Logique et Programmation Logique

Quentin Bramas

Largement inspiré par le cours de J.Narboux, C.Dubois et d'autres

ECOLE D'INGENIEURS TELECOM PHYSIQUE STRASBOURG

RT-INOC 1A

October 1, 2018

Table des matières I

Systèmes formels

Un système formel est composé de 3 éléments:

Systèmes formels

Un système formel est composé de 3 éléments:

1. le langage: un ensemble de formules

Systèmes formels

Un système formel est composé de 3 éléments:

1. le langage: un ensemble de formules
2. des axiomes: un sous ensemble des formules

Systèmes formels

Un système formel est composé de 3 éléments:

1. le langage: un ensemble de formules
2. des axiomes: un sous ensemble des formules
3. des règles de déduction (ou règles d'inférence): des fonctions qui associent des formules à d'autres formules

Systèmes formels

Un système formel est composé de 3 éléments:

1. le langage: un ensemble de formules
2. des axiomes: un sous ensemble des formules
3. des règles de déduction (ou règles d'inférence): des fonctions qui associent des formules à d'autres formules

Remarque: les axiomes peuvent être vus comme des règles sans prémisses.

Systèmes formels

Les manipulations effectuées dans un système formel sont purement syntaxiques et n'utilisent aucunement le sens que l'on peut associer aux formules.

Il est fréquent de noter les règles de la manière suivante:

$$\frac{P_1 \qquad P_2}{C} \text{ nom de la règle}$$

Les P_i sont appelées des prémisses, C la conclusion. La règle énonce le fait que de P_1 , P_2 on peut déduire C.

Théorème

Définition

Un théorème est une formule dont il existe une preuve.

Preuve

Définition

Preuve

Définition

Une preuve/déduction est un arbre dont:

- Les feuilles sont des axiomes.

Preuve

Définition

Une preuve/déduction est un arbre dont:

- Les feuilles sont des axiomes.
- Les noeuds correspondent à des applications des règles de déduction.

Preuve

Définition

Une preuve/déduction est un arbre dont:

- Les feuilles sont des axiomes.
- Les noeuds correspondent à des applications des règles de déduction.
- La racine est la formule prouvée.

Quelle est la différence entre un théorème, un lemme, un corollaire ?

Du point de vue de la logique formelle:

aucune.

Quelle est la différence entre un théorème, un lemme, un corollaire ?

Du point de vue de la logique formelle:

aucune.

Dans la pratique des mathématiques:

lemme assertion servant d'intermédiaire pour démontrer un théorème

corollaire assertion qui découle directement d'un théorème

Quelle est la différence entre une preuve mathématique et une preuve formelle ?

On pourrait dire qu'une preuve mathématique est une suite d'arguments pour convaincre un mathématicien de l'existence d'une preuve formelle.

Exemple 1

- Le langage: $L = \{(a, b) \in \mathbb{N}^2\}$
- Règles de déduction:

$$\frac{(n, n)}{(n+1, n+1)}\; n \in \mathbb{N}$$

- Axiomes: $A = \{(0, 0)\}$

Exemples de théorèmes

$(0,0)$, $(3,3)$, $(4,4)\ldots$

Exemple de déduction

$$\dfrac{\dfrac{\dfrac{\overline{(0,0)}}{(1,1)}}{(2,2)}}{(3,3)}$$

Exemple de formule qui n'est pas un théorème

$$(2, 3)$$

Pourquoi ?

Exemple de formule qui n'est pas un théorème

$$(2, 3)$$

Pourquoi ?

Si c'était un théorème alors il existerait un arbre de déduction dont c'est la racine, mais:

- Ce n'est pas un axiome.
- Aucune règle ne s'applique.

C'est donc impossible.

Remarque

Nous venons d'utiliser une méthode *syntaxique* pour montrer qu'une formule n'est pas un théorème. Il existe des méthodes *sémantiques*.

Après avoir donné un sens sémantique aux formules (lesquelles sont valides), on peux énoncer les propriétés qui suivent.

Correction, complétude

Correction

On dit qu'un système est correct quand tous les théorèmes sont des formules valides.

Correction, complétude

Correction

On dit qu'un système est correct quand tous les théorèmes sont des formules valides.

