Preuves en logique du premier ordre

David Delahaye
David.Delahaye@lirmm.fr

Université de Montpellier
Faculté des Sciences

Licence Informatique L3 2022-2023

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 l'on 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.

Sémantique de la logique classique

Interprétation

- Une interprétation I est un ensemble non vide D_I, appelé le domaine de l'interprétation, muni d'éléments $I(c)$ de D_I pour chaque symbole de constante (fonction d'arité 0), et d'une application $I(P)$ de D_I^n vers $\mathcal{B}$ pour chaque symbole de prédicat P d'arité n.

Affectation

- Une affectation ρ est une application de $\mathcal{V}$ vers D_I ;
- Pour toute affectation ρ, $\rho[v/x]$ est l'affectation envoyant chaque variable y autre que x vers $\rho(y)$, et x vers v.

Sémantique de la logique classique

Définition

- Dans une interprétation I, et modulo l'affectation ρ, la sémantique des formules est définie par :
  - Si $P \in \mathcal{S}_{\mathcal{P}}$ d'arité n et $t_1, \ldots, t_n \in \mathcal{T}$ alors $[\![P(t_1, \ldots, t_n)]\!]^I_\rho = I(P)([\![t_1]\!]^I_\rho, \ldots, [\![t_n]\!]^I_\rho)$;
  - $[\![\top]\!]^I_\rho = T$, $[\![\bot]\!]^I_\rho = F$;
  - Si $\Phi \in \mathcal{F}$ alors $[\![\neg\Phi]\!]^I_\rho = \neg_{\mathcal{B}}[\![\Phi]\!]^I_\rho$;
  - Si $\Phi, \Phi' \in \mathcal{F}$ alors :
    - $[\![\Phi \wedge \Phi']\!]^I_\rho = [\![\Phi]\!]^I_\rho \wedge_{\mathcal{B}} [\![\Phi']\!]^I_\rho$;
    - $[\![\Phi \vee \Phi']\!]^I_\rho = [\![\Phi]\!]^I_\rho \vee_{\mathcal{B}} [\![\Phi']\!]^I_\rho$;
    - $[\![\Phi \Rightarrow \Phi']\!]^I_\rho = [\![\Phi]\!]^I_\rho \Rightarrow_{\mathcal{B}} [\![\Phi']\!]^I_\rho$;
    - $[\![\Phi \Leftrightarrow \Phi']\!]^I_\rho = [\![\Phi]\!]^I_\rho \Leftrightarrow_{\mathcal{B}} [\![\Phi']\!]^I_\rho$.
  - Si $x \in \mathcal{V}$ et $\Phi \in \mathcal{F}$ alors :
    - $[\![\forall x.\Phi]\!]^I_\rho = \bigwedge_{v \in D_I} [\![\Phi]\!]^I_{\rho[v/x]}$;
    - $[\![\exists x.\Phi]\!]^I_\rho = \bigvee_{v \in D_I} [\![\Phi]\!]^I_{\rho[v/x]}$.

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 de Gentzen

Notion de séquent

- Plusieurs types de séquents suivant la logique considérée ;
- Forme générale : $\Gamma \vdash \Delta$
  où $\Gamma, \Delta \equiv$ ensembles de formules ;
- « $\vdash$ » se prononce « thèse » ;
- Sémantique du séquent classique :
  - Si $\Gamma = \phi_1, \ldots, \phi_n$ et $\Delta = \psi_1, \ldots, \psi_m$;
  - $\Gamma \vdash \Delta \equiv \phi_1 \wedge \ldots \wedge \phi_n \Rightarrow \psi_1 \vee \ldots \vee \psi_m$.
- Sémantique du séquent intuitionniste :
  - Si $\Gamma = \phi_1, \ldots, \phi_n$ et $\Delta = \psi$;
  - $\Gamma \vdash \Delta \equiv \phi_1 \wedge \ldots \wedge \phi_n \Rightarrow \psi$.

