Définitions préliminaires

Définitions préliminaires

Un préordre (noté $\succsim$) est une relation réflexive et transitive.

L'équivalence associée à un préordre $\succsim$ est définie par $\sim = \succsim \cap \precsim$.

Un ordre ou ordre partielle (noté $\succeq$) est une relation réflexive, anti-symétrique et transitive. On note $s \preceq t$ si $t \succeq s$.

Un ordre strict (noté $\succ$) est une relation iréflexive et transitive.

Chaque ordre $\geq$ définit un ordre strict $>$ par $x > y$ si $x \geq y$ et $x \neq y$.

Chaque ordre strict $>$ définit un ordre $\geq$ par $x \geq y$ si $x > y$ ou $x = y$.

Chaque préordre $\gtrsim$ définit un ordre $\succeq$ sur les classes d'équivalence de $\sim$ par $[s]_\sim \gtrsim [t]_\sim$ si $s \gtrsim t$.

Chaque préordre $\gtrsim$ définit un ordre strict $\succ = \gtrsim \setminus \sim$.

Un ordre strict est bien fondé ssi il n'existe aucune chaîne de la forme $a_0 \succ a_1 \succ a_2 \succ \ldots$.

Un préordre/ordre est bien fondé ssi son ordre strict est bien fondé.

Un élément $a \in \mathcal{A}$ est minimal s'il n'existe pas un autre élément $b \in \mathcal{A}$ t.q. $b \prec a$.

Définitions Inductives et preuves par induction

Définitions inductives en informatique

- Syntaxe concrete
- Syntaxe abstraite
- Règles de typage
- Règles d'évaluation
- ...

Le principe

Une définition inductive est caracterisée par :

- Une ou plusieures assertions
- Un ensemble de règles d'inférence pour dériver ces assertions

Exemple :

- Assertion : "`X est naturel`" ou "`X nat`"
- Règles d'inférence :

  R1 : `0 est naturel`

  R2 : Si `n est naturel`, alors `succ(n) est naturel`.

Notation

Les règles d'inférence sont notées

$$\frac{\texttt{Hypothèse}_1 \ldots \texttt{Hypothèse}_n}{\texttt{Conclusion}}\ \text{(Nom de la règle)}$$

- `Conclusion` est une assertion
- $\texttt{Hypothèse}_1 \ldots \texttt{Hypothèse}_n$ sont des assertions
- En général $n \geq 0$. Si $n = 0$ la règle est un axiome

Exemple (règle unaire)

Les entiers naturels

$$\frac{}{0 \texttt{ est naturel}}\,(Nat0) \qquad \frac{n \texttt{ est naturel}}{succ(n) \texttt{ est naturel}}\,(Nat+)$$

Exemple (règle binaire)

Les arbres binaires

$$\frac{}{vide \texttt{ est un arbre binaire}}\ \text{(Abin-nil)}$$

$$\frac{A_1 \texttt{ est un arbre binaire} \qquad A_2 \texttt{ est un arbre binaire}}{node(A_1, A_2) \texttt{ est un arbre binaire}}\ \text{(Abin-ind)}$$

Exemple

Les mots sur un alphabet A

$$\frac{}{\epsilon \ \texttt{mot}} \qquad \frac{a \in A \quad n \ \texttt{mot}}{a.n \ \texttt{mot}}$$

Exemple (plusieurs axiomes, règles unaires et binaires)

Les expressions de la logique propositionnelle sur l'alphabet A

$$\frac{p \in A}{p \texttt{ expr}}$$

$$\frac{A_1 \texttt{ expr} \qquad A_2 \texttt{ expr}}{A_1 \vee A_2 \texttt{ expr}} \qquad \frac{A_1 \texttt{ expr} \qquad A_2 \texttt{ expr}}{A_1 \wedge A_2 \texttt{ expr}}$$

$$\frac{A_1 \texttt{ expr} \qquad A_2 \texttt{ expr}}{A_1 \rightarrow A_2 \texttt{ expr}} \qquad \frac{A \texttt{ expr}}{\neg A \texttt{ expr}}$$

Exemple (plusieures assertions)

Les forêts

$$\frac{}{vide\ \texttt{arbre}} \qquad \frac{}{nil\ \texttt{foret}}$$

$$\frac{A\ \texttt{arbre} \qquad f\ \texttt{foret}}{cons(A, f)\ \texttt{foret}} \qquad \frac{f\ \texttt{foret}}{node(f)\ \texttt{arbre}}$$

Les termes typables du λ-calcul

$$\frac{}{\Gamma \vdash x : A}$$

$$\frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash (MN) : B} \qquad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x : A.M : A \to B}$$

Dérivation d'une assertion

Une assertion A est dérivable ssi

– A est un axiome

$$\frac{}{A}$$

– ou il y a une règle de la forme

$$\frac{A_1 \qquad A_n}{A}$$

telle que $A_1, \ldots, A_n$ sont dérivables

Ensemble inductif

Un ensemble inductif est le plus petit ensemble engendré par un système de règles d'inférence.

Exemple : L'ensemble de tous les termes typables en λ-calcul.

Remarque : Un ensemble structurelle est un ensemble inductif.

Preuves par Induction

Preuves par induction

- Induction sur les entiers
  - Induction mathématique
  - Induction complète
  - Équivalence
- Induction bien fondée
- Induction structurelle
- Induction sur un ensemble inductif

Induction sur les entiers I (induction mathématique)

Théorème : Soit P une propriété sur les entiers. Supposons

(IM1) $P(0)$,

(IM2) $\forall n \in \mathbb{N}.P(n) \rightarrow P(n+1)$,

alors $\forall n \in \mathbb{N}.P(n)$

Exemples

1) $\sum_{i=1}^{n} i = \frac{n * (n+1)}{2}$ 2) $n^2 = \sum_{i=1}^{n} (2i - 1)$

Mais comment prouver

1. "Tout entier naturel est décomposable en produit de nombres premiers"
2. "$fact(n) \leq 2^n$"

Induction sur les entiers II (induction complète)

Théorème : Soit P une propriété sur les entiers. Supposons

$$(IC) \qquad \forall n \in \mathbb{N}.\,((\forall k < n.P(k)) \rightarrow P(n))$$

alors $\forall n \in \mathbb{N}.P(n)$

Équivalence des deux principes

Malgré l'apparente supériorité du deuxième principe, on prouve

Théorème : Induction mathématique et complète sont équivalentes.

Principe d'induction bien fondée

Une preuve par induction bien fondée est une méthode de raisonnement qui vise à établir une propriété pour tous les éléments d'un ensemble muni d'un ordre strict bien fondé.

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

Principe d'induction :

Démontrer

1. "pour tout élément minimal $y \in \mathcal{A}$ on a $P(y)$"
2. "Si $\forall z \in \mathcal{A}$ t.q. $z \prec x$ on a $P(z)$, alors $P(x)$"

permet de conclure

"$\forall x \in \mathcal{A}.P(x)$"

Exemple

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

$$
\begin{aligned}
\text{Ackerman}(0,n) &= n+1 \\
\text{Ackerman}(m+1,0) &= \text{Ackerman}(m,1) \\
\text{Ackerman}(m+1,n+1) &= \text{Ackerman}(m,\text{Ackerman}(m+1,n))
\end{aligned}
$$

Ce principe est-il toujours bien défini ?

Théorème :

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

Théorème :

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

Principe d'induction pour les ensembles inductifs

Corollaire : Le principe d'induction est correcte pour les ensembles structurelles.

Corollaire : Le principe d'induction est correcte pour les ensembles inductifs.