III. Système de preuve

1. Introduction

Pour *prouver* qu'une formule est satisfaite ou non, qu'une formule est valide ou non, qu'un ensemble est compatible ou non, …etc., on dispose seulement de la table de vérité

Bien qu'il soit possible d'énumérer toutes les valuations pour établir une table de vérité, la méthode est coûteuse en espace et en temps :

- n variables dans la formule => 2^n lignes
- Formules complexes => un grand nombre de colonnes

Une preuve plus courte est préférable. Le problème est de comment prouver une formule sans utiliser la table de vérité ?

Il existe plusieurs systèmes de preuve développés dans les mathématiques. Dans ce chapitre, nous allons voir, la méthode des tableaux sémantiques, et la méthode de la déduction naturelle.

2. Méthode des Tableaux sémantiques

En utilisant la méthode des tableaux sémantiques, nous allons voir comment faire :

a) La preuve de la satisfaisabilité d'une formule propositionnelle.
b) La preuve de la validité d'une formule.
c) La preuve de la consistance d'un ensemble de FP.
d) La preuve de la conséquence logique.

Dans la suite, nous notons par φ une formule propositionnelle quelconque.

a) Preuve de la satisfiabilité d'une formule

Pour prouver qu'une FP φ est satisfaite on cherche systématiquement un modèle. Donc :

- On suppose que φ est Vraie.
- Et on cherche un modèle v pour φ.

Pour cela on applique l'algorithme de la méthode des tableaux sémantiques (TS) :

Algorithme de la méthode des TS

L'algorithme construit à partir d'une formule φ un arbre noté T dont les nœuds sont des ensembles de formules.

1-Initialisation : Au départ, l'arbre ne contient qu'un seul nœud : l'ensemble {φ} ;

2-Tant qu'il existe une feuille F de l'arbre qui contient une formule ψ qui est simplifiable (non littéral) **faire :**

- Si ψ est simplifiable par une α-règle, alors on créer un fils F0 à F où F0 est obtenu supprimant ψ de F et en ajoutant la formule (dans le cas d'une double négation) ou les deux formules (pour les autres cas) obtenues par la simplification.
- Si ψ est simplifiable par une β-règle, alors on créer deux fils F1 et F2, chacun étant obtenu en supprimant ψ de F et en ajoutant respectivement les formules obtenues par la simplification.

3-Si toutes les feuilles contiennent une paire de littéraux complémentaires **alors** φ non-satisfaite, **sinon** φ satisfaite.

Remarque :

1. Quand on sélectionne une conjonction on a une seule branche, on appelle ce type de règles α-règles
2. Quand on sélectionne une disjonction on a deux branches, on appelle ce type de règles les β-règles

Voici les tableaux sémantiques correspondants aux α-règles et β-règles

Les α-règles

{FP}	$\{\neg\neg\varphi\}$	$\{\varphi 1 \wedge \varphi 2\}$	$\{\neg(\varphi 1 \vee \varphi 2)\}$	$\{\neg(\varphi 1 \rightarrow \varphi 2)\}$	$\{\varphi 1 \leftrightarrow \varphi 2\}$
$\{\alpha 1\}$ $\{\alpha 1, \alpha 2\}$	$\{\varphi\}$	$\{\varphi 1, \varphi 2\}$	$\{\neg\varphi 1, \neg\varphi 2\}$	$\{\varphi 1, \neg\varphi 2\}$	$\{\varphi 1 \rightarrow \varphi 2,$ $\varphi 2 \rightarrow \varphi 1\}$

Toutes les α-règles sont synonymes à des conjonctions

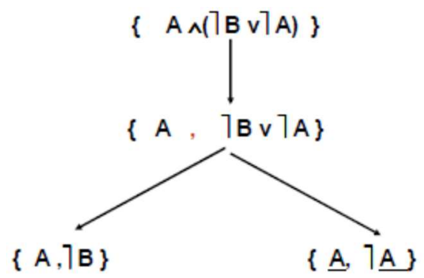
Les β-règles

{FP}	$\{\varphi 1 \vee \varphi 2\}$	$\{\neg(\varphi 1 \wedge \varphi 2)\}$	$\{\varphi 1 \rightarrow \varphi 2\}$	$\{\neg(\varphi 1 \leftrightarrow \varphi 2)\}$
$\{\beta 1\}$ $\{\beta 2\}$	$\{\varphi 1\}$ $\{\varphi 2\}$	$\{\neg\varphi 1\}$ $\{\neg\varphi 2\}$	$\{\neg\varphi 1\}$ $\{\varphi 2\}$	$\{\neg(\varphi 1 \rightarrow \varphi 2)\}$ $\{\neg(\varphi 2 \rightarrow \varphi 1)\}$

