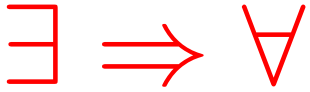
Logique et Calculabilité
INF551



Dr. Stéphane Lengrand,

Stephane.Lengrand@Polytechnique.edu

Point d'information

Une site web :

`http://www.lix.polytechnique.fr/~lengrand/`

Transparents, sujets de PC, ...

Une adresse e-mail :

`Stephane.Lengrand@Polytechnique.edu`

Horaires :

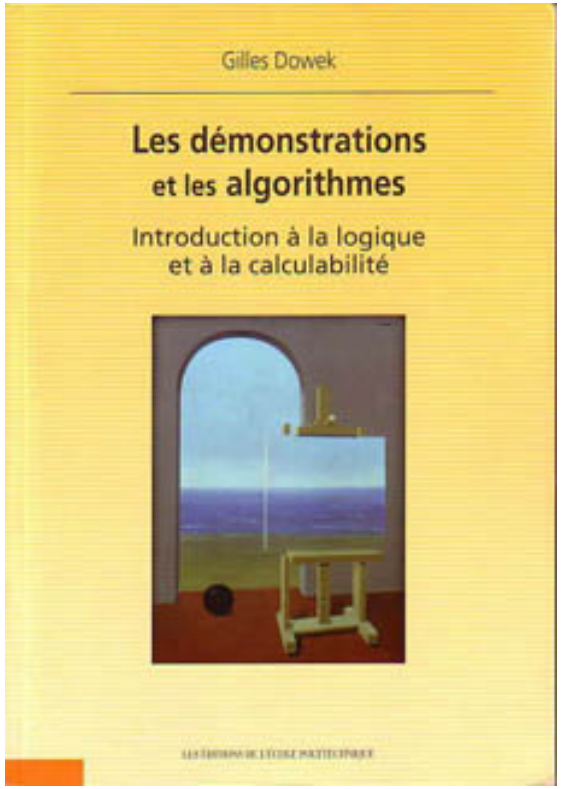
Cours : 9 séances, le Lundi 8h30 - 10h, à partir du 19/09

PC : 9 séances, le Lundi 10h15 - 12h15, à partir du 19/09

Une salle : PC17

Pale : TBA

Le poly de G. Dowek



Cours 0
Introduction

Raisonnements et algorithmes

Vous faites des raisonnements depuis vos premiers mots

. . .des calculs depuis la maternelle

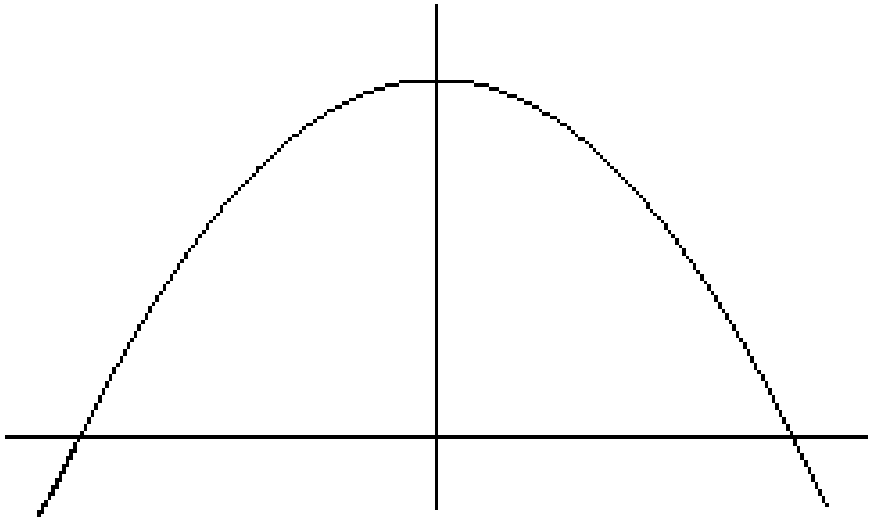
Sauriez-vous les définir ?

