Prouver = Programmer

David Delahaye
David.Delahaye@lirmm.fr

Université de Montpellier
Faculté des Sciences

Licence Informatique L3 2022-2023

Prouver = Programmer

Le mathématicien

Théorème. Pour tout $n \in \mathbb{N}$, il existe $p \in \mathbb{N}$ t.q. $n = 2p$ ou $n = 2p + 1$. *Preuve.* Par induction sur n :

- Si $n = 0$, on prend $p = 0$.
- Sinon, on suppose $n = m + 1$. Par hypothèse d'induction, on sait qu'il existe p t.q. $m = 2p$ ou $m = 2p + 1$:
  - Si $m = 2p$ alors $n = 2p + 1$.
  - Si $m = 2p + 1$ alors $n = 2(p + 1)$.

Le programmeur

```
val div2 : int → int * bool
(* [div2 n] retourne la
division entière par 2 de [n]
ainsi qu'un booléen indiquant
si [n] est pair. *)

let rec div2 n = match n with
| 0 → (0, true)
| m + 1 →
  let (p, even) = div2 m in
  if even then (p, false)
  else (p + 1, true)
```

Sémantiques de la logique

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

- Initiée par Luitzen Egbertus Jan Brouwer à partir de 1907
- Une formule est vraie, fausse, ou « on ne sait pas »
- Si on ne sait en démontrer la validité, alors « on ne sait pas »
- On exclut le tiers exclu !

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.

Logiques classique/intuitionniste

David Hilbert (1862-1943)

Priver le mathématicien du tertium non datur [pas de troisième possibilité] serait enlever son télescope à l'astronome, son poing au boxeur.

Luitzen Egbertus Jan Brouwer (1881-1966)

Il n'y a pas de vérité sans expérience de la vérité.

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 (pas simple !)
- On peut prendre e et $ln(2)$ par exemple :
  - Preuve de l'irrationnalité de e : preuve d'Euler en 1737
  - Preuve de l'irrationnalité de $ln(2)$: vraiment loin d'être triviale
    Méthode de Beukers (qui implique des polynômes de Legendre)

Exotisme de la logique classique

Des théorèmes vraiment classiques

La formule suivante est-elle valide ?

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

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 »

Formalisée par la formule suivante :

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

Que perd-on en logique intuitionniste ?

Des principes de preuve

- Raisonnement par l'absurde : une façon de prouver qu'un objet existe est de supposer qu'il n'existe pas, et d'aboutir à une contradiction. Alors, puisqu'il ne peut pas ne pas exister, c'est donc qu'il existe. Mais on n'est pas plus avancé s'il s'agit de le trouver !
- Règle d'élimination des doubles négations.
  Pourtant si naturelle !
  Le tiers exclu est souvent modélisé par cette règle.

Des théorèmes

- Avec un axiome en moins, on prouve moins de choses.
- Par exemple, le théorème qui affirme que toute suite croissante majorée converge n'est pas valide en mathématiques constructives.
- Les mathématiques sont à réinventer !

Que gagne-t-on en logique intuitionniste ?

Un lien avec l'informatique

- Une preuve constructive est souvent plus instructive qu'une preuve qui ne l'est pas car elle fournit un algorithme pour construire une solution au problème posé
- C'est ce contenu algorithmique des preuves que nous nous proposons d'expliciter dans la suite de l'exposé

Interprétation de Brouwer-Heyting-Kolmogorov

Interprétation BHK

- Interprétation de la logique intuitionniste (sans le tiers exclu)
- Proposée par Brouwer et Heyting, et aussi par Kolmogorov
- Appelée aussi « interprétation par réalisabilité » (Kleene)
- Idée : donner une interprétation fonctionnelle aux preuves

Interprétation de Brouwer-Heyting-Kolmogorov

Par induction sur les formules

- Une preuve de $A \Rightarrow B$ est une fonction qui associe à une preuve de A une preuve de B
- Une preuve de $A \wedge B$ est un couple (π_1, π_2), où π_1 est une preuve de A et π_2 une preuve de B
- Une preuve de $A \vee B$ est soit une preuve de A, soit une preuve de B
- Une preuve de $\forall x.A(x)$ est une fonction qui associe à tout objet t une preuve de $A(t)$
- Une preuve de $\exists x.A(x)$ est un couple (t, π), où t est un objet et π est une preuve de $A(t)$
- Une preuve de $\neg A$ (vue comme $A \Rightarrow \bot$) est une fonction qui associe à toute preuve de A une preuve de $\bot$
- On désigne par I la preuve de $\top$, et il n'existe pas de preuve $\bot$

