Exercice 1 : Preuves en déduction naturelle et en français (23 pt)

Q1. (4 pt) Donnez la preuve en déduction naturelle du théorème

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

$$
\dfrac{
  \dfrac{
    \dfrac{
      \overbrace{\neg A \vee B}^{H_1}
      \qquad
      \dfrac{
        \dfrac{
          \dfrac{
            \overbrace{A}^{H_2}
            \quad
            \dfrac{\overbrace{\neg A}^{H_3}}{H_3 \ \vdash \ A \Rightarrow \bot}\ def\ \neg
          }{H_2, H_3 \ \vdash \ \bot}\ \Rightarrow_e
        }{H_2, H_3 \ \vdash \ B}\ \bot_e
      }{H_2 \ \vdash \ \neg A \Rightarrow B}\ \Rightarrow_i [H_3]
      \qquad
      \dfrac{\overbrace{B}^{H_4}}{B \Rightarrow B}\ \Rightarrow_i [H_4]
    }{H_2, H_1 \ \vdash \ B}\ \vee_e
  }{H_1 \ \vdash \ A \Rightarrow B}\ \Rightarrow_i [H_2]
}{(\neg A \vee B) \Rightarrow (A \Rightarrow B)}\ \Rightarrow_i [H_1]
$$

Q2. (2 pt) Donnez, **sur votre copie**, la version en français de la preuve précédente.

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

```
Démontrons ((!A \/ B) ==> (A ==> B)) :
Pour cela, supposons (!A \/ B) (hypothèse [H1]) et montrons (A ==> B) :
{ Preuve de (A ==> B) :
  Supposons A (hypothèse [H2]) et montrons B :
  { Preuve de B :
    Exploitons la disjonction (!A \/ B) qui correspond à l'hypothèse [H1]
    Comme on ne sait pas lequel est vrai parmi les deux membres de la disjonction (!A \/ B)
    il nous faut montrer B prouver dans chacun des cas :
    - Cas 1: Démontrons (!A ==> B) :
       Supposons !A (hypothèse [H3]) et montrons B :
         On montre en fait que le cas !A est impossible.
         Puisqu'on a A d'après [H2] et !A d'après [H3], on aboutit à une absurdité
         qui prouve que le cas !A ne peut se produire et il n'y a donc rien à montrer.

    - Cas 2: Démontrons (B ==> B) : C'est trivial.
  }: on a ainsi montré B sous les hypothèses A et (!A \/ B)
}: on a ainsi montré (A ==> B) sous l'hypothèse (!A \/ B)

Ceci achève la démonstration de ((!A \/ B) ==> (A ==> B))
```

Q3. (3 pt) Donnez la preuve en déduction naturelle du théorème

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \overbrace{A \vee B}^{H_3}
        \quad
        \overbrace{A \Rightarrow C}^{H_1}
        \quad
        \overbrace{B \Rightarrow C}^{H_2}
      }{H_2, H_1, H_3 \ \vdash \ C}\ \vee_e
    }{H_2, H_1 \ \vdash \ (A \vee B) \Rightarrow C}\ \Rightarrow_i [H_3]
  }{H_1 \ \vdash \ (B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C)}\ \Rightarrow_i [H_2]
}{(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C))}\ \Rightarrow_i [H_1]
$$

Q4. (4 pt) Donnez la preuve en déduction naturelle du théorème

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

$$
\dfrac{\dfrac{\dfrac{\overbrace{\exists u,(\forall v,F(u,v))}^{H_1} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\forall v,F(U_1,v)}^{H_2}}{H_2 \;\vdash\; F(U_1,X_1)}\;\forall_e(v:=X_1)}{H_2 \;\vdash\; \exists y,F(y,X_1)}\;\exists_i}{(\forall v,F(U_1,v))\Rightarrow(\exists y,F(y,X_1))}\;\Rightarrow_i [H_2]}{\forall u,(\forall v,F(u,v))\Rightarrow(\exists y,F(y,X_1))}\;\forall_i(U_1\notin\mathscr{H}\cup\mathscr{C})}{H_1 \;\vdash\; \exists y,F(y,X_1)}\;\exists_e}{H_1 \;\vdash\; \forall x,\exists y,F(y,x)}\;\forall_i(X_1\notin\mathscr{H}\cup\mathscr{C})}{(\exists u,(\forall v,F(u,v)))\Rightarrow(\forall x,\exists y,F(y,x))}\;\Rightarrow_i [H_1]
$$

Q5. (2 pt) Donnez, **sur votre copie**, la version en français de la preuve précédente.

