

# Sécurité logicielle (HAI821I)

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



## TD/TP N°3 : Types inductifs

### Exercice 1 (Fonctions et preuves inductives sur les entiers)

1. Écrire la fonction *mult* sur les entiers naturels  $\mathcal{N}$ .
2. Démontrer que :  $\forall n \in \mathcal{N}. \text{mult}(2, n) = \text{plus}(n, n)$ .
3. Démontrer que :  $\forall n \in \mathcal{N}. \text{mult}(n, 2) = \text{plus}(n, n)$ .

### Exercice 2 (Fonctions et preuves inductives sur les listes)

1. Écrire la fonction *rev* qui inverse les éléments d'une liste.
2. Démontrer que :  $\forall l \in \mathcal{L}. \forall e \in \mathcal{A}. \text{rev}(\text{app}(l, [e])) = e :: \text{rev}(l)$ .
3. Démontrer que :  $\forall l \in \mathcal{L}. \text{rev}(\text{rev}(l)) = l$ .

### Exercice 3 (Type inductif des formules en logique)

1. Définir le type des formules en logique propositionnelle.
2. Écrire la fonction *sub*, qui rend l'ensemble des sous-formules d'une formule  $F$ .
3. Écrire la fonction *nbc*, qui rend le nombre de connecteurs d'une formule  $F$ .
4. Écrire le schéma d'induction structurelle des formules.
5. Démontrer que :  $|\text{sub}(F)| \leq 2 \times \text{nbc}(F) + 1$ , pour toute formule  $F$ .

### Exercice 4 (Relations inductives sur les listes)

1. Spécifier la relation « être une permutation de » pour deux listes.
2. Démontrer que la liste  $[1; 2; 3]$  est une permutation de  $[3; 2; 1]$ .
3. Spécifier la relation « être triée » pour une liste.
4. Démontrer que la liste  $[1; 2; 3]$  est triée.

### Exercice 5 (Preuves en Coq)

Faire les exercices 1, 2 et 4 en Coq.

## Exercice 6 (Preuves en Coq)

1. Écrire la relation inductive  $is\_even$  (vue en cours).
2. Écrire une tactique qui démontre des buts de la forme  $is\_even(n)$ .
3. Écrire une tactique qui démontre des buts de la forme  $\neg is\_even(n)$ .
4. Écrire une tactique qui démontre les buts précédents indifféremment.
5. Écrire la fonction  $f_{is\_even}$  qui teste si un entier est pair.
6. Démontrer que la fonction  $f_{is\_even}$  est correcte vis-à-vis de la relation  $is\_even$ .