

# Induction

MLO

*C. Dubois*

# L'induction

Un outil formel élégant très utile en informatique

- ▶ Pour définir des ensembles, des fonctions
- ▶ Pour démontrer des propriétés avec des techniques souvent plus élégante que la récursion sur les entiers

Déjà utilisée en AP1

- ▶ pour démontrer des propriétés sur des fonctions manipulant des listes
- ▶ l'induction se cache derrière les types sommes récursifs (type des listes, des arbres, des expressions arithmétiques etc.)

# Définition inductive

## Ensemble défini inductivement

- ▶ La définition inductive  $X$  d'un ensemble  $E$  consiste en la donnée explicite de certains éléments de  $X$  (**les éléments de base**)
- ▶ la donnée de règles de construction d'éléments de  $X$  à partir d'éléments déjà connus de  $X$  (**étapes inductives**)
- ▶ **+ règle implicite** : il n'y a pas d'autre moyen de définir des éléments de  $X$

Formellement :

### Définition

soit  $E$  un ensemble. Une définition inductive d'une partie  $X$  de  $E$  consiste en la donnée :

- ▶ d'un sous-ensemble  $B$  de  $E$
- ▶ d'un ensemble  $K$  d'opérations  $\phi : E^{a(\phi)} \rightarrow E$  où  $a(\phi)$  est l'arité de l'opération  $\phi$ .

$X$  est défini comme étant **le plus petit ensemble vérifiant les assertions (B) et (I)** suivantes :

$$(B) \quad B \subset X$$

$$(I) \quad \forall \phi \in K, \forall x_1, x_2 \dots x_{a(\phi)} \in X, \phi(x_1, x_2 \dots x_{a(\phi)}) \in X$$

L'ensemble  $X$  défini inductivement par  $B$  et  $K$  sera noté  $\langle B, K \rangle$  (schéma d'induction).

# Présentation à base de règles

On peut aussi présenter les règles de construction du schéma d'induction à l'aide de **règles d'inférence** :

$$\frac{\textit{premisses}}{\textit{conclusion}}$$

Les prémisses peuvent être omises dans certains cas.

## Exemples de définitions inductives

- Définition inductive de  $N$  :

$$(B) \ 0 \in N$$

$$(I) \text{ si } n \in N \text{ alors } n + 1 \in N$$

$N$  est réduit à un singleton, son unique opération est l'opération *successeur*.

On peut encore écrire :

$$(B) \frac{}{0 \in N},$$

$$(I) \frac{n \in N}{n + 1 \in N}$$

- Définition inductive de  $A^*$ , ensemble de tous les mots formés sur l'alphabet  $A$

$$(B1) \ \epsilon \in A^* \text{ (le mot vide)}$$

$$(B2) \ A \subset A^*$$

$$(I) \text{ si } m \in A^* \text{ et } n \in A^* \text{ alors } mn \in A^* \text{ (opération de concaténation)}$$

- Définition inductive de  $L_A$ , ensemble des listes formées d'éléments de  $A$

(B)  $[] \in L_A$

(I) si  $l \in L_A$  alors pour tout  $a \in A, a :: l \in L_A$

- Définition inductive des expressions arithmétiques formées à partir d'identificateurs pris dans  $A$  et des opérateurs  $+$  et  $*$  :  
c'est la partie de  $(A \cup \{+, *\})^*$  définie inductivement par :

(B)  $A \subset E$

(I) si  $e$  et  $f$  sont dans  $E$  alors  $e + f$  et  $e * f$  sont aussi dans  $E$

Généralisation :

Soit  $V$  un ensemble de variables (des noms), soit  $F$  un ensemble de symboles de fonctions. On associe à chaque symbole  $f$  de  $F$  son arité (nombre d'arguments, éventuellement nul)  $a(f)$

L'ensemble des termes sur  $V$  et  $F$  est défini inductivement par :

- ▶ si  $v \in V$  alors  $v$  est un terme
- ▶ si  $f \in F$ , si  $t_1, t_2 \dots t_{a(f)}$  sont des termes alors  $f(t_1, t_2, \dots, t_{a(f)})$  est un terme.

- Définition inductive du langage  $D \subset \{ (, ) \}^*$  de Dyck des parenthésages bien formés.

