LIFLC – Logique classique

CM6 – Logique du premier ordre: formules

Licence informatique UCBL – Automne 2018–2019

https://liris.cnrs.fr/ecoquery/dokuwiki/doku.php?id=enseignement:logique:start

Dpt Informatique

Faits et objets

Termes : valeur dans l'univers $\mathcal{U}$

Formules : valeur booléenne

Quel lien ?

Signature - étendue

Definition

Une *signature* $\mathcal{S} = (\mathcal{C}, \mathcal{F}, P, ar)$:

- $\mathcal{C}$: ensemble (non vide) de **symboles** de constantes
- $\mathcal{F}$: ensemble de **symboles** de fonction
- P : ensemble de **symboles** de prédicats
- $ar : \mathcal{F} \cup P \to \mathcal{N}^*$: nombre d'arguments de chaque symbole de fonction et de prédicat

Notation

f/n *signifie* $ar(f) = n$
p/n *signifie* $ar(p) = n$

Exemples

Entiers (de Peano) : $\mathcal{S}_{peano} = (\mathcal{C}_{peano}, \mathcal{F}_{peano}, ar_{peano})$

- $\mathcal{C}_{peano} = \{zero\}$
- $\mathcal{F}_{peano} = \{succ/1, plus/2, mult/2\}$
- $P_{peano} = \{inf/2, pair/1\}$

Chaînes de caractères : $\mathcal{S}_{char} = (\mathcal{C}_{char}, \mathcal{F}_{char}, ar_{char})$

- $\mathcal{C}_{char} = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$
- $\mathcal{F}_{char} = \{concat/2\}$
- $P_{char} = \{suff/2, pref/2\}$

Quantificateurs

Deux quantificateurs :

- $\forall$, $\exists$
- lie une variable

Formules

Le plus petit ensemble stable par les règles suivantes

- Si $t_1, \dots, t_n \in \mathcal{T}$ et si $P/n \in P$ alors $P(t_1, \dots, t_n)$ est une formule
- Si $t_1, t_2 \in \mathcal{T}$ alors $t_1 \doteq t_2$ est une formule
- $\perp$ est une formule
- Si A est une formule, alors $(\neg A)$ est une formule
- Si A et B sont des formules, alors $(A \vee B)$, $(A \wedge B)$ et $(A \Rightarrow B)$ sont des formules
- Si A est une formule et $x \in \mathcal{V}$ alors $(\forall x\ A)$ et $(\exists x\ A)$ sont des formules

⚠ terme $\neq$ formule ⚠

Exemples de formule

- $(x \doteq succ(y)) \wedge inf(x, y)$
- $\exists y \; inf(succ(x), y)$
- $\forall x \; \forall y \; (x \doteq succ(y) \wedge succ(x) \doteq y)$
- $\forall x \; inf(x, succ(x))$
- $\forall x \; \forall y \; (inf(x, y) \Rightarrow inf(x, succ(y)))$
- $inf(x, zero) \Rightarrow \exists y \; succ(y) \doteq zero$
- $inf(x, zero) \Rightarrow \exists x \; succ(x) \doteq zero$

Variables de termes

$V(t)$: variables de t

- $V(x) = \{x\}$ si $x \in \mathcal{V}$
- $V(c) = \emptyset$ si $c \in \mathcal{C}$
- $V(f(t_1, \dots, t_n)) = \bigcup_{i=1}^{n} V(t_i)$

Variables libres

Variables non masquées par un quantificateur

$FV(A)$: variables libres de A

- $FV(P(t_1, \dots, t_n)) = \bigcup_{i=1}^{n} V(t_i)$
- $FV(t_1 \doteq t_2) = V(t_1) \cup V(t_2)$
- $FV(\neg A) = FV(A)$
- $FV(A \vee B) = FV(A \wedge B) = FV(A \Rightarrow B) = FV(A) \cup FV(B)$
- $FV(\forall x\ A) = FV(\exists x\ A) = FV(A) \setminus \{x\}$

