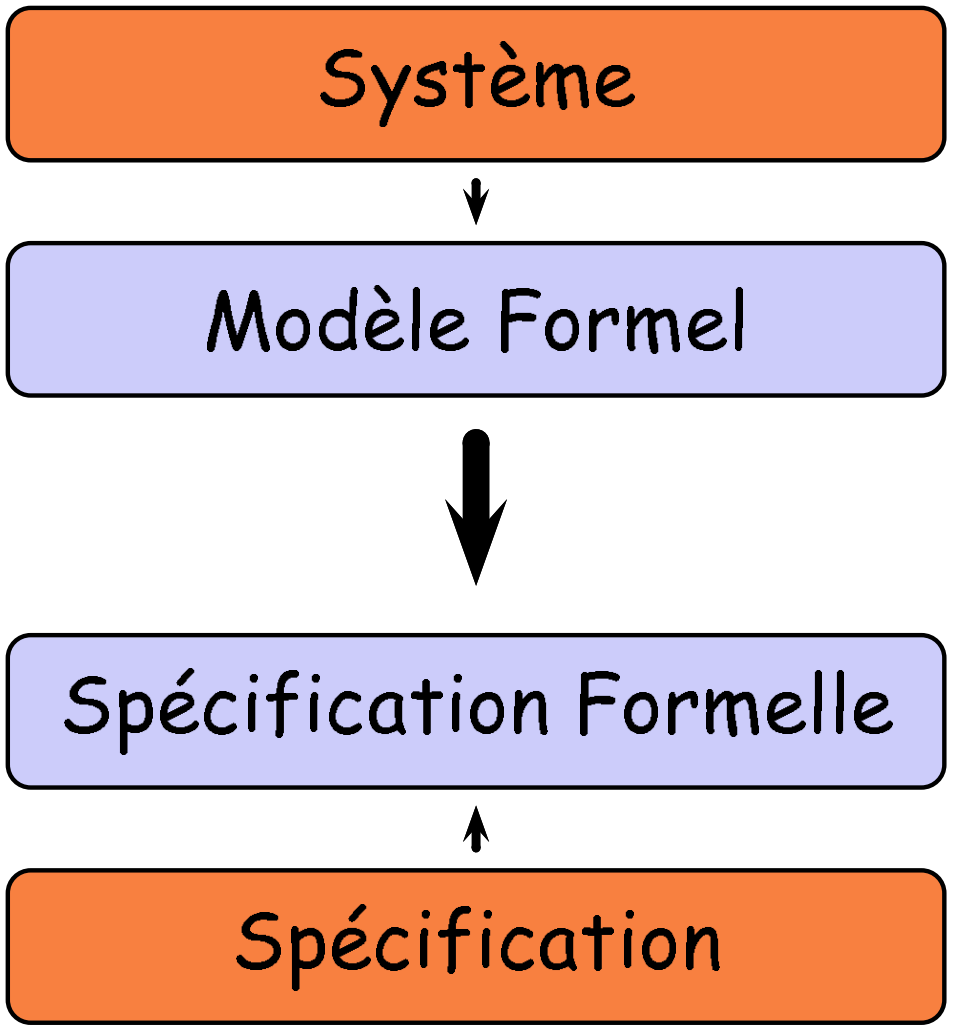
Preuve formelle pour les nuls

Laurent Théry
Marelle INRIA Sophia-Antipolis France

INRIA


Système
Modèle Formel
Spécification Formelle
Spécification

Plan

Fondamentaux:

- Qu'est-ce qu'une preuve?
- Spécifier et prouver
- Mélanger calcul et preuve

Outils pour TaMaDi

Preuve Formelle

Logique:

