Cours 7

Calcul propositionnel : déduction naturelle

Déduction naturelle (Gentzen)

Système de déduction :

$$\Gamma \vdash A$$

La formule A est prouvable à partir de l'ensemble de formules Γ

L'ensemble des *preuves* $\Gamma \vdash A$ est définie inductivement comme l'ensemble des couples (Γ, A)

- tels que $A \in \Gamma$ $\quad \text{ax}\dfrac{}{\Gamma, A \vdash A}$
- obtenus à partir d'autres preuves par des règles de déduction de la forme $\dfrac{\textit{hypotheses}}{\textit{conclusions}}$ (voir suite)

Notations :

$$\Gamma, A \;=\; \Gamma \cup \{A\} \qquad\qquad \Gamma, \Delta \;=\; \Gamma \cup \Delta$$

Logique minimale (NM)

$$\text{intro}_{\Rightarrow}\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \text{elim}_{\Rightarrow}\ \frac{\Gamma \vdash A \quad \Delta \vdash A \Rightarrow B}{\Gamma, \Delta \vdash B}$$

$$\text{intro}_{\wedge}\ \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}$$

$$\text{elim}^1_{\wedge}\ \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \text{elim}^2_{\wedge}\ \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\text{intro}^1_{\vee}\ \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \text{intro}^2_{\vee}\ \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

$$\text{elim}_{\vee}\ \frac{\Gamma \vdash A \vee B \quad \Delta, A \vdash C \quad \Delta', B \vdash C}{\Gamma, \Delta, \Delta' \vdash C}$$

Exemple

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

Exemple

$$\dfrac{\dfrac{}{a \wedge b \vdash b \wedge a}}{\vdash (a \wedge b) \Rightarrow (b \wedge a)}\, i_{\Rightarrow}$$

Exemple

$$\dfrac{\dfrac{\dfrac{}{a \wedge b \vdash b} \qquad \dfrac{}{a \wedge b \vdash a}}{a \wedge b \vdash b \wedge a}\, i_{\wedge}}{\vdash (a \wedge b) \Rightarrow (b \wedge a)}\, i_{\Rightarrow}$$

Exemple

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \wedge b \vdash a \wedge b}}{a \wedge b \vdash b}\, e^2_\wedge \qquad \dfrac{}{a \wedge b \vdash a}}{a \wedge b \vdash b \wedge a}\, i_\wedge}{\vdash (a \wedge b) \Rightarrow (b \wedge a)}\, i_\Rightarrow$$

Exemple

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \wedge b \vdash a \wedge b}\,Ax}{a \wedge b \vdash b}\,e^2_\wedge \qquad \dfrac{}{a \wedge b \vdash a}}{a \wedge b \vdash b \wedge a}\,i_\wedge}{\vdash (a \wedge b) \Rightarrow (b \wedge a)}\,i_\Rightarrow$$

Exemple

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \wedge b \vdash a \wedge b}\,Ax}{a \wedge b \vdash b}\,e^2_\wedge \qquad \dfrac{\dfrac{}{a \wedge b \vdash a \wedge b}}{a \wedge b \vdash a}\,e^1_\wedge}{a \wedge b \vdash b \wedge a}\,i_\wedge}{\vdash (a \wedge b) \Rightarrow (b \wedge a)}\,i_\Rightarrow$$

Exemple

$$\dfrac{\dfrac{\dfrac{\dfrac{}{a \wedge b \vdash a \wedge b}\,Ax}{a \wedge b \vdash b}\,e^2_\wedge \qquad \dfrac{\dfrac{}{a \wedge b \vdash a \wedge b}\,Ax}{a \wedge b \vdash a}\,e^1_\wedge}{a \wedge b \vdash b \wedge a}\,i_\wedge}{\vdash (a \wedge b) \Rightarrow (b \wedge a)}\,i_\Rightarrow$$

Logique intuitionniste (NJ)

Deux nouvelles règles :

$$\text{intro}_\neg \frac{\Gamma, A \vdash \neg B \qquad \Delta, A \vdash B}{\Gamma, \Delta \vdash \neg A} \qquad \text{elim}_\neg \frac{\Gamma \vdash \neg A \qquad \Delta \vdash A}{\Gamma, \Delta \vdash B}$$

De manière équivalente, on ajoute le symbole $\bot$ (= absurde), et la règle

$$\text{elim}_\bot \frac{\Gamma \vdash \bot}{\Gamma \vdash A} \qquad \textit{ex falso quodlibet sequitur}$$

et $\neg A$ devient une abréviation de $A \Rightarrow \bot$.

