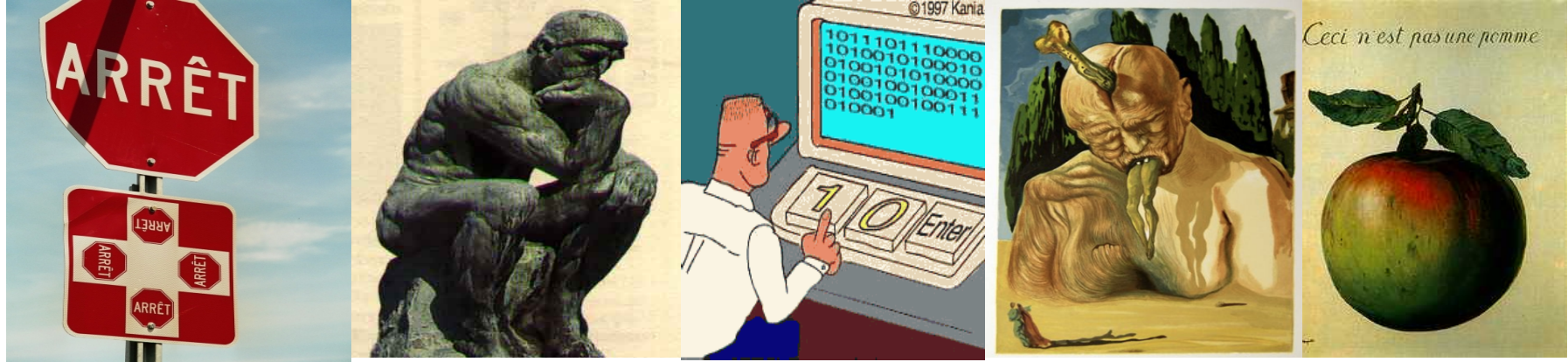


Introduction à la logique

Michel Rueher

S13

Qu'est ce que la logique ?



- Etre Logique ?
- Formaliser le raisonnement ?
- Automatiser le raisonnement ?
- Un art paradoxal ?

A quoi peut servir la logique ?

- Formaliser le **raisonnement** humain (**philosophie**, ...)
- Formaliser les **sciences** (**mathématiques**, ...)
- **Démontrer** (mathématiques, **preuves de propriétés de programmes**, ...)

Aristote (385-322) : syllogisme

Tous les hommes sont mortels.

Socrate est un homme.

Donc Socrate est mortel.

Toutes les poules ont trois pattes.

Bécassine est une poule.

Donc Bécassine a trois pattes.

Ce qui est rare est cher.

Un 4x4 bon marché est rare.

Donc un 4x4 bon marché est cher.

Le BDE a organisé une grande soirée dansante étudiants/enseignants. Mais les disques de -M- ont disparu !

Les SI3 déclarent:

si nous sommes coupables alors les professeurs sont coupables ou les SI5 sont coupables ou les SI4 sont innocents

Les SI4 déclarent:

les SI3 sont coupables et si les SI5 sont coupables alors les SI4 sont innocents

Les étudiants SI5 déclarent:

si les SI4 sont innocents alors les professeurs sont coupables

On formalisera ce problème en logique du premier ordre
(calcul propositionnel)

Axiomes :

$$A1: S3 \Rightarrow \neg S4 \vee S5 \vee P$$

$$A2 : S3$$

$$A3 : S5 \Rightarrow \neg S4$$

$$A4 : \neg S4 \Rightarrow P$$

\Rightarrow implication, \neg négation, \vee ou

On appliquera un procédé de **démonstration syntaxique déductif** noté \vdash

Procédé de déduction syntaxique :

$$\frac{P \vee T, P \Rightarrow Q}{Q \vee T}$$

" $Q \vee T$ se déduit syntaxiquement de $P \vee T$ et $P \Rightarrow Q$ "

Autre notation : $P \vee T, P \Rightarrow Q \vdash Q \vee T$

Axiomes :

A1: $S3 \Rightarrow \neg S4 \vee S5 \vee P$

A2 : S3

A3 : $S5 \Rightarrow \neg S4$

A4 : $\neg S4 \Rightarrow P$

On peut déduire de ces axiomes :