Gerhard Gentzen (1909-1945)

Calcul des séquents de Gentzen

Système de Gentzen

- Peu d'axiomes et beaucoup de règles de déduction (par rapport aux systèmes à la Frege-Hilbert) ;
- Système symétrique (règles gauches/droites pour chaque connecteur) ;
- Règle de coupure $\equiv$ règle identifiée (pas une combinaison de règles) ;
- Système adapté à la recherche de preuves (méthode des tableaux) ;
- Pour différentes logiques (classique, intuitionniste, linéaire, etc.).

Calcul des séquents de Gentzen

Règle de déduction (règle d'inférence ou de dérivation)

- Règle de la forme :

$$\dfrac{P_1 \qquad P_2 \qquad \ldots \qquad P_n}{C}\ nom$$

où :

  - $P_1, P_2, \ldots, P_n, C$ sont des séquents ;
  - $P_1, P_2, \ldots, P_n$ sont les prémisses de la règle ;
  - C est la conclusion de la règle ;
  - *nom* est le nom de la règle.
- Sémantique :
  - La règle se lit du haut vers le bas ;
  - Si on a P_1, P_2, ..., et P_n, alors on peut en déduire C.
- Si la règle n'a pas de prémisses, elle est appelée règle axiomatique ou plus simplement axiome.

Calcul des séquents de Gentzen

Arbre de preuve (arbre de dérivation)

- On part d'un séquent initial à démontrer ;
- On applique les règles en raisonnement abductif (raisonnement arrière), c'est-à-dire que l'on part de ce qu'on veut montrer pour aller vers les hypothèses/axiomes) ;
- On construit ainsi un arbre dont le séquent est la racine et les branches sont créées par les différentes prémisses des règles de déduction ;
- Dans une branche, on s'arrête lorsqu'on atteint une règle axiomatique, qui devient ainsi une feuille de l'arbre ;
- Un arbre de preuve est un arbre dont toutes les branches se terminent par une règle axiomatique (on parle alors de branche close).

Calcul des séquents intuitionniste (LJ)

Règles

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

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

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

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

Calcul des séquents intuitionniste (LJ)

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 (LJ)

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 ($\mathrm{LJ_{em}}$)

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

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

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

Calcul des séquents classique (LK)

Règles

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

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

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

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

Règles LJ

$$A, B \vdash A \qquad A, B \vdash B$$

$$A, B \vdash A \wedge B$$

$$A \vdash B \Rightarrow A \wedge B$$

$$\vdash A \Rightarrow B \Rightarrow A \wedge B$$

Exemple de preuve propositionnelle dans LJ/LK

Une preuve simple

▸ Règles LJ

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

Exemple de preuve propositionnelle dans LJ/LK

Une preuve simple

Règles LJ

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

Exemple de preuve propositionnelle dans LJ/LK

Une preuve simple

▸ Règles LJ

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

Exemple de preuve propositionnelle dans LJ/LK

Une preuve simple

▸ Règles LJ

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

Exemple de preuve propositionnelle dans LJ/LK

Une preuve simple

Règles LJ

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A}\,\mathrm{ax} \qquad \dfrac{}{A, B \vdash B}\,\mathrm{ax}}{A, B \vdash A \land B}\,\land_{\mathrm{right}}}{A \vdash B \Rightarrow A \land B}\,\Rightarrow_{\mathrm{right}}}{\vdash A \Rightarrow B \Rightarrow A \land B}\,\Rightarrow_{\mathrm{right}}
$$

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

Règles LJ

$$P(x) \vdash P(x)$$

$$P(x) \vdash \exists x.P(x)$$

$$\neg\exists x.P(x), P(x) \vdash \bot$$

$$\neg\exists x.P(x) \vdash \neg P(x)$$

$$\neg\exists x.P(x) \vdash \forall x.\neg P(x)$$

$$\vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x)$$

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

Règles LJ

$$P(x) \vdash P(x)$$
$$P(x) \vdash \exists x.P(x)$$
$$\neg\exists x.P(x), P(x) \vdash \bot$$
$$\neg\exists x.P(x) \vdash \neg P(x)$$
$$\dfrac{\neg\exists x.P(x) \vdash \forall x.\neg P(x)}{\vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x)} \Rightarrow_{\text{right}}$$

