Chapitre 9 : Logique propositionnelle

(Sémantique et mise sous forme normale)

slides disponibles sur `http://cahier-de-prepa/mp2i-fermat`

Plan

1. Syntaxe de la logique propositionnelle
2. Algèbre de Boole
3. Sémantique de la logique propositionnelle
4. Mise sous forme normale

Plan

Plan

Interprétation - définition

On considère encore $\mathcal{Q}$ un ensemble non vide de variables.
On note encore $\mathbb{B}$ l'algèbre de Boole.

Définition

Un ***environnement propositionnel*** *est une fonction de $\mathcal{Q}$ dans $\mathbb{B}$.*

Définition

*Soit $\rho \in \mathbb{B}^{\mathcal{Q}}$ un environnement propositionnel. On définit l'****interprétation selon*** *ρ des formules de la logique propositionnelle sur $\mathcal{Q}$ comme étant la fonction $[\bullet]^\rho$ ci-contre.*

$$\left(\begin{array}{rcc}
\mathbb{F}_p(\mathcal{Q}) & \rightarrow & \mathbb{B} \\
\top & \mapsto & V \\
\bot & \mapsto & F \\
q \in \mathcal{Q} & \mapsto & \rho(q) \\
\neg A & \mapsto & \overline{[A]^\rho} \\
A \vee B & \mapsto & [A]^\rho + [B]^\rho \\
A \wedge B & \mapsto & [A]^\rho \cdot [B]^\rho \\
A \rightarrow B & \mapsto & \overline{[A]^\rho} \cdot [B]^\rho \\
A \leftrightarrow B & \mapsto & ([A]^\rho \cdot [B]^\rho) \\
 & & +(\overline{[A]^\rho} \cdot \overline{[B]^\rho})
\end{array}\right)$$

Vocabulaire

Définition

Soit $A \in \mathbb{F}_p(\mathcal{Q})$.

*Pour $\rho \in \mathbb{B}^{\mathcal{Q}}$, si $[A]^\rho = V$, on dit que ρ **satisfait** A.*
*On dit que A est **satisfiable** s'il existe $\rho \in \mathbb{B}^{\mathcal{Q}}$ tel que $[A]^\rho = V$.*
*On dit que A est **une tautologie** (ou valide) si $\forall \rho \in \mathbb{B}^{\mathcal{Q}}$, $[A]^\rho = V$.*
*On dit que A est **une antilogie** (ou insatisfiable) si $\forall \rho \in \mathbb{B}^{\mathcal{Q}}$, $[A]^\rho = F$.*

Attention : antilogie n'est pas la négation de tautologie, mais celle de formule satisfiable.

Fonction booléenne associée à une formule - définition

informel Changement de point de vue : $[A]^\rho$ dépend de A et de ρ.
Pour la dépendance en A on a, pour $\rho \in \mathbb{B}^{\mathcal{Q}}$ fixé, la fonction $[\bullet]^\rho = A \mapsto [A]^\rho$.
Pour celle en ρ on veut, pour $A \in \mathbb{F}_p(\mathcal{Q})$ fixée, la fonction $\rho \mapsto [A]^\rho$.

Définition

Soit $A \in \mathbb{F}_p(\mathcal{Q})$.
*On appelle **fonction booléenne associée** à la formule A la fonction*

$$[\![\bullet]\!]^A = \begin{pmatrix} \mathbb{B}^{\mathcal{Q}} & \to & \mathbb{B} \\ \rho & \mapsto & [A]^\rho \end{pmatrix}$$

Remarque : Toute fonction booléenne d'arité $n \in \mathbb{N}^*$ est la fonction booléenne associée d'une formule propositionnelle sur un ensemble de variables propositionnelles de cardinal n.
(voir section mise sous forme normale)

Équivalence logique - définition

Définition

On définit la relation binaire $\equiv$ sur $\mathbb{F}_p(\mathcal{Q})$ par

$$\begin{aligned}\forall (A,B) \in \mathbb{F}_p(\mathcal{Q})^2,\ A \equiv B \text{ ssi } & [\![\bullet]\!]^A = [\![\bullet]\!]^B \\ \text{ssi } & \forall \rho \in \mathbb{B}^{\mathcal{Q}},\ [\![\rho]\!]^A = [\![\rho]\!]^B \\ \text{ssi } & \forall \rho \in \mathbb{B}^{\mathcal{Q}},\ [A]^\rho = [B]^\rho\end{aligned}$$

Autrement dit, $\left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [A]^\rho = V\right\} = \left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [B]^\rho = V\right\}$.

