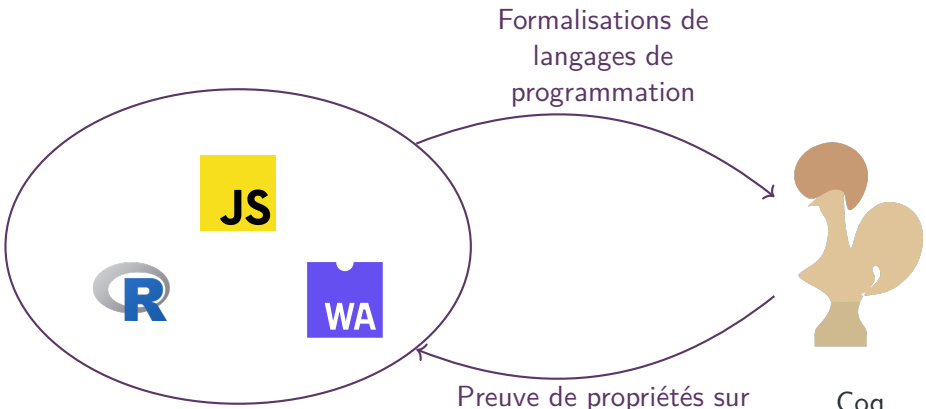
Les Assistants de preuve : l'exemple de Coq