A1 et A2 : $S3, (S3 \Rightarrow \neg S4 \vee S5 \vee P) \vdash \neg S4 \vee S5 \vee P$

Les SI4 sont innocents ou les SI5 ou les professeurs sont coupables

A3 et $\neg S4 \vee S5 \vee P$: $S5 \Rightarrow \neg S4, \neg S4 \vee S5 \vee P$ (A3) $\vdash \neg S4 \vee P$

Les SI4 sont innocents ou les professeurs sont coupables

A4 et $\neg S4 \vee P$: $\neg S4 \Rightarrow P, \neg S4 \vee P \vdash P$

Les professeurs sont coupables

*On ne peut rien déduire
sur SI4 et SI5 (ni sur MAM)*

Considérons les formules

$$\mathbf{A1 : } \forall \mathbf{x} \forall \mathbf{y} \forall \mathbf{z} (\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z})$$

$$\mathbf{A2 : } \forall \mathbf{x} (\mathbf{x} + \mathbf{0} = \mathbf{x})$$

$$\mathbf{A3 : } \forall \mathbf{x} \exists \mathbf{y} (\mathbf{x} + \mathbf{y}) = \mathbf{0}$$

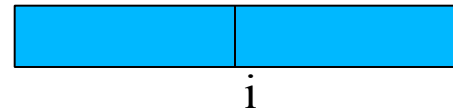
- Que représentent-elles ?
- La formule suivante peut-elle être prouvée à partir de A1, A2, A3 ?

$$\mathbf{\phi : } \forall \mathbf{x} \forall \mathbf{z} \exists \mathbf{y} \mathbf{x} + \mathbf{y} = \mathbf{z}$$

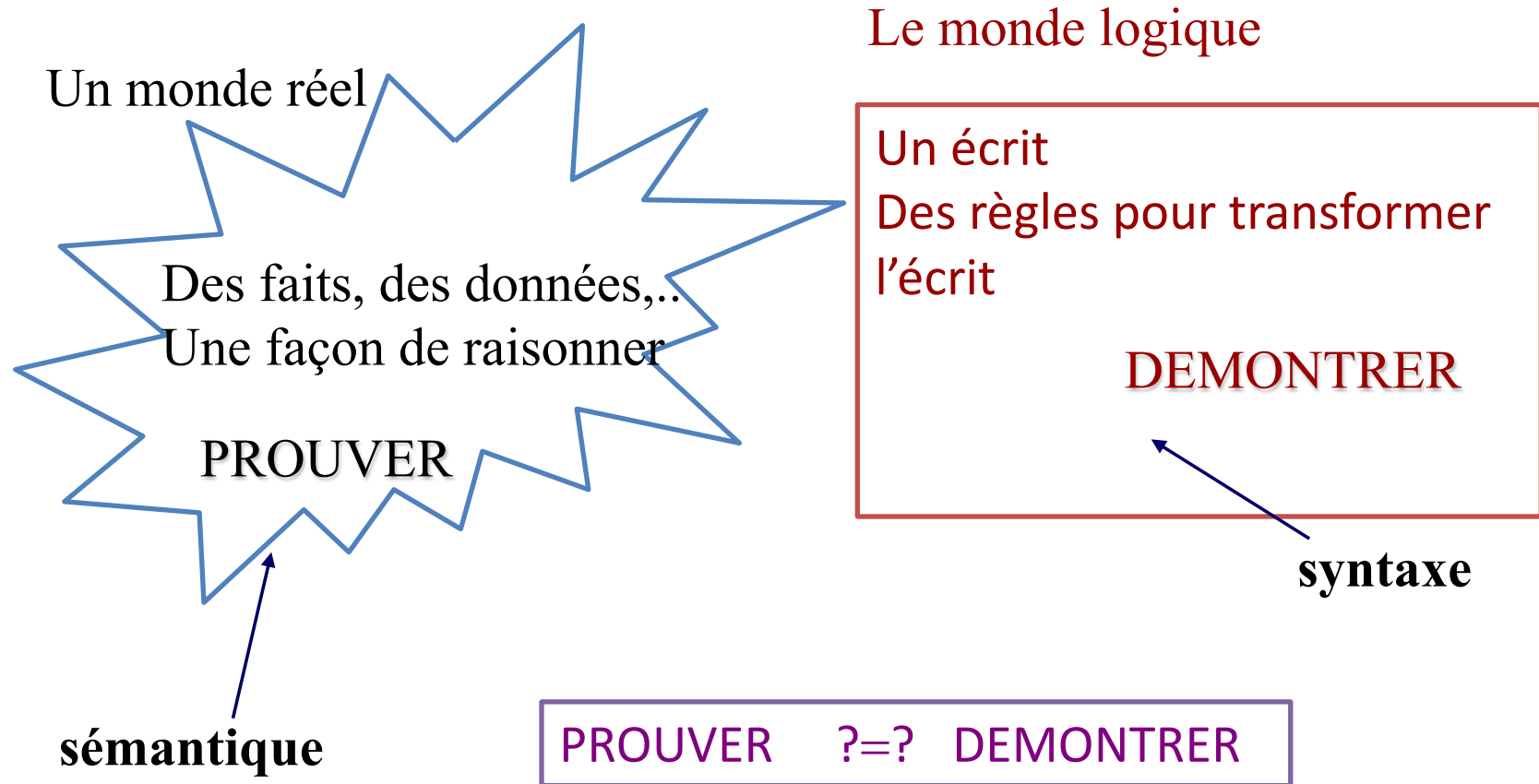
La méthode triInsertion est-elle **correcte** ?

```
/*@ public normal_behavior  
@ ensures (\forall int i; 0 <= i && i < t.length-1; t[i] <= t[i+1])  
@*/
```

```
static void triInsertion(int [] t) {  
  for (int i = 1; i < t.length; i++) {  
    int x = t[i];  
    int j = i - 1;  
    while ((j >= 0) && (x < t[j])) {  
      t[j + 1] = t[j];  
      j--;  
    }  
    t[j] = x;  
  }  
}
```