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

```
Démontrons ((EX u, (QQ v, F(u,v))) ==> (QQ x, (EX y, F(y,x)))) :
Pour cela, supposons (EX u, (QQ v, F(u,v))) (hypothèse [H1]) et montrons (QQ x, (EX y, F(y,x))).
{ Preuve de (QQ x, (EX y, F(y,x))) :
  Pour démontrer (QQ x, (EX y, F(y,x))) considérons un X1 quelconque et montrons (EX y, F(y,X1)).
  Pour cela, exploitons le fait qu'il existe un u tel que (QQ v, F(u,v))
  ce qu'on sait d'après l'hypothèse [H1]: (EX u, (QQ v, F(u,v))).

  Comme on ne connait pas explicitement le u qui satisfait la propriété
  on va devoir montrer (EX y, F(y,X1)) pour tout u qui satisferait (QQ v, F(u,v)).

  Démontrons donc (QQ u, ((QQ v, F(u,v)) ==> (EX y, F(y,X1)))) :
    Pour démontrer (QQ u, ((QQ v, F(u,v)) ==> (EX y, F(y,X1)))) considérons un U1 quelconque
    et montrons ((QQ v, F(U1,v)) ==> (EX y, F(y,X1))).
    Pour cela,
     supposons (QQ v, F(U1,v)) (hypothèse [H2]) et montrons (EX y, F(y,X1)) :
     { Preuve de (EX y, F(y,X1)) :
       Pour démontrer (EX y, F(y,X1)) il suffit de montrer la propriété F(y,X1)
       pour un y bien choisi.
       Prenons y = U1 et montrons F(U1,X1), c'est une instance particulière (pour v:=X1)
       de (QQ v, F(U1,v)) qui correspond à l'hypothèse [H2]
     }: on a ainsi montré (EX y, F(y,X1)) sous l'hypothèse H2
        ce qui prouve ((QQ v, F(U1,v)) ==> (EX y, F(y,X1))).

}: on a ainsi montré (QQ x, (EX y, F(y,x))) avec l'hypothèse H1

Ceci achève la démonstration de ((EX u, (QQ v, F(u,v))) ==> (QQ x, (EX y, F(y,x))))
```

Q6. (4 pt) La relation $R(x,q)$ représente le fait que « x connaît la réponse à la question q ». La relation $E(q,x)$ modélise le fait que « q est une énigme pour x ». Donnez la preuve en déduction naturelle du théorème

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

$$
\dfrac{\dfrac{\dfrac{\overbrace{\exists u, E(u, Platon)}^{H_2} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\forall v, R(S,v)}^{H_1}}{H_1 \vdash R(S,U_1)}\forall_e(v := U_1) \quad \overbrace{E(U_1, Platon)}^{H_3}}{H_1, H_3 \vdash R(S,U_1) \wedge E(U_1, Platon)}\wedge_i}{H_1, H_3 \vdash \exists y, (R(S,y) \wedge E(y, Platon))}\exists_i}{H_1 \vdash E(U_1, Platon) \Rightarrow (\exists y, (R(S,y) \wedge E(y, Platon)))}\Rightarrow_i [H_3]}{H_1 \vdash \forall u, E(u, Platon) \Rightarrow (\exists y, (R(S,y) \wedge E(y, Platon)))}\forall_i(U_1 \notin \mathscr{H} \cup \mathscr{C})}{H_2, H_1 \vdash \exists y, (R(S,y) \wedge E(y, Platon))}\exists_e}{H_1 \vdash (\exists u, E(u, Platon)) \Rightarrow (\exists y, (R(S,y) \wedge E(y, Platon)))}\Rightarrow_i [H_2]}{(\forall v, R(S,v)) \Rightarrow ((\exists u, E(u, Platon)) \Rightarrow (\exists y, (R(S,y) \wedge E(y, Platon))))}\Rightarrow_i [H_1]
$$

Q7. (4 pt) Donnez la preuve en déduction naturelle du théorème suivant :