Situation similaire dans l'histoire des sciences :

on a fait des raisonnements et des calculs depuis la préhistoire

. . .proprement définis qu'au XXième siècle

Quelle est l'aire sous cette parabole ?



$$1 - x^2$$

Réponse : 4/3

Deux méthodes pour résoudre ce problème

Le découper en une infinité de petits triangles

Déterminer l'aire de chacun d'eux par un raisonnement géométrique

Ajouter toutes ces aires

Calculer $\int_{-1}^{1}(1-x^2)dx$

Construire un raisonnement *v.s.* appliquer un algorithme :

Deux types de méthodes qui coexistent depuis longtemps

Depuis l'invention des machines, il est plus sympathique de calculer que de raisonner : nouvel essor des méthodes algorithmiques

Dans quel but ?

Depuis l'antiquité : pour établir une vérité.

La question que l'on se pose, c'est :

Un énoncé mathématique est-il vrai ou faux ?

Questions :

– **Complétude:** tout énoncé vrai peut-il être démontré par raisonnement ?
– **Décidabilité:** existe-t-il un algorithme pour décider si un énoncé est vrai ou faux ?

vrai ?

Depuis l'antiquité : confrontation avec la réalité.

Depuis. . .
– diversification des disciplines mathématiques
– éloignement de plus en plus important d'une réalité tangible

XIXème siècle, crise logique.

De la vérité au droit

Un exemple classique.

Supposons que a et b sont non nuls.

$$a = b$$
$$a^2 = ab$$
$$a^2 - b^2 = ab - b^2$$
$$(a - b)(a + b) = b(a - b)$$
$$a + b = b$$
$$b + b = b$$
$$2b = b$$
$$2 = 1$$

”C’est faux ! Tu divises par 0 !”

”J’ai pas le droit ?”

Les mathématiques sont une question de droit et non pas de vérité.

De la vérité au droit

Un énoncé mathématique est-il vrai ou faux ?

$$\Downarrow$$

Un énoncé mathématique est-il démontrable ou pas ?

Question :

Peut-on remplacer systématiquement la construction d'une démonstration par l'application d'un algorithme ?

Moui

De fait :

- Toute recherche de démonstration mathématique peut s'implémenter comme calcul sous les bonnes hypothèses
- Tout calcul peut être vu comme la recherche d'une démonstration mathématique
  Mais deux points restent critiques :
  - Les calculs terminent-ils ?
  - Les calculs sont-ils déterministes, et si oui à quel prix (sur le temps d'exécution) ?

Objectifs du cours

Définir les notions de démonstration et d'algorithme

Montrer des résultats d'indépendance

Montrer des résultats d'indécidabilité (pb de l'arrêt)

Diversité des langages d'expr. des algorithmes, unité (petits pas)

Church : démontrabilité indécidable (mais semi-décidable)

Gödel

Algorithmes de recherche de démonstrations

Grossièrement, quelques noms et contributions

Boole (1815-1864) : algèbres de Boole, booléens,. . .

Frege (1848-1925) :

bases -imparfaites- de la théorie des ensembles, formalismes logiques, . . .

Hilbert (1862-1943) : 23 problèmes ouverts, meta-mathématiques,. . .

Zermelo (1871-1953) : théorie des ensembles moderne, avec Fraenkel

Russell (1872-1970) :

célèbre pour son paradoxe trouvé chez Frege, Principia Mathematica

Brouwer (1881-1966) : constructivisme

Goedel (1906-1978) : théorèmes d'incomplétude

Church (1903-1995) : fonctions et calcul, théorèmes d'indécidabilité. . .

Gentzen (1909-1945) : théorèmes de cohérence et formalismes logiques

Cours I
La logique des prédicats

I. Par où commencer ?

Où le serpent se mort la queue

Si mathématiques = question de droit, il faut une Loi, i.e. des règles (logiques).

Comme les mathématiciens pendant des siècles, vous avez cotoyés ces règles implicitement sans les avoir jamais vues formalisées.

But de ce cours (et des logiciens depuis Hilbert) :
les construire et comprendre leurs conséquences.

