Partie II : Logique des propositions

I/ Introduction

1) Contexte

Logique des propositions

proposition = une formule logique

Exemple : $(p \vee q) \Rightarrow (q \wedge p)$

↳ variable ↳ opérateur

Ça contient
- opérateurs logiques $(\neg, \wedge, \vee \dots)$
  (connecteurs logiques)
- variables booléennes $(p, q, \dots)$
- constantes $(\top, \bot)$ ↳ (contradiction = faux)
  ↳ (tautologie = toujours vrai)

De plus cela respecte des règles de construction

Logique des prédicat

prédicat : propriété sur un élément de l'univers

Exemple : $P(x) \vee Q(y) \Rightarrow Q(x) \wedge P(y)$

↳ prédicat

Ça contient :
- opérateurs
- variables $(x \in U)$
- prédicats $\left(P : \begin{array}{l} U \to \mathbb{B}ool \\ x \mapsto b \in \{0, 1\} \end{array} \right)$

Respecte des règles de construction

Algèbre booléenne

- L'ensemble des formules (logique) forme une algèbre B.
  ↳ on fait du calcul $(1 + 1 = 2$
  $1 \vee 1 = 1)$

2) Rappel

Table de vérité des opérations

p	$\neg p$
0	1
1	0

p q	$p \wedge q$
0 0	0
0 1	0
1 0	0
1 1	1

p q	$p \vee q$
0 0	0
0 1	1
1 0	1
1 1	1

p q	$p \Rightarrow q$
0 0	1
0 1	1
1 0	0
1 1	1

p q	$p \Leftrightarrow q$
0 0	1
0 1	0
1 0	0
1 1	1

Cb peut on déf d'opérateurs binaire

→ entrée possible

$$2^4 = 16$$

2 valeurs résultat

Table de vérité des propositions

Étant donné P et Q deux propositions

$\neg P$ a pour valeur $\neg$ la valeur de P

$P \wedge Q$ " " " la valeur de P

Exemple :

p q	$(p \wedge q) \Rightarrow (q \vee p)$	$p \wedge q$	$q \vee p$
0 0	1	0	0
0 1	1	0	1
1 0	1	0	1
1 1	1	1	1

Principe de l'implication $P \Rightarrow Q$ c'est vrai si P est faux ou Q est vrai

Cb y a-t-il de lignes ds une table de prop à 3 var

$2^3 = 8$ → nb variables

↳ nb de valeurs pr p, q, r...

Compter en binaire

000
001
010
011
100
101
110
111
1000 et ainsi de suite

Les règles de calcule (étant donné P, Q des propositions)

- double négation $\neg\neg P \equiv P$
- tautologie et contradiction

$(P \vee \neg P) \equiv \top$ $\quad (\top \vee P \equiv \top)$ $\quad (\bot \vee P) \equiv P$

$(P \wedge \neg P) \equiv \bot$ $\quad (\top \wedge P \equiv P)$ $\quad (\bot \wedge P) \equiv \bot$

(utilisé pour l'équivalence)

- idempotence ou/et $\quad P \vee P = P$

$P \wedge P = P$

- associativité ou/et $\quad (P \vee Q) \vee R \equiv P \vee (Q \vee R)$

$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$

Ex : démontrer la règle d'associativité du ou par le calcule

Une proposition c'est une formule sur des variables booléennes

$x \wedge (y \vee \neg z)$ des variables booléennes

x	1	2	3	4
0	0	0	1	1
1	0	1	0	1
	faux	identité	non	vrai

x	y															
0	0	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1
0	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
								xor	NAND	et	=	y	$\Rightarrow$	$\Leftarrow$	ou	vrai

¬ et ou xor NAND

xor → crypto

Pour 3 portes logiques on a $2^{2^3} = 2^8 = 256$

II Syntaxe des propositions

↳ règles de construction

1) Symboles

Une proposition est constituée de symbole $V \cup C \cup L$

$V = \{p, q, r, \ldots\}$ ens des variables

$C = \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$ ens des connecteurs

$L = \{\top, \bot\}$ ens des constantes

⚠ formule "mal formé" $p \neg \top \Rightarrow p\, q\, r$

2) Structure inductive des propositions

On défini l'ensemble des propositions construites sur $V \cup C \cup L$ par induction