Martin Bodin

Inria, équipe Spades

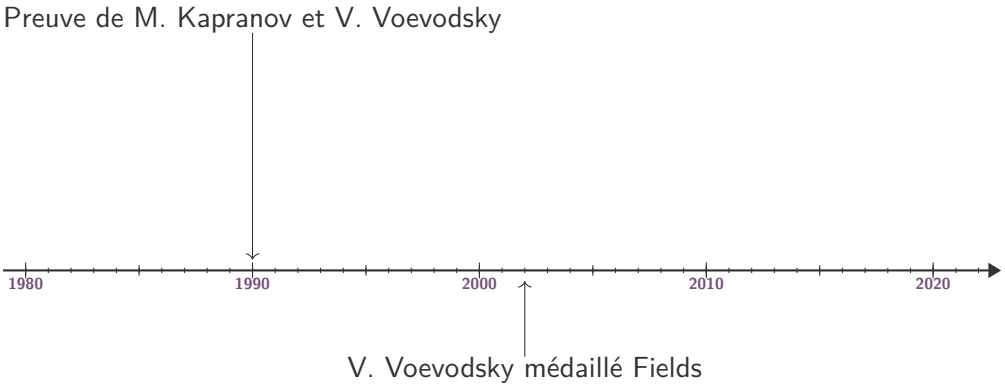
1er Juillet

Ma Recherche

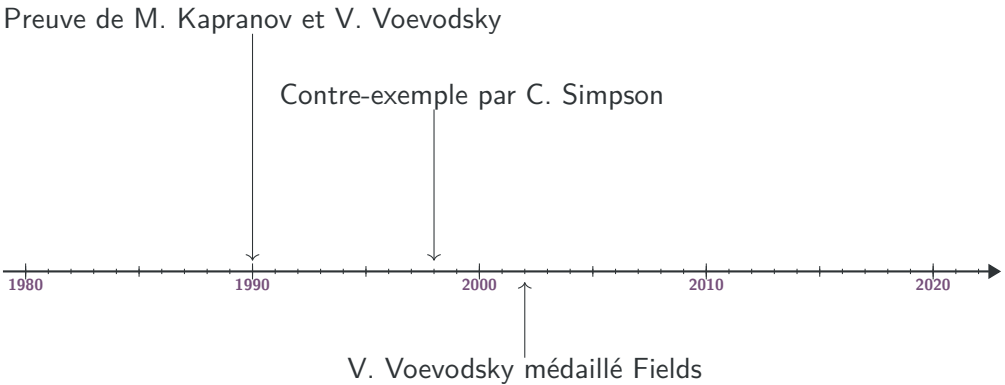


Du besoin de vérifier ses preuves

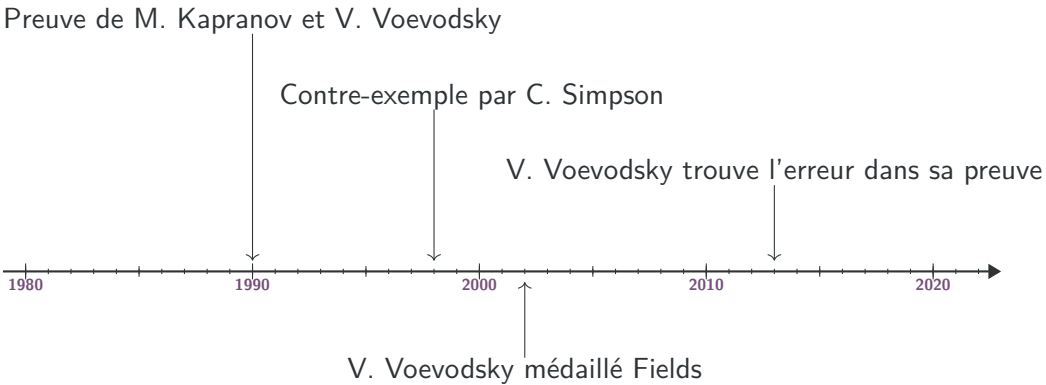
Histoire d'une preuve erronnée



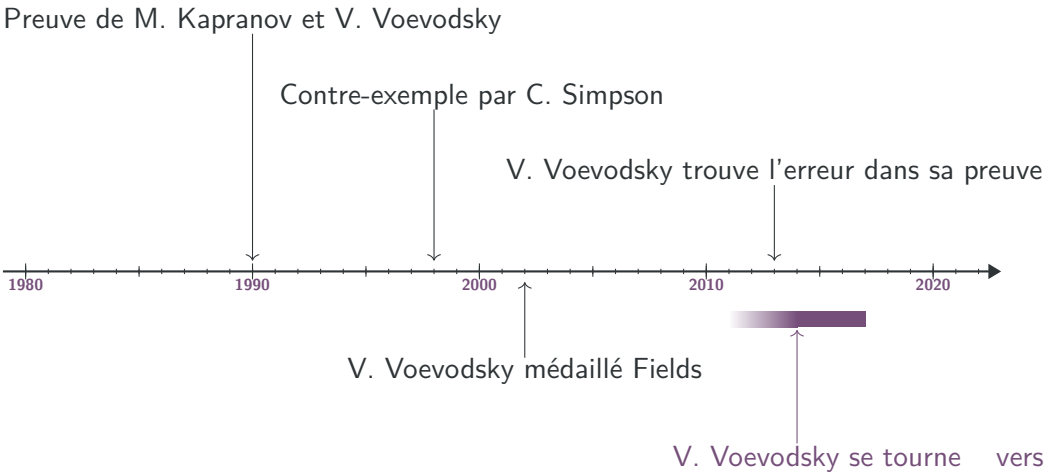
Histoire d'une preuve erronnée



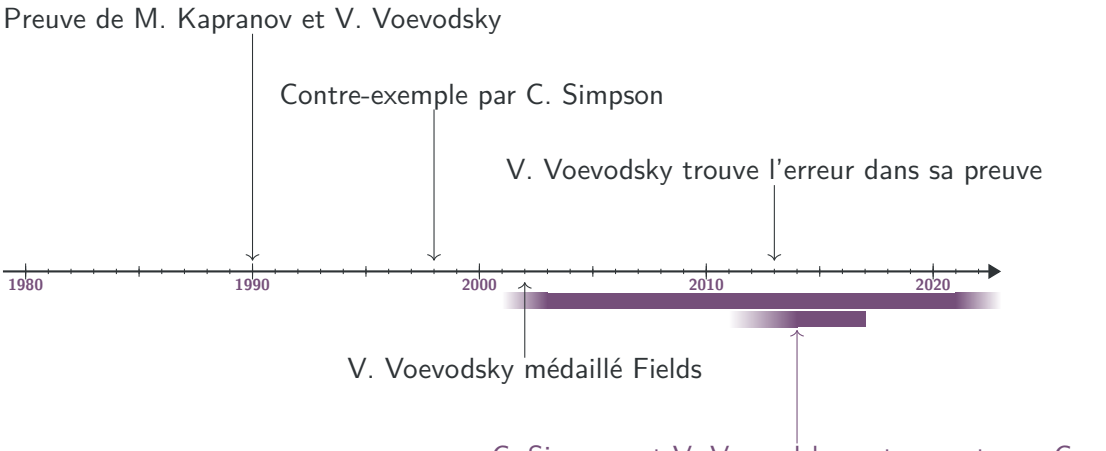
Histoire d'une preuve erronnée



Histoire d'une preuve erronnée



Histoire d'une preuve erronnée



Le diable se cache dans les détails.