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

Règles LJ

$$P(x) \vdash P(x)$$

$$P(x) \vdash \exists x.P(x)$$

$$\neg\exists x.P(x), P(x) \vdash \bot$$

$$\dfrac{\dfrac{\neg\exists x.P(x) \vdash \neg P(x)}{\neg\exists x.P(x) \vdash \forall x.\neg P(x)}\,\forall_{\text{right}}}{\vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x)}\,\Rightarrow_{\text{right}}$$

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

Règles LJ

$$P(x) \vdash P(x)$$

$$P(x) \vdash \exists x.P(x)$$

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

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

Règles LJ

$$P(x) \vdash P(x)$$

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

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

Règles LJ

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

Exemple de preuve au premier ordre dans LJ/LK

Négation et quantificateurs

▸ Règles LJ

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

Attention aux preuves fausses !

Négation et quantificateurs

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(x) \vdash P(x)}{\vdash P(x), \neg P(x)}}{\vdash P(x), \forall x.\neg P(x)}}{\vdash \exists x.P(x), \forall x.\neg P(x)}}{\neg(\exists x.P(x)) \vdash \forall x.\neg P(x)}}{\vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x)}
$$

Cette preuve est fausse car :

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

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Attention aux preuves fausses !

Négation et quantificateurs

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(x) \vdash P(x)}{\vdash P(x), \neg P(x)}}{\vdash P(x), \forall x.\neg P(x)}}{\vdash \exists x.P(x), \forall x.\neg P(x)}}{\neg(\exists x.P(x)) \vdash \forall x.\neg P(x)}}{\vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x)} \Rightarrow_{\text{right}}$$

Cette preuve est fausse car :

$$\dfrac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)} \forall_{\text{right}}, \ x \notin \Gamma, \Delta$$

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Attention aux preuves fausses !

Négation et quantificateurs

$$\dfrac{\dfrac{\begin{array}{c} P(x) \vdash P(x) \\ \vdash P(x), \neg P(x) \\ \vdash P(x), \forall x.\neg P(x) \\ \vdash \exists x.P(x), \forall x.\neg P(x) \end{array}}{\neg(\exists x.P(x)) \vdash \forall x.\neg P(x)}\neg_{\text{left}}}{\vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x)}\Rightarrow_{\text{right}}$$

Cette preuve est fausse car :

$$\dfrac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)}\forall_{\text{right}},\ \ x \notin \Gamma, \Delta$$

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Attention aux preuves fausses !

Négation et quantificateurs

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

Cette preuve est fausse car :

$$\dfrac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)}\,\forall_{\text{right}},\quad x \notin \Gamma, \Delta$$

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Attention aux preuves fausses !

Négation et quantificateurs

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

Cette preuve est fausse car :

$$
\dfrac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)}\forall_{\text{right}},\quad x \notin \Gamma, \Delta
$$

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Attention aux preuves fausses !

Négation et quantificateurs

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

Cette preuve est fausse car :

$$\dfrac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)}\ \forall_{\text{right}},\ \ x \notin \Gamma, \Delta$$

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Attention aux preuves fausses !

Négation et quantificateurs

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

Cette preuve est fausse car :

$$\dfrac{\Gamma \vdash \Delta, A(x)}{\Gamma \vdash \Delta, \forall x.A(x)}\forall_{\text{right}},\ x \notin \Gamma, \Delta$$

Et ici $x \in \Delta = P(x)$.

Donc attention aux conditions d'application des règles !

Quelle stratégie de preuve ?

Le nerf de la guerre : les quantificateurs

- Aucune stratégie pour les connecteurs, si ce n'est d'utiliser en priorité les règles qui ne branchent pas ;
- Pour les quantificateurs, utiliser les règles de Skolémisation en priorité ($\forall_{\text{right}}$, $\exists_{\text{left}}$), puis les règles d'instanciation ($\exists_{\text{right}}$, $\forall_{\text{left}}$) ;
- Les règles de Skolémisation donnent des variables qui peuvent être ensuite utilisées par les règles instanciation ;
- Les variables de Skolémisation peuvent être utilisées telles quelles ou dans des termes plus complexes (dans des applications de fonctions) ;
- Dans des cas rares, une instanciation factice peut être requise en priorité pour « dégager » une Skolémisation, mais c'est rare (voir la preuve du paradoxe des buveurs).

