Mathématiques pour l'informatique
Induction (fin)

Induction

Exercice 1. Quel est le sous-ensemble de $\boldsymbol{R}$ défini par

$$\begin{array}{lll} E & ::= & 0 \\ & \mid & x \qquad x \in]0,1[\\ & \mid & E+1 \end{array}$$

?

Prouver que cette définition n'est pas ambiguë.

Exercice 2. Dans l'ensemble E précédent, définir par induction structurelle la partie entière inférieure et la partie entière supérieure.

Pour la suite, nous allons considérer une suite $(u_n)_{n\in\boldsymbol{N}}$ définie par

- $u_0 = 0$
- $u_1 = 1$
- $\forall n \geqslant 1, u_{n+1} = a \cdot u_{\lfloor n/2 \rfloor} + b \cdot u_{\lceil n/2 \rceil} + f(n)$

où f est une application croissante de $\boldsymbol{N}^*$ dans $\boldsymbol{N}$

Exercice 3. Prouver que u est croissante.

Exercice 4. Prouver que, si $f(n) = \mathcal{O}(n^\alpha)$, alors $u_n = \mathcal{O}(n^\alpha \cdot \log_2(n))$.

Exercice 5. * Définir *strictement par induction* la soustraction de deux entiers de Peano. Implanter cela en OCaml. Prouver que la soustraction d'un entier à lui-même vaut toujours Zero.

Logique

Exercice 6. * Définir l'opérateur Xor (« ou exclusif ») à partir des opérateurs $\wedge$ et $\neg$.

Correction du TD 8

Exercice 2. Définir par induction l'ensemble AVL des arbres binaires équilibrés.

Intuitivement, un arbre binaire équilibré est soit une feuille, soit un nœud composé de deux arbres binaires équilibrés presque de même hauteur. Cela peut se formaliser d'au moins deux manières.

Définition non-ambiguë Considérons la suite d'ensembles $(\mathrm{AVL}_n)_{n\in\boldsymbol{N}}$ définie par

- $\mathrm{AVL}_0 = \{\mathrm{Feuille}(i) \,/\, i \in \boldsymbol{N}\}$, l'ensemble des arbres réduits à une feuille
- $\mathrm{AVL}_1 = \mathrm{Noeud}(\mathrm{AVL}_0, \mathrm{AVL}_0)$, l'ensemble des arbres équilibrés de hauteur 1.
- $\forall n \in \boldsymbol{N}$, $\mathrm{AVL}_{n+2} = \mathrm{Noeud}(\mathrm{AVL}_{n+1}, \mathrm{AVL}_{n+1}) \cup \mathrm{Noeud}(\mathrm{AVL}_{n+1}, \mathrm{AVL}_n) \cup \mathrm{Noeud}(\mathrm{AVL}_n, \mathrm{AVL}_{n+1})$, l'ensemble des arbres équilibrés de hauteur $n+2$.

Alors, l'ensemble des arbres équilibrés AVL se définit comme $\cup_{n\in\boldsymbol{N}} \{\mathrm{AVL}_n\}$.

Définition ambiguë Pour ce qui suit, nous allons employer une valeur spéciale Mauvais, qui représentera les arbres mal formés. Nous allons définir par induction structurelle BVL, ensemble qui contiendra exactement tous les arbres binaires équilibrés et Mauvais, par

$$\begin{array}{lll} \mathrm{BVL} & ::= & \mathrm{Feuille}(i) \qquad i \in \boldsymbol{N} \\ & \mid & \mathrm{Mauvais} \\ & \mid & \mathrm{combiner}(\mathrm{BVL}, \mathrm{BVL}) \end{array}$$

où la fonction combiner est définie par

$$\begin{array}{llll} \text{combiner} : & \text{BVL} & \longrightarrow & \text{BVL} \\ & a, b & \longmapsto & \text{Noeud}(a, b) \quad \text{si } a \neq \text{Mauvais}, b \neq \text{Mauvais et } |h(a) - h(b)| \leqslant 1 \\ & & & \text{Mauvais} \quad \text{sinon} \end{array}$$

Alors, l'ensemble des arbres binaires équilibrés AVL$'$ se définit comme BVL$\backslash\{$Mauvais$\}$.

Resterait à prouver que ces deux définitions sont équivalentes.

