Preuves par induction

David Delahaye

Faculté des Sciences
David.Delahaye@lirmm.fr

Master Informatique M1 2022-2023

Un premier petit exemple

Spécification

On définit la relation inductive *is_sum* de type $\mathbb{N} \times \mathbb{N} \to \mathrm{Prop}$ de la façon suivante :

1. On a : $is\_sum(0, 0)$;
2. Pour $n, s \in \mathbb{N}$, si $is\_sum(n, s)$, alors on a : $is\_sum(S(n), s + S(n))$.

Fonction

On définit la fonction suivante de type $\mathbb{N} \to \mathbb{N}$:

$$f_{is\_sum}(n) = \begin{cases} 0, \text{ si } n = 0 \\ f_{is\_sum}(p) + S(p), \text{ si } n = S(p), \text{ avec } p \in \mathbb{N} \end{cases}$$

Un premier petit exemple

Théorème de correction

L'adéquation entre la fonction et sa spécification se vérifie avec le théorème suivant :

$$\forall n, s \in \mathbb{N}. f_{is\_sum}(n) = s \Rightarrow is\_sum(n, s)$$

Preuve

La preuve se fait par induction sur n.
On utilise le schéma d'induction structurelle sur $\mathbb{N}$:

$$\forall P \in \mathbb{N} \to \mathrm{Prop}. P(0) \Rightarrow (\forall n \in \mathbb{N}. P(n) \Rightarrow P(S(n))) \Rightarrow \forall n \in \mathbb{N}. P(n)$$

Dans notre cas :

$$P(n) = \forall s \in \mathbb{N}. f_{is\_sum}(n) = s \Rightarrow is\_sum(n, s)$$

Un premier petit exemple

Preuve

On applique le schéma d'induction et on doit démontrer :

1. Cas de base :

$$\forall x \in \mathbb{N}. f_{is\_sum}(0) = s \Rightarrow is\_sum(0, s)$$

On calcule $f_{is\_sum}(0)$, ce qui donne :

$$\forall x \in \mathbb{N}. 0 = s \Rightarrow is\_sum(0, s)$$

On remplace s par 0, et on doit démontrer $is\_sum(0, 0)$, qui est le cas de base de la spécification inductive de la relation is_sum.

Un premier petit exemple

Preuve

On applique le schéma d'induction et on doit démontrer :

2. Cas inductif : pour $n \in \mathbb{N}$,

$$\forall s \in \mathbb{N}. f_{is\_sum}(S(n)) = s \Rightarrow is\_sum(S(n), s)$$

sous l'hypothèse d'induction :

$$\forall s \in \mathbb{N}. f_{is\_sum}(n) = s \Rightarrow is\_sum(n, s)$$

On calcule $f_{is\_sum}(S(n))$, ce qui donne :

$$\forall s \in \mathbb{N}. f_{is\_sum}(n) + S(n) = s \Rightarrow is\_sum(S(n), s)$$

On remplace s par $f_{is\_sum}(n) + S(n)$, et on doit démontrer :

$$is\_sum(S(n), f_{is\_sum}(n) + S(n))$$

Un premier petit exemple

Preuve

On applique le schéma d'induction et on doit démontrer :

2. Cas inductif :
   On applique le cas inductif de la spécification de is_sum, et on doit démontrer :

$$is\_sum(n, f_{is\_sum}(n))$$

   On applique l'hypothèse d'induction avec $s = f_{is\_sum}(n)$, et il nous reste à démontrer que $f_{is\_sum}(n) = f_{is\_sum}(n)$, ce qui est trivial.

Un deuxième exemple plus complexe ou quand l'induction structurelle ne suffit plus

Spécification

On définit la relation inductive *is_even* de type $\mathbb{N} \to \mathrm{Prop}$ de la façon suivante :

1. On a : $is\_even(0)$;
2. Pour $n \in \mathbb{N}$, si $is\_even(n)$, alors on a : $is\_even(S(S(n)))$.

Fonction

On définit la fonction suivante de type $\mathbb{N} \to \mathbb{B}$:

$$f_{is\_even}(n) = \begin{cases} \top, \text{ si } n = 0 \\ \bot, \text{ si } n = 1 \\ f_{is\_even}(p), \text{ si } n = S(S(p)), \text{ avec } p \in \mathbb{N} \end{cases}$$

Un deuxième exemple plus complexe ou quand l'induction structurelle ne suffit plus

Théorème de correction

L'adéquation entre la fonction et sa spécification se vérifie avec le théorème suivant :

$$\forall n \in \mathbb{N}. f_{is\_even}(n) = \top \Rightarrow is\_even(n)$$

Preuve

Par induction structurelle sur n :

1. Cas de base :

$$f_{is\_even}(0) = \top \Rightarrow is\_even(0)$$

On applique simplement le cas de base de is_even.

