Mise à niveau: propositions et prédicats

Lionel Vaux Auclair

I2M, université d'Aix-Marseille

M2 IMD

Plan

Calcul propositionnel

On fixe un ensemble infini dénombrable $\mathcal{V}_p$ de variables propositionnelles (ou propositions indéterminées, ou formules propositionnelles atomiques), notées $X, Y, \ldots$.

Définition

L'ensemble $\mathcal{F}_p$ des formules propositionnelles est l'ensemble des expressions de la forme :

$$A, B, \ldots \ ::= \ X \mid A \wedge B \mid A \vee B \mid \neg A \mid A \Rightarrow B \mid A \Leftrightarrow B \mid \top \mid \bot$$

$=$ les expressions sur la signature $\{\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow, \top, \bot\}$.

Les tables de la véritable vérité vraie (100% garanti)

La validité d'une formule propositionnelle se *calcule* dans $\mathbf{B} = \{0, 1\}$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\top$	$\bot$
0	0	0	0	1	1	1	1	0
0	1	0	1	1	1	0	1	0
1	0	0	1	0	0	0	1	0
1	1	1	1	0	1	1	1	0

- On voit les connecteurs comme des opérations.
- La valeur d'une expression se déduit *inductivement* de celle de ses sous-expressions.

Les tables de la véritable vérité vraie (100% garanti)

La validité d'une formule propositionnelle se *calcule* dans $\mathbf{B} = \{0, 1\}$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\top$	$\bot$	X
0	0	0	0	1	1	1	1	0	?
0	1	0	1	1	1	0	1	0	?
1	0	0	1	0	0	0	1	0	?
1	1	1	1	0	1	1	1	0	?

- On voit les connecteurs comme des opérations.
- La valeur d'une expression se déduit *inductivement* de celle de ses sous-expressions.

Les tables de la véritable vérité vraie (100% garanti)

La validité d'une formule propositionnelle se *calcule* dans $\mathbf{B} = \{0, 1\}$:

A	B	$A \wedge B$	$A \vee B$	$\neg A$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\top$	$\bot$	X
0	0	0	0	1	1	1	1	0	?
0	1	0	1	1	1	0	1	0	?
1	0	0	1	0	0	0	1	0	?
1	1	1	1	0	1	1	1	0	?

- On voit les connecteurs comme des opérations.
- La valeur d'une expression se déduit *inductivement* de celle de ses sous-expressions.

$\rightsquigarrow$ Une distribution de valeurs de vérités $d : \mathcal{V}_p \to \mathbf{B}$ s'étend en une valuation de toutes les formules $A \in \mathcal{F}_p \mapsto d(A) \in \mathbf{B}$.

- A est une tautologie ssi $d(A) = 1$ pour toute dvv d.

Quelques tautologies

$$A \Rightarrow A \qquad (A \wedge B) \Rightarrow A \qquad A \Rightarrow (A \vee B)$$

$$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$$

$$A \vee (A \Rightarrow B) \qquad (\neg A) \vee A$$

$$\ldots$$

Priorités et associations

On donne les priorités

$$\{\neg\} > \{\wedge, \vee\} > \{\Rightarrow\} > \{\Leftrightarrow\}$$

donc on écrit par exemple

$$\neg A \vee B \Leftrightarrow A \Rightarrow B \quad = \quad ((\neg A) \vee B) \Leftrightarrow (A \Rightarrow B).$$

On note

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

donc on écrit par exemple

$$A \wedge B \wedge C \Rightarrow A \wedge B \Rightarrow B \wedge C \quad = \quad (A \wedge B) \wedge C \Rightarrow (A \wedge B \Rightarrow B \wedge C)$$

Quelques tautologies

$$A \Rightarrow A \qquad A \wedge B \Rightarrow A \qquad A \Rightarrow A \vee B$$

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow A \Rightarrow C$$

$$A \vee (A \Rightarrow B) \qquad \neg A \vee A$$

$$\ldots$$

Équivalence

On dit que A et B sont équivalentes ssi, pour toute dvv d, $d(A) = d(B)$:
on note $A \equiv B$.

Lemme

On a $A \equiv B$ ssi $A \Leftrightarrow B$ est une tautologie .