(B)  $\epsilon \in D$

(I1) si  $x \in D$  alors  $(x) \in D$

(I2) si  $x \in D$  et  $y \in D$  alors  $xy \in D$

$((()())())$  est un élément de  $D$ .

(1)  $\epsilon \in D$  (par B)

(2)  $() \in D$  (par I1 sur 1)

(3)  $()() \in D$  (par I2 sur 2 et 2)

(4)  $((()())) \in D$  (par I1 sur 3)

(5)  $((())) \in D$  (par I1 sur 2)

$((()())()) \in D$  (par I2 sur 4 et 5)

► Définition inductive de  $S_{a,b} \subset \{a, b\}^*$

(B)  $a \in S_{a,b}, b \in S_{a,b}$

(I1) *si  $x$  est dans  $S_{a,b}$ , alors  $axb$  est dans  $S_{a,b}$*

(I2) *si  $x$  est dans  $S_{a,b}$ , alors  $bxa$  est dans  $S_{a,b}$*

(I3) *si  $x$  et  $y$  sont dans  $S_{a,b}$  alors  $xy$  est aussi dans  $S_{a,b}$*

Exemples ? Quel est cet ensemble ?

# 1ère caractérisation

## Théorème

Soit  $X \subset E$ ,  $X = \langle B, K \rangle$

L'ensemble ainsi défini est

$$X = \bigcap_{Y \in F} Y$$

où  $F = \{Y \subset E / B \subset Y \text{ et } Y \text{ vérifie (I)}\}$ .

(ceci justifie l'expression *le plus petit ensemble* de la définition)

## 2ème caractérisation : approche itérative

### Définition explicite

#### Théorème

Si  $X$  est défini par les conditions (B) et (I), tout élément de  $X$  peut s'obtenir à partir de la base en appliquant un nombre fini d'étapes inductives.

$$X = \bigcup_{i \in \mathbb{N}} X_i$$

où  $X_0 = B$  et  $X_{i+1} = X_i \cup K(X_i)$

On rappelle que  $K(X_i)$  désigne les images des éléments de  $X_i$  par les opérations de  $K$ , i.e. les éléments de  $X$  générés à partir des éléments de  $X_i$  en appliquant une fois les différentes étapes inductives.

⇒ On peut représenter graphiquement un élément de  $X$  par un arbre :  
feuilles = éléments appartenant à  $X_0$ , nœuds = les opérations de  $K$  appliquées à chaque étape.

Démonstration : par double inclusion.

- ▶  $\bigcup_{i \in N} X_i \subset X$  : il suffit de montrer, par récurrence sur  $i$ , que pour tout  $i$ ,  $X_i \subset X$ .
- ▶  $X \subset \bigcup_{i \in N} X_i$ , il suffit de montrer que l'ensemble  $\bigcup_{i \in N} X_i$  vérifie les assertions (B) et (I) de la définition de  $X$ .  
On pourra alors affirmer que cet ensemble contient  $X$  car  $X$  est le plus petit ensemble vérifiant les conditions (B) et (I).

# Types récurifs de Ocaml

Ils cachent une définition inductive

```
type list = Nil | Cons of int*list;;
```

```
type arbreb = Empty | Noeud of arbreb * int * arbreb;;
```

```
type expr = Var of string |  
            Plus of expr*expr | Mult of expr*expr;;
```

# Principe d'induction - Démonstration par induction

## Définition du principe d'induction (structurelle)

Soit  $X$  un ensemble défini inductivement par  $B$  et  $K$  et soit  $P(x)$  un prédicat exprimant une propriété de  $x$ , élément de  $X$ .

Si les conditions suivantes sont vérifiées :

B''  $P(b)$  est vraie pour chaque  $b$  de  $B$

I'' si  $P(x_1), P(x_2) \dots P(x_{a(\phi)})$  alors  $P(\phi(x_1, x_2 \dots x_{a(\phi)}))$  pour chaque  $\phi$  de  $K$

alors  $P(x)$  est vraie pour tout  $x$  de  $X$ .

Faire une démonstration par induction, c'est vérifier B'' et I''.

Démonstration du principe d'induction :

Posons  $A = \{x \in X / P(x) \text{ vraie}\}$ . Montrons  $A = X$ .

De la même façon que précédemment, on montre que :

- ▶  $A$  vérifie (B) et (I), alors  $X$  est inclus dans  $A$ .
- ▶ Et bien sûr,  $A$  est inclus dans  $X$ , d'où le résultat.