Isomorphisme ou correspondance de Curry-Howard

Principe et historique

- Basé sur une double correspondance :
  - Correspondance preuves/programmes
  - Correspondance formules/types
- Curry : analogie entre les preuves dans les systèmes à la Hilbert et la logique combinatoire
- Howard : analogie entre les preuves en déduction naturelle intuitionniste et les termes du λ-calcul typé

Cas de la logique implicative minimale

Règles en déduction naturelle (avec séquent)

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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\Rightarrow_I \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\Rightarrow_E$$

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

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

$$A \Rightarrow B, A \vdash B$$

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

$$\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B$$

Cas de la logique implicative minimale

Règles en déduction naturelle (avec séquent)

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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow_I \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \Rightarrow_E$$

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

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

$$A \Rightarrow B, A \vdash B$$

$$\frac{A \Rightarrow B \vdash A \Rightarrow B}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\ \Rightarrow_I$$

Cas de la logique implicative minimale

Règles en déduction naturelle (avec séquent)

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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow_E$$

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

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

$$\cfrac{\cfrac{A \Rightarrow B, A \vdash B}{A \Rightarrow B \vdash A \Rightarrow B} \Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B} \Rightarrow_I$$

Cas de la logique implicative minimale

Règles en déduction naturelle (avec séquent)

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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_I \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow_E$$

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\cfrac{\cfrac{\cfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B} \Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B} \Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B} \Rightarrow_I$$

Cas de la logique implicative minimale

Règles en déduction naturelle (avec séquent)

$$\dfrac{}{\Gamma, A \vdash A}\ \mathrm{ax}$$

$$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \Rightarrow_I \qquad \dfrac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B} \Rightarrow_E$$

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\ \mathrm{ax} \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B} \Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B} \Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B} \Rightarrow_I$$

Cas de la logique implicative minimale

Règles en déduction naturelle (avec séquent)

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

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow_I \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \Rightarrow_E$$

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\ \text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\ \text{ax}}{A \Rightarrow B, A \vdash B}\ \Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\ \Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\ \Rightarrow_I$$

λ-calcul simplement typé

Termes et types

- Termes :
  - Les variables x, y, ... sont des variables
  - Si x est une variable, τ un type, et t un terme, alors $\lambda x : \tau.t$ est un terme (notation à la Church)
  - Si t_1 et t_2 sont des termes, alors $t_1\ t_2$ est un terme
- Types :
  - Les types de base ι_1, ι_2, ... sont des types
  - Si τ_1 et τ_2 sont des types, alors $\tau_1 \to \tau_2$ est un type

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1.t : \tau_1 \to \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x,\tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x,\tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \rightarrow \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \rightarrow \iota_B . \lambda y : \iota_A . x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x,\iota_A \rightarrow \iota_B) \in (x,\iota_A \rightarrow \iota_B),(y,\iota_A)}{(x,\iota_A \rightarrow \iota_B),(y,\iota_A) \vdash x : \iota_A \rightarrow \iota_B} \qquad \dfrac{(y,\iota_A) \in (x,\iota_A \rightarrow \iota_B),(y,\iota_A)}{(x,\iota_A \rightarrow \iota_B),(y,\iota_A) \vdash y : \iota_A}}{(x,\iota_A \rightarrow \iota_B),(y,\iota_A) \vdash x\ y : \iota_B}}{(x,\iota_A \rightarrow \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \rightarrow \iota_B}}{\vdash \lambda x : \iota_A \rightarrow \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1.t : \tau_1 \rightarrow \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y$

$$(x, \iota_A \rightarrow \iota_B) \in (x, \iota_A \rightarrow \iota_B), (y, \iota_A) \qquad (y, \iota_A) \in (x, \iota_A \rightarrow \iota_B), (y, \iota_A)$$

$$(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash x : \iota_A \rightarrow \iota_B \qquad (x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash y : \iota_A$$

$$(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash x\ y : \iota_B$$

$$\frac{(x, \iota_A \rightarrow \iota_B) \vdash \lambda y : \iota_A.x\ y : \iota_A \rightarrow \iota_B}{\vdash \lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y : (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \to \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y$

