Chapitre 1 / 2e Partie / TPGO

Concepts préliminaires :

A. Rappel sur les systèmes formels

B. Introduction à la théorie du point fixe

Objectif : Aborder les outils mathématiques pour faire du <u>raisonnement sur les programmes</u>

A. Systèmes Formels (SF)

Introduction

Définition

Quelques propriétés

SF : Introduction

Un Système Formel (SF) permet d'étudier de façon mathématique (formelle) les notions d'axiomatique et de mécanisme déductif.

En général, on cherche à modéliser (formaliser) une théorie afin qu'elle s'exprime entièrement dans le SF.

En informatique, les langages de programmation reposent sur des SF (sémantique, raisonnement, ...).

Ex : Lamda Calcul, Système de preuve de programme, ...

Certains types d'application (comme l'IA par exemple) utilisent aussi beaucoup les SF.

SF : Définition

On appelle Système Formel S, la donnée de 4 ensembles :

a) un **alphabet $\boldsymbol{\Sigma_S}$** fini ou infini dénombrable

b) un sous-ensemble <u>récursif</u> **$\mathbf{F_S}$** de l'ensemble de toutes les suites finies de $\Sigma_S{}^*$. F_S est appelé l'ensemble des **formules bien formées**

c) un sous-ensemble <u>récursif</u> **$\mathbf{A_S}$** de F_S.
A_S est appelé l'ensemble des **axiomes**.

d) un ensemble fini **$\mathbf{R_S}$** de prédicats <u>décidables</u>, définis sur F_S.
R_S est appelé l'ensemble des **règles d'inférence**.
Un prédicat r(f1, f2, … fn, g) de R_S est noté : f1, f2, … fn **|---**$_r$ g

a) et b) : <u>partie morphologique</u>   c) et d) : <u>partie axiomatique</u>

SF : Exemple

Soit S le système formel suivant :

$\Sigma_S = \{ 1 , + , = \}$

F_S = l'ensemble des mots de la forme :

111...1 + 111....1 = 111….11

(n fois) (m fois) (p fois) avec n,m et p $\in \mathbb{N} - \{0\}$

notés : $1^n + 1^m = 1^p$

$A_S = \{ 1 + 1 = 11 \}$ un seul axiome

$R_S = \{ r1 , r2 \}$ 2 règles d'inférence :

$1^n + 1^m = 1^p \;|\text{--}_{r1}\; 1^{n+1} + 1^m = 1^{p+1}$

$1^n + 1^m = 1^p \;|\text{--}_{r2}\; 1^n + 1^{m+1} = 1^{p+1}$

SF : Déductions

On appelle **déduction** à partir de $h_1, h_2, \dots h_n$, toute suite de formules :
$f_1, f_2, \dots f_p$, telle que pour tout i dans {1,2, … p}, on a :

a) fi est un axiome, ou alors,

b) fi est l'une des formules $h_1, h_2, \dots h_n$, ou alors,

c) fi est obtenue par application d'une règle rk, à partir des formules $fi_1, fi_2, \dots fi_m$, placées avant fi dans la déduction,
c-a-d $i_1 < i, i_2 < i , \dots i_m < i$

Dans une telle situation, on dit aussi que $f_1, f_2, \dots f_p$ est une déduction de fp <u>à partir des hypothèses</u> : $h_1, h_2, \dots h_n$ dans S

et on note alors : $h_1, h_2, \dots h_n \mid\!\!-\!-_S fp$

SF : Théorèmes

Un **théorème** d'un système formel S est une formule t bien formée, pour laquelle il existe une <u>déduction</u> à partir d'un <u>ensemble vide d'hypothèses</u> : $|\text{--}_S$ t

L'ensemble des théorèmes de S est noté T_S

Exemple :

Dans l'exemple vu précédemment, la suite de formules
1+1=1 , 11+1=11 , 11+11=111 représente une déduction de 11+11=111 à partir de l'hypothèse 1+1=1

la 2e formule étant obtenue par la règle r1 à partir de la 1ere formule
et la 3e formule est obtenue par la règle r2 à partir de la 2e formule.

