Raisonnement par récurrence

F. Alexandre

École Supérieure d'Informatique et Applications de Lorraine

September 23, 2008

Problème : soit E un ensemble et P une propriété définie sur E, on considère la formule :

$$(\forall x \in E)\ (P(x)) \qquad (A)$$

Signification : la propriété P est vraie pour tous les éléments de E.

Pour établir des principes (de récurrence ou d'induction) permettant de démontrer de telles assertions (A), il est nécessaire que les ensembles E sur lesquels portent P vérifient certaines propriétés, (ensembles définis inductivement, ensembles bien fondés,...).

Definition (Principe de récurrence sur $\mathbb{N}$ à un cran)

Soit P une propriété définie sur l'ensemble des entiers naturels $\mathbb{N}$, le principe de récurrence à un cran s'exprime par la formule logique suivante :

$$[P(0) \text{ } et \text{ } (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))] \Rightarrow (\forall n \in \mathbb{N})(P(n))$$

Exemple de mise en œuvre

Démonstration de $(\forall n \in \mathbb{N})$ $(7^n - 1$ *est divisible par* $6)$.
On pose $P(n) \equiv\ 7^n - 1$ *est divisible par* 6

1. On démontre $P(0)$ le cas de base i.e. $7^O - 1 = 1 - 1 = 0$, 0 est divisible par 6.
2. On démontre le pas de récurrence $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$.
   On suppose $P(n)$ (c'est l'hypothèse de récurrence H.R.), et à partir de H.R. on démontre $P(n+1)$.
   H.R. : $7^n - 1$ *est divisible par* 6 i.e. $(\exists k \in \mathbb{N})(7^n - 1 \ = 6k)$
   calculons $7^{n+1} - 1$
   $$\begin{aligned} 7^{n+1} - 1 &= 7^{n+1} - 7 + 7 - 1 \\ &= 7(7^n - 1) + 6 \\ &= 7 \times 6k + 6 \quad (\textit{par application de } H.R.) \\ &= 6(7k+1) \end{aligned}$$
   d'où $7^{n+1} - 1$ est multiple de 6, i.e. $P(n+1)$

Conclusion : $(\forall n \in \mathbb{N})(P(n))$, c'est-à-dire que pour tout entier naturel n, $7^n - 1$ est divisible par 6.

Remarque

On peut commencer la récurrence à un entier quelconque $a \in \mathbb{N}$, le principe s'énonce ainsi :

$$[P(a) \textit{ et } (\forall n \in \mathbb{N} \setminus [0, a[)\ (P(n) \Rightarrow P(n+1))] \Rightarrow (\forall n \in \mathbb{N} \setminus [0, a[)\ (P(n))$$

Definition (Récurrence à k crans sur $\mathbb{N}$)

Soit P une propriété définie sur $\mathbb{N}$, le principe de récurrence à k crans s'exprime par la formule logique suivante :

$$\begin{array}{l} [(P(0) \textit{ et } P(1) \ \ldots \textit{et } P(k-1)) \textit{ et} \\ (\forall n \in \mathbb{N})\ (P(n) \textit{ et } P(n+1) \textit{ et } \ \ldots \ \textit{et } P(n+k-1) \Rightarrow P(n+k))] \\ \Rightarrow (\forall n \in \mathbb{N})(P(n)) \end{array}$$

Remarques

1. Le cas de base est constitué des k propositions $P(0)$, $P(1)$, ... et $P(k-1)$ à vérifier.
2. $(\forall n \in \mathbb{N})\ (P(n) \textit{ et } P(n+1) \textit{ et } \ \ldots \ \textit{et } P(n+k-1) \Rightarrow P(n+k))$ est le pas de récurrence.
   L'hypothèse de récurrence est constituée des k propositions $P(n)$, ..., $P(n+k-1)$.
3. On peut définir des variantes de ce principe qui commencent pour des entiers strictement supérieurs à 0.
4. Pour $k = 1$, on retrouve le principe précédent (à 1 cran).

