NUMÉRO ANONYMAT ....

INF122 2008-2009

Examen final, session de mai   Corrigé

La durée prévue pour l'ensemble de l'épreuve est de 120 minutes. Les parties A et B comptent respectivememt pour $\frac{8}{20}$ et $\frac{12}{20}$ des points. La partie B est à rendre sur le présent sujet. Le barème est indicatif.

Pour tous les exercices, il s'agit de démontrer un théorème en déduction naturelle en écrivant un arbre de preuve *correct* : bien noter le nom de chacune des règles utilisées et, le cas échéant, les hypothèses levées.

On autorise (et recommande...) l'utilisation des résultats des exercices de numéro strictement inférieur au numéro de l'exercice en cours, même si ces exercices ne sont pas résolus.

Exercice 1   (2 pt)

$$
\begin{prooftree}
\AxiomC{$\overbrace{x \in A_0}^{[1]}$}
\AxiomC{$\overbrace{x \in A_0}^{[1]}$}
\doubleLine
\RightLabel{$\vee_{\mathrm{I2}}\cup$}
\UnaryInfC{$x \in A_0 \cup B_0$}
\doubleLine
\RightLabel{$\wedge_{\mathrm{I}}\cap$}
\BinaryInfC{$x \in A_0 \cap (A_0 \cup B_0)$}
\doubleLine
\RightLabel{$\Rightarrow_{\mathrm{I}}\forall_{\mathrm{I}}\subseteq[1]$}
\UnaryInfC{$A_0 \subseteq A_0 \cap (A_0 \cup B_0)$}
\RightLabel{$\forall_{\mathrm{I}}$}
\UnaryInfC{$\forall B\ A_0 \subseteq A_0 \cap (A_0 \cup B)$}
\RightLabel{$\forall_{\mathrm{I}}$}
\UnaryInfC{$\forall A\ \forall B\ A \subseteq A \cap (A \cup B)$}
\end{prooftree}
$$

Exercice 2   (2,5 pts)

Indication : Cherchez à obtenir la contradiction $\perp$ en démontrant $\neg(Q \vee \neg P)$.

$$
\begin{prooftree}
\AxiomC{$\overbrace{\neg\neg(Q \vee \neg P)}^{[2]}$}
\AxiomC{$\overbrace{Q \vee \neg P}^{[4]}$}
\AxiomC{$\overbrace{\neg Q}^{[3]}$}
\AxiomC{$\overbrace{Q}^{[5]}$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{$\perp$}
\AxiomC{$\overbrace{\neg P}^{[6]}$}
\AxiomC{$\overbrace{P}^{[1]}$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{$\perp$}
\RightLabel{$\vee_{\mathrm{E}}[5,6]$}
\TrinaryInfC{$\perp$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[4]$}
\UnaryInfC{$\neg(Q \vee \neg P)$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{$\perp$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[3]$}
\UnaryInfC{$\neg\neg Q$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[2]$}
\UnaryInfC{$\neg\neg(Q \vee \neg P) \Rightarrow \neg\neg Q$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[1]$}
\UnaryInfC{$P \Rightarrow [\neg\neg(Q \vee \neg P) \Rightarrow \neg\neg Q]$}
\end{prooftree}
$$

Exercice 3 (3 pts)

On pose $B \overset{\text{déf}}{\equiv} (A \Rightarrow Q) \vee \exists\, x\ P(x)$.

