

Ensembles inductifs, Preuves par induction

Christophe Moulleron



Induction =

① outil pour **définir** de manière formelle

- ▶ les ensembles
- ▶ les fonctions
- ▶ les propriétés

$\mathbb{N}$, arbres binaires
+, hauteur, nb. de feuilles
être pair / impair

② outil pour **démontrer** formellement des propriétés

- ▶ preuve par induction (structurale)

“Un arbre binaire de hauteur n a au plus 2^n feuilles”

③ généralise le principe de récurrence vu pour les entiers

- 1 Définition par induction
 - Définition d'un ensemble
 - Règles d'inférences
 - Définition d'une fonction
- 2 Principe d'induction structurelle

- 1 Définition par induction
 - Définition d'un ensemble
 - Règles d'inférences
 - Définition d'une fonction
- 2 Principe d'induction structurelle

- 1 Définition par induction
 - Définition d'un ensemble
 - Règles d'inférences
 - Définition d'une fonction
- 2 Principe d'induction structurelle

Definition (Ensembles définis inductivement)

Soit $\mathcal{B}$ un ensemble de base et $\mathcal{K}$ un ensemble d'opérations.

L'**ensemble inductif** $\langle \mathcal{B}, \mathcal{K} \rangle$ est le plus petit ensemble E tel que :

- $\mathcal{B} \subset E$
- Si $f \in \mathcal{K}$ est d'arité n et si $x_1, \dots, x_n \in E$, alors $f(x_1, \dots, x_n) \in E$

Ensembles définis inductivement

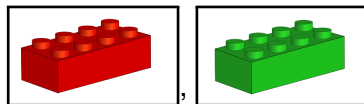
Definition (Ensembles définis inductivement)

Soit $\mathcal{B}$ un ensemble de base et $\mathcal{K}$ un ensemble d'opérations.

L'**ensemble inductif** $\langle \mathcal{B}, \mathcal{K} \rangle$ est le plus petit ensemble E tel que :

- $\mathcal{B} \subset E$
- Si $f \in \mathcal{K}$ est d'arité n et si $x_1, \dots, x_n \in E$, alors $f(x_1, \dots, x_n) \in E$

$\mathcal{B}$ = briques de base



Ensembles définis inductivement

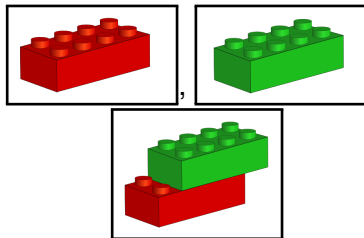
Definition (Ensembles définis inductivement)

Soit $\mathcal{B}$ un ensemble de base et $\mathcal{K}$ un ensemble d'opérations.

L'**ensemble inductif** $\langle \mathcal{B}, \mathcal{K} \rangle$ est le plus petit ensemble E tel que :

- $\mathcal{B} \subset E$
- Si $f \in \mathcal{K}$ est d'arité n et si $x_1, \dots, x_n \in E$, alors $f(x_1, \dots, x_n) \in E$

$\mathcal{B}$ = briques de base



$\mathcal{K}$ = règles de construction

Ensembles définis inductivement – Exemple (1)

Comment définir l'ensemble $\mathbb{N}$ des entiers naturels ?

$\mathcal{B} =$

$\mathcal{K} =$

$\mathbb{N} = \langle \mathcal{B}, \mathcal{K} \rangle$

Ensembles définis inductivement – Exemple (1)

Comment définir l'ensemble $\mathbb{N}$ des entiers naturels ?

- $0 \in \mathbb{N}$ plus petit entier
- Si $n \in \mathbb{N}$, alors $n + 1 \in \mathbb{N}$ construction d'un entier plus grand

$$\mathcal{B} = \{0\} \quad \mathcal{K} = \{\text{succ}\} \text{ où } \text{succ} : \mathbb{N} \rightarrow \mathbb{N} \quad \mathbb{N} = \langle \mathcal{B}, \mathcal{K} \rangle$$
$$n \mapsto n + 1$$

Ensembles définis inductivement – Exemple (1)

Comment définir l'ensemble **Nat** des entiers naturels ?

