

# Preuves en logique du premier ordre

David Delahaye

[David.Delahaye@lirmm.fr](mailto:David.Delahaye@lirmm.fr)

Université de Montpellier  
Faculté des Sciences

Licence Informatique L3 2021-2022



# 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  $m : \mathcal{S}_{\mathcal{F}} \cup \mathcal{S}_{\mathcal{P}} \rightarrow \mathbb{N}$ .

## 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  $t_1, \dots, t_n \in \mathcal{T}$ , alors  $f(t_1, \dots, t_n) \in \mathcal{T}$ .

# 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  $m : \mathcal{S}_{\mathcal{F}} \cup \mathcal{S}_{\mathcal{P}} \rightarrow \mathbb{N}$ .

## Formules du premier ordre

- Plus petit ensemble  $\mathcal{F}$  t.q. :
  - ▶ Si  $P \in \mathcal{S}_{\mathcal{P}}$  d'arité  $n$  et  $t_1, \dots, t_n \in \mathcal{T}$ , alors  $P(t_1, \dots, t_n) \in \mathcal{F}$  ;
  - ▶  $\perp, \top \in \mathcal{F}$  ;
  - ▶ 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  $\rho$  est une application de  $\mathcal{V}$  vers  $D_I$  ;
- Pour toute affectation  $\rho$ ,  $\rho[v/x]$  est l'affectation envoyant chaque variable  $y$  autre que  $x$  vers  $\rho(y)$ , et  $x$  vers  $v$ .

## Définition

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

# Systèmes de preuves

## Plusieurs systèmes

- Systèmes à la Frege-Hilbert ;
- Systèmes à la Gentzen :
  - ▶ Dédution 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  $\Gamma = \phi_1, \dots, \phi_n$  et  $\Delta = \psi_1, \dots, \psi_m$  ;
  - ▶  $\Gamma \vdash \Delta \equiv \phi_1 \wedge \dots \wedge \phi_n \Rightarrow \psi_1 \vee \dots \vee \psi_m$ .
- Sémantique du séquent intuitionniste :
  - ▶ Si  $\Gamma = \phi_1, \dots, \phi_n$  et  $\Delta = \psi$  ;
  - ▶  $\Gamma \vdash \Delta \equiv \phi_1 \wedge \dots \wedge \phi_n \Rightarrow \psi$ .



Gerhard Gentzen (1909-1945)



## 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 :

$$\frac{P_1 \quad P_2 \quad \dots \quad P_n}{C} \text{ nom}$$

où :

- ▶  $P_1, P_2, \dots, P_n, C$  sont des séquents ;
- ▶  $P_1, P_2, \dots, P_n$  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  $P_1, P_2, \dots$ , 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

$$\frac{}{\Gamma, A \vdash A} \text{ax}$$

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

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

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

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

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

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

# Calcul des séquents intuitionniste (LJ)

## Règles

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

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge_{\text{right}}$$

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

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

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee_{\text{right2}}$$

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

$$\frac{\Gamma, A \vdash \perp}{\Gamma \vdash \neg A} \neg_{\text{right}}$$

$$\frac{}{\Gamma, \perp \vdash A} \perp_{\text{left}}$$

$$\frac{}{\Gamma \vdash \top} \top_{\text{right}}$$

# Calcul des séquents intuitionniste (LJ)

## Règles

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

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

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

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists_{\text{right}}$$

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

# Calcul des séquents classique ( $\text{LJ}_{\text{em}}$ )

## Règles

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

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

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

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x. A(x)} \exists_{\text{right}}$$

