Aspects Fondamentaux du Calcul: Induction

Paysage syntaxique: récursion - induction

1. des propriétés importantes et nécessaires
2. définitions inductives et par récurrence: construire des objets finis, à partir d'autres, selon des règles
3. définitions inductives aussi les objets infinis définis par des définitions récursives
4. définitions récursives: dans les structures de données, et programmes récursifs
5. preuves de programmes récursifs par récurrence
6. preuves de terminaison de programme itératifs par récurrence

Paysage syntaxique : récursion - induction

Premier principe d'induction

- souvent appelé principe de récurrence mathématique
- mode de raisonnement utile
- preuve par induction ou preuve par récurrence pour les preuves utilisant ce principe

Théorème Soit $P(n)$ un prédicat (propriété) dépendant de l'entier n. Si les 2 propriétés suivantes sont vérifiées:

- (B) $P(0)$ est vrai
- (I) $\forall n \in \mathbb{N}, (P(n) \Rightarrow P(n+1))$

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

Remarque

- (B) étape de base de la récurrence (ou induction)
- (I) étape inductive

Premier principe d'induction: démonstration

par l'absurde

- on considère: $X = \{k \in \mathbb{N} | P(k)\ est\ faux\}$
- si X non vide, alors il admet un plus petit élément n
- de (B), $n \neq 0$
- donc $n - 1$ entier et $n - 1 \notin X$ (car n le plus petit de X)
- $n - 1 \notin X$ donc $P(n - 1)$ est vrai
- de (I) et $P(n - 1)$ est vrai, on a $P(n)$ est vrai
- ce qui est en contradiction avec $n \in X$
- donc X vide, et preuve du théorème

Premier principe d'induction: exemple

Calculer $S_n = 1 + 2 + \ldots + n$

- on remarque: $2.S_1 = 2 = 1 \times 2$, $2.S_2 = 2 + 4 = 2 \times 3$, $2.S_3 = 2 + 4 + 6 = 3 \times 4$
- on conjecture: $\forall n > 0, 2.S_n = n.(n+1)$
- on le montre par récurrence
- soit $P(n)$ la propriété "$2.S_n = n.(n+1)$"
- on vérifie:
  - (B) $2.S_1 = 1 \times 2$
  - (I) Soit $n \geq 1$, supposons $P(n)$. On a:

    $$2.S_{n+1} = 2.S_n + 2.(n+1) = n.(n+1) + 2.(n+1) = (n+1)(n+2)$$

  - donc $P(n+1)$ est vraie.
- on peut en conclure: $\forall n \geq 1, P(n)$ et donc $\forall n > 0, 2.S_n = n.(n+1)$

Deuxieme principe d'induction

- premier principe: $P(n+1)$ dépend de $P(n)$
- deuxieme principe: plus complexe, $P(n+1)$ dépend de par ex. $P(0)$, $P(1)$, ..., $P(n)$
- les 2 principes sont équivalents
  (seul le 2-ème se généralise à des ensembles ordonnés plus généraux)

Deuxieme principe d'induction

Théorème Soit $P(n)$ un prédicat (propriété) dépendant de l'entier n. Si la propriété suivante est vérifiée:

- (I') $\forall n \in \mathbb{N}, ((\forall k < n, P(k)) \Rightarrow P(n))$

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

Remarques:

- étape de base cachée dans (I'):
  - il est démontré pour $n = 0$ que $(\forall k < 0, P(k)) \Rightarrow P(0)$
  - or $\forall k < 0, P(k)$ est toujours vrai (pas de tel k dans $\mathbb{N}$)
  - donc si (I') alors $P(0)$
- plus généralement: $(\forall x \in \emptyset, P(x))$ est toujours vrai.
- possibilité de commencer à n_0:
  (I_{n_0}') $\forall n \geq n_0, ((\forall k \in \{n_0, \ldots, n-1\}, P(k)) \Rightarrow P(n))$
  pour déduire: $\forall n \geq n_0,\ P(n)$

Deuxieme principe d'induction: exemple

Montrons que tout entier $n \geq 2$ est décomposable en un produit de nombres premiers.