"We had proved that an assertion was indeed true in all of the difficult cases, but it turned out to be false in the simple case. We never bothered to check." — V. Voevodsky

Conjecture sur le futur

Conjecture [V. Voevodsky]

Les mathématiciens du futur prouveront leurs théorèmes dans des assistants de preuve.

Conjecture sur le futur

Conjecture [V. Voevodsky]

Les mathématiciens du futur prouveront leurs théorèmes dans des assistants de preuve.

Corollaire

Les universités enseigneront aux étudiants comment utiliser des assistants de preuve.

Projet Inria : LiberAbaci

Adaptation des Systèmes de preuve pour l'enseignement des mathématiques universitaires

- Collaborations avec des enseignants,
- Fondements de la théorie des types,
- Structures, inférence et hiérarchies,
- Notations extensibles et langage de surface,
- Traitements automatiques,
- Environnements interactifs,
- Création de bibliothèque sur des domaines précis.

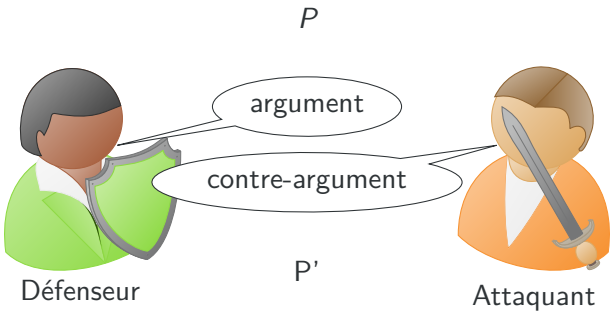
`https://liberabaci.gitlabpages.inria.fr/`

Comment fonctionne Coq ?

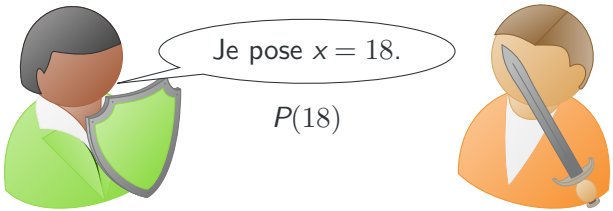
P

Défenseur

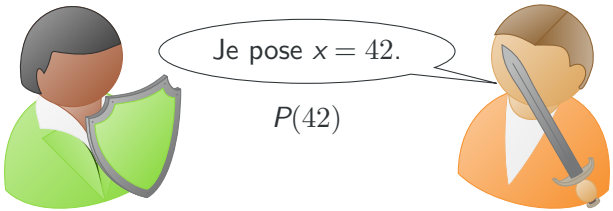
Attaquant


P
argument
contre-argument
P'
Défenseur
Attaquant

$\exists x, P(x)$



$\forall x, P(x)$



$A \Rightarrow B$

Défenseur

Attaquant

$A \Rightarrow B$

A

Attaquant

Défenseur

Défenseur

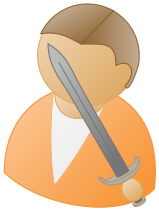
$A \Rightarrow B$

A

$\vdots$

A est montré

B



Attaquant

P

Défenseur

Attaquant

Definition (preuve)

Une preuve est une stratégie gagnante pour le défenseur.

Coq comme un adversaire

$$\forall x, P(x) \Rightarrow P(x)$$

Utilisateur

Coq

Coq comme un adversaire

$$\forall x, P(x) \Rightarrow P(x)$$

Je choisis x, sans dire lequel.

