Nb : Les exercices 1 et 2 seront rédigés sur des feuilles séparées. Par ailleurs, on pourra admettre tout résultat intermédiaire afin de poursuivre la résolution d'un exercice.

Exercice 1 *Logique*

1.1 *Première partie*

Étant données les formules $\phi_1, \phi_2, \cdots, \phi_n, \psi$ du calcul des propositions, prouver que $\phi_1, \phi_2, \cdots, \phi_n \models \psi$ si et seulement si $\models \phi_1 \rightarrow (\phi_2 \rightarrow \cdots \rightarrow (\phi_n \rightarrow \psi)...)$. Nous rappelons que le symbole $\models$ représente la conséquence logique et que $\models \varphi$ signifie que la formule φ est valide.

Indications :

- La preuve de :

  $$\textbf{\textit{si}} \quad \models \phi_1 \rightarrow (\phi_2 \rightarrow \cdots \rightarrow (\phi_n \rightarrow \psi)...) \quad \textbf{\textit{alors}} \quad \phi_1, \phi_2, \cdots, \phi_n \models \psi$$

  se fait facilement en supposant qu'une certaine valuation rend vraies toutes les formules $\phi_1, \phi_2, \cdots, \phi_n$ et en voyant ce qu'on peut dire de ψ compte tenu du fait qu'on suppose $\models \phi_1 \rightarrow (\phi_2 \rightarrow \cdots \rightarrow (\phi_n \rightarrow \psi)...)$.
- La preuve de :

  $$\textbf{\textit{si}} \quad \phi_1, \phi_2, \cdots, \phi_n \models \psi \quad \textbf{\textit{alors}} \quad \models \phi_1 \rightarrow (\phi_2 \rightarrow \cdots \rightarrow (\phi_n \rightarrow \psi)...)$$

  se fait facilement par contradiction : on commence par supposer qu'une certaine valuation rend fausse la formule $\phi_1 \rightarrow (\phi_2 \rightarrow \cdots \rightarrow (\phi_n \rightarrow \psi)...)$ et on explique pourquoi cela contredit la supposition que $\phi_1, \phi_2, \cdots, \phi_n \models \psi$.

1.2 *Deuxième partie*

La consistance et la complétude du calcul des séquants permet de dire :

$$\phi_1, \phi_2, \cdots, \phi_n \models \varphi \quad \text{si et seulement si} \quad \phi_1, \phi_2, \cdots, \phi_n \vdash \varphi.$$

En particulier, $\models \varphi$ si et seulement si $\vdash \varphi$.

- Se servir de ce fait et de la propriété établie en première partie pour simplifier l'obtention d'une preuve de :

  $$\vdash (p \rightarrow q) \rightarrow ((r \rightarrow t) \rightarrow ((p \wedge r) \rightarrow (q \wedge t)))$$

  par la déduction naturelle.

- Fournir cette preuve.

Exercice 2 *Induction*

On considère la partie $\mathcal{A}$ de $\mathbb{N}$ définie par :

$$\mathcal{A} = \left\{ x \in \mathbb{N}^* \quad / \quad \exists (a,b,c) \in \mathbb{N}^3 \quad x = 2^a 3^b 5^c \right\}.$$

2.1 *Etude d'un schéma d'induction*

On définit l'ensemble $\mathcal{M}$ par le schéma $(\mathcal{S})$ suivant :

- Base : $1 \in \mathcal{M}$.
- Règles :
  - (R_2) : $\forall m \in \mathbb{N} \quad [(m \in \mathcal{M}) \Rightarrow (2m \in \mathcal{M})]$;
  - (R_3) : $\forall m \in \mathbb{N} \quad [(m \in \mathcal{M}) \Rightarrow (3m \in \mathcal{M})]$;
  - (R_5) : $\forall m \in \mathbb{N} \quad [(m \in \mathcal{M}) \Rightarrow (5m \in \mathcal{M})]$.

a) Fournir un arbre de dérivation de $m_1 = 18$ et de $m_2 = 60$.

b) Montrer que $\mathcal{M} \subset \mathcal{A}$. Que dire du schéma $(\mathcal{S})$?

c) Montrer que $\mathcal{A} \subset \mathcal{M}$. Que dire du schéma $(\mathcal{S})$?

2.2 *Définition de fonctions par induction*

Sur $\mathcal{M}$, donc $\mathcal{A}$, on définit les trois fonctions v_2, v_3, v_5 par :

- $v_2(1) = 0; \quad v_3(1) = 0; \quad v_5(1) = 0.$
- Si m est élément de $\mathcal{M}$ alors

$$\begin{aligned} v_2(2m) &= v_2(m) + 1; \quad v_3(2m) = v_3(m); \quad v_5(2m) = v_5(m); \\ v_2(3m) &= v_2(m); \quad v_3(3m) = v_3(m) + 1; \quad v_5(3m) = v_5(m); \\ v_2(5m) &= v_2(m); \quad v_3(5m) = v_3(m); \quad v_5(5m) = v_5(m) + 1. \end{aligned}$$

a) Utiliser la question 2.1 a) pour fournir, pour tout i de $\{2,3,5\}$ et tout j de $\{1,2\}$, les valeurs de $v_i(m_j)$. Que représentent les fonctions v_i?

b) On définit sur $\mathcal{M}$ la relation binaire interne $\mid$ par :

$$[m \mid m'] \Leftrightarrow [\forall i \in \{2,3,5\} \quad v_i(m) \leq v_i(m')].$$

- Montrer que la relation $\mid$ est réflexive, antisymétrique et transitive.
- Comment se traduit dans le langage mathématique ordinaire, $m \mid m'$?
- Quelles sont les primitives nécessaires pour exprimer $m \mid m'$? A-t-on besoin de connaître le quotient ? Commenter brièvement.

c) Comment définir sur $\mathcal{M}^2$ le plus simplement possible, en utilisant les outils précédents, les fonctions *pgcd* et *ppcm* ? Quelles sont les seules primitives nécessaires ?

2.3 *Etudes des arbres de dérivation relatifs au schéma* $(\mathcal{S})$

On note $\mathcal{D}$ l'ensemble des arbres de dérivation relatifs au schéma $(\mathcal{S})$.

a) Sur $\mathcal{D}$, on définit la relation binaire interne $\sim$ suivante: on dit que deux arbres de dérivation D_1 et D_2 sont liés par $\sim$ si et seulement si ils conduisent au même entier m.

Donner un exemple d'arbres de dérivation D_1 et D_2 tels que $D_1 \sim D_2$.

b) Montrer que $\sim$ est une relation d'équivalence sur l'ensemble des arbres de dérivation.

c) On choisit un entier m de $\mathcal{M}$.

- Déterminer un élément de la classe d'équivalence $\mathcal{C}_m$ des arbres de dérivation qui conduisent à m.
- Déterminer en fonction de la décomposition en facteurs premiers de m, le cardinal de $\mathcal{C}_m$; on le notera $|\mathcal{C}_m|$.

d) On pose $N = 2^A 3^B 5^C$.

- Combien existe-t-il de m dans $\mathcal{M}$ vérifiant $m \mid N$?
- Fournir un exemple d'utilisation des résultats de c) et d) pour un ingénieur informaticien.