Le défi de la logique



Démontrer [?] = Prouver

Démontrer :

- une théorie τ (langage + axiomes)

- une formule Φ

Φ est-elle une conséquence logique de la théorie τ ?

- Etant donné un monde réel, **existe-t-il une théorie** pour le décrire?
- Une formule prouvée (sémantiquement) peut-elle être démontrée (syntaxiquement) ?
- Quand on démontre syntaxiquement une formule, **dans quels domaines sémantiques est-elle vraie** ?

Ingénieur informaticien

- le programme termine ou boucle
- si le programme termine alors il affiche « don' t worry »
- si le programme boucle ou affiche « don' t worry » alors l'ingénieur informaticien est bien payé

Montrer que l'ingénieur informaticien est bien payé.

sémantique

On peut formaliser ces énoncés par :

- $A1 : P \vee Q$
- $A2 : P \Rightarrow R$
- $A3 : Q \vee R \Rightarrow T$

On peut déduire T par la règle de déduction syntaxique

$$X \vee Y, X \Rightarrow Z \quad \vdash \quad Z \vee Y$$

- $A1, A2 \quad \vdash \quad Q \vee R$
- $Q \vee R, A3 \quad \vdash \quad T$

syntaxe

Si on pose :

P : l'eau est potable

Q : l'eau est abondante

R : les hommes sont heureux

T : la paix règne sur terre

On obtient :

- L'eau est potable ou abondante
- Si l'eau est potable alors les hommes sont heureux
- Si l'eau est abondante ou les hommes sont heureux, alors la paix règne sur terre

Peut-on en déduire que la paix règne sur terre ?