- ▶ Le premier principe de récurrence correspond à la définition ci-dessus si on prend la définition inductive précédente de  $\mathbb{N}$ .
- ▶ Pour montrer une propriété  $P(l)$  sur les listes de  $L_A$ , il suffira donc de montrer que :
  - ▶  $P([])$  vraie
  - ▶ pour tout  $l$ , si  $P(l)$  vraie alors pour tout  $a \in A$ ,  $P(a :: l)$  vraie

- ▶ Pour montrer une propriété  $P(e)$  sur les expressions arithmétiques définies comme précédemment, il suffira donc de montrer que :
  - ▶  $P(lf)$  vraie, pour tout identificateur  $lf$  de  $A$
  - ▶ pour tout  $e_1$  et  $e_2$  telles que  $P(e_1)$  vraie et  $P(e_2)$  alors  $P(e_1 + e_2)$  est vraie
  - ▶ pour tout  $e_1$  et  $e_2$  telles que  $P(e_1)$  vraie et  $P(e_2)$  alors  $P(e_1 * e_2)$  est vraie

# Définitions non ambiguës

## Définition

On dit qu'un ensemble inductif  $X$  est non ambigu si pour chaque élément de  $X$ , il existe une unique façon de construire cet élément en utilisant les règles  $B$  et  $I$  de  $X$ .

Par exemple, la définition de  $S_{a,b}$  donnée plus haut ne satisfait pas cette condition : on peut construire le mot  $abab$  de  $S_{a,b}$  en utilisant (I3) sur  $ab$  et  $ab$  et en utilisant (I1) sur  $ba$ .

## Fonctions définies inductivement

On définit la fonction  $\psi$  sur un ensemble  $E$  défini inductivement de façon non ambiguë :

- ▶ sur la base  $(\psi(x), x \in B)$
- ▶ puis inductivement sur les nouveaux éléments construits à partir d'éléments déjà connus (i.e. l'expression de  $\psi(\phi(x_1, x_2, \dots, x_{a(\phi)}))$  à partir de  $\psi(x_1), \psi(x_2), \dots, \psi(x_{a(\phi)})$  pour chaque  $\phi$  de  $K$ ).

Exemple de la fonction longueur  $lg$  sur  $A^*$  :

- ▶  $lg(\epsilon) = 0$
- ▶  $lg(a) = 1$  pour  $a \in A$
- ▶  $lg(mn) = lg(m) + lg(n)$  pour  $m, n \in A^*$

Exemples : factorielle sur  $\mathbb{N}$ , miroir sur  $A^*$ , longueur sur  $L_A$ .

Et toutes les fonctions récursives définies par filtrage en OCaml

## Définitions inductives de relations

On peut définir la relation  $<$  sur les entiers naturels de manière inductive à l'aide des 2 règles suivantes :

- ▶ (B) pour tout  $n$  de  $\mathbb{N}$ ,  $0 < n + 1$
- ▶ (I) si  $n < m$  alors  $n + 1 < m + 1$

La relation  $<$  est alors la plus petite relation vérifiant les 2 propriétés (B) et (I).

Explication : si on assimile la relation  $<$  à un ensemble de couples de  $\mathbb{N} \times \mathbb{N}$  ( $<$ ), on peut définir l'ensemble ( $<$ ) inductivement par :

(B) pour tout  $n$  de  $\mathbb{N}$ ,  $(0, n + 1) \in (<)$

(I) si  $(n, m) \in (<)$  alors  $(n + 1, m + 1) \in (<)$

Et c'est comme avant ....

On peut donc associer à une telle définition un principe d'induction.

*Ainsi pour montrer que tout  $n$ -uplet d'une relation vérifie une propriété  $P$ , nous devons montrer que  $P$  est clos par les règles de production de la relation.*

Par exemple, soit  $P$  un prédicat binaire sur  $\mathbb{N}$ . Pour montrer que  $P(n, m)$  est vraie pour tout  $n, m$  tel que  $n < m$ , on doit montrer :

- ▶ pour tout  $n \in \mathbb{N}$ ,  $P(0, n + 1)$
- ▶ si pour tout  $x, y \in \mathbb{N}^2$  tels que  $x < y$  et  $P(x, y)$  alors  $P(x + 1, y + 1)$

On le retrouve en partant de la vision *ensemble de couples* pour la relation  $<$ .