Exemples

- $FV((x \doteq succ(y)) \wedge inf(x, y)) = \{x, y\}$
- $FV(\exists y \; inf(succ(x), y)) = \{x\}$
- $FV(\forall x \; \forall y \; (x \doteq succ(y) \wedge succ(x) \doteq y)) = \emptyset$
- $FV(\forall x \; inf(x, succ(x))) = \emptyset$
- $FV(\forall x \; \forall y \; (inf(x, y) \Rightarrow inf(x, succ(y))) = \emptyset$
- $FV(inf(x, zero) \Rightarrow \exists y \; succ(y) \doteq zero) = \{x\}$
- $FV(inf(x, zero) \Rightarrow \exists x \; succ(x) \doteq zero) = \{x\}$

Fermetures

Ajout de quantificateurs pour les variables libres

Fermeture *universelle*

Si $FV(A) = \{x_1, \dots, x_n\}$ alors sa fermeture universelle (notée $\forall A$) est

$$\forall x_1 \ \dots \forall x_n \ A$$

Fermeture *existentielle*

Si $FV(A) = \{x_1, \dots, x_n\}$ alors sa fermeture existentielle (notée $\exists A$) est

$$\exists x_1 \ \dots \exists x_n \ A$$

Interprétations

Interprétation I des symboles dans $\mathcal{C}, \mathcal{F}$ et P

- Si $c \in \mathcal{C}$ alors $I(c) \in \mathcal{U}$
- Si $f/n \in \mathcal{F}$ alors $I(f) : \mathcal{U}^n \to \mathcal{U}$
- Si $P/n \in P$ alors $I(P) \subseteq \mathcal{U}^n$

Évaluation - 1

Fonction récursive $eval(I, \zeta)(A)$:

- Si $A = P(t_1, \dots, t_n)$
  Si $eval(I, \zeta)(t_1) = u_1 \ \dots \ eval(I, \zeta)(t_n) = u_n$ et si $I(P/n) = R$
  alors $eval(I, \zeta)(A) = 1$ ssi $(u_1, \dots, u_n) \in R$
- Si $A = (t_1 \doteq t_2)$
  Si $eval(I, \zeta)(t_1) = u$ et $eval(I, \zeta)(t_2) = u$
  alors $eval(I, \zeta)(A) = 1$
  sinon $eval(I, \zeta)(A) = 0$
- $eval(I, \zeta)(\neg B) = non(eval(I, \zeta)(B))$
- $eval(I, \zeta)(B \vee C) = ou(\ eval(I, \zeta)(B)\ ,\ eval(I, \zeta)(C)\ )$
- $eval(I, \zeta)(B \wedge C) = et(\ eval(I, \zeta)(B)\ ,\ eval(I, \zeta)(C)\ )$
- $eval(I, \zeta)(B \Rightarrow C) = implique(\ eval(I, \zeta)(B)\ ,\ eval(I, \zeta)(C)\ )$

Évaluation - 2

- Si $A = \forall x\ B$ et pour tous les $u \in \mathcal{U}$ alors
  si $eval(I, \zeta[x := u])(B) = 1$
  alors $eval(I, \zeta)(A) = 1$
  sinon $eval(I, \zeta)(A) = 0$
- Si $A = \exists x\ B$:
  si on peut trouver $u \in \mathcal{U}$ tel que
  $eval(I, \zeta[x := u])(B) = 1$,
  alors $eval(I, \zeta)(A) = 1$
  sinon $eval(I, \zeta)(A) = 0$

$$\zeta[x := u] : \quad \begin{array}{l} x \mapsto u \\ y \mapsto \zeta(y) \text{ si } x \neq y \end{array}$$

Interprétation dans les entier naturels

Univers $\mathcal{U}_{\mathcal{N}} = \mathcal{N}$ entiers naturels

$$
\begin{aligned}
I_{\mathcal{N}}(zero) &= 0 \\
I_{\mathcal{N}}(succ) &= n \mapsto n + 1 \\
I_{\mathcal{N}}(plus) &= n, m \mapsto n + m \\
I_{\mathcal{N}}(mult) &= n, m \mapsto n \times m \\
I_{\mathcal{N}}(inf) &= \{(n, m) \mid n < m\} \\
I_{\mathcal{N}}(pair) &= \{n \mid n\%2 = 0\}
\end{aligned}
$$

