Correction TD N°4 : Preuves par induction

Exercice 1 (Fonction factorielle)

1. Spécifier la fonction factorielle à l'aide d'une relation inductive.
2. Écrire la fonction factorielle.
3. Écrire le schéma d'induction fonctionnelle associé à cette fonction.
4. Démontrer la correction de la fonction en utilisant le schéma d'induction structurelle.
5. Démontrer la correction de la fonction en utilisant le schéma d'induction fonctionnelle.
6. Démontrer la complétude de la fonction en utilisant le schéma d'induction sur la relation.
7. Répondre aux questions précédentes en utilisant `Coq`.

1. Définissons la relation inductive is_fact, de type $\mathbb{N} \to \mathbb{N} \to Prop$ de la façon suivante :

   (is_fact_1) On a $is\_fact(0, 1)$;

   (is_fact_2) Pour $n, f \in \mathbb{N}$, si $is\_fact(n, f)$ alors on a : $is\_fact(S\ n, f \times S\ n)$.

2. Nous pouvons également écrire la factorielle sous forme de fonction $fact$, de type $\mathbb{N} \to \mathbb{N}$:

   ($fact_1$) On a $fact(0) = 1$;

   ($fact_2$) Pour $n \in \mathbb{N}$, $fact(S\ n) = fact(n) \times S\ n$.

3. Le schéma d'induction fonctionnelle se base sur la fonction prédéfinie. Pour prouver qu'une propriété P est vraie pour tout élément de l'ensemble de définition (ici $\mathbb{N}$), on doit d'abord prouver les cas de bases (ici $fact_1$), puis prouver les règles (ici $fact_2$).
   Le schéma est donc le suivant :

$$\forall P \in \mathbb{N} \to \mathbb{N} \to Prop.$$
$$P(0, 1) \Rightarrow$$
$$(\forall n \in \mathbb{N}.\ P(n, fact(n)) \Rightarrow P(S\ n, fact(n) \times S\ n)) \Rightarrow$$
$$\forall n \in \mathbb{N}.\ P(n, fact(n))$$

4. La démonstration de la correction de la fonction factorielle ($fact$) revient à montrer l'adéquation entre la fonction $fact$ et sa spécification is_fact. Celà se vérifie en prouvant la formule suivante :

$$\forall n, f \in \mathbb{N}.\ fact(n) = f \Rightarrow is\_fact(n, f)$$

   On rappelle le schéma d'induction structurelle de $fact$ qui est le suivant (nous agissons sur les entiers naturels – $\mathbb{N}$) :

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

   Dans notre cas :

$$P(n) = \forall f \in \mathbb{N}.\ fact(n) = f \Rightarrow is\_fact(n, f)$$

   Prouvons cette propriété par induction structurelle :

Base Prouvons la propriété vraie pour le cas $P(0)$.

$$\begin{array}{ll}
\forall f \in \mathbb{N}.\ fact(0) = f \Rightarrow is_fact(0, f) & \\
\forall f \in \mathbb{N}.\ 1 = f \Rightarrow is_fact(0, f) & \text{(application de } fact_1\text{)} \\
\forall f \in \mathbb{N}.\ 1 = f \Rightarrow is_fact(0, 1) & \text{(substitution } f = 1\text{)} \\
\forall f \in \mathbb{N}.\ 1 = f \Rightarrow \top & \text{(application de } is_fact_1\text{)} \\
\qquad\qquad \top & \text{(valeur de vérité de } \Rightarrow\text{)}
\end{array}$$

$P(0)$ est donc vraie.

Induction Supposons $P(n)$ et prouvons $P(S\ n)$.