Démonstration: On a $d(A \Leftrightarrow B) = 1$ ssi $d(A) = d(B)$. □

Équivalences classiques

Le quotient $\mathcal{F}_p/\equiv$ est un treillis ...

$$
\begin{array}{ccc}
A \wedge B \equiv B \wedge A & (A \wedge B) \wedge C \equiv A \wedge (B \wedge C) & A \wedge (A \vee B) \equiv A \\
A \vee B \equiv B \vee A & (A \vee B) \vee C \equiv A \vee (B \vee C) & A \vee (A \wedge B) \equiv A
\end{array}
$$

$$
(\text{et donc :} \quad A \wedge A \equiv A \quad A \vee A \equiv A)
$$

... distributif ...

$$
A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) \quad A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)
$$

... borné et complémenté...

$$
A \wedge \top \equiv A \quad A \vee \bot \equiv A \quad A \wedge \neg A \equiv \bot \quad A \vee \neg A \equiv \top
$$

$$
(\text{et donc :} \quad A \wedge \bot \equiv \bot \quad A \vee \top \equiv \top)
$$

$\rightsquigarrow$ c'est une algèbre de Boole.

Équivalences classiques

Lois de De Morgan :

$$\neg\neg A \equiv A \quad \neg(A \wedge B) \equiv \neg A \vee \neg B \qquad \neg(A \vee B) \equiv \neg A \wedge \neg B$$
$$\neg\top \equiv \bot \qquad \neg\bot \equiv \top$$

Autour de l'implication :

$$A \Rightarrow B \equiv \neg A \vee B \equiv \neg B \Rightarrow \neg A$$
$$(A \wedge B) \Rightarrow C \equiv A \Rightarrow B \Rightarrow C$$
$$\neg(A \Rightarrow B) \equiv A \wedge \neg B$$
$$\neg A \equiv A \Rightarrow \bot$$

L'équivalence est une congruence

Autrement dit, elle est compatible avec les constructeurs de formules :

Lemme

Si $A \equiv A'$ et $B \equiv B'$ alors

$$\neg A \equiv \neg A', \quad A \wedge B \equiv A' \wedge B', \quad A \Rightarrow B \equiv A' \Rightarrow B', \ldots$$

Démonstration: Par exemple $A \wedge B \equiv A' \wedge B'$ car, pour toute dvv d,
$d(A \wedge B) = \min(d(A), d(B)) = \min(d(A'), d(B')) = d(A' \wedge B')$. $\square$

L'équivalence est une congruence

Autrement dit, elle est compatible avec les constructeurs de formules :

Lemme

Si $A \equiv A'$ et $B \equiv B'$ alors

$$\neg A \equiv \neg A', \quad A \wedge B \equiv A' \wedge B', \quad A \Rightarrow B \equiv A' \Rightarrow B', \ldots$$

Démonstration: Par exemple $A \wedge B \equiv A' \wedge B'$ car, pour toute dvv d, $d(A \wedge B) = \min(d(A), d(B)) = \min(d(A'), d(B')) = d(A' \wedge B')$. □

On peut donc établir la validité des formules *par le calcul* :

$$\begin{aligned}(A \Rightarrow B) \vee (B \Rightarrow C) &\equiv (\neg A \vee B) \vee (\neg B \vee C) \\ &\equiv \neg A \vee (B \vee \neg B) \vee C \\ &\equiv \neg A \vee \top \vee C \\ &\equiv \top\end{aligned}$$

En pratique. . .

Exercice 1

Jeux de connecteurs complets

Théorème

Toute formule propositionnelle est équivalente à une formule n'utilisant que les connecteurs $\wedge$ *et* $\neg$ *(ou* $\vee$ *et* $\neg$*, ou encore* $\Rightarrow$ *et* $\neg$*, ou* $\ldots$*).*

Démonstration: Par induction sur les formules. $\square$

Amusette : il y a des connecteurs qui sont complets à eux tous seuls.

Formes normales

Si on prend les connecteurs $\wedge$, $\vee$ et $\neg$, on peut *pousser les négations jusqu'aux atomes*.

Théorème

Toute formule propositionnelle est équivalente à une formule de la forme :

$$P, Q ::= X \mid \neg X \mid P \wedge Q \mid P \vee Q$$

Démonstration: Il suffit de vérifier (inductivement) que si P est de cette forme, alors $\neg P$ peut s'y ramener (par les lois de De Morgan). $\square$

On dit que P est une forme normale.

Clauses

- Un littéral est un atome X ou un atome nié $\neg X$.
- Une clause disjonctive est une forme normale sans $\wedge$:
  autrement dit, c'est une disjonction de littéraux.
  Ex : $X \vee \neg Y$.
- Une clause conjonctive est une forme normale sans $\vee$:
  autrement dit, c'est une conjonction de littéraux.
  Ex : $\neg X \wedge Y$.
- Il y a des formules qui ne sont équivalentes à aucune clause : par ex. $X \vee (Y \wedge Z)$.