- Soit $P(n)$ la propriété "n est décomposable en un produit de nombres premiers"
- il suffit de vérifier (I_2')
- Soit $n \geq 2$, supposons $\forall k \in \{2, \ldots, n-1\}, P(k)$
- 2 cas:
  - n premier, alors n décomposable en produit de nombres premiers (1 seul nombre est considéré comme un produit)
  - n non premier, alors $n = a.b$ avec a et b entiers entre 2 et $n-1$
    Par hypothèse, $P(a)$ et $P(b)$ sont vrais.
    On en déduit que n est aussi décomposable en le produit des décompositions de a et b.

Ensembles définis inductivement

- ex: définition de parties d'ensemble (e.g., structures de données)
- la définition inductive d'une partie X d'un ensemble consiste en:
  - la donnée explicite de certains éléments de X
  - et de moyens pour construire de nouveaux éléments de X a partir d'éléments déjà connus
- Forme générique:
  - (B) certains éléments de X sont donnés explicitement (base de la def.)
  - (I) les autres éléments de X sont définis en fonction d'éléments appartenant déjà à X (étape inductive)

Ensembles définis inductivement

Definition

Soit E un ensemble. Une définition inductive d'une partie X de E consiste en la donnée:

- d'un sous-ensemble B de E,
- d'un ensemble K d'opérations $\phi : E^{a(\phi)} \to E$, où $a(\phi) \in \mathbb{N}$ est l'arité de ϕ

X est défini comme étant le plus petit ensemble vérifiant les assertions (B) et (I) suivantes:

- (B) $B \subseteq X$,
- (I) $\forall \phi \in K, \forall x_1, \ldots, x_{a(\phi)} \in X, \phi(x_1, \ldots, x_{a(\phi)}) \in X$.

L'ensembe défini est donc:

$$X = \bigcap_{Y \in \mathcal{F}} Y \text{ } avec \text{ } \mathcal{F} = \{Y \subseteq E | B \subseteq Y, \text{ } et \text{ } Y \text{ } verifie \text{ } (I)\}$$

Ensembles définis inductivement

On notera les définitons inductives sous la forme:

- (B) $x \in X$ $(\forall X \in B)$,
- (I) $x_1, \ldots, x_{a(\phi)} \in X \;\Rightarrow\; \phi(x_1, \ldots, x_{a(\phi)}) \in X$ $(\forall \phi \in K)$.

Pourquoi $X = \bigcap_{Y \in \mathcal{F}} Y$?
car plusieurs ensembles peuvent vérifier les conditions (B) et (I)

Exemple:

- (B) $0 \in P$
- (I) $n \in P \;\Rightarrow\; n + 2 \in P$

Une infinité de parties de $\mathbb{N}$ vérifient (B) et (I): $\mathbb{N}$, $\mathbb{N} \setminus \{1\}$, $\mathbb{N} \setminus \{1, 3\}$, $\mathbb{N} \setminus \{1, 3, 5\}$, ...
or P est l'ensemble des entiers pairs
par contre, $\mathbb{N} \setminus \{3\}$ ne vérifie pas (I)

Ensembles définis inductivement: exemples

- la partie X de $\mathbb{N}$ définie inductivement par:
  - (B) $0 \in X$
  - (I) $n \in X \;\Rightarrow\; n+1 \in X$

  est $\mathbb{N}$.
  (B) et (I) constituent une définition inductive de $\mathbb{N}$
- la partie X du monoide libre $A^\star$ définie inductivement par:
  - (B) $\epsilon \in X$
  - (I) $u \in X \;\Rightarrow\; \forall a \in A, u.a \in X$

  est $A^\star$.
  (B) et (I) constituent une définition inductive de $A^\star$
- Soit $A = \{(,)\}$. D, le langage de Dyck (parenthésages bien formés) est défini inductivement par:
  - (B) $\epsilon \in D$
  - (I) si x et y sont dans D, alors (x) et $x.y$ sont aussi dans D.
- les fonctions récursives primitives???