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

$$\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A} \text{em}$$

# Calcul des séquents classique (LK)

## Règles

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

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

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

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



# Calcul des séquents classique (LK)

## Règles

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

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

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

# Calcul des séquents classique (LK)

## Règles

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

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

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

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

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

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

$$\frac{}{\Gamma, \perp \vdash \Delta} \perp_{\text{left}}$$

$$\frac{}{\Gamma \vdash \Delta, \top} \top_{\text{right}}$$

# Calcul des séquents classique (LK)

## Règles

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

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

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

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

# Exemple de preuve propositionnelle dans LJ/LK

## Une preuve simple

### ▸ Règles LJ

$$A, B \vdash A \quad A, B \vdash B$$

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

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

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

# Exemple de preuve propositionnelle dans LJ/LK

## Une preuve simple

### ▸ Règles LJ

$$\frac{\begin{array}{c} A, B \vdash A \quad A, B \vdash B \\ A, B \vdash A \wedge B \\ A \vdash B \Rightarrow A \wedge B \end{array}}{\vdash A \Rightarrow B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}$$

# Exemple de preuve propositionnelle dans LJ/LK

## Une preuve simple

### ▸ Règles LJ

$$\frac{\frac{A, B \vdash A \quad A, B \vdash B}{A, B \vdash A \wedge B} \Rightarrow_{\text{right}}}{\frac{A \vdash B \Rightarrow A \wedge B}{\vdash A \Rightarrow B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}}$$

# Exemple de preuve propositionnelle dans LJ/LK

## Une preuve simple

### ▸ Règles LJ

$$\frac{\frac{\frac{A, B \vdash A \quad A, B \vdash B}{A, B \vdash A \wedge B} \wedge_{\text{right}}}{A \vdash B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}}{\vdash A \Rightarrow B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}$$

# Exemple de preuve propositionnelle dans LJ/LK

## Une preuve simple

### ▸ Règles LJ

$$\frac{\frac{\frac{\overline{A, B \vdash A}^{\text{ax}} \quad A, B \vdash B}{A, B \vdash A \wedge B} \wedge_{\text{right}}}{A \vdash B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}}{\vdash A \Rightarrow B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}$$



# Exemple de preuve propositionnelle dans LJ/LK

## Une preuve simple

### ▸ Règles LJ

$$\frac{\frac{\frac{}{A, B \vdash A} \text{ax} \quad \frac{}{A, B \vdash B} \text{ax}}{A, B \vdash A \wedge B} \wedge_{\text{right}}}{\frac{}{A \vdash B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}} \Rightarrow_{\text{right}} \frac{}{\vdash A \Rightarrow B \Rightarrow A \wedge B} \Rightarrow_{\text{right}}$$

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

### ▸ Règles LJ

$$\begin{array}{l} P(x) \vdash P(x) \\ P(x) \vdash \exists x.P(x) \\ \neg\exists x.P(x), P(x) \vdash \perp \\ \neg\exists x.P(x) \vdash \neg P(x) \\ \neg\exists x.P(x) \vdash \forall x.\neg P(x) \\ \vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x) \end{array}$$

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

### ▸ Règles LJ

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

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

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

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

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

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

### ▸ Règles LJ

$$\begin{array}{c} P(x) \vdash P(x) \\ P(x) \vdash \exists x.P(x) \\ \neg \exists x.P(x), P(x) \vdash \perp \\ \hline \neg \exists x.P(x) \vdash \neg P(x) \\ \hline \neg \exists x.P(x) \vdash \forall x.\neg P(x) \quad \forall_{\text{right}} \\ \hline \vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x) \quad \Rightarrow_{\text{right}} \end{array}$$

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

### ▸ Règles LJ

$$\begin{array}{c} P(x) \vdash P(x) \\ P(x) \vdash \exists x.P(x) \\ \hline \frac{\neg \exists x.P(x), P(x) \vdash \perp}{\neg \exists x.P(x) \vdash \neg P(x)} \neg_{\text{right}} \\ \hline \frac{\neg \exists x.P(x) \vdash \neg P(x)}{\neg \exists x.P(x) \vdash \forall x.\neg P(x)} \forall_{\text{right}} \\ \hline \vdash \neg(\exists x.P(x)) \Rightarrow \forall x.\neg P(x) \Rightarrow_{\text{right}} \end{array}$$