$$(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A) \qquad (y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)$$

$$(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B \qquad (x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A$$

$$\cfrac{\cfrac{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \to \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\ \text{App}}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x,\tau)\in\Gamma}{\Gamma\vdash x:\tau}\;\text{Var}$$

$$\frac{\Gamma,(x,\tau_1)\vdash t:\tau_2}{\Gamma\vdash\lambda x:\tau_1.t:\tau_1\to\tau_2}\;\text{Fun}\qquad\qquad\frac{\Gamma\vdash t_1:\tau_1\to\tau_2\qquad\Gamma\vdash t_2:\tau_1}{\Gamma\vdash t_1\ t_2:\tau_2}\;\text{App}$$

Typage de $\lambda x:\iota_A\to\iota_B.\lambda y:\iota_A.x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x,\iota_A\to\iota_B)\in(x,\iota_A\to\iota_B),(y,\iota_A)}{(x,\iota_A\to\iota_B),(y,\iota_A)\vdash x:\iota_A\to\iota_B}\;\text{Var}\qquad\dfrac{(y,\iota_A)\in(x,\iota_A\to\iota_B),(y,\iota_A)}{(x,\iota_A\to\iota_B),(y,\iota_A)\vdash y:\iota_A}}{(x,\iota_A\to\iota_B),(y,\iota_A)\vdash x\ y:\iota_B}\;\text{App}}{(x,\iota_A\to\iota_B)\vdash\lambda y:\iota_A.x\ y:\iota_A\to\iota_B}\;\text{Fun}}{\vdash\lambda x:\iota_A\to\iota_B.\lambda y:\iota_A.x\ y:(\iota_A\to\iota_B)\to\iota_A\to\iota_B}\;\text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \to \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\ \text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\ \text{Var}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\ \text{App}}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1.t : \tau_1 \rightarrow \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \rightarrow \iota_B) \in (x, \iota_A \rightarrow \iota_B), (y, \iota_A)}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash x : \iota_A \rightarrow \iota_B}\ \text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \rightarrow \iota_B), (y, \iota_A)}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash y : \iota_A}\ \text{Var}}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\ \text{App}}{(x, \iota_A \rightarrow \iota_B) \vdash \lambda y : \iota_A.x\ y : \iota_A \rightarrow \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y : (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \rightarrow \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \rightarrow \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \rightarrow \iota_B . \lambda y : \iota_A . x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \rightarrow \iota_B) \in (x, \iota_A \rightarrow \iota_B), (y, \iota_A)}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash x : \iota_A \rightarrow \iota_B}\ \text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \rightarrow \iota_B), (y, \iota_A)}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash y : \iota_A}\ \text{Var}}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\ \text{App}}{(x, \iota_A \rightarrow \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \rightarrow \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \rightarrow \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x,\tau)\in\Gamma}{\Gamma\vdash x:\tau}\ \text{Var}$$

$$\frac{\Gamma,(x,\tau_1)\vdash t:\tau_2}{\Gamma\vdash\lambda x:\tau_1.t:\tau_1\to\tau_2}\ \text{Fun}\qquad\frac{\Gamma\vdash t_1:\tau_1\to\tau_2\qquad\Gamma\vdash t_2:\tau_1}{\Gamma\vdash t_1\ t_2:\tau_2}\ \text{App}$$

Typage de $\lambda x:\iota_A\to\iota_B.\lambda y:\iota_A.x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x,\iota_A\to\iota_B)\in(x,\iota_A\to\iota_B),(y,\iota_A)}{(x,\iota_A\to\iota_B),(y,\iota_A)\vdash x:\iota_A\to\iota_B}\ \text{Var}\qquad\dfrac{(y,\iota_A)\in(x,\iota_A\to\iota_B),(y,\iota_A)}{(x,\iota_A\to\iota_B),(y,\iota_A)\vdash y:\iota_A}\ \text{Var}}{(x,\iota_A\to\iota_B),(y,\iota_A)\vdash x\ y:\iota_B}\ \text{App}}{(x,\iota_A\to\iota_B)\vdash\lambda y:\iota_A.x\ y:\iota_A\to\iota_B}\ \text{Fun}}{\vdash\lambda x:\iota_A\to\iota_B.\lambda y:\iota_A.x\ y:(\iota_A\to\iota_B)\to\iota_A\to\iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \to \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y$

$$\cfrac{\cfrac{\cfrac{\cfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\ \text{Var} \qquad \cfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\ \text{Var}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\ \text{App}}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\ \text{Fun}$$