Propriété

La relation $\equiv$ est une relation d'équivalence sur $\mathbb{F}_p(\mathcal{Q})$.

Définition

Soit $(A,B) \in \mathbb{F}_p(\mathcal{Q})^2$.
*On dit que A et B sont **logiquement équivalentes** si $A \equiv B$.*

Équivalence logique - exemples

Pour $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$ on a $A \vee B \equiv B \vee A$.

En effet, $\forall \rho \in \mathbb{B}^{\mathcal{Q}}$,
$$\begin{aligned}[A \vee B]^\rho &= [A]^\rho + [B]^\rho && \text{par déf de l'interprétation}\\ &= [B]^\rho + [A]^\rho && \text{par commutativité de } +\\ &= [B \vee A]^\rho && \text{par déf de l'interprétation}\end{aligned}$$

Exercice : Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$. Montrer que

- $\to$ $A \wedge B \equiv B \wedge A$
- $\to$ $A \to B \equiv (\neg A) \vee B$
- $\to$ $A \to B \equiv (\neg B) \to (\neg A)$
- $\to$ $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$
- $\to$ $A \vee \neg A \equiv \top$
- $\to$ $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- $\to$ $\neg(A \vee B) \equiv \neg A \wedge \neg B$

Conséquence logique - définition

Définition

Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$.

On dit que B est ***conséquence logique*** *de A, noté* $A \models B$ *ssi tout environnement propositionnel satisfaisant A satisfait aussi B.*

c'est-à-dire en terme d'ensemble d'environnements ? Autrement dit, $\left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [A]^\rho = V\right\} \subseteq \left\{\rho \in \mathbb{B}^{\mathcal{Q}} \middle| [B]^\rho = V\right\}$.

Propriété

La relation binaire $\models$ *est réflexive et transitive.*

Propriété

Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$. $A \equiv B$ *ssi* $A \models B$ *et* $B \models A$.

preuve à faire (+ remarque csq sémantique vs déduction)

Conséquence logique - exemples

Définition

Soit $X \subseteq \mathbb{F}_p(\mathcal{Q})$. Soit $B \in \mathbb{F}_p(\mathcal{Q})$.
*On note $X \models B$ ssi tout environnement propositionnel satisfaisant **toutes** les formules de X satisfait aussi B.*
Autrement dit, $\left\{\rho \in \mathbb{B}^{\mathcal{Q}} \,\middle|\, \forall A \in X,\ [A]^{\rho} = V\right\} \subseteq \left\{\rho \in \mathbb{B}^{\mathcal{Q}} \,\middle|\, [B]^{\rho} = V\right\}$.

différence avec "B est conséquence de la conjonction des formules de X" ? $\hookrightarrow$ X *peut être de cardinal infini.*

Exercice : Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$. Montrer que

$\rightarrow$ $\{(A \rightarrow B), A\} \models B$

$\rightarrow$ $\{(A \rightarrow B), \neg B\} \models \neg A$

Reformulation des définitions avec $\equiv$

Propriété

Soit $A \in \mathbb{F}_p(\mathcal{Q})$.

- $\rightarrow$ *A est une tautologie ssi* $A \equiv \top$
- $\rightarrow$ *A est une antilogie ssi* $A \equiv \bot$
- $\rightarrow$ *A est une tautologie ssi* $\neg A$ *est une antilogie*

Propriété

Soit $(A, B) \in \mathbb{F}_p(\mathcal{Q})^2$.

- $\rightarrow$ $A \equiv B$ *ssi* $A \leftrightarrow B \equiv \top$ *(i.e.* $A \leftrightarrow B$ *est une tautologie)*
- $\rightarrow$ $A \models B$ *ssi* $A \rightarrow B \equiv \top$ *(i.e.* $A \rightarrow B$ *est une tautologie)*

preuves à faire en exercice

Espace quotient

L'espace des formules logiques quotienté par équivalence $\mathbb{F}_p(\mathcal{Q})/\equiv$ est en bijection avec $\mathcal{F}(\mathbb{B}^{\mathcal{Q}}, \mathbb{B})$. En effet une classe d'équivalence selon $\equiv$ est caractérisée par la fonction booléenne à laquelle sont associées tous ses éléments. Cela justifie que $[\![\bullet]\!]^A$ soit parfois appelée la **représentation** de A.

