Numéro d'anonymat : ....

INF124

Durée : 2h00, sans documents.

- Tous les appareils électroniques sont interdits à l'exception des montres
- Le barème est donné à titre indicatif
- Le sujet comporte 7 exercices indépendants
- Le sujet est sur 64 mais il suffit d'avoir 30 pour avoir la moyenne.
- Répondez sur le sujet

Exercice 1 : Preuve par récurrence en déduction naturelle (10 pt)

On considère le type OCAML suivant

```
type nat =
  | Z
  | S of nat
```

Q1. (1.5 pt) Rappelez le principe de récurrence associé au type `nat`.

$$\frac{\boxed{P(\mathrm{z})} \quad \boxed{\forall p,\ P(p) \Rightarrow P(\mathrm{s}(p))}}{\forall n \in \texttt{nat},\ P(n)}\ {\scriptstyle rec-nat}$$

Implantation d'un prédicat défini par des axiomes On considère le prédicat *pair* défini par les axiomes suivants :

Ax_1 : $pair(\mathrm{z})$
Ax_2 : $\neg pair(\mathrm{s}(\mathrm{z}))$
Ax_3 : $\forall n,\ pair(\mathrm{s}(\mathrm{s}(n))) \Longleftarrow pair(n)$

Q2. (1.5 pt) Écrire en OCAML la fonction *pair* de type `nat` $\rightarrow$ `bool` qui correspond à ces axiomes.

SOLUTION

```
let rec (pair: nat -> bool) = fun n' ->
 match n' with
  | Z -> true
  | S(Z) -> false
  | S(S(n)) -> pair n
;;
```

Q3. (7 pt) Utilisez les axiomes qui définissent *pair* et le principe de récurrence sur `nat` pour démontrer sous forme d'arbre de preuve le théorème suivant : $\forall n \in \texttt{nat},\ pair(n)\ \vee\ pair(\mathrm{S}(n))$

$$\forall n \in \texttt{nat},\ pair(n)\ \vee\ pair(\mathrm{S}(n)))$$

$$\dfrac{\dfrac{\dfrac{\overbrace{pair(\mathrm{z})}^{Ax_1}}{pair(\mathrm{z}) \ \lor\ pair(\mathrm{s}(\mathrm{z})))}\ {\scriptstyle \lor_{i1}}}{P(\mathrm{z})}\ {\scriptstyle def\ P} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{P(K)}^{[Hr]}}{pair(K)\ \lor\ pair(\mathrm{s}(K)))}\ {\scriptstyle def\ P} \quad \dfrac{\dfrac{\overbrace{pair(K)}^{[H_1]} \quad \dfrac{\overbrace{pair(n) \Rightarrow pair(\mathrm{s}(\mathrm{s}(n)))}^{Ax_3}}{pair(K) \Rightarrow pair(\mathrm{s}(\mathrm{s}(K)))}\ {\scriptstyle \forall_e\ (n=K)}}{pair(\mathrm{s}(\mathrm{s}(K)))}\ {\scriptstyle \Rightarrow_e}}{pair(\mathrm{s}(K))\ \lor\ pair(\mathrm{s}(\mathrm{s}(K)))}\ {\scriptstyle \lor_{i1}} \quad \dfrac{\overbrace{pair(\mathrm{s}(K))}^{[H_2]}}{pair(\mathrm{s}(K))\ \lor\ pair(\mathrm{s}(\mathrm{s}(K)))}\ {\scriptstyle \lor_{i2}}}{pair(\mathrm{s}(K))\ \lor\ pair(\mathrm{s}(\mathrm{s}(K)))}\ {\scriptstyle \lor_e\ [H_1,H_2]}}{P(\mathrm{s}(K))}\ {\scriptstyle def\ P}}{P(K) \Rightarrow P(\mathrm{s}(K))}\ {\scriptstyle \Rightarrow_i\ [Hr]}}{\forall k,\ P(k) \Rightarrow P(\mathrm{s}(k))}\ {\scriptstyle \forall_i\ K \notin \mathcal{H}, K \notin C}}{\forall n \in \texttt{nat},\ pair(n)\ \lor\ pair(\mathrm{s}(n))}\ {\scriptstyle rec-nat\ avec\ P(n) \overset{def}{=} pair(n)\ \lor\ pair(\mathrm{S}(n)))}$$

Exercice 2 : Arbre de preuve et traduction en français (10 pt)

Q4. (2 pt) Démontrez sous forme d'arbre de preuve en déduction naturelle le théorème suivant

$$\dfrac{}{(A \Rightarrow C \;\wedge\; B \Rightarrow C) \Longrightarrow ((A \;\vee\; B) \Rightarrow C)}$$

