Pourquoi faire appel à un ordinateur pour faire des preuves?

Yves Bertot

Février 2012

Motivation

- L'esprit humain
  - La matière première : émotions, souvenirs, désirs
  - Les techniques : rêveries, apprentissage, parole, absraction
  - La création : modèles, plans, savoir-faire
  - De la perception à la pensée consciente: subconscient et réflexes
- La rigueur est un outil précieux
  - La nature n'a pas d'émotions
  - Il faut vivre ensemble, convaincre et apprendre des autres
  - Toute oeuvre d'art respecte des règles
- L'ordinateur est un outil de créativité
  - Prendre en charge les tâches routinières
  - Libérer l'énergie créatrice

Illustration: Raphael: l'école d'Ahtènes, philosophie et logique utilisation de règles de perspective

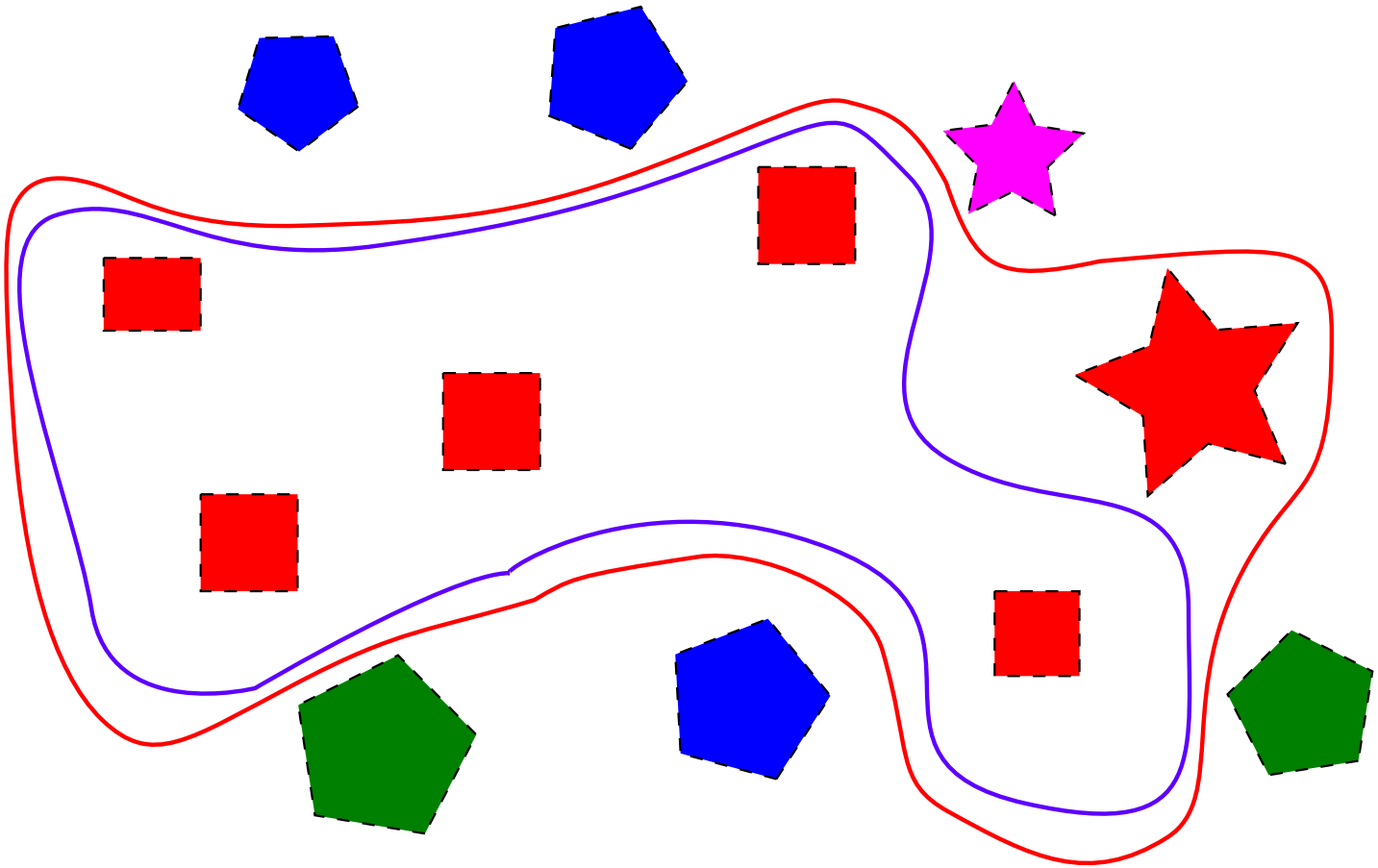
La logique

- L'art de convaincre un interlocuteur
- Indépendant de la connaissance des faits
  - Très abstrait
  - Important pour la découverte scientifique
- Utilise des règles qui ne s'intéressent qu'à la forme des phrases