$\hookrightarrow$ Quel est représentant d'une classe préfère-t-on ?
$\hookrightarrow$ Peut-on choisir une formule canonique pour représenter une classe de formules équivalentes ?

Plan

1. Syntaxe de la logique propositionnelle
2. Algèbre de Boole
3. Sémantique de la logique propositionnelle
4. Mise sous forme normale
   - Mise sous FND à partir d'une table de vérité
   - Mise sous FNC à partir d'une table de vérité

Sur un exemple

Comment mettre sous FND la formule $A = (a \vee b) \rightarrow (c \wedge a)$

a	b	c	$(a \vee b)$	$(c \wedge a)$	A	
V	V	V	V	V	V	$\rightarrow (a \wedge b \wedge c)$
V	V	F	V	F	F	
V	F	V	V	V	V	$\rightarrow (a \wedge \neg b \wedge c)$
V	F	F	V	F	F	
F	V	V	V	F	F	
F	V	F	V	F	F	
F	F	V	F	F	V	$\rightarrow (\neg a \wedge \neg b \wedge c)$
F	F	F	F	F	V	$\rightarrow (\neg a \wedge \neg b \wedge \neg c)$

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

$$(a \wedge b \wedge c) \vee \underbrace{(a \wedge \neg b \wedge c) \vee (\neg a \wedge \neg b \wedge c)}_{(\neg b \wedge c)} \vee (\neg a \wedge \neg b \wedge \neg c)$$

Table de vérité d'une formule

On étend ici la définition de table de vérité aux formules, pour une numérotation des variables fixée : $\mathcal{Q}=\{q_1, q_2, \ldots q_n\}$ où $n=\mathrm{Card}(\mathcal{Q})$.

Une table de vérité d'une formule $A \in \mathbb{F}_p(\mathcal{Q})$ est en fait une table de vérité de la fonction associée $[\![\bullet]\!]^A$:

- $\rightarrow$ $\{(T_{i,j})_{j\in[1..n]} \mid i\in[1..2^n]\} = \mathbb{B}^{\mathcal{Q}}$
- $\rightarrow$ pour tout $i\in[1..2^n]$, $T_{i,n+1}$ vaut $[\![\rho^i]\!]^A$
  où $\rho^i \in \mathbb{B}^{\mathcal{Q}}$ est défini par $\forall j\in[1..n]$, $\rho^i(q_j) = T_{i,j}$.

En calculant une FND à partir de T on calcule bien quelque chose qui ne dépend pas exactement de A mais de sa classe...

Calculer une FND à partir d'une table de vérité - 1/3

Soit $A \in \mathbb{F}_p(\mathcal{Q})$ où $\mathcal{Q} = \{q_1, q_2, \ldots q_n\}$.
Soit T une table de vérité de A suivant cette numérotation de $\mathcal{Q}$.

Pour tout $i \in [1..2^n]$ et $j \in [1..n]$, on note $\ell_{i,j}$ comme étant

- $\rightarrow$ le littéral q_j si $T_{i,j} = V$
- $\rightarrow$ le littéral $\neg q_j$ si $T_{i,j} = F$

Lemme

$\forall i \in [1..2^n], \forall j \in [1..n], [\ell_{i,j}]^{\rho^i} = V$

Preuve: Soit $i \in [1..2^n]$. Soit $j \in [1..n]$.

Si $T_{i,j} = V$, alors $\ell_{i,j} = q_j$, donc $[\ell_{i,j}]^{\rho^i} = \rho^i(q_j)$ par définition de l'interprétation d'une variable. Or par définition de ρ^i, $\rho^i(q_j) = T_{i,j}$, donc $[\ell_{i,j}]^{\rho^i} = V$.

Si $T_{i,j} = F$, alors $\ell_{i,j} = \neg q_j$ donc $[\ell_{i,j}]^{\rho^i} = \overline{\rho^i(q_j)}$ par définition de l'interprétation d'une négation. Or par définition de ρ^i, $\rho^i(q_j) = T_{i,j} = F$, donc $[\ell_{i,j}]^{\rho^i} = \overline{F} = V$.

