Cours 7 et 8

Calcul des prédicats

Motivations

Le calcul propositionnel n'est pas suffisamment expressif pour raisonner sur les structures mathématiques usuelles.

Exemple de structure mathématique : les groupes

- un ensemble A (non vide)
- un élément distingué e (le neutre)
- une fonction unaire i (inverse)
- une fonction binaire o (loi interne)
- un prédicat binaire E (égalité)
- des règles de base (axiomes)

$$\begin{array}{l} \forall x \ \ (E(o(x,e),x) \wedge E(o(e,x),x)) \\ \forall x \ \ (E(o(i(x),x),e) \wedge E(o(x,i(x)),e)) \\ \forall x \forall y \forall z \ E(o(x,o(y,z)),o(o(x,y),z)) \\ \ldots \end{array}$$

Logique du 1^{er} ordre : les ingrédients

Désigner les objets

- variables,
- constantes (ex : e),
- fonctions appliquées à d'autres objets (ex : i et o)

Construire des formules

- prédicats (ex : E),
- connecteurs propositionnels ($\wedge, \vee, \Rightarrow, \neg, \Longleftrightarrow$),
- quantificateurs ($\forall, \exists$)

La limitation du 1^{er} ordre : on ne quantifie que sur les objets.

Un exemple de quantification du second ordre : les treillis complets

- un ensemble A (non vide)
- prédicats binaires = et $\sqsubseteq$

$$\begin{array}{ll}
\forall x,\ x \sqsubseteq x & \text{(réflexivité)} \\
\forall x \forall y\ x \sqsubseteq y\ \wedge\ y \sqsubseteq x\ \Rightarrow\ x = y & \text{(antisymétrie)} \\
\forall x \forall y \forall z\ x \sqsubseteq y\ \wedge\ y \sqsubseteq z\ \Rightarrow\ x \sqsubseteq z & \text{(transitivité)}
\end{array}$$

- existence d'une borne supérieure

Pour tout sous-ensemble B de A, si B est non vide, il existe un plus petit majorant

$$\forall \mathbf{B}\ \ (\exists x\ B(x)) \Rightarrow \exists m$$
$$((\forall a\ B(a) \Rightarrow a \sqsubseteq m) \wedge (\forall b\ (\forall a,\ B(a) \Rightarrow a \sqsubseteq b) \Rightarrow m \sqsubseteq b))$$

Syntaxe

Langage du premier ordre

Définition

Un *langage du premier ordre* est un ensemble L de symboles qui se compose de deux parties

- la première, commune à tous les langages
  - un ensemble infini dénombrable de symboles de variables $\mathbb{V} = \{v_1, v_2, \ldots\}$
  - $(,), \wedge, \vee, \neg, \Rightarrow, \Longleftrightarrow$ + deux symboles de quantificateurs $\forall$ et $\exists$
- La seconde, spécifique au langage
  - un ensemble $\mathcal{C}$ de symboles de constantes
  - deux suites $(\mathcal{F}_n)_{n\in\mathbb{N}^*}$ et $(\mathcal{R}_n)_{n\in\mathbb{N}^*}$ d'ensembles (deux à deux disjoints et disjoints de $\mathcal{C}$)
    pour chaque n,

    $\mathcal{F}_n$: symboles de fonctions à n places (ou d'arité n)

    $\mathcal{R}_n$: symboles de prédicats (ou relations) à n places

Le symbole = de relation binaire (arité 2) joue un rôle particulier

- on parle de langage égalitaire

En pratique, on considère un petit nombre de symboles et de constantes, fonctions et prédicats : pour définir un langage, on donne la liste de ceux-ci.