On a démontré que T se déduit de :

- A1 : $P \vee Q$
- A2 : $P \Rightarrow R$
- A3 : $Q \vee R \Rightarrow T$

syntaxe

en appliquant la règle de déduction \vdash

On peut conclure que la paix règne sur terre
si deux conditions sont vérifiées :

sémantique

- le domaine sémantique est un **modèle** de $\{A1, A2, A3\}$
A1, A2 et A3 sont vrais quand on interprète P par « l'eau est potable »,
Q par « l'eau est abondante », R par « les hommes sont heureux » et T
par « la paix règne sur terre »
- la règle de déduction \vdash a la propriété :
« si $A \vdash T$, alors T est valide dans **tous les modèles de A** »,

*Tous les modèles de A :
quel que soit le domaine des variables, quel que soit
le sens des fonctions et des prédicats, qui valident A*

Questions à se poser sur les procédés de démonstration syntaxique :

- **Question 1 :**

Quand on déduit une formule Φ d'un ensemble d'axiomes A par un procédé de démonstration syntaxique, peut-on en conclure que Φ est valide dans tous les domaines sémantiques qui sont des modèles de A ?

correction

- **Question 2 :**

Quand une formule Φ se déduit d'un ensemble d'énoncés A dans un domaine sémantique, le procédé de déduction syntaxique permet-t-il de démontrer Φ ?

complétude

Où il faut être prudent avant d'énoncer une vérité

Monde syntaxique S

$$A1: f(\perp, x) = x$$

$$A2 : f(g(x), y) = g(f(x, y))$$

Monde sémantique M1

domaine : les entiers naturels

opérations :

f : + (addition)

g : s (successeur)

\perp : 0 (la constante 0)

M1 est un « modèle » de S :

A1 et A2 sont valides dans le monde M1

$0+x = x$ et $s(x) + y = s(x+y)$ sont vrais

Monde sémantique M2

domaine : les listes de a et b

opérations :

f : append (concaténation)

g : cons_a (rajoute a en tête de liste)

⊥ : null (la constante liste vide)

Monde syntaxique S (rappel)

A1: $f(\perp, x) = x$

A2 : $f(g(x), y) = g(f(x, y))$

M2 est un « modèle » de S : A1 et A2 sont vrais dans le monde M2

$\text{append}(\text{null}, l) = l$ et $\text{append}(\text{cons}_a(l1), l2) = \text{cons}_a(\text{append}(l1, l2))$ sont vrais

Monde sémantique M3

domaine : les entiers naturels

opérations :

f : * (multiplication)

g : s (successeur)

⊥ : 0 (la constante 0)

M3 n'est pas un « modèle » de S : $x * 0 = x$ est faux dans M3

On suppose connus deux procédés syntaxiques qui permettent de faire des démonstrations dans S:

Déduction syntaxique : utiliser les égalités des axiomes de gauche à droite

Induction syntaxique : utiliser les égalités des axiomes de gauche à droite **puis la formule à prouver**

- On peut démontrer avec *la déduction syntaxique* que

$$f (g (g (x)) , y) = g (g (f (x , y)))$$

- On peut démontrer avec *l'induction syntaxique* que

$$f (x , y) = f (y , x)$$

D'un point de vue sémantique

Validité de $f(g(g(x)), y) = g(g(f(x, y)))$

- Dans M1 : $s(s(x)) + y = s(s(x + y))$ est vrai
- Dans M2 : $\text{append}(\text{cons}_a(\text{cons}_a(11)), 12) = \text{cons}_a(\text{cons}_a(\text{append}(11, 12)))$
est vrai

Validité de $f(x, y) = f(y, x)$

- Dans M1 : $x + y = y + x$ est vrai

MAIS

- Dans M2 : $\text{append}(l1, l2) = \text{append}(l2, l1)$ est **faux!!!!**

contre-exemple: - $\text{append}(aaaba, baa)$ vaut $aaababaa$

- $\text{append}(baa, aaaba)$ vaut $baaaaaba$

Où est la faille ?

- Les axiomes A1 et A2 permettent « de construire de façon unique » tout entier (i.e toute donnée du monde M1).

M1 est un modèle particulier « *modèle initial* » de S

- Les axiomes A1 et A2 **ne disent rien** sur les listes contenant des b!!! (i.e certaines données du monde M2 **ne sont pas représentées** par S)

Exemple : les éléments aaaba et aab ne peuvent pas être dérivés à partir de null, cons_a et append.