Toutes les β-règles sont synonymes à des disjonctions

Dans les exemples suivants, on utilise l'algorithme précédent pour prouver que les formules suivantes sont satisfaites ou non, et en déduire leurs modèles

Exemple1 : la formule φ : $A \wedge(\neg B \vee \neg A)$ est satisfaite ou non ?



V(A)=1, V(B)=0

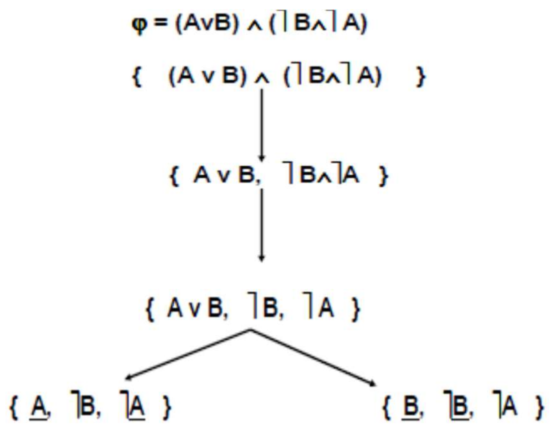
Donc $A \wedge(\neg B \vee \neg A)$ est satisfaite

Remarque :

Le problème de preuve de satisfaisabilité de φ a été réduit à un problème de satisfaisabilité d'un ensemble de littéraux.

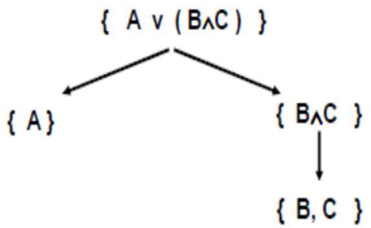
Un ensemble de littéraux est satisfaisable ssi il ne contient pas deux littéraux complémentaire ex : $\{A, \neg A\}$

Exemple 2 : la formule $\varphi = (A \vee B) \wedge (\neg B \wedge \neg A)$ est satisfaite ou non ?



Donc $\varphi = (A \vee B) \wedge (\neg B \wedge \neg A)$ non satisfaite

Exemple 3 : la formule $\varphi = A \vee (B \wedge C)$ est-elle satisfaite ?



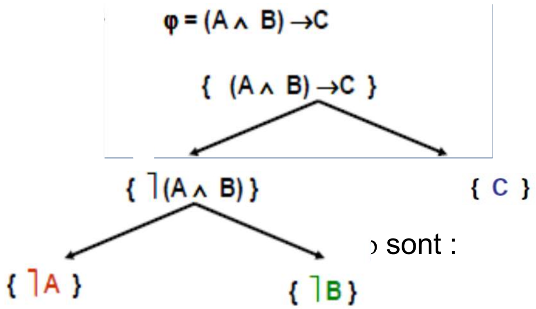
Les modèles de φ considérant l'ensemble de littéraux {A} sont :

1. V(A)=1 V(B)= 0 V(C)=0
2. V(A)=1 V(B)= 0 V(C)=1
3. V(A)=1 V(B)= 1 V(C)=0
4. V(A)=1 V(B)= 1 V(C)=1

Les modèles de φ considérant l'ensemble de littéraux {B, C} sont :

1. V(A)=0 V(B) =1 V(C)=1
2. V(A)=1 V(B) =1 V(C)=1

Exemple 4: idem pour la formule $\varphi = (A \wedge B) \rightarrow C$



› sont :

En considérant le premier ensemble de littéraux :