λ-calcul simplement typé

Règles de typage

$$\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau}\ \text{Var}$$

$$\frac{\Gamma, (x, \tau_1) \vdash t : \tau_2}{\Gamma \vdash \lambda x : \tau_1 . t : \tau_1 \to \tau_2}\ \text{Fun} \qquad \frac{\Gamma \vdash t_1 : \tau_1 \to \tau_2 \qquad \Gamma \vdash t_2 : \tau_1}{\Gamma \vdash t_1\ t_2 : \tau_2}\ \text{App}$$

Typage de $\lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y$

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\ \text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\ \text{Var}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\ \text{App}}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\ \text{Fun}}{\vdash \lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\ \text{Fun}$$

Isomorphisme de Howard

Correspondance formules/types : Φ

- $\Phi(A) = \iota_A$;
- $\Phi(A \Rightarrow B) = \Phi(A) \rightarrow \Phi(B)$.

Correspondance preuves/termes : φ

- Pour chaque contexte de preuve $\Gamma = A_1, \ldots, A_n$,
  $\varphi(\Gamma) = (x_{A_1}, \Phi(A_1)), \ldots, (x_{A_n}, \Phi(A_n))$
  (une variable unique par formule)
- Si la preuve π est de la forme :

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

alors $\varphi(\pi) = x_A$

Isomorphisme de Howard

Correspondance formules/types : Φ

- $\Phi(A) = \iota_A$;
- $\Phi(A \Rightarrow B) = \Phi(A) \rightarrow \Phi(B)$.

Correspondance preuves/termes : φ

- Si la preuve π est de la forme :

$$\dfrac{\dfrac{\pi'}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\Rightarrow_I$$

alors $\varphi(\pi) = \lambda x_A : \Phi(A).\varphi(\pi')$

Isomorphisme de Howard

Correspondance formules/types : Φ

- $\Phi(A) = \iota_A$;
- $\Phi(A \Rightarrow B) = \Phi(A) \rightarrow \Phi(B)$.

Correspondance preuves/termes : φ

- Si la preuve π est de la forme :

$$\dfrac{\dfrac{\pi_1}{\Gamma \vdash A \Rightarrow B} \qquad \dfrac{\pi_2}{\Gamma \vdash A}}{\Gamma \vdash B} \Rightarrow_E$$

  alors $\varphi(\pi) = \varphi(\pi_1)\ \varphi(\pi_2)$
- Théorème : pour une preuve π de $\Gamma \vdash A$, on a donc $\varphi(\Gamma) \vdash \varphi(\pi) : \Phi(A)$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}}{A \Rightarrow B \vdash A \Rightarrow B}}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}}{A \Rightarrow B \vdash A \Rightarrow B}}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B} \Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I
$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\text{ax} \quad \dfrac{}{A \Rightarrow B, A \vdash A}\text{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_A \rightarrow \iota_B}\,\text{ax} \qquad \dfrac{}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_A}\,\text{ax}}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_B}\,\Rightarrow_E}{\iota_A \rightarrow \iota_B \vdash \iota_A \rightarrow \iota_B}\,\Rightarrow_I}{\vdash (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}\,\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\mathrm{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\mathrm{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I
$$

Arbre de typage correspondant

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_A \rightarrow \iota_B}\,\mathrm{ax} \qquad \dfrac{}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_A}\,\mathrm{ax}}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_B}\Rightarrow_E}{(x, \iota_A \rightarrow \iota_B) \vdash \iota_A \rightarrow \iota_B}\Rightarrow_I}{\vdash (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}\Rightarrow_I
$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\mathrm{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\mathrm{ax}}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_A \rightarrow \iota_B}\,\mathrm{ax} \qquad \dfrac{}{\iota_A \rightarrow \iota_B, \iota_A \vdash \iota_A}\,\mathrm{ax}}{(x, \iota_A \rightarrow \iota_B), (y, \iota_A) \vdash \iota_B}\,\Rightarrow_E}{(x, \iota_A \rightarrow \iota_B) \vdash \iota_A \rightarrow \iota_B}\,\Rightarrow_I}{\vdash (\iota_A \rightarrow \iota_B) \rightarrow \iota_A \rightarrow \iota_B}\,\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \quad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash \iota_A \to \iota_B}\,\text{ax} \quad \dfrac{}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash \iota_A}\,\text{ax}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash \iota_B}\Rightarrow_E}{(x, \iota_A \to \iota_B) \vdash \iota_A \to \iota_B}\Rightarrow_I}{\vdash (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I
$$

