Induction

Luigi Santocanale

Laboratoire d'Informatique Fondamentale,
Centre de Mathématiques et Informatique,
39, rue Joliot-Curie - F-13453 Marseille

Plan

L'arithmétique de Peano

Langage : $\mathcal{L} = \{0, s, +, =\}$.

$$\neg\exists x(\, 0 = s(x)\,)$$
$$\forall x, y(\, s(x) = s(y) \Rightarrow x = y\,)$$
$$\forall x(\, x + 0 = x\,)$$
$$\forall x, y(\, x + s(y) = s(x + y)\,)$$

Les axiomes d'induction :

$$(\, P(0) \wedge \forall x(\, P(x) \Rightarrow P(s(x))\,)\,) \Rightarrow \forall y P(y)$$

Exemple : on peut dériver $\forall y P(y)$ où

$$P(y) \equiv y \neq 0 \Rightarrow \exists z(s(z) = y)$$

Remarques

Soit

$$x < y \equiv \exists z(\, x + s(z) = y\,).$$

On peut dériver, dans l'arithmétique de Peano, le principe d'induction complète (« course of values ») :

$$\forall x(\, \forall y(\, y < x \Rightarrow P(y)\,) \;\Rightarrow\; P(x)\,) \;\Rightarrow\; \forall z P(z)$$

Induction structurelle

Ensembles inductives, exemple, les termes :

- $\forall x \in X, x \in \mathcal{T}(\Omega, X)$,
- si $f \in \Omega$, $ar(f) = n$, et $t_1, \ldots, t_n \in \mathcal{T}(\Omega, X)$, alors $f(t_1, \ldots, t_n) \in \mathcal{T}(\Omega, X)$,
- rien d'autre appartient à $\mathcal{T}(\Omega, X)$.

Principe d'induction structurelle : si

$$\forall x \in X, P(x),$$
$$P(t_1), \ldots, P(t_n) \text{ implique } P(f(t_1, \ldots, t_n)),$$

alors,

$$P(t)\,, \quad \text{pour tout } t \in \mathcal{T}(\Omega, X)$$

Autres exemples : les arbres, les types inductives de OCaml...

De l'induction structurelle à l'induction complète

Définissons *par induction* la fonction de complexité

$$\chi(x) = 0$$
$$\chi(f(t_1, \ldots, t_n)) = 1 + \max(\chi(t_1, \ldots, t_n))\,.$$

L'induction structurelle pour $P(t)$, $t \in \mathcal{T}(\Omega, X)$, se réduit au principe d'induction complète pour $Q(x)$, $x \in \mathcal{N}$:

$$Q(x) \equiv \forall t \in \mathcal{T}(\Omega, X)(\,\chi(t) = x \Rightarrow P(t)\,)\,.$$

Problème : ça veut dire quoi « définir par induction » ?
Solution :
prendre cette propriété (possibilité de définir par induction) comme point de départ pour définir les ensembles inductifs.

Induction et foncteurs

Soit

$$\Omega_n = \{\, f \in \Omega \mid ar(f) = n \,\}$$
$$T(Y) = X + \sum_{n \geq 0} \Omega_n \times Y^n\,.$$

$T(Y)$ est un foncteur :

$$h : Y \longrightarrow Z \qquad T(h) : T(Y) \longrightarrow T(Z)$$
$$T(h)(x) = x$$
$$T(h)(f, y_1, \ldots, y_n) = (f, h(y_1), \ldots, h(y_n))\,.$$

L'ensemble $\mathcal{T}(\Omega, X)$ satisfait :

$$\gamma : T(\mathcal{T}(\mathcal{O}, X)) \longrightarrow \mathcal{T}(\mathcal{O}, X)$$
$$\text{et si } \alpha : T(Y) \longrightarrow Y$$

alors $\exists! f : \mathcal{T}(\Omega, X) \longrightarrow Y$ telle que $f \circ \gamma = \alpha \circ T(f)$.