1. V(A)=0 V(B)=0 V(C)=0
2. V(A)=0 V(B)=0 V(C)=1
3. V(A)=0 V(B)=1 V(C)=0
4. V(A)=0 V(B)=1 V(C)=1

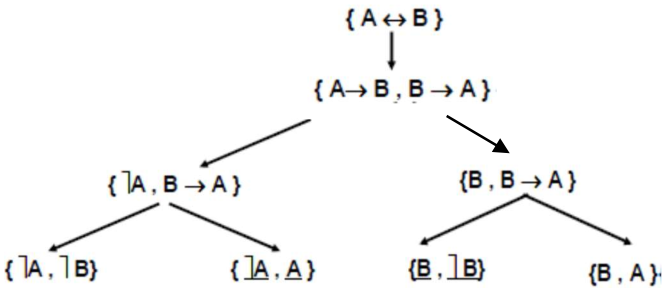
En considérant le deuxième ensemble de littéraux :

1. V(A)=0 V(B)=0 V(C)=0
2. V(A)=0 V(B)=0 V(C)=1
3. V(A)=1 V(B)=0 V(C)=0
4. V(A)=1 V(B)=0 V(C)=1

En considérant le troisième ensemble de littéraux :

1. V(A)=0 V(B)=0 V(C)=1
2. V(A)=0 V(B)=1 V(C)=1
3. V(A)=1 V(B)=0 V(C)=1
4. V(A)=1 V(B)=1 V(C)=1

<u>Exemple</u> 5 : En utilisant la méthode des tableaux sémantiques, quels sont les modèles de la formule $\varphi = A \leftrightarrow B$?



Les modèles sont :

V(A)=0 V(B)=0 V(A)=1 V(B)=1

Remarques :

La méthode des tableaux sémantiques permet de:

- ✓ Prouver si une formule est satisfaite ou non
- ✓ Déterminer un ou tous les modèles d'une formule

b) Preuve de la validité d'une formule

Noter que : Une formule φ est valide veut dire φ est une tautologie.

Théorème : φ valide ⇔ $\neg$φ est non satisfaite

Démonstration

$$\varphi \text{ valide } \Leftrightarrow \forall v[\varphi]_v = 1$$
$$\Leftrightarrow \forall v[\neg\varphi]_v = 0$$
$$\Leftrightarrow \neg\varphi \text{ est non satisfaite}$$

Prouver que φ est valide revient à prouver que $\neg$φ est non satisfaite (en utilisant l'algorithme précédent)

Donc, pour prouver que φ valide, il faut :

1. φ' = $\neg$φ
2. Algorithme des tableaux sémantiques précédent pour φ'
3. Si φ' non satisfaite Alors φ valide Sinon φ non valide

Exemple : La formule φ =A v $\neg$A est valide ou non ?

$\varphi' = \neg(A \vee \neg A)$

$\{\neg(A \vee \neg A)\}$

↓

$\{\neg A, \neg(\neg A)\}$

↓

$\{\neg A, A\}$

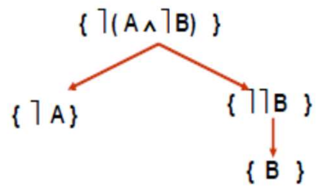
↓

φ' non satisfaite

$\Rightarrow \varphi = A \vee \neg A$ valide

Exemple : la formule φ =A ∧ $\neg$B est valide ou non ?

φ' = $\neg$(A ∧ $\neg$B)



φ' Satisfaite (pour A=0) ⇒ φ Non valide

c) Preuve de la consistance d'un ensemble de formules

Noter qu'un ensemble ∑ est consistant veut dire ∑ est compatible

Théorème

$$\begin{pmatrix} \Sigma = \{\varphi 1, .. \varphi n\} \\ \text{est compatible} \end{pmatrix} \Leftrightarrow \begin{pmatrix} \varphi 1 \wedge ... \wedge \varphi n \\ \text{est satisfaite} \end{pmatrix}$$

Prouver que Σ= {φ_1, ...φ_n} est compatible revient à prouver que la FP φ =φ1∧ .... ∧φn est satisfaite

Démonstration

$$\Sigma = \{\varphi 1, .. \varphi n\} \text{ est compatible } \Leftrightarrow \exists v[\varphi 1]_v = [\varphi 2]_v = \cdots [\varphi n]_v = 1$$
$$\Leftrightarrow \exists v[\varphi 1 \wedge \ldots \wedge \varphi n]_v = 1$$
$$\Leftrightarrow \varphi 1 \wedge \ldots \wedge \varphi n \text{ est satisfaite}$$

