Formules

$\mathcal{T}(\mathcal{F}, X)$ termes

Symboles de relation $(\mathcal{S}, \rho)$

Formules ensemble défini inductivement par :

- $P \in \mathcal{S}, \rho(P) = n$, $t_1, \dots, t_n$ termes $\to P(t_1, \dots, t_n)$ formule (atomique)
- F formule $\to \neg F$ formule
- F et G formules $\to F \diamond G$ formule où $\diamond \in \{\Rightarrow, \vee, \wedge\}$
- F formule, $x \in X \to \forall x, F$ formule, $\exists x, F$ formule

$\forall$ et $\exists$ quantificateurs priorité minimale

Formules et. . . ?

Pourquoi ?

Sémantique ?

Déduc. nat. ?

Sémantique

Pourquoi ? pour parler des gens qui vont à Paris. . ., des hommes. . .

- Termes : objets du discours $\rightsquigarrow$ ensembles connus
- Relations/prédicats : propriétés des objets $\rightsquigarrow$ algèbre $\mathbb{B}$

Sémantique

$(\mathcal{F}, \tau)$ signature termes, $(\mathcal{S}, \rho)$ signature relations

Interprétation I : $(D, I_{\mathcal{F}}, I_{\mathcal{S}})$

- D domaine, ensemble non vide
- $I_{\mathcal{F}}$: pour chaque $f \in \mathcal{F}, \tau(f) = n, \quad I_{\mathcal{F}}(f) = f_I : D^n \to D$
- $I_{\mathcal{S}}$: pour chaque $P \in \mathcal{S}, \rho(P) = k, \quad I_{\mathcal{S}}(P) = P_I : D^k \to \mathbb{B}$

Valuation $\nu : X \to D$

Notation : $\nu[x/v_0]$ telle que $\nu[x/v_0](x) = v_0$

Interprétation : extension de ν par I à $\mathcal{T}(\mathcal{F}, X)$: puis aux formules :

- $I_\nu(x) = \nu(x)$ pour $x \in X$
- $I_\nu(f(t_1, \ldots, t_n)) = f_I(I_\nu(t_1), \ldots, I_\nu(t_n))$ pour $f \in \mathcal{F}$
- $I_\nu(P(t_1, \ldots, t_k)) = P_I(I_\nu(t_1), \ldots, I_\nu(t_k))$ pour $P \in \mathcal{S}$
- $I_\nu(F \vee G) = I_\nu(F) + I_\nu(G)$ pour F et G formules
- $I_\nu(F \wedge G) = I_\nu(F) \cdot I_\nu(G)$ pour F et G formules
- $I_\nu(\bot) = 0$
- $I_\nu(\neg F) = \overline{I_\nu(F)}$ pour F formule
- $I_\nu(\forall x, F) = \{1$ si pour tout $d \in D,$ on a $I_{\nu[x/d]}(F) = 1,$ 0 sinon
- $I_\nu(\exists x, F) = \{1$ s'il existe un $d \in D,$ tel que $I_{\nu[x/d]}(F) = 1,$ 0 sinon

Petit retour de syntaxe : variables sous quantificateur

$$P(x, z) \wedge \forall x, R(f(x, y), g(y))$$

et puis « muettes » $\rightsquigarrow$ renommage

$$P(x, z) \wedge \forall z, R(f(z, y), g(y))$$
$$P(x, z) \wedge \forall v, R(f(v, y), g(y))$$

mais pas y !

$$P(x, z) \wedge \forall y, R(f(y, y), g(y))$$

Petit retour de syntaxe : variables libres

Variables libres d'un terme :

- $\mathsf{FV}_\mathcal{T}(x) = \{x\}$ pour $x \in X$
- $\mathsf{FV}_\mathcal{T}(f(t_1, \ldots, t_n)) = \mathsf{FV}_\mathcal{T}(t_1) \cup \cdots \cup \mathsf{FV}_\mathcal{T}(t_n)$

d'une formule :

- $\mathsf{FV}(P(t_1, \ldots, t_k)) = \mathsf{FV}_\mathcal{T}(t_1) \cup \cdots \cup \mathsf{FV}_\mathcal{T}(t_k)$
- $\mathsf{FV}(F \diamond G) = \mathsf{FV}(F) \cup \mathsf{FV}(G)$ pour $\diamond \in \{\Rightarrow, \wedge, \vee\}$
- $\mathsf{FV}(\neg F) = \mathsf{FV}(F)$
- $\mathsf{FV}(\bot) = \varnothing$
- $\mathsf{FV}(\forall x, F) = \mathsf{FV}(\exists x, F) = \mathsf{FV}(F) \setminus \{x\}$

Petit retour de syntaxe : variables sous quantificateur

Quid de la substitution étendue aux formules ?