Exemple :

$$\mathcal{F} = \{c : 0,\ f : 1,\ \circ : 2,\ \bullet : 2\} \qquad P = \{z : 1,\ =: 2\}$$

$$L = \{v_1, v_2, \ldots\} \cup \{(,), \wedge, \vee, \neg, \Rightarrow, \Longleftrightarrow, \forall, \exists\} \cup \{c, f, \circ, \bullet, z, =\}$$

Quelques mots sur L^* :

- $z(c) \wedge \forall x \forall y\, (f(x \circ y) = f(x) \bullet f(y))$
- $))y(f\bullet)x(f\ =)y \circ x(f(y\forall x\forall\wedge)c(z$

Désigner les objets : termes

Définition

L'ensemble $\mathcal{T}(L) \subseteq L^*$ des *termes* de L est défini inductivement par

- $\mathbb{V} \subseteq \mathcal{T}(L)$
- $\mathcal{C} \subseteq \mathcal{T}(L)$
- pour chaque entier $n \geqslant 1$, et chaque $f \in \mathcal{F}_n$, $\mathcal{T}(L)$ est stable pour l'opération $(t_1, .., t_n) \mapsto ft_1 \dots t_n$.

Remarque : on se passe de parenthèses et de virgules.

Définition explicite

On pose

- $\mathcal{T}_0(L) = \mathcal{C} \cup \mathbb{V}$
- pour tout $k \in \mathbb{N}$,
$\mathcal{T}_{k+1}(L) = \mathcal{T}_k(L) \cup \bigcup_{n \in \mathbb{N}^*} \{ft_1..t_n \mid f \in \mathcal{F}_n, t_1, .., t_n \in \mathcal{T}_k(L)\}$

Lemme

$$\mathcal{T}(L) = \bigcup_{n \in N} \mathcal{T}_k(L)$$

La *hauteur* d'un terme $t \in \mathcal{T}(L)$ est le plus petit entier k tel que $t \in \mathcal{T}_k(L)$.

Décomposition unique

La définition inductive de $\mathcal{T}(L)$ est non ambiguë

Théorème

Pour tout terme $t \in \mathcal{T}(L)$, un et un seul des cas suivants se présente :

- *t est une variable de L,*
- *t est un symbole de constante de $\mathcal{C}$,*
- *il existe un unique $k \geqslant 1$, un unique symbole de fonction k-aire f et un unique k-uplet de termes $t_1, \ldots, t_k$ tels que $t = ft_1..t_k$.*

Exemple : $\mathcal{F} = \{c : 0,\ f : 1,\ g : 2\}$

$$ggffv0gv_2v_0cfcffgfcgv_2fv_0ffcfcfc$$

Variable libres d'un terme

Définition inductive :

$$\begin{array}{rcl} \mathrm{VL}(v) & = & \{v\} \\ \mathrm{VL}(c) & = & \emptyset \\ \mathrm{VL}(ft_1 \ldots t_n) & = & \mathrm{VL}(t_1) \cup \cdots \cup \mathrm{VL}(t_n) \end{array}$$

Définition

Un terme sans variables libres est appelé *terme clos*.

On notera $t[v_{i_1}, \ldots, v_{i_n}]$ (ou $i_1, \ldots, i_n$ sont 2 à 2 distincts) pour indiquer que $\mathrm{VL}(t) \subseteq \{v_{i_1}, \ldots, v_{i_n}\}$.

Substitution de termes

Définition

Soient $k \in \mathbb{N}$, $w_1, \ldots, w_k$ variables 2 à 2 distincts, t, $u_1, \ldots, u_k$ termes. La substitution $t[u_1/w_1, \ldots, u_k/w_k]$ des termes $u_1, \ldots, u_k$ aux variables $w_1, \ldots, w_k$ est définie par induction sur t :

- si t est un symbole de constante ou de variable différent de $w_1, \ldots, w_k$, alors $t[u_1/w_1, \ldots, u_k/w_k] = t$
- si $t = w_i$, $t[u_1/w_1, \ldots, u_k/w_k] = u_i$
- si $t = ft_1 \ldots t_n$, alors

$$t[u_1/w_1, \ldots, u_k/w_k] = ft_1[u_1/w_1, \ldots, u_k/w_k] \ldots t_n[u_1/w_1, \ldots, u_k/w_k]$$

Remarques :

- C'est bien un terme.
- Ce n'est pas équivalent à une composition de substitution.