Exemple :

– Définir l'ensemble des propositions
– Définir le (sous)-ensemble des propositions démontrables

Les mathématiques permettent d'étudier formellement des objets.
Le raisonnement mathématique (et ses notions associées) sont un objet d'étude comme un autre.

Où le serpent se mort la queue

– Mais pour ce faire, un minimum de constructions mathématiques sont nécessaires.
  Exemples : on a déjà parlé d'ensembles ; de plus les formules, les démonstrations sont des arbres (voir plus loin) ; comment sont définis les arbres ?
– si l'objet d'étude est le raisonnement mathématique lui-même, comment raisonnons-nous sur cet objet ?

Impossible de faire des mathématiques ex-nihilo

Méta-mathématiques

On distingue le niveau objet et le niveau méta :

- Le niveau objet est la logique / la théorie / les règles que l'on définit / étudie
- Le niveau méta est la logique / la théorie / les règles que l'on utilise pour raisonner à propos du niveau objet.

Le niveau méta est souvent laissé implicite (tout comme lorsqu'au college vous étudiiez la géométrie).
Si un jour on veut définir proprement la logique du niveau méta, on se placera dans un niveau méta-méta, et ainsi de suite.

Pour démarrer, il faut donc entre nous, que l'on prenne pour acquis quelques notions de base. Exemple : les arbres.

Questions meta-mathématiques

– Existe-t-il un langage adéquat pour parler de toutes les mathématiques ?

OUI : langage des prédicats = langage du 1er ordre

– Qu'est-ce qu'une démonstration / preuve / deduction ?

Toujours pas d'accord. Raisonnement par l'absurde ? ou pas ?

Brouwer, Heyting, Kolmogorov,. . .le refusent

ensuite, questions de présentations (calcul des séquents,. . .)

– Existe-t-il une collection d'axiomes (si possible la plus petite) à partir desquelles se déduisent toutes les maths ?

Théorie des ensembles, Zermelo-Fraenkel : 9 "axiomes" (ou schémas)

Frege : pour chaque propriété P, autorise la construction $\{x \mid P(x)\}$

Paradoxe :

Soit $F = \{x \mid x \notin x\}$. Est-ce que $F \in F$ ou est-ce que $F \notin F$?: . . .

Questions meta-mathématiques, suite

– Etant donné une proposition P, existe-t-il toujours soit une preuve de P soit une preuve de $\neg P$? (in)complétude1

– Les mathématiques peuvent-elles démontrer qu'elles ne se contredisent pas ? (in)complétude2

– Existe-il un algorithme qui réponde OUI s'il existe une preuve de P, qui réponde NON sinon ? (in)décidabilité

Réponses aux trois réponses dans les années 30.

II. Des arbres et des inductions

Définition par récurrence (faible) sur les entiers

Exemple : La suite arithmétique

$$\begin{array}{lll} f(0) & := \ldots & u_0 := 0 \\ f(n+1) & := \ldots f(n) \ldots & u_{n+1} := 2 + u_n \end{array}$$

définit une fonction sur tous les entiers (aussi appelée suite).

Correspond à des programmes récursifs. Le même exemple en Java ou C :

```
int geo2(int n){
   if (n==0) return 0;
   return 2+geo2(n-1);
}
```

définit bien une fonction sur tous les entiers car les appels récursifs terminent.

Principe de récurrence (faible) sur les entiers

Soit $\mathcal{P}$ une propriété qu'un entier peut avoir ou ne pas avoir.

Exemple : $\mathcal{P}$ est "être pair"

"n satisfait la propriété $\mathcal{P}$" se note $\mathcal{P}(n)$

Principe de récurrence "faible":

Si $\mathcal{P}(0)$

et si pour tout entier n, $\mathcal{P}(n)$ implique $\mathcal{P}(n+1)$

alors pour tout entier n, on a $\mathcal{P}(n)$.