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

### ▸ Règles LJ

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

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

### ► Règles LJ

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

# Exemple de preuve au premier ordre dans LJ/LK

## Négation et quantificateurs

► Règles LJ

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



# Attention aux preuves fausses !

## Négation et quantificateurs

$$\begin{aligned} &P(x) \vdash P(x) \\ &\vdash P(x), \neg P(x) \\ &\vdash P(x), \forall x. \neg P(x) \\ &\vdash \exists x. P(x), \forall x. \neg P(x) \\ &\neg(\exists x. P(x)) \vdash \forall x. \neg P(x) \\ &\vdash \neg(\exists x. P(x)) \Rightarrow \forall x. \neg P(x) \end{aligned}$$

Cette preuve est fausse car :

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

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

Donc attention aux conditions d'application des règles !

# Attention aux preuves fausses !

## Négation et quantificateurs

$$\begin{array}{l} P(x) \vdash P(x) \\ \vdash P(x), \neg P(x) \\ \vdash P(x), \forall x. \neg P(x) \\ \vdash \exists x. P(x), \forall x. \neg P(x) \\ \frac{\neg(\exists x. P(x)) \vdash \forall x. \neg P(x)}{\vdash \neg(\exists x. P(x)) \Rightarrow \forall x. \neg P(x)} \Rightarrow_{\text{right}} \end{array}$$

Cette preuve est fausse car :

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

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

Donc attention aux conditions d'application des règles !

# Attention aux preuves fausses !

## Négation et quantificateurs

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

Cette preuve est fausse car :

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

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

Donc attention aux conditions d'application des règles !

# Attention aux preuves fausses !

## Négation et quantificateurs

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

Cette preuve est fausse car :

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

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

Donc attention aux conditions d'application des règles !

# Attention aux preuves fausses !

## Négation et quantificateurs

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

Cette preuve est fausse car :

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

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

Donc attention aux conditions d'application des règles !

# Attention aux preuves fausses !

## Négation et quantificateurs

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

Cette preuve est fausse car :

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

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

Donc attention aux conditions d'application des règles !

# Attention aux preuves fausses !

## Négation et quantificateurs

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

Cette preuve est fausse car :

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

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 d'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  $t_1, t_2, \dots, t_n$  tels que  $P(t_1) \vee P(t_2) \vee \dots \vee P(t_n)$  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

$$\begin{array}{l} \Gamma \vdash P(a), P(a) \wedge P(b) \quad \Gamma \vdash P(b), P(a) \wedge P(b) \\ \Gamma = P(a), P(b) \vdash P(a) \wedge P(b), P(a) \wedge P(b) \\ P(a) \vdash P(a) \wedge P(b), P(b) \Rightarrow P(a) \wedge P(b) \\ P(a) \vdash P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b) \\ \vdash P(a) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b) \\ \vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b) \\ \vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b) \end{array}$$

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ▸ Règles LK

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

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

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

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

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

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

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ▸ Règles LK

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

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

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

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

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

$$\frac{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b)} \begin{array}{l} \exists_{\text{right}} \\ \text{cont}_{\text{right}} \end{array}$$

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ▸ Règles LK

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

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

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

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

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

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

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ▸ Règles LK

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

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

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

$$\frac{P(a) \vdash P(a) \wedge P(b), P(b) \Rightarrow P(a) \wedge P(b)}{P(a) \vdash P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)} \exists_{\text{right}}$$

$$\frac{\vdash P(a) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}{\vdash P(a) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)} \Rightarrow_{\text{right}}$$

$$\frac{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b), \exists x.P(x) \Rightarrow P(a) \wedge P(b)}{\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b)} \exists_{\text{right}}$$

$$\vdash \exists x.P(x) \Rightarrow P(a) \wedge P(b) \quad \text{cont}_{\text{right}}$$



# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ► Règles LK

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

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

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ► Règles LK

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

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ► Règles LK

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

# Un autre exemple de preuve en logique classique

## Preuve dans LK

### ► Règles LK

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

# 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 ».

$$\begin{aligned} &P(x), P(y) \vdash P(y), \forall y.P(y) \\ &P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y) \\ &P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ &P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ &\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ &\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ &\vdash \exists x.P(x) \Rightarrow \forall y.P(y) \end{aligned}$$