Interprétation dans les chaînes de caractères

Univers $\mathcal{U}_{str} = \{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\}^*$: chaînes de caractères sur l'alphabet $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$

$$
\begin{aligned}
I_{str}(a) &= \mathfrak{a} \\
I_{str}(b) &= \mathfrak{b} \\
I_{str}(c) &= \mathfrak{c} \\
I_{str}(concat) &= s_1, s_2 \mapsto s_1 s_2 \\
I_{str}(pref) &= \{(s_1, s_2) \mid s_2 \text{ commence par } s_1\} \\
I_{str}(suff) &= \{(s_1, s_2) \mid s_2 \text{ fini par } s_1\}
\end{aligned}
$$

Évaluation : exemple

$$\zeta : \begin{array}{l} x \mapsto 4 \\ y \mapsto 3 \end{array}$$

$$eval(I_{\mathcal{N}}, \zeta)((x \doteq succ(y)) \wedge inf(x, y))$$

$$et \ {\color{green}0}$$

$$\underbrace{x}_{\color{cyan}4} \doteq \underbrace{succ(\underbrace{y}_{\color{cyan}3})}_{\color{cyan}4} \ {\color{green}1} \qquad inf(\underbrace{x}_{\color{cyan}4}, \underbrace{y}_{\color{cyan}3}) \ {\color{green}0}$$

Évaluation : exemple - avec quantificateur

$$eval(I_{\mathcal{N}}, \zeta)(\forall x\ \forall y\ (inf(x, y) \Rightarrow inf(x, succ(y)))) = 1$$

Vérification compliquée
car pas directement calculable

Modèle

Interprétation “correspondant” à la formule :

Définition

Soit un univers $\mathcal{U}$ et une interprétation I. L'interprétation est un modèle de A (noté $I \models A$) si **pour toute valuation** $\zeta : \mathcal{V} \to \mathcal{U}$:

$$eval(I, \zeta)(A) = 1$$

Satisfiabilité - validité

Définition : satisfiabilité

Une formule est *satisfiable* si elle admet un modèle.

Définition : validité

Une formule est *valide* si toute interprétation est un modèle de cette formule.

Conséquence logique

Définition

Soit E un ensemble de formules et A une formule.
E a pour conséquence logique A (noté $E \models A$) si **pour tout** univers $\mathcal{U}$, interprétation I et valuation ζ

- si **pour toute formule** $B \in E$:

$$eval(I, \zeta)(B) = 1$$

- alors

$$eval(I, \zeta)(A) = 1$$

Équivalence de formule

Définition

A est logiquement équivalente à B (noté $A \equiv B$) ssi :

$$A \models B \qquad \text{et} \qquad B \models A$$

Application de substitution sur une formule

Substitution $\sigma : \mathcal{V} \to \mathcal{T}$

- $P(t_1, \dots, t_n)\sigma = P(t_1\sigma, \dots, t_n\sigma$
- $(t_1 \doteq t_2)\sigma = (t_1\sigma) \doteq (t_2\sigma)$
- $(\neg A)\sigma = \neg(A\sigma)$,
  $(A \vee B)\sigma = (A\sigma) \vee (B\sigma)$,
  $(A \wedge B)\sigma = (A\sigma) \wedge (B\sigma)$,
  $(A \Rightarrow B)\sigma = (A\sigma) \Rightarrow (B\sigma)$
- $\left.\begin{array}{l}(\forall x\ A)\sigma = \forall x\ (A\sigma) \\ (\exists x\ A)\sigma = \exists x\ (A\sigma)\end{array}\right\}$ si $x \notin dom(\sigma)$ et $x \notin \bigcup_{y \in dom(\sigma)} V(\sigma(y))$