Exemple : la fonction complexité

La fonction $\chi : \mathcal{T}(\Omega, X) \longrightarrow \mathcal{N}$ est la seule telle que

$$\chi \circ \gamma = \alpha \circ T(\chi)$$

où $\alpha : T(\mathcal{N}) \longrightarrow \mathcal{N}$ est définie par

$$\alpha(x) = 0$$
$$\alpha(f, n_1, \ldots, n_k) = 1 + max(n_1, \ldots, n_k)\,.$$

Proposition

Étant donné un foncteur T, il existe au plus (à bijection prise) un couple $(\mu.T, \gamma)$ (ensemble plus fonction $\gamma : T(\mu.T) \longrightarrow \mu.T$) satisfaisant une telle propriété.

Cette propriété définit $\mathcal{T}(\Omega, X)$ de façon univoque.

Exemple/Exercice : induction structurelle

Démontrer, par induction structurelle, que pour tout $a \in \mathcal{A}exp$

$$\forall \sigma \in \mathcal{S}, n \in \mathcal{N}$$
$$(a,\sigma) \to n \wedge (a,\sigma) \to n' \Rightarrow n = n' .$$

Démonstration.

La propriété est vraie si $a = \hat{n}$ ou $a = X$: ...
Supposons que la propriete est vraie pour a_0, a_1, demontrons-la pour $a_0 + a_1$, $a_0 - a_1$, $a_0 * a_1$: ...

□

Exercice : démontrer que $\forall a, \sigma \exists n$ t.q. $(a,\sigma) \to n$.

Relations bien fondées et induction

Une relation $<$ est bien fondée ssi il n'existe pas une suite infinie de la forme

$$\ldots a_n < \ldots < a_1 < a_0$$

Exemple : $(\mathcal{N}, <)$ sont données, définissons $(\mathcal{N} \times \mathcal{N}, <)$ par

$$(a,b) < (c,d) \text{ ssi } a \leq c, b \leq d \text{ et } a < c \text{ ou } b < d$$

Principe de l'induction bien fondée (cf.l'induction complète) :

$$\forall x(\ \forall y(\ y < x \Rightarrow P(y)\ ) \Rightarrow P(x)) \Rightarrow \forall z P(z)$$

Exemple

Le programme *Euclid*

$$\begin{aligned} \mathit{Euclid} \equiv\ & \mathit{while}\ \mathit{not}(M = N)\ \mathit{do} \\ & \mathit{if}\ (M \leq N)\ \mathit{then}\ N := N - M\ \mathit{else}\ M := M - N \end{aligned}$$

On veut montrer que ce programme se termine ... et plus.

Proposition

Pour tout état σ tel que $\sigma(M) > 0$ et $\sigma(N) > 0$, il existe un état σ' tel que

$$(\mathit{Euclid}, \sigma) \to_{\mathcal{C}om} \sigma'$$
$$\sigma'(M) = \sigma'(N) > 0$$

Preuve

Posons

$$\begin{aligned} \mathcal{N}_+ &= \{\ n \in \mathcal{N} \mid n > 0\ \} \\ \mathcal{S}_+ &= \{\ \sigma \in \mathcal{S} \mid (\sigma(M), \sigma(N)) \in \mathcal{N}_+ \times \mathcal{N}_+\ \} \\ \chi : \mathcal{S}_+ &\longrightarrow \mathcal{N}_+ \times \mathcal{N}_+ \quad \text{définie par} \\ \chi(\sigma) &= (\ \sigma(M), \sigma(N)\ ) . \end{aligned}$$

Soit $\sigma \in \mathcal{S}_+$, et supposons que pour tout $\tilde{\sigma} \in \mathcal{S}_+$ tel que $\chi(\tilde{\sigma}) < \chi(\sigma)$ la proposition est vraie.

Preuve II

Si $(\neg(M = N), \sigma) \to 0$ alors $(Euclid, \sigma) \to \sigma$.

Sinon $(\neg(M = N), \sigma) \to 1$ et $\sigma(M) \neq \sigma(N)$.

On a que

$$(\mathit{if}\ (M \leq N)\ \mathit{then}\ N := N - M\ \mathit{else}\ M - N, \sigma) \to_{\mathcal{C}om} \tilde{\sigma}$$

pour un unique état $\tilde{\sigma}$.

On prétends que $\tilde{\sigma} \in \mathcal{S}_+$ et $\chi(\tilde{\sigma}) < \chi(\sigma)$.