Entrons dans le vif du sujet

- *Tous les hommes sont mortels*,
  Socrate est un homme,
  Donc Socrate est mortel
- Ceci est un syllogisme
- Les syllogismes sont connus et étudiés depuis l'antiquité

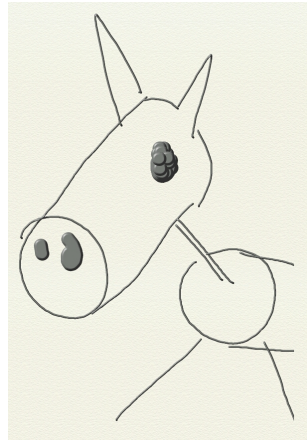
Une vision plus graphique



- Tous les rectangles sont rouges

Comment tricher

- Introduire une prémisse fausse ou incertaine
  - *Tout ce qui est rare est cher*
  - *Un cheval bon marché est rare*
  - *Donc un cheval bon marché est cher*
- Enfreindre la règle formelle
  - *Tous les chats sont mortels,*
  - *Socrate est mortel,*
  - *Donc Socrate est un chat*



Illustrations: Y. Bertot, Siné

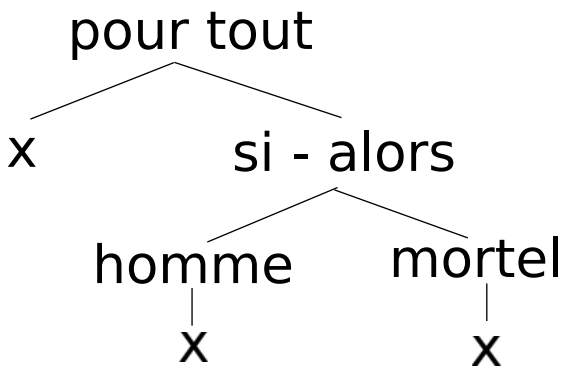
Et l'ordinateur dans tout ça?

- Un ordinateur ne manipule que des tableaux de (petits) nombres
- Mais un tableau de nombres peut représenter un graphe
- un graphe peut représenter une phrase
- Pour l'ordinateur, pas de différence entre un objet "concret" et un objet "abstrait"

d'une phrase à un tableau de nombres

Tout homme est mortel

Pour tout x, si (homme x) alors (mortel x)



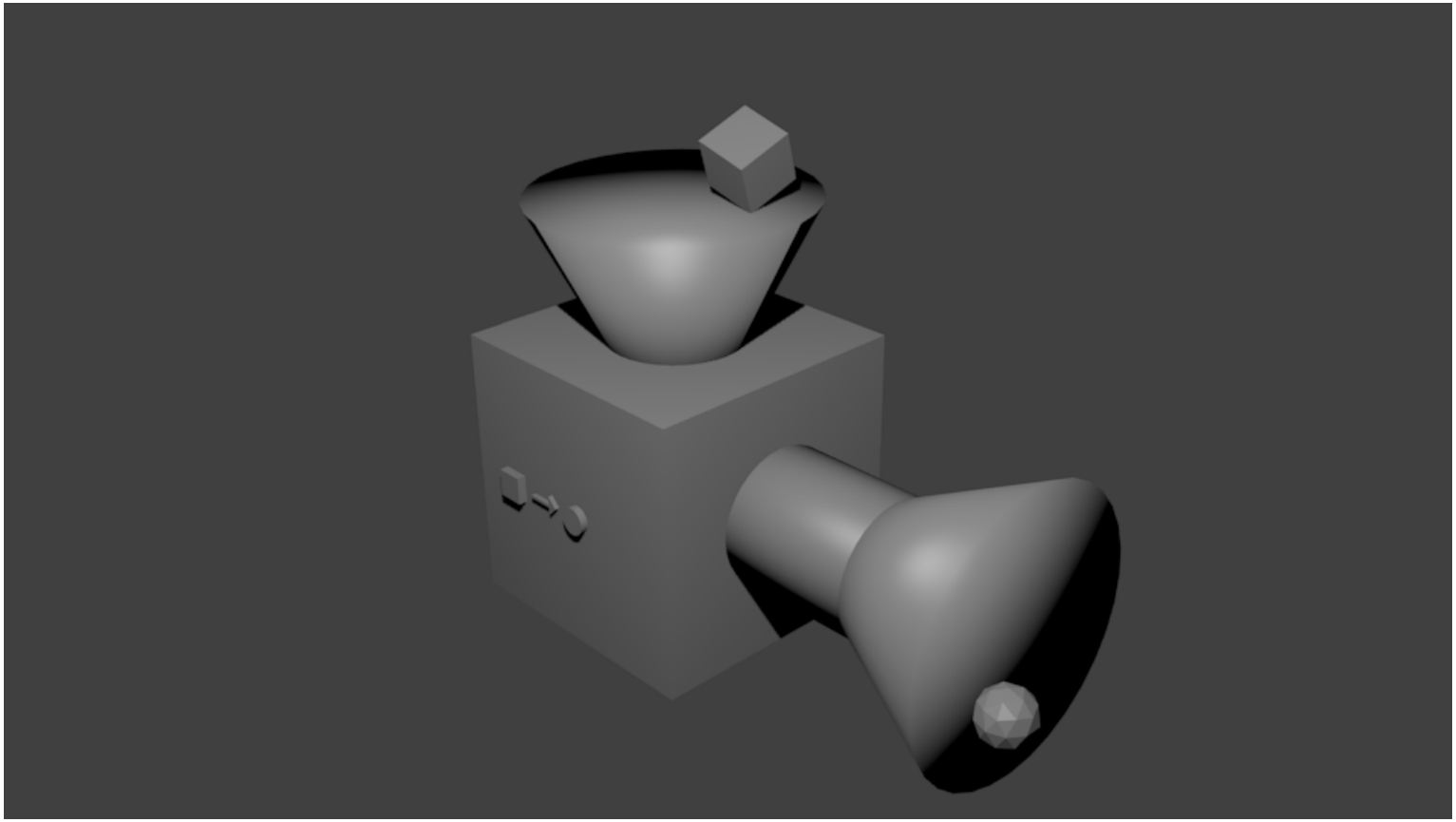
1	2	3	4	5	6	7	8	9	10	11
1	5	4	2	7	9	3	11	4	11	5