$\rightsquigarrow$ remplacement des variables libres… facile ?

Pour $\sigma = \{y \to t \ldots\}$

- Blabla sur constructions formules…
- $(\forall x, F)\sigma = \forall x, F\sigma$ si $x \neq y$ et $x \notin \mathsf{FV}(t)$
- $(\exists x, F)\sigma = \exists x, F\sigma$ si $x \neq y$ et $x \notin \mathsf{FV}(t)$

Exemple capture

Solution ? renommer les occ. liées (non libres)

F formule, I interprétation, $I_\nu(F)$ ne dépend pas des variables liées
Si F telle que FV$(F) = \varnothing$ alors $I_\nu(F) = I_\mu(F)$ pour toutes valuations ν, μ

- Si $I_\nu(F) = 1$ alors I_ν satisfait F, noté $I_\nu \vDash F$
- Si $I_\nu \vDash F$ pour tout $F \in \Gamma$ alors I_ν satisfait Γ, noté $I_\nu \vDash \Gamma$
- S'il n'existe aucune I_ν telle que $I_\nu \vDash \Gamma$ alors Γ contradictoire
- Si $I_\nu \vDash F$ pour tout I et tout ν alors F valide
- Si $I_\nu \vDash F$ pour tout I et tout ν telles que $I_\nu \vDash \Gamma$ alors $\Gamma \vDash F$
- F et G équivalentes : $F \vDash G$ et $G \vDash F$

Proposition.

F et G formules, Γ ensemble de formules.

- $\Gamma \vDash F \Rightarrow G$ si et seulement si $\Gamma \cup \{F\} \vDash G$
- $\Gamma \vDash F$ si et seulement si $\Gamma \cup \{\neg F\}$ contradictoire.

Celles de la logique propositionnelle +

$$\forall x, \forall y, F \equiv \forall y, \forall x, F$$
$$\exists x, \exists y, F \equiv \exists y, \exists x, F$$

$$\neg \forall x, F \equiv \exists x, \neg F$$
$$\neg \exists x, F \equiv \forall x, \neg F$$

$$(\forall x, F_1) \wedge F_2 \equiv \forall x, F_1 \wedge F_2 \quad \text{si } x \notin \text{FV}(F_2)$$
$$(\exists x, F_1) \wedge F_2 \equiv \exists x, F_1 \wedge F_2 \quad \text{si } x \notin \text{FV}(F_2)$$

$$(\forall x, F_1) \vee F_2 \equiv \forall x, F_1 \vee F_2 \quad \text{si } x \notin \text{FV}(F_2)$$
$$(\exists x, F_1) \vee F_2 \equiv \exists x, F_1 \vee F_2 \quad \text{si } x \notin \text{FV}(F_2)$$

Dans les faits...
Exemple : $\{Z : 0; S : 1; Plus : 2; Mult : 2\}$
$Mult(S(x), Plus(S(Z), y))$

$\nu(x) = 3 \qquad \nu(y) = 2$

$$D = \mathbb{N} \quad \begin{array}{lcllcl} I_{\mathcal{F}}(Z) & = & 0 & I_{\mathcal{F}}(S) & = & x \mapsto x +_{\mathbb{N}} 1 \\ I_{\mathcal{F}}(Plus) & = & x, y \mapsto x +_{\mathbb{N}} y & I_{\mathcal{F}}(Mult) & = & x, y \mapsto x \times_{\mathbb{N}} y \end{array}$$

$\nu(x)$ = place la plus à gauche $\quad \nu(y) = 3^{e}$ place en partant de la gauche
D = 10 places de parking en ligne

$I_{\mathcal{F}}(Z) =$ la place la plus à droite

$I_{\mathcal{F}}(S) =$ $p \mapsto$ la place à droite de p ou p si pas de place à droite de p

...