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 construire 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

Règles LK

$$\Gamma \vdash P(a), P(a) \wedge P(b) \qquad \Gamma \vdash P(b), P(a) \wedge P(b)$$

$$\Gamma = P(a), P(b) \vdash P(a) \wedge P(b), P(a) \wedge P(b)$$

$$P(a) \vdash P(a) \wedge P(b), P(b) \Rightarrow P(a) \wedge P(b)$$

$$P(a) \vdash P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)$$

$$\vdash P(a) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)$$

$$\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)$$

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

Un autre exemple de preuve en logique classique

Preuve dans LK

Règles LK

$$\Gamma \vdash P(a), P(a) \wedge P(b) \qquad \Gamma \vdash P(b), P(a) \wedge P(b)$$

$$\Gamma = P(a), P(b) \vdash P(a) \wedge P(b), P(a) \wedge P(b)$$

$$P(a) \vdash P(a) \wedge P(b), P(b) \Rightarrow P(a) \wedge P(b)$$

$$P(a) \vdash P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)$$

$$\vdash P(a) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)$$

$$\dfrac{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b)}\ \mathrm{cont}_{\mathrm{right}}$$

Un autre exemple de preuve en logique classique

Preuve dans LK

▸ Règles LK

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

Un autre exemple de preuve en logique classique

Preuve dans LK

Règles LK

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

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

Un autre exemple de preuve en logique classique

Preuve dans LK

▸ Règles LK

$$\Gamma \vdash P(a), P(a) \wedge P(b) \qquad \Gamma \vdash P(b), P(a) \wedge P(b)$$

$$\Gamma = P(a), P(b) \vdash P(a) \wedge P(b), P(a) \wedge P(b)$$

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

Un autre exemple de preuve en logique classique

Preuve dans LK

▸ Règles LK

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

Un autre exemple de preuve en logique classique

Preuve dans LK

▸ Règles LK

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

Un autre exemple de preuve en logique classique

Preuve dans LK

▸ Règles LK

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

Un autre exemple de preuve en logique classique

Preuve dans LK

▸ Règles LK

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

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

$$P(x), P(y) \vdash P(y), \forall y.P(y)$$
$$P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)$$
$$P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash \exists x.P(x) \Rightarrow \forall y.P(y)$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

Règles LK

$$P(x), P(y) \vdash P(y), \forall y.P(y)$$
$$P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)$$
$$P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash \exists x.P(x) \Rightarrow \forall y.P(y)$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

Règles LK

$$P(x), P(y) \vdash P(y), \forall y.P(y)$$
$$P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)$$
$$P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$
$$\dfrac{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)}\ \mathrm{cont}_{\mathrm{right}}$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

Règles LK

$$P(x), P(y) \vdash P(y), \forall y.P(y)$$

$$P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)$$

$$P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$

$$P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$

$$\dfrac{\dfrac{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\ \exists_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)}\ \text{cont}_{\text{right}}$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

Règles LK

$$P(x), P(y) \vdash P(y), \forall y.P(y)$$

$$P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)$$

$$P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)$$

$$\dfrac{\dfrac{\dfrac{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \Rightarrow_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \exists_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)} \text{cont}_{\text{right}}$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

▸ Règles LK

$$P(x), P(y) \vdash P(y), \forall y.P(y)$$

$$P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\,\forall_{\text{right}}}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\,\Rightarrow_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\,\exists_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)}\,\text{cont}_{\text{right}}$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

Règles LK

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(x), P(y) \vdash P(y), \forall y.P(y)}{P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)}}{P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\exists_{\text{right}}}{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\forall_{\text{right}}}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\Rightarrow_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\exists_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)}\text{cont}_{\text{right}}$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

▸ Règles LK

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(x), P(y) \vdash P(y), \forall y.P(y)}{P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)}\Rightarrow_{\text{right}}}{P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\exists_{\text{right}}}{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\forall_{\text{right}}}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\Rightarrow_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\exists_{\text{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)}\text{cont}_{\text{right}}
$$

Une preuve classique un peu plus complexe

Paradoxe (pas si paradoxal) des buveurs

Énoncé : « Il y a quelqu'un dans un bar tel que, s'il boit alors tout le monde dans le bar boit ».