Logique intuitionniste (NJ)

Exercice : Prouver $(a \Rightarrow b) \Rightarrow (\neg b \Rightarrow \neg a)$ en logique minimale.

Exercice : intro$_\neg$ est dérivable dans NM.

Remarque : elim$_\neg$ est *équivalent* à elim$_\bot$.

NJ est *plus forte* que NM :

$$\Gamma \vdash_{NM} A \text{ implique } \Gamma \vdash_{NJ} A$$

Logique classique (NK)

On ajoute un nouveau moyen d'inférence : le *tiers exclus*.

3 règles possibles :

$$\text{TE}\,\frac{}{\Gamma \vdash A \vee \neg A} \qquad \text{abs}\,\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A} \qquad \text{elim}_{\neg\neg}\,\frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

NK strictement plus forte que NJ : il existe des formules sans négation dérivables dans NK et pas dans NJ.

$$\vdash_{NK} ((p \Rightarrow q) \Rightarrow p) \Rightarrow p \qquad \text{(loi de Peirce)}$$

NK *vs* NJ

Tautologies prouvables dans NK :

$$\vdash_{NK} (A \vee B) \iff \neg(\neg A \wedge \neg B)$$
$$\vdash_{NK} (A \Rightarrow B) \iff (\neg A \vee B)$$
$$\vdash_{NK} (A \wedge B) \iff \neg(\neg A \vee \neg B)$$

Dans NJ on ne peut en prouver qu'un sens.

Traduction de NK vers NJ

Définition

Soient $\mathcal{L}$ et $\mathcal{L}'$ deux logiques, $\mathcal{L}$ plus forte que $\mathcal{L}'$, et φ associant à toute formule de $\mathcal{L}$ une formule de $\mathcal{L}'$. φ est une *traduction* de $\mathcal{L}$ vers $\mathcal{L}'$ si pour toute formule A de $\mathcal{L}$ on a :

- $\vdash_{\mathcal{L}} A \iff \varphi(A)$
- si $\vdash_{\mathcal{L}} A$ alors $\vdash_{\mathcal{L}'} \varphi(A)$

Traduction de NK vers NJ (Glivenko 1929) : $\varphi(A) = \neg\neg A$
(ça ne marche pas avec le calcul des prédicats).

Correction et complétude

Théorème (Correction)

Si $\Gamma \vdash_{NM} A$, *alors* $\Gamma \models A$.
Si $\Gamma \vdash_{NJ} A$, *alors* $\Gamma \models A$.
Si $\Gamma \vdash_{NK} A$, *alors* $\Gamma \models A$.

Théorème (Complétude)

Si $\Gamma \models A$, *alors* $\Gamma \vdash_{NK} A$.

Preuve de complétude

Nous le considérons le système de connecteur complet $\{\neg, \Rightarrow\}$. Nous ne prouvons la complétude de $\vdash_{NK}$ que pour les formules ne contenant que les connecteurs $\neg$ et $\Rightarrow$. Attention, cela ne prouve pas la complétude pour les formules comportant d'autres connecteurs !

$$\begin{aligned}\mu(A) = \ & \text{nombre}^1 \text{ d'occurrence de } \neg \text{ dans } A \\ & + 2\times \text{ nombre d'occurrence de } \Rightarrow \text{ dans } A\end{aligned}$$

$$\mu(\Gamma, A) = \mu(A) + \sum_{F\in\Gamma} \mu(F)$$

Nous montrons par récurrence sur $n \in \mathbb{N}$,

$$\begin{aligned}\mathcal{P}(n) = \ & \text{"pour tout } \Gamma, A \text{ tels que } \mu(\Gamma, A) = n, \\ & \Gamma \models A \text{ implique } \Gamma \vdash_{NK} A\text{"}\end{aligned}$$

[1] Nous supposons /*Gamma* fini.