Preuve III

Car

$$\begin{aligned}(M \leq N, \sigma) \to 1 &\Rightarrow \sigma(M) < \sigma(N)\\ &\Rightarrow 0 < \sigma(N) - \sigma(M) < \sigma(N)\\ &\Rightarrow 0 < \tilde{\sigma}(N) < \sigma(N)\\ &\Rightarrow \tilde{\sigma} < \sigma\end{aligned}$$

et

$$\begin{aligned}(M \leq N, \sigma) \to 0 &\Rightarrow \sigma(N) < \sigma(M)\\ &\Rightarrow 0 < \sigma(M) - \sigma(N) < \sigma(M)\\ &\Rightarrow 0 < \tilde{\sigma}(M) < \sigma(M)\\ &\Rightarrow \tilde{\sigma} < \sigma\end{aligned}$$

Preuve IV

Par hypothèse d'induction $(Euclid, \tilde{\sigma}) \to_{\mathcal{C}om} \sigma'$ et donc :

$$\frac{\begin{array}{ccc}\vdots & \vdots & \vdots\\ (\mathit{not}(M = N), \sigma) \to 1 & (\mathit{if}\ (M \leq N)\ \mathit{then} \ldots, \sigma) \to \tilde{\sigma} & (Euclid, \tilde{\sigma}) \to \sigma'\end{array}}{(Euclid, \sigma) \to \sigma'}$$

□

Induction sur les règles

Règles de la sémantique opérationnelle ont la forme :

$$\frac{x_1, \ldots, x_n}{x}$$

où x_i, x ont la forme

$$\begin{array}{ll}(a, \sigma) \to n & \text{i.e. } x \in \mathcal{A}exp \times \Sigma \times \mathcal{N}\\ (b, \sigma) \to v & \text{i.e. } x \in \mathcal{B}exp \times \Sigma \times \mathcal{N}\\ (c, \sigma) \to \sigma' & \text{i.e. } x \in \mathcal{C}om \times \Sigma \times \mathcal{N}\end{array}$$

Système des règles

Définition

Un système de regles est un couple $R = (U, R)$ où

- U est un enseble,
- R est un ensemble de couples ordonnées X/y, X sous ensemble fini de Y, et $y \in U$,

Definition

Posons

- $\Vdash_R y$ ssi il est possible de construire une arbre étiqueté (arbre de dérivation), à l'aide des telles règles, dont la racine est étiquetée par y,
- $I_R = \{ x \in U \mid \Vdash_R x \}$.

L'induction sur les règles

Si pour tout règle $X/y \in R$

$$\forall x(x \in X \Rightarrow P(x)) \quad \Rightarrow \quad P(y)$$

alors

$$P(x) , \forall x \in I_R .$$

Justification de ce principe

Soit

$$f_R : \mathcal{P}(U) \longrightarrow \mathcal{P}(U)$$
$$f_R(Z) = \{ y \mid \exists X/y \in R \text{ t.q. } X \subseteq Z \}$$

On a :

$$\begin{aligned} f_R(\emptyset) &= \{ x \mid \emptyset/x \in R \} \\ &= \{ x \mid x \text{ est dérivable à l'aide d'un arbre d'hauteur au plus } 1 \} \\ &= \{ x \mid x \text{ est un axiome } \} \end{aligned}$$

Justification de ce principe (II)

Supposons que

$f_R^n(\emptyset) = \{ x \mid x \text{ est derivable à l'aide d'un arbre d'hauteur au plus } n \}$

alors

$$\begin{aligned} f_R^{n+1}(\emptyset) &= f(f_R^n(\emptyset)) \\ &= \{ y \mid \exists X/y \in R,\ X \subseteq f_R^n(\emptyset) \} \\ &= \{ y \mid y \text{ est dérivable en un seul coup d'un ensemble } X, \\ &\qquad \text{et, pour tout } x \in X, \\ &\qquad x \text{ est dérivable à l'aide d'un arbre d'hauteur au plus } n \} \\ &= \{ y \mid y \text{ est dérivable à l'aide d'un arbre d'hauteur au plus } n+1 \} \end{aligned}$$