Exemple ::

Prouvez que pour tout entier n, on a $u_n = 2 * n$

Définition par récurrence (forte) sur les entiers

$f(n) := \ldots f(i) \ldots$ où $i < n$

Exemple : La suite

$$\begin{aligned} v_0 &:= 0 \\ v_n &:= v_{n/2} + 1 \quad n \geq 1 \end{aligned}$$

définit aussi une fonction sur tous les entiers (aussi appelée suite).

Correspond à des programmes récursifs. Le même exemple en Java ou C :

```
int suite(int n){
   if (n==0) return 0;
   return suite(n/2)+1;
}
```

définit bien une fonction sur tous les entiers car les appels récursifs terminent.

Principe de récurrence (fort) sur les entiers

Si pour tout entier n, $(\forall i < n, \mathcal{P}(i))$ implique $\mathcal{P}(n)$

alors pour tout entier n, on a $\mathcal{P}(n)$.

Exemple ::

Prouvez que pour tout entier n, on a $v_n \leq n$

Les entiers comme structure inductive (libre)

Induction = récurrence en anglais.

Les 5 axiomes de Peano

- 0 est un entier
- Si n est un entier,

  alors $S(n)$ est un entier.

"Construction inductive" des entiers

- 0 n'est le successeur d'aucun entier
- Si $S(n) = S(m)$ alors $n = m$

Structure **libre**

= injectivité des constructeurs

- Principe de récurrence (faible ou fort)

. . .définissent le comportement des entiers naturels.

Autres structures inductives (libres)

Ce qu'on peut faire avec les entiers, on peut le faire avec autre chose.

Définition des listes d'entiers :

– `nil`, la liste vide, est une liste.

– Si l est une liste et n un entier, alors $n :: l$ est une liste

(de tête n et de queue l)

Définition de la taille d'une liste, "par récurrence sur la liste" :

– la taille de `nil` est 0.

– la taille de $n :: l$ est la taille de l plus 1.

On pourrait poser des principes de récurrence sur les listes

mais en général, on se ramène à ceux sur les entiers via la notion de taille.

Autres structures inductives (libres)

Définition des arbres étiquetés :

– une feuille, étiquetée par un symbole s, est un arbre

– Si A_1,..., A_n sont des arbres, et f est un symbole,
  alors $f(A_1, \ldots, A_n)$ est un arbre.

Voir dessin au tableau.

(Exemple de) définition de la taille d'un arbre, "par récurrence sur l'arbre" :

– la taille d'une feuille est 1.

– la taille de $f(A_1, \ldots, A_n)$ est la somme des tailles de A_1,..., A_n, plus 1.

On pourrait poser des principes de récurrence sur les structures inductives

mais en général, on se ramène à ceux sur les entiers.

Exemple de formalisation en théorie des ensemble

Comment définir un ensemble ou une relation ?

On peut définir

$$\{x \in \mathbb{N} \mid \exists z \in \mathbb{N}\, x = 2 \times z\}$$

$$\{(x, y) \in \mathbb{N}^2 \mid \exists z \in \mathbb{N}\, x = y \times z\}$$

Un autre outil utile : La notion de définition inductive

Pour justifier les définitions inductives en théorie des ensembles :

