q(x,y)) \rightarrow (q(x,z) \wedge q(z,z)))\}$$

Pour montrer que F est valide, nous allons montrer par la méthode de résolution que ¬F est insatisfaisable. En tranformant ¬F sous forme clausale on obtient les clauses suivantes :

(1) $p(x_1,\ y_1)$
(2) $\neg p(y_2,f(x_2,y_2)) \vee \neg p(f(x_2,y_2),f(x_2,y_2)) \vee q(x_2,y_2)$
(3) $\neg p(y_3,f(x_3,y_3)) \vee \neg p(f(x_3,y_3),f(x_3,y_3)) \vee q(x_3y,f(x_3,y_3)) \vee \neg q(f(x_3,y_3),f(x_3,y_3))$

En appliquant la règle de résolution, nous obtenons les clauses suivantes. A partir des clauses 1 et 2 et la substitution $\{(x_1,\ y_2),\ (y_1,f(x_2,y_2))\ \}$ *nous obtenons*

(4) $\neg p(f(x_2,y_2),f(x_2,y_2)) \vee q(x_2,y_2)$

A partir des clauses 1 et 4 avec la substitution $\{(x_1,\ f(x_2,y_2)),\ (y_1,f(x_2,y_2))\}$ *nous obtenons :*

(5) $q(x_2,y_2)$

A partir des clauses 3 et 5 avec la substitution $\{(x_2,\ f(x_3,y_3)),\ (y_2,f(x_3,y_3))\}$ *nous obtenons :*

(6) $\neg p(y_3,f(x_3,y_3)) \vee \neg p(f(x_3,y_3),f(x_3,y_3)) \vee q(x_3y,f(x_3,y_3))$

A partir des clauses 5 et 6 avec la substitution $\{(x_2,\ x_3),\ (y_2,f(x_3,y_3))\}$ *nous obtenons :*

(7) $\neg p(y_3,f(x_3,y_3)) \vee \neg p(f(x_3,y_3),f(x_3,y_3))$

A partir des clauses 1 et 7 avec la substitution $\{(x_1,\ f(x_3,y_3)),\ (y_1,f(x_3,y_3))\}$ *nous obtenons :*

(8) $\neg p(y_3,f(x_3,y_3))$

A partir des clauses 1 et 8 avec la substitution $\{(x_1,y_3),\ (y_1,f(x_3,y_3))\}$ *nous obtenons finalement :*

(9) $\emptyset$ *: Ceci implique que ¬F est insatisfaisable et donc F est valide.*

10. Exercices

(1) Soit F la formule suivante :

$$\mathrm{F} : \exists \mathrm{x}\ (\mathrm{p(x)} \rightarrow (\mathrm{q(x)} \vee \forall \mathrm{y}\ \mathrm{p(y)})) \wedge \forall \mathrm{x} \exists \mathrm{y} (\mathrm{q(y)} \rightarrow \mathrm{p(x)})$$

  (a) Donner la forme prenexe conjonctive de F.
  (b) Skolémiser F.

(2) On considère les deux formules suivantes :

$$F : \exists x\ h(x) \rightarrow \forall y h(y)$$
$$G : \forall x\ (h(x) \vee r(x))$$
$$C : \exists x \neg r(x) \rightarrow \forall y\ p(y)$$

(a) Trouver un ensemble de clauses `C` équivalent à $\{F, G, \neg C\}$.

(b) Trouver le domaine de Herbrand de `C`

(c) Montrer par la méthode de résolution que `C` est contradictoire.

(3) On veut montrer, en utilisant le langage du calcul des prédicats, que dans un groupe (structure algébrique), tout élément idempotent est nécessairement l'élément neutre.

(a) Poser complètement le problème (en forme de clauses)

(b) Appliquer la méthode résolution.

(4) Montrer par la méthode de résolution que pour tout prédicat p, ayant les propriétés de symétrie,de transitivité et tel que $\forall x \exists y\ p(x,y)$ alors, p a la propriété de reflexivité.

(5) Tahar, Malika et Mohamed font partie d'un "Club-musique". Chaque membre de ce club est soit un chanteur ou guitariste ou les deux à la fois. Aucun guitariste n'aime le style "rai" et tous les chanteurs aiment le style "chaabi". Malika n'aime pas tout ce que Tahar aime et elle aime tout ce que Mohamed n'aime pas. Tahar aime le style "rai" et le style "chaabi". Existe-t-il un adhérent de ce club qui soit guitariste et pas chanteur ? Utiliser les prédicats suivants : M(x) : x appartient au club ; G(x) : x est guitariste ; C(x) : x est chanteur ; A(x,y) : x aime y.