Exercice 4. Considérons le sous-ensemble E de $\boldsymbol{N}^2$ défini par induction comme

$$\begin{array}{lll} E & ::= & (0,0) \\ & | & (0,1) \\ & | & f(E, E) \\ & | & g(E) \end{array}$$

où

- $f: \boldsymbol{N}^2 \times \boldsymbol{N}^2 \longrightarrow \boldsymbol{N}^2$ est définie par $\forall (m, n) \in \boldsymbol{N}^2, \forall (m', n') \in \boldsymbol{N}^2, f((m, n), (m', n')) = (m + m', n + n')$;
- $g: \boldsymbol{N} \longrightarrow \boldsymbol{N}$ est définie par $\forall (m, n) \in \boldsymbol{N}^2, g(m, n) = (n, m)$.

Prouver que $E = \boldsymbol{N}^2$. Prouver que cette définition est ambiguë.

Lemme 1. $\forall k \in \boldsymbol{N}^*, (0, k) \in E$.

Prouvons ceci par récurrence sur k que .

Initialisation. Par définition de E, $(0, 1) \in E$.

Héritage. Soit k tel que $(0, k) \in E$. Nous savons que $(0, 1) \in E$. Par conséquent, par définition de E, nous avons aussi $f((0, 1), (0, k)) \in E$. Or $f((0, 1), (0, k)) = (0, k + 1)$. Nous en déduisons donc que $(0, k+1) \in E$.

Nous venons de prouver par récurrence sur k que $\forall k \in \boldsymbol{N}^*, (0, k) \in E$.

Preuve

Commençons par prouver que $E = \boldsymbol{N}^2$. Par définition de E, nous avons $E \subseteq \boldsymbol{N}^2$. Si nous arrivons à prouver que $\boldsymbol{N}^2 \subseteq E$, nous pourrons en déduire l'égalité. Pour ce faire, considérons tous les couples (m, n) possibles dans $\boldsymbol{N}^2$ et prouvons qu'ils apparaissent dans E.

- Si $m = 0$ et $n = 0$, nous avons $(m, n) = (0, 0)$ et, par définition de E, $(0, 0) \in E$. Ce qui prouve le cas.
- Si $m = 0$ et $n \neq 0$, nous avons $(m, n) = (0, n)$. D'après le lemme, comme $n \in \boldsymbol{N}^*$, nous en déduisons que $(0, n) \in E$. Ce qui prouve le cas.
- Si $m \neq 0$ et $n = 0$, nous avons $(m, n) = (m, 0)$. D'après le lemme, comme $m \in \boldsymbol{N}^*$, nous avons $(0, m) \in E$. Par définition de E, nous avons donc $g(0, m) \in E$, c'est-à-dire $(m, 0) \in E$. Ce qui prouve le cas.
- Si $m \neq 0$ et $n \neq 0$, nous savons déjà que $(m, 0) \in E$ et $(0, n) \in E$. Par définition de E, nous avons donc $f((m, 0), (0, n)) \in E$, c'est-à-dire $(m, n) \in E$. Ce qui prouve le cas.

Nous avons donc prouvé que $\forall (m, n) \in \boldsymbol{N}^2, (m, n) \in E$, c'est-à-dire $\boldsymbol{N}^2 \subseteq E$.

De la double inclusion, nous déduisons que $E = \boldsymbol{N}^2$.

Pour prouver que la définition de E est ambiguë, contentons-nous de remarquer que $g(0, 0) = (0, 0)$. Il existe donc au moins deux manières d'atteindre $(0, 0)$ dans E.

Exercice 5. Considérons le sous-ensemble E de $\boldsymbol{N} \times \boldsymbol{N}^*$ défini par induction à l'aide des bases $\mathcal{B} = \{(m, n) \in \boldsymbol{N} \times \boldsymbol{N}^* / m < n\}$ et des opérateurs d'induction $\mathcal{I} = \{(m, n) \longmapsto (m + n, n)\}$.

Montrer que $E = \boldsymbol{N} \times \boldsymbol{N}^*$.

Montrer que cette définition n'est pas ambiguë !

Lemme 2. *Soient n et p deux entiers naturels tels que $n \neq 0$ et $0 \leqslant p < n$. Alors, pour tout entier naturel k, le couple $(k \cdot n + p, n)$ appartient à E.*

Nous prouvons ceci par récurrence sur k.

Initialisation. Si $k=0$, nous avons un couple (p,n) avec $0 \leqslant p < n$ et $n \neq 0$. Par définition, de $\mathcal{B}$, ce couple est dans $\mathcal{B}$.

Héritage. Soit k tel que $(k \cdot n + p, n) \in E$. Alors, par définition de E, $(k \cdot n + p + n, n) \in E$, c'est-à-dire $((k+1) \cdot n + p, n) \in E$, ce qui prouve le cas.

