Preuves par induction structurelle

MP2I - Informatique

Anthony Lick
Lycée Janson de Sailly

Introduction

Introduction

Induction

Nous avons définis précédemment un **arbre**, comme un objet mathématique précis : un ensemble muni d'une certaine **relation binaire** (de parenté).

Ceci dit, lors de l'implémentation concrète, il a fallu s'éloigner de cette définition pour **ordonner** les fils.

Une autre possibilité (peut-être plus naturelle) est de donner une **définition inductive** : un arbre est

- soit réduit à un sommet,
- soit constitué de sa racine est de la liste (ordonnée !) des sous-arbres de la racine.

Introduction

Induction

On pourrait donner des définitions du même style pour les autres types d'arbres un peu plus restreints comme les **arbres binaires**.

Ce genre de définition a le mérite d'être facilement manipulable, à la fois pour prouver des propriétés mathématiques (par exemple, un arbre binaire entier possède une feuille de plus que de nœuds internes) et transposable aisément en une implémentation.

Introduction

Mot

Dans la suite, on utilise la notion de **mot** sur un **alphabet** A (fini ou dénombrable), qui sera vu plus tard.

Ce dont on a besoin est assez intuitif : un **mot sur** A est un n-uplet d'éléments de A, qu'on préfère noter $a_1 a_2 \cdots a_n$ plutôt que $(a_1, a_2, \cdots, a_n)$.

L'entier n peut être nul : on note ε le **mot vide**.

Exemple

- $abcaab$ est un mot sur $\{a, b, c\}$.
- $(4+5) \times 2$ est un mot sur $\{+, \times, (,)\} \cup \mathbb{N}$.

Définitions inductives

Définition inductive

Définition inductive

Une **définition inductive** définit une partie d'un certain ensemble E, comme la plus petite contenant un certain **sous-ensemble de base**, et **stable** par application de certaines **règles de construction**.

Remarque

L'ensemble E ne joue pas un rôle prépondérant. Néanmoins, il est nécessaire de supposer son existence, pour éviter de se retrouver coincé par des considérations du type "ensemble de tous les ensembles", qui **n'existe pas**.

Pour l'ensemble E, on prendra souvent l'ensemble des mots sur un certain alphabet, ensemble qui a le mérite d'exister, en confondant les **objets** avec leurs **écritures syntaxiques**.

Définition inductive

Définition (Outils pour la définition inductive)

Soit E un ensemble. On appelle :

- **ensemble de base** un certain sous-ensemble $B \subset E$;
- **règle** une application partielle $r : E^n \to E$, avec $n \in \mathbb{N}^*$, appelé l'**arité** de r.

Définition inductive

La **définition inductive** d'une partie de E repose sur le théorème qui suit.

Théorème du point fixe

Théorème (Théorème du point fixe)

Soit E un ensemble. Considérons :

- $B \subset E$ un **ensemble de base** ;
- $R = \{r_j | j \in J\}$ un ensemble de **règles**, avec $r_j \ : \ E^{n_j} \to E$. Ces règles sont appelées **règles d'inférence**.

Alors il existe un plus petit ensemble $X \subset E$, tel que :

(B) : $B \subset X$;

(I) : $\forall j \in J$, $\forall (x_1, \cdots, x_{n_j}) \in X^{n_j}$ appartenant à l'ensemble de définition de r_j, on a $r_j(x_1, \cdots, x_{n_j}) \in X$.

Théorème du point fixe

Preuve

L'ensemble des sous-ensembles de E vérifiant (B) et (I) est non vide, car il contient E lui-même.

On peut donc considérer X l'intersection de tous ces sous-ensembles. Alors :

- X vérifie B ;
- si $(x_1, \cdots, x_{n_j})$ est un n_j-uplet d'éléments de X appartenant à l'ensemble de définition de r_j, alors par définition, $r_j(x_1, \cdots, x_{n_j})$ appartient à l'intersection de tous les sous-ensembles de E vérifiant (B) et (I), donc à X.

Ainsi, X est un sous-ensemble de E vérifiant (B) et (I), et c'est forcément le plus petit.

Définition (Ensemble défini par induction)

L'ensemble X donné par le théorème précédent s'appelle l'**ensemble défini par induction** avec l'ensemble de base B et les règles de R.