On peut aussi utiliser **Z** (zéro) et **S** (successeur) :

$$\mathcal{B}' = \{Z\} \quad \mathcal{K}' = \{S\} \quad \text{Nat} = \langle \mathcal{B}', \mathcal{K}' \rangle$$

syntaxe volontairement $\neq$ pour éviter de confondre :

- l'ensemble inductif Nat (définition formelle)
- le concept mathématique $\mathbb{N}$ (utilisé dans les preuves)

Ensembles définis inductivement – Exemple (2)

Comment définir l'ensemble L des listes de booléens ?

Ensembles définis inductivement – Exemple (2)

Comment définir l'ensemble L des listes de booléens ?

- $[] \in L$
- Si $\ell \in L$, alors $\text{true} :: \ell \in L$
- Si $\ell \in L$, alors $\text{false} :: \ell \in L$

liste vide

ajout à gauche

$$\begin{aligned}\mathcal{B} &= \{[]\} \\ \mathcal{K} &= \{ \ell \mapsto \text{true} :: \ell, \\ &\quad \ell \mapsto \text{false} :: \ell \}\end{aligned}$$

$\rightsquigarrow$ 1 elt de base + 2 constructeurs

Ensembles définis inductivement – Exemple (3)

Comment définir l'ensemble T des arbres binaires (sans valeurs) ?

Ensembles définis inductivement – Exemple (3)

Comment définir l'ensemble T des **arbres binaires** (sans valeurs) ?

• $\bullet \in T$

feuille

• Si $\triangle_{t_1} \in T$ et $\triangle_{t_2} \in T$, alors $\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \triangle_{t_1} \quad \triangle_{t_2} \end{array} \in T$

noeud interne

$$\mathcal{K} = \left\{ (t_1, t_2) \mapsto \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ t_1 \quad t_2 \end{array} \right\}$$

$\mathcal{B} = \{\bullet\}$

$\rightsquigarrow$ 1 elt de base + 1 constructeur d'arité 2

Modélisation d'un concept par un ensemble inductif **pas unique**

~> $\mathbb{N}$ et Nat

~> pour les listes, ajout à droite (au lieu de gauche)

Modélisation d'un concept par un ensemble inductif **pas unique**

↪ $\mathbb{N}$ et Nat

↪ pour les listes, ajout à droite (au lieu de gauche)

$E = \langle \mathcal{B}, \mathcal{K} \rangle =$ **plus petit ensemble** contenant $\mathcal{B}$ et stable par $\mathcal{K}$

↪ $\mathbb{C}$ contient 0 et est stable par $f : x \mapsto x + 1$

mais $\mathbb{C} \neq \langle \{0\}, \{\text{succ}\} \rangle$

- 1 Définition par induction
 - Définition d'un ensemble
 - Règles d'inférences
 - Définition d'une fonction
- 2 Principe d'induction structurelle

Règles d'inférences

règles d'inférences = représentation alternative pour $E = \langle \mathcal{B}, \mathcal{K} \rangle$

forme de règles d'inférences = $\frac{\text{prémisses}}{\text{conclusion}}$

Règles d'inférences

règles d'inférences = représentation alternative pour $E = \langle \mathcal{B}, \mathcal{K} \rangle$

forme de règles d'inférences =
$$\frac{\text{prémisses}}{\text{conclusion}}$$

une règle pour

- chaque x de $\mathcal{B}$: $\overline{x}$

- chaque opération f de $\mathcal{K}$ d'arité n :
$$\frac{x_1 \quad x_2 \quad \dots \quad x_n}{f(x_1, \dots, x_n)}$$