SOLUTION PROPOSÉE PAR LE PROUVEUR INF124

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{A}^{H_{11}} \quad \overbrace{A \Rightarrow B}^{H_1}}{H_{11}, H_1 \vdash B}\Rightarrow_e}{H_{11}, H_1 \vdash \neg A \vee B}\vee_{i_2} \quad \dfrac{\overbrace{\neg(\neg A \vee B)}^{H_{10}}}{H_{10} \vdash (\neg A \vee B) \Rightarrow \bot}def\ \neg}{H_1, H_{11}, H_{10} \vdash \bot}\Rightarrow_e}{H_1, H_{10} \vdash A \Rightarrow \bot}\Rightarrow_i [H_{11}]}{H_1, H_{10} \vdash \neg A}def\ \neg}{H_1, H_{10} \vdash \neg A \vee B}\vee_{i_1} \quad \dfrac{\overbrace{\neg(\neg A \vee B)}^{H_{10}}}{H_{10} \vdash (\neg A \vee B) \Rightarrow \bot}def\ \neg}{H_1, H_{10} \vdash \bot}\Rightarrow_e}{H_1 \vdash \neg(\neg A \vee B) \Rightarrow \bot}\Rightarrow_i [H_{10}]}{H_1 \vdash \neg A \vee B}\neg\neg_e}{(A \Rightarrow B) \Rightarrow (\neg A \vee B)}\Rightarrow_i [H_1]
$$

Exercice 2 : Preuve de propriétés des ensembles (10 pt)

Q8. (4 pt) Démontrez à l'aide d'une preuve en déduction naturelle que les 3 règles de déduction suivantes sont correctes :

1. $\dfrac{a \in A \qquad A \subseteq B}{a \in B}$

2. $\dfrac{a \in A}{a \in A \cup B}$

3. $\dfrac{a \in A \cap B}{a \in A}$

Q9. (2 pt) Utilisez les règles de la déduction naturelle et les règles de déduction sur les ensembles (y compris les règles de la question précédente) pour montrer le théorème

Q10. (4 pt) On désigne l'ensemble vide par $\emptyset$. Utilisez les règles de la déduction naturelle et les règles de déduction sur les ensembles pour montrer le théorème

Exercice 3 : Schéma de récurrence associé à un type OCAML (6 pt)

Q11. (2 pt) Soit `expr` un type défini par :

```
type expr =
  | I of int
  | Op of expr
  | Plus of expr * expr
```

- Donnez trois élements différents de type `expr`.
- Complétez le schéma de récurrence associé au type `expr`.

$$\frac{\begin{array}{c}\forall i \in int,\ Q(\mathrm{I}(\textsc{i})) \\ \forall e,\ Q(e) \Rightarrow Q(\textsc{Op}(e)) \\ \forall e_1, e_2,\ Q(e_1)\ \wedge\ Q(e_2) \Rightarrow Q(\textsc{Plus}(e_1, e_2))\end{array}}{\forall e \in \texttt{expr},\ Q(e)}\ rec{-}expr$$

Q12. (2 pt) Soit `desc` un type défini par :

```
type desc =
  | P
  | C
  | F of desc
```

- Donnez trois élements différents de type `desc`.
- Complétez le schéma de récurrence associé au type `desc`.

$$\frac{Q(\textsc{p}) \quad Q(\textsc{c}) \quad \forall d,\ Q(d) \Rightarrow Q(\textsc{f}(d))}{\forall d \in \texttt{desc},\ Q(d)}\ rec{-}desc$$

Q13. (2 pt) Donnez le schéma de récurrence associé au type `a3int` défini par :

```
type a3int =
 | AVIDE
 | AB of int * a3int * a3int * a3int
```

SOLUTION

$$\frac{P(\textsc{Avide}) \quad \forall a_1, a_2, a_3,\ P(a_1)\ \wedge\ P(a_2)\ \wedge\ P(a_3) \Rightarrow (\forall n,\ P(\textsc{Ab}(n, a_1, a_2, a_3)))}{\forall a \in \texttt{a3int},\ P(a)}\ rec{-}abint$$

Exercice 4 : Preuve par récurrence en déduction naturelle (21 pt)

On considère le type OCAML suivant

```
type zint =
 | Z
 | S of zint
 | P of zint
```

On rappele le schéma de récurrence associé au type `zint`

$$\frac{Q(\textsc{z}) \quad \forall i,\ Q(i) \Rightarrow Q(\textsc{s}(i)) \quad \forall i,\ Q(i) \Rightarrow Q(\textsc{p}(i))}{\forall i \in \texttt{zint},\ Q(i)}\ rec{-}zint$$

Implantation de fonctions définies par des axiomes On considère la fonction *neg* définie par les axiomes suivants :

$$\begin{array}{ll} Ax_1: & neg(\textsc{z}) = \textsc{z} \\ Ax_2: & \forall i,\ neg(\textsc{s}(i)) = \textsc{p}(neg(i)) \\ Ax_3: & \forall i,\ neg(\textsc{p}(i)) = \textsc{s}(neg(i)) \end{array}$$

Q14. (2 pt) Écrire en OCAML la fonction *neg* de type `zint` $\rightarrow$ `zint` qui correspond à ces axiomes.