Une proposition est :

- une proposition atomique
  - variable $p, q, \ldots$
  - constante $\bot, \top$
- une proposition construite à partir de une ou deux propositions bien construites : P Q.

r_1 - negation $\neg P$

r_2 - conjonction $(P \wedge Q)$

r_3 - disjonction $(P \vee Q)$

r_4 - implication $(P \Rightarrow Q)$

r_5 - équivalence $(P \Leftrightarrow Q)$

Exemple :

$P = (\neg p \vee q) \wedge \neg(p \Rightarrow q)$

Vérifions qu'elle est bien construite

P est construit par r_2 $(\wedge)$ à partir de

$Q = (\neg p \vee q)$; $R = \neg(p \Rightarrow q)$

Vérifions que Q et R sont bien construit

Q est construit par r_3 $(\vee)$ à partir de $\neg p$ et de q

Vérifions que $\neg p$ est q sont bien construites

- $\neg p$ est construit par r_1 à partir de p
  - p est une prop atomique
- q est une prop atomique

Vérifions que R est bien construit

~~R est construit par par r_4 à partir de~~

R est construit par r_1 à partir de $S = p \Rightarrow q$

S est construit par r_4 à partir de p et q.

- p atomique
- q "

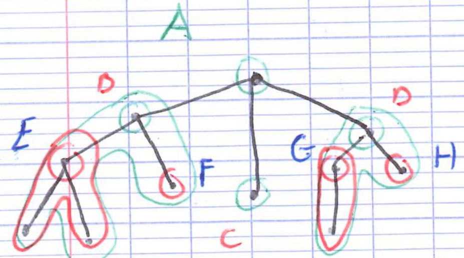
La proposition est donc bien formé.

3) Représentation par arbre

Un arbre est construit par induction sur $\mathbb{N}$

ou bien - ~~feuille~~ feuille • (représente le cas de base)

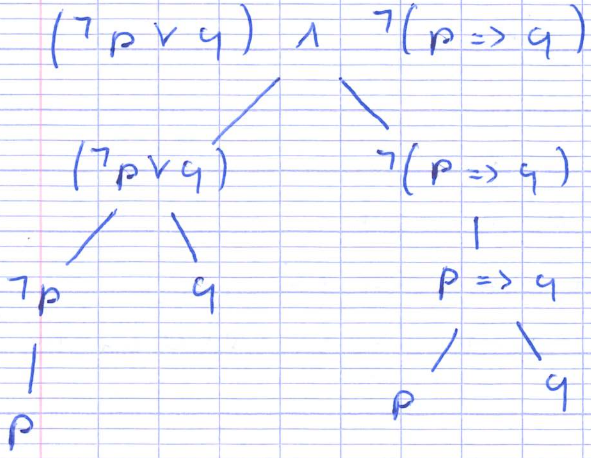
ou bien - noeud 
+ liste de fils
↳ arbres

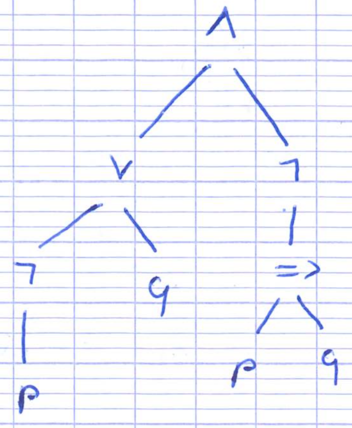


Pour représenter une formule (bien formé) on étiquette les feuilles par des symboles $V \cup L$ et les ~~noeuf~~ noeud par des symboles de C.

p $\neg$ → noeud à 1 fils

p $\wedge \vee \Rightarrow \Leftrightarrow$ → 2 fils





algo constr_arbre (P) :

cas de base :