$f(x_1, \dots, x_n) \in E$ à condition que $x_1, \dots, x_n \in E$

Règles d'inférences

règles d'inférences = représentation alternative pour $E = \langle \mathcal{B}, \mathcal{K} \rangle$

forme de règles d'inférences =
$$\frac{\text{prémisses}}{\text{conclusion}}$$

une règle pour

- chaque x de $\mathcal{B}$: $\overline{x}$

- chaque opération f de $\mathcal{K}$ d'arité n :
$$\frac{x_1 \quad x_2 \quad \dots \quad x_n}{f(x_1, \dots, x_n)}$$

$x \in E$
 $f(x_1, \dots, x_n) \in E$ à condition que $x_1, \dots, x_n \in E$

Exemple pour Nat :
$$\overline{z} \quad \frac{n}{S(n)}$$

Arbre d'inférence

Idée :

$\simeq$ principe des dominos

- juxtaposer plusieurs règles d'inférence
- bas de l'arbre = conclusion que l'on souhaite inférer
- haut de l'arbre = prémisses restantes à inférer idéalement rien

$\rightsquigarrow$ utile pour représenter une **preuve** d'appartenance à un ens. inductif

Arbre d'inférence

Idée :

$\simeq$ principe des dominos

- juxtaposer plusieurs règles d'inférence
- bas de l'arbre = conclusion que l'on souhaite inférer
- haut de l'arbre = prémisses restantes à inférer idéalement rien

$\rightsquigarrow$ utile pour représenter une **preuve** d'appartenance à un ens. inductif

Exemple : $S(S(Z)) \in \text{Nat}$

$$\frac{\frac{\overline{Z}}{S(Z)}}{S(S(Z))}$$

haut = vide = plus aucune prémisses

bas = $S(S(Z))$

$\Rightarrow S(S(Z)) \in \text{Nat}$

- 1 Définition par induction
 - Définition d'un ensemble
 - Règles d'inférences
 - Définition d'une fonction
- 2 Principe d'induction structurelle

Définition par induction d'une fonction

Si $E = \langle \mathcal{B}, \mathcal{K} \rangle$, on peut définir une fonction φ sur E **inductivement** comme suit :

- Pour chaque élément $x \in \mathcal{B}$, on donne une valeur $\varphi(x)$
- Pour chaque fonction $f \in \mathcal{K}$ et pour tout $x_1, \dots, x_n$ dans E , on note $v_1 = \varphi(x_1), \dots, v_n = \varphi(x_n)$ et on définit $\varphi(f(x_1, \dots, x_n))$ en fonction de $v_1, \dots, v_n$.

$$\varphi : E \rightarrow F$$

Définitions inductives de fonctions – Exemple (1)

Sur les entiers Nat , on définit *double* inductivement par :

- $\text{double}(Z) = Z$ $2 \times 0 = 0$
- si $n \in \text{Nat}$, alors
 $\text{double}(S(n)) = S(S(\text{double}(n)))$ $2 \times (n + 1) = 2n + 2$

Définitions inductives de fonctions – Exemple (2)

Sur les entiers Nat , on définit $\text{add}(n, m)$ inductivement sur n par :

- $\text{add}(Z, m) = m$ $0 + m = m$
- si $n \in \text{Nat}$, alors
 $\text{add}(S(n), m) = S(\text{add}(n, m))$ $(n + 1) + m = (n + m) + 1$

autre définition possible par induction sur m

Définitions inductives de fonctions – Exemple (3)

Sur les entiers Nat , on définit $\llbracket \cdot \rrbracket : \text{Nat} \rightarrow \mathbb{N}$ inductivement par :

- $\llbracket Z \rrbracket = 0$
- si $n \in \text{Nat}$, alors $\llbracket S(n) \rrbracket = \llbracket n \rrbracket + 1$

$\llbracket \cdot \rrbracket = \text{interprétation}$

Sur $\mathbb{N}$, on définit $\text{encoding} : \mathbb{N} \rightarrow \text{Nat}$ inductivement par :