les théorèmes du point fixe

Le premier théorème du point fixe

$E, \leq$ relation d'ordre

$u_0, u_1, ...$ suite croissante

l limite de $(u_i)_i$ si $l = sup\ \{u_0, u_1, ...\}$

$E, \leq$ faiblement complète si toute suite croissante a une limite

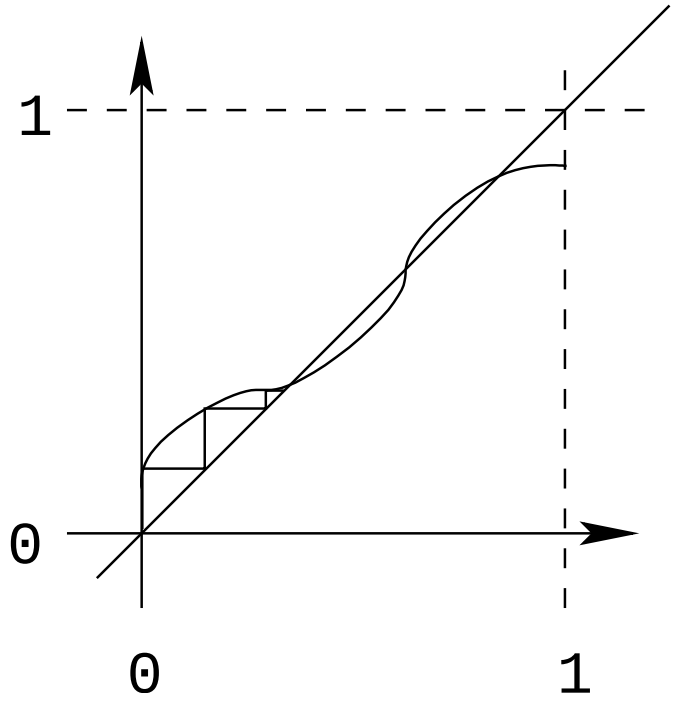
f croissante est continue si $lim_i\ (f\ u_i) = f\ (lim_i\ u_i)$

Th : $\leq$ faiblement complète et a un minimum et f continue alors f a un point fixe

Le plus petit point fixe est $lim_i\ (f^i\ m)$

Exemple

[0,1], $\leq$ est faiblement complète



$\mathbb{R}^+$, $\leq$ est-elle faiblement complète ?

Le deuxième théorème du point fixe

Pour les fonctions croissantes (mais pas forcément continues)

$E, \leq$ fortement complète si tout ensemble a une borne sup

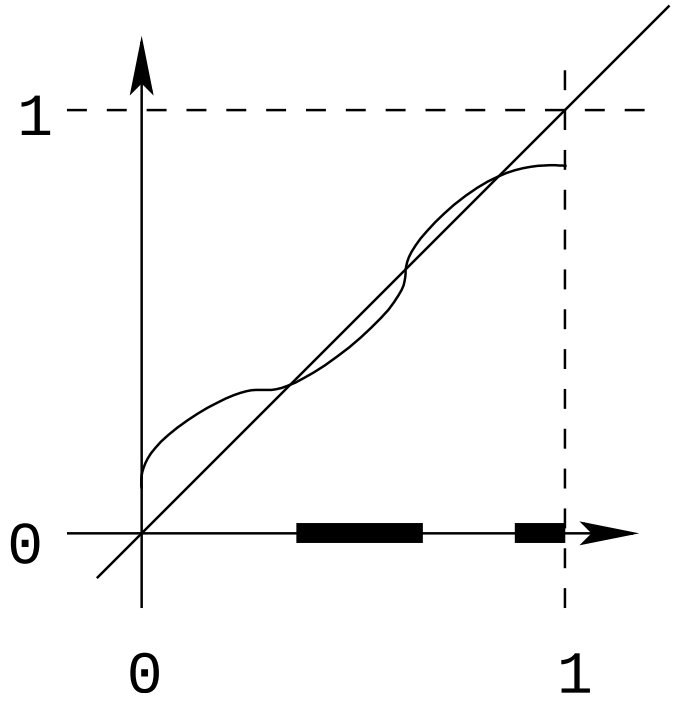
Donc tout ensemble a une borne inf

Th : $\leq$ fortement complète et f croissante alors f a un point fixe

Le plus petit point fixe est $inf\ \{c \mid fc \leq c\}$

Exemple

[0,1], $\leq$ est fortement complète



$\mathbb{R}^+$, $\leq$ est-elle fortement complète ?

Un autre exemple

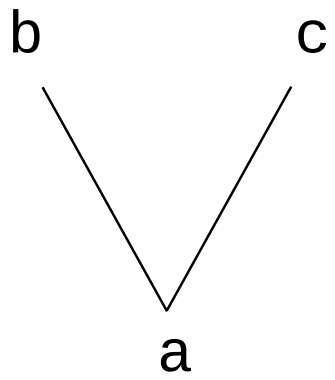
A ensemble quelconque

$\wp(A)$, $\subseteq$ est faiblement et fortement complète

f fonction croissante de $\wp(A)$ dans $\wp(A)$ a un point fixe

Le plus petit point fixe est $\bigcap_{C \mid f\ C \subseteq C} C$

(et aussi $\bigcup_i f^i(\varnothing)$ si f est continue)



Faiblement / fortement complète ?