Exemple

$$(\ (x \doteq succ(y)) \land inf(x, y) \ )[x := succ(y), y := plus(zero, z)]$$

$$=$$

$$(succ(y) \doteq succ(plus(zero, z))) \land inf(succ(y), plus(zero, z))$$

Exemple - 2

$$(\ \exists y\ \mathit{inf}(\mathit{succc}(x), y)\ )[x := z] = \exists y\ \mathit{inf}(\mathit{succ}(z), y)$$

$$(\ \exists y\ \mathit{inf}(\mathit{succ}(x), y)\ )[y := z] \qquad \text{non défini}$$

$$(\ \exists y\ \mathit{inf}(\mathit{succ}(x), y)\ )[x := y] \qquad \text{non défini}$$

Équivalences remarquables

Renommage de variable :

- $\forall x\ A \equiv \forall y\ A[x := y]$ si $y \notin FV(A)$
- $\exists x\ A \equiv \exists y\ A[x := y]$ si $y \notin FV(A)$

Autres équivalences

- $\forall x \forall y\ A \equiv \forall y \forall x\ A$
- $\exists x \exists y\ A \equiv \exists y \exists x\ A$
- $\exists x\ \neg A \equiv \neg \forall x\ A$
- $\forall x\ \neg A \equiv \neg \exists x\ A$

Inversions $\exists\forall$: pas d'équivalence

- $\exists y\ \forall x\ A \models \forall x\ \exists y\ A$
- $\forall x\ \exists y\ A \not\models \exists y\ \forall x\ A$

Raisonnement sur une interprétation difficile

- Possible de raisonner sur un univers *fini* en faisant des vérifications systématiques
  - Très coûteux en général
- Pas toujours possible sur un univers *infini* : pas de vérification systématique
- Infinité d'interprétation possibles

Représenter les hypothèses / la connaissance

Utiliser des formules pour représenter ce que l'on sait.

Théorie : ensemble de formules représentant la connaissance d'un domaine

Savoir si une formule est "vraie" : savoir si elle est conséquence logique de la théorie

Extension de la déduction naturelle au premier ordre

Règles additionnelles pour les quantificateurs et pour $\doteq$

Manipulation des termes à travers des substitutions

Théories à gauche dans les séquents

Règles propositionnelles

Axiome

$$\frac{}{\Gamma, A \vdash A}\ (ax)$$

Affaiblissement

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A}\ (aff)$$

Règles pour $\Rightarrow$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow_i) \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow_e)$$

Règles pour $\bot$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ (\bot_i) \text{ ou } (\neg_e) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (\bot_e)$$

Règles pour $\neg$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ (\neg_i) \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (\neg_c)$$

Règles propositionnelles - 2

règles pour $\wedge$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge_i) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge_e^g) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge_e^d)$$

règles pour $\vee$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee_i^g) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\vee_i^d)$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\vee_e)$$

Règles sur les quantificateurs et l'égalité

Règles pour $\forall$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ (\forall_i)\ \text{si } x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[^t/_x]}\ (\forall_e)$$

Règles pour $\exists$

$$\frac{\Gamma \vdash A[^t/_x]}{\Gamma \vdash \exists x\ A}\ (\exists_i) \qquad \frac{\Gamma \vdash \exists x\ B \quad \Gamma, B \vdash A}{\Gamma \vdash A}\ (\exists_e)\ \text{si } x \notin FV(\Gamma, B)$$

Règle pour $\doteq$

$$\frac{}{\Gamma \vdash t \doteq t}\ (\doteq_i) \qquad \frac{\Gamma \vdash A[^t/_x] \quad \Gamma \vdash t \doteq t'}{\Gamma \vdash A[^{t'}/_x]}\ (\doteq_e)$$

Exemple de dérivation

$$\Gamma \ = \ \forall x \, \forall y \ (inf(x, y) \Rightarrow inf(x, succ(y))\ , \ \forall x \ inf(x, succ(x))$$

$$\dfrac{\dfrac{}{\Gamma \vdash \forall x \ \ inf(x, succ(x))}\,(ax)}{\Gamma \vdash inf(zero, succ(zero))}\,(\forall_e)$$