

Fondements des systèmes de preuves – TP n° 5

La correspondance de Curry-Howard

En Coq, une proposition $A : \text{Prop}$ est un type de données, et une preuve de A est un objet de type A . Le mécanisme initié par la commande `Theorem toto : A` sert en réalité à construire un objet de type A pour stocker ensuite sa valeur dans la constante `toto`. Comme pour toute autre constante définie dans le système, il est possible de vérifier le type de `toto` à l'aide de la commande `Check toto` et d'afficher sa valeur à l'aide de la commande `Print toto`.

Attention : La définition d'une constante à l'aide du système de tactiques (invoqué par `Theorem`, etc.) est *opaque* par défaut ; il n'est donc pas possible de consulter sa valeur.¹ Pour que la définition soit *transparente*, il suffit de remplacer `Qed` par `Defined` à la fin de la preuve.

Exercice 0.1 Prouvez la proposition `forall A : Prop, A -> A` et affichez sa preuve.

En Coq, l'abstraction (typée) $\lambda x:T. f(x)$ se note `fun (x : T) => f x`. Son type est un produit dépendant $\Pi x:T. U(x)$ qui s'écrit `forall (x : T), U(x)`. Dans le cas où $U(x) = U$ ne dépend pas de la variable $x : T$, le produit (non) dépendant s'abrège en `T -> U`.

Exercice 0.2 Vérifiez qu'en Coq, l'implication n'est qu'un cas particulier de la quantification universelle en faisant la commande : `Check (forall n : nat, True)`.

La tactique `exact <terme de preuve>` permet de résoudre n'importe quel sous-but en donnant un terme de preuve explicitement. Plus généralement, on peut démontrer un théorème en donnant directement le terme de preuve à l'aide de la construction

```
Theorem <constante> : <proposition>.    (* ou Lemma, Fact, Remark ... *)
Proof <terme de preuve>.
```

Le but de ce TP est d'effectuer des démonstrations de cette manière, en donnant les termes de preuve explicitement. Pour cela, on se fixe les paramètres suivants :

```
Parameter A B C : Prop.           Parameter T : Set.
Parameter P Q R : T -> Prop.     Parameter c : T.           Parameter f : T -> T.
```

Exercice 1 (Logique minimale) Donnez des termes de preuve des propositions suivantes :

1. $A \rightarrow A$
2. $(A \rightarrow B) \rightarrow (B \rightarrow C) \rightarrow A \rightarrow C$
3. $A \rightarrow B \rightarrow A$
4. $(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$

¹Ceci afin d'éviter qu'un résultat établi ultérieurement ne repose sur la *démonstration* du théorème, et pas simplement sur le fait que le théorème a été démontré.

Exercice 2 (La négation) On rappelle que $\sim A$ est une abréviation pour $A \rightarrow \text{False}$.
 Donnez des termes de preuve des propositions suivantes :

1. $A \rightarrow \sim\sim A$.
2. $\sim\sim A \rightarrow A$.
3. $(A \rightarrow B) \rightarrow (\sim B \rightarrow \sim A)$.
4. $\sim(\sim\sim A \rightarrow A)$.

Indication : Pour éliminer la proposition `False`, on pourra utiliser la constante prédéfinie `false_ind` : `forall P : Prop, False -> P` (*ex falso quod libet*).

Exercice 3 (La quantification universelle) Donnez des termes de preuve des propositions suivantes :

1. $(\text{forall } x, P\ x \rightarrow Q\ x) \rightarrow (\text{forall } x, P\ x) \rightarrow (\text{forall } x, Q\ x)$.
2. $(\text{forall } x, P\ x \rightarrow Q\ x) \rightarrow (\text{forall } x, Q\ x \rightarrow R\ x) \rightarrow (\text{forall } x, P\ x \rightarrow R\ x)$.
3. $(\text{forall } x, P\ x \rightarrow P\ (f\ x)) \rightarrow (\text{forall } x, P\ x \rightarrow P\ (f\ (f\ x)))$.
4. $(\text{forall } x, P\ x \rightarrow Q\ x) \rightarrow \sim Q\ c \rightarrow \sim (\text{forall } x, P\ x)$

Exercice 4 (La conjonction) À l'aide des constantes prédéfinies

```
and      : Prop -> Prop -> Prop    (* Sucre: A /\ B := and A B *)
conj     : forall A B : Prop, A -> B -> A /\ B.
proj1    : forall A B : Prop, A /\ B -> A.
proj2    : forall A B : Prop, A /\ B -> B.
```

donnez des termes de preuve des propositions suivantes :

1. $A \wedge B \rightarrow B \wedge A$.
2. $(A \wedge B) \wedge C \rightarrow A \wedge (B \wedge C)$.
3. $(A \rightarrow B) \wedge (A \rightarrow C) \leftrightarrow (A \rightarrow B \wedge C)$.
4. $(\text{forall } x, P\ x \wedge Q\ x) \leftrightarrow (\text{forall } x, P\ x) \wedge (\text{forall } x, Q\ x)$.

Exercice 5 (La disjonction) À l'aide des constantes prédéfinies

```
or       : Prop -> Prop -> Prop    (* Sucre: A \/ B := or A B *)
or_introl : forall A B : Prop, A -> A \/ B.
or_intror : forall A B : Prop, B -> A \/ B.
or_ind    : forall A B P : Prop, (A -> P) -> (B -> P) -> A \/ B -> P.
```

donnez des termes de preuve des propositions suivantes :

1. $A \vee B \rightarrow B \vee A$.
2. $(A \vee B) \vee C \rightarrow A \vee (B \vee C)$.
3. $(A \vee B \rightarrow C) \leftrightarrow (A \rightarrow C) \wedge (B \rightarrow C)$.
4. $\sim\sim (A \vee \sim A)$.