SOLUTION

$$\dfrac{\dfrac{\dfrac{\overbrace{\overbrace{A \vee B}^{H_2} \qquad \dfrac{\dfrac{\overbrace{A}^{H_3} \qquad \dfrac{\overbrace{(A \Rightarrow C) \;\wedge\; (B \Rightarrow C)}^{H_1}}{H_1 \;\vdash\; A \Rightarrow C}\;\wedge_{e_1}}{H_3, H_1 \;\vdash\; C}\;\Rightarrow_e}{H_1 \;\vdash\; A \Rightarrow C}\;\Rightarrow_i [H_3] \qquad \dfrac{\dfrac{\overbrace{B}^{H_4} \qquad \dfrac{\overbrace{(A \Rightarrow C) \;\wedge\; (B \Rightarrow C)}^{H_1}}{H_1 \;\vdash\; B \Rightarrow C}\;\wedge_{e_2}}{H_4, H_1 \;\vdash\; C}\;\Rightarrow_e}{H_1 \;\vdash\; B \Rightarrow C}\;\Rightarrow_i [H_4]}^{}}{H_1, H_2 \;\vdash\; C}\;\vee_e}{H_1 \;\vdash\; (A \vee B) \Rightarrow C}\;\Rightarrow_i [H_2]}{((A \Rightarrow C) \;\wedge\; (B \Rightarrow C)) \Rightarrow ((A \vee B) \Rightarrow C)}\;\Rightarrow_i [H_1]$$

Q5. (2 pt) Donnez la traduction en français de cette preuve.

SOLUTION

```
D?montrons (((A ==> C) /\ (B ==> C)) ==> ((A \/ B) ==> C)) :
supposons ((A ==> C) /\ (B ==> C)) (hypoth?se [H1]) et montrons ((A \/ B) ==> C) :
{ Preuve de ((A \/ B) ==> C) :
  supposons (A \/ B) (hypoth?se [H2]) et montrons C :
  { Preuve de C :Pour cela exploitons la disjonction (A \/ B)
      qui correspond ? l'hypoth?se [H2]
    Comme on ne sait pas lequel est vrai parmi les deux membres de la disjonction (A \/ B)
    Pour montrer C il nous faut le prouver dans chacun des cas :
    - Cas 1: D?montrons (A ==> C) :
          supposons A (hypoth?se [H3]) et montrons C :
          c'
            Puisqu'on a A d'apr?s [H3], il suffit, pour obtenir C, de montrer (A ==> C)
```

```
            qui est la partie droite de la conjonction ((A ==> C) /\ (B ==> C))
              qui correspond ? l'hypoth?se [H1]

    - Cas 2: D?montrons (B ==> C) :
          supposons B (hypoth?se [H4]) et montrons C :
          c'
            Puisqu'on a B d'apr?s [H4], il suffit, pour obtenir C, de montrer (B ==> C)

            qui est la partie gauche de la conjonction ((A ==> C) /\ (B ==> C))
              qui correspond ? l'hypoth?se [H1]

  }: on a ainsi montr? C
}: on a ainsi montr? ((A \/ B) ==> C)
Ceci ach?ve la d?monstration de (((A ==> C) /\ (B ==> C)) ==> ((A \/ B) ==> C))
```

Q6. (3 pt) Démontrez sous forme d'arbre de preuve en déduction naturelle le théorème suivant

$$\frac{}{\big(\forall x,\ \forall y,\ \ F(x) \vee\ \big(G(y) \Rightarrow F(x)\big)\big) \Longrightarrow (\forall z, G(z) \Rightarrow F(z))}$$

SOLUTION

$$\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\forall x, \forall y, F(x) \vee (G(y) \Rightarrow F(x))}^{H_1}}{H_1 \ \vdash\ \forall y, F(X_1) \vee (G(y) \Rightarrow F(X_1))}\ \forall_e(x := X_1)}{H_1 \ \vdash\ F(X_1) \vee (G(X_1) \Rightarrow F(X_1))}\ \forall_e(y := X_1) \qquad \dfrac{\overbrace{F(X_1)}^{H_3}}{F(X_1) \Rightarrow F(X_1)}\ \Rightarrow_i [H_3] \qquad \dfrac{\dfrac{\overbrace{G(X_1)}^{H_2} \quad \overbrace{G(X_1) \Rightarrow F(X_1)}^{H_4}}{H_2, H_4 \ \vdash\ F(X_1)}\ \Rightarrow_e}{H_2 \ \vdash\ (G(X_1) \Rightarrow F(X_1)) \Rightarrow F(X_1)}\ \Rightarrow_i [H_4]}{\dfrac{H_2, H_1 \ \vdash\ F(X_1)}{H_1 \ \vdash\ G(X_1) \Rightarrow F(X_1)}\ \Rightarrow_i [H_2]}\ \vee_e}{\dfrac{H_1 \ \vdash\ \forall x, G(x) \Rightarrow F(x)}{(\forall x, \forall y, F(x) \vee (G(y) \Rightarrow F(x))) \Rightarrow (\forall x, G(x) \Rightarrow F(x))}\ \Rightarrow_i [H_1]}\ \forall_i(X_1 \notin \mathscr{H} \cup \mathscr{C})$$

Q7. (3 pt) Donnez la traduction en français de cette preuve.