▸ Règles LK

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(x), P(y) \vdash P(y), \forall y.P(y)}\ \mathrm{ax}}{P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)}\ \Rightarrow_{\mathrm{right}}}{P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\ \exists_{\mathrm{right}}}{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\ \forall_{\mathrm{right}}}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\ \Rightarrow_{\mathrm{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}\ \exists_{\mathrm{right}}}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y)}\ \mathrm{cont}_{\mathrm{right}}
$$

Outil d'aide à la preuve Coq

Caractéristiques

- Développement par l'équipe Inria πr^2 ;
- Preuve de programmes fonctionnels ;
- Théorie des types (calcul des constructions inductives) ;
- Isomorphisme de Curry-Howard (objets preuves).

Implantation

- Premières versions milieu des années 80 ;
- Implantation actuelle en OCaml ;
- Preuve interactive (peu d'automatisation) ;
- En ligne de commande ou avec l'interface graphique CoqIDE.

Installation

- Tout est indiqué ici : `https://coq.inria.fr/`.

Logique propositionnelle

Exemples de preuves

- Implication :

```
Coq < Parameter A : Prop.
A is assumed

Coq < Goal A -> A.
1 subgoal

  ============================
   A -> A
```

Logique propositionnelle

Exemples de preuves

- Implication :

```
Coq < intro.
1 subgoal

  H : A
  ============================
   A
```

Logique propositionnelle

Exemples de preuves

- Implication :

```
Coq < assumption.
No more subgoals.

Coq < Save my_thm.
intro.
assumption.
my_thm is defined
```

Logique propositionnelle

Exemples de preuves

- Application (modus ponens) :

```
Coq < Parameters A B : Prop.
A is assumed
B is assumed

Coq < Goal (A -> B) -> A -> B.
1 subgoal

  ============================
   (A -> B) -> A -> B
```

Logique propositionnelle

Exemples de preuves

- Application (modus ponens) :

```
Coq < intros.
1 subgoal

  H : A -> B
  H0 : A
  ============================
   B

Coq < apply (H H0).
No more subgoals.
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < Parameters A B : Prop.
A is assumed
B is assumed

Coq < Goal A /\ B -> A.
1 subgoal


  ============================
   A /\ B -> A
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < intro.
1 subgoal

  H : A /\ B
  ============================
   A
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < elim H.
1 subgoal

  H : A /\ B
  ============================
   A -> B -> A
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < intros.
1 subgoal

  H : A /\ B
  H0 : A
  H1 : B
  ============================
   A

Coq < assumption.
No more subgoals.
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < Parameters A B : Prop.
A is assumed
B is assumed

Coq < Goal A -> A \/ B.
1 subgoal

  ============================
   A -> A \/ B
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < intro.
1 subgoal

  H : A
  ============================
   A \/ B
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\wedge$ et $\vee$:

```
Coq < left.
1 subgoal

  H : A
  ============================
   A

Coq < assumption.
No more subgoals.
```

Logique propositionnelle

Exemples de preuves

- Connecteurs $\neg$:

```
Coq < Parameters A B : Prop.
A is assumed
B is assumed

Coq < Goal A -> ~A -> False.
1 subgoal

  ============================
   A -> ~ A -> False
```

Logique propositionnelle

Exemples de preuves

- Connecteurs ¬ :

```
Coq < intros.
1 subgoal

  H : A
  H0 : ~ A
  ============================
   False

Coq < apply (H0 H).
No more subgoals.
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∀ :

```
Coq < Parameter E : Set.
E is assumed

Coq < Parameter P : E -> Prop.
P is assumed

Coq < Goal forall x : E, (P x) -> (P x).
1 subgoal

  ============================
   forall x : E, P x -> P x
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\forall$:

```
Coq < intros.
1 subgoal

  x : E
  H : P x
  ============================
   P x

Coq < assumption.
No more subgoals.
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\forall$:

```
Coq < Parameter E : Set.
E is assumed

Coq < Parameter a : E.
a is assumed

Coq < Parameter P : E -> Prop.
P is assumed

Coq < Goal (forall x : E, (P x)) -> (P a).
1 subgoal

  ============================
   (forall x : E, P x) -> P a
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∀ :

```
Coq < intro.
1 subgoal

  H : forall x : E, P x
  ============================
   P a

Coq < apply H.
No more subgoals.
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\exists$:

```
Coq < Parameter E : Set.
E is assumed

Coq < Parameter a : E.
a is assumed

Coq < Parameter P : E -> Prop.
P is assumed

Coq < Goal (P a) -> exists x : E, (P x).
1 subgoal

  ============================
   P a -> exists x : E, P x
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\exists$:

```
Coq < intro.
1 subgoal

  H : P a
  ============================
   exists x : E, P x
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∃ :

```
Coq < exists a.
1 subgoal

  H : P a
  ============================
   P a

Coq < assumption.
No more subgoals.
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∃ :

```
Coq < Parameter E : Set.
E is assumed

Coq < Parameter a : E.
a is assumed

Coq < Parameter P : E -> Prop.
P is assumed
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\exists$:

```
Coq < Goal (exists x : E, ~(P x)) ->
           ~(forall x : E, (P x)).
1 subgoal

  ============================
   (exists x : E, ~ P x) -> ~ (forall x : E, P x)
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\exists$:

```
Coq < intros.
1 subgoal

  H : exists x : E, ~ P x
  ============================
   ~ (forall x : E, P x)

Coq < red.
1 subgoal

  H : exists x : E, ~ P x
  ============================
   (forall x : E, P x) -> False
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∃ :

```
Coq < intro.
1 subgoal

  H : exists x : E, ~ P x
  H0 : forall x : E, P x
  ============================
   False
```

Logique du premier ordre

Exemples de preuves

- Quantificateur $\exists$:

```
Coq < elim H.
1 subgoal

  H : exists x : E, ~ P x
  H0 : forall x : E, P x
  ============================
   forall x : E, ~ P x -> False
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∃ :

```
Coq < intros.
1 subgoal

  H : exists x : E, ~ P x
  H0 : forall x : E, P x
  x : E
  H1 : ~ P x
  ============================
   False
```

Logique du premier ordre

Exemples de preuves

- Quantificateur ∃ :

```
Coq < apply H1.
1 subgoal

  H : exists x : E, ~ P x
  H0 : forall x : E, P x
  x : E
  H1 : ~ P x
  ============================
   P x

Coq < apply H0.
No more subgoals.
```

Guide de survie du petit Coq-uin

Correspondance LK/Coq

Logique propositionnelle		Logique du premier ordre	
Règle LK	Tactique Coq	Règle LK	Tactique Coq
ax	`assumption`	$\forall_{\text{right}}$	`intro`
cut	`cut`	$\forall_{\text{left}}$	`apply`
$\Rightarrow_{\text{right}}$	`intro`	$\exists_{\text{right}}$	`exists`
$\Rightarrow_{\text{left}}$	`apply`	$\exists_{\text{left}}$	`elim`
$\Leftrightarrow_{\text{right}}$	`split`		
$\Leftrightarrow_{\text{lefti}}$	`elim`		
$\wedge_{\text{right}}$	`split`		
$\wedge_{\text{left}}$	`elim`		
$\vee_{\text{right1}}$	`left`		
$\vee_{\text{right2}}$	`right`		
$\vee_{\text{left}}$	`elim`		
$\neg_{\text{right}}$	`intro`		
$\neg_{\text{left}}$	`elimtype False` + `apply`		
$\top_{\text{right}}$, $\bot_{\text{left}}$	`auto`		