Formes normales disjonctives (FND)

- Une forme normale disjonctive est une disjonction de clauses conjonctives.
  Ex : $X \vee (Y \wedge Z)$.

Théorème

Toute formule propositionnelle peut être mise en FND.

Démonstration: Par distributivité. □

Formes normales conjonctives (FNC)

- Une forme normale conjonctive est une conjonction de clauses disjonctives.
  Ex : $(X \vee Y) \wedge (X \vee Z)$.

Théorème

Toute formule propositionnelle peut être mise en FNC.

Démonstration: Par distributivité. $\square$

Formes normales conjonctives (FNC)

- Une forme normale conjonctive est une conjonction de clauses disjonctives.
  Ex : $(X \vee Y) \wedge (X \vee Z)$.

Théorème

Toute formule propositionnelle peut être mise en FNC.

Démonstration: Par distributivité. □

Ça peut faire grossir les formules : à quel point ?

Formes normales conjonctives (FNC)

- Une forme normale conjonctive est une conjonction de clauses disjonctives.
  Ex : $(X \vee Y) \wedge (X \vee Z)$.

Théorème

Toute formule propositionnelle peut être mise en FNC.

Démonstration: Par distributivité. □

Ça peut faire grossir les formules : à quel point ?

Vous reverrez ces formes normales en parlant du problème SAT.

Logique du premier ordre

$$\forall \epsilon > 0,\ \exists \delta > 0,\ \forall x(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon)$$

- On remplace les propositions indéterminées (les variables $X, Y, Z, \ldots$) par des propositions atomiques $R(t_1, \ldots, t_n)$ où :
  - $t_1, \ldots, t_n$ sont des termes représentant des éléments d'un ensemble (les individus) ;
  - R est un symbole de relation représentant une propriété vérifiée ou non suivant les valeurs de $t_1, \ldots, t_n$.
- Les termes sont des expressions construites à partir des variables d'individus par application de symboles de fonctions.
- On peut quantifier sur les individus : si A est une formule, alors $\forall x A$ et $\exists x A$ aussi.

Logique du premier ordre

$$\forall \epsilon \Big(\epsilon > 0 \Rightarrow \exists \delta \Big(\delta > 0 \wedge \forall x \big(|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon \big) \Big) \Big)$$

- On remplace les propositions indéterminées (les variables $X, Y, Z, \ldots$) par des propositions atomiques $R(t_1, \ldots, t_n)$ où :
  - $t_1, \ldots, t_n$ sont des termes représentant des éléments d'un ensemble (les individus) ;
  - R est un symbole de relation représentant une propriété vérifiée ou non suivant les valeurs de $t_1, \ldots, t_n$.
- Les termes sont des expressions construites à partir des variables d'individus par application de symboles de fonctions.
- On peut quantifier sur les individus : si A est une formule, alors $\forall x A$ et $\exists x A$ aussi.

Logique du premier ordre

$$\forall\epsilon\Big(C(0,\epsilon)\Rightarrow\exists\delta\Big(C(0,\delta)\wedge\forall x\big(C(a(m(x,x_0)),\delta)\Rightarrow C(a(m(f(x),f(x_0))),\epsilon)\big)\Big)\Big)$$

- On remplace les propositions indéterminées (les variables $X, Y, Z, \ldots$) par des propositions atomiques $R(t_1, \ldots, t_n)$ où :
  - $t_1, \ldots, t_n$ sont des termes représentant des éléments d'un ensemble (les individus) ;
  - R est un symbole de relation représentant une propriété vérifiée ou non suivant les valeurs de $t_1, \ldots, t_n$.
- Les termes sont des expressions construites à partir des variables d'individus par application de symboles de fonctions.
- On peut quantifier sur les individus : si A est une formule, alors $\forall xA$ et $\exists xA$ aussi.

Logique du premier ordre

$$\forall\epsilon\Big(C(0,\epsilon)\Rightarrow\exists\delta\Big(C(0,\delta)\wedge\forall x\big(C(a(m(x,x_0)),\delta)\Rightarrow C(a(m(f(x),f(x_0))),\epsilon)\big)\Big)\Big)$$

- On remplace les propositions indéterminées (les variables $X, Y, Z, \ldots$) par des propositions atomiques $R(t_1, \ldots, t_n)$ où :
  - $t_1, \ldots, t_n$ sont des termes représentant des éléments d'un ensemble (les individus) ;
  - R est un symbole de relation représentant une propriété vérifiée ou non suivant les valeurs de $t_1, \ldots, t_n$.
- Les termes sont des expressions construites à partir des variables d'individus par application de symboles de fonctions.
- On peut quantifier sur les individus : si A est une formule, alors $\forall x A$ et $\exists x A$ aussi.
- La vérité d'une formule dépend :
  - de la structure dans laquelle on l'interprète ;
  - de la valeur des variables d'individus (l'environnement) qui y apparaissent librement.