Arbre de typage correspondant

$$
\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\,\text{Var} \qquad \dfrac{}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash \iota_A}\,\text{ax}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash \iota_B}\,\Rightarrow_E}{(x, \iota_A \to \iota_B) \vdash \iota_A \to \iota_B}\,\Rightarrow_I}{\vdash (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\,\Rightarrow_I
$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\text{ax}}{\dfrac{A \Rightarrow B, A \vdash B}{\dfrac{A \Rightarrow B \vdash A \Rightarrow B}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I}\Rightarrow_I}\Rightarrow_E$$

Arbre de typage correspondant

$$\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\text{Var}}{\dfrac{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash \iota_B}{\dfrac{(x, \iota_A \to \iota_B) \vdash \iota_A \to \iota_B}{\vdash (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\Rightarrow_I}\Rightarrow_I}\Rightarrow_E$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\,\text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\,\text{Var}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\,\text{App}}{(x, \iota_A \to \iota_B) \vdash \iota_A \to \iota_B}\,\Rightarrow_I}{\vdash (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\,\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\,\text{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\,\text{Var}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\,\text{App}}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\,\text{Fun}}{\vdash (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\Rightarrow_I$$

Retour sur l'exemple

Preuve de $(A \Rightarrow B) \Rightarrow A \Rightarrow B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\mathsf{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\mathsf{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Arbre de typage correspondant

$$\dfrac{\dfrac{\dfrac{\dfrac{(x, \iota_A \to \iota_B) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x : \iota_A \to \iota_B}\,\mathsf{Var} \qquad \dfrac{(y, \iota_A) \in (x, \iota_A \to \iota_B), (y, \iota_A)}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash y : \iota_A}\,\mathsf{Var}}{(x, \iota_A \to \iota_B), (y, \iota_A) \vdash x\ y : \iota_B}\,\mathsf{App}}{(x, \iota_A \to \iota_B) \vdash \lambda y : \iota_A . x\ y : \iota_A \to \iota_B}\,\mathsf{Fun}}{\vdash \lambda x : \iota_A \to \iota_B . \lambda y : \iota_A . x\ y : (\iota_A \to \iota_B) \to \iota_A \to \iota_B}\,\mathsf{Fun}$$

D'autres exemples

Logique implicative minimale

Démontrer les propositions suivantes en déduction naturelle et en extraire les termes correspondants en λ-calcul simplement typé :

- $A \Rightarrow B \Rightarrow A$
- $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$

D'autres exemples

Logique implicative minimale

Démontrer les propositions suivantes en déduction naturelle et en extraire les termes correspondants en λ-calcul simplement typé :

- $A \Rightarrow B \Rightarrow A$:
  $\lambda x : \tau_A.\lambda y : \tau_B.x$
- $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$

D'autres exemples

Logique implicative minimale

Démontrer les propositions suivantes en déduction naturelle et en extraire les termes correspondants en λ-calcul simplement typé :

- $A \Rightarrow B \Rightarrow A$:
  $\lambda x : \tau_A.\lambda y : \tau_B.x$
- $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$:
  $\lambda f : \tau_A \rightarrow \tau_B \rightarrow \tau_C.\lambda g : \tau_A \rightarrow \tau_B.\lambda x : \tau_A.f\ x\ (g\ x)$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}}{A \Rightarrow B, A \vdash A \Rightarrow B} \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}}{A \Rightarrow B \vdash A \Rightarrow B}}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

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

$$A \Rightarrow B, A \vdash B$$

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

$$A \Rightarrow B, A \vdash B$$

$$\frac{A \Rightarrow B \vdash A \Rightarrow B}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B} \Rightarrow_I$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

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

$$A \Rightarrow B, A \vdash B$$

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

$$\cfrac{\cfrac{A \Rightarrow B, A \vdash B}{A \Rightarrow B \vdash A \Rightarrow B} \Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B} \Rightarrow_I$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