Complétude

On dit qu'un système est complet quand toutes les formules valides sont des théorèmes.

Reprenons notre exemple

Définissons la validité pour cet exemple

On dit qu'une formule $F = (a, b)$ est valide ssi $a = b$.

L'exemple 1 est-il un système correcte ?

L'exemple 1 est-il un système complet ?

Cohérence, consistance

Cohérence

On dit qu'un système formel est cohérent si les formules ne sont pas toutes des théorèmes.

Cohérence, consistance

Cohérence

On dit qu'un système formel est cohérent si les formules ne sont pas toutes des théorèmes.

Consistance

On dit qu'un système formel (comportant un symbole de négation $\neg$) est consistant s'il n'existe aucune formule F telle que F et $\neg F$ soient des théorèmes.

L'exemple 1 est-il un système cohérent ?

Saturé

On dit qu'un système formel S est saturé si pour toute formule F qui n'est pas une théorème, le système formel S' obtenu en ajoutant F aux axiomes de S est inconsistant.

Saturé

On dit qu'un système formel S est saturé si pour toute formule F qui n'est pas une théorème, le système formel S' obtenu en ajoutant F aux axiomes de S est inconsistant.

Décidable

On dit qu'un système formel S est décidable, si le problème de savoir si une formule est un théorème de S est décidable.

L'exemple 1 est-il un système saturé ?

L'exemple 1 est-il un système décidable ?

Exemple 2

- Le langage: $L = \{(a, b) \in \mathbb{N}^2\}$
- Règles de déduction:

$$\frac{(n, n)}{(n+1, n+1)}\ I$$

- Axiomes: $A = \{(1, 1)\}$

Exemple 3

- Le langage: $L = \{(a, b) \in \mathbb{N}^2\}$
- Règles de déduction:

$$\frac{(n, n)}{(n+2, n+2)}\ I$$

- Axiomes: $A = \{(0, 0)\}$

Exemple 4

- Le langage: $L = \{(a, b) \in \mathbb{N}^2\}$
- Règles de déduction: $\emptyset$
- Axiomes: $A = \{(n, n), n \in \mathbb{N}\}$

Exemple 5

- Le langage: $L = \{(a, b) \in \mathbb{N}^2\}$
- Règles de déduction:

$$\frac{(n, m)}{(n+1, m)}\ I_G$$

$$\frac{(n, m)}{(n, m+1)}\ I_D$$

- Axiomes: $A = \{(0, 0)\}$

David Hilbert (1862-1943)

Les systèmes *à la Hilbert*

Les systèmes *à la Hilbert* comportent

- de nombreux schémas d'axiomes,
- peu de règles d'inférence (souvent une seule).
- On ne manipule pas les hypothèses explicitement.

La logique propositionnelle minimale

- Une syntaxe très simple.
- Deux schémas d'axiomes.
- Une règle.

Langage

On se donne un seul connecteur binaire noté $\Rightarrow$ et des variables propositionnelles.

Exemples de formules

- P
- $A \Rightarrow A$
- $(A \Rightarrow B) \Rightarrow (B \Rightarrow A)$

Une règle

Le modus ponens:

$$\frac{A \Rightarrow B \qquad A}{B}\ \mathrm{MP}$$

Deux schémas d'axiomes

1. Axiome K: $A \Rightarrow (B \Rightarrow A)$
2. Axiome S: $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

Schémas d'axiomes

Définition

Un schéma d'axiomes est la définition d'une infinité d'axiomes à l'aide d'un motif.

Exemple:

Les axiomes suivants sont des instances du schéma $A \Rightarrow (B \Rightarrow A)$:

- $x \Rightarrow (y \Rightarrow x)$
- $(a \Rightarrow b) \Rightarrow (c \Rightarrow (a \Rightarrow b))$
- $(a \Rightarrow b) \Rightarrow ((a \Rightarrow b) \Rightarrow (a \Rightarrow b))$

Les systèmes à la Hilbert sont

- compliqués pour construire des preuves *dans* le système.
- plus adaptés pour construire des preuves *à propos* du système.

Exemple

Exercice:

Montrez que $A \Rightarrow A$ est un théorème de la logique minimale de Hilbert.