Par contre, la formule 11+11=1111 est un théorème, car il existe une déduction sans utiliser d'hypothèses : 1+1=11 , 11+1=111 , 11+11=1111

la 1ere formule est un axiome,
la 2e est obtenue par r1 à partir de la 1ere et
la 3e est obtenue par r2 à partir de la 2e formule.
On a donc bien $|\text{--}_S$ 11+11=1111

Remarquons que nous ne pouvons pas démontrer une formule de type 11+1+1=1111 avec ce système formel (pourquoi?)

SF : Propriétés

Soit S un système formel.

S est **cohérent**, s'il existe des formules bien formées qui ne soient pas des théorèmes.

S est **consistant**, s'il n'existe aucune formule bien formée f, tel que f soit un théorème ainsi que sa négation non f.
Sinon on dit que S est inconsistant (ou contradictoire).

S est **décidable** si son ensemble de théorèmes T_S est récursif.

Lorsqu'on a en vu la modélisation d'une théorie particulière (ayant comme ensemble de théorèmes T), on dit que :
S est **correct** (ou sain) si T_S est inclus dans T
S est **complet** si T_S coïncide exactement avec T

SF : quelques résultats généraux

a) Si h $|--_S$ g et g $|--_S$ f alors h $|--_S$ f

b) L'ensemble des déductions est toujours récursif

c) L'ensemble des théorèmes TS est toujours au moins récursivement énumérable

d) Il existe des SF pour lesquels l'ensemble des théorèmes n'est pas récursif

En particulier, tous les systèmes formels basés sur la logique du premier ordre sont semi-décidables.

B. Théorie du Point Fixe (PF)

Introduction

Définition

Théorème du Point Fixe

PF : Introduction

La (les) solution(s) de toute équation de la forme $x = F(x)$
est (sont) appelée(s) : **Point(s) Fixe(s) de F**

La théorie du point fixe concerne l'étude des formes d'équations précédentes et généralise leurs application à des domaines très divers.

Nous nous intéressons dans ce cours à certaines applications en informatique, telles que :

- Expressions de langages de programmation
- Preuve de programmes
- Calcul de fonctions récursives
- Définition de types de données complexes

PF : Définitions

Soit (E,≤) un ensemble partiellement ordonné et soit X une partie de E

Un **Majorant** de X est un élément a de E, /que pour tout x de X, x ≤ a.

Un **Minorant** de X est un élément b de E, /que pour tout x de X, b ≤ x.

Exemple

Soient (N, 'divise') et X = {6,9,15,21} une partie de ℕ.
L'entier 6*9*15*21 est un majorant de X.
Les entiers 1 et 3 sont des minorants de X

La **borne supérieure** de X (Sup X) est le plus petit (au sens de la relation d'ordre) des majorants de X.

La **borne inférieure** de X (Inf X) est le plus grand (au sens de la relation d'ordre) des minorants de X.

Une **chaîne** est une suite croissante (au sens de la relation d'ordre) d'éléments de E

$(x_n)_{n\geq 0} = x_0 \leq x_1 \leq x_2 \leq \dots \leq x_n \leq \dots$

La chaîne est dite **stationnaire** s'il existe un seuil m /que pour tout n ≥ m, $x_n = x_m$.

PF : Définitions (suite)

Un ensemble ordonné est dit **<u>inductif</u>** (au sens des chaînes),

- s'il admet un plus petit élément ($\perp$) et
- si toute chaîne admet une borne supérieure.

Soient X et Y deux ensembles ordonnés inductifs
Soit f une application de X vers Y

On dit que f est **<u>continue</u>** (au sens des chaînes)
si pour toutes chaîne $(x_n)_{n\geq 0}$, la suite $(f(x_n))_{n\geq 0}$ admet une borne supérieure vérifiant :

$$\mathrm{Sup}\,(\, f(x_n)\,)_{n\geq 0} = f(\,\mathrm{Sup}(x_n)_{n\geq 0}\,)$$

PF : Théorème

Soit (X, $\leq$) un ensemble ordonné inductif et soit f une application continue de X vers X

Alors toute équation de la forme **x = f(x)** admet une plus petite solution x_0 (appelée : plus petit point fixe de f) et vérifiant :

$$x_0 = \mathrm{Sup}\ (f^n(\perp))_{n\geq 0}$$

c-a-d

$$x_0 = \mathrm{Sup}\ \{ \perp, f(\perp), f(f(\perp)), f(f(f(\perp))), \ldots \}$$

Les autres solutions de l'équation sont appelées des points fixes.