Hypothèse de récurrence forte (HR) :

$$\text{pour tout } k \in \mathbb{N},\ k < n \text{ implique } \mathcal{P}(k)$$

Nous supposons : $\Gamma \models A$ et $\mu(\Gamma, A) = n$

Étude de cas sur la forme de A :

- $A = \neg\neg A'$
- $A = A_1 \Rightarrow A_2$
- $A = \neg(A_1 \Rightarrow A_2)$
- $A = p$ ou $A = \neg p$

Nous nous appuyons sur plusieurs lemmes techniques sur $\vdash$ et $\models$ (listés en fin de preuve).

Si $A = \neg\neg A'$

- $\Gamma \models \neg\neg A'$ implique $\Gamma \models A'$
- HR sur $\mu(\Gamma, A') = n - 2 : \Gamma \models A'$ implique $\Gamma \vdash A'$
- $\Gamma \vdash A'$ implique $\Gamma \vdash \neg\neg A'$

Si $A = A_1 \Rightarrow A_2$

- $\Gamma \models A_1 \Rightarrow A_2$ implique $\Gamma, A_1 \models A_2$
- HR sur $\mu(\Gamma \cup \{A_1\}, A_2) = n - 2 : \Gamma, A_1 \models A_2$ implique $\Gamma, A_1 \vdash A_2$
- $\Gamma, A_1 \vdash A_2$ implique $\Gamma \vdash A_1 \Rightarrow A_2$

Si $A = \neg(A_1 \Rightarrow A_2)$

- $\Gamma \models \neg(A_1 \Rightarrow A_2)$ implique $\Gamma \models A_1$ et $\Gamma \models \neg A_2$
- HR sur $\mu(\Gamma, A_1) = n - \mu(A_2) - 3$ et $\mu(\Gamma, \neg A_2) = n - \mu(A_1) - 2$: donc $\Gamma \models A_1$ implique $\Gamma \vdash A_1$ et $\Gamma \models \neg A_2$ implique $\Gamma \vdash \neg A_2$
- $\Gamma \vdash A_1$ et $\Gamma \vdash \neg A_2$ implique $\Gamma \vdash \neg(A_1 \Rightarrow A_2)$

Si $A = p$ ou $A = \neg p$: on étudie la forme des formules dans Γ

- $\Gamma = \Gamma', \neg\neg B$
- $\Gamma = \Gamma', B_1 \Rightarrow B_2$
- $\Gamma = \Gamma', \neg(B_1 \Rightarrow B_2)$
- Γ ne contient que des formules de la forme $r, \neg r$

Si $\Gamma = \Gamma', \neg\neg B$

- $\Gamma', \neg\neg B \models A$ implique $\Gamma', B \models A$
- HR sur $\mu(\Gamma' \cup \{B\}, A) = n - 2 : \Gamma', B \models A$ implique $\Gamma', B \vdash A$
- $\Gamma', B \vdash A$ implique $\Gamma', \neg\neg B \vdash A$

Si $\Gamma = \Gamma', B_1 \Rightarrow B_2$

- $\Gamma', B_1 \Rightarrow B_2 \models A$ implique $\Gamma', \neg B_1 \models A$ et $\Gamma', B_2 \models A$
- HR sur $\mu(\Gamma' \cup \{\neg B_1\}, A) = n - \mu(B_2) - 1$ et $\mu(\Gamma' \cup \{B_2\}, A) = n - \mu(B_1) - 2$: $\Gamma', \neg B_1 \models A$ implique $\Gamma', \neg B_1 \vdash A$ et $\Gamma', B_2 \models A$ implique $\Gamma', B_2 \vdash A$
- $\Gamma', \neg B_1 \vdash A$ et $\Gamma', B_2 \vdash A$ implique $\Gamma', B_1 \Rightarrow B_2 \vdash A$

