Transformation d’une formule logique

Benjamin Wack

Université Grenoble Alpes

Janvier 2022

Au dernier cours

- Pourquoi la logique formelle ?
- Logique propositionnelle
- Syntaxe
- Sens des formules

Notre exemple avec une table de vérité

Hypothèses :

- (H1) : Si Pierre est grand, alors Jean n'est pas le fils de Pierre
- (H2) : Si Pierre n'est pas grand, alors Jean est le fils de Pierre
- (H3) : Si Jean est le fils de Pierre alors Marie est la soeur de Jean

Conclusion (C) : Marie est la soeur de Jean ou Pierre est grand.

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

p	j	m	$p \Rightarrow \neg j$	$\neg p \Rightarrow j$	$j \Rightarrow m$	$H_1 \wedge H_2 \wedge H_3$	$m \vee p$	$H_1 \wedge H_2 \wedge H_3 \Rightarrow C$
0	0	0	1	0	1	0	0	1
0	0	1	1	0	1	0	1	1
0	1	0	1	1	0	0	0	1
0	1	1	1	1	1	1	1	1
1	0	0	1	1	1	1	1	1
1	0	1	1	1	1	1	1	1
1	1	0	0	1	0	0	1	1
1	1	1	0	1	1	0	1	1

Plan

Conséquence

Définition 1.2.24

A est conséquence de l'ensemble Γ d'hypothèses ($\Gamma \models A$) si tout modèle de Γ est modèle de A.

Remarque 1.2.26

$\models A$ signifie donc bien que A est valide.
(Toute assignation est modèle de l'ensemble vide.)

Exemple de Conséquence

Exemple 1.2.28

$a \Rightarrow b, b \Rightarrow c \models a \Rightarrow c$.

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

Propriété INCONTOURNABLE

Constamment utilisée dans les exercices et examens.

Propriété 1.2.27

Soit $H_n = A_1 \wedge \ldots \wedge A_n$.
Les trois formulations suivantes sont équivalentes :

1. $A_1, \ldots, A_n \models B$
2. $H_n \Rightarrow B$ est valide.
3. $H_n \wedge \neg B$ est insatisfaisable.

Démonstration.

Elle se base sur les tables de vérité des connecteurs.
On procède en démontrant que $1 \Rightarrow 2$ puis $2 \Rightarrow 3$ et $3 \Rightarrow 1$. □

Preuve (1/3)

- $1 \Rightarrow 2$: supposons que $A_1, \dots, A_n \models B$.

Soit une assignation v :

- si v n'est pas modèle de $A_1, \dots, A_n$:
  pour un certain i on a $[A_i]_v = 0$, d'où $[H_n]_v = 0$.
  Ainsi $[H_n \Rightarrow B]_v = 1$.
- si v est modèle de $A_1, \dots, A_n$:
  alors par hypothèse v est un modèle de B donc $[B]_v = 1$.
  Ainsi $[H_n \Rightarrow B]_v = 1$.

Donc $H_n \Rightarrow B$ est valide.

Preuve (2/3)

- $2 \Rightarrow 3$: supposons que $H_n \Rightarrow B$ est valide.
  Pour toute assignation v on a alors :
  - soit $[H_n]_v = 0$,
  - soit $[H_n]_v = 1$ et $[B]_v = 1$.

  Or $[H_n \wedge \neg B]_v = \min([H_n]_v, [\neg B]_v) = \min([H_n]_v, 1 - [B]_v)$.

  Dans les deux cas, nous obtenons $[H_n \wedge \neg B]_v = 0$.
  Donc $H_n \wedge \neg B$ est insatisfaisable.

Preuve (3/3)

- $3 \Rightarrow 1$: supposons que $H_n \wedge \neg B$ est insatisfaisable.
  Montrons que $A_1, \ldots, A_n \models B$.

  Soit v un modèle de $A_1, \ldots, A_n$:
  - $[H_n]_v = [A_1 \wedge \ldots \wedge A_n]_v = 1$.
  - D'après notre hypothèse $[\neg B]_v = 0$.
    D'où $1 - [B]_v = 0$ et donc $[B]_v = 1$: v est un modèle de B.

La validité du raisonnement par implications circulaires sera démontrée en exercice.

