Vérification (HAI603I)

Licence Informatique
Département Informatique
Faculté des Sciences de Montpellier
Université de Montpellier

TD/TP 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`.

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

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 : $\forall a, b, r \in \mathbb{N}^*. gcd(a, b) = r \Rightarrow bezout(r, (a, b))$.