Induction

But : Définir un nouveau mode de raisonnement (une récurrence généralisée)

1. Ensembles inductifs

1.1. Définitions

Définir un ensemble T de manière inductive c'est :

* définir des éléments de base qui appartiennent à T
* définir des manières de construire des nouveaux éléments de T à partir d'éléments de T

__Exemples__ : Entiers de Peano : $(T = \mathbb{N})$

$$B = \{Zero\} \qquad C = \{Successeur\ t \mapsto Successeur(t)\}$$

Ici : Deux $=$ Successeur $\circ$ Successeur (Zero)

Listes d'entiers : ($T =$ " listes d'entiers ")

$$B = \{[\,]\} \quad C = \{Cons_i : l \mapsto i :: l,\ i \in \mathbb{Z}\}$$

__Déf__ Une définition inductive d'un ensemble T est la donnée de :

* Un ensemble $B \subseteq E$ d'éléments de base.
* Un ensemble C de fonctions $f : E^k \longrightarrow E$ pour un $k \in \mathbb{N}^*$ appellé " arité " de f.

tels que T est le plus petit ensemble qui

* Contient les éléments de B
* Est stable par les constructeurs c'est à dire que :

$$\forall f \in C\ \forall (t_1, \dots, t_{a(f)}) \in T^{a(f)},\ f(t_1, \dots, t_{a(f)}) \in T$$

où $a : f \mapsto a(f)$ donne l'arité de f.

__Prop__ Cette définition marche, il existe un plus petit ensemble qui contient les éléments de B (1) et stable par les constructeurs de C (2

__Preuve__ On définit $\mathcal{F}$ l'ensemble des parties de E qui vérifient (1) et (2)

On a $\mathcal{F} \neq \emptyset$ car $E \in \mathcal{F}$. Considérons $T = \bigcap_{Y \in \mathcal{F}} Y$

Montrons que $T \in \mathcal{F}$.

On a : $\forall Y,\ Y \in \mathcal{F} \Rightarrow B \subseteq Y$ donc $B \subseteq \bigcap_{Y \in \mathcal{F}} Y$ ce qui prouve (1)

Soit $f \in C$ d'arité $k \in \mathbb{N}^*$ et soient $t_1, \dots, t_k \in T$

On a : $\forall i \in [\![1, k]\!]\ \forall Y,\ Y \in \mathcal{F} \Rightarrow t_i \in Y$ donc puisque tout $Y \in \mathcal{F}$ est stable par f on a :

$$\forall Y,\ Y \in \mathcal{F} \Longrightarrow f(t_1, \dots, t_k) \in \mathcal{F}$$

Donc
$$f(t_1, \dots, t_k) \in \bigcap_{Y \in \mathcal{F}} Y \triangleq T$$

ce qui prouve (2)

Montrons que T est le plus petit élément de $(\mathcal{F}, \subseteq)$

Soit $Y \in \mathcal{F}$. T est en particulier l'intersection de Y avec d'autres éléments de $\mathcal{F}$ donc $T \subseteq Y$.

Il n'existe pas d'élément de $\mathcal{F}$ qui n'est pas inclus dans T. □

2. Taille des termes et caractérisations

__Déf__ Un élément de T est appellé un terme

__Déf__ Pour tout $t \in T$, Si $t = f(t_1, \dots, t_{a(f)})$ pour un certain $f \in C$ et de certaines $t_1, \dots, t_{a(f)} \in T$, Alors $t_1, \dots, t_{a(f)}$ sont des sous termes immédiats de t.

__Exemple__ Soit $l = 1 :: 5 :: 3 :: [\,] = Cons_1(5 :: 3 :: [\,])$ donc $5 :: 3 :: [\,]$ est un sous terme immédiat de l.

Autre exemple de définition inductive :

$$B = \mathbb{N}$$
$$C = \left\{ \begin{array}{ll} + : (t_1, t_2) \longmapsto t_1 + t_2 \\ - : (t_1, t_2) \longmapsto t_1 - t_2 \\ \times : (t_1, t_2) \longmapsto t_1 \cdot t_2 \\ \div : (t_1, t_2) \longmapsto t_1 / t_2 \end{array} \right\} \text{Tous d'arité 2.}$$

T l'ensemble des opérations arithmétiques.