Definition (Ensemble défini inductivement)

Un ensemble E défini inductivement est la donnée d'un ensemble B et d'un ensemble $\mathcal{O}p$ d'opérations tels que :

- $B \subseteq E$.
- pour toute opération ϕ de $\mathcal{O}p$, pour tout $x_1, \ldots x_n \in E$: $\phi(x_1, \ldots, x_n) \in E$.
- E est le plus petit ensemble (au sens de l'inclusion des ensembles) vérifiant les deux propriétés précédentes.

Remarques

- L'ensemble B s'appelle la base.
- Une opération de $\mathcal{O}p$ d'arité n est une application de $\underbrace{E \times \ldots \times E}_{n \text{ fois}} \rightarrow E$, mais peut aussi faire intervenir d'autres ensembles.
- La troisième condition de la définition signifie que les éléments de l'ensemble E sont soit des éléments de la base B, soit des éléments obtenus en appliquant un nombre fini de fois les opérations de $\mathcal{O}p$ aux éléments de la base B.

Ensemble défini inductivement (exemple)

Example (Arbres binaires)

AB l'ensemble des arbres binaires étiquetés par des éléments de $\mathbb{N}$ est défini inductivement par :

- la base $B = \{avide\}$ (*avide* est appelé l'arbre vide).
- L'ensemble des opérations comporte un seul élément défini par :
  $(\forall e \in \mathbb{N})(\forall g \in AB)(\forall d \in AB) \ < g, \ e, \ d > \in AB$

Exemples d'arbres binaires étiquetés par $\mathbb{N}$:
$a_1 = avide$, $a_2 =< avide, \ 4, \ avide >$, $a_3 =<< avide, \ 4, \ avide >, \ 5, \ avide >$,
$a_4 =<< avide, \ 4, \ avide >, \ 5, \ < avide, \ 1, \ avide >>$,
$a_5 =<< avide, \ 3, \ < avide, \ 2, \ avide >>, \ 5, \ < avide, \ 1, \ avide >>$, sont des éléments de AB (dessiner ces arbres).

Example (Listes)

Liste, l'ensemble des listes d'éléments de $\mathbb{N}$ est définie inductivement par :

- la base $B = \{nil\}$ (*nil* est appelé la liste vide).
- L'ensemble des opérations comporte la seule opération :: définie comme suit :
  $(\forall e \in \mathbb{N})(\forall l \in Liste) \ e :: l \in Liste$

nil, $4 :: nil$, $6 :: (2 :: nil)$,, $0 :: (5 :: (1 :: nil))$ sont des listes d'entiers.

Example (Entiers naturels $\mathbb{N}$)

Tout entier naturel n peut être obtenu à partir de 0 par un nombre fini (n) d'additions successives de 1, ainsi :
$2 = 0 + 1 + 1$
$6 = 0 + 1 + 1 + 1 + 1 + 1 + 1$
$12 = 0 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$
L'ensemble $\mathbb{N}$ est défini inductivement par :

- 0 est l'élément formant la base.
- L'opération $suc\ :\ x \mapsto x + 1$ est la seule opération de $\mathcal{O}p$.

Exemples :
$2 = suc(suc(0))$
$6 = suc(suc(suc(suc(suc(suc(0))))))$
$12 = suc(suc(suc(suc(suc(suc(suc(suc(suc(suc(suc(suc(0))))))))))))$

Example (Entiers naturels impairs)

Les entiers naturels impairs $\mathbb{I}$ peuvent être définis inductivement par :

- l'ensemble de base est $\{1\}$
- l'opération

$$plus2 : \begin{array}{ccc} \mathbb{I} & \longrightarrow & \mathbb{I} \\ x & \longmapsto & x + 2 \end{array}$$

Definition (Principe d'induction)

Soit E un ensemble défini inductivement par

- une base B.
- un ensemble d'opération $\mathcal{O}p$.

soit P une propriété définie sur E, le principe d'induction sur E s'exprime de la façon suivante :

$$\left[\begin{array}{l}(\forall x \in B)\ P(x)\ \textit{et} \\ (\forall \phi \in \mathcal{O}p)\ [(\forall x_1 \in E) \ldots (\forall x_n \in E)\ (P(x_1)\ \textit{et} \ldots \textit{et}\ P(x_n) \Rightarrow P(\phi(x_1, \ldots, x_n)))]\end{array}\right] \Rightarrow (\forall x \in E)\ (P(x))$$