On a donc

$$I_R = \bigcup_{n \geq 0} f_R^n(\emptyset) .$$

Propriétés de f_R et I_R

f_R est *croissante* (monotone) :

$$A \subseteq B \;\Rightarrow\; f_R(A) \subseteq f_R(B) \qquad (1)$$

I_R est un *point préfixe* de f_R :

$$f_R(I_R) \subseteq I_R \qquad (2)$$

I_R est le *plus petit point préfixe* de f_R :

$$f_R(A) \subseteq A \;\Rightarrow\; I_R \subseteq A\,. \qquad (3)$$

Preuve : $A \subseteq B \;\Rightarrow\; f_R(A) \subseteq f_R(B)$

Soit $A \subseteq B$.

$$\begin{aligned} y \in f_R(A) \text{ ssi } & \exists X / y \in R \text{ tel que } X \subseteq A && \text{définition } f_R \\ \text{alors } & \exists X / y \in R \text{ tel que } X \subseteq B && A \subseteq B \\ \text{ssi } & y \in f_R(B)\,. && \text{définition } f_R \end{aligned}$$

Donc $f_R(A) \subseteq f_R(B)$.

□

Preuve : $f_R(I_R) \subseteq I_R$.

Soit $y \in f_R(I_R)$, c.-à-d.

$$\exists X / y \in R \text{ tel que } X \subseteq I_R = \bigcup_{n \geq 0} f_R^n(\emptyset)$$

Car X est fini et

$$\emptyset \subseteq f_R(\emptyset) \subseteq \ldots \subseteq f_R^n(\emptyset) \subseteq \ldots$$

il existe $n \geq 0$ tel que $X \subseteq f_R^n(\emptyset)$.

On a donc

$$\exists X / y \in R \text{ tel que } X \subseteq f_R^n(\emptyset)\,,$$

c.-à-d. $y \in f_R(f_R^n(\emptyset)) = f_R^{n+1}(\emptyset) \subseteq I_R$.

□

Preuve : $f_R(A) \subseteq A \;\Rightarrow\; I_R \subseteq A$

Soit $A \subseteq U$ tel que $f_R(A) \subseteq A$.
Car

$$I_R = \bigcup f_R^n(\emptyset)$$

il suffit de montrer que $f^n(\emptyset) \subseteq A$ pour tout $n \geq 0$.
Par induction sur n :

$$f_R^0(\emptyset) = \emptyset \subseteq A$$

Supposons $f^n(\emptyset) \subseteq A$:

$$\begin{aligned} f_R^{n+1}(\emptyset) &= f_R(f_R^n(\emptyset)) \\ &\subseteq f_R(A) && f_R^n(\emptyset) \subseteq A,\ f_R \text{ croissante} \\ &\subseteq A && f_R(A) \subseteq A. \end{aligned}$$

□

Justification du principe d'induction sur les règles

Analysons la propriété

$$f_R(P) \subseteq P \Rightarrow I_R \subseteq P$$

$f(P) \subseteq P$ ssi $(\exists X / y \in R$ tel que $X \subseteq P)$ implique $y \in P$
ssi $\forall X / y \in R\ (X \subseteq P$ implique $y \in P)$
ssi P est un ensemble fermé sous les règles
$I_R \subseteq P$ ssi tout élément dérivable est dans P

c.-à-d. : La propriété de plus petit point fixe donne :

si P est une propriété fermée sous les règles,
alors tout élément dérivable possède cette propriété.

Il s'agit du principe d'induction sur les règles.

Les axiomes de plus petit point préfixe

On peut dériver un grand nombre de conséquences à partir de 1-3.

Par exemple :

Proposition

On a l'égalité suivante :

$$f_R(I_R) = I_R\,.$$

Preuve

Il suffit de demontrer que $I_R \subseteq f_R(I_R)$.

On a

$$f_R(I_R) \subseteq I_R$$

et donc

$$f_R(f_R(I_R)) \subseteq f_R(I_R) \qquad f_R \text{ croissante}$$

ce que implique

$$I_R \subseteq f_R(I_R) \qquad I_R \text{ p.p.p.pf.}$$

□

Le theorème de Tarski

Théorème

Soit

$$f : \mathcal{P}(U) \longrightarrow \mathcal{P}(U)$$

une fonction croissante. Alors

$$\bigcap \{\, A \mid f(A) \subseteq A \,\}$$

est le plus petit point fixe de f.