Un deuxième exemple plus complexe ou quand l'induction structurelle ne suffit plus

Preuve

Par induction structurelle sur n :

2. Cas inductif : pour $n \in \mathbb{N}$,

$$f_{is\_even}(S(n)) = \top \Rightarrow is\_even(S(n))$$

sous l'hypothèse d'induction :

$$f_{is\_even}(n) = \top \Rightarrow is\_even(n)$$

Un deuxième exemple plus complexe ou quand l'induction structurelle ne suffit plus

Preuve

Par induction structurelle sur n :

2. Cas inductif :
   On doit refaire une deuxième induction sur n :
   1. Cas de base :

$$f_{is\_even}(1) = \top \Rightarrow is\_even(1)$$

On calcule $f_{is\_even}(1)$, ce qui donne :

$$\bot = \top \Rightarrow is\_even(1)$$

ce qui est trivial car $\bot = \top$ est faux.

Un deuxième exemple plus complexe ou quand l'induction structurelle ne suffit plus

Preuve

Par induction structurelle sur n :

2. Cas inductif :
   On doit refaire une deuxième induction sur n :
   2. Cas inductif :

$$f_{is\_even}(S(S(n))) = \top \Rightarrow is\_even(S(S(n)))$$

sous les hypothèses :

$$f_{is\_even}(S(n)) = \top \Rightarrow is\_even(S(n))$$

$$(f_{is\_even}(n) = \top \Rightarrow is\_even(n)) \Rightarrow$$
$$f_{is\_even}(S(n)) = \top \Rightarrow is\_even(S(n))$$

Un deuxième exemple plus complexe ou quand l'induction structurelle ne suffit plus

Preuve

Par induction structurelle sur n :

2. Cas inductif :
   On doit refaire une deuxième induction sur n :
   2. Cas inductif :
      On calcule $f_{is\_even}(S(S(n)))$ et on applique le cas inductif de la relation is_even, et on doit démontrer $is\_even(n)$ sous les hypothèses :

$$f_{is\_even}(n) = \top$$

$$f_{is\_even}(S(n)) = \top \Rightarrow is\_even(S(n))$$

$$(f_{is\_even}(n) = \top \Rightarrow is\_even(n)) \Rightarrow f_{is\_even}(S(n)) = \top \Rightarrow is\_even(S(n))$$

Un deuxième exemple plus complexe ou quand on a besoin d'induction fonctionnelle

Induction fonctionnelle

- Nouveau schéma d'induction qui « suit » la fonction ;
- Le schéma sera propre à la fonction ;
- N'introduit pas un axiome (démontrable).

Dans le cas de f_{is_even}

$$\forall P \in \mathbb{N} \times \mathbb{B} \to Prop.$$
$$P(0, \top) \Rightarrow P(1, \bot) \Rightarrow$$
$$(\forall p \in \mathbb{N}. P(p, f_{is\_even}(p)) \Rightarrow P(S(S(p)), f_{is\_even}(p))) \Rightarrow$$
$$\forall n \in \mathbb{N}. P(n, f_{is\_even}(n))$$

Un deuxième exemple plus complexe ou quand on a besoin d'induction fonctionnelle

Preuve

$$\forall n \in \mathbb{N}. f_{is\_even}(n) = \top \Rightarrow is\_even(n)$$

Ici, le prédicat P du schéma d'induction est :

$$P(n, b) = b = \top \Rightarrow is\_even(n)$$

1. Cas de base (1) :

   $$\top = \top \Rightarrow is\_even(0)$$

   On applique le cas de base de la relation is_even.

Un deuxième exemple plus complexe ou quand on a besoin d'induction fonctionnelle

Preuve

2. Case de base (2) :

$$\bot = \top \Rightarrow is\_even(1)$$

ce qui est trivial car $\bot = \top$ est faux.