Termes

- On fixe un ensemble $\mathcal{V}$ (infini, dénombrable) de variables d'individus, notées $x, y, \ldots$
- On se donne une signature $\mathcal{F}$ de symboles de fonctions.

Définition

L'ensemble $\mathcal{T}_{\mathcal{F}}$ des termes sur la signature $\mathcal{F}$ est le plus petit ensemble contenant $\mathcal{V}$ et clos par application des symboles de fonctions, en respectant l'arité :

$$\mathcal{T}_{\Sigma} \ni s, t, u, \ldots ::= x \mid f(s_1, \ldots, s_{a(f)})$$

$$(x \in \mathcal{V},\ f \in \mathcal{F})$$

Termes

- On fixe un ensemble $\mathcal{V}$ (infini, dénombrable) de variables d'individus, notées $x, y, \ldots$
- On se donne une signature $\mathcal{F}$ de symboles de fonctions.

Définition

L'ensemble $\mathcal{T}_{\mathcal{F}}$ des termes sur la signature $\mathcal{F}$ est le plus petit ensemble contenant $\mathcal{V}$ et clos par application des symboles de fonctions, en respectant l'arité :

$$\mathcal{T}_{\Sigma} \ni s, t, u, \ldots ::= x \mid f(s_1, \ldots, s_{a(f)})$$

$$(x \in \mathcal{V},\ f \in \mathcal{F})$$

En bref : un terme = une expression.

Exemple

Avec $f, g \in \mathcal{F}$, $a_{\mathcal{F}}(f) = 2$ et $a_{\mathcal{F}}(g) = 0$: $f(x, y)$ et $g() \in \mathcal{T}_{\mathcal{F}}$.

Termes

- On fixe un ensemble $\mathcal{V}$ (infini, dénombrable) de variables d'individus, notées $x, y, \ldots$
- On se donne une signature $\mathcal{F}$ de symboles de fonctions.

Définition

L'ensemble $\mathcal{T}_{\mathcal{F}}$ des termes sur la signature $\mathcal{F}$ est le plus petit ensemble contenant $\mathcal{V}$ et clos par application des symboles de fonctions, en respectant l'arité :

$$\mathcal{T}_{\Sigma} \ni s, t, u, \ldots ::= x \mid f(s_1, \ldots, s_{a(f)})$$

$$(x \in \mathcal{V},\ f \in \mathcal{F})$$

En bref : un terme = une expression.

Exemple

Avec $+, 0 \in \mathcal{F}_{\mathcal{F}}$, $a_{\mathcal{F}}(+) = 2$ et $a_{\mathcal{F}}(0) = 0$: $+(x, y)$ et $0() \in \mathcal{T}_{\mathcal{F}}$.

Termes

- On fixe un ensemble $\mathcal{V}$ (infini, dénombrable) de variables d'individus, notées $x, y, \ldots$
- On se donne une signature $\mathcal{F}$ de symboles de fonctions.

Définition

L'ensemble $\mathcal{T}_{\mathcal{F}}$ des termes sur la signature $\mathcal{F}$ est le plus petit ensemble contenant $\mathcal{V}$ et clos par application des symboles de fonctions, en respectant l'arité :

$$\mathcal{T}_{\Sigma} \ni s, t, u, \ldots ::= x \mid f(s_1, \ldots, s_{a(f)})$$

$$(x \in \mathcal{V},\ f \in \mathcal{F})$$

En bref : un terme = une expression.

Exemple

Avec $+, 0 \in \mathcal{F}_{\mathcal{F}}$, $a_{\mathcal{F}}(+) = 2$ et $a_{\mathcal{F}}(0) = 0$: $x + y$ et $0 \in \mathcal{T}_{\mathcal{F}}$.

Formules du premier ordre (= prédicats)

On étend la signature avec un ensemble de symboles de relations : $\Sigma = (\mathcal{F}, \mathcal{R}, a)$.

Définition

L'ensemble $\mathcal{F}_\Sigma$ des formules sur la signature Σ est l'ensemble d'expressions défini par :

$$\mathcal{F}_\Sigma \ni A, B, \ldots \ ::= \ R(t_1, \ldots, t_{a(R)}) \mid A \wedge B \mid \neg A \mid \cdots \mid \forall x A \mid \exists x A$$

$$(R \in \mathcal{R},\ t_1, \ldots, t_{a(R)} \in \mathcal{T}_\Sigma = \mathcal{T}_\mathcal{F})$$

Une formule = une expression construite par application des connecteurs et quantificateurs, à partir des formules atomiques $R(t_1, \ldots, t_n)$.