Notations

Dans la suite, on notera les définitions d'un ensemble inductif X comme suit :

(B) : $B \subset X$;

(I) : $(x_1, \cdots, x_n) \in E^n \Rightarrow r(x_1, \cdots, x_n) \in X$ pour chaque règle.

Exemples d'ensembles inductifs

Exemple : Entiers naturels pairs

(B) : $0 \in P$;

(I) : $x \in P \Rightarrow x + 2 \in P$.

Remarque

Comme on le voit, l'ensemble E n'a pas un rôle très important : on peut prendre $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$.

Exemples d'ensembles inductifs

Exemple : Mots de Dyck

L'ensemble $\mathcal{D}$ des **mots de Dyck** (mots bien parenthésés) sur l'alphabet $\{(,)\}$ est défini par :

(B) : $\varepsilon \in \mathcal{D}$ **(mot vide)** ;

(I) : $(x, y) \in \mathcal{D}^2 \Rightarrow (x)y \in \mathcal{D}$.

Exemples d'ensembles inductifs

Exemple : Listes chaînées

Les **listes chaînées** sur un ensemble F sont définies de la manière suivante :

(B) : la **liste vide** est une liste ;

(I) : si $x \in F$ et ℓ est une liste, alors $Cons(x, \ell)$ est une liste.

Exemples d'ensembles inductifs

Exemple : Arbres binaires

Soit F un ensemble. Les **arbres binaires** étiquetés par F sont définis ainsi :

(B) : l'**arbre vide** est un arbre binaire ;

(I) : si $x \in F$, et $\mathcal{A}_g$ et $\mathcal{A}_d$ sont deux arbres binaires, alors $Noeud(\mathcal{A}_g, x, \mathcal{A}_d)$ est un arbre binaire.

Exemples d'ensembles inductifs

Exemple : Arbres quelconques

L'ensemble des **arbres** (non étiquetés) peuvent être définis sur l'alphabet $\{(,)\} \cup \{a_0, a_1, a_2, a_3, \cdots\}$ par :

(B) : a_0 est un arbre ;

(I) : $\forall n \in \mathbb{N}^*$, pour tout n-uplet $(t_1, \cdots, t_n)$ d'arbres, $a_n(t_1, \cdots, t_n)$ est un arbre.

Remarque

Visuellement, on représente avec la règle d'inférence un arbre dont la racine possède n sous-arbres qui sont dans l'ordre $t_1, \cdots, t_n$.

Le nombre de règles étant ici infini (dénombrable), cette construction théorique est intéressante, mais pas utile pour une implémentation.

Exemples d'ensembles inductifs

Exemple : Arbres et forêts

les **règles d'inférence** sur les **arbres** et **forêts** (ensembles d'arbres) étiquetés par des éléments d'un ensemble F sont :

(B) : l'arbre vide `Vide` est un **arbre** ;

(B) : la forêt vide `[]` est une **forêt** ;

(I) : si $\mathcal{A}$ est un arbre, et $\mathcal{F}$ une forêt, alors `Cons`$(\mathcal{A}, \mathcal{F})$ est une **forêt** ;

(I) : si $\mathcal{F}$ est une forêt, et $x \in F$, alors `Noeud`$(x, \mathcal{F})$ est un **arbre**.

Exemples d'ensembles inductifs

Exemple : Expressions arithmétiques sur les entiers

On note $\mathcal{N}$ l'ensemble des mots sur l'alphabet $\{0, \cdots, 9\}$ représentant les entiers naturels (0, plus l'ensemble des mots ne commençant pas par un 0).

On peut définir $\mathcal{N}$ par induction structurelle :

(B) : $\{0, \cdots, 9\} \subset \mathcal{N}$;

(I) : pour $i \in \{0, \cdots, 9\}$, on a $r_i : n \in \mathcal{N} \setminus \{0\} \Rightarrow ni \in \mathcal{N}$.

Exemple : Expressions arithmétiques sur les entiers

L'ensemble des **expressions arithmétiques** $\mathcal{A}$ sur $\mathcal{N}$ peut être défini ainsi, sur l'alphabet $\{0, \cdots, 9, +, \times, -, /, (,)\}$:

(B) : $\mathcal{N} \subset \mathcal{A}$;

(I) : pour tout $op \in \{+, \times, -, /\}$, on a :
$(a, b) \in \mathcal{A}^2 \Rightarrow a\ op\ b \in \mathcal{A}$;

(I) : $x \in \mathcal{A} \Rightarrow (x) \in \mathcal{A}$.