Une première définition inductive

$P = 2\mathbb{N}$ est défini par

$0 \in P$ et si $n \in P$ alors $n + 2 \in P$

$$\frac{}{0}$$

$$\frac{n}{n+2}$$

$$\frac{}{0 \in P}$$

$$\frac{n \in P}{n+2 \in P}$$

P n'est pas le seul ensemble qui contient 0 et qui est clos par la fonction $n \mapsto n+2$
Mais c'est le plus petit de ces ensembles

F de $\wp(\mathbb{N})$ dans $\wp(\mathbb{N})$

$F(A) = \{0\} \cup \{x+2 \mid x \in A\}$

F croissante et continue

(A contient 0 et clos par $n \mapsto n+2$) : $F(A) \subseteq A$

P est défini comme le plus petit point fixe de F

Second th. du pf : c'est l'intersection de tous les ensembles qui contiennent 0 et qui sont clos par $n \mapsto n+2$

Premier th. du pf : c'est la réunion de $\varnothing$, $F(\varnothing)$, $F(F(\varnothing))$,...

Cas général

Un ensemble E

On définit un sous-ensemble B de E

par des fonctions de fermeture (règles) f_1, f_2, ...

$$F(A) = \bigcup_i \{f_i(a_1, ..., a_{n_i}) \mid a_1, ..., a_{n_i} \in A\}$$

F croissante et continue

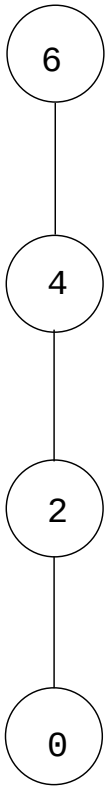
B est le plus petit point fixe de F

La notion de dérivation

$x \in B$ si $x \in F^k(\varnothing)$ pour un certain k

c.-à-d. s'il existe i, $y_1, ..., y_n \in F^{k-1}(\varnothing)$ tq $x = f_i(y_1, ..., y_n)$

Par récurrence sur k si $x \in B$ alors il existe un arbre dont les nœuds sont étiquetés par des éléments de E et les enfants d'un nœud x sont $y_1, ..., y_n$ tq il existe i tq $x = f_i(y_1, ..., y_n)$



$$\frac{}{0} \qquad \frac{}{0 \in P}$$

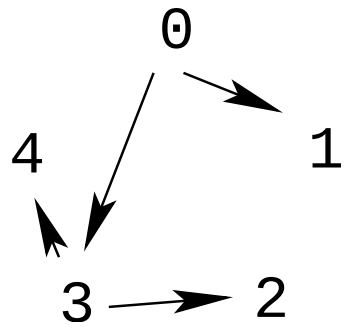
$$\frac{}{2} \qquad \frac{}{2 \in P}$$

$$\frac{}{4} \qquad \frac{}{4 \in P}$$

$$\frac{}{6} \qquad \frac{}{6 \in P}$$

Exemple

$E = \{0, 1, 2, 3, 4\}$



$$\frac{}{x \; C \; x}$$

$$\frac{}{x \; C \; y} \text{ si } x \; R \; y$$

$$\frac{x \; C \; y \quad y \; C \; z}{x \; C \; z}$$

$$\frac{0 \; C \; 3 \quad 3 \; C \; 2}{0 \; C \; 2}$$

La notion de fermeture réflexive-transitive

Exemple

$$\frac{A \wedge B}{A}$$

$$\frac{A \wedge B}{B}$$

$$\frac{A \Rightarrow B \quad A}{B}$$

$$\frac{}{(P \Rightarrow Q) \wedge P}$$

Exemple

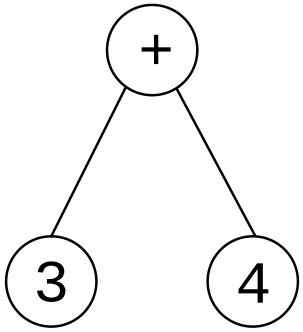
$$\dfrac{\dfrac{\dfrac{}{(P \Rightarrow Q) \wedge P}}{P \Rightarrow Q} \qquad \dfrac{\dfrac{}{(P \Rightarrow Q) \wedge P}}{P}}{Q}$$