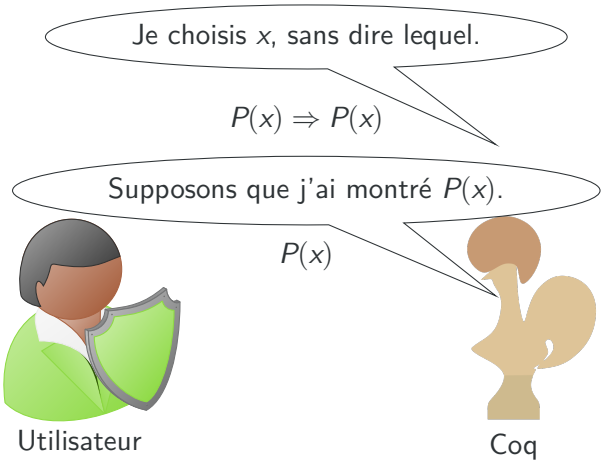
$$P(x) \Rightarrow P(x)$$

Utilisateur

Coq

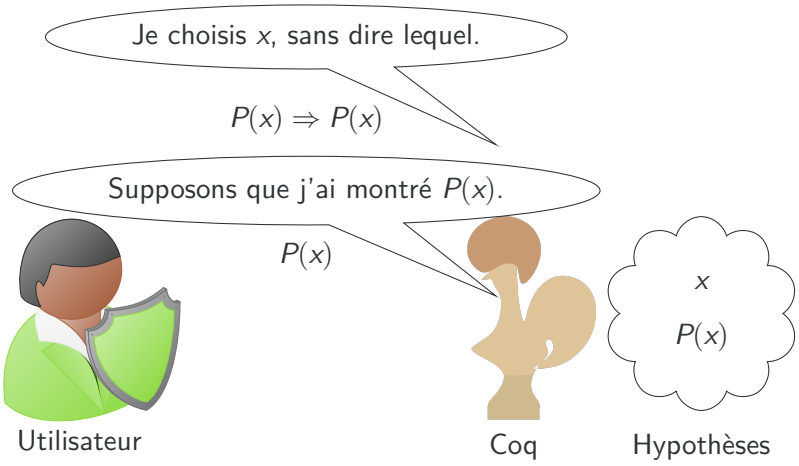
Coq comme un adversaire

$$\forall x, P(x) \Rightarrow P(x)$$



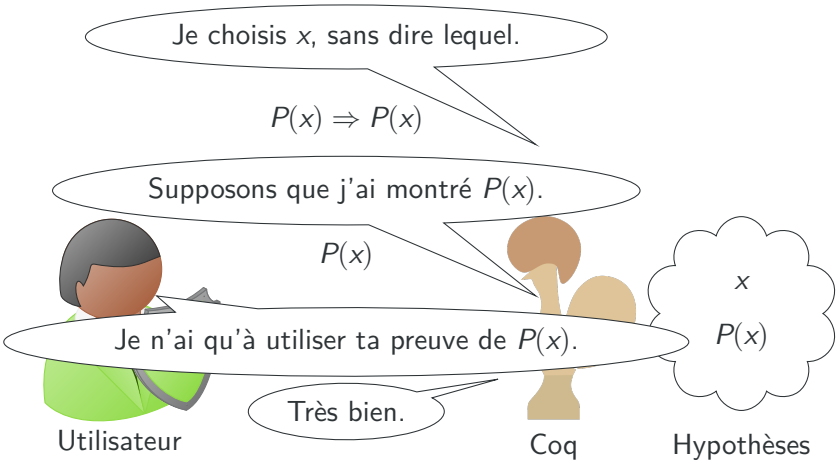
Coq comme un adversaire

$\forall x, P(x) \Rightarrow P(x)$



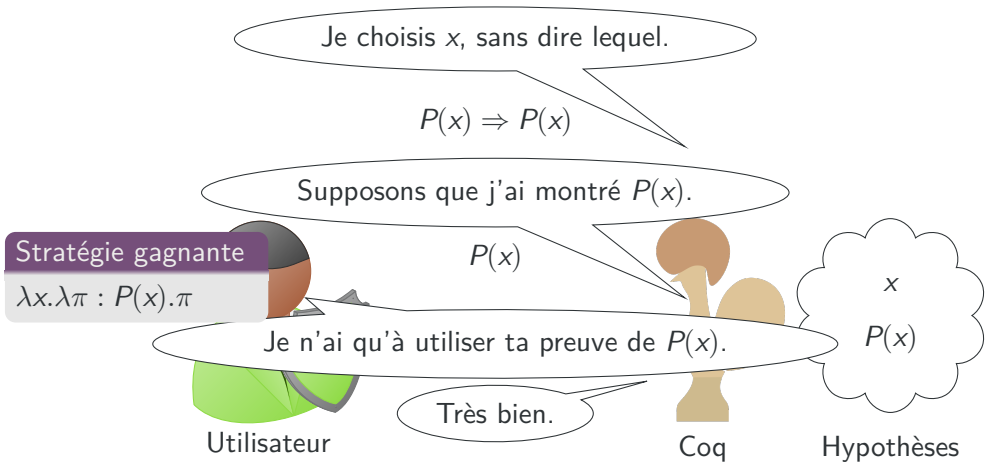
Coq comme un adversaire

$\forall x, P(x) \Rightarrow P(x)$



Coq comme un adversaire

$\forall x, P(x) \Rightarrow P(x)$



La stratégie $\lambda x.\lambda \pi : P(x).\pi$ est une preuve de $\forall x, P(x) \Rightarrow P(x)$.

La stratégie $\lambda x.\lambda \pi : P(x).\pi$ est une preuve de $\forall x, P(x) \Rightarrow P(x)$.

$$\lambda x.\lambda \pi : P(x).\pi : \forall x, P(x) \Rightarrow P(x)$$

La stratégie $\lambda x.\lambda \pi : P(x).\pi$ est une preuve de $\forall x, P(x) \Rightarrow P(x)$.

$$\lambda x.\lambda \pi : P(x).\pi : \forall x, P(x) \Rightarrow P(x)$$

Lorsqu'on utilise cette preuve, on devient l'adversaire

$$(\lambda x.\lambda \pi : P(x).\pi)\,(42) : P(42) \Rightarrow P(42)$$

$$(\lambda x.\lambda \pi : P(x).\pi)\,(42)(\pi : P(42)) : P(42)$$

Coq est correspond exactement à cette « joute »

"You tell the computer, 'Try,' and it tries, and it gives you back the result of its actions... Sometimes it's unexpected what comes out of it. It's fun."