Illustration de la propriété

Exemple 1.2.28

a	b	c	$a \Rightarrow b$	$b \Rightarrow c$	$a \Rightarrow c$	$(a \Rightarrow b) \land (b \Rightarrow c) \Rightarrow (a \Rightarrow c)$	$(a \Rightarrow b) \land (b \Rightarrow c) \land \neg(a \Rightarrow c)$
0	0	0	1	1	1	1	0
0	0	1	1	1	1	1	0
0	1	0	1	0	1	1	0
0	1	1	1	1	1	1	0
1	0	0	0	1	0	1	0
1	0	1	0	1	1	1	0
1	1	0	1	0	0	1	0
1	1	1	1	1	1	1	0

Compacité

Théorème 1.2.30 Compacité propositionnelle

Un ensemble de formules propositionnelles a un modèle si et seulement si tous ses sous-ensembles finis ont un modèle.

Preuve difficile car l’ensemble peut être infini !

Nous l’utiliserons pour la démonstration automatique au premier ordre.

Préambule

Comment prouver qu'une formule est valide ?

- Table de vérité
  - Problème : pour une formule à 100 variables, la table de vérité aura 2^{100} lignes (non calculable même par un ordinateur !).
- Idée :
  - Simplifier la formule en utilisant des règles de calcul
  - Puis étudier la formule simplifiée en utilisant les tables de vérités ou un raisonnement logique

La disjonction

- associative $x \vee (y \vee z) \equiv (x \vee y) \vee z$
- commutative $x \vee y \equiv y \vee x$
- idempotente $x \vee x \equiv x$

Idem pour la conjonction.

Distributivité

- La conjonction est distributive sur la disjonction
  $x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z)$
- La disjonction est distributive sur la conjonction
  $x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z)$

Neutralité et Absorption

- 0 est l'élément neutre de la disjonction $0 \vee x \equiv x$
- 1 est l'élément neutre de la conjonction $1 \wedge x \equiv x$
- 1 est l'élément absorbant de la disjonction $1 \vee x \equiv 1$
- 0 est l'élément absorbant de la conjonction $0 \wedge x \equiv 0$

Négation

- Les lois de la négation :
  - $x \wedge \neg x \equiv 0$
  - $x \vee \neg x \equiv 1$ (Le tiers-exclus)
- $\neg\neg x \equiv x$
- $\neg 0 \equiv 1$
- $\neg 1 \equiv 0$

Les lois de De Morgan

- $\neg(x \wedge y) \equiv \neg x \vee \neg y$
- $\neg(x \vee y) \equiv \neg x \wedge \neg y$

Augustus De Morgan (1860) étend les notions de l'algèbre de Boole :

- Travail sur les quantificateurs
- Notion de calcul sur des relations
  (voir aussi les travaux de C.S. Peirce)

qui déboucheront sur la logique du premier ordre (cf 2è partie du cours).

- Notion de dualité dans les algèbres de Boole

aujourd'hui connue principalement sous la forme des lois de De Morgan

- Participation (assez anecdotique) aux premières conjectures sur le théorème des quatre couleurs

Lois de simplification

Propriété 1.2.31

Pour tout x, y nous avons :

- $x \vee (x \wedge y) \equiv x$
- $x \wedge (x \vee y) \equiv x$
- $x \vee (\neg x \wedge y) \equiv x \vee y$

Substitution

Définition 1.3.1

Une substitution σ est une application de l'ensemble des variables dans l'ensemble des formules.

$A\sigma$ = remplacer dans la formule toute variable x par la formule $\sigma(x)$.

Exemple : $A = \neg(p \land q) \Leftrightarrow (\neg p \lor \neg q)$

- Soit σ la substitution suivante : $\sigma(p) = (a \lor b), \sigma(q) = (c \land d)$
- $A\sigma = \neg((a \lor b) \land (c \land d)) \Leftrightarrow (\neg(a \lor b) \lor \neg(c \land d))$

Substitution à support fini

Définition 1.3.2

- Le support d'une substitution σ est l'ensemble des variables x telles que $x\sigma \neq x$.
- Une substitution σ à support fini est notée $< x_1 := A_1, \ldots, x_n := A_n >$

Exemple 1.3.3

$A = x \vee x \wedge y \Rightarrow z \wedge y$ et $\sigma =< x := a \vee b, z := b \wedge c >$

$\boxed{A\sigma = (a \vee b) \vee (a \vee b) \wedge y \Rightarrow (b \wedge c) \wedge y}$

Propriétés des substitutions

Propriété 1.3.4

Si v est une assignation et σ une substitution :
Soit l'assignation $w : x \mapsto [\sigma(x)]_v$.
Alors pour tout A on a $[A\sigma]_v = [A]_w$.