Ensembles définis inductivement

Théorème: Si X est défini par les conditions (B) et (I), tout élément de X peut s'obtenir à partir de la base en appliquant un nombre fini d'étapes inductives.

Preuves par induction (ou induction structurelle)

Généralisation du principe de récurrence sur les entiers
Proposition: Soit X un ensemble défini inductivement, et soit $P(x)$ un prédicat exprimant une propriété de $x \in X$. Si les conditions suivantes sont vérifiées:

- (B") $P(x)$ est vrai pour chaque $x \in B$
- (I") $(P(x_1), \ldots, P(x_{a(\phi)})) \Rightarrow P(\phi(x_1, \ldots, x_{a(\phi)}))$

alors $P(x)$ est vrai pour tout x dans X.
Vérifier (B") et (I") constitue une preuve par induction de la propriété P sur X.

Preuves par induction: exemple

Montrons que tout mot du langage D de Dyck a autant de parenthèses ouvrantes que fermantes.

- Pour $x \in D$, notons:
  - $g(x) = |x|_($
  - $d(x) = |x|_)$
- Soit $P(x)$ la propriété $g(x) = d(x)$
- par induction:
  - (B) l'unique élément de base est ϵ qui satisfait P car $g(\epsilon) = d(\epsilon) = 0$
  - (I) Soient $x, y \in D$ tq $g(x) = d(x)$ et $g(y) = d(y)$
  - par induction:
    - Soit par ex. $z = x.y$
      On a $d(z) = d(x) + d(y) = g(x) + g(y) = g(z)$, d'où $P(z)$ vérifié.
    - le cas $z = (x)$ se vérifie aussi car: $d(z) = d(x) + 1 = g(x) + 1 = g(z)$
  - on en déduit que $\forall x \in D, g(x) = d(x)$

Définition non ambiguë

Definition

Définition intuitive: Une définition inductive d'un ensemble X est dite non-ambiguë s'il n'existe qu'une seule façon de construire un élément x de X.

Exemple: la définition suivante de $\mathbb{N}^2$ est ambiguë

- (B) $(0,0) \in \mathbb{N}^2$
- (I1) $(n,m) \in \mathbb{N}^2 \ \Rightarrow \ (n+1,m) \in \mathbb{N}^2$
- (I2) $(n,m) \in \mathbb{N}^2 \ \Rightarrow \ (n,m+1) \in \mathbb{N}^2$

car (par ex.) $(1,1)$ s'obtient à partir de $(0,0)$ en utilisant la règle (I1) puis (I2) **ou** (I2) puis (I1)

Fonctions définies inductivement

- Pour définir une fonction sur un ensemble défini inductivement de façon non-ambiguë
- Intuitivement:
  - on définit la fonction directement sur les éléments de la base
  - inductivement sur les nouveaux éléments construits à partir d'éléments déjà connus

Fonctions définies inductivement

Definition

Soit $X \subseteq E$ un ensemble défini inductivement de façon non-ambiguë , et soit F un ensemble quelconque.
La définition inductive d'une application ψ de X dans F consiste en:

- la donnée $\psi(x) \in F$ pour chaque x de B,
- l'expression de $\psi(\phi(x_1, \dots, x_{a(\phi)}))$ à partir des $x_1, \dots, x_{a(\phi)}$ et des $\psi(x_1), \dots, \psi(x_{a(\phi)})$ pour chaque ϕ de K.
  On écrira:

$$\psi(\phi(x_1, \dots, x_{a(\phi)})) = \psi_\phi(x_1, \dots, x_{a(\phi)}, \psi(x_1), \dots, \psi(x_{a(\phi)}))$$

où ψ_ϕ est une application de $E^{a(\phi)} \times F^{a(\phi)}$ dans F.

Fonctions définies inductivement: exemples

- la fonction factorielle de $\mathbb{N}$ dans $\mathbb{N}$ se définit inductivement par:
  - (B) $Fact(0) = 1$
  - (I) $Fact(n+1) = (n+1) \times Fact(n)$

  (utilise la définition inductive de $\mathbb{N}$ avec $n \in X \;\Rightarrow\; n+1 \in X$)