SOLUTION

```
Démontrons ((QQ x, (QQ y, (F(x) \/ (G(y) ==> F(x))))) ==> (QQ x, (G(x) ==> F(x)))) :
supposons (QQ x, (QQ y, (F(x) \/ (G(y) ==> F(x))))) (hypothèse [H1]) et montrons (QQ x, (G(x) ==> F(x))) :
{ Preuve de (QQ x, (G(x) ==> F(x))) :
  Pour démontrer (QQ x, (G(x) ==> F(x))) considérons un X1 quelconque
  et montrons (G(X1) ==> F(X1)).
  Pour cela, supposons G(X1) (hypothèse [H2]) et montrons F(X1) :
  { Preuve de F(X1) : exploitons la disjonction (F(X1) \/ (G(X1) ==> F(X1)))
      qui est une instance particulière (pour y:=X1) de (QQ y, (F(X1) \/ (G(y) ==> F(X1))))
        qui est une instance particulière (pour x:=X1) de (QQ x, (QQ y, (F(x) \/ (G(y) ==> F(x)))))
          qui correspond à l'hypothèse [H1]
    Comme on ne sait pas lequel des membres de la disjonction (F(X1) \/ (G(X1) ==> F(X1))) est vrai
    Pour montrer F(X1) il nous faut le prouver dans chacun des cas :
    - Cas 1: Démontrons (F(X1) ==> F(X1)) : C'est trivial.
    - Cas 2: Démontrons ((G(X1) ==> F(X1)) ==> F(X1)) :
          supposons (G(X1) ==> F(X1)) (hypothèse [H4]) et montrons F(X1) :
          c'est une conséquence directe des hypothèses H2: G(X1) et H4: (G(X1) ==> F(X1))
  }: on a ainsi montré F(X1)
}: on a ainsi montré (QQ x, (G(x) ==> F(x)))

Ceci achève la démonstration de ((QQ x, (QQ y, (F(x) \/ (G(y) ==> F(x))))) ==> (QQ x, (G(x) ==> F(x))))
```

CORRECTION FOURNIE PAR KAMIKAZE

```
open Term
open Exercice

(* Exo 1 *)

let a = Term.P "A" and b = Term.P "B" and c = Term.P "C" ;;

let exo_1 = ("1" , ((a ==> c) & (b ==> c))  ==> ( (a || b) ==> c) ) ;;

Solution.corrige (Prover.intuitionistic []) exo_1 ;;

(* Exo 2 *)

let (predicat: string -> Term.t -> Term.t) = fun p x -> Term.Pred(p,[x]) ;;

let x = Term.quantified_var "x"
and y = Term.quantified_var "y"
and z = Term.quantified_var "z" ;;

let f = predicat "F" ;;
let g = predicat "G" ;;

let exo_2 = ("2", (Qq(x, Qq(y, (f x) || ((g y) ==> (f x))))) ==> (Qq(z, (g z) ==> (f z))) ) ;;

Solution.corrige (Prover.intuitionistic []) exo_2 ;;
```

Exercice 3 : Preuve par récurrence en déduction naturelle (10 pt)

On considère le type OCAML des `asn` (arbres sans nœud) définis de la manière suivante :

```
type asn =
 | F of int
 | C of asn * asn
```

Ce type comporte deux cas : soit un `asn` est une feuille qui porte un entier, soit c'est la concaténation de deux `asn`. Puisque ces arbres n'ont pas de nœuds, on ne s'intéresse qu'à leurs feuilles. Les feuilles de l'arbre, parcourues de gauche à droite, forment une liste d'entiers.

Exemple : Les feuilles de l'arbre $\textsc{c}(\textsc{c}(\textsc{f}\,1, \textsc{f}\,2), \textsc{c}(\textsc{f}\,3, \textsc{f}\,4))$ correspondent à la liste d'entiers $([1] \,@\, [2]) \,@\, ([3] \,@\, [4])$ c'est-à-dire $[1; 2; 3; 4]$

Q8. (1.5 pt) À l'aide de l'opérateur (@), écrire en OCAML la fonction *avl* de type `asn` → `int list` qui transforme un arbre sans nœud en la liste des entiers portés par les feuilles de l'arbre.

SOLUTION

```
let rec (avl: asn -> int list) = fun asn ->
 match asn with
 | F i -> [i]
 | C (a1,a2) -> (avl a1) @ (avl a2)
;;
```

Q9. (1.5 pt) Écrire en OCAML une fonction *rev* de type `asn` → `asn`, définie par les axiomes suivants :

$Ax_1 :\quad rev\ \textsc{f}\,(n) = \textsc{f}\,(n)$

$Ax_2 :\quad rev\ \textsc{c}(x, y) = \textsc{c}(rev\ y, rev\ x)$

SOLUTION

```
let rec (rev : asn -> asn) = fun asn ->
 match asn with
 | F n -> F n
 | C (x,y) -> C(rev y, rev x)
```

Q10. (1 pt) Expliquez en une phrase ce que fait la fonction *rev*

SOLUTION

La fonction rev inverse l'ordre de la séquence des feuilles de l'arbre passé en paramètre.