Remarques

- Cas de base : la propriété doit être prouvée pour tous les éléments de la base B.
- Pas d'induction : la propriété doit être prouvée pour tout élément construit à partir d'une opération sous l'hypothèse que la propriété est vraie pour tous les éléments utilisés dans la construction. Ce pas d'induction est à démontrer pour toute opération de l'ensemble d'opérations $\mathcal{O}p$.
- La conclusion signifie que la propriété est vraie pour tout élément de l'ensemble.

Definition (Principe d'induction sur les arbres binaires)

Soit l'ensemble AB des arbres binaires défini inductivement par :

- la base $\{avide\}$,
- l'opération

$$\begin{array}{rccc} <\_>: & AB \times \mathbb{N} \times AB & \rightarrow & AB \\ & (g,\ e,\ d) & \mapsto & <g,\ e,\ d> \end{array}$$

Soit P une propriété définie sur AB, le principe d'induction structurelle sur l'ensemble AB s'exprime de la façon suivante :

$$[P(avide) \textit{ et } (\forall g \in AB)(\forall d \in AB)(\forall e \in \mathbb{N})(P(g) \textit{ et } P(d) \ \Rightarrow P(<g, e, d>))] \Rightarrow (\forall a \in AB)(P(a))$$

Definition (Principe d'induction sur les listes)

L'ensemble *Liste* des listes d'entiers est défini inductivement par :

- la base $\{nil\}$,
- l'opération

$$\begin{array}{lllll} :: & : & \mathbb{N} \times Liste & \longrightarrow & Liste \\ & & (e,\ l) & \longmapsto & e :: l \end{array}$$

Soit P une propriété définie sur AB, le principe d'induction structurelle sur l'ensemble AB s'exprime de la façon suivante :

$$[P(nil)\ et\ (\forall e \in \mathbb{N})(\forall l' \in Liste)(P(l') \ \Rightarrow P(e :: l'))] \Rightarrow (\forall l \in Liste)\ (P(l))$$

Definition (Fonction récursive)

Soient E un ensemble défini inductivement à partir de B, $\mathcal{O}p$ et F un ensemble quelconque, la définition d'une fonction $f : E \longrightarrow F$ récursive consiste à donner :

- pour tout x de B des valeurs $f(x) \in F$
- pour toute règle ϕ de $\mathcal{O}p$ des valeurs de $f(\phi(x_1, \ldots, x_n))$ pouvant dépendre de $f(x_1), \ldots, f(x_n)$ et $x_1, \ldots, x_n$.

Remarques

Il est possible d'étendre cette définition à des fonctions récursives à plusieurs arguments c'est-à-dire à des profils
$E \times \ldots \times E \longrightarrow F$ ou
$E \times \ldots \times E \times A_1 \times \ldots \times A_n \longrightarrow F$ où les A_i sont des ensembles quelconques.
Dans ce cas les schémas des fonctions récursives peuvent être plus compliqués ..., peuvent alors se poser des problèmes de terminaisons.

Fonctions récursives sur les arbres binaires

Soit la fonction $n : AB \rightarrow \mathbb{N}$ définissant le nombre d'éléments (entiers) d'un arbre binaire :

$$\begin{cases} n(avide) = 0 \\ n(< g, e, d >) = 1 + n(g) + n(d) \end{cases}$$

Soit la fonction $h : AB \rightarrow \mathbb{N}$ définissant la hauteur d'un arbre binaire :

$$\begin{cases} h(avide) = 0 \\ h(< g, e, d >) = 1 + max(h(g),\ h(d)) \end{cases}$$

