Cours 2: preuves en logique du premier ordre

David Delahaye

Polytech' Montpellier
David.Delahaye@lirmm.fr

AIGLE M1

Logique du premier ordre

Définitions préliminaires

- $\mathcal{V} \equiv$ ensemble de variables d'individu x, y, etc. ;
- $\mathcal{S}_{\mathcal{F}} \equiv$ ensemble de symboles de fonctions f, g, etc. ;
- $\mathcal{S}_{\mathcal{P}} \equiv$ ensemble de symboles de prédicats P, Q, etc. ;
- $\mathcal{S}_{\mathcal{F}} \cap \mathcal{S}_{\mathcal{P}} = \emptyset$;
- Arité $m : \mathcal{S}_{\mathcal{F}} \cup \mathcal{S}_{\mathcal{P}} \to \mathbb{N}$.

Termes du premier ordre

- Plus petit ensemble $\mathcal{T}$ t.q. :
  - Si $x \in \mathcal{V}$ alors $x \in \mathcal{T}$;
  - Si $f \in \mathcal{S}_{\mathcal{F}}$ d'arité n et $t_1, \ldots, t_n \in \mathcal{T}$, alors $f(t_1, \ldots, t_n) \in \mathcal{T}$.

Logique du premier ordre

Définitions préliminaires

- $\mathcal{V} \equiv$ ensemble de variables d'individu x, y, etc. ;
- $\mathcal{S}_\mathcal{F} \equiv$ ensemble de symboles de fonctions f, g, etc. ;
- $\mathcal{S}_\mathcal{P} \equiv$ ensemble de symboles de prédicats P, Q, etc. ;
- $\mathcal{S}_\mathcal{F} \cap \mathcal{S}_\mathcal{P} = \emptyset$;
- Arité $m : \mathcal{S}_\mathcal{F} \cup \mathcal{S}_\mathcal{P} \to \mathbb{N}$.

Formules du premier ordre

- Plus petit ensemble $\mathcal{F}$ t.q. :
  - Si $P \in \mathcal{S}_\mathcal{P}$ d'arité n et $t_1, \ldots, t_n \in \mathcal{T}$, alors $P(t_1, \ldots, t_n) \in \mathcal{F}$;
  - $\bot, \top \in \mathcal{F}$;
  - Si $\Phi \in \mathcal{F}$ alors $\neg\Phi \in \mathcal{F}$;
  - Si $\Phi, \Phi' \in \mathcal{F}$ alors $\Phi \wedge \Phi', \Phi \vee \Phi', \Phi \Rightarrow \Phi' \in \mathcal{F}$;
  - Si $x \in \mathcal{V}$ et $\Phi \in \mathcal{F}$, alors $\forall x.\Phi, \exists x.\Phi \in \mathcal{F}$.

Sémantiques

Logique classique

- Une formule est toujours vraie ou fausse ;
- Que je puisse en démontrer la validité ou non ;
- Logique bi-valuée (vrai, faux) ;
- Logique du « tiers exclu » : $A \vee \neg A$.

Logique intuitionniste ou constructive

- Une formule est vraie, fausse, ou « on ne sait pas » ;
- Si on ne sait en démontrer la validité, alors « on ne sait pas » ;
- Logique tri-valuée d'une certaine manière ;
- Le « tiers exclu » n'est pas admis dans cette logique.

Systèmes de preuves

Plusieurs systèmes

- Systèmes à la Frege-Hilbert ;
- Systèmes à la Gentzen :
  - Déduction naturelle ;
  - Calcul des séquents.

Adéquation vis-à-vis de la sémantique

- Correction et complétude par rapport à la sémantique ;
- Correction : si je trouve une preuve de P alors P est vraie ;
- Complétude : si P est vraie alors il existe une preuve de P ;
- Preuve $\equiv$ moyen syntaxique de vérifier la validité d'une formule.

Calcul des séquents intuitionniste

Règles

$$\frac{}{\Gamma, A \vdash A}\ \mathrm{ax} \qquad \frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B}\ \mathrm{cont}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \Rightarrow B \vdash C}\ \Rightarrow_{\mathrm{left}} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow_{\mathrm{right}}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, B \vdash C}{\Gamma, A \Leftrightarrow B \vdash C}\ \Leftrightarrow_{\mathrm{left1}}$$

$$\frac{\Gamma \vdash B \qquad \Gamma, A \vdash C}{\Gamma, A \Leftrightarrow B \vdash C}\ \Leftrightarrow_{\mathrm{left2}} \qquad \frac{\Gamma, A \vdash B \qquad \Gamma, B \vdash A}{\Gamma \vdash A \Leftrightarrow B}\ \Leftrightarrow_{\mathrm{right}}$$