- $\text{encoding}(0) = Z$
- si $n \in \mathbb{N}$, alors $\text{encoding}(n + 1) = S(\text{encoding}(n))$

Définitions inductives de fonctions – Exemple (3)

Sur les entiers Nat , on définit $\llbracket \cdot \rrbracket : \text{Nat} \rightarrow \mathbb{N}$ inductivement par :

- $\llbracket Z \rrbracket = 0$
- si $n \in \text{Nat}$, alors $\llbracket S(n) \rrbracket = \llbracket n \rrbracket + 1$

$\llbracket \cdot \rrbracket = \text{interprétation}$

Sur $\mathbb{N}$, on définit $\text{encoding} : \mathbb{N} \rightarrow \text{Nat}$ inductivement par :

- $\text{encoding}(0) = Z$
- si $n \in \mathbb{N}$, alors $\text{encoding}(n + 1) = S(\text{encoding}(n))$

$\rightsquigarrow \llbracket \cdot \rrbracket$ et encoding sont des bijections réciproques.

- 1 Définition par induction
 - Définition d'un ensemble
 - Règles d'inférences
 - Définition d'une fonction
- 2 Principe d'induction structurelle

Principe d'induction structurelle

Induction structurelle

Soit $X = \langle \mathcal{B}, \mathcal{K} \rangle$ un ensemble inductif.

Soit P une propriété sur les éléments de X telle que :

- $P(x)$ est vérifiée sur tous les éléments x de $\mathcal{B}$
- pour tous $x_1, \dots, x_n$ de X tels que $P(x_1), \dots, P(x_n)$ est vérifiée et tout $f \in \mathcal{K}$, on peut montrer que $P(f(x_1, \dots, x_n))$ est vérifiée

alors la propriété P est vérifiée pour **tous les éléments** de X .

Principe d'induction structurelle

Induction structurelle

Soit $X = \langle \mathcal{B}, \mathcal{K} \rangle$ un ensemble inductif.

Soit P une propriété sur les éléments de X telle que :

- $P(x)$ est vérifiée sur tous les éléments x de $\mathcal{B}$
- pour tous $x_1, \dots, x_n$ de X tels que $P(x_1), \dots, P(x_n)$ est vérifiée et tout $f \in \mathcal{K}$, on peut montrer que $P(f(x_1, \dots, x_n))$ est vérifiée

alors la propriété P est vérifiée pour **tous les éléments** de X .

Preuve :

On pose $U = \{x \in X \mid P(x) \text{ est vérifiée}\}$ et on montre que $X = U$.

$U \subseteq X$ Par définition de U .

$X \subseteq U$ Par hypothèse, $\mathcal{B} \subseteq U$ et U stable par $\mathcal{K}$. Donc $X \subseteq U$.

Induction structurelle – Exemple (1)

On note $P(x) = \text{“}add(x, Z) = x\text{”}$.

$$x + 0 = x$$

Pour montrer que $P(x)$ est vraie pour tout $x \in \text{Nat}$, on doit procéder par **induction sur x** :

Induction structurelle – Exemple (1)

On note $P(x) = \text{“}add(x, Z) = x\text{”}$.

$$x + 0 = x$$

Pour montrer que $P(x)$ est vraie pour tout $x \in \text{Nat}$, on doit procéder par **induction sur x** :

($\mathcal{B}$) un seul cas de base : $x = Z$

Dans ce cas, on a bien $add(Z, Z) = Z$ par déf. de add .

Induction structurelle – Exemple (1)

On note $P(x) = \text{“}add(x, Z) = x\text{”}$.

$$x + 0 = x$$

Pour montrer que $P(x)$ est vraie pour tout $x \in \text{Nat}$, on doit procéder par **induction sur x** :

($\mathcal{B}$) un seul cas de base : $x = Z$

Dans ce cas, on a bien $add(Z, Z) = Z$ par déf. de add .