PF : Démonstration 1/2

a) Montrons que x_0 = Sup ($f^n(\perp)$)$_{n\geq 0}$ est une solution de x = f(x)

c-a-d montrons que : $x_0 = f(x_0)$

Puisque f est continue au sens des chaînes (donc monotone), la suite $(f^n(\perp))_{n\geq 0}$ est forcément croissante

on peut facilement le démontrer par récurrence sur la taille des chaînes

$(\perp \leq f(\perp)$; $\perp \leq f(\perp) \leq f(f(\perp))$; $\perp \leq f(\perp) \leq f(f(\perp)) \leq f(f(f(\perp)))...)$

Puisque l'ensemble X est inductif, la chaîne $(f^n(\perp))_{n\geq 0}$ est stationnaire.

Soit x_0 sa borne supérieure

Donc $x_0 = f^m(\perp) = f^{m+1}(\perp) = f^{m+2}(\perp)$ ... pour un certain seuil m > 0

Or $f^{m+1}(\perp)$ n'est rien d'autre que f($f^m(\perp)$) c-a-d $f(x_0)$

On a donc bien $\mathbf{x_0 = f(x_0)}$

PF : Démonstration 2/2

b) Montrons que x_0 = Sup ($f^n(\perp)$)$_{n\geq 0}$ est la plus petite des solutions

c-a-d montrons que : s'il existe y /que $y = f(y)$ alors $x_0 \leq y$

// par récurrence sur n :

- remarquons que $f^0(\perp) = \perp \leq y$ pour tout y de X donc en particulier pour tout point fixe y de f
- supposons que $f^n(\perp) \leq y$ est vraie jusqu'à un certain n et montrons que $f^{n+1}(\perp) \leq y$ et aussi vraie et ce, pour tout point fixe y de f

puisque f est continue au sens des chaînes (donc monotone), il s'en suit

$f^n(\perp) \leq y \Rightarrow f(f^n(\perp)) \leq f(y)$

or $f(f^n(\perp))$ n'est rien d'autre que $f^{n+1}(\perp)$ de plus $f(y) = y$ (point fixe)

donc $f^n(\perp) \leq y \Rightarrow f^{n+1}(\perp) \leq y$.

Conclusion : $\forall$ n, $f^n(\perp) \leq y$

En particulier pour x_0 = **Sup ($f^n(\perp)$)$_{n\geq 0}$ $\leq$ y** pour tout point fixe y de f

PF : Exemple

Soit $\mathscr{F}$(E,F) l'espace des fonctions partielles de E dans F

Soit $\preccurlyeq$ la relation d'ordre partielle 'moins définie que' :

    $f \preccurlyeq g$: $\forall$ x /que f(x) est définie, g(x) est aussi définie et g(x) = f(x)

Par exemple : $f_0 \preccurlyeq f_1 \preccurlyeq f_2 \preccurlyeq \ldots \preccurlyeq f_\infty = fact$

f0(x) = SI (x=0) Alors retourner 1 FSI
f1(x) = SI (x=0 ou x=1) Alors retourner 1 FSI
f2(x) = Si (x=0 ou x=1) Alors retourner 1 FSI
    SI (x=2) Alors retourner 2 FSI
f3(x) = Si (x=1 ou x=0) Alors retourner 1 FSI
    SI (x=2) Alors retourner 2 FSI
    SI (x=3) Alors retourner 6 FSI
...
fact(x) = x!

($\mathscr{F}$(E,F), $\preccurlyeq$) est inductif

Son plus petit élément est Ω(x), la fonction nulle part définie

Toute chaîne possède une borne supérieure qui n'est rien d'autre qu'une des fonctions de $\mathscr{F}$(E,F). Nous verrons plus de détails dans le chapitre sur la programmation fonctionnelle.