Extension des séquents au premier ordre couple ensemble / formules

Séquents prouvables définis inductivement par

- Déduc. nat. logique propositionnelle
- $\dfrac{\Gamma \vdash F \text{ où } x \text{ non libre dans } \Gamma}{\Gamma \vdash \forall x, F}\ (\forall_i)$
- $\dfrac{\Gamma \vdash \forall x, F}{\Gamma \vdash F[x \to t]}\ (\forall_e)$
- $\dfrac{\Gamma \vdash F[x \to t]}{\Gamma \vdash \exists x, F}\ (\exists_i)$
- $\dfrac{\Gamma \vdash \exists x, F \quad \Gamma \cup \{F\} \vdash G \quad x \text{ libre ni dans } \Gamma \text{ ni dans } G}{\Gamma \vdash G}\ (\exists_e)$

Théorème.
Si F formule sans variable libre,
alors $\vdash F$ séquent prouvable si et seulement $\vDash F$

$\leadsto$ extensible sans perte de cohérence (difficile)

Exemple : $\dfrac{}{\Gamma \vdash t = t}\ (=_i)$ reflexivity $\qquad \dfrac{\Gamma \vdash F[x \to t] \quad \Gamma \vdash t = s}{\Gamma \vdash F[x \to s]}\ (=_e)$

Tout homme est mortel, Socrate est un homme donc Socrate est mortel

Termes $\{S : 0\}$ Relations $\{H : 1,\ M : 1\}$

Modélisation

$$\Gamma = \left\{ \begin{array}{l} \forall x, H(x) \Rightarrow M(x) \\ H(S) \end{array} \right\}$$

Montrer $\Gamma \vdash M(S)$ est prouvable

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall x, H(x) \Rightarrow M(x)}\ (\text{ax})}{\Gamma \vdash H(S) \Rightarrow M(S)}\ (\forall_e) \qquad \dfrac{}{\Gamma \vdash H(S)}\ (\text{ax})}{\Gamma \vdash M(S)}\ (\Rightarrow_e)$$

$\leadsto$ extensible sans perte de cohérence (difficile)

Ex. : $\dfrac{}{\Gamma \vdash t = t}\ (=_i)$ `reflexivity` $\qquad \dfrac{\Gamma \vdash F[x \to t] \quad \Gamma \vdash t = s}{\Gamma \vdash F[x \to s]}\ (=_e)$

$\dfrac{\Gamma \vdash t = s}{\Gamma \vdash s = t}\ (=_{sym})$ `symmetry` $\qquad \dfrac{\Gamma \vdash s = t \quad \Gamma \vdash t = u}{\Gamma \vdash s = u}\ (=_{trans})$ `transitivity`

Termes inductifs + bonnes propriétés : possibilités ?

Entiers E définis inductivement :

- $\to Z$ — $Z \in E$
- $n \to Sn$ — $n \in E \to Sn \in E$

Prouver P sur E par induction : stabilité de $F \subseteq E$ t.q. si $n \in F$ alors Pn

- PZ
- Si Pn alors $P(Sn)$ — $n \in F \to Sn \in F$

$$\frac{PZ \quad \forall y, Py \to P(Sy)}{\forall x, Px}\ (E_{\text{ind}})$$

Listes de `nat` L définies inductivement :

- $\to$ `[]` — `[]` $\in L$
- $l \to n :: l$ pour n `nat` — $l \in L \to n :: l \in L$

Prouver P sur L par induction : stabilité de $F \subseteq L$ t.q. si $l \in F$ alors Pl

- P `[]`
- Si Pl alors pour tout n, $P(n :: l)$ — $l \in F \to n :: l \in F$

$$\frac{P\,[\,] \quad \forall n, \forall l', Pl' \to P(n :: l')}{\forall l, Pl}\ (L_{\text{ind}})$$

++Premier ordre

Termes pour calculer (données, programmes sur ces données)

Formules pour raisonner (propriétés sur termes, *preuves*)

Induction

$\leadsto$ sens d'un programme ? **sémantique des langages**. . .