SOLUTION

```
let rec (neg: zint -> zint) =
  function
  | Z -> Z
  | S i -> P (neg i)
  | P i -> S (neg i)
```

On considère deux fonctions *nbP* et *nbS* qui comptent le nombre de S, respectivement le nombre de P, dans un élement $i \in$ `zint`. Les fonctions sont définies par les axiomes suivants :

$$\begin{array}{llcll} Ax_4: & nbP(\text{Z}) = 0 & & Ax_7: & nbS(\text{Z}) = 0 \\ Ax_5: & \forall i,\ nbP(\text{S}(i)) = nbP(i) & et & Ax_8: & \forall i,\ nbS(\text{S}(i)) = 1 + nbS(i) \\ Ax_6: & \forall i,\ nbP(\text{P}(i)) = 1 + nbP(i) & & Ax_9: & \forall i,\ nbS(\text{P}(i)) = nbS(i) \end{array}$$

Q15. (3 pt) Écrire en OCAML les fonctions *nbP* et *nbS* de type `zint` $\rightarrow$ `nat` qui correspondent à ces axiomes.

SOLUTION

```
let rec (nbP: zint -> int) =
  function
  | Z -> 0
  | P i -> 1 + (nbP i)
  | S i -> nbP i

let rec (nbS: zint -> int) =
  function
  | Z -> 0
  | P i -> nbS i
  | S i -> 1 + (nbS i)
```

Q16. (6 pt) Utilisez les axiomes qui définissent *neg* et le principe de récurrence sur `zint` pour démontrer sous forme d'arbre de preuve le théorème suivant :

$Thm_1: \quad \forall i \in \texttt{zint},\ neg(neg(i)) = i$

SOLUTION

$$\dfrac{\dfrac{neg(neg(\mathrm{Z})) \overset{Ax_1}{=} neg(\mathrm{Z}) \overset{Ax_1}{=} \mathrm{Z}}{neg(neg(\mathrm{Z})) = \mathrm{Z}}\ {=_{trans}} \qquad \nabla_{\mathrm{S}} \quad \nabla_{\mathrm{P}}}{\forall i \in \texttt{zint},\ neg(neg(i)) = i}\ rec - \texttt{zint}$$

$$\nabla_{\mathrm{S}} \overset{def}{=} \left\{ \dfrac{\dfrac{\dfrac{neg(neg(\mathrm{S}(\mathcal{I}_0))) \overset{Ax_2}{=} neg(\mathrm{P}(neg(\mathcal{I}_0))) \overset{Ax_3}{=} \mathrm{S}(neg(neg(\mathcal{I}_0))) \overset{Hrec}{=} \mathrm{S}(\mathcal{I}_0)}{neg(neg(\mathrm{S}(\mathcal{I}_0))) = \mathrm{S}(\mathcal{I}_0)}}{neg(neg(\mathcal{I}_0)) = \mathcal{I}_0 \Rightarrow neg(neg(\mathrm{S}(\mathcal{I}_0))) = \mathrm{S}(\mathcal{I}_0)}\ \Rightarrow_i [Hrec]}{\forall i,\ neg(neg(i)) = i \Rightarrow neg(neg(\mathrm{S}(i))) = \mathrm{S}(i)}\ \forall_i\ \mathcal{I}_0 \notin Hyp, \notin Conc \right.$$

$$\nabla_{\mathrm{P}} \overset{def}{=} \left\{ \dfrac{\dfrac{\dfrac{neg(neg(\mathrm{P}(\mathcal{I}_0))) \overset{Ax_3}{=} neg(\mathrm{S}(neg(\mathcal{I}_0))) \overset{Ax_2}{=} \mathrm{P}(neg(neg(\mathcal{I}_0))) \overset{Hrec}{=} \mathrm{P}(\mathcal{I}_0)}{neg(neg(\mathrm{P}(\mathcal{I}_0))) = \mathrm{P}(\mathcal{I}_0)}}{neg(neg(\mathcal{I}_0)) = \mathcal{I}_0 \Rightarrow neg(neg(\mathrm{P}(\mathcal{I}_0))) = \mathrm{P}(\mathcal{I}_0)}\ \Rightarrow_i [Hrec]}{\forall i,\ neg(neg(i)) = i \Rightarrow neg(neg(\mathrm{P}(i))) = \mathrm{P}(i)}\ \forall_i\ \mathcal{I}_0 \notin Hyp, \notin Conc \right.$$