Nous avons donc l'hypothèse d'induction suivante :

$$\forall f \in \mathbb{N}.\ fact(n) = f \Rightarrow is\_fact(n, f)$$

$$\begin{array}{ll}
\forall f \in \mathbb{N}.\ fact(S\ n) = f \Rightarrow is_fact(S\ n, f) & \\
\forall f \in \mathbb{N}.\ fact(n) \times S\ n = f \Rightarrow is_fact(S\ n, f) & \text{(application de } fact_2\text{)} \\
\forall f \in \mathbb{N}.\ fact(n) \times S\ n = f \Rightarrow is_fact(S\ n, fact(n) \times S\ n) & \text{(substitution } f = fact(n) \times S\ n\text{)} \\
\forall f \in \mathbb{N}.\ fact(n) \times S\ n = f \Rightarrow is_fact(n, fact(n)) & \text{(application de } is_fact_2\text{)}
\end{array}$$

L'application de is_fact_2 peut paraître étrange au premier abord. En fait, il s'agit de l'application de la règle de construction de is_fact qui nous permet de dire : « Si j'ai $is\_fact(n, f)$ alors je sais que j'ai $is\_fact(S\,n, f \times S\,n)$ » ($f = fact(n)$ dans la preuve).

Si on prouve que la première partie est toujours vraie (et c'est ce qu'on va faire), alors la deuxième est toujours vraie également.

Utilisons l'hypothèse d'induction en remplaçant f par $fact(n)$.

$$\begin{array}{rl}
fact(n) = fact(n) \Rightarrow is_fact(n, fact(n)) \equiv \top & \\
is_fact(n, fact(n)) \equiv \top & \text{(Car } fact(n) = fact(n) \text{ est trivial)}
\end{array}$$

On remplace alors notre valeur dans l'équation de base

$$\begin{array}{ll}
\forall f \in \mathbb{N}.\ fact(n) \times S\ n = f \Rightarrow \top & \text{(substitution)} \\
\qquad\qquad \top & \text{(valeur de vérité de } \Rightarrow\text{)}
\end{array}$$

On a bien $\forall n \in \mathbb{N}.\ P(n) \Rightarrow P(S\ n)$.

Par induction structurelle nous avons prouvé la correction de le fonction $fact$.

5. Nous pouvons également prouver cette correction en utilisant le schéma d'induction fonctionnel défini dans la question 3. Soit dans notre cas, prouver la propriété suivante :

$$P(n, f) = fact(n) = f \Rightarrow is\_fact(n, f)$$

Prouvons cette propriété par induction fonctionnelle :

Base Prouvons la propriété vraie pour le cas $P(0,1)$.

$$\begin{aligned}
& fact(0) = 1 \Rightarrow is_fact(0,1) & \\
& fact(0) = 1 \Rightarrow \top & \text{(application de } is_fact_1\text{)} \\
& \top & \text{(valeur de vérité de } \Rightarrow\text{)}
\end{aligned}$$

$P(0,1)$ est donc vraie.

Induction Supposons $P(n, fact(n))$ et prouvons $P(S\ n, fact(n) \times S\ n)$.

Nous avons donc l'hypothèse d'induction suivante :

$$fact(n) = fact(n) \Rightarrow is\_fact(n, fact(n))$$

Soit, par trivialité de $fact(n) = fact(n)$:

$$is\_fact(n, fact(n)) \equiv \top$$

$$\begin{aligned}
& fact(S\ n) = fact(n) \times S\ n \Rightarrow is_fact(S\ n, fact(n) \times S\ n) & \\
& fact(S\ n) = fact(n) \times S\ n \Rightarrow is_fact(n, fact(n)) & \text{(application de } is_fact_2\text{)} \\
& fact(S\ n) = fact(n) \times S\ n \Rightarrow \top & \text{(hypothèse d'induction)} \\
& \top & \text{(valeur de vérité de } \Rightarrow\text{)}
\end{aligned}$$

On a bien $\forall n \in \mathbb{N}.\ P(n, fact(n)) \Rightarrow P(S\ n, fact(n) \times S\ n)$.

Par induction fonctionnelle nous avons prouvé la correction de la fonction $fact$.