Exemple 1.3.5 :
Soit $A = x \vee y \vee d$
Soit $\sigma =< x := a \vee b, y := b \wedge c >$
Soit v telle que $v(a) = 1$, $v(b) = 0$, $v(c) = 0$, $v(d) = 0$

$$\boxed{\begin{array}{ll} A\sigma = (a \vee b) \vee (b \wedge c) \vee d & w(x) = [a \vee b]_v = 1 \vee 0 = 1 \\ & w(y) = [b \wedge c]_v = 0 \wedge 0 = 0 \\ & w(d) = [d]_v = 0 \\ [A\sigma]_v = (1 \vee 0) \vee (0 \wedge 0) \vee 0 & \\ \qquad = 1 \vee 0 \vee 0 = 1 & [A]_w = 1 \vee 0 \vee 0 = 1 \end{array}}$$

Cas de base : $|A| = 0$

Deux cas possibles :

- Si A est $\top$ ou $\perp$ alors $A\sigma = A$ et $[A]_v$ ne dépend pas de v.
- Si A est une variable x, par construction $[x\sigma]_v = w(x)$.

Induction

Hypothèse : Supposons que la propriété soit vraie pour toute formule de taille inférieure ou égale à n.
Soit A une formule de taille $n+1$, deux cas possibles :

- Cas 1 : $A = \neg B$ avec $|B| = n$.
  $[A\sigma]_v = [\neg B\sigma]_v = 1 - [B\sigma]_v$ et $[A]_w = [\neg B]_w = 1 - [B]_w$.
  Par hypothèse de récurrence $[B\sigma]_v = [B]_w$
  D'où $[A\sigma]_v = [A]_w$.

Induction

Hypothèse : Supposons que la propriété soit vraie pour toute formule de taille inférieure ou égale à n.
Soit A une formule de taille $n+1$, deux cas possibles :

- Cas 2 : $A = (B \circ C)$ avec $|B| < n+1$ et $|C| < n+1$.
  D'une part $[A\sigma]_v = [B\sigma \circ C\sigma]_v$, d'autre part $[A]_w = [B \circ C]_w$.

  Par hypothèse de récurrence $[B\sigma]_v = [B]_w$ et $[C\sigma]_v = [C]_w$.
  La sémantique de $\circ$ restant la même dans les deux cas, $[A\sigma]_v = [A]_w$.

Substitution d'une formule valide

Théorème 1.3.6

Si A est valide alors $A\sigma$ aussi (quelle que soit σ !).

Démonstration.

Soit v une assignation quelconque.

D'après la propriété 1.3.4 : $[A\sigma]_v = [A]_w$ avec $w : x \mapsto [\sigma(x)]_v$.

Puisque A est valide, $[A]_w = 1$.

$A\sigma$ vaut 1 dans toute assignation, c'est donc une formule valide. $\square$

Exemples

Exemple 1.3.7

Soit A la formule $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$. Cette formule est valide, c'est une équivalence remarquable. Soit σ la substitution suivante : $< p := (a \vee b), q := (c \wedge d) >$. La formule

$$\boxed{A\sigma = \neg((a \vee b) \wedge (c \wedge d)) \Leftrightarrow (\neg(a \vee b) \vee \neg(c \wedge d)) \text{ est aussi valide.}}$$

Remplacement

Définition 1.3.8

La formule D est obtenue en remplaçant dans C certaines occurrences de A par B si :

- C s'écrit $E < x := A >$
- D s'écrit $E < x := B >$

pour une certaine formule E.

Exemples

Exemple 1.3.9

Considérons la formule $C = ((a \Rightarrow b) \vee \neg(a \Rightarrow b))$.

- La formule obtenue en remplaçant toutes les occurrences de $(a \Rightarrow b)$ par $(a \wedge b)$ est

  $$\boxed{D = ((a \wedge b) \vee \neg(a \wedge b))}$$

  avec $E = (x \vee \neg x)$.
- La formule obtenue en remplaçant la *première* occurrence de $(a \Rightarrow b)$ par $(a \wedge b)$ est

  $$\boxed{D = ((a \wedge b) \vee \neg(a \Rightarrow b))}$$

  avec $E = (x \vee \neg(a \Rightarrow b))$.