Donc, pour prouver que $\Sigma = \{\varphi_1, \ldots \varphi_n\}$ est compatible, il faut :

1. $\varphi' = \varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n$
2. Algorithme des tableaux sémantiques précédent pour φ'
3. Si φ' satisfaite Alors Σ est compatible, sinon Σ est incompatible

d) *Preuve de conséquence logique*

Théorème

$(\varphi 1, \ldots, \varphi n \vdash \varphi) \Leftrightarrow (\varphi 1 \wedge \ldots \wedge \varphi n \rightarrow \varphi$ tautologie $)$

Démonstration

$\varphi 1, \ldots, \varphi n \vdash \varphi \Leftrightarrow \forall v$ (v modèle de $\{\varphi 1, \ldots, \varphi n\} \Rightarrow$ v modèle de φ)

$\varphi 1, \ldots, \varphi n \vdash \varphi \Leftrightarrow \forall v\ ([\varphi 1]_v = \ldots [\varphi n]_v = 1 \Rightarrow [\varphi]_v = 1)$

$\varphi 1, \ldots, \varphi n \vdash \varphi \Leftrightarrow \forall v\ ([\varphi 1 \wedge \varphi 2 \ldots \varphi n]_v = 1 \Rightarrow [\varphi]_v = 1)$

$\varphi 1, \ldots, \varphi n \vdash \varphi \Leftrightarrow \forall v\ ([\varphi 1 \wedge \varphi 2 \ldots \varphi n \Rightarrow \varphi]_v = 1)$

$\varphi 1, \ldots, \varphi n \vdash \varphi \Leftrightarrow \varphi 1 \wedge \varphi 2 \ldots \varphi n \Rightarrow \varphi$ est valide (tautologie□

Prouver que $\varphi 1, \ldots, \varphi n \vdash \varphi$ revient à prouver que la FP $\varphi 1 \wedge \ldots \wedge \varphi n \rightarrow \varphi$ est valide

3- Méthode de déduction naturelle

La méthode de *déduction naturelle* formalise bien la méthode de démonstration en mathématique. Quand on fait des preuves en mathématique, on utilise :

- ✓ Des axiomes
- ✓ Des règles qui permettent pas à pas, de déduire des conséquences à partir de prémisses.

Définition :

Soit le séquent $S = \varphi_1\ \varphi_2 \ldots \varphi_n \vdash \varphi$

Une preuve par déduction du séquent S est une suite finie (non vide) de séquents $S_1, S_2, \ldots S_m$ telle que :

- ➢ $S_m = S = \varphi_1\ \varphi_2 \ldots \varphi_n \vdash \varphi$
- ➢ $\forall 1 \leq i \leq m$ on est dans l'un des cas :
  - ✓ S_i est un axiome
  - ✓ S_i est obtenu par application d'une des règles d'inférence sur des séquents de la suite $S_1, S_2, \ldots S_{i-1}$

Les axiomes :

$\varphi_1\ \varphi_2 \ldots \varphi_n \vdash \varphi_i \quad 1 \leq i \leq n$ sont des axiomes

Ceci signifie que lorsqu'une formule φ_i figure dans une liste des prémisses (hypothèses), la preuve de φ_i est immédiate.

Exemple :

$AvB, B, C \wedge A \vdash AvB$ (axiome)

$F \rightarrow N \wedge M\ F\ M \rightarrow \neg T \vdash F \rightarrow N \wedge M$ axiome

Règles d'inférence :

Une règle d'inférence définit une transition valide dans le déroulement d'une preuve.