Si $\Gamma = \Gamma', \neg(B_1 \Rightarrow B_2)$

- $\Gamma', \neg(B_1 \Rightarrow B_2) \models A$ implique $\Gamma', B_1, \neg B_2 \models A$
- HR sur $\mu(\Gamma' \cup \{B_1, \neg B_2\}, A) = n - 2 : \Gamma', B_1, \neg B_2 \models A$ implique $\Gamma', B_1, \neg B_2 \vdash A$
- $\Gamma', B_1, \neg B_2 \vdash A$ implique $\Gamma', \neg(B_1 \Rightarrow B_2) \vdash A$

Enfin, si Γ ne contient que des littéraux et $A = p$ ou $A = \neg p$.
Notons $\Gamma = \Gamma^+ \cup \Gamma^-$ (séparation littéraux positifs/négatifs)

- Si $\neg\Gamma^+ \cap \Gamma^- \neq \emptyset$, Γ est de la forme $\Gamma', r, \neg r$ et donc $\Gamma', r, \neg r \vdash A$.
- $A = p$ et $p \in \Gamma^+$: OK
- $A = p$ et $p \notin \Gamma^+$: $\Gamma \not\models A$
- $A = \neg p$ et $\neg p \in \Gamma^-$: OK
- $A = \neg p$ et $\neg p \notin \Gamma^+$: $\Gamma \not\models A$

Lemmes techniques sur $\models$

Lemme

- $\Gamma \models \neg\neg A$ *implique* $\Gamma \models A$
- $\Gamma \models A_1 \Rightarrow A_2$ *implique* $\Gamma, A_1 \models A_2$
- $\Gamma \models \neg(A_1 \Rightarrow A_2)$ *implique* $\Gamma \models A_1$ *et* $\Gamma \models \neg A_2$
- $\Gamma, \neg\neg B \models A$ *implique* $\Gamma, B \models A$
- $\Gamma, B_1 \Rightarrow B_2 \models A$ *implique* $\Gamma, \neg B_1 \models A$ *et* $\Gamma, B_2 \models A$
- $\Gamma, \neg(B_1 \Rightarrow B_2) \models A$ *implique* $\Gamma, B_1, \neg B_2 \models A$

Lemmes techniques sur $\vdash$

Lemme

Si $\Gamma \vdash A$ *alors* $\Gamma, B \vdash A$.

Lemme

- $\Gamma \vdash A$ *implique* $\Gamma \vdash \neg\neg A$
- $\Gamma, A_1 \vdash A_2$ *implique* $\Gamma \vdash A_1 \Rightarrow A_2$
- $\Gamma \vdash A_1$ *et* $\Gamma \vdash \neg A_2$ *implique* $\Gamma \vdash \neg(A_1 \Rightarrow A_2)$
- $\Gamma, B \vdash A$ *implique* $\Gamma, \neg\neg B \vdash A$
- $\Gamma, \neg B_1 \vdash A$ *et* $\Gamma, B_2 \vdash A$ *implique* $\Gamma, B_1 \Rightarrow B_2 \vdash A$
- $\Gamma, B_1, \neg B_2 \vdash A$ *implique* $\Gamma, \neg(B_1 \Rightarrow B_2) \vdash A$
- $\Gamma, B, \neg B \vdash A$

Complétude sur l'ensemble des formules

$\mathcal{F}$: ensemble des formules formées avec $\{\neg, \wedge, \vee, \Rightarrow, \Longleftrightarrow\}$