Propriétés des remplacements

Théorème 1.3.10

Si D est obtenue en remplaçant, dans C, des occurrences de A par B alors : $(A \Leftrightarrow B) \models (C \Leftrightarrow D)$.

Démonstration.

Par définition, $C = E < x := A >$ et $D = E < x := B >$.
Si $[A]_v = [B]_v$ alors les w pour ces deux substitutions sont identiques.
Donc $[C]_v = [D]_v$: l'assignation v est modèle de $(C \Leftrightarrow D)$. $\square$

Exemple 1.3.12 : $p \Leftrightarrow q \models (p \vee (\boxed{p} \Rightarrow r)) \Leftrightarrow (p \vee (\boxed{q} \Rightarrow r))$.

Corollaire 1.3.11

Soit D obtenue en remplaçant, dans C, une occurrence de A par B.
Si $A \equiv B$ alors $C \equiv D$.

Définitions

Définition 1.4.1

- Un littéral est une variable ou la négation d'une variable.
- Un monôme est une conjonction de littéraux.
- Une clause est une disjonction de littéraux.
  (cas particuliers : 0 et 1)

Exemple 1.4.2

- $x, y, \neg z$ sont des littéraux.
- $x \wedge \neg y \wedge z$ est un monôme
- Le monôme $x \wedge \neg y \wedge z \wedge \neg x$ comporte x et $\neg x$: il vaut 0.
- $x \vee \neg y \vee z$ est une clause
- La clause $x \vee \neg y \vee z \vee \neg x$ comporte x et $\neg x$: elle vaut 1.

Forme normale

Definition 1.4.3

Formule en forme normale = seulement $\wedge, \vee$ et des négations sur les variables.

Exemple 1.4.4

La formule $\neg a \vee b$ est en forme normale.
$a \Rightarrow b$ est équivalente mais n'est pas en forme normale.

Toute formule admet une forme normale équivalente.

Mise en forme normale

1. **Élimination des équivalences**
   Remplacer $A \Leftrightarrow B$ par
   (a) $(\neg A \vee B) \wedge (\neg B \vee A)$
   OU
   (b) $(A \wedge B) \vee (\neg A \wedge \neg B)$
2. **Élimination des implications**
   Remplacer $A \Rightarrow B$ par $\neg A \vee B$
3. **Déplacement des négations vers les variables**
   Remplacer
   (a) $\neg\neg A$ par A
   (b) $\neg(A \vee B)$ par $\neg A \wedge \neg B$
   (c) $\neg(A \wedge B)$ par $\neg A \vee \neg B$

Remarque 1.4.5 : simplifications

Simplifier le plus tôt possible :

1. Remplacer $\neg(A \Rightarrow B)$ par $A \wedge \neg B$
2. Remplacer une conjonction par 0 si elle comporte une formule et sa négation
3. Remplacer une disjonction par 1 si elle comporte une formule et sa négation
4. Appliquer :
   - l'idempotence de la conjonction et de la disjonction,
   - le caractère neutre ou absorbant de 0 et de 1,
   - remplacer $\neg 1$ par 0 et $\neg 0$ par 1.
5. Appliquer les simplifications :
   - $x \vee (x \wedge y) = x$,
   - $x \wedge (x \vee y) = x$,
   - $x \vee (\neg x \wedge y) = x \vee y$

Forme normale disjonctive

Définition 1.4.6

Une formule est en forme normale disjonctive (FND) si et seulement si elle est une disjonction (somme) de monômes.

Méthode : distribuer les conjonctions sur les disjonctions
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
L'intérêt des FND est de mettre en évidence les modèles.

Exemple 1.4.7

$(x \wedge y) \vee (\neg x \wedge \neg y \wedge z)$ est une FND, qui a deux modèles principaux :

- $x = 1, y = 1$
- $x = 0, y = 0, z = 1$

Forme normale conjonctive

Définition 1.4.11

Une formule est en forme normale conjonctive (FNC) si et seulement si elle est une conjonction (produit) de clauses.

Appliquer la distributivité (!) de la disjonction sur la conjonction :

- $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

L'intérêt des FNC est de mettre en évidence les contre-modèles.