\begin{prooftree}
\AxiomC{$\overbrace{A}^{[3]}$}
\AxiomC{$\overbrace{A \Rightarrow (\forall x\ [P(x) \Rightarrow Q]) \Rightarrow Q}^{[1]}$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{$(\forall x\ [P(x) \Rightarrow Q]) \Rightarrow Q$}
\AxiomC{$\overbrace{P(x_0)}^{[4]}$}
\RightLabel{$\exists_{\mathrm{I}}$}
\UnaryInfC{$\exists\, x\ P(x)$}
\RightLabel{$\vee_{\mathrm{I}2}$}
\UnaryInfC{B}
\AxiomC{$\overbrace{B \Rightarrow Q}^{[2]}$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{Q}
\RightLabel{$\Rightarrow_{\mathrm{I}}[4]$}
\UnaryInfC{$P(x_0) \Rightarrow Q$}
\RightLabel{$\forall_{\mathrm{I}}$}
\UnaryInfC{$\forall x\ [P(x) \Rightarrow Q]$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{Q}
\RightLabel{$\Rightarrow_{\mathrm{I}}[3]$}
\UnaryInfC{$A \Rightarrow Q$}
\RightLabel{$\vee_{\mathrm{I}1}$}
\UnaryInfC{B}
\AxiomC{$\overbrace{B \Rightarrow Q}^{[2]}$}
\RightLabel{$\Rightarrow_{\mathrm{E}}$}
\BinaryInfC{Q}
\RightLabel{$\Rightarrow_{\mathrm{I}}[2]$}
\UnaryInfC{$\big(B \Rightarrow Q\big) \Rightarrow Q$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[1]$}
\UnaryInfC{$\big(A \Rightarrow (\forall x\ [P(x) \Rightarrow Q]) \Rightarrow Q\big) \Rightarrow \big(B \Rightarrow Q\big) \Rightarrow Q$}
\end{prooftree}

Les trois exercices suivants ont pour but de démontrer l'existence de la division euclidienne par 2. On pose $D2(n,q) \overset{\text{déf}}{\equiv} (n = q+q) \vee (S(n) = q+q)$ et $div2(n,q) \overset{\text{déf}}{\equiv} (n = q+q) \vee (n = S(q+q))$

Exercice 4 (2,5 pts)

Indication : ne pas utiliser de récurrence.

\begin{prooftree}
\AxiomC{$\overbrace{\forall m\ \exists q_1, D2(m,q_1)}^{[1]}$}
\RightLabel{$\forall_{\mathrm{E}}(\frac{m}{S(n_0)})$}
\UnaryInfC{$\exists q_1, D2(S(n_0),q_1)$}
\AxiomC{$\overbrace{D2(S(n_0),q_2)}^{[2]}$}
\AxiomC{$\overbrace{S(n_0) = q_2 + q_2}^{[3]}$}
\AxiomC{}
\RightLabel{$=_{\mathrm{I}}$}
\UnaryInfC{$S(S(n_0)) = S(S(n_0))$}
\RightLabel{$=_{\mathrm{E}}$}
\BinaryInfC{$S(S(n_0)) = S(q_2 + q_2)$}
\RightLabel{$\vee_{\mathrm{I}2}$}
\UnaryInfC{$div2(S(S(n_0)),q_2)$}
\AxiomC{$\overbrace{S(S(n_0)) = q_2 + q_2}^{[4]}$}
\RightLabel{$\vee_{\mathrm{I}1}$}
\UnaryInfC{$div2(S(S(n_0)),q_2)$}
\RightLabel{$\vee_{\mathrm{E}}[3,4]$}
\TrinaryInfC{$div2(S(S(n_0)),q_2)$}
\RightLabel{$\exists_{\mathrm{I}}$}
\UnaryInfC{$\exists q, div2(S(S(n_0)),q)$}
\RightLabel{$\exists_{\mathrm{E}}[2]$}
\BinaryInfC{$\exists q, div2(S(S(n_0)),q)$}
\RightLabel{$\forall_{\mathrm{I}}$}
\UnaryInfC{$\forall n\ \exists q, div2(S(S(n)),q)$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[1]$}
\UnaryInfC{$[\forall m\ \exists q_1, D2(m,q_1)] \Rightarrow [\forall n\ \exists q, div2(S(S(n)),q)]$}
\end{prooftree}

Exercice 5 (2,5 pts)

Indication : par récurrence sur m.