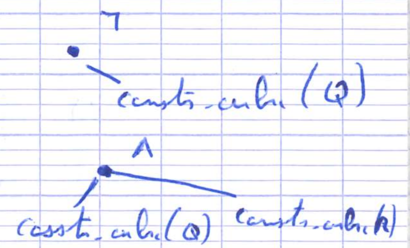
si P est variable alors • p

sinon si P est constante alors • ⊥ • T } feuille

appel récursif

sinon si P est negation ($P = \neg Q$) alors

sinon si P est conjonction ($P = Q \wedge R$) alors



⋮

si P est équivalence

4) Algorithmes utiles

Algorithmes pour compter le nb de connecteurs :

algo nb_connecteur (P)

si P var ou cst alors 0

sinon si $P = \neg Q$ alors 1 + nb_connecteur (Q)

si $P = Q * R$ alors 1 + nb_connecteur(Q) + nb_connecteur (R)

↳ connecteur binaire $\wedge$ $\vee$ $\Rightarrow$ $\Leftrightarrow$

algo : ens des variables.

algo ens_var (P)

si $P = p$ alors $\{p\}$

si $P = \bot$ ou $\top$ alors $\{\}$

si $P = \neg Q$ alors ens_var (Q)

si $P = Q * R$ alors ens_var (Q) $\cup$ ens_var (R)

↳ $\wedge$ $\vee$ $\Rightarrow$ $\Leftrightarrow$

5) Convention ?

III Sémantique des propositions

↳ donner un sens aux opérateurs / variables

À chaque proposition on veut associer une valeur de vérité calculée à partir des composantes de la formule.

1) Interprétation de logique

Une interprétation $\mathcal{I}$ associe - une valeur de vérité aux constantes

- une fonction booléenne aux opérateurs.

$I(\top) = 1$

$I(\bot) = 0$

$I(\neg) : \mathbb{B} \longrightarrow \mathbb{B}$

$0 \longmapsto 1$

$1 \longmapsto 0$

$I(\vee) : \mathbb{B} \times \mathbb{B} \longrightarrow \mathbb{B}$

$I(\vee)(a, b) = 0$ ssi $a = b = 0$

$I(\wedge) : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ $\quad$ $I(\wedge)(a,b) = 1$ ssi $a = b = 1$

$I(\Rightarrow) : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$I(\Leftrightarrow) : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

(cf tables de vérité section I)

$(P \Rightarrow Q)$ $\quad$ $I(\Rightarrow)\,(v(P), v(Q))$

p, q	$p \Rightarrow q$

2) Interprétation des variables

$I(p) \in \mathbb{B}$

~~exemples~~

Exemple : $V = \{p, q, r\}$

$I(p) = 0$ $\quad$ $I(q) = 0$ $\quad$ $I(r) = 1$

Pour n variables il y a 2^n interprétations possibles

3) Valeur de vérité d'une proposition

↳ résultat de son calcul

La valeur de vérité $v_I(P)$ d'une proposition P dans l'interprétation I est défini par induction (récurrence)

Cas de base

~~v_I~~

$$v_I(\bot) = 0 \; ; \; v_I(\top) = 1 \; ; \; v_I(p) = I(p)$$

Cas construit

$v_I(P)$: si $P = \neg Q$ alors $v_I(P) = I(\neg)(v_I(Q))$

si $P = R \wedge Q$ alors $v_I(P) = I(\wedge)(v_I(R), v_I(Q))$
si $P = R \vee Q$
$P = R \Rightarrow Q$
$P = R \Leftrightarrow Q$

(cf table de vérité des propositions)
La table de vérité de P donne la valeur de vérité de P pour ttes les interprétations possibles.