Exemple 1.4.12

$(x \vee y) \wedge (\neg x \vee \neg y \vee z)$ est une FNC, qui a deux contre-modèles

- $x = 0, y = 0$
- $x = 1, y = 1, z = 0.$

Utilisée en modélisation (SAT-solvers)

Exemples 1.4.8 et 1.4.13

Mise en FND de :

$$(a \vee b) \wedge (c \vee d \vee e) \equiv$$

$$\boxed{(a \wedge c) \vee (a \wedge d) \vee (a \wedge e) \vee (b \wedge c) \vee (b \wedge d) \vee (b \wedge e).}$$

Mise en FNC de :

$$(a \wedge b) \vee (c \wedge d \wedge e) \equiv$$

$$\boxed{(a \vee c) \wedge (a \vee d) \wedge (a \vee e) \wedge (b \vee c) \wedge (b \vee d) \wedge (b \vee e).}$$

Une autre utilisation de la FND

La mise en forme normale disjonctive permet également de déterminer si une formule est valide ou non.

Soit A une formule dont on souhaite déterminer la validité :

On transforme $\neg A$ en une disjonction de monômes équivalente B :

- Si $B = 0$ alors $\neg A = 0$, donc $A = 1$, c'est-à-dire, A est valide
- Sinon B est égal à une disjonction de monômes non nuls équivalente à $\neg A$, qui nous donnent des modèles de $\neg A$, donc des contre-modèles de A.

Exemple 1.4.9

Soit $A = (p \Rightarrow (q \Rightarrow r)) \Rightarrow (p \wedge q \Rightarrow r)$

Déterminer si A est valide.

$$
\begin{array}{ll}
\neg A & \\
\equiv (p \Rightarrow (q \Rightarrow r)) \wedge \neg(p \wedge q \Rightarrow r) & \text{car } \neg(B \Rightarrow C) \equiv B \wedge \neg C \\
\equiv (\neg p \vee \neg q \vee r) \wedge \neg(p \wedge q \Rightarrow r) & \text{élimination de deux } \Rightarrow \\
\equiv (\neg p \vee \neg q \vee r) \wedge (p \wedge q \wedge \neg r) & \neg(\ldots \Rightarrow \ldots) \\
\equiv (\neg q \vee r) \wedge p \wedge q \wedge \neg r & \text{simplification } x \wedge (\neg x \vee y) \\
\equiv (r) \wedge p \wedge q \wedge \neg r & \text{simplification } x \wedge (\neg x \vee y) \\
= 0 & \text{car on a } r \wedge \neg r \text{ dans le monôme}
\end{array}
$$

Donc $\neg A = 0$ et $A = 1$, c'est-à-dire A est valide.

Exemple 1.4.10

$$
\begin{aligned}
&\neg A \\
&= \neg((a \Rightarrow b) \wedge c) \wedge \neg(a \wedge d) && \text{(de Morgan)} \\
&= (\neg(a \Rightarrow b) \vee \neg c) \wedge (\neg a \vee \neg d) && \text{(de Morgan)} \\
&= ((a \wedge \neg b) \vee \neg c) \wedge (\neg a \vee \neg d) && (\neg(\ldots \Rightarrow \ldots)) \\
&= (a \wedge \neg b \wedge \neg a) \vee (a \wedge \neg b \wedge \neg d) \vee (\neg c \wedge \neg a) \vee (\neg c \wedge \neg d) \\
& && \text{(distributivité } \vee \text{ sur } \wedge) \\
&= (a \wedge \neg b \wedge \neg d) \vee (\neg c \wedge \neg a) \vee (\neg c \wedge \neg d) && \text{(1er monôme contradictoire)}
\end{aligned}
$$

On obtient 3 modèles de $\neg A$: $(a = 1, b = 0, d = 0)$, $(a = 0, c = 0)$, $(c = 0, d = 0)$.

C'est-à-dire, des contre-modèles de A.

Donc A n'est pas valide.

Aujourd'hui

- Les substitutions permettent de **déduire la validité** d'une formule à partir d'une autre
- Les remplacements permettent de modifier une partie d'une formule **sans changer sa signification** et autorisent donc à effectuer des calculs sur les formules
- Toute formule admet des formes normales qui permettent d'**identifier ses modèles** ou ses contre-modèles

La prochaine fois

- Algèbre de Boole
- Fonctions booléennes
- Résolution

À chercher : prouver par simplification de formule notre exemple

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$