Formules

Définition

Un mot $m \in \mathcal{L}^*$ est une *formule atomique* si il existe $n \in \mathbb{N}^*$, $R \in \mathcal{R}_n$ et n termes $t_1, \ldots, t_n$ tels que $m = Rt_1 \cdots t_n$

Si L est égalitaire, on notera $t = u$ à la place de $= tu$.

Définition

L'ensemble $\mathcal{F}(L) \subseteq L^*$ des *formules du 1^er^ ordre* est définie inductivement par :

- $\mathcal{F}(L)$ contient les formules atomiques
- si $F \in \mathcal{F}(L)$ et $G \in \mathcal{F}(L)$, alors $\neg F \in \mathcal{F}(L)$, $(F \wedge G) \in \mathcal{F}(L)$, $(F \vee G) \in \mathcal{F}(L)$, $(F \Rightarrow G) \in \mathcal{F}(L)$, $(F \iff G) \in \mathcal{F}(L)$ et pour tout $k \in N$, $\exists v_k F \in \mathcal{F}(L)$ et $\forall v_k F \in \mathcal{F}(L)$.

Définition explicite

$$
\begin{array}{rcl}
\mathcal{F}_0(L) & = & \{Rt_1 \cdots t_n \mid R \in \mathcal{R}_n \text{ et } t_1, \ldots, t_n \in \mathcal{T}(L)\} \\
\mathcal{F}_{n+1}(L) & = & F_n(L) \; \cup\{\neg F \mid F \in \mathcal{F}_n(L)\} \\
 & & \qquad\quad \cup\{(F \bowtie G) \mid F, G \in \mathcal{F}_n(L),\; \bowtie \in \{\wedge, \vee, \Rightarrow, \Longleftrightarrow\}\} \\
 & & \qquad\quad \cup\{\forall v F \mid F \in \mathcal{F}_n(L), v \in \mathbb{V}\} \\
 & & \qquad\quad \cup\{\exists v F \mid F \in \mathcal{F}_n(L), v \in \mathbb{V}\}
\end{array}
$$

Lemme

$$\mathcal{F}(L) = \bigcup_{n \in N} \mathcal{F}_n(L)$$

La *hauteur* d'une formule $F \in \mathcal{F}(L)$ est le plus petit entier k tel que $F \in \mathcal{F}_k(L)$.

Décomposition unique

Théorème

La définition inductive de $\mathcal{F}(L)$ est non-ambiguë.

Variable libres

Les variables libres d'une formules sont définie de manière inductive

$$\begin{aligned} \mathrm{VL}(Rt_1 \cdots t_n) &= \\ \mathrm{VL}(\neg F) &= \\ \mathrm{VL}((F \bowtie G)) &= \\ \mathrm{VL}(\forall v F) &= \\ \mathrm{VL}(\exists v F) &= \end{aligned}$$

Définitions et notations :

- On appelle *formule close* une formule sans variable libre.
- On note $F[v_{i_1}, \ldots, v_{i_n}]$ quand $\mathrm{VL}(F) \subseteq \{v_{i_1}, \ldots, v_{i_n}\}$.
- Si $F = F[v_{i_1}, \ldots, v_{i_n}]$, une *clôture universelle* est $\forall v_{i_1} \ldots \forall v_{i_n} F$

Substitution dans les formules

On souhaite substituer de termes à des occurrences **libres** de variables. définition par induction sur les formules.