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

$$A \Rightarrow B, A \vdash B$$

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad\qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

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

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash B}{A \Rightarrow B, A \vdash A \Rightarrow B}\Rightarrow_I \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow B, A \vdash A \Rightarrow B \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B, A \vdash A \Rightarrow B}\Rightarrow_I \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\Rightarrow_I \qquad A \Rightarrow B, A \vdash A}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\Rightarrow_I \qquad A \Rightarrow B, A \vdash A}{\dfrac{\dfrac{A \Rightarrow B, A \vdash B}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I}\,\Rightarrow_E
$$

Élimination des coupures

Notion coupure

- Une coupure est une succession d'une règle d'introduction suivie d'une règle d'élimination portant sur le même connecteur
- Exemple :

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax}
      \qquad
      \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}
    }{A \Rightarrow B, A \vdash B}\,\Rightarrow_E
  }{A \Rightarrow B, A \vdash A \Rightarrow B}\,\Rightarrow_I
  \qquad
  \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}
}{
  \dfrac{
    \dfrac{A \Rightarrow B, A \vdash B}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I
  }{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I
}\,\Rightarrow_E
$$

Élimination des coupures

Même preuve sans coupure

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\mathrm{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\mathrm{ax}}{A \Rightarrow B, A \vdash B}\,{\Rightarrow_E}}{A \Rightarrow B \vdash A \Rightarrow B}\,{\Rightarrow_I}}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,{\Rightarrow_I}$$

Théorème d'élimination des coupures

- « Hauptsatz » de Gentzen (1934)
- Toute formule qui possède une preuve faisant usage d'une coupure, possède aussi une preuve sans coupure
- Il existe un algorithme qui prend une preuve d'une formule et la transforme en une preuve sans coupure de la même formule
- Cela permet, entre autres, de montrer la cohérence de la logique

Élimination des coupures

Conséquence sur la partie calculatoire (fonctions) ?

- Preuve avec coupures :

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\,\Rightarrow_E}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\Rightarrow_I \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{\dfrac{A \Rightarrow B, A \vdash B}{A \Rightarrow B \vdash A \Rightarrow B}\,\Rightarrow_I}\,\Rightarrow_E}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\,\Rightarrow_I
$$

Terme preuve : $t_1 = \lambda x : \tau_A \to \tau_B . \lambda y : \tau_A . (\lambda z : \tau_A . x\ z)\ y$

Élimination des coupures

Conséquence sur la partie calculatoire (fonctions) ?

- Preuve après élimination des coupures :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, A \vdash A \Rightarrow B}\,\text{ax} \qquad \dfrac{}{A \Rightarrow B, A \vdash A}\,\text{ax}}{A \Rightarrow B, A \vdash B}\Rightarrow_E}{A \Rightarrow B \vdash A \Rightarrow B}\Rightarrow_I}{\vdash (A \Rightarrow B) \Rightarrow A \Rightarrow B}\Rightarrow_I$$

Terme preuve : $t_2 = \lambda x : \iota_A \to \iota_B.\lambda y : \iota_A.x\ y$

Élimination des coupures

Conséquence sur la partie calculatoire (fonctions) ?

- Comparaison des termes preuves :
  $t_1 = \lambda x : \tau_A \rightarrow \tau_B.\lambda y : \tau_A.(\lambda z : \tau_A.x\ z)\ y$
  $t_2 = \lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y$

Élimination des coupures

Conséquence sur la partie calculatoire (fonctions) ?

- Comparaison des termes preuves :
  $t_1 = \lambda x : \tau_A \rightarrow \tau_B.\lambda y : \tau_A.(\lambda z : \tau_A.x\ z)\ y$
  $t_2 = \lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y$
- On observe que : $t_1 \rightarrow_\beta t_2$

Élimination des coupures

Conséquence sur la partie calculatoire (fonctions) ?