Exemple de terme :

$$12$$
$$1+2 \equiv +(1, 2)$$
$$5 \times 3 + 45 \equiv +(\times(5, 3), 45)$$

__Déf__ On dit qu'une définition par induction est ambigüe s'il existe un terme t qu'ont peut obtenir en combinant les constructeurs et les éléments de base de deux manières différentes.

__Déf__ Une définition inductive (B, C) est non ambigüe si

* $\forall f \in C,\ \forall (t_1, \dots, t_{a(f)}) \in T^{a(f)}\ f(t_1, \dots, t_{a(f)}) \notin B$
* $\forall (f, g) \in C^2\ \forall (t_1, \dots, t_{a(f)}) \in T^{a(f)}\ \forall (u_1, \dots, u_{a(g)}) \in T^{a(g)}$

$$f(t_1, \dots, t_{a(f)}) \neq g(u_1, \dots, u_{a(g)})$$

__Ex__ L'ensemble des entiers de Peano a une définition inductive non ambigüe
La définition des listes (c.f. plus haut) est non ambigüe.

__Déf__ Soit (B, C) une définition inductive non ambigüe.

La taille d'un terme t est le nombre de constructeur utilisées pour le définir
La hauteur d'un terme est le nombre de constructeurs emboîtés nécessaires pour le définir.

__Ex__ $Cons_1 \circ Cons_3 \circ Cons_{12} \circ Vide \equiv [1, 3, 12]$

Sa taille vaut 3 (de même que sa hauteur)

$$+(-(5, 4), \times(2, 12)) \equiv 5 - 4 + 2 \times 12$$

Sa taille vaut 3 mais sa hauteur vaut 2.

$$+(\times(+(5, 2), 3), \times(\times(1, 0), \times(12, -(3, 5))))$$

Sa taille vaut 7 mais sa hauteur vaut 4

__Rq__ Pour les définitions ambigües la notion n'a pas de sens car on ne peut pas garantir l'unicité taille, hauteur dans deux définitions d'un même terme

__Ex__ $B = \mathbb{N} \quad C = \{* : (a, b) \longmapsto a \wedge b\}$ où $\wedge$ est un concaténateur.

$$1.337 \longrightarrow 1337 \longleftarrow 133.7$$
$$13.37 \longrightarrow 1337$$

__Déf__ On définit $(T_i)_{i \in \mathbb{N}} \in \mathcal{P}(E)^{\mathbb{N}}$ par récurrence :

* $T_0 := B$
* $\forall n \in \mathbb{N},\ T_{n+1} := T_n \cup \left\{ f(t_1, \dots, t_k) \;\middle|\; \begin{array}{l} f \in C \text{ d'arité } k \\ t_1, \dots, t_k \in T \end{array} \right\}$

__Rq__ Pour tout $n \in \mathbb{N}$, T_n est l'ensemble des termes qu'on peut obtenir en imbriquant au plus n constructeurs.

__Ex__ Pour T les entiers de Peano :

$$T_0 = \{Zero\}$$
$$T_1 = \{Zero,\ s(Zero)\}$$
$$T_2 = \{Zero,\ s(Zero),\ s \circ s(Zero)\}$$

Par récurrence : $T_n = \bigcup_{k=0}^{n} \{s^k(Zero)\}$ $(s^0 = id)$

Pour T les listes :

$$T_0 = \{[\,]\}$$
$$T_1 = \{[\,]\} \cup \{Cons_i([\,]),\ i \in \mathbb{Z}\}$$

__Rq__ $(T_i)_{i \in \mathbb{N}}$ est croissante pour l'inclusion

__Théorème__ Caractérisation de T : $\quad T = \bigcup_{i \in \mathbb{N}} T_i$

__Preuve__ On note $T' = \bigcup_{i \in \mathbb{N}} T_i$

$\boxed{\supset}$ Montrons par récurrence sur $i \in \mathbb{N}$ que $T_i \in T$

Cas de base : $T_0 \triangleq B \subseteq T$: c'est bon

Hérédité : Supposons, à $i \in \mathbb{N}$ fixé que $T_i \subseteq T$
Soit f un constructeur, on note k sont arité et on prend $t_1, \dots, t_k$ dans T_i
Puisque T est stable par les constructeurs et que quelque soit $j \in [\![1, k]\!]$ $t_j \in T$, on a :

$$f(t_1, \dots, t_k) \in T$$

Donc tout élément de T_{i+1} est dans T
i.e. $T_{i+1} \subseteq T$.

