Assistants de Preuve
Modèles, Réalisabilité

Bruno Barras et Christine Paulin-Mohring

INRIA, Université Paris-Sud 11

13/1/09

Plan

Rappels

- Modèles
- Modèle booléen “proof-irrelevent” de CC

Modèles de CC

- Modèle non “proof-irrelevent”

Réalisabilité

- Réalisabilté de Kleene
- Réalisabilité modifiée de Kreisel

Plan

Rappels
- Modèles
- Modèle booléen “proof-irrelevent” de CC

Modèles de CC
- Modèle non “proof-irrelevent”

Réalisabilité
- Réalisabilté de Kleene
- Réalisabilité modifiée de Kreisel

Modèles

But des modèles :

- démontrer qu'une proposition n'est pas démontrable (cohérence)
- démontrer qu'un énoncé est cohérent
- traduction (sémantique dénotationnelle)

Modèles de CC :

- Modèles booléens (card(Prop)=2) :
  - Modèle "proof-irrelevent" (Prop=bool)
  - Modèle non "proof-irrelevent" (Prop=$\{\emptyset, \Lambda\}$)
- Modèles de réalisabilité (Prop$\subseteq \mathcal{P}(\Lambda)$)

Modèle “proof-irrelevent”

Interprétation par niveaux :

- kinds (K :Type) : $[\mathrm{Prop}] = \mathrm{bool}$, $[\Pi X : K_1.K_2] = [K_1] \to [K_2]$, $[\Pi x : T.K] = [K]$
- types (T :K :Type) : $[\Pi x : T_1.T_2] = \neg[T_1] \vee [T_2]$, $[\Pi X : K.T] = \bigcap_{X \in [K]} [T]$, $[\lambda X : K.T] = X \in [K] \mapsto [T]$, $[\lambda x : T_1.T_2] = [T_2]$ $[T_1\ T_2] = [T_1]([T_2])$, $[T\ t] = [T]$
- preuves (t :T :Prop) : $[t] = \emptyset$

Exemples : $[\mathrm{nat}] = \{\emptyset\}$, $[\mathrm{Prop} \to \mathrm{Prop}] = \mathrm{bool} \to \mathrm{bool}$, $[\mathrm{nat} \to \mathrm{Prop}] = \mathrm{bool}$, $[\Pi X : \mathit{Prop}.X] = \emptyset$, $[\Pi X : \mathit{Prop}.X \to X] = \{\emptyset\}$, $[\mathrm{nat} \to \mathrm{False}] = \emptyset$.

Conséquences du modèles “proof-irrelevent”

Thm : $\vdash M : U \Rightarrow [M] \in [U]$

- Cohérence de CC étendu avec :
  - Tiers-exclu : $\forall A : Prop.(A \vee \neg A)$
  - Extentionalité
- Non dérivabilité de $0 \neq 1$ dans CC (cohérence de $0 = 1$)

Plan

Rappels
- Modèles
- Modèle booléen “proof-irrelevent” de CC

Modèles de CC
- Modèle non “proof-irrelevent”

Réalisabilité
- Réalisabilté de Kleene
- Réalisabilité modifiée de Kreisel

Modèle non “proof-irrelevent”

Similaire au modèle “proof-irrelevent”, sauf :

- kinds : $[\mathrm{Prop}] = \{\emptyset, \Lambda\}$, $[\Pi x : T.K] = \Pi_{x \in [T]}[K]$
- types : $[\Pi x : T_1.T_2] = \{t \in \Lambda \mid \forall u \in [T_1], t\,u \in [T_2]\}$,
  $[\lambda x : T_1.T_2]_= x \in [T_1] \mapsto [T_2]$, $[T\ t] = [T]([t])$
- preuves : $[\lambda X : K.t] = [t]$
  $[\lambda x : T.t] = \lambda x.[t]$
  $[t\ T] = [t]$
  $[t_1\ t_2] = [t_1]([t_2])$

Exemples : $[\mathrm{nat}] = \Lambda$, $[\mathrm{nat} \to \mathrm{Prop}] = \Lambda \to \{\emptyset, \Lambda\}$

Utilisé pour montrer la non-dérivabilité du schéma d’induction sur les entiers :
$\forall P : \mathrm{nat} \to \mathrm{Prop}, P\ 0 \to (\forall n, P\ n \to P\ (S\ n)) \to \forall n, P\ n$

Plan

Rappels
- Modèles
- Modèle booléen “proof-irrelevent” de CC

Modèles de CC
- Modèle non “proof-irrelevent”

Réalisabilité
- Réalisabilté de Kleene
- Réalisabilité modifiée de Kreisel

Réalisabilité

- Interpréter les termes par des programmes
- L'interprétation produit une spécification du programme
- On montre que pour tout jugement dérivable, il existe un programme qui le réalise

Rappel : sémantique de Heyting

Constructivité :

- preuves de $A \wedge B$: paire (π_A, π_B)
- preuves de $A \Rightarrow B$: fonction $(\pi_A \mapsto \pi_B)$
- preuves de $\exists x.P$: paire $(t, \pi_{P(t)})$
  (contre-exemples en logique classique)

Idée : extraire le témoin et obtenir une preuve qu'il satisfait P.