3. Cas inductif : pour $p \in \mathbb{N}$,

$$f_{is\_even}(p) = \top \Rightarrow is\_even(S(S(p)))$$

sous l'hypothèse d'induction :

$$f_{is\_even}(p) = \top \Rightarrow is\_even(p)$$

Un deuxième exemple plus complexe ou quand on a besoin d'induction fonctionnelle

Preuve

3. Cas inductif : pour $p \in \mathbb{N}$,
   On suppose $f_{is\_even}(p) = \top$, puis on applique le cas inductif de la relation is_even, et on doit démontrer :

$$is\_even(p)$$

   sous les hypothèses :

$$f_{is\_even}(p) = \top$$

$$f_{is\_even}(p) = \top \Rightarrow is\_even(p)$$

   ce qui se démontre en appliquant l'hypothèse d'induction à l'hypothèse introduite précédemment.

Spécifications inductives non calculatoires

Spécifications quelconques

- Les spécifications sont parfois plus abstraites ;
- Elles ne contiennent pas forcément un algorithme ;
- C'est même mieux si elles n'en contiennent pas ;
- Si elles contiennent un algorithme, elles n'en imposent pas forcément un au niveau de l'implantation (il faudra en démontrer l'équivalence).

Exemple

- Le pgcd d de deux entiers relatifs a et b peut être spécifié par :
  - d divise a et b, et il existe deux entiers relatifs x et y (co-facteurs) tels que $ax + by = d$ (théorème de Bachet-Bézout) ;
- La spécification précédente n'offre aucun schéma de calcul ;
- Il existe plusieurs algorithmes (algorithme d'Euclide, méthode des soustractions, etc.).

Un troisième exemple qui nécessite une induction plus générale

Fonction de pgcd

On définit le pgcd par soustractions successives par la fonction suivante de type $\mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*$:

$$gcd(a,b) = \begin{cases} a, \text{ si } a = b \\ gcd(a, b-a), \text{ si } b > a \\ gcd(a-b, b), \text{ sinon} \end{cases}$$

- En l'état, cette fonction est mathématiquement mal définie, car on ne sait pas si elle termine ;
- On a besoin de se convaincre qu'elle termine en utilisant une relation bien fondée ;
- On a donc besoin d'induction bien fondée, appelée aussi induction Nœtherienne, qui est une induction plus générale.

Un troisième exemple qui nécessite une induction plus générale

Relation bien fondée

Soit une relation binaire $\mathcal{R}$ sur un ensemble A, c'est-à-dire que $\mathcal{R} \subseteq A \times A$.

La relation $\mathcal{R}$ sera bien fondée dans A s'il n'existe pas de chaînes descendantes infinies, c'est-à-dire de suite (u_i) dans A telle que $u_{i+1}\ \mathcal{R}\ u_i$ pour tout i.

Une fonction f sur A sera définie par induction bien fondée si elle est de la forme suivante :

$$f(x) = g(x, f_{|\inf(x)})$$

où $f_{|\inf(x)} = \{f(y) \mid y\ \mathcal{R}\ x\}$.

Un troisième exemple qui nécessite une induction plus générale

Retour à l'exemple

$$gcd(a,b) = \begin{cases} a, \text{ si } a = b \\ gcd(a, b-a), \text{ si } b > a \\ gcd(a-b, b), \text{ sinon} \end{cases}$$

Quelle est la relation bien fondée ?

$$(x,y)\ \mathcal{R}\ (x',y') = x + y < x' + y'$$

Un troisième exemple qui nécessite une induction plus générale

Schéma d'induction bien fondée

Pour faire des preuves sur le pgcd, on a besoin du schéma d'induction bien fondée correspondant.

Le schéma général d'induction bien fondée est le suivant :

$$\forall P \in A \to \mathit{Prop}.(\forall x \in A.\forall y \in \inf(x).P(y) \Rightarrow P(x)) \Rightarrow \forall x \in A.P(x)$$

où $\inf(x) = \{y \mid y \mathrel{\mathcal{R}} x\}$.

Sur $\mathbb{N}$, on retrouve les schémas d'induction habituels :

- Schéma d'induction structurelle : $x \mathrel{\mathcal{R}} y \equiv y = x + 1$;
- Schéma d'induction généralisée : $x \mathrel{\mathcal{R}} y \equiv x < y$.

Exercices

Factorielle

- Spécifier la fonction factorielle à l'aide d'une relation inductive ;
- Écrire la fonction factorielle ;
- Écrire le schéma d'induction fonctionnelle ;
- Démontrer la correction de la fonction.

Pgcd

- Démontrer que $gcd(a, b)$ (en utilisant la version fonctionnant par soustractions successives) est un diviseur de a et de b.