Calcul des séquents intuitionniste

Règles

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\ \wedge_{\text{left}} \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_{\text{right}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_{\text{right1}}$$

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\ \vee_{\text{left}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_{\text{right2}}$$

$$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash B}\ \neg_{\text{left}} \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_{\text{right}}$$

$$\frac{}{\Gamma, \bot \vdash A}\ \bot_{\text{left}} \qquad \frac{}{\Gamma \vdash \top}\ \top_{\text{right}}$$

Calcul des séquents intuitionniste

Règles

$$\frac{\Gamma, A(t) \vdash B}{\Gamma, \forall x\ A(x) \vdash B}\ \forall_{\text{left}} \qquad \frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x\ A(x)}\ \forall_{\text{right}},\ \ x \notin \Gamma$$

$$\frac{\Gamma, A(x) \vdash B}{\Gamma, \exists x.A(x) \vdash B}\ \exists_{\text{left}},\ \ x \notin \Gamma, B \qquad \frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x.A(x)}\ \exists_{\text{right}}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{cut}$$

Calcul des séquents classique

Règles

$$\frac{\Gamma, A(t) \vdash B}{\Gamma, \forall x\ A(x) \vdash B}\ \forall_{\text{left}} \qquad \frac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x\ A(x)}\ \forall_{\text{right}},\ x \notin \Gamma$$

$$\frac{\Gamma, A(x) \vdash B}{\Gamma, \exists x.A(x) \vdash B}\ \exists_{\text{left}},\ x \notin \Gamma, B \qquad \frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x.A(x)}\ \exists_{\text{right}}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{cut} \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ \text{em}$$

Calcul des séquents classique (LK)

Règles

$$\frac{}{\Gamma, A \vdash \Delta, A}\ \mathrm{ax} \qquad \frac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ \mathrm{cut}$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ \mathrm{cont}_{\mathrm{left}} \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ \mathrm{cont}_{\mathrm{right}}$$

Calcul des séquents classique (LK)

Règles

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta} \Rightarrow_{\text{left}} \qquad \frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta, A \Rightarrow B} \Rightarrow_{\text{right}}$$

$$\frac{\Gamma \vdash \Delta, A \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Leftrightarrow B \vdash \Delta} \Leftrightarrow_{\text{left1}}$$

$$\frac{\Gamma \vdash \Delta, B \qquad \Gamma, A \vdash \Delta}{\Gamma, A \Leftrightarrow B \vdash \Delta} \Leftrightarrow_{\text{left2}}$$

$$\frac{\Gamma, A \vdash \Delta, B \qquad \Gamma, B \vdash \Delta, A}{\Gamma \vdash \Delta, A \Leftrightarrow B} \Leftrightarrow_{\text{right}}$$

Calcul des séquents classique (LK)

Règles

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_{\text{left}} \qquad \frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}\ \wedge_{\text{right}}$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee_{\text{left}} \qquad \frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}\ \vee_{\text{right}}$$

$$\frac{\Gamma \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta}\ \neg_{\text{left}} \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\ \neg_{\text{right}}$$

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot_{\text{left}} \qquad \frac{}{\Gamma \vdash \Delta, \top}\ \top_{\text{right}}$$

Calcul des séquents classique (LK)

Règles

$$\frac{\Gamma, A(t) \vdash \Delta}{\Gamma, \forall x.A(x) \vdash \Delta}\,\forall_{\text{left}} \qquad \frac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)}\,\forall_{\text{right}},\ \ x \notin \Gamma, \Delta$$

$$\frac{\Gamma, A(x) \vdash \Delta}{\Gamma, \exists x.A(x) \vdash \Delta}\,\exists_{\text{left}},\ \ x \notin \Gamma, \Delta \qquad \frac{\Gamma \vdash \Delta, A(t)}{\Gamma \vdash \Delta, \exists x.A(x)}\,\exists_{\text{right}}$$

Exemple de preuve propositionnelle dans LJ/LK

Une preuve simple

$$\dfrac{\dfrac{}{A, B \vdash A}\,\text{ax} \qquad \dfrac{}{A, B \vdash B}\,\text{ax}}{\dfrac{A, B \vdash A \wedge B}{\dfrac{A \vdash B \Rightarrow A \wedge B}{\vdash A \Rightarrow B \Rightarrow A \wedge B}\,\Rightarrow_{\text{right}}}\,\Rightarrow_{\text{right}}}\,\wedge_{\text{right}}$$

