

Preuves assistées par ordinateur – TD n° 4

Mathématiques élémentaires en Coq

Exercice 1 – Relations d'ordre

En Coq, on considèr un typ $E : \text{Set}$ muni d'un r lation binair R dont on suppos qu'il satisfait aux axiom s d s r lations d'ordr :

```

P r meter E : Set.
P r meter R : E -> E -> Prop.

Axiom refl : for ll x : E, R x x.
Axiom tr ns : for ll x y z : E, R x y -> R y z -> R x z.
Axiom ntisym : for ll x y : E, R x y -> R y x -> x = y.

```

On définit l s notions d plus p tit élém nt t d'élém nt minimal d la façon suivant :

```

Definition sm llest (x0 : E) := for ll x : E, R x0 x.
Definition minim l (x0 : E) := for ll x : E, R x x0 -> x = x0.

```

Qu ls sont l s typ s d s obj ts `sm llest` t `minim l`?

Énonc r n Coq puis démontr r l s l mm s suivants :

1. Si R adm t un plus p tit élém nt, alors c lui-ci st uniqu .
2. L plus p tit élém nt, s'il xist , st un élém nt minimal.
3. Si R adm t un plus p tit élém nt, alors il n'y a pas d'autr élém nt minimal qu c lui-ci.

Indications : En Coq, un définition s'utilis n r mplaçant l *definiendum* par son *definiens* à l'aïd d la tactiqu `unfold <definiendum>` (*unfold* = dépli r). L'égalité s trait à l'aïd d s tactiqu s `reflexivity`, `symmetry`, `tr nsitivity` *<terme>* t `rewrite <hypothèse>`.

Exercice 2 – Logique classique

Dans c t x rcic , on suppos la règl d raisonn m nt par l'absurd , qu l'on déclar n Coq d la manière suivant :

```

Axiom not_not_elim : for ll A : Prop, ~~A -> A.

```

1. Montr r n Coq qu c t axiom ntraîn l ti rs- xclus : `for ll A : Prop, A \ / ~ A`.

On s propos maint nant d formalis r l paradox d s buv urs, dû à Smullyan :

*Dans toute pièce non vide on peut trouver une personne ayant la propriété suivante :
Si cette personne boit, alors tout le monde dans la pièce boit.*

2. Déclar r n Coq l s div rs élém nts du problèm (n s'inspirant d l' x rcic 1).
3. Énonc r l paradox t n ff ctu r la pr uv (laqu ll r pos sur l ti rs- xclus).

Exercice 3 – Sous-ensembles

Étant donné un type $E : \text{Set}$ dans Coq, on s'intéresse aux sous-ensembles de E , qu'il est commode de représenter par des prédicats unaires sur E , c'est-à-dire par des objets de type $E \rightarrow \text{Prop}$.

1. Définir en Coq un prédicat binaire $\text{subset} : (E \rightarrow \text{Prop}) \rightarrow (E \rightarrow \text{Prop}) \rightarrow \text{Prop}$ exprimant l'inclusion entre deux sous-ensembles. Montrer que cette relation est réflexive et transitive. Est-elle antisymétrique ?
2. Définir en Coq un prédicat binaire $\text{eq} : (E \rightarrow \text{Prop}) \rightarrow (E \rightarrow \text{Prop}) \rightarrow \text{Prop}$ exprimant l'égalité extensionnelle de deux ensembles. Montrer qu'il s'agit d'une relation d'équivalence.
3. Définir en Coq les opérateurs d'union et d'intersection binaires sur les sous-ensembles de E . Montrer que ces deux opérations sont associatives, commutatives, idempotentes, et distributives l'une par rapport à l'autre.