Formules du premier ordre (= prédicats)

On étend la signature avec un ensemble de symboles de relations : $\Sigma = (\mathcal{F}, \mathcal{R}, a)$.

Définition

L'ensemble $\mathcal{F}_\Sigma$ des formules sur la signature Σ est l'ensemble d'expressions défini par :

$$\mathcal{F}_\Sigma \ni A, B, \dots \quad ::= \quad R(t_1, \dots, t_{a(R)}) \mid A \wedge B \mid \neg A \mid \cdots \mid \forall x A \mid \exists x A$$

$$(R \in \mathcal{R},\ t_1, \dots, t_{a(R)} \in \mathcal{T}_\Sigma = \mathcal{T}_\mathcal{F})$$

Une formule = une expression construite par application des connecteurs et quantificateurs, à partir des formules atomiques $R(t_1, \dots, t_n)$.

Exemple

En ajoutant $R \in \mathcal{R}$ avec $a(R) = 2$: $\exists y R(x + y, 0) \in \mathcal{F}$.

Formules du premier ordre (= prédicats)

On étend la signature avec un ensemble de symboles de relations : $\Sigma = (\mathcal{F}, \mathcal{R}, a)$.

Définition

L'ensemble $\mathcal{F}_\Sigma$ des formules sur la signature Σ est l'ensemble d'expressions défini par :

$$\mathcal{F}_\Sigma \ni A, B, \ldots \ ::= \ R(t_1, \ldots, t_{a(R)}) \mid A \wedge B \mid \neg A \mid \cdots \mid \forall x A \mid \exists x A$$

$$(R \in \mathcal{R},\ t_1, \ldots, t_{a(R)} \in \mathcal{T}_\Sigma = \mathcal{T}_\mathcal{F})$$

Une formule = une expression construite par application des connecteurs et quantificateurs, à partir des formules atomiques $R(t_1, \ldots, t_n)$.

Exemple

En ajoutant $= \in \mathcal{R}$ avec $a(=) = 2$: $\exists y\, x + y = 0 \in \mathcal{F}$.

Formules du premier ordre (= prédicats)

On étend la signature avec un ensemble de symboles de relations : $\Sigma = (\mathcal{F}, \mathcal{R}, a)$.

Définition

L'ensemble $\mathcal{F}_\Sigma$ des formules sur la signature Σ est l'ensemble d'expressions défini par :

$$\mathcal{F}_\Sigma \ni A, B, \ldots \ ::= \ R(t_1, \ldots, t_{a(R)}) \mid A \wedge B \mid \neg A \mid \cdots \mid \forall x A \mid \exists x A$$

$$(R \in \mathcal{R},\ t_1, \ldots, t_{a(R)} \in \mathcal{T}_\Sigma = \mathcal{T}_\mathcal{F})$$

Une formule = une expression construite par application des connecteurs et quantificateurs, à partir des formules atomiques $R(t_1, \ldots, t_n)$.

On obtient (à peu près) le calcul propositionnel comme cas particulier :
$\mathcal{F} = \emptyset$, $\mathcal{R} = \mathcal{V}_p$ et $a(X) = 0$ pour tout $X \in \mathcal{V}_p$.

Interprétations

Définition

Une interprétation (ou structure) $\mathcal{I}$ de Σ est la donnée de :

- un ensemble *non vide* $|\mathcal{I}|$;
- pour chaque symbole de fonction $f \in \mathcal{F}_\Sigma$, une fonction $f_\mathcal{I} : |\mathcal{I}|^{a_\Sigma(f)} \to |\mathcal{I}|$;
- pour chaque symbole de relation $R \in \mathcal{R}_\Sigma$, une partie $R_\mathcal{I} \subset \mathcal{I}^{a_\Sigma(R)}$.

N.B. : Quand Σ contient le symbole d'égalité, on exige que $=_\mathcal{I} = \{(a, a); a \in |\mathcal{I}|\}$.

Interprétations

Définition

Une interprétation (ou structure) $\mathcal{I}$ de Σ est la donnée de :

- un ensemble *non vide* $|\mathcal{I}|$;
- pour chaque symbole de fonction $f \in \mathcal{F}_\Sigma$, une fonction $f_\mathcal{I} : |\mathcal{I}|^{a_\Sigma(f)} \to |\mathcal{I}|$;
- pour chaque symbole de relation $R \in \mathcal{R}_\Sigma$, une partie $R_\mathcal{I} \subset \mathcal{I}^{a_\Sigma(R)}$.