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(x) \vdash P(x)}\,\text{ax}}{P(x) \vdash \exists x.P(x)}\,\exists_{\text{right}}}{\neg(\exists x.P(x)), P(x) \vdash \bot}\,\neg_{\text{left}}}{\neg(\exists x.P(x)) \vdash \neg P(x)}\,\neg_{\text{right}}}{\neg(\exists x.P(x)) \vdash \forall x.\neg P(x)}\,\forall_{\text{right}}}{\vdash \neg(\exists x.P(x)) \rightarrow \forall x.\neg P(x)}\,\Rightarrow_{\text{right}}
$$

Logiques classique/intuitionniste

Sémantique du « il existe »

- En logique classique : $\exists x.P(x) \equiv$ il existe n termes $t_1, t_2, \ldots, t_n$ tels que $P(t_1) \vee P(t_2) \vee \ldots \vee P(t_n)$ est vraie (théorème de Herbrand) ;
- En logique intuitionniste : $\exists x.P(x) \equiv$ il existe un terme t tel que $P(t)$ est vraie.
  On doit contruire un témoin t qui vérifie P et en avoir l'intuition.
  D'où le nom de logique « intuitionniste » ou « constructive ».

Logique classique

- La logique classique est une logique assez « exotique » ;
- On peut démontrer une formule $\exists x.P(x)$ sans jamais montrer un seul témoin qui fonctionne (c'est-à-dire qui vérifie P) !
- De ce fait, c'est plus facile de faire des preuves en logique classique qu'en logique intuitionniste.

Exemple de preuve en logique classique

Petit théorème mathématique

- Il existe a et b irrationnels tels que a^b est rationnel ;
- Preuve :
  - Utilisation du tiers exclu : $\sqrt{2}^{\sqrt{2}}$ est rationnel ou non ; deux cas :
    - Si $\sqrt{2}^{\sqrt{2}}$ est rationnel, alors le théorème est vrai ;
    - Si $\sqrt{2}^{\sqrt{2}}$ est irrationnel, alors $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, qui est rationnel.

En logique intuitionniste

- Le théorème est vrai en logique intuitionniste ;
- Mais on doit montrer un a et b qui fonctionnent ;
- Plusieurs pages de théorie des nombres non triviales !

Un autre exemple de preuve en logique classique

Preuve dans LK

Démontrer : $\exists x.P(x) \Rightarrow P(a) \wedge P(b)$.

Cette formule est-elle valide ?

Un autre exemple de preuve en logique classique

Preuve dans LK

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash P(a), P(a) \wedge P(b)}\,\text{ax} \qquad \dfrac{}{\Gamma \vdash P(b), P(a) \wedge P(b)}\,\text{ax}}{\Gamma = P(a), P(b) \vdash P(a) \wedge P(b), P(a) \wedge P(b)}\,\wedge_{\text{right}}}{P(a) \vdash P(a) \wedge P(b), P(b) \Rightarrow P(a) \wedge P(b)}\,\Rightarrow_{\text{right}}}{P(a) \vdash P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}\,\exists_{\text{right}}}{\vdash P(a) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}\,\Rightarrow_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}\,\exists_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b)}\,\text{cont}_{\text{right}}
$$

Exercices en logique propositionnelle

Propositions à démontrer

1. $A \Rightarrow B \Rightarrow A$
2. $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$
3. $A \wedge B \Rightarrow B$
4. $B \Rightarrow A \vee B$
5. $(A \vee B) \Rightarrow (A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow C$
6. $A \Rightarrow \bot \Rightarrow \neg A$
7. $\bot \Rightarrow A$
8. $(A \Leftrightarrow B) \Rightarrow A \Rightarrow B$
9. $(A \Leftrightarrow B) \Rightarrow B \Rightarrow A$
10. $(A \Rightarrow B) \Rightarrow (B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$

Exercices en logique du premier ordre

Propositions à démontrer

1. $\forall x.P(x) \Rightarrow \exists y.P(y) \vee Q(y)$
2. $(\exists x.P(x) \vee Q(x)) \Rightarrow (\exists x.P(x)) \vee (\exists x.Q(x))$
3. $(\forall x.P(x)) \wedge (\forall x.Q(x)) \Rightarrow \forall x.P(x) \wedge Q(x)$
4. $(\forall x.P(x) \wedge Q(x)) \Rightarrow (\forall x.P(x)) \wedge (\forall x.Q(x))$
5. $(\forall x.\neg P(x)) \Rightarrow \neg(\exists x.P(x))$
6. $\neg(\forall x.P(x)) \Rightarrow \exists x.\neg P(x)$

Partie TP

Utilisation du logiciel Edukera

- URL : `http://edukera.com/` ;
- Création de compte : email, Google+, ou Facebook ;
- Code pour accéder aux exercices : « 9A01FB4 ».

Démo