# 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

$$\begin{array}{l} P(x), P(y) \vdash P(y), \forall y.P(y) \\ P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y) \\ P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \vdash \exists x.P(x) \Rightarrow \forall y.P(y) \end{array}$$

# 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

$$\begin{array}{c} P(x), P(y) \vdash P(y), \forall y.P(y) \\ P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y) \\ P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \quad \text{cont}_{\text{right}} \\ \vdash \exists x.P(x) \Rightarrow \forall y.P(y) \end{array}$$

# 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

$$\begin{array}{c} P(x), P(y) \vdash P(y), \forall y.P(y) \\ P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y) \\ P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \hline \vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y) \end{array} \begin{array}{l} \\ \\ \\ \\ \exists_{\text{right}} \\ \text{cont}_{\text{right}} \end{array}$$



# 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

$$\begin{array}{c} P(x), P(y) \vdash P(y), \forall y.P(y) \\ P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y) \\ P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \hline \frac{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \Rightarrow_{\text{right}} \\ \hline \frac{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \exists_{\text{right}} \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y) \quad \text{cont}_{\text{right}} \end{array}$$

# 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

$$\begin{array}{c} P(x), P(y) \vdash P(y), \forall y.P(y) \\ P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y) \\ \hline P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \\ \hline P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \quad \forall_{\text{right}} \\ \hline \vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \quad \Rightarrow_{\text{right}} \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y) \quad \exists_{\text{right}} \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y) \quad \text{cont}_{\text{right}} \end{array}$$

# 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

$$\begin{array}{c} P(x), P(y) \vdash P(y), \forall y.P(y) \\ \hline \frac{P(x) \vdash P(y), P(y) \Rightarrow \forall y.P(y)}{P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \exists_{\text{right}} \\ \hline \frac{P(x) \vdash P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \forall_{\text{right}} \\ \hline \frac{P(x) \vdash \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \Rightarrow_{\text{right}} \\ \hline \frac{\vdash P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)}{\vdash \exists x.P(x) \Rightarrow \forall y.P(y), \exists x.P(x) \Rightarrow \forall y.P(y)} \exists_{\text{right}} \\ \hline \vdash \exists x.P(x) \Rightarrow \forall y.P(y) \quad \text{cont}_{\text{right}} \end{array}$$

# 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

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



# Outil d'aide à la preuve Coq

## Caractéristiques

- Développement par l'équipe Inria  $\pi r^2$  ;
- 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
```

## Exemples de preuves

- Implication :

```
Coq < intro.
```

```
1 subgoal
```

```
H : A
```

```
=====
```

```
A
```



## 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
```

## 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  $\vee$  B.
```

```
1 subgoal
```

```
=====
```

```
A -> A  $\vee$  B
```



## Exemples de preuves

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

```
Coq < intro.
```

```
1 subgoal
```

```
H : A
```

```
=====
```

```
A  $\vee$  B
```

## 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  $\neg$  :

```
Coq < intros.
```

```
1 subgoal
```

```
H : A
```

```
H0 : ~ A
```

```
=====
```

```
False
```

```
Coq < apply (H0 H).
```

```
No more subgoals.
```

# Logique du premier ordre

## Exemples de preuves

- Quantificateur  $\forall$  :

```
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  $\forall$  :

```
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  $\exists$  :

Coq < exists a.

1 subgoal

H : P a

=====

P a

Coq < assumption.

No more subgoals.

## 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

# 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  $\exists$  :

```
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  $\exists$  :

```
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  $\exists$  :

Coq < apply H1.

1 subgoal

H : exists x : E,  $\sim$  P x

H0 : forall x : E, P x

x : E

H1 :  $\sim$  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		
$\Leftrightarrow_{\text{left}}$	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		
$\top_{\text{right}}, \perp_{\text{left}}$	auto		