Conclusion : Par principe de récurrence : $\forall i \in \mathbb{N}\ T_i \subseteq T$.

donc $T' = \bigcup_{i \in \mathbb{N}} T_i \subseteq T$

$\boxed{\supset}$ On sait que $T_0 \triangleq B \subseteq T'$. Montrons que T' est stable par les constructeurs de C : soit f un constructeur d'arité k et soient $t_1, \dots, t_k \in T'$.

Comme T' est une union, on sait que :

$$\forall i \in [\![1, k]\!],\ \exists n_i \in \mathbb{N},\ t_i \in T_{n_i}$$

On considère $n := \max_{i \in [\![1, k]\!]} n_i$, puisque la suite $(T_i)_{i \in \mathbb{N}}$ est croissante, on a : $\forall i \in [\![1, k]\!],\ t_i \in T_n$
Donc $f(t_1, \dots, t_k) \in T_{n+1} \subseteq T'$ donc $f(t_1, \dots, t_k) \in T'$.

Or T est le plus petit ensemble qui contient B et que est stable par les constructeurs

Ainsi : $T \subseteq T'$

$\boxed{\text{Cc}}$ Finalement on a $T = T'$

Preuve par Induction Structurelle

On considère un ensemble E et un ensemble T défini inductivement par (B, C).

Soit $P : E \to \{vrai, faux\}$ un prédicat. On s'intéresse aux manières de montrer que pour $t \in T$, $P(t)$ est vrai.

<u>Théorème</u> Si les conditions suivantes sont vérifiées

* Pour tout $t \in B$, $P(t)$ est vrai
* Pour tout $f \in C$ d'arité k et pour tous $(t_1, \dots, t_k) \in E^k$
  Si $P(t_1), \dots, P(t_k)$ sont vrais,
  Alors $P(f(t_1, \dots, t_k))$ doit être vrai.

Alors pour tout $t \in T$, $P(t)$ est vrai

<u>Preuve</u> Soit $\mathcal{A} = \{x \in E \mid P(x) \text{ vrai}\}$

Montrons que $B \subseteq \mathcal{A}$ et que $\mathcal{A}$ est stable par les constructeurs.

Par hypothèse, tous les éléments de B vérifient P donc $B \subseteq \mathcal{A}$.

Soit f un constructeur d'arité k et $t_1, \dots, t_k \in \mathcal{A}$ alors $P(f(t_1, \dots, t_k))$ est vrai donc $f(t_1, \dots, t_k) \in \mathcal{A}$

D'où $T \subseteq \mathcal{A}$ par minimalité de T.

<u>Ex</u> On considère T défini de manière inductive par

$B = \{a\}$

$C = \{f_b : (t_1, t_2) \longmapsto b \wedge t_1 \wedge t_2 \ ; \ f_c : (t_1, t_2, t_3) \mapsto c \wedge t_1 \wedge t_2 \wedge t_3\}$

Exemples de termes : $\{baa, a, caaa, \dots\}$

$cbaaaa = f_c(f_b(a, a), a, a)$

$ccaaacaaacbbaaaaa = f_c\left(f_c\begin{pmatrix} a \\ a \\ a \end{pmatrix}, f_c\begin{pmatrix} a \\ a \\ a \end{pmatrix}, f_c\begin{pmatrix} f_b(f_b(a,a),a) \\ a \\ a \end{pmatrix}\right)$

On veut montrer que $|t|_a = 2|t|_c + |t|_b + 1$.

On raisonne par induction structurelle sur la structure des termes

$\boxed{I}$ $|a|_a = 2 \times 0 + 0 + 1 = 1$: ça marche.

$\boxed{H}$ Considérons le cas inductif. Soit u un mot

* Si $u = f_b(t_1, t_2)$ avec $t_1, t_2 \in T$ qui vérifient la propriété

  Alors $u = bt_1t_2$ et donc
  $|u|_a = |t_1|_a + |t_2|_a$
  $|u|_b = |t_1|_b + |t_2|_b + 1$
  $|u|_c = |t_1|_c + |t_2|_c$

  Ainsi : $|u_a| = |t_1|_a + |t_2|_a$
  $\overset{(H)}{=} 2|t_1|_c + |t_1|_b + 1 + 2|t_2|_c + |t_2|_b + 1$
  $= 2(|t_1|_c + |t_2|_c) + (|t_1|_b + |t_2|_b + 1) + 1$
  $= 2|u|_c + |u|_b + 1$

* Si $u = f_c(t_1, t_2, t_3)$ avec $t_1, t_2, t_3 \in T$ qui vérifient la propriété.