On pose $Q_n(m) \overset{\text{déf}}{\equiv} S(n)+m = S(n+m)$

$$\mathcal{Q}_0 \left\{ \begin{array}{ll} & S(n)+0 \\ = & \qquad \{+0 \text{ avec } \frac{n}{S(n)}\} \\ & S(n) \\ = & \qquad \{+0 \text{ avec } \frac{n}{n}\} \\ & S(n+0) \end{array}\right.$$

$$\mathcal{Q}_S \left\{ \begin{array}{ll} & S(n)+S(p) \\ = & \qquad \{+\text{S avec } \frac{n}{S(n)} \text{ et } \frac{m}{p}\} \\ & S(S(n)+p) \\ = & \qquad \{\text{hypothèse de récurrence } hrec\} \\ & S(S(n+p)) \\ = & \qquad \{+\text{S avec } \frac{n}{n} \text{ et } \frac{m}{p}\} \\ & S(n+S(p)) \end{array}\right.$$

\begin{prooftree}
\AxiomC{}
\RightLabel{$\mathcal{Q}_0$}
\doubleLine
\UnaryInfC{$S(n)+0=S(n+0)$}
\AxiomC{$\overbrace{S(n)+p=S(n+p)}^{[hrec]}$}
\RightLabel{$\mathcal{Q}_S$}
\doubleLine
\UnaryInfC{$S(n)+S(p)=S(n+S(p))$}
\RightLabel{$\Rightarrow_{\mathrm{I}}[hrec]$}
\UnaryInfC{$Q_n(p)\Rightarrow Q_n(S(p))$}
\RightLabel{$\forall_{\mathrm{I}}$}
\UnaryInfC{$\forall m\ Q_n(m)\Rightarrow Q_n(S(m))$}
\RightLabel{nat-rec[$hrec$]}
\BinaryInfC{$\forall m\ S(n)+m=S(n+m)$}
\RightLabel{$\forall_{\mathrm{I}}$}
\UnaryInfC{$\forall n\ \forall m\ S(n)+m=S(n+m)$}
\end{prooftree}

Exercice 6 (3 pts)

$$\mathcal{Q}_2 \left\{ \begin{array}{ll} & S(S(m)) \\ = & \qquad \{\text{hypothèse 2}\} \\ & S(S(q_2+q_2)) \\ = & \qquad \{+\text{S avec } \frac{n}{q_2} \text{ et } \frac{m}{q_2}\} \\ & S(q_2+S(q_2)) \\ = & \qquad \{\text{exercice 4 avec } \frac{n}{q_2} \text{ et } \frac{m}{S(q_2)}\} \\ & S(q_2)+S(q_2) \end{array}\right.$$

\begin{prooftree}
\AxiomC{}
\RightLabel{$+0$}
\UnaryInfC{$\forall n\ \ n+0=n$}
\RightLabel{$\forall_{\mathrm{E}}(\frac{n}{0})$}
\UnaryInfC{$0+0=0$}
\RightLabel{$\vee_{\mathrm{I1}}$}
\UnaryInfC{$D2(0,0)$}
\RightLabel{$\exists_{\mathrm{I}}$}
\UnaryInfC{$\exists q_1, D2(0,q_1)$}
\AxiomC{$\overbrace{\exists q1, D2(m,q_1)}^{[hrec]}$}
\AxiomC{$\overbrace{D2(m,q_2)}^{[1]}$}
\AxiomC{$\overbrace{m=q_2+q_2}^{[2]}$}
\RightLabel{$\mathcal{Q}_2$}
\doubleLine
\UnaryInfC{$S(S(m))=S(q_2)+S(q_2)$}
\RightLabel{$\vee_{\mathrm{I2}}$}
\UnaryInfC{$D2(S(m),S(q_2))$}
\RightLabel{$\exists_{\mathrm{I}}$}
\UnaryInfC{$\exists q1, D2(S(m),q1)$}
\AxiomC{$\overbrace{S(m)=q_2+q_2}^{[3]}$}
\RightLabel{$\vee_{\mathrm{I1}}$}
\UnaryInfC{$D2(S(m),q_2)$}
\RightLabel{$\exists_{\mathrm{I}}$}
\UnaryInfC{$\exists q1, D2(S(m),q1)$}
\RightLabel{$\vee_{\mathrm{E}}[2,3]$}
\TrinaryInfC{$\exists q1, D2(S(m),q1)$}
\RightLabel{$\exists_{\mathrm{E}}[1]$}
\BinaryInfC{$\exists q1, D2(S(m),q1)$}
\RightLabel{nat-rec[$hrec$]}
\BinaryInfC{$\forall m\ \exists q_1, D2(m,q_1)$}
\end{prooftree}