Preuve par récurrence sur le type `asn` Le principe de récurrence associé au type `asn` est le suivant :

$$\frac{\forall i,\ P(\textsc{f}\,(i)) \qquad \forall a_1, \forall a_2,\ P(a_1)\ \wedge\ P(a_2) \Rightarrow P(\textsc{c}(a_1, a_2))}{\forall a \in \texttt{asn},\ P(a)}\ {}_{rec-\texttt{asn}}$$

Q11. (6 pt) Utilisez les axiomes qui définissent la fonction *rev* et le principe de récurrence associé au type `asn` pour démontrer le théorème suivant : $\forall a \in \texttt{asn},\ rev\ (rev\ (a)) = a$

$$\forall a \in \texttt{asn},\ rev\ (rev\ (a)) = a$$

$$
\dfrac{
\dfrac{
\dfrac{AX_1}{rev\ \left(rev\ \left(\mathrm{F}\left(I_0\right)\right)\right) = \mathrm{F}\left(I_0\right)}\,{\scriptstyle (i=I_0)}
}{P\left(\mathrm{F}\left(I_0\right)\right)}\,{\scriptstyle def\ P}
}{\forall n \in \texttt{nat},\ P\left(\mathrm{F}\left(n\right)\right)}\,{\scriptstyle \forall_i}
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{Ax_2\ \ avec\ x = A_1,\ y = A_2}{rev\ \left(\mathrm{C}(A_1, A_2)\right) = \mathrm{C}(rev\ \ A_2, rev\ \ A_1)}\,{\scriptstyle \forall_e}
}{rev\ \left(rev\ \left(\mathrm{C}(A_1, A_2)\right)\right) = rev\ \left(\mathrm{C}(rev\ \ A_2, rev\ \ A_1)\right)}\,{\scriptstyle app\ \ rev}
\quad
\dfrac{Ax_2\ \ avec\ x = rev\ \ A_2, y = rev\ \ A_1}{rev\ \left(\mathrm{C}(rev\ \ A_2, rev\ \ A_1)\right) = \mathrm{C}(rev\ \ rev\ \ A1, rev\ \ rev\ \ A_2)}
\quad
\dfrac{
\dfrac{\dfrac{Hrec}{P(A_1)}\,{\scriptstyle \wedge_{e_1}}}{rev\ \ rev\ \ A_1 = A_1}\,{\scriptstyle def\ \ P}
\quad
\dfrac{\dfrac{Hrec}{P(A_2)}\,{\scriptstyle \wedge_{e_2}}}{rev\ \ rev\ \ A_2 = A_2}\,{\scriptstyle def\ \ P}
}{\mathrm{C}(rev\ \ rev\ \ A1, rev\ \ rev\ \ A_2) = \mathrm{C}(A_1, A_2)}\,{\scriptstyle app\ \mathrm{C}}
}{rev\ \left(rev\ \left(\mathrm{C}(A_1, A_2)\right)\right) = \mathrm{C}(A_1, A_2)}\,{\scriptstyle =_{trans}}
}{P(\mathrm{C}(A_1, A_2))}\,{\scriptstyle def\ \ P}
}{P(A_1)\ \wedge\ P(A_2) \Rightarrow P(\mathrm{C}(A_1, A_2))}\,{\scriptstyle \Rightarrow_i [Hrec]}
}{\forall a_2,\ P(A_1)\ \wedge\ P(a_2) \Rightarrow P(\mathrm{C}(A_1, a_2))}\,{\scriptstyle \forall_i\ \ A_2 \notin conc}
}{\forall a_1,\ \forall a_2,\ P(a_1)\ \wedge\ P(a_2) \Rightarrow P(\mathrm{C}(a_1, a_2))}\,{\scriptstyle \forall_i\ \ A_1 \notin conc}
}{\forall a \in \texttt{asn},\ rev\ \ (rev\ \ (a)) = a}\,{\scriptstyle rec-\texttt{asn}\ avec\ P(a) \overset{def}{=} rev\ \ (rev\ \ (a)) = a}
$$

Exercice 4 : Preuves en déduction naturelle (10 pt)

Q12. (3 pt) Démontrez à l'aide d'une preuve en déduction naturelle le théorème suivant :

$$\frac{}{\big(\forall x,\ P(x)\ \wedge\ Q(x)\big) \Longrightarrow \big(\exists y,\ P(y)\big)}$$