Propriété à démontrer : $(\forall a \in AB)\ n(a) \leq 2^{h(a)} - 1$

- Cas de base : on vérifie la propriété pour les éléments de la base, c'est à dire l'arbre vide *avide*.
  $n(avide) = 0$ d'après la définition de n
  $$\begin{aligned} 2^{h(avide)} - 1 &= 2^0 - 1 \quad d'aprés\ la\ définition\ de\ h \\ &= 1 - 1 \\ &= 0 \end{aligned}$$
  d'où $n(avide) \leq 2^{h(avide)} - 1$ et P est vérifiée pour *avide*.
- Pas d'induction.
  $(\forall g \in AB)(\forall d \in AB)(\forall e \in \mathbb{N})(P(g)\ et\ P(d)\ \Rightarrow P(< g, e, d >))$
  L'hypothèse d'induction : $P(g)$ et $P(d)$
  Conclusion : $P(< g, e, d >)$
  Hypothèse d'induction : $n(g) \leq 2^{h(g)} - 1$ et $n(d) \leq 2^{h(d)} - 1$
  $$\begin{aligned} n(< g, e, d >) &= 1 + n(g) + n(d) \quad (définition\ de\ n) \\ &\leq 1 + 2^{h(g)} - 1 + 2^{h(d)} - 1 \quad (hypothèse\ d'induction) \\ &\leq 2^{max(h(g),h(d))} + 2^{max(h(g),\ h(d))} - 1 \quad (car\ n \mapsto 2^n\ est\ croissante) \\ &= 2^{1+max(h(g),h(d))} - 1 \\ &= 2^{h(<g,e,d>)} - 1 \quad (définition\ de\ h) \end{aligned}$$
  d'où la conclusion : $n(< g, e, d >) \leq 2^{h(<g,e,d>)} - 1$, càd $P(< g, e, d >)$.
- Conclusion générale : $(\forall a \in AB)\ n(a) \leq 2^{h(a)} - 1$

Les récurrences vues précédemment sont des cas particuliers de la récurrence nœthérienne.

Definition (Ordre strict, ordre strict nœthérien)

Soit E un ensemble et $\prec$ une relation binaire sur E.

- $\prec$ est un ordre strict sur E si elle possède les propriétés suivantes :
  $\prec$ est irréflexive : $(\forall x \in E)(\neg(x \prec x))$
  $\prec$ est transitive : $(\forall x \in E)(\forall y \in E)(\forall z \in E)(x \prec y \text{ et } y \prec z \Rightarrow x \prec z)$
- $\prec$ est un ordre strict nœthérien, s'il n'existe pas dans E de suite infinie décroissante $x_1 \succ x_2 \succ \ldots$.

Definition (Principe d'induction nœthérienne)

Soit l'ensemble E muni de l'ordre strict nœthérien $\prec$, le principe d'induction nœthérienne sur E s'exprime de la façon suivante :

$$[(\forall x \in E)((\forall y \in E)(y \prec x \Rightarrow P(y)) \Rightarrow P(x))] \Rightarrow (\forall x \in E)(P(x))$$

Remarque

Il n'y a pas de cas de base dans ce principe d'induction.

$$[(\forall x \in E)((\forall y \in E)(y \prec x \Rightarrow P(y)) \Rightarrow P(x))] \Rightarrow (\forall x \in E)(P(x))$$

Preuve

Raisonnons par l'absurde, en supposant que la formule ci-dessus est fausse.

$(\forall x \in E)(P(x))$ est donc fausse, c'est à dire qu'il existe $x_0 \in E$ tel que $\neg P(x_0)$,
on a alors $(\forall x \in E)((\forall y \in E)(y \prec x \Rightarrow P(y)) \Rightarrow P(x))$ vraie,
en particulier cette formule est vraie pour x_0, donc $((\forall y \in E)(y \prec x_0 \Rightarrow P(y)) \Rightarrow P(x_0))$ est vraie,

d'où comme $P(x_0)$ est faux ceci implique alors que $((\forall y \in E)(y \prec x_0 \Rightarrow P(y))$ est faux,

donc il existe $y \in E$ tel que $y \prec x_0$ et $\neg P(y)$, posons $x_1 = y$,

on a ainsi construit le début d'une suite strictement $x_0 \succ x_1 \ldots$ décroissante, on peut continuer le raisonnement en construisant une suite infinie décroissante, ce qui contredit l'hypothèse $(E, \prec)$ ordre nœthérien.