Nous venons de prouver par récurrence sur k que pour tout entier naturel k, le couple $(k \cdot n + p, n)$ appartient à E.

Preuve Comme précédemment, commençons par remarquer que $E \subseteq \boldsymbol{N} \times \boldsymbol{N}^*$. Soit maintenant (m,n) dans $\boldsymbol{N} \times \boldsymbol{N}^*$. Prouvons que $(m,n) \in E$.

- Si $m < n$, nous avons $(m,n) \in \mathcal{B}$ donc $(m,n) \in E$.
- Si $m \geqslant n$, notons p le reste de la division euclidienne de m par n. Par définition, nous avons $0 \leqslant p < n$ et il existe $k \in \boldsymbol{N}$ tel que $m = k \cdot n + p$. D'après le lemme, nous en déduisons que $(m,n) \in E$.

Nous avons donc prouvé que, pour tout (m,n) de $\boldsymbol{N} \times \boldsymbol{N}^*$, nous avons $(m,n) \in E$. En d'autres termes, nous avons $\boldsymbol{N} \times \boldsymbol{N}^* \subseteq E$. Comme $E \subseteq \boldsymbol{N} \times \boldsymbol{N}^*$, nous pouvons conclure que $E = \boldsymbol{N} \times \boldsymbol{N}^*$.

Pour l'ambiguïté, procédons par l'absurde. Considérons donc un élément (m, n) de E ayant deux écritures différentes.

1. soit (m,n) apparaît deux fois dans $\mathcal{B}$ sous deux écritures distinctes
2. soit (m, n) apparaît dans $\mathcal{B}$ et il existe aussi une manière d'obtenir (m, n) à partir d'un opérateur d'induction et d'éléments de E
3. soit il existe deux manières d'obtenir (m, n) à partir d'opérateurs d'induction et d'éléments de E qui ne disposent que d'une seule écriture
4. soit (m, n) peut s'obtenir à partir d'opérateurs d'induction et d'un élément de E disposant d'au moins deux écritures.

Traitons successivement ces quatre cas.

1. Si (m,n) apparaît deux fois dans $\mathcal{B}$ sous deux écritures distinctes, nous avons $(m,n) = (a, b)$ où $a \neq m$ ou $b \neq n$, ce qui est absurde. Le cas ne peut donc se produire.
2. Si (m, n) apparaît dans $\mathcal{B}$ et s'il existe aussi une manière d'obtenir (m, n) à partir d'un opérateur d'induction et d'éléments de E, notons donc $(m, n) = (m' + n', n')$, où (m', n') appartient à E. Comme $(m,n) = (m' + n', n')$, nous déduisons immédiatement que $n = n'$. Or, comme (m, n) apparaît dans $\mathcal{B}$, nous avons $m < n$. Comme (m', n') appartient à E, nous avons $m' \geqslant 0$ donc $m' + n' \geqslant n$, c'est-à-dire $m \geqslant n$, ce qui est absurde.

   Nous en déduisons que le cas ne peut se produire.
3. S'il existe deux manières d'obtenir (m, n) à partir d'opérateurs d'induction et d'éléments de E ne disposant que d'une seule écriture, notons $(m, n) = (m' + n', n')$ et $(m, n) = (m'' + n'', n'')$, où (m', n') et (m'', n'') sont deux éléments distincts de E. Or, à partir des égalités précédentes, nous obtenons immédiatement $m'' = m'$ et $n'' = n'$, ce qui est absurde.

   Nous en déduisons que le cas ne peut se produire.
4. Si (m, n) peut s'obtenir à partir d'opérateurs d'induction et d'un élément de E disposant d'au moins deux écritures, alors il existe au moins un élément de E disposant d'au moins deux écritures et que l'on peut obtenir en appliquant moins d'opérateurs d'induction. Comme tout élément de E peut s'obtenir en appliquant un nombre fini d'opérateurs d'induction, en appliquant suffisamment de fois ce raisonnement, nous pouvons nous ramener au cas 3. Comme le cas 3 ne peut se produire, nous en déduisons que le cas 4 non plus.

Note J'ai légèrement simplifié la gestion des cas 3 et 4. Normalement, en partant du fait que le nombre d'opérateurs d'induction appliqués pour obtenir un élément de E est fini et que $\boldsymbol{N}$ (l'ensemble contenant le nombre d'opérateurs d'induction) est un ensemble bien ordonné, on commence par se ramener à un cas minimal, c'est-à-dire à un cas qui s'obtient sans faire appel à des éléments de E disposant de deux écritures. En d'autres termes, on ramène systématiquement le cas 4 au cas 3.