SOLUTION

$$\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\forall x, P(x)\ \wedge\ Q(x)}^{H_1}}{H_1\ \vdash\ P(?_3)\ \wedge\ Q(?_3)}\ \forall_e(x := ?_3)}{H_1\ \vdash\ P(?_3)}\ \wedge_{e_1}}{H_1\ \vdash\ \exists y, P(y)}\ \exists_i}{(\forall x, P(x)\ \wedge\ Q(x)) \Rightarrow (\exists y, P(y))}\ \Rightarrow_i [H_1]$$

Q13. (4 pt) Démontrez à l'aide d'une preuve en déduction naturelle le théorème suivant :

$$\frac{}{\big(\exists x,\ \forall y,\ R(x,y)\big) \Longrightarrow \big(\forall u,\ \exists v,\ R(v,u)\big)}$$

La preuve suivante recontrée dans de nombreuse est incorrecte car la condition $X_2 \notin \mathscr{H} \cup \mathscr{C})$ n'est pas respectée.

$$\dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\exists x, (\forall y, x\ R\ y)}^{H_1} \qquad \dfrac{\dfrac{\dfrac{\overbrace{\forall y, X_2\ R\ y}^{H_3}}{H_3\ \vdash\ X_2\ R\ U_1}\ \forall_e(y := U_1)}{(\forall y, X_2\ R\ y) \Rightarrow (X_2\ R\ U_1)}\ \Rightarrow_i [H_3]}{\forall x, (\forall y, x\ R\ y) \Rightarrow (X_2\ R\ U_1)}\ \forall_i(X_2 \notin \{H_1\} \cup \mathscr{C})}{H_1\ \vdash\ X_2\ R\ U_1}\ \exists_e}{H_1\ \vdash\ \exists v, (v\ R\ U_1)}\ \exists_i}{H_1\ \vdash\ \forall u, \exists v, (v\ R\ u)}\ \forall_i(U_1 \notin \mathscr{H} \cup \mathscr{C})}{(\exists x, (\forall y, x\ R\ y)) \Rightarrow (\forall u, \exists v, (v\ R\ u))}\ \Rightarrow_i [H_1]$$

SOLUTION

$$\dfrac{\dfrac{\dfrac{\overbrace{\exists x, (\forall y, x\ R\ y)}^{H_1} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overbrace{\forall y, X_2\ R\ y}^{H_3}}{H_3\ \vdash\ X_2\ R\ U_1}\ \forall_e(y := U_1)}{H_3\ \vdash\ \exists v, v\ R\ U_1}\ \exists_i}{(\forall y, X_2\ R\ y) \Rightarrow (\exists v, v\ R\ U_1)}\ \Rightarrow_i [H_3]}{\forall x, (\forall y, x\ R\ y) \Rightarrow (\exists v, v\ R\ U_1)}\ \forall_i(X_2 \notin \{H_1\} \cup \mathscr{C})}{H_1\ \vdash\ \exists v, v\ R\ U_1}\ \exists_e}{H_1\ \vdash\ \forall u, \exists v, (v\ R\ u)}\ \forall_i(U_1 \notin \mathscr{H} \cup \mathscr{C})}{(\exists x, (\forall y, x\ R\ y)) \Rightarrow (\forall u, \exists v, (v\ R\ u))}\ \Rightarrow_i [H_1]$$

Q14. (3 pt) Utilisez la règle du tiers-exclu pour démontrer le théorème suivant :

$$\dfrac{}{\big(A \Rightarrow B\big) \ \vee \ \big((\neg A) \Rightarrow B\big)}$$

SOLUTION

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$\frac{1}{3}$ ex}
\UnaryInfC{$A \vee \neg A$}
\AxiomC{$\overbrace{A}^{H_1}$}
\AxiomC{$\overbrace{\neg A}^{H_3}$}
\RightLabel{$^{def\ neg}$}
\UnaryInfC{$H_3 \ \vdash \ A \Rightarrow \bot$}
\RightLabel{$\Rightarrow_e$}
\BinaryInfC{$H_1, H_3 \ \vdash \ \bot$}
\RightLabel{$\bot_e$}
\UnaryInfC{$H_1, H_3 \ \vdash \ B$}
\RightLabel{$\Rightarrow_i$ $[H_3]$}
\UnaryInfC{$H_1 \ \vdash \ \neg A \Rightarrow B$}
\RightLabel{$\vee_{i_2}$}
\UnaryInfC{$H_1 \ \vdash \ (A \Rightarrow B) \vee (\neg A \Rightarrow B)$}
\RightLabel{$\Rightarrow_i$ $[H_1]$}
\UnaryInfC{$A \Rightarrow ((A \Rightarrow B) \vee (\neg A \Rightarrow B))$}
\AxiomC{$\overbrace{A}^{H_5}$}
\AxiomC{$\overbrace{\neg A}^{H_4}$}
\RightLabel{$^{def\ neg}$}
\UnaryInfC{$H_4 \ \vdash \ A \Rightarrow \bot$}
\RightLabel{$\Rightarrow_e$}
\BinaryInfC{$H_5, H_4 \ \vdash \ \bot$}
\RightLabel{$\bot_e$}
\UnaryInfC{$H_5, H_4 \ \vdash \ B$}
\RightLabel{$\Rightarrow_i$ $[H_5]$}
\UnaryInfC{$H_4 \ \vdash \ A \Rightarrow B$}
\RightLabel{$\vee_{i_1}$}
\UnaryInfC{$H_4 \ \vdash \ (A \Rightarrow B) \vee (\neg A \Rightarrow B)$}
\RightLabel{$\Rightarrow_i$ $[H_4]$}
\UnaryInfC{$\neg A \Rightarrow ((A \Rightarrow B) \vee (\neg A \Rightarrow B))$}
\RightLabel{$\vee_e$}
\TrinaryInfC{$(A \Rightarrow B) \vee (\neg A \Rightarrow B)$}
\end{prooftree}
$$