III. La notion de langage en général

On oublie la contrainte de séquentialité du langage

On ne s'intéresse pas à savoir si on écrit $3 + 4$, $+(3, 4)$ ou $34+$

Les expressions sont des arbres

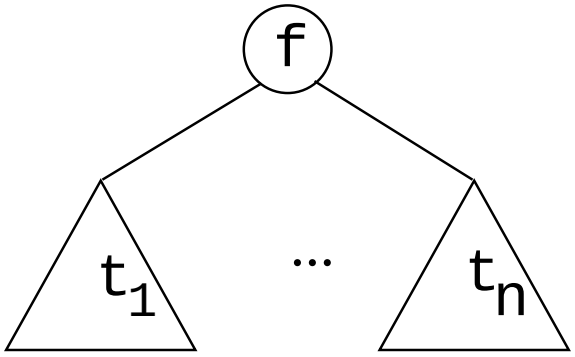


Les langages sans variables

Un langage (sans variables) est un ensemble de symboles, chacun muni d'un nombre entier appelé son arité ou nombre d'arguments

L'ensemble des expressions du langage est l'ensemble d'arbres défini inductivement par la règle

$$\frac{t_1 \quad t_n}{f(t_1, ..., t_n)} \text{ si } f \text{ est un symbole d'arité } n$$



Exemple

Une constante (c.-à-d. symbole d'arité nulle) 0

Un symbole unaire S

Deux symboles binaires $+$, $\times$

Deux symboles unaires $pair$, $impair$

Un symbole binaire $\Rightarrow$

$$impair(S(S(S(0)))) \Rightarrow pair(S(S(S(S(0)))))$$

Si un nombre est impair alors son successeur est pair

$$\forall x \; (impair(x) \Rightarrow pair(S(x)))$$

Des variables

Des symboles qui lient des variables

Les langages avec variables

L'arité d'un symbole est un n-uplet $(k_1, ..., k_n)$

le symbole a n arguments, il lie k_1 variables dans le premier, ..., k_n variables dans le $_n$ème

Exemple : $\forall$ a l'arité (1)

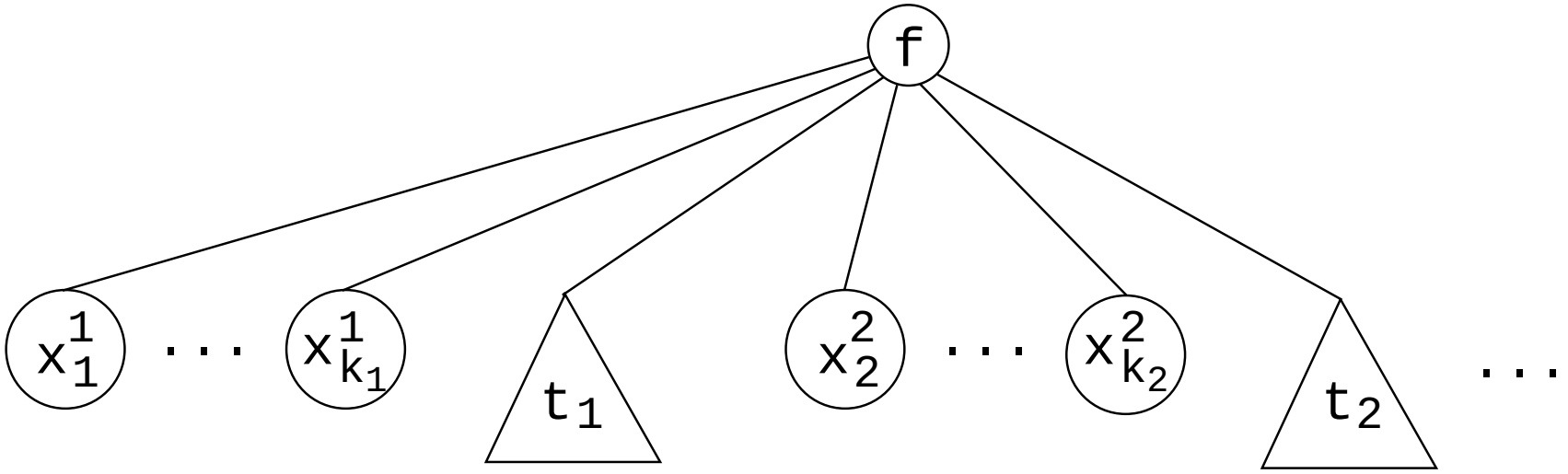
Un ensemble de symboles et un ensemble infini de variables