- Comparaison des termes preuves :
  $t_1 = \lambda x : \tau_A \rightarrow \tau_B.\lambda y : \tau_A.(\lambda z : \tau_A.x\ z)\ y$
  $t_2 = \lambda x : \iota_A \rightarrow \iota_B.\lambda y : \iota_A.x\ y$
- On observe que : $t_1 \rightarrow_\beta t_2$
- L'élimination des coupures correspond donc à la β-réduction, c'est-à-dire à l'exécution des fonctions et donc des programmes !
- Une coupure correspond ainsi à un β-rédex
- Comme l'élimination des coupures est un processus qui termine, cela signifie que tous les programmes sont terminants dans ce calcul

Extensions

Autres connecteurs et quantificateurs

- $\wedge$: produit cartésien, couple/projections ;
- $\vee$: union disjointe, injections/filtrage ;
- $\neg$: revient à l'implication ($\neg A \equiv A \Rightarrow \bot$) ;
- $\forall$: produit (implication dépendante), fonction/application ;
- $\exists$: sigma (produit cartésien dépendant), couple/projections.

Extraction de programmes

Idée

- Extraire des programmes à partir de preuves
- Preuves avec un comportement calculatoire

Extraction : deux cas possibles

- On a une spécification, un programme, et une preuve :
  - On élimine la spécification et la preuve, et on garde le programme.
- On a une spécification et une preuve :
  - On élimine la spécification, et on extraie le programme de la preuve.

Une spécification et une preuve

Un exemple

Pour implémenter une fonction de tri d'une liste d'entiers naturels, on écrira et démontrera le théorème suivant :

$$\forall l \in list(nat).\exists l' \in list(nat).is\_sorted(l) \wedge is\_permutation(l, l')$$

- La preuve contient à la fois l'algorithme de tri et la preuve que cet algorithme est correct !

Des outils basés sur Curry-Howard

Caractéristiques de l'extraction dans Coq

- Utilisation de l'isomorphisme de Curry-Howard
- Preuves encodées comme des fonctions Coq
- Extraction du comportement calculatoire dans une spécification :
  - Extraction des fonctions
  - Extraction des parties purement calculatoires des preuves
- Plusieurs langages cibles : OCaml, Haskell, et Scheme

Extraction d'une fonction

Fonction successeur

```
Coq < Require Extraction.
[Loading ML file extraction_plugin.cmxs ... done]

Coq < Definition succ (n : nat) : nat := S n.
succ is defined

Coq < Extraction succ.
(** val succ : nat -> nat **)
let succ n =
  S n
```

Extraction d'une preuve

Fonction double

```
Coq < Lemma double :
  forall n : nat, {v : nat | v = 2 * n}.
1 subgoal
  ============================
  forall n : nat, {v : nat | v = 2 * n}

double < intro.
1 subgoal
  n : nat
  ============================
  {v : nat | v = 2 * n}
```

Extraction d'une preuve

Fonction double

```
double < exists (2 * n).
1 subgoal
  n : nat
  ============================
  2 * n = 2 * n

double < reflexivity.
No more subgoals.

double < Defined.
double is defined
```

Extraction d'une preuve

Fonction double

```
Coq < Extraction double.
(** val double : nat → nat **)
let double n =
  mul (S (S O)) n

Coq < Definition f_double (n : nat) : nat :=
  proj1_sig (double n).
f_double is defined

Coq < Eval compute in (f_double 3).
     = 6
     : nat
```

Écriture d'une fonction avec une preuve

Fonction successeur

```
Coq < Definition succ (n : nat) : nat.
1 subgoal
  n : nat
  ============================
  nat

succ < exact (S n).
No more subgoals.

succ < Defined.
succ is defined
```

Écriture d'une fonction avec une preuve

Fonction successeur

```
Coq < Print succ.
succ = fun n : nat => S n
     : nat → nat
Argument scope is [nat_scope]

Coq < Eval compute in (succ 2).
     = 3
     : nat
```

Écriture d'une fonction avec une preuve

Fonction factorielle

```
Coq < Definition fact (n : nat) : nat.
1 subgoal
  n : nat
  ============================
  nat

fact < elim n.
2 subgoals
  n : nat
  ============================
  nat

subgoal 2 is:
 nat → nat → nat
```

Écriture d'une fonction avec une preuve

Fonction factorielle

```
fact < exact 1.
1 subgoal
  n : nat
  ============================
  nat -> nat -> nat

fact < intros.
1 subgoal
  n, n0, H : nat
  ============================
  nat
```

Écriture d'une fonction avec une preuve

Fonction factorielle

```
fact < exact ((S n0) * H).
No more subgoals.

fact < Defined.
fact is defined

Coq < Eval compute in (fact 3).
     = 6
     : nat
```