$\mathcal{F}'$: ensemble des formules formées avec $\{\neg, \Rightarrow\}$

Proposition

La transformation $\Phi : \mathcal{F} \to \mathcal{F}'$ définie par induction par

$$\begin{aligned}
\Phi(p) &= p \\
\Phi(\neg F) &= \neg\Phi(F) \\
\Phi((F_1 \Rightarrow F_2)) &= (\Phi(F_1) \Rightarrow \Phi(F_2)) \\
\Phi((F_1 \wedge F_2)) &= \neg(\Phi(F_1) \Rightarrow \neg\Phi(F_2)) \\
\Phi((F_1 \vee F_2)) &= (\neg\Phi(F_1) \Rightarrow \Phi(F_2)) \\
\Phi((F_1 \Longleftrightarrow F_2)) &= \dots
\end{aligned}$$

vérifie :

$$\text{pour tout } F \in \mathcal{F},\ \Phi(F) \vdash F$$

Complétude

Lemme

Pour toute formule $F \in \mathcal{F}$, si $\models F$ alors $\vdash F$.

Proposition

Pour tout ensemble de formule $\Gamma \subseteq \mathcal{F}$ et toute formule $F \in \mathcal{F}$, si $\Gamma \models F$ alors $\Gamma \vdash F$.

Preuve :

- théorème de compacité : il existe un sous ensemble $\{G_1, \ldots, G_n\}$ fini de Γ, $\{G_1, \ldots, G_n\} \subseteq \Gamma$ tel que $G_1, \ldots, G_n \models F$.
- Par récurrence sur n il est facile de démontrer que pour toutes formules $G_1, \ldots, G_n, F$

$$G_1, \ldots, G_n \models F \text{ ssi } \models G_1 \Rightarrow (G_2 \Rightarrow \cdots (G_n \Rightarrow F))$$

Donc $G_1 \Rightarrow (G_2 \Rightarrow \cdots (G_n \Rightarrow F))$ est une tautologie

Complétude (preuve)

- D'après le lemme précédent, cela implique que $\vdash G_1 \Rightarrow (G_2 \Rightarrow \cdots (G_n \Rightarrow F))$ qui, par une suite d'application de la règle $e_{\Rightarrow}$, permet d'établir $G_1, \ldots, G_n \vdash F$
- Nous concluons alors par le résultat suivant

  pour tout ensemble Γ_1, Γ_2 *et toute formule* F, *si* $\Gamma_1 \subseteq \Gamma_2$ *et* $\Gamma_1 \vdash F$ *alors* $\Gamma_2 \vdash F$.

  Ce résultat se prouve facilement par induction sur $\Gamma_1 \vdash F$.
- Nous pouvons alors en conclure que $\Gamma \vdash F$, car $\{G_1, \ldots, G_n\} \subseteq \Gamma$, ce qui termine notre preuve.

Introduction à l'isomorphisme de Curry-Howard

Le λ-calcul simplement typé

Soit $\{x, y, \ldots\}$ un ensemble dénombrable de variables, et $\{\alpha, \beta, \ldots\}$ un ensemble dénombrable d'éléments appelés *types de base*.

Définition (Types simples)

L'ensemble des *types simples* est défini inductivement par

- tout type de base est un type simple,
- si A, B sont des types simples alors $(A \to B)$ est un type simple.

Définition (Contexte)

Un *contexte* est un ensemble de couples de la forme (x, A) (noté $x : A$) avec x une variable et A un type, tel que chaque variable apparaît au plus une fois.

Notation $\Gamma[x : A]$ le contexte Γ auquel on ajoute (x, A) en supprimant l'ancienne occurrence (éventuelle) de x.

λ-termes bien typés

Définition

Soit Γ un contexte, t un terme et A un type. L'ensemble des triplets (Γ, t, A) *bien typés* est défini inductivement par

- si $(x, A) \in \Gamma$ alors (Γ, x, A) est bien typé,
- si $(\Gamma, u, A \to B)$ et (Γ, v, A) sont bien typés alors $(\Gamma, (u\ v), B)$ est bien typé,
- si $(\Gamma[x : A], t, B)$ est bien typé alors $(\Gamma, \lambda x.\, t, A \to B)$ est bien typé.

Notation Quand le triplet (Γ, t, A) est bien typé, on dit que t *a le type* A *dans* Γ, et on écrit $\Gamma \vdash t : A$.