Définition

La substitution $F[t/v]$ du termes t à la variable v dans la formule F est définie par induction sur F :

$$\begin{aligned} \mathrm{VL}(Rt_1 \cdots t_n) &= \\ \mathrm{VL}(\neg F) &= \\ \mathrm{VL}((F \bowtie G)) &= \\ \mathrm{VL}(\forall v F) &= \mathrm{VL}(\exists v F) = \end{aligned}$$

Remarque : on peut définir de manière similaire la substitution simultanée.

Cas particulier : changement de nom de variable liée

Définition

Étant donné une formule F de la forme $\Box v G$ avec $\Box \in \{\forall, \exists\}$, le *renommage de v par w* est

$$\Box w F[w/v]$$

Cette transformation est utile pour éviter la capture de variable lors d'une substitution sous un quantificateur.

Sémantique

Sémantique

But : Interpréter les objets et donner un sens aux formules. En maths, une structure est un ensemble muni d'opérations et de relations avec éventuellement des éléments distingués.

Définition

Une *structure* (réalisation) $\mathcal{M}$ pour un langage L est la donnée de :

- un ensemble M non vide (dit ensemble de base, domaine),
- un élément $c^{\mathcal{M}}$ de M pour chaque symbole de constante $c \in \mathcal{C}$,
- pour chaque arité $k \geqslant 1$ et chaque symbole f de fonction d'arité k, une application $f^{\mathcal{M}}$ de M^k dans M,
- pour chaque entier $k \geqslant 1$ et chaque symbole de prédicat R d'arité k, un sous-ensemble $R^{\mathcal{M}}$ de M^k.

Exemple

Donner un exemple de structure pour le langage définie par

$$\mathcal{F} = \{c : 0,\ f : 1,\ \circ : 2,\ \bullet : 2\} \qquad P = \{z : 1,\ =: 2\}$$

Interprétation d'un terme

L'interprétation d'un terme dépend des valeurs que l'on donne au variables.

Une valuation est une fonction $\mathbb{V} \to M$ avec M le domaine de la structure.

Notation : pour $\rho \in \mathbb{V} \to M$, $v \in \mathbb{V}$ et $d \in M$, la valuation $\rho[v \mapsto d]$ est définie par

$$\rho[x \mapsto d](y) = \begin{cases} d & \text{si } x = y \\ \rho(y) & \text{si } x \neq y \end{cases}$$

Interprétation d'un terme

Définition

L'interprétation du terme t dans la structure $\mathcal{M}$ par rapport à une valuation $\rho \in \mathbb{V} \to M$, notée $[\![t]\!]_\rho^\mathcal{M}$ est définie par induction sur t :

- si $t = v \in \mathbb{V}$, $[\![t]\!]_\rho^\mathcal{M} = \rho(v)$
- si $t = c \in \mathcal{C}$, $[\![t]\!]_\rho^\mathcal{M} = c^\mathcal{M}$
- si $t = ft_1..t_k$, $[\![t]\!]_\rho^\mathcal{M} = f^\mathcal{M}([\![t_1]\!]_\rho^\mathcal{M}, .., [\![t_k]\!]_\rho^\mathcal{M})$

Remarque : la valeur de t ne dépend que des variables qui apparaissent dans t.

Interprétation d'une formule

Définition

L'interprétation $[\![F]\!]^{\mathcal{M}}_{\rho} \in \{0,1\}$ d'une formule F par rapport à une valuation ρ est définie par induction sur F :