  Alors $u = ct_1t_2t_3$ donc
  $|u|_a = |t_1|_a + |t_2|_a + |t_3|_a$
  $|u|_b = |t_1|_b + |t_2|_b + |t_3|_b$
  $|u|_c = 1 + |t_1|_c + |t_2|_c + |t_3|_c$

  Ainsi $|u|_a = |t_1|_a + |t_2|_a + |t_3|_a$
  $= 2(|t_1|_c + |t_2|_c + |t_3|_c + 1) + |t_1|_b + |t_2|_b + |t_3|_b + 1$
  $= 2|u|_c + |u|_b + 1$.

Par principe d'induction structurelle, la propriété est vraie pour tous les termes.

<u>Exo</u> $B = \{c\}$

$C = \{f_1 : t \longmapsto atb \ ; \ f_2 : t \longmapsto tb\}$

Montrer que $\forall t \in T$, $|t|_b \geq |t|_a$

$\boxed{I}$ Pour $t = c$: $|c|_b = 0 = |c|_a$: c'est bon

$\boxed{H}$ Soit t un mot

* Si $t = f_1(t_1)$, alors $t = at_1b$ (t_1 vérifie les conditions)

  Donc $|t|_b = |t_1|_b + 1 \overset{(H)}{\geq} |t_1|_a + 1 = |t|_a$

* Si $t = f_2(t_1)$, alors $t = t_1b$ ($t_1 \dots$)

  Donc $|t|_b = |t_1|_b + 1 \overset{(H)}{\geq} |t_1|_a + 1 \geq |t_1|_a$

Dans tous les cas $|t_1|_b \geq |t_1|_a$.

$\boxed{C}$ Par induction, $\forall t \in T$, $|t_1|_b \geq |t_1|_a$.

Ordre induit

Rappel Un ordre est une relation binaire transitive, réflexive, antisymétrique

On considère une définition non-ambigüe de T
On note $t_1 \prec_i t_2$ pour $t_1, t_2 \in T$ si t_1 est un sous terme immédiat de t_2. La relation $\prec_i$ n'est ni reflexive ni transitive, ce n'est pas une relation d'ordre. Cependant elle est antisymétrique car la définition est non ambigüe.
On veut trouver un ordre sur T, on va transformer T en un ordre.

Déf La cloture transitive d'une relation binaire $\mathcal{R} \subseteq E^2$ est une relation $\mathcal{R}^{trans} \subseteq E^2$ telle que :

$$\forall (x,y) \in E^2,\ x \mathcal{R} y \iff \left[\exists n \in \mathbb{N}^* \ \exists (c_0, \dots, c_n) \in E^{n+1},\ c_0 = x \wedge c_n = y \wedge (\forall i \in [\![0, n-1]\!]\ c_i \mathcal{R} c_{i+1})\right]$$

Prop Cette relation est transitive

Prop On a : $\forall (x,y) \in E^2,\quad x \mathcal{R} y \implies x \mathcal{R}^{trans} y$

Prop $\mathcal{R}_{trans}$ est la plus petite relation transitive qui contient $\mathcal{R}$

Cor $\prec_i^{trans}$ est une relation transitive.

Déf Soit $\mathcal{R} \subseteq E^2$ une relation binaire. Sa cloture transitive reflexive $\mathcal{R}^{trans} \subseteq E^2$ est définie par :

$$\mathcal{R}^{trans\text{-}refl} := \mathcal{R}^{trans} \cup \{(x,x) \mid x \in E\}$$

Prop $\mathcal{R}^{trans\text{-}refl}$ est transitive, reflexive, et $\mathcal{R} \subseteq \mathcal{R}^{trans\text{-}refl}$

Déf On appelle ordre induit sur T la relation $\preceq$ qui est la cloture transitive reflexive de $\prec_i$

Lemme Si $t_1 \preceq t_2$ et $t_1 \neq t_2$ Alors la taille de t_1 est strictement inférieure à celle de t_2.