Les expressions sont définies inductivement par les règles :

– les variables sont des expressions,

– si f est un symbole d'arité $(1, 3)$, t et u sont des expressions, w, x, y, z sont des variables alors $f(w\ t, x\ y\ z\ u)$ est une expression (à généraliser)

$f(x_1^1 ... x_{k_1}^1 t_1, ..., x_1^n ... x_{k_n}^n t_n)$ est l'arbre



Les langages à plusieurs sortes d'objets

$0, S, +, \times, pair, impair, \Rightarrow, \forall$

On veut distinguer 0, $S(0)$, $S(x)$, ... termes

de $pair(0)$, $impair(0)$, $\forall x\ (pair(x))$, ... propositions

Mais aussi peut-être les termes de vecteurs, les termes de scalaires, ...

Les langages à plusieurs sortes d'objets

Un ensemble de sortes $\{Terme, Prop\}$ plus généralement $\mathcal{S}$

L'arité d'un symbole est un $n+1$-uplet de sortes $(s_1, ..., s_n, s')$

Si t_1 terme de sorte s_1, t_2 terme de sorte s_2, ..., t_n terme de sorte s_n et f d'arité $(s_1, ..., s_n, s')$ alors $f(t_1, ..., t_n)$ de sorte s'

Plusieurs sortes d'objets + lieurs

$$((s_1^1, ..., s_{k_1}^1, s'^1), ..., (s_1^n, ..., s_{k_n}^n, s'^n), s'')$$

Exemple $\forall$ d'arité $((Terme, Prop), Prop)$

IV. Le langage de la logique des prédicats et la notion de proposition démontrable

Le langage de la logique des prédicats

Ensemble $\mathcal{S}$ de sortes de termes et une sorte de plus $Prop$

Seulement deux symboles lieurs $\forall$ et $\exists$

Les symboles se divisent en

- les symboles de fonction f d'arité $(s_1, ..., s_n, s')$
- les symboles de prédicat P d'arité $(s_1, ..., s_n, Prop)$ (notée $(s_1, ..., s_n)$)
- les symboles communs à tous les langages $\top$, $\bot$, $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\forall$, $\exists$

$$\forall x\ (pair(x) \Rightarrow impair(S(x)))$$

Notion de proposition démontrable : première tentative

Une première (et presque bonne) idée :

Un sous-ensemble de l'ensemble des propositions

inductivement défini par des règles de déduction

$$\frac{A \wedge B}{A}$$

$$\frac{A \wedge B}{B}$$

$$\frac{A \Rightarrow B \quad A}{B}$$

Mais...

Pour démontrer $A \Rightarrow B$: supposons A et démontrons B

Non seulement la proposition à démontrer varie, mais aussi l'ensemble d'hypothèses

Un séquent $\Gamma \vdash A$ formé d'un ensemble d'hypothèses Γ et d'une conclusion A

Les règles

Un sous-ensemble de l'ensemble des séquents inductivement défini par des règles de déduction

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$$

Toutes les règles : page 27-28

La suite

En PC : des exemples de démonstrations

La prochaine fois :

– Les règles en détail (substitution)
– Comment démontrer qu'une proposition n'est pas démontrable ?

Questions?