Le principe d'induction bien fondée

Preuves par induction bien fondée

Une preuve par induction est une méthode de raisonnement qui vise à établir une propriété pour tous les éléments d'un ensemble.

Elle s'appuie sur un ordre strict bien fondé de l'ensemble des éléments pour lequel on cherche à établir la propriété.

Preuves par récurrence sur un ensemble inductif

Soit $\mathcal{A}$ un ensemble et $>$ un ordre strict bien fondé sur $\mathcal{A}$.
Démontrer une propriété P sur $\mathcal{A}$ revient à

– Montrer que la propriété P est vérifiée par tous les éléments minimaux de $>$:

$$\text{pour tout } x \in \mathcal{A} \text{ minimal on a } P(x)$$

– Montrer que la propriété P est vérifiée par tous les éléments non minimaux de $\mathcal{A}$ en sachant qu'elle est vérifiée par ses prédécesseurs :

$$\text{Si pour tout } \ z \in \mathcal{A} \text{ t.q.} z < x \text{ on a } P(z), \text{alors on a } P(x)$$

Principe d'induction bien fondée

Un ensemble $\mathcal{A}$, un ordre strict $>$ et une propriété P sur $\mathcal{A}$

Principe d'induction :

Si

1. "pour tout élément minimal $y \in \mathcal{A}$ on a $P(y)$"
2. "le fait que $P(z)$ soit vérifiée pour tout élément $z<x$ implique $P(x)$"

alors

"pour tout $x \in \mathcal{A}$ on a $P(x)$"

Exemple I

Soit $\mathbb{N}$ l'ensemble des entiers naturels muni de l'ordre

$$m > n \text{ ssi } m \neq n, 1 \text{ et } m \text{ est divisible par } n$$

L'ordre $>$ est strict et bien fondé. Les éléments minimaux sont les nombres premiers.

Soit P la propriété

$$P(n) \text{ ssi } n \text{ possède une factorisation en nombres premiers}$$

Montrer que P est vrai pour tout entier $n \geq 2$.

Exemple II

Montrer que le programme suivant termine sur les entiers naturels positifs.

```
while m <> n do
begin
    if m > n
       then m:= m-n
       else n:= n-m
end
```


Exemple III

Montrer que la fonction d'Ackerman termine sur les entiers naturels.

Ackerman(0,n)	=	n+1
Ackerman(m+1,0)	=	Ackerman(m,1)
Ackerman(m+1,n+1)	=	Ackerman(m,Ackerman(m+1,n))

Ce principe est-il toujours bien défini ?

Théorème :

Si $>$ est bien fondé, alors le principe d'induction est correct.

Théorème :

Si le principe d'induction est correct, alors $>$ est bien fondé.

Preuves par récurrence

Une preuve par récurrence est une méthode de raisonnement qui vise à établir une propriété pour tous les éléments d'un ensemble inductif

Elle s'appuie sur une définition récursive de l'ensemble des éléments pour lequel on cherche à établir la propriété.

Preuves par récurrence sur un ensemble inductif

Soit $\mathcal{A}$ l'ensemble inductif engendré par un système de règles d'inférence. Démontrer une propriété P sur $\mathcal{A}$ revient à

1. Montrer que la propriété P est vérifiée par tous les cas de base de la définition de l'ensemble, c'est à dire par tous les axioms.
2. Montrer que la propriété P est préservée par toute règle d'inférence de la forme

$$\frac{\mathtt{Hyp}_1 \ldots \mathtt{Hyp}_n}{\mathtt{Conclusion}}$$

   C'est à dire, si P est vraie sur $\mathtt{Hyp}_1 \ldots \mathtt{Hyp}_n$, alors P est vraie pour la $\mathtt{Conclusion}$.

Quelle relation entre l'induction bien fondée et recurrence ?

Corollaire : Le principe d'induction bien fondée est correct pour les ensembles inductifs.

Exemple I

Soit $\mathcal{A}$ l'ensemble de tous les entiers naturels.

$P(n) =_{def} 8^n - 1$ est un multiple de 7.

P est-il vraie sur les entiers natures positifs ?

Exemple II

Soit $\mathcal{A}$ l'ensemble de tous les entiers naturels.

$P(n) =_{def} 8^n + 1$ est un multiple de 7.

P est-il vraie sur les entiers natures positifs ?

Exemple III

Soit $\mathcal{A}$ l'ensemble de tous les mots sur un alphabet A.

Soit $concat$ l'opération définie par :

$$\begin{aligned} concat(\epsilon, k) &= k \\ concat(aj_a(l), k) &= aj_a(concat(l, k)) \end{aligned}$$

Montrer que $concat$ est une opération associative.

Exemple IV

Soit $\mathcal{A}$ l'ensemble de tous les arbres binaires.

Soit :

$$\begin{aligned} n(a) &= \text{nb de noeuds internes de } a \\ f(a) &= \text{nb de feuilles de } a \end{aligned}$$

Montrer que $f(a) = n(a) + 1$.

Exemple V

Les expressions sur $\{a, b\}$ avec les opérations binaires S et M, où S et M vérifient les propriétés suivantes :

$$\begin{array}{lll} S(a,a) = a & & M(a,a) = a \\ S(a,b) = b & & M(a,b) = a \\ S(b,a) = b & & M(b,a) = a \\ S(b,b) = b & & M(b,b) = b \end{array}$$

$$\begin{aligned} S(S(e_1,e_2),e_3) &= S(e_1,S(e_2,e_3)) \\ M(M(e_1,e_2),e_3) &= M(e_1,M(e_2,e_3)) \\ S(M(e_1,e_2),e_3) &= M(S(e_1,e_3),S(e_2,e_3)) \\ M(S(e_1,e_2),e_3) &= S(M(e_1,e_3),M(e_2,e_3)) \end{aligned}$$

Démontrer $S(e,b) = b$, $S(e,a) = e$, $M(e,b) = e$ et $M(e,a) = a$.