Prop $\preceq$ est antisymétrique.

Preuve Soit $(x,y) \in T^2$. Supposons par l'absurde que $x \preceq y$ et $y \preceq x$ et $x \neq y$.

D'après le lemme, la taille de x est strictement inférieure à celle de y. Le lemme dit aussi que la taille de x est strictement inférieure à celle de y.

C'est absurde

Donc $\preceq$ est bien une relation d'ordre.

Déf On dit qu'une relation d'ordre $\mathcal{R} \subseteq E^2$ est bien foudée s'il n'existe pas de suite strictement décroissante infinie dans E.

Prop L'ordre induit $\preceq$ sur T est bien foudé.

Preuve Supposons l'existence d'une suite strictement décroissante et infinie $(t_n) \in T^{\mathbb{N}}$. Pour tout $i \in \mathbb{N}$, on note τ_i la taille du terme t_i.

On a : $\forall i \in \mathbb{N},\ t_i \succeq t_{i+1} \wedge t_i \neq t_{i+1}$ (stricte décroissance)

Le lemme nous indique $\tau_i > \tau_{i+1}$. Donc (τ_n) est une suite infinie strictement décroissante d'éléments de $\mathbb{N}$

C'est absurde, la suite (t_n) n'existe pas.

Rq La relation $\preceq$ n'est pas totale.

Ex
$[1;3] \ \underset{\prec_i}{\preceq}\ [5;1;3]$ (sous terme immédiat $Cons_5$)
$[2;12] \ ? \ [4;5]$: (pas comparable)
$[1;2;3] \succeq [3]$ ($Cons_2 \circ Cons_1$)

$$[1;2;3] \succeq [2;3] \succeq [3]$$

Applications inductives

Ex $B = \{[\,]\}$ $\quad C = \{ Cons_i : l \mapsto i :: l \ ,\ i \in \mathbb{Z} \}$

On veut définir la longueur d'une liste par :

$$longueur : \begin{array}{rcl} T & \longrightarrow & \mathbb{N} \\ [\,] & \longmapsto & 0 \\ x :: xs & \longmapsto & 1 + longueur(xs) \end{array}$$

Soit $T(B, C)$ quelconque et soit F un ensemble.
Pour définir $\varphi : T \longrightarrow F$, il suffit de définir $\varphi(b)$ pour tout $b \in B$ et de décrire, pour tout $f \in C$ d'arité k et pour tous $t_1, \dots, t_k \in T$, comment obtenir $\varphi(f(t_1, \dots, t_k))$ à partir de $\varphi(t_1), \dots, \varphi(t_k)$ et $t_1, \dots, t_k$.
Pour chaque $f \in C$ d'arité k, cela revient à définir une fonction

$$\varphi_f : E^k \times F^k \longrightarrow F$$

avec $\varphi(f(t_1, \dots, t_k)) = \varphi_f(t_1, \dots, t_k ; \varphi(t_1), \dots, \varphi(t_k))$

Ex Pour la fonction somme d'une liste d'entiers

$$\begin{cases} somme : 0 \longmapsto 0 \\ somme_{Cons_i} : l, somme(l) \longmapsto i + somme(l) \end{cases}$$

Rq Définir une application de cette manière ne marche que si la définition est non ambigüe

Ex $T : \begin{array}{l} B = \mathbb{N} \\ C = \{ \cdot : (a, b) \mapsto a \wedge b \} \end{array}$

On veut définir $\varphi : T \to \mathbb{N}$ qui compte le nombre de $\cdot$ qui ont été utilisés.

Or $\varphi(1920) = \varphi(1.920) = \varphi(1.9.20)$

$$\underset{1}{\parallel} \quad \overset{?}{=} \text{ absurde} \quad \underset{2}{\parallel}$$

Prop Si la définition de T est non ambigüe, alors définir φ par la manière exposée associe une et une seule image à chaque terme

Preuve Par induction structurelle.

Rq Les constructeurs peuvent être des fonctions partielles et n'être définies que sur une partie de E^k

Ex $B = \{\varepsilon\}$ $\quad C = \left\{ \begin{array}{l} f_1 : u = a(*)b \mapsto au \\ f_2 : u = a(*)a \mapsto ub \end{array} \right\}$