Système d'inférence associé

$$\frac{}{\Gamma, x : A \vdash x : A}\ \text{Cont}$$

$$\frac{\Gamma \vdash u : A \to B \quad \Delta \vdash v : A}{\Gamma, \Delta \vdash (u\ v) : B}\ \text{App}$$

$$\frac{\Gamma[x : A] \vdash t : B}{\Gamma \vdash \lambda x.\, t : A \to B}\ \text{Gen}$$

Exemple

Quel(s) type(s) peut-on associer au lambda-terme $\lambda x.x$?

Exemple

Quel(s) type(s) peut-on associer au lambda-terme $\lambda x.x$?

Le lambda-terme $\lambda x.x$ admet pour type $A \to A$, quel que soit le type A.

$$\dfrac{\dfrac{}{x : A \vdash x : A}\,\text{Cont}}{\vdash \lambda x.x : A \to A}\,\text{Gen}$$

Un terme non typable

Montrer que le terme $(x\ x)$ n'est pas typable.

Un terme non typable

Montrer que le terme $(x\ x)$ n'est pas typable.

Si $(x\ x)$ était typable, on aurait d'après la règle App, x à la fois de type $A \to B$ et de type A. Or, pour tous types A et B, on peut montrer (par induction sur A) que $A \neq A \to B$.

Exemples

Donner un type pour les termes suivants.

1. $\lambda x.\, \lambda y.\, \lambda z.\, ((x\ y)\ z)$
2. $\lambda x.\, \lambda y.\, \lambda z.\, (x\ (y\ z))$

Exemples

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a : B \to (C \to A) \vdash a : B \to (C \to A)}\,\text{Cont} \quad \dfrac{}{b : B \vdash B}\,\text{Cont}}{a : B \to (C \to A), b : B \vdash (a\ b) : C \to A}\,\text{App} \quad \dfrac{}{c : C \vdash c : C}\,\text{Cont}}{a : B \to (C \to A), b : B, c : C \vdash ((a\ b)\ c) : A}\,\text{App}}{a : B \to (C \to A), b : B \vdash \lambda c.\,((a\ b)\ c) : C \to A}\,\text{Gen}}{a : B \to (C \to A) \vdash \lambda b.\,\lambda c.\,((a\ b)\ c) : B \to (C \to A)}\,\text{Gen}}{\vdash \lambda a.\,\lambda b.\,\lambda c.\,((a\ b)\ c) : (B \to (C \to A)) \to (B \to (C \to A))}\,\text{Gen}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a : B \to A \vdash a : B \to A}\,\text{Cont} \quad \dfrac{\dfrac{}{b : C \to B \vdash b : C \to B}\,\text{Cont} \quad \dfrac{}{c : C \vdash c : C}\,\text{Cont}}{b : C :\to B, c : C \vdash (b\ c) : B}\,\text{App}}{a : B \to A, b : C :\to B, c : C \vdash (a\ (b\ c)) : A}\,\text{App}}{a : B \to A, b : C :\to B \vdash \lambda c.\,(a\ (b\ c)) : C \to A}\,\text{Gen}}{a : B \to A \vdash \lambda b.\,\lambda c.\,(a\ (b\ c)) : (C \to B) \to (C \to A)}\,\text{Gen}}{\vdash \lambda a.\,\lambda b.\,\lambda c.\,(a\ (b\ c)) : (B \to A) \to ((C \to B) \to (C \to A))}\,\text{Gen}$$

Théorème de correspondance

On restreint ici la logique minimale NM aux formule formées avec $\Rightarrow$ uniquement. Seuls les règles intro$_\Rightarrow$, elim$_\Rightarrow$ et Ax sont nécessaires.

Nous identifions les variables propositionnelles et les types de base par une bijection Φ et étendons cette bijection aux formules en posant

$$\Phi((p \Rightarrow q)) = \Phi(p) \rightarrow \Phi(q)$$

Théorème de correspondance

Théorème

Soient $A_1, \ldots, A_n, A$ des formules propositionnelles (uniquement avec $\Rightarrow$), $A_1, \ldots, A_n \vdash A$ si et seulement si il existe un terme typé de type $\Phi(A)$ dans le contexte $x_1 : \Phi(A_1), \ldots, x_n : \Phi(A_n)$.