N.B. : Quand Σ contient le symbole d'égalité, on exige que $=_\mathcal{I} = \{(a,a); a \in |\mathcal{I}|\}$.

Exemple

Avec $\mathcal{F} = \{+, 0\}$ et $\mathcal{R} = \{=\}$, on peut considérer :

- $|\mathcal{N}| = \mathbf{N}$ avec les opérations usuelles ;
- $|\mathcal{Z}| = \mathbf{Z}$ avec les opérations usuelles ;
- $|\mathcal{Z}_2| = \{0, 1\}$ vu comme $\mathbf{Z}/2\mathbf{Z}$;
- $|\mathcal{B}| = \{0, 1\}$, avec $+ = \max$;

mais aussi $|\mathcal{I}| = \mathbf{N}$ avec $p +_\mathcal{I} q = 3p + 1$ et $0_\mathcal{I} = 42$.

Environnements et valeurs

- La valeur $[\![t]\!]_{\mathcal{I}}$ d'un terme t se calcule inductivement :

$$[\![f(t_1,\dots,t_n)]\!]_{\mathcal{I}} = f_{\mathcal{I}}([\![t_1]\!]_{\mathcal{I}},\dots,[\![t_n]\!]_{\mathcal{I}})$$

Environnements et valeurs

- La valeur $[\![t]\!]_{\mathcal{I}}$ d'un terme t se calcule inductivement :

$$[\![f(t_1, \ldots, t_n)]\!]_{\mathcal{I}} = f_{\mathcal{I}}([\![t_1]\!]_{\mathcal{I}}, \ldots, [\![t_n]\!]_{\mathcal{I}})$$
$$[\![x]\!]_{\mathcal{I}} = ?$$

Environnements et valeurs

- Un environnement est une fonction $e : \mathcal{V} \to |\mathcal{I}|$.
- La valeur $[\![t]\!]_{\mathcal{I},e}$ d'un terme t dans l'environnement e se calcule inductivement :

$$[\![f(t_1, \ldots, t_n)]\!]_{\mathcal{I},e} = f_{\mathcal{I}}([\![t_1]\!]_{\mathcal{I},e}, \ldots, [\![t_n]\!]_{\mathcal{I},e})$$
$$[\![x]\!]_{\mathcal{I},e} = e(x)$$

Environnements et valeurs

- Un environnement est une fonction $e : \mathcal{V} \to |\mathcal{I}|$.
- La valeur $[\![t]\!]_{\mathcal{I},e}$ d'un terme t dans l'environnement e se calcule inductivement :

$$\begin{aligned}[\![f(t_1, \dots, t_n)]\!]_{\mathcal{I},e} &= f_{\mathcal{I}}([\![t_1]\!]_{\mathcal{I},e}, \dots, [\![t_n]\!]_{\mathcal{I},e}) \\ [\![x]\!]_{\mathcal{I},e} &= e(x)\end{aligned}$$

- La valeur d'une formule atomique s'en déduit :

$$[\![R(t_1, \dots, t_n)]\!]_{\mathcal{I},e} = \begin{cases} 1 & \text{si } ([\![t_1]\!]_{\mathcal{I},e}, \dots, [\![t_n]\!]_{\mathcal{I},e}) \in R_{\mathcal{I}} \\ 0 & \text{sinon} \end{cases}$$

Vérité en calcul des prédicats

On obtient inductivement une valeur pour toute formule par les tables de vérité et :

$$[\![\forall x A]\!]_{\mathcal{I},e} = \begin{cases} 1 & \text{si } [\![A]\!]_{\mathcal{I},e[a/x]} = 1 \text{ pour tout } a \in |\mathcal{I}| \\ 0 & \text{sinon} \end{cases}$$

$$[\![\exists x A]\!]_{\mathcal{I},e} = \begin{cases} 1 & \text{s'il existe } a \in |\mathcal{I}| \text{ tel que } [\![A]\!]_{\mathcal{I},e[a/x]} = 1 \\ 0 & \text{sinon} \end{cases}$$

où $e[a/x](y) = a$ si $y = x$ et $e[a/x](y) = e(y)$ sinon.
On note $\mathcal{I}, e \models A$ ssi $[\![A]\!]_{\mathcal{I},e} = 1$: A est valide pour $(\mathcal{I}, e)$.