Exercice 7 (4,5 pts)

Soit $R \subseteq \mathbb{N}^* \times \mathbb{N}^*$ la relation sur l'ensemble des entiers naturels différents de 0, définie par $R \overset{\text{déf}}{\equiv} \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid pgcd(m,n) = 1\}$ c-à-d. les paires d'entiers (m,n) qui sont différents de 0 et tels que leur plus grand diviseur commun est 1.

Indiquer les propriétés de la relation R en mettant des croix dans le tableau suivant et donnez un contre-exemple si vous répondez non :

	oui	non	contre-exemple
réflexive		x	
symétrique	x		
antisymétrique		x	
transitive		x	
relation d'équivalence		x	
relation d'ordre		x	

On définit R^k, la "composition k fois" de la relation R avec elle même comme suit :

$$R^1 \overset{\text{déf}}{\equiv} R \qquad (p_1)$$

$$\forall k \in \mathbb{N},\ R^{k+1} \overset{\text{déf}}{\equiv} R^k \circ R \qquad (p_r)$$

Donner la relation R^2 (Indice : "que peut-on dire de $pgcd(1,m)$ et $pgcd(m,1)$ pour tout $m \in \mathbb{N}^*$?").

$$\begin{array}{rcl}
\mathbb{N}^* \times \mathbb{N}^* \supseteq R^2 & \overset{p_r}{=} & R^1 \circ R \overset{p_1}{=} R \circ R \\
& = & \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid \exists p \in \mathbb{N}^*, (m,p) \in R \wedge (p,n) \in R\} \\
& = & \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid \exists p \in \mathbb{N}^*, pgcd(m,p) = 1 \wedge pgcd(p,n) = 1\} \\
& \supseteq & \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid pgcd(m,1) = 1 \wedge pgcd(1,n) = 1\} \\
& = & \mathbb{N}^* \times \mathbb{N}^*
\end{array}$$

donc, $R^2 = \mathbb{N}^* \times \mathbb{N}^*$.

Montrer que $R^3 = R^2$.

$$\begin{array}{rcl}
\mathbb{N}^* \times \mathbb{N}^* \supseteq R^3 & \overset{p_r}{=} & R^2 \circ R \\
& = & \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid \exists p \in \mathbb{N}^*, (m,p) \in R^2 \wedge (p,n) \in R\} \\
& = & \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid \exists p \in \mathbb{N}^*, pgcd(p,n) = 1\} \\
& \supseteq & \{(m,n) \in \mathbb{N}^* \times \mathbb{N}^* \mid pgcd(1,n) = 1\} \\
& = & \mathbb{N}^* \times \mathbb{N}^*
\end{array}$$

donc, $R^3 = \mathbb{N}^* \times \mathbb{N}^* = R^2$.

Montrer (sans arbre de preuve!) par récurrence sur k que $\forall k \in \mathbb{N},\ R^{k+2} = R^2$.

On pose $P(k) \overset{\text{déf}}{\equiv} R^{k+2} = R^2$. Alors $P(0) \equiv R^{0+2} = R^2 \overset{arith}{\Leftrightarrow} R^2 = R^2$.
Pour le pas inductif. Supposons $P(k)$.
Alors
$P(k+1) \equiv R^{k+1+2} = R^2 \overset{arith}{\Leftrightarrow} R^{k+2+1} = R^2 \overset{p_r}{\Leftrightarrow} R^{k+2} \circ R = R^2 \overset{hyp\_rec}{\Leftrightarrow} R^2 \circ R = R^2 \overset{p_r}{\Leftrightarrow} R^{2+1} = R^2 \overset{arith}{\Leftrightarrow} R^3 = R^2$.