Coq est correspond exactement à cette « joute »

"You tell the computer, 'Try,' and it tries, and it gives you back the result of its actions... Sometimes it's unexpected what comes out of it. It's fun."

$\approx$ jeu vidéo en mode texte.

Démos

Preuves mathématiques vérifiées par Coq

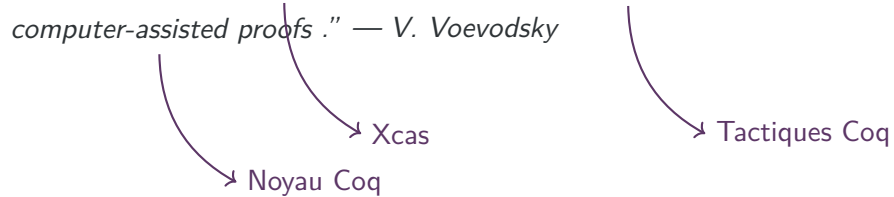
- Théorème fondamental de l'algèbre (d'Alembert-Gauss),
- Théorèmes d'incomplétude de Gődel,
- Indénombrabilité de $\mathbb{R}$,
- La série de Leibniz calcule π,
- Théorème des quatre couleurs,
- Inégalité de Cauchy-Schwarz,
- Et beaucoup d'autres !

Coq n'est là que pour vérifier des preuves

"Lots of people don't understand the difference between using computers for calculation , for computer-generated proofs , and for computer-assisted proofs ." — V. Voevodsky

Coq n'est là que pour vérifier des preuves

"Lots of people don't understand the difference between using computers for calculation , for computer-generated proofs , and for computer-assisted proofs ." — V. Voevodsky



Seriez-vous intéressés ?

Coq pour de l'enseignement universitaire

- Recueil des besoins (interface ou bibliothèque),
- Réflexions sur des TP en Coq,
- Expérimentations,
- Autres échanges.