($\mathcal{K}$) un seul cas de construction : $x = S(n)$

On **suppose** $P(n)$ vraie, c'est-à-dire $add(n, Z) = n$.

On en que **déduit** $P(S(n)) = P(x)$ est vraie aussi :

Induction structurelle – Exemple (1)

On note $P(x) = \text{“}add(x, Z) = x\text{”}$.

$$x + 0 = x$$

Pour montrer que $P(x)$ est vraie pour tout $x \in \text{Nat}$, on doit procéder par **induction sur x** :

($\mathcal{B}$) un seul cas de base : $x = Z$

Dans ce cas, on a bien $add(Z, Z) = Z$ par déf. de add .

($\mathcal{K}$) un seul cas de construction : $x = S(n)$

On **suppose** $P(n)$ vraie, c'est-à-dire $add(n, Z) = n$.

On en **déduit** $P(S(n)) = P(x)$ est vraie aussi :

$$\begin{aligned} add(S(n), Z) &= S(add(n, Z)) \\ &= S(n) \end{aligned}$$

déf. de add

hypothèse d'induction

Induction structurelle – Exemple (2)

Montrons $P(x) = \llbracket \text{double}(x) \rrbracket = 2 \llbracket x \rrbracket$ par induction sur x :

($\mathcal{B}$) un seul cas de base : $x = Z$

($\mathcal{K}$) un seul cas de construction : $x = S(n)$

On suppose que $\llbracket \text{double}(n) \rrbracket = 2 \llbracket n \rrbracket$.

Induction structurelle – Exemple (2)

Montrons $P(x) = “\llbracket \text{double}(x) \rrbracket = 2 \llbracket x \rrbracket”$ par induction sur x :

($\mathcal{B}$) un seul cas de base : $x = Z$

$$\llbracket \text{double}(Z) \rrbracket = \llbracket Z \rrbracket = 0 \quad \text{déf. de } \text{double} \text{ et } \llbracket \cdot \rrbracket$$

$$2 \llbracket Z \rrbracket = 2 \times 0 = 0 \quad \text{déf. de } \llbracket \cdot \rrbracket$$

($\mathcal{K}$) un seul cas de construction : $x = S(n)$

On suppose que $\llbracket \text{double}(n) \rrbracket = 2 \llbracket n \rrbracket$.

Induction structurelle – Exemple (2)

Montrons $P(x) = “\llbracket \text{double}(x) \rrbracket = 2 \llbracket x \rrbracket”$ par induction sur x :

($\mathcal{B}$) un seul cas de base : $x = Z$

$$\begin{aligned}\llbracket \text{double}(Z) \rrbracket &= \llbracket Z \rrbracket = 0 && \text{d\'ef. de } \text{double} \text{ et } \llbracket \cdot \rrbracket \\ 2 \llbracket Z \rrbracket &= 2 \times 0 = 0 && \text{d\'ef. de } \llbracket \cdot \rrbracket\end{aligned}$$

($\mathcal{K}$) un seul cas de construction : $x = S(n)$

On suppose que $\llbracket \text{double}(n) \rrbracket = 2 \llbracket n \rrbracket$.

$$\begin{aligned}\llbracket \text{double}(S(n)) \rrbracket &= \llbracket S(S(\text{double}(n))) \rrbracket && \text{d\'ef. de } \text{double} \\ &= \llbracket \text{double}(n) \rrbracket + 2 && \text{d\'ef. de } \llbracket \cdot \rrbracket \quad (2\times) \\ &= 2 \llbracket n \rrbracket + 2 && \text{hypoth\`ese d'induction} \\ 2 \llbracket S(n) \rrbracket &= 2 (\llbracket n \rrbracket + 1) = 2 \llbracket n \rrbracket + 2 && \text{d\'ef. de } \llbracket \cdot \rrbracket\end{aligned}$$