Exemples d’ensembles inductifs

Exemple

Nous verrons plus tard cette année, et l’année prochaine, d’autres exemples d’ensembles pouvant être définis par **induction** : comme les **formules logiques**, ou les **expressions rationnelles**.

Preuves par induction

Preuves par induction

Théorème (Preuve par induction structurelle)

Soit $X \subset E$ un ensemble inductif, défini par l'ensemble de base B et les règles d'induction R. On considère un prédicat P sur les éléments de E. Supposons que :

- $\forall x \in B,\ P(x)$ est vrai (**initialisation**) ;
- P est **héréditaire** pour les règles de R : $\forall r \in R$, soit n l'arité de r, si $(x_1, \cdots, x_n)$ est dans l'ensemble de définition de r, et si $\forall i \in [\![1, n]\!],\ P(x_i)$ est vrai, alors $P(r(x_1, \cdots, x_n))$ est vrai.

Alors $\forall x \in X,\ P(x)$ est vrai.

Preuves par induction

Preuve

Considérons $Y = \{x \in E \mid P(x) \text{ est vrai}\}$. Alors :

- $B \subset Y$;
- Y est stable par les règles de R.

Donc, par définition de l'ensemble inductif X, $X \subset Y$.

Donc $\forall x \in X,\ P(x)$ est vrai.

Remarque

Le théorème précédent généralise la preuve par récurrence, car l'ensemble $\mathbb{N}$ peut être décrit inductivement par :

- $0 \in \mathbb{N}$;
- $x \in \mathbb{N} \Rightarrow x + 1 \in \mathbb{N}$.

Exemple

L'ensemble des **arbres binaires entiers** peut être défini inductivement sur l'alphabet $\{N; \emptyset; (\,;\,,\,;\,)\}$ par :

- $\emptyset$ est un arbre binaire entier ;
- Si $g$et d sont deux arbres binaires entiers, alors $N(g, d)$ est un arbre binaire entier.

Alors, en notant n le nombre de N dans l'écriture d'un arbre, et f le nombre de $\emptyset$, on a $f = n + 1$.

Preuve

Montrons cette propriété par induction structurelle sur un arbre a.

- Si $a = \emptyset$, alors $n = 0$ et $f = 1$: OK.
- Si $a = N(g, d)$, supposons que $f_g = n_g + 1$ et $f_d = n_d + 1$. Alors $n = n_g + n_d + 1$ et $f = f_g + f_d = n_g + 1 + n_d + 1 = n + 1$.

Ainsi, par principe d'induction structurelle, la propriété est vraie pour tout arbre a.

Induction non ambiguë et définitions de fonctions sur un ensemble inductif

Définition non ambiguë d'un ensemble inductif

Définition de fonctions

Revenons sur l'ensemble des **expressions arithmétiques** sur $\mathbb{N}$ définie précédemment.

On voit sans peine que $3-4+5$ ou $1+2\times 6$ sont des expressions arithmétiques valides.

Dans la suite, on aimerait définir par exemple l'**évaluation** d'une telle expression, dont le résultat est un élément de $\mathbb{Q}$ (ou $\mathbb{Q} \cup \{\text{Erreur !}\}$ pour gérer les divisions par zéro).

Naturellement, on voudrait une fonction f sur un ensemble inductif X en exploitant la définition **inductive** de l'ensemble.

Ainsi, il faudrait pouvoir définir $f(r(x_1, \cdots, x_n))$ en fonction des $f(x_i)$, où r est une règle d'arité n.

Définition non ambiguë d'un ensemble inductif

Problème : ambiguïté

On voit ici apparaître un problème pour les expressions arithmétiques que l'on a défini : l'expression $3 - 4 + 5$ peut être **dérivée** à partir de $3 - 4$ et 5, mais aussi à partir de 3 et $4 + 5$.

Qu'importe la valeur que l'on veut donner à $3-4+5$: celle-ci est incompatible avec les deux dérivations différentes proposées.