Vérité en calcul des prédicats

On obtient inductivement une valeur pour toute formule par les tables de vérité et :

$$[\![\forall x A]\!]_{\mathcal{I},e} = \begin{cases} 1 & \text{si } [\![A]\!]_{\mathcal{I},e[a/x]} = 1 \text{ pour tout } a \in |\mathcal{I}| \\ 0 & \text{sinon} \end{cases}$$

$$[\![\exists x A]\!]_{\mathcal{I},e} = \begin{cases} 1 & \text{s'il existe } a \in |\mathcal{I}| \text{ tel que } [\![A]\!]_{\mathcal{I},e[a/x]} = 1 \\ 0 & \text{sinon} \end{cases}$$

où $e[a/x](y) = a$ si $y = x$ et $e[a/x](y) = e(y)$ sinon.
On note $\mathcal{I}, e \models A$ ssi $[\![A]\!]_{\mathcal{I},e} = 1$: A est valide pour $(\mathcal{I}, e)$.

Exemple (Avec $A = \exists y x + y = 0$)

- $\mathcal{N}, e \models A$ ssi $e(x) = 0$;
- $\mathcal{Z}, e \models A$ toujours ;
- $\mathcal{Z}_2, e \models A$ toujours ;
- $\mathcal{B}, e \models A$ ssi $e(x) = 0$;
- $\mathcal{I}, e \models A$ ssi $3e(x) + 1 = 42$ (donc jamais).

Vérité et équivalence

- On note $\mathcal{I} \models A$ ssi $\mathcal{I}, e \models A$ pour tout environnement e : $\mathcal{I}$ valide A.
- Une tautologie sur Σ est une formule A valide dans toute interprétation : on note $\models A$.
- On note $A \equiv B$ et on dit que A et B sont équivalentes si : pour toute interprétation $\mathcal{I}$ et tout environnement e, $[\![A]\!]_{\mathcal{I},e} = [\![B]\!]_{\mathcal{I},e}$.

Lemme

$A \equiv B$ ssi $\models A \Leftrightarrow B$.

Démonstration: $[\![A]\!]_{\mathcal{I},e} = [\![B]\!]_{\mathcal{I},e}$ ssi $\mathcal{I}, e \models A \Leftrightarrow B$. $\square$

Quelques vérités et équivalences

Priorités : $\{\forall x, \exists x\} < \cdots$

$$\neg\forall xA \equiv \exists x\neg A \qquad \neg\exists xA \equiv \forall x\neg A$$

$$\forall xA \wedge B \equiv (\forall xA) \wedge (\forall xB) \qquad \exists xA \vee B \equiv (\exists xA) \vee (\exists xB)$$

$$(\forall xA) \Rightarrow A[t/x] \qquad A[t/x] \Rightarrow (\exists xA) \qquad (\forall xA) \Rightarrow (\exists xA)$$

$$\exists x\forall yA[x/z] \Rightarrow A[y/z]$$

$$\cdots$$

Quelques vérités et équivalences

Priorités : $\{\forall x, \exists x\} < \cdots$

$$\neg\forall xA \equiv \exists x\neg A \qquad \neg\exists xA \equiv \forall x\neg A$$

$$\forall xA \wedge B \equiv (\forall xA) \wedge (\forall xB) \qquad \exists xA \vee B \equiv (\exists xA) \vee (\exists xB)$$

$$(\forall xA) \Rightarrow A[t/x] \qquad A[t/x] \Rightarrow (\exists xA) \qquad (\forall xA) \Rightarrow (\exists xA)$$

$$\exists x\forall yA[x/z] \Rightarrow A[y/z]$$

$$\cdots$$

où $A[t/x]$ dénote la substitution par le terme t de toutes les occurrences *libres* de x (quitte à renommer les variables liées pour éviter les confusions).

Substitution

Soit $A = (\exists y\, x + y = 0)$:

$$\begin{aligned} A[0/x] &= (\exists y\, 0 + y = 0) \\ A[z + 0/x] &= (\exists y\, (z + 0) + y = 0) \\ A[0/y] &= A \\ A[y/x] &= (\exists y\, y + y = 0) \end{aligned}$$