$$
\begin{array}{rcll}
[\![Rt_1 \cdots t_n]\!]^{\mathcal{M}}_{\rho} & = & 1 & \text{si } \left([\![t_1]\!]^{\mathcal{M}}_{\rho}, \ldots, [\![t_n]\!]^{\mathcal{M}}_{\rho}\right) \in R^{\mathcal{M}} \\
 & & 0 & \text{sinon} \\
[\![(F \wedge G)]\!]^{\mathcal{M}}_{\rho} & = & \multicolumn{2}{l}{[\![\wedge]\!]([\![F]\!]^{\mathcal{M}}_{\rho}, [\![G]\!]^{\mathcal{M}}_{\rho})} \\
\ldots & & & \\
[\![\forall x F]\!]^{\mathcal{M}}_{\rho} & = & 1 & \text{si pour tout} d \in M,\ [\![F]\!]^{M}_{\rho[x \mapsto d]} = 1 \\
 & & 0 & \text{sinon} \\
[\![\exists x F]\!]^{\mathcal{M}}_{\rho} & = & 1 & \text{s'il existe } d \in M \text{ tel que } [\![F]\!]^{\mathcal{M}}_{\rho[x \mapsto d]} = 1 \\
 & & 0 & \text{sinon}
\end{array}
$$

Interprétation d'une formule

Remarque : $[\![F]\!]_\rho^{\mathcal{M}}$ ne dépend que des valeurs de ρ sur $\mathrm{FV}(F)$.

Définition

$\mathcal{M}$ est *un modèle de F* (noté $\mathcal{M} \models F$) si pour tout valuation ρ $[\![F]\!]_\rho^{\mathcal{M}} = 1$.

Vocabulaire : F est aussi dite *valide* (ou *vraie*) dans $\mathcal{M}$.

Remarque : Si F non close, F est valide dans $\mathcal{M}$ si et seulement si une de ses clôtures universelles est valide dans $\mathcal{M}$.

Exercice

$$\mathfrak{F} = \{c : 0,\ f : 1,\ \circ : 2, \bullet : 2\} \qquad P = \{z : 1,\ = : 2\}$$

$$F = (zc \wedge \forall x\, \forall y\, f{\circ}xy = \bullet fxfy)$$

- Montrer que F est valide dans plusieurs structures sur $\mathbb{R}$.
- Montrer que F n'est pas valide dans toutes structures.

Exercice : complément

Les structures de ce langage sont de la forme

$$\begin{aligned}\mathcal{M} = \ & (M, c^{\mathcal{M}} \in M, f^{\mathcal{M}} \in M \to M, \circ^{\mathcal{M}} \in M \times M \to M, \\ & \bullet^{\mathcal{M}} \in M \times M \to M, z^{\mathcal{M}} \subseteq M, =^{\mathcal{M}} \subseteq M \times M)\end{aligned}$$

Pour tout valuation ρ,

$$\begin{aligned}
[\![F]\!]^{\mathcal{M}}_{\rho} = 1 \quad & \text{ssi} \quad [\![zc]\!]^{\mathcal{M}}_{\rho} = 1 \text{ et } [\![\forall x\, \forall y\, f{\circ}xy = \bullet fxfy]\!]^{\mathcal{M}}_{\rho} = 1 \\
& \text{ssi} \quad c^{\mathcal{M}} \in z^{\mathcal{M}} \text{ et} \\
& \qquad \text{si pour tout } d_x \in M,\ [\![\forall y\, f{\circ}xy = \bullet fxfy]\!]^{\mathcal{M}}_{\rho[x \mapsto d_x]} = 1 \\
& \text{ssi} \quad c \in z^{\mathcal{M}} \text{ et} \\
& \qquad \text{si pour tout } d_x \in M, \\
& \qquad \text{si pour tout } d_y \in M,\ [\![f{\circ}xy = \bullet fxfy]\!]^{\mathcal{M}}_{\rho[x \mapsto d_x][y \mapsto d_y]} = 1 \\
& \ldots \\
& \text{ssi} \quad c \in z^{\mathcal{M}} \text{ et si pour tout } d_x \in M \text{ et } d_y \in M, \\
& \qquad (f^{\mathcal{M}}(\circ^{\mathcal{M}}(d_x, d_y)), \bullet^{\mathcal{M}}(f^{\mathcal{M}}(d_x), f^{\mathcal{M}}(d_y))) \in =^{\mathcal{M}}
\end{aligned}$$

Définitions

- Une formule est *universellement valide* si et seulement si elle est valide dans toute structure. Notation : $\models^* F$.
- Une formule est *contradictoire* si et seulement si il n'existe pas de structure dans laquelle elle soit valide.
- F et G sont *équivalentes* si $F \iff G$ est universellement valide, noté $F \equiv G$.