Exemples

Donner une preuve des formules suivantes sous forme de lambda-terme.

1. $A \Rightarrow B \Rightarrow A$
2. $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$
3. $(A \Rightarrow B \Rightarrow (C \Rightarrow D) \Rightarrow E) \Rightarrow ((A \Rightarrow D) \Rightarrow F) \Rightarrow$
   $(A \Rightarrow (B \Rightarrow E) \Rightarrow C) \Rightarrow (C \Rightarrow D) \Rightarrow F$

La solution en Caml...

```
# let f = fun a b -> a;;
val f : 'a -> 'b -> 'a = <fun>
```

La solution en Caml...

```
# let f = fun a b -> a;;
val f : 'a -> 'b -> 'a = <fun>

# let f = fun x y z -> x z (y z);;
val f : ('a -> 'b -> 'c) -> ('a -> 'b) -> 'a -> 'c = <fun>
```

La solution en Caml...

```
# let f = fun a b -> a;;
val f : 'a -> 'b -> 'a = <fun>

# let f = fun x y z -> x z (y z);;
val f : ('a -> 'b -> 'c) -> ('a -> 'b) -> 'a -> 'c = <fun>

# let f =
  fun x y z t -> y (fun u -> (t (z u (fun v -> x u v t))));;
val f :
  ('a -> 'b -> ('c -> 'd) -> 'e) ->
  (('a -> 'd) -> 'f) -> ('a -> ('b -> 'e) -> 'c) ->
  ('c -> 'd) -> 'f = <fun>
```

L'assistant de preuve Coq

En Coq, toutes les preuves sont représentées par des λ-termes.

- La logique sous-jacente est beaucoup plus riche que la logique propositionnelle (ou même du premier ordre).
- Le λ-calcul sous-jacent est muni d'un système de type beaucoup plus riche que celui du λ-calcul simplement typé.

En Coq,

$$\text{programme} = \text{preuve}\,!$$

Exemple : la preuve de $\forall \mathtt{n} : \mathtt{nat},\ \mathtt{n} \neq \mathtt{0} \Rightarrow \exists p,\ \mathtt{n} = \mathtt{p} + \mathtt{1}$ correspond au programme qui calcule le prédécesseur d'un entier.

Toutes les règles de déduction

$$\text{intro}_{\Rightarrow}\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \text{elim}_{\Rightarrow}\ \frac{\Gamma \vdash A \quad \Delta \vdash A \Rightarrow B}{\Gamma, \Delta \vdash B}$$

$$\text{intro}_{\wedge}\ \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B} \qquad \text{elim}^1_{\wedge}\ \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \text{elim}^2_{\wedge}\ \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\text{intro}^1_{\vee}\ \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \text{intro}^2_{\vee}\ \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

$$\text{elim}_{\vee}\ \frac{\Gamma \vdash A \vee B \quad \Delta, A \vdash C \quad \Delta', B \vdash C}{\Gamma, \Delta, \Delta' \vdash C}$$

$$\text{intro}_{\neg}\ \frac{\Gamma, A \vdash \neg B \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash \neg A} \qquad \text{elim}_{\neg}\ \frac{\Gamma \vdash \neg A \quad \Delta \vdash A}{\Gamma, \Delta \vdash B}$$

$$\text{elim}_{\bot}\ \frac{\Gamma \vdash \bot}{\Gamma \vdash A}$$

$$\text{TE}\ \frac{}{\Gamma \vdash A \vee \neg A} \qquad \text{abs}\ \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A} \qquad \text{elim}_{\neg\neg}\ \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$$

Plan

1. Logique minimale
2. Logique intuitionniste
3. Logique classique
4. Correction et complétude
5. Introduction à l'isomorphisme de Curry-Howard
6. Memento