La représentation d'une règle d'inférence est de la forme :

$$\frac{\boldsymbol{S1 \;\; S2 \dots Sk}}{\boldsymbol{S}}$$

Où S, S1 S2 …Sk sont des séquents, tel que :

- S1 S2 …Sk sont appelés *antécédents*
- S est appelé *conséquent*

Exemple :

$$\frac{\boldsymbol{\varphi 1 \varphi 2 \varphi 3 \mid -\varphi \qquad \varphi 1 \varphi 2 \varphi 3 \mid -\varphi'}}{\boldsymbol{\varphi 1 \varphi 2 \varphi 3 \mid -\varphi \wedge \varphi'}}$$

Les règles d'inférence de la méthode de déduction naturelle sont divisées en deux catégories :

- Les règles *d'introduction (notées par i)*
- Les règles *d'élimination (notées par e)*

Le tableau suivant présente les règles des deux catégories :

$\dfrac{\Sigma,\varphi \vdash \varphi 1 \wedge \neg\varphi 1}{\Sigma \vdash \neg\varphi}\ \neg i$	$\dfrac{\Sigma,\neg\varphi \vdash \varphi 1 \wedge \neg\varphi 1}{\Sigma \vdash \varphi}\ \neg e$
$\dfrac{\Sigma \vdash \varphi 1 \quad \Sigma \vdash \varphi 2}{\Sigma \vdash \varphi 1 \wedge \varphi 2}\ \wedge i$	$\dfrac{\Sigma \vdash \varphi 1 \wedge \varphi 2}{\Sigma \vdash \varphi 1}\ \wedge e1 \qquad \dfrac{\Sigma \vdash \varphi 1 \wedge \varphi 2}{\Sigma \vdash \varphi 2}\ \wedge e2$
$\dfrac{\Sigma \vdash \varphi}{\Sigma \vdash \varphi 1 \vee \varphi}\ \vee i1 \qquad \dfrac{\Sigma \vdash \varphi}{\Sigma \vdash \varphi \vee \varphi 2}\ \vee i2$	$\dfrac{\Sigma \vdash \varphi 1 \vee \varphi 2 \quad \Sigma,\varphi 1 \vdash \varphi \quad \Sigma,\varphi 2 \vdash \varphi}{\Sigma \vdash \varphi}\ \vee e$
$\dfrac{\Sigma,\varphi \vdash \varphi 1}{\Sigma \vdash \varphi \rightarrow \varphi 1}\ \rightarrow i$	$\dfrac{\Sigma \vdash \varphi 1 \rightarrow \varphi 2 \quad \Sigma \vdash \varphi 1}{\Sigma \vdash \varphi 2}$ **Modus Ponens**

Les règles d'inférence de la déduction naturelle sont Valides, elles sont démontrées.

Exemples de démonstrations :

En utilisant la démonstration par déduction naturelle, démontrer les séquents suivant :

a) A∧B |— B∧A
b) (A∧B)∧C |—A∧(B∧C)

Réponses

a) A∧B |— B∧A

1. A∧B |— A∧B	**axiome**
2- A∧B |— A	**∧e1 sur 1**
3- A∧B |— B	**∧e2 sur 1**
4- A∧B |— B∧A	**∧i sur (3,2)**

b) (A∧B)∧C |—A∧(B∧C)

1. $(A \wedge B) \wedge C \vdash (A \wedge B) \wedge C$ axiome

2- $(A \wedge B) \wedge C \vdash C$ $\wedge$e2 sur 1

3- $(A \wedge B) \wedge C \vdash A \wedge B$ $\wedge$e1 sur 1

4- $(A \wedge B) \wedge C \vdash A$ $\wedge$e1 sur 3

5- $(A \wedge B) \wedge C \vdash B$ $\wedge$e2 sur 3

6- $(A \wedge B) \wedge C \vdash B \wedge C$ $\wedge$i sur (5,2)

7- $(A \wedge B) \wedge C \vdash A \wedge (B \wedge C)$ $\wedge$i sur (4,6)

Exemple applicatif

Soit le problème réel suivant :

1- S'il fait froid alors il neige et Ali est malade

2- Il fait froid

3- Si Ali est malade alors il ne travaille pas

Démontrer que : « Ali ne travaille pas et il neige »

Solution

Problème réel → Formulation → Problème logique → démonstration par déduction naturelle

Problème logique :

On propose les variables propositionnelles suivantes :

F: « Il fait froid »

N: « il neige »

M: « Ali est malade »

T: « Ali travaille »

Donc, le problème écrit en logique propositionnelle est :