Calculer une FND à partir d'une table de vérité - 2/3

Ensuite on pose, pour tout $i \in [1..2^n]$, $L^i = \bigwedge_{j=1}^{n} \ell_{i,j}$.

Lemme

- $\forall i \in [1..2^n]$, $[L^i]^{\rho^i} = V$
- $\forall (i,k) \in [1..2^n]^2$, $i \neq k$, $[L^i]^{\rho^k} = F$

Preuve : Soit $i \in [1..2^n]$. Par définition de l'interprétation d'une conjonction, $[L^i]^{\rho^i} = \prod_{j=1}^{n} [\ell_{i,j}]^{\rho^i} = \prod_{j=1}^{n} V$ d'après le lemme précédent, d'où $[L^i]^{\rho^i} = V$.

Soit $k \in [1..2^n]$ tel que $k \neq i$.Puisque les lignes de T restreintes à leurs n premières colonnes sont deux à deux distinctes, il existe $j_0 \in [1..n]$ tel que $T_{i,j_0} \neq T_{k,j_0}$.

$\hookrightarrow$Si $T_{i,j_0} = V$, alors $\ell_{i,j_0} = q_{j_0}$ et $T_{k,j_0} = F$. Par déf. de l'interprétation d'une variable $[\ell_{i,j_0}]^{\rho^k} = \rho^k(q_{j_0})$, or par déf. de ρ^k on a $\rho^k(q_{j_0}) = T_{k,j_0} = F$, donc $[\ell_{i,j_0}]^{\rho^k} = F$.

$\hookrightarrow$Si au contraire $T_{i,j_0} = F$, alors $\ell_{i,j_0} = \neg q_{j_0}$ et $T_{k,j_0} = V$. Par déf. de l'interprétation de la négation d'une variable $[\ell_{i,j_0}]^{\rho^k} = \overline{\rho^k(q_{j_0})}$ or par déf. de ρ^k on a $\rho^k(q_{j_0}) = T_{k,j_0} = V$, donc $[\ell_{i,j_0}]^{\rho^k} = \overline{V} = F$.

Dans les deux cas le terme d'indice j_0 de la somme qu'est l'interprétation de L^i vaut F, et F étant absorbant pour $\times$, on en déduit que $[L^i]^{\rho^k} = F$.

Calculer une FND à partir d'une table de vérité - 3/3

Finalement on pose $D = \bigvee_{\substack{i\in[1..2^n] \\ T_{i,n+1}=V}} L^i$

Propriété

$D \equiv A.$

Preuve : Soit $\rho\in\mathbb{B}^{\mathcal{Q}}$. On note $I = \{i\in[1..2^n] \mid T_{i,n+1}=V\}$ ainsi $D = \bigvee_{i\in I} L^i$.

De plus par déf. de l'interprétation d'une disjonction $[D]^\rho = \sum_{i\in I}[L^i]^\rho$.

Puisque les lignes de T restreintes à leurs n premières colonnes couvrent $\mathbb{B}^{\mathcal{Q}}$, il existe $i_0\in[1..2^n]$ tel que $\rho = \rho^{i_0}$.

$\hookrightarrow$ Si $[A]^\rho = V$, on a $V = [\![\rho]\!]^A = [\![\rho^{i_0}]\!]^A = T_{i_0,n+1}$, donc $i_0\in I$. Ainsi le terme $[L^{i_0}]^\rho$ apparaît dans la somme qu'est $[D]^\rho$, or par le lemme préc., $[L^{i_0}]^\rho = [L^{i_0}]^{\rho^{i_0}} = V$,et V étant absorbant pour la somme, on en déduit que $[D]^\rho = V$, soit $[D]^\rho = [A]^\rho$.

$\hookrightarrow$ Si au contraire $[A]^\rho = F$, alors $T_{i_0,n+1} = F$ donc $i_0\notin I$. Autrement dit $\forall i\in I$, $i\neq i_0$ donc d'après le lemme précédent $[L^i]^{\rho^{i_0}} = F$ soit $[L^i]^\rho = F$. Une somme de F étant F, on en déduit que $[D]^\rho = F$, soit $[D]^\rho = [A]^\rho$.