Q17. (6 pt) Utilisez les axiomes qui définissent nbP et nbS et le principe de récurrence sur `zint` pour démontrer sous forme d'arbre de preuve le théorème suivant :

Thm_2 : $\forall i \in \texttt{zint},\ nbP(neg(i)) = nbS(i)$

SOLUTION

$$\dfrac{\dfrac{nbP(neg(\mathrm{Z})) \overset{Ax_1}{=} nbP(\mathrm{Z}) \overset{Ax_4}{=} 0 \overset{Ax_7}{=} nbS(\mathrm{Z})}{nbP(neg(\mathrm{Z})) = nbS(\mathrm{Z})}\ {=_{trans}} \qquad \nabla_{\mathrm{S}} \quad \nabla_{\mathrm{P}}}{\forall i \in \texttt{zint},\ nbP(neg(i)) = nbS(i)}\ rec - \texttt{zint}$$

$$\nabla_{\mathrm{S}} \overset{def}{=} \left\{ \dfrac{\dfrac{\dfrac{nbP(neg(\mathrm{S}(\mathcal{I}_0))) \overset{Ax_2}{=} nbP(\mathrm{P}(neg(\mathcal{I}_0))) \overset{Ax_6}{=} 1 + nbP(neg(\mathcal{I}_0)) \overset{Hrec}{=} 1 + \mathrm{S}(\mathcal{I}_0) \overset{Ax_8}{=} nbS(\mathrm{S}(\mathcal{I}_0))}{nbP(neg(\mathrm{S}(\mathcal{I}_0))) = nbS(\mathrm{S}(\mathcal{I}_0))}\ {=_{trans}}}{nbP(neg(\mathcal{I}_0)) = nbS(\mathcal{I}_0) \Rightarrow nbP(neg(\mathrm{S}(\mathcal{I}_0))) = nbS(\mathrm{S}(\mathcal{I}_0))}\ \Rightarrow_i [Hrec]}{\forall i,\ nbP(neg(i)) = nbS(i) \Rightarrow nbP(neg(\mathrm{S}(i))) = nbS(\mathrm{S}(i))}\ \forall_i\ \mathcal{I}_0 \notin Hyp, \notin Conc \right.$$

$$\nabla_{\mathrm{P}} \overset{def}{=} \left\{ \dfrac{preuve\ similaire}{\forall i,\ nbP(neg(i)) = nbS(i) \Rightarrow nbP(neg(\mathrm{P}(i))) = nbS(\mathrm{P}(i))} \right.$$

Q18. (4 pt) En réutilisant les théorèmes Thm_1 et Thm_2, démontrez (sans récurrence) le théorème suivant : $\forall i \in \texttt{zint},\ nbS(neg(i)) = nbP(i)$

SOLUTION

$$\dfrac{\dfrac{\dfrac{\overbrace{\forall i \in \texttt{zint},\ nbP(neg(i)) = nbS(i)}^{Thm_2}}{nbS(neg(\mathcal{I}_0)) = nbP(neg(neg(\mathcal{I}_0)))}\ \forall_e(i := neg(\mathcal{I}_0)) \qquad \dfrac{\dfrac{\overbrace{\forall i \in \texttt{zint},\ nbP(neg(i)) = nbS(i)}^{Thm_1}}{neg(neg(\mathcal{I}_0)) = \mathcal{I}_0}\ \forall_e(i := \mathcal{I}_0)}{nbP(neg(neg(\mathcal{I}_0))) = nbP(\mathcal{I}_0)}\ app\ nbP}{nbS(neg(\mathcal{I}_0)) = nbP(\mathcal{I}_0)}\ {=_{trans}}}{\forall i \in \texttt{zint},\ nbS(neg(i)) = nbP(i)}\ \forall_i\ \mathcal{I}_0 \notin Hyp, I_0 \notin Conc$$