4) Vocabulaire

Etant donné P :
I est un modèle pour P si $v_I(P) = 1$
I' est un contre-modèle pour P si $v_{I'}(P) = 0$

P est insatisfiable si P n'a pas de modèle
P est satisfiable { P est contingeante si P a au moins 1 modèle et un contre-modèle
P valide si P n'a pas de cts modèle

Exemple : $P = \neg p \Rightarrow q$
Un modèle de P est I tq $I(p) = 1$
$I(q) = 0$

$\neg p \Rightarrow q$ $\quad \neg 1 \Rightarrow 0 \quad 0 \Rightarrow 0 \quad 1$

$$v_I(p) = v_I(I(\Rightarrow)(v_I(\neg p) ; v_I(q)))$$
$$= \underbrace{v_I(I(\Rightarrow)(\underbrace{I(\neg)(\underset{1}{v_I(p)})}_{0}, \underset{0}{v_I(q)}))}_{1}$$

soit I' tq $I'(p)=0$ et $I'(q)=0$
alors I' est un contre-modèle.

		p	q	$\neg p$	$\neg p \to q$
ctr modèl	I_1	0	0	1	0
modèle	I_2	0	1	1	1
	I_3	1	0	0	1
	I_4	1	1	0	1

Exemple :

$P = \top$ — P est valide (et donc satisfiable
$Q = (\bot \Rightarrow p)$ — Q est valide
$R = p$
$S = \neg p \Rightarrow p$ } contingente
$T = \bot \vee p$
$U = \bot$ } insatisfiable
$V = \neg p \wedge p$ } insatisfiable

Propriété :

P satisfiable ssi $\neg P$ (pas valide)
P satisfiable $\to$ $\exists$ un modèle
$\neg P$ insati $\leftarrow$ ↳ ttes interprétations est un modèle ↔ valide
$\neg P$ contingente ↳ $\exists$ modèles / contre-modèles
↳ contingente

Les modèles de P sont les ctr-modèle de $\neg P$
" " $\neg P$ " " " P

P insatisfiable ssi $\neg P$ valide
P contingente ssi $\neg P$ contingente

L'ensemble des propositions est partitionné par
l'ensemble des prop. insatisfiables
" " contingentes
" " valides

IV Substitution

EQUIVALENCE SEMANTIQUE

Définition

Deux propositions P Q sont sémantiquement équivalentes $P \equiv Q$ ssi pour $\forall$ interprétation I, P et Q ont la m̂ valeur de vérité

$$\forall_I \quad v_I(P) = v_I(Q)$$

Remarque : équivalence sémantique $\neq$ égalité syntaxique

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

$$\neg p \vee \neg q \neq \neg(p \wedge q)$$

connecteur équiv ($\leftrightarrow$)

égalité en valeur de vérité

$$|V| = |V|$$

$$I : \begin{array}{l} p \to 1 \\ q \to 0 \\ r \to 1 \end{array} \qquad v_I(p \vee q) = v_I(p \vee r)$$

Théorème :

Etant donné une proposition P, et une sous formule (proposition) Q, une proposition $R \equiv Q$, on pose P' la prop. obtenue en remplaçant Q par R et alors $P \equiv P'$

$$R = \neg p \vee \neg q$$

$$P = \underbrace{\neg(p \wedge q)}_{Q} \to (r \vee (q \to r))$$

Propriété : $P \equiv Q$ ssi $P \leftrightarrow Q$ valide

$P = (p \vee q) \vee r$

$Q = p \vee (q \vee r)$

p	q	r	P	Q	$P \leftrightarrow Q$
0	0	0	0	0	1
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	1	1	1
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	1	1

exc : $P = (p \vee \neg p) \wedge (\neg q \wedge \neg r)$

$P' = \neg(r \vee q)$

p	q	r	① $p \vee \neg p$	② $\neg q \wedge \neg r$	① $\wedge$ ②
0	0	0	1	1	1
0	0	1	1	0	0
0	1	0	1	0	0
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	0	0
1	1	1	1	0	0

p	r	q	$r \vee q$	$\neg(r \vee q)$
0	0	0	0	1
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

$P = (p \vee \neg p) \wedge (\neg q \wedge \neg r)$ par le théorème

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

$\equiv \top \wedge \neg(q \vee r)$ $\qquad \top \wedge Q \equiv Q$

$\equiv \neg(q \vee r)$

$\equiv \neg(r \vee q) = P'$