Substitution

Soit $A = (\exists y\, x + y = 0)$:

$$A[0/x] = (\exists y\, 0 + y = 0)$$

$$A[z + 0/x] = (\exists y\, (z + 0) + y = 0)$$

$$A[0/y] = A \qquad \text{(et pas } \exists y\, x + 0 = 0\,!\text{)}$$

$$A[y/x] = (\exists y\, y + y = 0)$$

Substitution

Soit $A = (\exists y\, x + y = 0)$:

$$A[0/x] = (\exists y\, 0 + y = 0)$$

$$A[z + 0/x] = (\exists y\, (z + 0) + y = 0)$$

$$A[0/y] = A \qquad \text{(et pas } \exists y\, x + 0 = 0\,!\text{)}$$

$$A[y/x] = \cancel{(\exists y\, y + y = 0)} \qquad \text{NON !}$$

Substitution

Soit $A = (\exists y\, x + y = 0)$:

$$\begin{aligned} A[0/x] &= (\exists y\, 0 + y = 0) \\ A[z+0/x] &= (\exists y\, (z+0) + y = 0) \\ A[0/y] &= A && \text{(et pas } \exists y\, x + 0 = 0\,!) \\ A[y/x] &= \cancel{(\exists y\, y + y = 0)} && \text{NON !} \end{aligned}$$

- Les occurrences de x dans A sont liées dans $\forall x A$ et $\exists x A$.

  On dit aussi "variable muette", *cf.* $\sum_{i=0}^{n} x^i$, $\int_{x \in I} f(x)dx$, …

- On considère les formules modulo le renommage des variables liées, *sans confusion* : ici, $A = (\exists y'\, x + y' = 0)$.

Substitution

Soit $A = (\exists y\, x + y = 0)$:

$$\begin{aligned} A[0/x] &= (\exists y\, 0 + y = 0) \\ A[z+0/x] &= (\exists y\, (z+0) + y = 0) \\ A[0/y] &= A && \text{(et pas } \exists y\, x + 0 = 0\,!\text{)} \\ A[y/x] &= \cancel{(\exists y\, y + y = 0)} && \text{NON !} \\ A[y/x] &= (\exists y'\, y + y' = 0) \end{aligned}$$

- Les occurrences de x dans A sont liées dans $\forall x A$ et $\exists x A$.
  On dit aussi "variable muette", *cf.* $\sum_{i=0}^{n} x^i$, $\int_{x \in I} f(x)dx$, ...
- On considère les formules modulo le renommage des variables liées, *sans confusion* : ici, $A = (\exists y'\, x + y' = 0)$.

Substitution

Soit $A = (\exists y\, x + y = 0)$:

$$
\begin{aligned}
A[0/x] &= (\exists y\, 0 + y = 0) \\
A[z + 0/x] &= (\exists y\, (z + 0) + y = 0) \\
A[0/y] &= A & \text{(et pas } \exists y\, x + 0 = 0\,!) \\
A[y/x] &= \cancel{(\exists y\, y + y = 0)} & \text{NON !} \\
A[y/x] &= (\exists y'\, y + y' = 0)
\end{aligned}
$$

- Les occurrences de x dans A sont liées dans $\forall x A$ et $\exists x A$.
  On dit aussi "variable muette", *cf.* $\sum_{i=0}^{n} x^i$, $\int_{x \in I} f(x)dx$, ...
- On considère les formules modulo le renommage des variables liées, *sans confusion* : ici, $A = (\exists y'\, x + y' = 0)$.

Lemme

On a $[\![t[u/x]]\!]_{\mathcal{I},e} = [\![t]\!]_{\mathcal{I},e[[\![u]\!]_{\mathcal{I},e}/x]}$ *et* $[\![A[u/x]]\!]_{\mathcal{I},e} = [\![A]\!]_{\mathcal{I},e[[\![u]\!]_{\mathcal{I},e}/x]}$.

Variables libres

- Une occurrence de x qui n'est pas liée dans A est dite libre dans A.
- Si les variables libres de A sont parmi $x_1, \dots, x_n$, on note parfois $A[x_1, \dots, x_n]$ pour marquer cette dépendance, et alors $A[t_1, \dots, t_n] \coloneqq A[x_1 \coloneqq t_1, \dots, x_n \coloneqq t_n]$.
- On note $\mathrm{VL}(A)$ l'ensemble des variables libres de A.
- Si $\mathrm{VL}(A) = \emptyset$, on dit que A est une formule close.

Lemme

Si $x \notin \mathrm{VL}(A)$ alors $[\![A]\!]_{\mathcal{I},e}$ ne dépend pas de la valeur de e en x.

En particulier, si A est close alors : pour toute interprétation $\mathcal{I}$, on a $\mathcal{I} \models A$ ou $\mathcal{I} \models \neg A$.

Convention

Sauf si c'est explicitement écrit, on suppose toujours qu'aucune variable n'apparait à la fois libre et liée dans une formule (et on peut toujours se ramener à ce cas par renommage) : quand on écrit $A \Rightarrow \forall x.B$, on sous-entend que x n'est pas libre dans A.

En pratique. . .

Exercices