Exemple

Exercice:

Montrez que $A \Rightarrow A$ est un théorème de la logique minimale de Hilbert.

$$
\dfrac{
  \dfrac{
    \dfrac{}{(A \Rightarrow ((B \Rightarrow A) \Rightarrow A)) \Rightarrow ((A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A))}\,\mathrm{S}
    \qquad
    \dfrac{}{(A \Rightarrow ((B \Rightarrow A) \Rightarrow A)}\,\mathrm{K}
  }{(A \Rightarrow (B \Rightarrow A)) \Rightarrow (A \Rightarrow A)}\,\mathrm{MP}
  \qquad
  \dfrac{}{A \Rightarrow (B \Rightarrow A)}\,\mathrm{K}
}{A \Rightarrow A}\,\mathrm{MP}
$$

Le modèle

On utilise l'ensemble $\{0,1\}$ comme modèle. On fixe l'interprétation du symbole $\Rightarrow$ par la fonction de $\{0,1\}^2$ dans $\{0,1\}$ suivante:

A	B	$A \Rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

Exercice

1. Montrer que les axiomes sont valides.

Exercice

1. Montrer que les axiomes sont valides.
2. Montrer que la règle du modus ponens préserve la validité.

Exercice

1. Montrer que les axiomes sont valides.
2. Montrer que la règle du modus ponens préserve la validité.
3. Que peut-on en déduire ?

Méta-théorème

La notation $\vdash A$ signifie que A est un théorème.

Théorème d'adéquation/correction

Si $\vdash A$ alors $\models A$

Méta-théorème

La notation $\Gamma \vdash A$ signifie que, si on ajoute comme hypothèses les formules de Γ, alors A est un théorème.

Théorème de la déduction

$\Gamma \vdash B$ ssi $\vdash \Gamma \Rightarrow B$

Incomplétude

Formule de Peirce

$$((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$$

Exercice: montrer que la formule de Peirce est valide.

Incomplétude

Formule de Peirce

$$((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$$

Exercice: montrer que la formule de Peirce est valide.
On peut montrer que la formule de Peirce n'est pas un théorème de la logique minimale: la logique minimale est donc incomplète.

Solutions

On peut soit:

1. trouver un modèle adapté à la logique minimale ou bien,
2. modifier le système pour en trouver un qui corresponde à notre modèle.

Exercice: Preuve de la non-prouvabilité de la formule de Peirce
On définie un nouvelle interprétation pour les formules de la logique propositionnelle. On définie l'interprétation J comme une fonction de l'ensemble des variables propositionnelles dans l'ensemble $\{-1, 0, 1\}$. Une interprétation J s'étend à toutes les formules (n'utilisant que le connecteur $\Rightarrow$) de la façon suivante, $J(A \Rightarrow B)$

- est égale à -1 si $J(A) = 1$ et $J(B) = -1$
- est égale à 0 si $J(B) = 0$ et $J(A) \neq 0$
- est égale à 1 dans tous les autres cas

Le tableau suivant résume la valeur de $J(A \Rightarrow B)$ en fonction de $J(A)$ et de $J(B)$. En utilisant cette interprétation, on dit qu'une interprétation J satisfait une formule F si $J(F) = 1$ et **on dit qu'une formule F est valide, si toute interprétation satisfait F**. Dans la suite, on admettra que la formule axiome S: $(A \Rightarrow B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow A \Rightarrow C$ est valide.

A	B	$A \Rightarrow B$
0	0	1
0	1	1
0	-1	1
1	0	0
1	1	1
1	-1	-1
-1	0	0
-1	1	1
-1	-1	1

Questions :

1. Dresser le tableau de vérité des formules suivantes (en utilisant l'interprétation J).
    1. Axiome K: $B \Rightarrow A \Rightarrow B$
    2. Schéma de Peirce $\mathcal{P}$: $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
2. Pour notre interprétation, le système de Hilbert minimal H est-il correct ?
3. La formule de Peirce est-elle un théorème dans le système H ?
4. Que peut-on en déduire pour le système H avec l'interprétation standard I des formules (la définition de I vue au début du cours).
5. Soit H_+ le système H de Hilbert augmenté du schéma d'axiomes $\mathcal{P}$.
    1. Sous l'interprétation J, le système H_+ est-il correct ?
    2. Sous l'interprétation I, le système H_+ est-il correct ?