La définition que l'on a donné d'une expression arithmétique sur $\mathbb{N}$ est **ambiguë** : il est possible d'obtenir un élément de plusieurs façons.

Il est nécessaire de lever toute ambiguïté pour définir une fonction sur un ensemble inductif.

Définition non ambiguë d'un ensemble inductif

Définition (non ambiguïté)

Une définition d'un ensemble inductif X est dite **non ambiguë** si chaque élément de X ne peut s'obtenir que d'une seule façon à partir de B et des règles d'inférences de R.

Définition non ambiguë d'un ensemble inductif

Remarque

Cette définition est assez peu formelle, bien qu'intuitive. Il est possible de donner une définition beaucoup plus rigoureuse, donc voici l'idée.

Définition non ambiguë d'un ensemble inductif

Remarque

Dans une définition inductive d'un ensemble X, on peut voir les éléments de B comme des feuilles, et l'application d'une règle d'inférence r d'arité n comme un arbre de racine r ayant n fils.

Ainsi, notons $\mathbb{A}$ l'ensemble des arbres dont les nœuds internes sont étiquetés par les éléments de R (avec compatibilité entre l'arité de l'étiquette et le nombre de fils du nœud), et les feuilles par les éléments de B (on appelle ces arbres des **termes**).

On obtient alors une **surjection** de $\mathbb{A}$ dans X.

La définition inductive de X est **non ambiguë** si et seulement si cette surjection est **injective**.

Définition non ambiguë d'un ensemble inductif

Exemple

Parmi les définitions inductives des exemples précédents, seule celle des expressions arithmétiques est **ambiguë**. Voici une autre définition **non ambiguë** :

- $\mathcal{N} \subset \mathcal{A}$;
- pour tout $op \in \{+, \times, -, /\}$: $(a, b) \in \mathcal{A}^2 \Rightarrow (a\ op\ b) \in \mathcal{A}$.

Par exemple, les deux dérivations différentes qui donnaient $3 - 4 + 5$ précédemment donnent maintenant $((3 - 4) + 5)$ et $(3 - (4 + 5))$.

Ordre induit sur un ensemble inductif

Ordre induit

Un **ensemble inductif** défini de manière **non ambiguë** peut être muni d'une **relation d'ordre** (non totale) directement liée à la définition, comme on va le voir.

On va d'abord définir la relation entre les x_i et $r(x_1, \cdots, x_n)$ où r est une **règle d'inférence** d'arité n, et **prolonger** cette relation.

Ordre induit sur un ensemble inductif

Définition (fermeture réflexive-transitive)

Soit $\mathcal{R}$ une relation sur un ensemble E. On appelle **fermeture réflexive-transitive** de $\mathcal{R}$ la relation $\mathcal{R}'$ définie par :

$$x \,\mathcal{R}'\, y \iff \exists n \geq 0,\ \exists (x_0, x_1, \cdots, x_n) \in E^{n+1},$$
$$x = x_0 \text{ et } y = x_n \text{ et } \forall i \in [\![0, n-1]\!], x_i \,\mathcal{R}\, X_{i+1}$$

Proposition

La **fermeture réflexive-transitive** d'une relation est **réflexive** et **transitive**.

Preuve

La **transitivité** est évidente.

Pour la **réflexivité**, il suffit de prendre $n = 0$ dans la définition.

Ordre induit sur un ensemble inductif

Théorème (ordre induit)

Soit X un **ensemble inductif** défini de manière **non ambiguë**.

On introduit la relation $\prec_1$ telle que $x_i \prec_1 r(x_1, \cdots, x_n)$ pour toute **règle d'inférence** r d'arité n, et tout n-uplet $(x_1, \cdots, x_n)$.

Notons $\preceq$ la **fermeture réflexive-transitive** de $\prec_1$.

Alors $\preceq$ est une **relation d'ordre bien fondée** sur X.

Ordre induit sur un ensemble inductif

Preuve

La relation est déjà **réflexive** et **transitive**.

Montrons l'**anti-symétrie** : si $x \preceq y$ et $y \preceq x$, alors $x = y$, car sinon la non ambiguïté serait contredite.