Substitution

On ne veut pas changer le "sens" d'une formule

Exemple : substituer $X - 1$ à Y dans $\forall X, X < Y)$.
Il faut interdire la capture des variables libres.

Substitution licite : Soit $t = t[w_1, .., w_n]$ un terme, la substitution $F[t/v]$ est *licite* si pour toute sous-formule F' de F de la forme $\Box w_i F''$, v n'est pas libre dans F''.

Lemme

Si $F[t/v]$ est licite alors

$$[\![F[t/v]]\!]^{\mathcal{M}}_{\rho} = [\![F]\!]^{\mathcal{M}}_{\rho[v \mapsto [\![t]\!]^{\mathcal{M}}_{\rho}]}$$

Propriétés sur $\equiv$

Proposition

Pour toutes formules F, F', G, G', si $F \equiv F$ et $G \equiv G$, alors $\neg F, F \wedge G, F \vee G, F \Rightarrow G, F \iff G, \forall v F$ et $\exists v F$ sont respectivement équivalentes a $\neg F', F' \wedge G', F' \vee G', F' \Rightarrow G', F' \iff G', \forall v F'$ et $\exists F'$

Proposition

Si w n'a aucune occurrence dans F, alors $\forall v F$ (resp. $\exists v F$) et $\forall w F[w/v]$ (resp. $\exists w F[w/v]$ sont équivalentes.

Propriétés sur $\equiv$

Pour toutes formules F et G et toutes variables v et w,

$$\begin{array}{rcl} \neg\forall vF & \equiv & \exists v\neg F \\ \forall v(F \wedge G) & \equiv & (\forall vF \wedge \forall vG) \\ \forall v\forall wF & \equiv & \forall w\forall vF \\ \forall v(F \Rightarrow G) & \equiv & (\exists vF \Rightarrow \forall vG) \end{array} \qquad \begin{array}{rcl} \neg\exists vF & \equiv & \forall v\neg F \\ \exists v(F \vee G) & \equiv & (\exists vF \vee \exists vG) \\ \exists v\exists wF & \equiv & \exists w\exists vF \\ \exists v(F \Rightarrow G) & \equiv & (\forall vF \Rightarrow \exists vG) \end{array}$$

Les trois formules suivantes sont universellement valides :

$$\begin{array}{rcl} \exists v(F \wedge G) & \Rightarrow & (\exists vF \wedge \exists vG) \\ \forall v(F \vee G) & \Rightarrow & (\forall vF \vee \forall vG) \\ \exists v\forall wF & \Rightarrow & \forall w\exists vF \end{array}$$

Propriétés sur $\equiv$

Pour toutes formules F et G et toutes variables v non libre dans G,

$$\forall v G \equiv \exists v G \equiv G$$

$$\begin{array}{rcl}
\forall v(F \wedge G) & \equiv & (\forall v F \wedge G) \\
\exists v(F \wedge G) & \equiv & (\exists v F \wedge G) \\
\forall v(F \vee G) & \equiv & (\forall v F \vee G) \\
\exists v(F \vee G) & \equiv & (\exists v F \vee G) \\
\forall v(G \Rightarrow F) & \equiv & (G \Rightarrow \forall v F) \\
\exists v(G \Rightarrow F) & \equiv & (G \Rightarrow \exists v F) \\
\forall v(F \Rightarrow G) & \equiv & (\exists v F \Rightarrow G) \\
\exists v(F \Rightarrow G) & \equiv & (\forall v F \Rightarrow G)
\end{array}$$

Propriétés sur $\equiv$

Théorème

Toute formule du 1^er ordre est universellement équivalente à au moins une formule ne contenant pas de symbole de connecteur ou de quantificateur autre que $\neg, \vee$ *et* $\exists$.