M2 est un modèle quelconque

Ce qui est démontré avec *la déduction syntaxique* est vrai dans *tous_les_modèles*

$f (g (g (x)) , y) = g (g (f (x , y)))$ est donc valide dans M1 et M2

Ce qui est démontré avec *l'induction syntaxique* est vrai dans les *modèles_initiaux*

$f (x , y) = f (y , x)$ est donc valide dans M1

***L'induction syntaxique* ne nous dit rien sur la validité de**

$f (x , y) = f (y , x)$ dans M2

Remarque :

Cf cours utilisation des schémas d'induction libres pour faire des preuves inductives

Dans quels types de modèles le procédé de démonstration syntaxique assure-t-il la validité des formules déduites ?

Dans ce cours nous verrons trois procédés de démonstration syntaxique : la résolution et le remplacement d'égaux (déduction) et l'induction.

Les deux premiers assurent la validité dans tous les modèles, l'induction assure la validité dans les modèles initiaux

Syntaxe et sémantique : que nous apporte la logique (du premier ordre) ?

- Des méthodes de démonstration (syntaxique) qui assurent :
 - ce qui est démontré est vrai dans *tous les modèles*
 - ce qui est vrai dans *tous les modèles* est démontrable (théorème de complétude de Gödel 1930)

Les formules qui sont vraies dans *tous les modèles* ne sont pas les plus intéressantes pour l'informatique.

Ce sont les formules qui correspondent à un raisonnement logique. Par exemple, la formule « $M(a)$ » est vraie dans *tous les modèles* de

A1 : $\forall x (H(x) \Rightarrow M(x))$

A2 : $H(a)$

Les formules qui nous intéressent le plus en informatique, sont les formules qui sont vraies dans les *modèles initiaux*

Ces formules nécessitent une connaissance de la structure des éléments.

Par exemple, la formule « $x + y = y + x$ » est vraie dans les *modèles initiaux* de

$$A1 : 0 + x = x$$

$$A2 : s(x) + y = s(x+y)$$

Elle **n'est pas vraie dans tous les modèles** de $\{A1, A2\}$
(on a vu que l'interprétation M2 dans les listes de a et b est un modèle de $\{A1, A2\}$ mais que $x + y = y + x$ est fausse dans M2)

Synthèse

- Il existe des méthodes de démonstration (syntaxique) qui assurent que *ce qui est démontré est vrai dans le modèle initial*
- Il n'existe pas de procédé de démonstration qui permette de démontrer *n'importe quelle formule vraie du modèle initial*
- Quel que soit le système finiment axiomatisé cohérent et capable de formaliser l'arithmétique, on peut toujours construire une formule vraie de l'arithmétique que l'on ne peut pas démontrer (*théorème d'incomplétude de Gödel*, 1931, basé sur l'autoréférence)

Autoréférences et Paradoxes

- « *Le barbier rase tous ceux et seulement ceux qui ne se rasent pas eux-mêmes* »



- « **Cette phrase est un mensonge** » (paradoxe du Crétois)
- « **La phrase suivante est fausse. La phrase précédente est vraie.** »
- « **Jésus-Christ, un autonomiste palestinien mort en 33 après lui-même** »

Pierre Desproges

Plan du cours

Une théorie est la donnée d'un langage et d'un ensemble d'axiomes

Théorie : syntaxe

- langage
- axiome

Théorie : sémantique

- interprétation
- validité

Théorie : preuves

- déductives
- inductives

Cas particulier des théories dont le langage est propositionnel (algèbre de boole)

Calcul des prédicats

Cadre de la logique équationnelle

Bibliographie

Zohar Manna: Mathematical Theory of Computation, Dover, 2003.

J. P. Delahaye : Outils logiques pour l'intelligence artificielle, Eyrolles

R. Lassaigne, M. de Rougemont : Logique et fondements de l'informatique Traité des nouvelles technologies, série informatique, Hermes

E. Burke, E. Foxley : Logic and its applications, Prentice hall int.

Open free courses:

<https://class.coursera.org/intrologic-005>

<http://oli.cmu.edu/courses/free-open/logic-proofs-course-details/>