Problème : dans $\forall x, P(x) \Rightarrow \exists y, Q(x, y)$, y peut dépendre de la preuve de $P(x)$.

Réalisabilité de Kleene

Réalisations : fonctions récursives partielles

$$
\begin{array}{ll}
x \,\mathbf{r}\, A & = x = 0 \wedge A \quad \text{si } A \text{ atomique} \\
x \,\mathbf{r}\, A \wedge B & = \mathrm{fst}(x) \,\mathbf{r}\, A \ \wedge \ \mathrm{snd}(x) \,\mathbf{r}\, B \\
f \,\mathbf{r}\, A \Rightarrow B & = \forall x, x \,\mathbf{r}\, A \ \Rightarrow \ f(x) \Downarrow \ \wedge f(x) \,\mathbf{r}\, B \\
x \,\mathbf{r}\, \exists x, P & = \mathrm{snd}(x) \,\mathbf{r}\, P(x \backslash \mathrm{fst}(x)) \\
f \,\mathbf{r}\, \forall x, P & = \forall x, f(x) \Downarrow \ \wedge f(x) \,\mathbf{r}\, P(x)
\end{array}
$$

Thm : $\vdash A \Rightarrow \exists x, x \Downarrow \ \wedge \, x \,\mathbf{r}\, A$
(Généralisation : $\Gamma \vdash A \Rightarrow \forall \rho, \rho \,\mathbf{r}\, \Gamma \Rightarrow \exists x, x \Downarrow \wedge x \,\mathbf{r}\, A\rho$)

Conséquences de la réalisabilité de Kleene

- justification du principe de Markov :
  $(\forall x : \mathrm{nat}, P(x) \vee \neg P(x)) \Rightarrow \neg\neg\exists x, P(x) \Rightarrow \exists x, P(x)$
  (justifié par un programme testant $P(n)$ avec n croissant)
- non dérivabilité de l'indépendance des prémisses :
  $(\neg A \Rightarrow \exists x, P(x)) \Rightarrow \exists x, \neg A \Rightarrow P(x)$
  (si le témoin ne termine pas lorsque A est vrai)

Réalisabilité modifiée de Kreisel

Réalisations : λ-termes simplement typés (terminants)

$$
\begin{array}{ll}
\mathbf{t}(A) & = \mathrm{nat} \\
\mathbf{t}(A \wedge B) & = \mathbf{t}(A) \times \mathbf{t}(B) \\
\mathbf{t}(A \Rightarrow B) & = \mathbf{t}(A) \to \mathbf{t}(B) \\
\mathbf{t}(\exists x : \tau, P) & = \tau \times \mathbf{t}(P) \\
\mathbf{t}(\forall x : \tau, P) & = \tau \to \mathbf{t}(P)
\end{array}
\qquad
\begin{array}{ll}
x \,\mathbf{r}\, A & = x = 0 \wedge A \quad \text{si } A \text{ atomique} \\
x \,\mathbf{r}\, A \wedge B & = \mathrm{fst}(x) \,\mathbf{r}\, A \ \wedge \ \mathrm{snd}(x) \,\mathbf{r}\, B \\
f \,\mathbf{r}\, A \Rightarrow B & = \forall x, x \,\mathbf{r}\, A \ \Rightarrow \ f(x) \Downarrow \ \wedge f(x) \,\mathbf{r}\, B \\
x \,\mathbf{r}\, \exists x : \tau, P & = \mathrm{snd}(x) \,\mathbf{r}\, P(x \backslash \mathrm{fst}(x)) \\
f \,\mathbf{r}\, \forall x : \tau, P & = \forall x, f(x) \Downarrow \ \wedge f(x) \,\mathbf{r}\, P(x)
\end{array}
$$

Thm : $\vdash A \Rightarrow \exists x : \mathbf{t}(A), x \,\mathbf{r}\, A$

Conséquences de la réalisabilité modifiée de Kreisel

- non dérivabilité du principe de Markov :
  $(\forall x : \mathrm{nat}, P(x) \vee \neg P(x)) \Rightarrow \neg\neg\exists x, P(x) \Rightarrow \exists x, P(x)$
- justification de l'indépendance des prémisses :
  $(\neg A \Rightarrow \exists x, P(x)) \Rightarrow \exists x, \neg A \Rightarrow P(x)$
  $\lambda f.(\mathrm{fst}(f\ 0), \lambda p.\mathrm{snd}(fp))$