Formes prénexes

Définition

F est *prénexe* ssi il existe $k \in \mathbb{N}$, $x_1, .., x_k \in V$, $\square_1, .., \square_k$ symboles de quantificateurs et G formule sans quantificateurs tels que
$F = \underbrace{\square_1 x_1 .. \square_k x_k}_{\text{préfixe}} G.$

F est *prénexe polie* ssi son préfixe contient au plus une occurrence de chaque variable.

Théorème

Toute formule admet au moins une forme prénexe polie.

Formes de Skolem

On part d'une formule prénexe polie et on cherche à éliminer les quantificateurs existentiels.

On ajoute pour cela des nouveaux symboles de fonctions au langage. A chaque variable x quantifiée existentiellement on associe un symbole d'arité égal au nombre d'occurrences de $\forall$ à gauche de $\exists x$ dans le préfixe de F.

A F on associe $L_{Sk}(F)$, enrichissement de L par p symboles, p étant le nombre d'occurrences de $\exists$ dans le préfixe de F. La formule obtenue est appelée *forme de Skolem* de F.

Exemple : si $F = \forall x_1 \forall x_2 \exists x_3 \forall x_4 \exists x_5 G$,
$L_{Sk}(F) = \forall x_1 \forall x_2 \forall x_4 G[f_3 x_1 x_2 / x_3, f_5 x_1 x_2 x_4 / x_5]$.

Remarque

Si F_{Sk} est une forme de Skolem de F, F et F_{Sk} ne sont pas universellement équivalentes

Exemple : $F = \forall v_0 \exists v_1 R v_0 v_1$, $F_{Sk} = \forall v_0 R v_0 f v_0$, la structure

$$\mathcal{M} = (\mathbb{Z}, \leqslant \ (R^{\mathcal{M}}), n \mapsto n-1 \ (f^{\mathcal{M}}))$$

est telle que $\mathcal{M} \models F$ mais $\mathcal{M} \not\models F_{Sk}$.

Propriété des formes de Skolem

Lemme

Soit F une formule prénexe polie de L, alors la formule $F_{Sk} \Rightarrow F$ de L_{Sk} est universellement valide.

Lemme

Soit F une formule prénexe polie de L et $\mathcal{M}$ une structure et ρ une valuation telles que $[\![F]\!]^{\mathcal{M}}_{\rho} = 1$. Il est possible d'enrichir $\mathcal{M}$ en une structure $\mathcal{M}'$ de $L_{Sk}(F)$ telle que $[\![F_{Sk}]\!]^{\mathcal{M}'}_{\rho} = 1$

Théorème

Une formule close admet un modèle si et seulement une quelconque de ses formes de Skolem admet un modèle.

Théories

Une *théorie* T est un ensemble de formules closes (appelées *axiomes*).

- Soit $\mathcal{M}$ une structure, $\mathcal{M}$ est un *modèle* de la théorie T ($\mathcal{M} \models T$) ssi $\mathcal{M} \models F$ pour tout $F \in T$.
- T est *consistante* (non contradictoire) ssi elle admet au moins un modèle.
- F est *conséquence* de T ssi $\mathcal{M} \models T$ implique $\mathcal{M} \models F$, noté $T \models^* F$.
- T est *complète* ssi t est consistante et pour toute formule close F, on a $T \models^* F$ ou $T \models^* \neg F$.
- L'ensemble $\mathrm{Thm}(T)$ des *théorèmes* de T est l'ensemble des formules F telles que[1] $T \models^* F$.
- T est *récursive* si l'ensemble des formules de T est récursif.
- T est *décidable* si l'ensemble $\mathrm{Thm}(T)$ est récursif.

[1] ⚠ Nous confondons $\models^*$ et $\vdash$ (voir plus loin).