En effet, on pourrait dériver en boucle :

$$x \rightsquigarrow y \rightsquigarrow x \rightsquigarrow y \rightsquigarrow x \cdots$$

De plus, la relation est **bien fondée** : on peut le montrer par exemple en montrant la propriété suivante par **induction structurelle** :

$P(x)$: Il n'existe pas de suite strictement décroissante pour $\prec$ commençant par x

Ordre induit sur un ensemble inductif

Preuve

$P(x)$: Il n'existe pas de suite strictement décroissante pour $\prec$ commençant par x.

- Pour $x \in B$, il n'existe pas de $y \prec x$, donc $P(x)$ est vrai.
- Soit $x = r(x_1, \cdots, x_n)$ avec r une règle d'inférence d'arité n, et supposons $P(x_i)$ pour $i \in [\![1, n]\!]$. Supposons qu'il existe une suite $(y_k)_{k \in \mathbb{N}}$ infinie strictement décroissante pour $\prec$ avec $y_0 = x$.
  - Si $y_1 = x_i$ pour un $i \in [\![1, n]\!]$, alors la suite $(y_k)_{k \in \mathbb{N}^*}$ est strictement décroissante, et commence par x_i : impossible car $P(x_i)$ est vrai par hypothèse d'induction.

Ordre induit sur un ensemble inductif

Preuve

$P(x)$: Il n'existe pas de suite strictement décroissante pour $\prec$ commençant par x.

- Sinon, comme $y_1 \prec x$, par définition de $\preceq$, $\exists i \in [\![1, n]\!]$ tel que $y_1 \prec x_i \prec x$. Ainsi, la suite définie par $y'_0 = x_i$ et $y'_k = y_k$ pour $k \in \mathbb{N}^*$ est une suite strictement décroissante commençant par x_i : impossible.

Donc, par l'absurde, $P(x)$ est vrai.

Ainsi, par principe d'induction structurelle, $\forall x \in X$, $P(x)$.

Donc $(X, \preceq)$ est **bien fondé**.

Ordre induit sur un ensemble inductif

Définition (prédécesseurs et successeurs)

Soit X un **ensemble inductif** défini de manière **non ambiguë**.
Soit $(x, y) \in X^2$.

- Si $x \prec_1 y$, on dit que :
  - x est un **prédécesseur immédiat** de y ;
  - y est le **successeur immédiat** de x.
- Si $x \prec y$, on dit que :
  - x est un **prédécesseur** de y ;
  - y est un **successeur** de x.

Fonctions sur un ensemble inductif

Fonctions sur un ensemble inductif

Il est facile de définir une fonction sur un ensemble inductif, pourvu qu'on en possède une définition **non ambiguë**.

Théorème

Soit X un ensemble défini **inductivement** de manière **non ambiguë**, avec ensemble de base B et ensemble de règles R. Alors, la donnée de :

- valeurs de $f(x)$ pour tout $x \in B$;
- valeurs de $f(r(x_1, \cdots, x_n))$ en fonction des x_i et des $f(x_i)$ pour toute règle r d'arité n ;

permet de définir une fonction f sur X.

Fonctions sur un ensemble inductif

Preuve

Montrons la propriété suivante par **induction structurelle** :

$P(x)$: les hypothèses du théorème définissent la valeur $f(x)$ de manière **unique**.

- C'est vrai pour les éléments $x \in B$.
- Tout autre élément $x \in X$ s'obtient de manière unique sous la forme $x = r(x_1, \cdots, x_n)$ (car X est défini de manière **non ambiguë**).
  De plus, par hypothèse d'induction, les $f(x_i)$ sont biens définis de manière unique, donc $f(x)$ est bien défini de manière unique.

Fonctions sur un ensemble inductif

Exemple

On peut définir la hauteur h d'un arbre binaire de la façon suivante :

- l'arbre vide a pour hauteur -1 ;
- $h(Noeud(g, x, d)) = 1 + \max(h(g), h(d))$.

Analyse d'une fonction récursive

Analyse d'une fonction récursive

Considérons un ensemble inductif X défini de manière **non ambigüe**.

Une fonction récursive sur X utilisant la structure à la manière du théorème précédent est facile à analyser :

- sa **terminaison** est évidente car l'**ordre induit** sur X est **bien fondé** ;
- sa **correction** se montre par induction ;
- sa **complexité** s'analyse de la même manière qu'une fonction récursive quelconque.