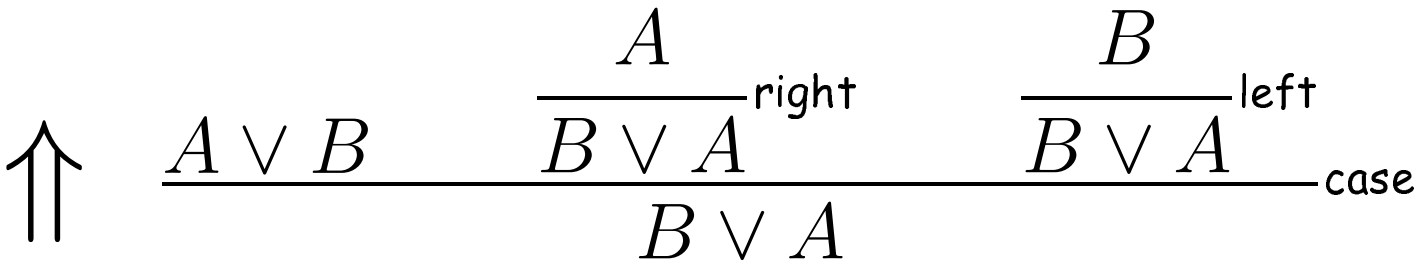
$$\neg \quad \wedge \quad \vee \quad \Rightarrow \quad \forall \quad \exists$$

Règles de base:

$$\frac{A}{A \vee B}\,\text{left} \qquad \frac{B}{A \vee B}\,\text{right} \qquad \frac{A \vee B \qquad \begin{array}{c}[A]\\ C\end{array} \qquad \begin{array}{c}[B]\\ C\end{array}}{C}\,\text{case}$$

Preuve Formelle

Preuve:



Preuve par chaînage arrière

Preuve Formelle

Preuve Interactive:

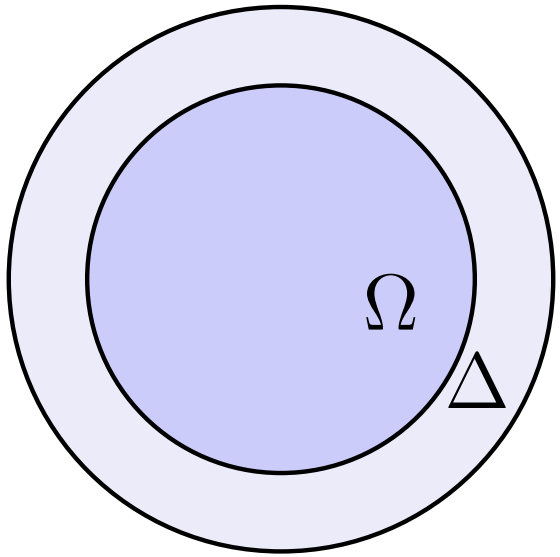
État:

$$\begin{array}{l} \mathrm{Hyp}_1 : \quad \ldots \\ \mathrm{Hyp}_2 : \quad \ldots \\ \vdots \\ \mathrm{Hyp}_n : \quad \ldots \\ \hline \qquad \mathrm{But} \end{array}$$

Tactique: État $\mapsto$ liste d'États

Preuve: Séquence de tactiques

Spécifier et Prouver



Extension

Si T est un théorème de Ω alors T est un théorème de $\Omega + \Delta$

Extension conservatrice

Si T est un théorème de $\Omega + \Delta$ et si T peut s'exprimer dans Ω alors T est un théorème dans Ω.

INRIA

Spécifier et Prouver

Définir un nouvel objet: définir un nouveau type

Les booléens:

$$\begin{aligned} \texttt{bool} &: \texttt{Type} \\ \texttt{true} &: \texttt{bool} \\ \texttt{false} &: \texttt{bool} \end{aligned}$$

$$\forall x : \texttt{bool}, x = \texttt{true} \vee x = \texttt{false}$$

Spécifier et Prouver

Définition à la ML

```
Inductive bool:Type := true | false.
```

Définition de fonctions par filtrage

```
Definition x && y :=
match x,y with
| true, true → true
|    _ , _ → false
end.
```

Mélanger calcul et preuve

Prouver des calculs

Calculer des preuves

Calculs externes/Vérifications internes

...

Outils Pour Tamadi

Bibliothèque des réels

Bibliothèque d'algèbre SSREFLECT

Preuve de programmes C