1	pour tout	3	homme	5	x
2	si-alors	4	mortel		

Calcul symbolique avec des formules

- avec une formule *si-alors* vraie et son premier terme aussi, on démontre le deuxième terme
- Dans une formule *pour tout* on peut remplacer la variable par n'importe quelle expression
- Pour démontrer une formule *si-alors*, on prouve le deuxième terme, en supposant que le premier terme est vrai
- Règles décrites très précisément dès la fin du XIXe siècle Boole, Frege, Gentzen

La logique c'est mécanique



Plus facile avec des exemples

- pour tout x, si (homme x) alors (mortel x)
- si (homme Socrate) alors (mortel Socrate)
- Par ailleurs on sait (homme Socrate)
- Donc on déduit (mortel Socrate)

Les preuves aussi sont des phrases, des graphes, des . . .

$$\dfrac{\dfrac{\dfrac{}{\text{A et B'}}}{\text{B}} \qquad \dfrac{\dfrac{}{\text{A et B'}}}{\text{A}}}{\dfrac{\text{B et A}}{\text{si (A et B') alors (B et A)}}}$$

- Chaque règle est représentée par une barre horizontale
- On doit vérifier des égalités entre formules
- Si B est la même chose que B' *par calcul* alors ça va

Preuves incomplètes et construction interactive

$$\dfrac{\dfrac{\dfrac{}{\text{A et B'}}}{\text{B}} \qquad \text{A}}{\text{B et A}}$$
$$\overline{\text{si (A et B') alors (B et A)}}$$

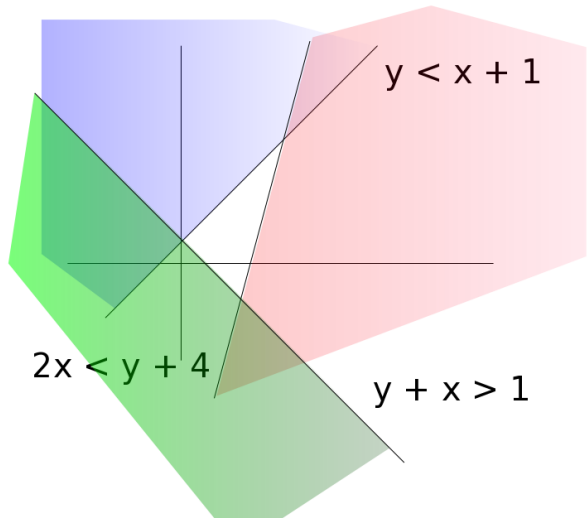
- Avec le système Coq, on affiche tous les faits autorisés et la formule à prouver
- `H : A et B'`
  `==================`
  `A`

Démonstrations automatiques

- Pour certaines classes de problème, on peut écrire un programme qui dit si oui ou non le problème admet une solution
- Exemples
  - Egalité entre formules obtenues par addition et multiplication
  - Comparaisons entre formules obtenues par addition et soustractions
  - Comparaisons entre formules obtenues par addition et multiplication

Comparaisons : Fourier et Presburger

- Existe-t-il x et y tels que (a) $2\,x < y + 4$, (b) $x + y > 1$, (c) $y < x + 1$?



- La combinaison de (a) et (c) donne $x < 5/2$, (b) et (c) donne $x > 0$
- Elimination de variable: y a disparu

Algorithmes de décision et preuve formelle

Trois méthodes

- Demander à l'algorithme de construire un bout de preuve à chaque étape
- Faire une preuve sur l'algorithme, puis faire confiance à l'algorithme
  - Pour tout p inférieur à n, diviser n par p,
  - n est premier si et seulement si le reste est 0 au moins une fois

Oui, mais . . . pourquoi?

- Cryptographie
- Mathématiques prouvées par programmes
- Logiciel fiable
- Calcul numérique sur ordinateur