Exercice 5 : Preuve de propriétés des ensembles (10 pt)

Q15. (2 pt) Démontrez à l'aide d'une preuve en déduction naturelle que la règle de déduction suivante est correcte :

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

Q16. (4 pt) Utilisez les règles de la déduction naturelle et les règles de déduction sur les ensembles pour montrer le théorème suivant :

$$\dfrac{}{\big((A \cup B) \subseteq (A \cap B)\big) \Longrightarrow (A \subseteq B)}$$

SOLUTION

$$
\dfrac{
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{
\dfrac{\dfrac{\overbrace{X_1 \in E}^{H_2}}{H_2 \vdash (X_1 \in E) \vee (X_1 \in F)}\,\vee_{i_1}}{H_2 \vdash X_1 \in (E \cup F)}\,{}_{def}\in
\qquad
\dfrac{\dfrac{\overbrace{(E \cup F) \subseteq (E \cap F)}^{H_1}}{H_1 \vdash \forall x, (x \in (E \cup F)) \Rightarrow (x \in (E \cap F))}\,{}_{def}\subseteq}{H_1 \vdash (X_1 \in (E \cup F)) \Rightarrow (X_1 \in (E \cap F))}\,\forall_e(x := X_1)
}{H_2, H_1 \vdash X_1 \in (E \cap F)}\,\Rightarrow_e
}{H_2, H_1 \vdash (X_1 \in E) \wedge (X_1 \in F)}\,{}_{def}\in
}{H_2, H_1 \vdash X_1 \in F}\,\wedge_{e_2}
}{H_1 \vdash (X_1 \in E) \Rightarrow (X_1 \in F)}\,\Rightarrow_i [H_2]
}{H_1 \vdash \forall x, (x \in E) \Rightarrow (x \in F)}\,\forall_i(X_1 \notin \mathscr{H} \cup \mathscr{C})
}{H_1 \vdash E \subseteq F}\,{}_{def}\subseteq
}{((E \cup F) \subseteq (E \cap F)) \Rightarrow (E \subseteq F)}\,\Rightarrow_i [H_1]
$$

Q17. (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 suivant :

$$
\dfrac{}{\big((A \cup B) \subseteq \emptyset\big) \Longrightarrow A = \emptyset}
$$