Exemples de théorie (1/3)

La théorie vide ($T = \emptyset$) correspond au calcul des prédicats.

- elle est consistante,
- elle est complète,
- ses théorèmes sont les formules universellement valides.
- elle est récursive,
- elle n'est pas décidable (pour un langage de 1$^{\text{er}}$ ordre suffisamment riche) : c'est le théorème de Church (admis)

Exemples de théorie (2/3)

La théorie de l'égalité. $\mathcal{R}_2$ contient un symbole de relation binaire $=$.

Axiomes :

$$\begin{array}{lcl}
A^1 & : & \forall x =xx \\
A^2 & : & \forall xy =xy \Rightarrow =yx \\
A^3 & : & \forall xyz =xy \wedge =yz \Rightarrow =xz \\
A^f & : & \forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n \\
 & & \quad =x_1y_1 \wedge \cdots \wedge =x_ny_n \Rightarrow =fx_1 \cdots x_n fy_1 \cdots y_n \\
 & & \text{pour tout } f \in \mathcal{F}_n \\
A^R & : & \forall x_1 \cdots \forall x_n \forall y_1 \cdots \forall y_n \\
 & & \quad =x_1y_1 \wedge \cdots \wedge =x_ny_n \Rightarrow (Rx_1 \cdots x_n \Rightarrow Ry_1 \cdots y_n) \\
 & & \text{pour tout } R \in \mathcal{R}_n
\end{array}$$

Exemples de théorie (3/3)

La théorie de l'arithmétique de Peano. $L = \{0, s, +, \times, <, =\}$
Théorie de l'égalité[2] + :

$$\begin{array}{ll}
\forall x & \neg(s\ x = 0) \\
\forall x\ \forall y & s\ x = s\ y \Rightarrow x = y \\
\forall x & x + 0 = x \\
\forall x\ \forall y & x + s\ y = s(x + y) \\
\forall x & x \times 0 = 0 \\
\forall x\ \forall y & x \times s\ y = x + (x \times y) \\
\forall x & \neg(x < 0) \\
\forall x\ \forall y & x < s\ y \iff x < y \vee x = y
\end{array}$$

+ une infinité (dénombrable) d'axiomes de récurrence :

$$F[0/x] \wedge (\forall x (F \Rightarrow F[s\ x/x]) \Rightarrow \forall x F)$$

pour chaque formule F et chaque variable libre x dans F.

[2] On utilise les conventions syntaxiques courantes.

Propriété de l'arithmétique de Peano

Théorème (Ryll - Nardzewski)

L'arithmétique de Peano n'est pas finiment axiomatisable.

Théorème

L'arithmétique de Peano n'est pas décidable

C'est un corollaire des *grands* théorèmes qui suivent.

Les grands théorèmes

Théorème

Une théorie complète et récursive est décidable.

Théorème

Une théorie consistante contenant l'arithmétique de Peano est indécidable.

Ces deux théorèmes ont pour *corollaire* un théorème célèbre.

Théorème (1$^{\text{er}}$ théorème d'incomplétude de Gödel)

Une théorie recursive et consistante contenant l'arithmétique de Peano n'est pas complète.

Propriétés axiomatisables

Définition

Soit L un langage du 1^{er} ordre et $\mathcal{P}$ une propriété que chaque L−structure est susceptible de vérifier (ou non).
La propriété $\mathcal{P}$ est dite *axiomatisable* s'il existe une théorie T de L telle que, pour tout L−structure $\mathcal{M}$,

$$\mathcal{M} \text{ vérifie } \mathcal{P} \text{ ssi } \mathcal{M} \models T$$

Théorème

La propriété « être un ensemble fini » n'est pas axiomatisable.

C'est une conséquence du théorème de compacité (*cf* suite).

Théorème

La propriété « être un ensemble infini » n'est pas axiomatisable avec une théorie finie.

Plan