Année 2007–2008 — Session 1

Parcours : MCSB71–74 **Date :** 17 Décembre 2007
Code UE : INF461 **Durée :** 3h00
Épreuve de : Modèles de calcul - M. Zeitoun

Notes et documents de cours et TD autorisés. Autres documents interdits.
La notation tiendra compte de la clarté de la rédaction et du soin apporté dans les justifications.

Exercice 1 Répondre par vrai ou faux aux questions suivantes, sans donner une justification. Barème : $+0,5$ pour une réponse juste, $-0,5$ pour une réponse fausse, 0 pour une absence de réponse.

1. L'ensemble des graphes orientés finis est dénombrable.
2. Tout langage fini est décidable.
3. Pour tous $K, L \subseteq \Sigma^*$ avec $\Sigma = \{0, 1\}$, si K se réduit à L, alors $\Sigma^* \setminus K$ se réduit à $\Sigma^* \setminus L$.
4. Tout langage sur un alphabet à une lettre est décidable.
5. Étant donnés une machine de Turing M, un mot w et un entier k, on peut décider si M accepte w en au plus k pas de calcul.
6. Étant données deux machines de Turing M_1 et M_2, on peut décider si $\mathcal{L}(M_1) \subseteq \mathcal{L}(M_2)$.
7. Il existe une infinité de fonctions récursives totales qui ne sont pas primitives récursives.
8. Le langage des mots sur l'alphabet ASCII représentant un programme C syntaxiquement correct est décidable.
9. Le complément de tout ensemble récursivement énumérable est aussi récursivement énumérable.
10. Pour tout entier $k \geqslant 1$, il existe une bijection primitive récursive de $\mathbb{N}^k$ dans $\mathbb{N}$.

Exercice 2 Dans cet exercice les entiers seront codés en binaire. On pourra utiliser les machines usuelles de manipulation d'entiers en binaire (comparaisons, opérateurs arithmétiques,...) sans en refaire les constructions. On note $L \subseteq \{0, 1\}^*$ l'ensemble des représentations binaires des entiers non premiers (c'est-à-dire, des entiers $n \in \mathbb{N}$ qui ont un diviseur différent de n et de 1).

1. Décrire de façon informelle, mais précisément, une machine de Turing déterministe qui décide le langage L. Donner une borne supérieure (raisonnable) pour le temps de calcul de cette machine de Turing sur une entrée de taille k.
2. Décrire de façon informelle, mais précisément, une machine de Turing non-déterministe qui décide le langage L avec une complexité (en temps) polynomiale. Justifier cette complexité.

Exercice 3 Montrer que la fonction $f : \mathbb{N} \to \mathbb{N}$ définie par $f(n) = \lfloor \log_2(\sqrt{n^3} + 1) \rfloor$ est primitive récursive. Ici, $\lfloor x \rfloor$ désigne le plus grand entier inférieur ou égal à x. On pourra utiliser les fonctions primitives récursives et les schémas de construction de fonctions primitives récursives vus en cours.

Exercice 4 Soit $\Sigma = \{0, 1\}$. L'ordre *hiérarchique* $\leqslant$ est un ordre (total) sur Σ^* défini par :

$$u < v \text{ si } |u| < |v|, \text{ ou } |u| = |v| \text{ et } u <_{\text{lex}} v.$$

où $<_{\text{lex}}$ est l'ordre lexicographique, avec sur Σ l'ordre $0 <_{\text{lex}} 1$.

1. Donner les 5 premiers mots de Σ^*, dans l'ordre hiérarchique.

2. Donner le principe d'une machine de Turing qui sur l'entrée $k > 0$ codée en unaire, calcule le k-ième mot de Σ^* dans l'ordre hiérarchique.

On dit qu'un langage infini $L \subseteq \Sigma^*$ peut être *énuméré en ordre croissant* s'il existe une bijection calculable $f : \mathbb{N} \setminus \{0\} \to L$ qui à chaque $n > 0$ associe le n-ième mot de L dans l'ordre hiérarchique.

3. Montrer que tout langage décidable infini peut être énuméré en ordre croissant.
4. Montrer que tout langage qui peut être énuméré en ordre croissant est décidable.