SOLUTION

```
open Term
open Exercice
(*
```


$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{\overbrace{X_1 \in E}^{H_2}}{H_2 \vdash (X_1 \in E) \vee (X_1 \in F)}\,\vee_{i_1}
}{H_2 \vdash X_1 \in (E \cup F)}\,\mathit{def :}
\qquad
\dfrac{
\dfrac{\overbrace{(E \cup F) \subseteq \emptyset}^{H_1}}{H_1 \vdash \forall x, (x \in (E \cup F)) \Rightarrow (x \in \emptyset)}\,\mathit{def\ inclus}
}{H_1 \vdash (X_1 \in (E \cup F)) \Rightarrow (X_1 \in \emptyset)}\,\forall_e(x := X_1)
}{H_2, H_1 \vdash X_1 \in \emptyset}\,\Rightarrow_e
}{H_1 \vdash (X_1 \in E) \Rightarrow (X_1 \in \emptyset)}\,\Rightarrow_i [H_2]
}{H_1 \vdash \forall x, (x \in E) \Rightarrow (x \in \emptyset)}\,\forall_i(X_1 \notin \mathscr{H} \cup \mathscr{C})
}{H_1 \vdash E \subseteq \emptyset}\,\mathit{def\ inclus}
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{\overbrace{X_2 \in \emptyset}^{H_3}}{H_3 \vdash \bot}\,\mathit{def :}
}{H_3 \vdash X_2 \in E}\,\bot_e
}{(X_2 \in \emptyset) \Rightarrow (X_2 \in E)}\,\Rightarrow_i [H_3]
}{\forall x, (x \in \emptyset) \Rightarrow (x \in E)}\,\forall_i(X_2 \notin \mathscr{H} \cup \mathscr{C})
}{\emptyset \subseteq E}\,\mathit{def\ inclus}
}{H_1 \vdash (E \subseteq \emptyset) \wedge (\emptyset \subseteq E)}\,\wedge_i
}{H_1 \vdash E =_{ens} \emptyset}\,\mathit{def\ =ens=}
}{((E \cup F) \subseteq \emptyset) \Rightarrow (E =_{ens} \emptyset)}\,\Rightarrow_i [H_1]
$$

```

(* Exo 1 *)

let (predicat: string -> Term.t -> Term.t) = fun p x -> Term.Pred(p,[x]) ;;

let x = Term.quantified_var "x" and y = Term.quantified_var "y" ;;
let p = predicat "P" ;;
let q = predicat "Q" ;;

let exo_1 = ("1" , ( Term.Qq(x, (p x) & (q x)) ) ==> ( Term.Ex(y, p y)) ) ;;

Solution.corrige (Prover.intuitionistic []) exo_1 ;;

(* Exo 2 *)

let r = fun x y -> Term.Pred("R",[x;y]) ;;

let x = Term.quantified_var "x"
and y = Term.quantified_var "y"
and u = Term.quantified_var "u"
and v = Term.quantified_var "v" ;;

let exo_2 = ("2", (Term.Ex(x, Term.Qq(y, (r x y)))) ==> (Term.Qq(u, Term.Ex(v, r v u))) ) ;;

Solution.corrige (Prover.intuitionistic []) exo_2 ;;


(* Exo 3 *)

let a = Term.P "A" and b = Term.P "B" ;;

let exo_3 = ("3", (a ==> b) || ((non a) ==> b) ) ;;

let prover_3 =
  (Ou.elim
     (Axiom.exploit (Proof.AXM("1/3ex", a || (non a))))
     (Prover.intuitionistic [])
     (Prover.intuitionistic [])
  )
in
  Solution.corrige prover_3 exo_3 ;;

*)

(* Exo 4 *)

let vide = S "{}" ;;

(* On donne les définitions nécessaires pour travailler sur des ensembles *)

let definitions_ensemble =
  [
   (":", function
     | [x ; S "{}"] ->
             (Pred(":",[x; S "{}"])) =$= False
     | [x ; Op("U",[e;f]) ] ->
             (Pred(":",[x ; Op("U",[e;f])]) ) =$= (Ou(Pred(":",[x;e]) , Pred(":",[x;f])))
     | [x ; Op("inter",[e;f])] ->
             (Pred(":",[x ; Op("inter",[e;f])])) =$= (Et( Pred(":",[x;e]) , Pred(":",[x;f])))
     | [x ; e] ->
             let error = Term.Error (String.concat "" ["no definition for" ; Term.pretty (Pred(":",[x;e]))])
```

```
             in error =$= error
    );

    ("inclus", function [e;f] ->
          ( Pred("inclus",[e;f]) )
            =$=
          ( let x = quantified_var "x" in Qq(x, Impl(Pred(":",[x;e]) , Pred(":",[x;f]))) )
    );

    ("=ens=", function [e;f] ->
          ( Pred("=ens=",[e;f]) )
            =$=
          ( Et(Pred("inclus",[e;f]), Pred("inclus",[f;e])) )
    );

  ] ;;

(* On ajoute ces définitions aux définitions existantes *)

_THE_DEFINITIONS_ :=  definitions_ensemble @ !(_THE_DEFINITIONS_) ;;

let inclus = fun e1 e2 -> Term.Pred("inclus",[e1;e2]) ;;
let union  = fun e1 e2 -> Term.Op("U",[e1;e2]) ;;
let inter  = fun e1 e2 -> Term.Op("inter",[e1;e2]) ;;

let e = Term.S "E" and f = Term.S "F" ;;

let exo_4 = ("4", (inclus (union e f) (inter e f)) ==> (inclus e f) ) ;;

Solution.corrige (Prover.intuitionistic []) exo_4 ;;

let exo_5 = ("5", (inclus (union e f) vide) ==> (Pred("=ens=",[e;vide])) ) ;;

Solution.corrige (Prover.intuitionistic []) exo_5 ;;
```

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

Q18. (2 pt) Donnez le schéma de récurrence associé au type `abint` défini par :

```
type abint =
 | Avide
 | Ab of abint * int * abint
```

SOLUTION

$$\frac{P(\text{AVIDE}) \quad \forall a_1, a_2,\ P(a_1)\ \wedge\ P(a_2) \Rightarrow (\forall n,\ P(\text{AB}(a_1, n, a_2)))}{\forall a \in \texttt{abint},\ P(a)}\ {\scriptstyle rec-abint}$$