Sur le même exemple

Comment mettre sous FNC la formule $A = (a \vee b) \rightarrow (c \wedge a)$

a	b	c	$(a \vee b)$	$(c \wedge a)$	A	
V	V	V	V	V	V	
V	V	F	V	F	F	$\rightarrow \quad (\neg a \vee \neg b \vee c)$
V	F	V	V	V	V	
V	F	F	V	F	F	$\rightarrow \quad (\neg a \vee b \vee c)$
F	V	V	V	F	F	$\rightarrow \quad (a \vee \neg b \vee \neg c)$
F	V	F	V	F	F	$\rightarrow \quad (a \vee \neg b \vee c)$
F	F	V	F	F	V	
F	F	F	F	F	V	

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

Calculer une FNC à partir d'une table de vérité

Soit $A \in \mathbb{F}_p(\mathcal{Q})$ où $\mathcal{Q} = \{q_1, q_2, \ldots q_n\}$.
Soit T une table de vérité de A suivant cette numérotation de $\mathcal{Q}$.

Pour tout $i \in [1..2^n]$ et $j \in [1..n]$, on note $r_{i,j}$ comme étant

- $\rightarrow$ le littéral $\neg q_j$ si $T_{i,j} = V$
- $\rightarrow$ le littéral q_j si $T_{i,j} = F$

Ensuite on pose, pour tout $i \in [1..2^n]$, $R^i = \bigvee_{j=1}^{n} r_{i,j}$.

Finalement on pose $C = \bigwedge_{\substack{i \in [1..2^n] \\ T_{i,n+1} = F}} R^i$

Propriété

- $\rightarrow$ $\forall i \in [1..2^n], \forall j \in [1..n], [r_{i,j}]^{\rho^i} = F$
- $\rightarrow$ $\forall i \in [1..2^n], [R^i]^{\rho^i} = F$ *et* $\forall k \in [1..2^n], k \neq i, [R^i]^{\rho^k} = V$
- $\rightarrow$ $C \equiv A$

Bilan sur FNC/FND

- certaines formules sont à la fois sous FNC et FND

exemple : $a \vee b \vee c$

- il y a **existence** de la FNC/FND équivalente à une formule

(on vient de le montrer).

- il n'y a **pas unicité** de de la FNC équivalente à une formule

ex : $(a \vee \neg b) \wedge (c \vee d) \equiv (c \vee d) \wedge (a \vee \neg b)$ du à la commutativité
$(a \vee \neg b \vee b) \wedge (c \vee d) \equiv a \wedge (c \vee d)$ du à la simplfication

- Attention **la taille peut exploser** en passant d'une forme à l'autre

ex : $A = \bigvee_{i=1}^{n} (a_i \wedge b_i)$ est une conj. de n termes, écrite avec $2n$ littéraux,

mais une FND équivalente est une disjonction de 2^n termes étant chacun le produit de n littéraux (pour chaque $i \in [1..n]$, a_i ou b_i apparaît)

$A \equiv (a_1 \vee a_2 \vee a_3 ... a_n) \wedge (b_1 \vee a_2 \vee a_3 ... a_n) \wedge (a_1 \vee b_2 \vee a_3 ... a_n) \ldots \wedge (a_1 \vee b_2 \vee a_3 ... \vee a_{n-1} \vee b_n) \ldots \wedge (b_1 \vee b_2 \vee b_3 ... \vee b_{n-1} \vee b_n)$

Exercices

Quelques simplifications utiles :

- → $A \wedge \neg A \equiv \bot$
- → $A \wedge \top \equiv A$
- → $A \wedge \bot \equiv \bot$
- → $A \wedge (\neg A \vee B) \equiv A \wedge B$
- → $(A \vee B) \wedge (\neg A \vee B) \equiv B$
- → $A \vee \neg A \equiv \top$
- → $A \vee \top \equiv \top$
- → $A \vee \bot \equiv A$
- → $A \vee (\neg A \wedge B) \equiv A \vee B$
- → $(A \wedge B) \vee (\neg A \wedge B) \equiv B$

Mettre sous FNC et FND les formules suivantes :

- → $U : (x \wedge y) \vee (z \wedge \neg z \wedge q) \vee (\neg x \wedge z)$
- → $W : (x \wedge q) \rightarrow ((y \vee \neg z) \wedge q)$
- → $X : (x \wedge y) \leftrightarrow (\neg x \wedge z)$