6. La démonstration de la complétude de la fonction factorielle ($fact$) est l'inverse de la correction. Elle se vérifie en prouvant la formule suivante :

$$\forall n, f \in \mathbb{N}.\ is\_fact(n, f) \Rightarrow fact(n) = f$$

On utilise pour celà le schéma d'induction de la relation is_fact qui est le suivant :

$$\begin{gathered}
\forall P \in \mathbb{N} \to \mathbb{N} \to Prop. \\
P(0,1) \Rightarrow \\
(\forall n, f \in \mathbb{N}.\ is_fact(n, f) \Rightarrow P(n, f) \Rightarrow P(S\ n, f \times S\ n)) \Rightarrow \\
\forall n, f \in \mathbb{N}.\ is_fact(n, f) \Rightarrow P(n, f)
\end{gathered}$$

On utilise notre schéma avec la propriété $P(n, f) = fact(n) = f$ pour prouver la complétude par induction structurelle.

Base Prouvons la propriété vraie pour le cas $P(0,1)$, soit $fact(0) = 1$.

On calcul $fact(0)$ qui est le cas de base de la fonction $(fact_1)$. Il nous reste alors à prouver $1 = 1$ ce qui est tirvial.

$P(0,1)$ est donc vraie.

Induction Supposons $is\_fact(n, f)$ et $P(n, f)$ et prouvons $P(S\ n, f \times S\ n)$.

Soit les hympthèses d'induction suivante :

$$is\_fact(n, f) \tag{1}$$
$$fact(n) = f \tag{2}$$

$$\begin{aligned}
&fact(S\ n) = f \times S\ n \\
&fact(n) \times S\ n = f \times S\ n && \text{(application de } fact_2\text{)} \\
&f \times S\ n = f \times S\ n && \text{(substitution avec (2))}
\end{aligned}$$

Ce qui est toujours vrai.

On a donc bien $\forall n, f \in \mathbb{N}.\ is\_fact(n, f) \Rightarrow P(n, f) \Rightarrow P(S\ n, f \times S\ n))$

Par induction sur la relation is_fact, la fonction $fact$ est complète.

7. $\diamond$ Voir TP4.

Exercice 2 (Fonction de parité)

Cet exercice est à faire entièrement en `Coq`.

1. Écrire la relation inductive is_even vue en cours.
2. Écrire la fonction récursive f_{is_even} vue en cours.
3. Démontrer que : $\forall n \in \mathbb{N}.\ f_{is\_even}(n) = \top \Rightarrow is\_even(n)$.
4. Démontrer que : $\forall n \in \mathbb{N}.\ f_{is\_even}(n) = \bot \Rightarrow \neg is\_even(n)$.
5. Démontrer que : $\forall n \in \mathbb{N}.\ is\_even(n) \Rightarrow f_{is\_even}(n) = \top$.
6. Démontrer que : $\forall n \in \mathbb{N}.\ \neg is\_even(n) \Rightarrow f_{is\_even}(n) = \bot$.

$\diamond$ Voir TP4.

Exercice 3 (Fonction pgcd))

Cet exercice est à faire entièrement en `Coq`.

1. Écrire la fonction gcd vue en cours.
2. Définir $divides(r, (a, b))$ qui exprime que r divise a et b, avec $r \in \mathbb{N}^*$ et $a, b \in \mathbb{N}$.
3. Démontrer que : $\forall a, b, r \in \mathbb{N}^*.\ gcd(a, b) = r \Rightarrow divides(r, (a, b))$.
4. Définir $bezout(r, (a, b))$ qui exprime qu'il existe $p, q \in \mathbb{Z}$ t.q. $p \times a + q \times b = r, r, a, b \in \mathbb{N}$.
5. Démontrer que : $\forall a, b, r \in \mathbb{N}^*.\ gcd(a, b) = r \Rightarrow bezout(r, (a, b))$.

$\diamond$ Voir TP4.