Exercice 5 On dit qu'une machine de Turing M sur l'alphabet d'entrée $\Sigma = \{0, 1, \ldots, 9\}$ *calcule la constante 2008* si quelle que soit sa donnée, elle s'arrête en ayant sur sa bande les 4 caractères 2008, entourés de $\square$.

1. Décrire une machine de Turing qui calcule la constante 2008.
2. Décrire un algorithme qui, à partir d'une machine de Turing M_1, construit une machine de Turing M telle que M_1 accepte le mot vide si et seulement si M calcule la constante 2008.

Le problème 2008 est le suivant :

Donnée Une machine de Turing M (codée par un mot de $\{0,1\}^*$).
Question La machine de Turing M calcule-t-elle la constante 2008 ?

3. Exprimer précisément le résultat de la question précédente en terme de réduction, en justifiant.
4. Montrer que le problème 2008 est indécidable, en justifiant.

Exercice 6 On rappelle que le problème de correspondance de Post (PCP en abrégé) est le suivant.

Donnée n paires de mots $(x_1, y_1), \ldots, (x_n, y_n)$.
Question Existe-t-il une suite d'indices $i_1, \ldots, i_k$ telle que $x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$?

On rappelle également que ce problème est indécidable sur un alphabet ayant au moins deux lettres. On se place sur l'alphabet $\Sigma = \{1, 2, \ldots, 9\}$. On note $v : \Sigma^* \to \mathbb{N}$ la fonction qui à un mot associe l'entier ayant ce mot comme représentation en base 10. Par exemple, v associe au mot $1\,2\,3\,4$ de Σ^* l'entier 1234. On note $|w|$ la longueur d'un mot $|w|$.

1. Exprimer $v(xx')$ en fonction de $v(x)$, $v(x')$ et $|x'|$.

On considère la fonction f qui a un couple de mots (x, y) associe la matrice $\begin{pmatrix} 10^{|x|} & 10^{|x|} - 10^{|y|} & 0 \\ 0 & 10^{|y|} & 0 \\ v(x) & v(x) - v(y) & 1 \end{pmatrix}$.

2. Montrer que $f(x, y)f(x', y') = f(xx', yy')$ pour tous mots x, x', y, y' sur l'alphabet Σ. On rappelle que si $A = (a_{i,j})_{1 \leqslant i,j \leqslant 3}$ et $B = (b_{i,j})_{1 \leqslant i,j \leqslant 3}$ sont des matrices 3×3, leur produit $C = (c_{i,j})_{1 \leqslant i,j \leqslant 3}$ est donné par $c_{i,j} = a_{i,1}b_{1,j} + a_{i,2}b_{2,j} + a_{i,3}b_{3,j}$.
3. Soit $(x_1, y_1), \ldots, (x_n, y_n)$ une instance du PCP, et soit $M_i = f(x_i, y_i)$ pour $i = 1, \ldots, n$. Déduire de la question précédente que $x_{i_1} \cdots x_{i_k} = y_{i_1} \cdots y_{i_k}$ si et seulement si la composante (3,2) de la matrice $M_{i_1} \cdots M_{i_k}$ est nulle.
4. En déduire que le problème suivant est indécidable, en justifiant soigneusement.
   Donnée n matrices $M_1, \ldots, M_n$ carrées 3×3, à coefficients dans $\mathbb{Z}$.
   Question Existe-t-il un produit de la forme $M_{i_1} \cdots M_{i_k}$ dont la composante $(3, 2)$ est nulle ?

Exercice 7 On représente l'entier n par le λ-terme $\lceil n \rceil = \lambda sz.s^n z$, où $s^0 z = z$ et $s^{n+1} z = s(s^n z)$. On rappelle que les Booléens sont conventionnellement représentés par $\lceil \mathsf{T} \rceil = \lambda xy.x$ (true) et $\lceil \mathsf{F} \rceil = \lambda xy.y$ (false). Soit $Z = \lambda a(a(\lambda b \lceil \mathsf{F} \rceil) \lceil \mathsf{T} \rceil)$. Vérifier que $Z\lceil 0 \rceil \xrightarrow{\beta}{}^* \lceil \mathsf{T} \rceil$, et $Z\lceil n \rceil \xrightarrow{\beta}{}^* \lceil \mathsf{F} \rceil$ si $n \neq 0$.