# Assistants de preuve

MPRI - 2007-2008

8- Sémantique du Calcul des Constructions et du Calcul des Constructions Inductives

# Des modèles, pour quoi faire ?

Pour déterminer si un théorème est prouvable dans un théorie telle que le CC ou le CCI, une seule méthode... exhiber une preuve !

Mais comment montrer qu'un théorème, ou un axiome standard des mathématiques, n'est pas prouvable. C'est-à-dire, comment montrer des résultats de la forme $\not\vdash A$ pour $A$ un énoncé donné ? Par exemple :

- montrer la cohérence de CC ou du CCI : $\not\vdash \bot$

- montrer la cohérence de CC étendu avec la logique classique : $\forall A\!:\!Prop.(A \vee \neg A) \not\vdash_{CC} \bot$

- montrer la cohérence de CC étendu avec l'axiome de description :

$$\forall A\,B\!:\!\texttt{Type}.\,\forall P\!:\!A \to B \to \texttt{Prop}.\,(\forall x\!:\!A.\,\exists!y\!:\!B.\,P\,x\,y) \to (\exists f\!:\!A \to B.\,\forall x\!:\!A.\,P\,x\,(f\,x)) \not\vdash_{CC} \bot$$

- montrer la non dérivabilité de $0 \neq 1$ dans le CC : $\not\vdash_{CC} 0 \neq 1$

- montrer la non dérivabilité du schéma d'induction dans le CC :

$$\not\vdash_{CC} \forall P\!:\!N \to \texttt{Prop}.\,P\,0 \to (\forall n\!:\!N.\,P\,n \to P\,(S\,n)) \to \forall n\!:\!N.\,P\,n$$

- etc.

$\hookrightarrow$ c'est là qu'un « modèle » s'avère utile!

# Les modèles : des outils pour mettre en évidence des invariants des preuves

Les modèles intéressants mettent en évidence des invariants mathématiques compatibles avec les choix de syntaxe...

L'exemple de base, et le plus standard, est le modèle booléen de la logique : à toute formule $A$ est associée une valeur de vérité $[\![A]\!] : bool$ et on a $\vdash A \ \Rightarrow \ [\![A]\!] = true$... la valeur booléenne d'une formule est un invariant pour les formules prouvables, puisque celles-ci (dans un système cohérent) sont toutes interprétés par la valeur booléenne $true$.

Si de plus on s'arrange pour que la formule $\bot$ ne préserve pas l'invariant des formules prouvables, alors, on peut affirmer que $\bot$ n'est pas dérivable et que la logique (ou la logique étendue avec certaines axiomes intéressants) est cohérente.

D'une manière plus générale, on va pouvoir montrer des résultats de non dérivabilité si on sait uniformément interpréter tout séquent de la forme $\Gamma \vdash t : A$ (ici, c'est CC ou CCI qui nous intéressent) comme une proposition $[\![\Gamma \vdash A]\!]$ telle que

1- $\Gamma \vdash t : A \ \rightarrow \ [\![\Gamma \vdash A]\!]$

2- pour une formule digne d'intérêt $B$, l'interprétation de $[\![\vdash t : B]\!]$ est une proposition équivalente à $\bot$

car alors, on aura $\vdash t : B \ \rightarrow \ [\![\vdash t : B]\!]$, qui, littéralement, revient à $\vdash t : B \ \rightarrow \ \bot$, c'est-à-dire $\not\vdash t : B$

Notons qu'un tel raisonnement ne peut se dérouler, par le théorème d'incomplétude de Gödel, que dans un système logiquement strictement plus puissant que le langage initial puisque l'existence d'une formule non prouvable implique en particulier la cohérence du language initial.

# Les modèles : des outils pour mettre en évidence des invariants des preuves

Alternativement, on peut aussi se contenter de résultats de non dérivabilité relative en ne se plaçant que dans une logique faible (l'arithmétique) dans laquelle :

- on sait définir une interprétation $[\![\ ]\!]\ :\ \vdash_L\ \longmapsto\ \vdash_{L'}$ d'un système logique $L$ (ici, c'est donc CC ou CCI qui nous intéressent) vers un système d'inférence $L'$ bien choisi tel que $\Gamma \vdash_L t : \bot\ \rightarrow\ [\![\Gamma \vdash_L t : \bot]\!]$
- l'interprétation $[\![\vdash_L t : B]\!]$ d'une potentielle preuve de $B$ dans $L$ donne un séquent équivalent à la cohérence de $L'$

car alors, par contraposition, la cohérence de $L'$, équivalente à la non-dérivabilité de $[\![\vdash_L t : B]\!]$, entraînera l'absence de preuve de $B$ dans $L$.

Regardons quelques exemples...

# Modèles booléens et modèles de réalisabilité

Il existe deux grandes classes de modèles :

- les modèles « proof-irrelevant » identifient toutes les preuves et ils caractérisent donc des invariants logiques des formules

- les modèles de réalisabilité interprètent les formules comme des ensembles de termes-preuves et ils caractérisent des invariants calculatoires des preuves

Suite dans le chapitre 9 du polycopié...