Q19. (2 pt) Complétez le schéma de récurrence associé au type `pos` défini par :

```
type pos =
  | U
  | O of pos
  | E of pos
```

$$\frac{\boxed{Q(U)} \quad \boxed{\forall p,\ Q(p) \Rightarrow Q(O(p))} \quad \boxed{\forall p,\ Q(p) \Rightarrow Q(E(p))}}{\forall p \in \texttt{pos},\ Q(p)}\ \textit{rec-pos}$$

Q20. (2 pt) Complétez le schéma de récurrence associé au type `machin` défini par :

```
type machin =
  | A
  | B of bool
  | C of int
```

$$\frac{\boxed{P(A)} \quad \boxed{\forall b \in \texttt{bool},\ P(b)} \quad \boxed{\forall i \in \texttt{int},\ P(i)}}{\forall m \in \texttt{machin},\ P(m)}\ \textit{rec-machin}$$

Exercice 7 : Équivalence entre deux régles (10 pt)

Le but de cet exercice est de démontrez que les règle du tiers-exclu est de l'élimation de la double négation sont équivalentes.

Q21. (2 pt) Expliquez comment on doit procéder pour démontrer une telle chose ?

SOLUTION

Il faut démontrer que chaque règle est un conséquence de l'autre. Il faut donc montrer deux choses :

- *d'une part qu'on peut démontrer la conclusion de la règle du $\frac{1}{3}ex$ en utilisant la règle $\neg\neg E$ et les autres règles de la déduction naturelle.*
- *d'autre part il faut démontrer la réciproque, c'est-à-dire démontrer la conclusion de la règle $\neg\neg E$ en utilisant la règle du $\frac{1}{3}ex$ et les autres règles de la déduction naturelle.*

Q22. (4 pt) Faîtes la preuve que la régle du $\frac{1}{3}ex$ est une conséquence de la règle $\neg\neg E$.

SOLUTION

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{\overbrace{\neg A}^{H_5}}{H_5 \;\vdash\; A \vee \neg A}\;{\vee_{i_2}}
          \qquad
          \dfrac{\overbrace{\neg(A \vee \neg A)}^{H_4}}{H_4 \;\vdash\; (A \vee \neg A) \Rightarrow \bot}\;{\scriptstyle def\ \neg}
        }{H_5, H_4 \;\vdash\; \bot}\;{\Rightarrow_e}
      }{H_4 \;\vdash\; \neg A \Rightarrow \bot}\;{\Rightarrow_i [H_5]}
    }{H_4 \;\vdash\; A}\;{\neg\neg_e}
  }{H_4 \;\vdash\; A \vee \neg A}\;{\vee_{i_1}}
  \qquad
  \dfrac{\overbrace{\neg(A \vee \neg A)}^{H_4}}{H_4 \;\vdash\; (A \vee \neg A) \Rightarrow \bot}\;{\scriptstyle def\ \neg}
}{
  \dfrac{
    \dfrac{H_4 \;\vdash\; \bot}{\neg(A \vee \neg A) \Rightarrow \bot}\;{\Rightarrow_i [H_4]}
  }{A \vee \neg A}\;{\neg\neg_e}
}\;{\Rightarrow_e}
$$

Q23. (4 pt) Faîtes la preuve réciproque.

SOLUTION

$$
\dfrac{
  \dfrac{}{A \vee \neg A}\;{\scriptstyle \text{AX}\ (tiers-exclu)}
  \qquad
  \dfrac{
    \dfrac{\overbrace{A}^{H_1}}{H_1 \;\vdash\; \neg\neg A \Rightarrow A}\;{\Rightarrow_i [H_2]}
  }{A \Rightarrow (\neg\neg A \Rightarrow A)}\;{\Rightarrow_i [H_1]}
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \overbrace{\neg A}^{H_3}
          \quad
          \dfrac{\overbrace{\neg\neg A}^{H_4}}{H_4 \;\vdash\; \neg A \Rightarrow \bot}\;{\scriptstyle def\ \neg}
        }{H_3, H_4 \;\vdash\; \bot}\;{\Rightarrow_e}
      }{H_3, H_4 \;\vdash\; A}\;{\bot_e}
    }{H_3 \;\vdash\; \neg\neg A \Rightarrow A}\;{\Rightarrow_i [H_4]}
  }{\neg A \Rightarrow (\neg\neg A \Rightarrow A)}\;{\Rightarrow_i [H_3]}
}{\neg\neg A \Rightarrow A}\;{\vee_e}
$$

CORRECTION FOURNIE PAR KAMIKAZE

```
open Term
open Exercice

let a = Term.P "A" ;;
Solution.corrige (Prover.classic []) ("1", a || (non a)) ;;

let prover_tiers_exclu =
  (Ou.elim
     (Axiom.exploit (Proof.AXM("tiers-exclu", a || (non a))))
     (Prover.intuitionistic [])
     (Prover.intuitionistic [])
  )
in
  Solution.corrige prover_tiers_exclu ("2", (non (non a)) ==> a) ;;
```