$\varphi 1 = F \rightarrow N \wedge M$

$\varphi 2 = F$

$\varphi 3 = M \rightarrow \neg T$

$\varphi = \neg T \wedge N$

Démontrer que : $\varphi 1\ \varphi 2\ \varphi 3 \vdash \varphi$

Démonstration par déduction

1- $\varphi 1\ \varphi 2\ \varphi 3 \vdash F \rightarrow N \wedge M$ - - - - - - - → axiome

2- $\varphi 1\ \varphi 2\ \varphi 3 \vdash F$ - - - - - - - - - - - → axiome

3- $\varphi 1\ \varphi 2\ \varphi 3 \vdash N \wedge M$ - - - - - - - - - - → MP 1,2

4- $\varphi 1\ \varphi 2\ \varphi 3 \vdash M$ - - - - - - - - - - - - → $\wedge$e2 sur 3

5- $\varphi 1\ \varphi 2\ \varphi 3 \vdash M \rightarrow \neg T$ - - - - - - - - - → axiome

6- $\varphi 1\ \varphi 2\ \varphi 3 \vdash \neg T$ - - - - - - - - - - - - → MP 5,4

7- $\varphi 1\ \varphi 2\ \varphi 3 \vdash N$ - - - - - - - - - - - - - → $\wedge$e1 sur 3

8- $\varphi 1\ \varphi 2\ \varphi 3 \vdash \neg T \wedge N$ - - - - - - - - - - - → $\wedge$i sur 6,7

Règles dérivées :

Règle d'augmentation des prémisses	$\dfrac{\Sigma \vdash \varphi}{\Sigma, \Sigma' \vdash \varphi}$	AP
Règle d'introduction de la double négation	$\dfrac{\Sigma \vdash \varphi}{\Sigma \vdash \neg\neg\varphi}$	$\neg\neg$ i
Règle d'élimination de la double négation	$\dfrac{\Sigma \vdash \neg\neg\varphi}{\Sigma \vdash \varphi}$	$\neg\neg$ e
Règle d'élimination de l'implication	$\dfrac{\Sigma \vdash \varphi 1 \rightarrow \varphi 2}{\Sigma\ \varphi 1 \vdash \varphi 2}$	→e
Règle de Modus Tollens	$\dfrac{\Sigma \vdash \varphi 1 \rightarrow \varphi 2 \quad \Sigma \vdash \neg \varphi 2}{\Sigma \vdash \neg \varphi 1}$	MT
Règle du Tiers Exclus	$\overline{\Sigma \vdash \varphi \vee \neg\varphi}$	RTE

67

Remarque :

- L'objectif des règles dérivées et de rendre les preuves plus courtes en évitant certains détails.
- Chaque règle dérivée remplace une suite de séquents.

Quelques exemples d'application des règles dérivées :

a) Règle d'introduction de la double négation

Supposons la démonstration de $\varphi \vdash \neg\neg\varphi \wedge \varphi$

1-	φ	$\vdash$	φ	**axiome**
2-	$\varphi, \neg\varphi$	$\vdash$	φ	**axiome**
3-	$\varphi, \neg\varphi$	$\vdash$	$\neg\varphi$	**axiome**
4-	$\varphi, \neg\varphi$	$\vdash$	$\varphi \wedge \neg\varphi$	**$\wedge$i sur 2,3**
5-	φ	$\vdash$	$\neg\neg\varphi$	**$\neg$i sur 4**
6-	φ	$\vdash$	$\neg\neg\varphi \wedge \varphi$	**$\wedge$i sur (1,5)**

Dans l'exemple ci-dessus on peut passer directement de la ligne1 à la ligne 5 en appliquant la règle dérivée de $\neg\neg$i.

1-	φ	$\vdash$	φ	**axiome**
2-	φ	$\vdash$	$\neg\neg\varphi$	**$\neg\neg$i sur 1**
3-	φ	$\vdash$	$\neg\neg\varphi \wedge \varphi$	**$\wedge$i sur (1,2)**

b) Règle d'augmentation des prémisses

Démontrer $A \wedge B \vdash C \rightarrow A$

1-	$A \wedge B$	$\vdash A \wedge B$	axiome
2-	$A \wedge B$	$\vdash A$	$\wedge$e1 sur 1
3-	$A \wedge B, C$	$\vdash A$	AP sur 2
4-	$A \wedge B$	$\vdash C \rightarrow A$	$\rightarrow$i sur 3