Fondements de l'informatique. Examen
Durée: 3h

Sujet proposé par Olivier Bournez
Version 11

Les 5 parties sont indépendantes, et peuvent être traitées dans un ordre quelconque. On pourra admettre le résultat d'une question pour passer aux questions suivantes. On pourra utiliser tous les résultats et les théorèmes démontrés ou énoncés en cours ou en petite classe ou dans le polycopié sans chercher à les redémontrer. Il est possible d'avoir la note maximale sans répondre à toutes les questions. La difficulté des questions n'est pas une fonction linéaire ni croissante de leur numérotation. La qualité de votre argumentation et de votre rédaction est une partie importante de votre évaluation.

1 Machines de Turing

On considère des machines de Turing qui travaillent sur l'alphabet qui contient les lettres $a, b, \ldots, z, A, B, \ldots Z$ ainsi que le caractère espace.

Question 1. *Le problème suivant est-il décidable ? Déterminer si le langage accepté par une machine de Turing M est le langage réduit au mot "je suis une machine de Turing".*

Question 2. *Existe-t'il une machine de Turing M dont le codage est $< M >$ qui accepte si une entrée w est le mot "je suis la machine de Turing $< M >$" et refuse sinon*[1]*.*

2 Ordres bien fondés

On rappelle qu'une relation d'ordre totale est une relation réflexive, transitive et antisymétrique, telle que tout élément est comparable à tout autre.

On dit qu'un ordre total est *bien fondé* s'il n'existe pas de suite infinie strictement décroissante. Par exemple, $\leq$ est bien fondé sur l'ensemble des entiers $\mathbb{N}$, mais pas sur l'ensemble des entiers relatifs $\mathbb{Z}$.

Question 3. *On considère la signature avec les symboles de relation $=, \leq$ et aucun symbole de constante et de fonction.*

Démontrer qu'il n'existe aucune théorie sur cette signature dont les modèles égalitaires sont exactement les ensembles tels que l'interprétation de $\leq$ est une relation d'ordre total bien fondé sur l'ensemble de base.

3 NP-complétude

Pour un graphe $G = (V, E)$, V désigne les sommets du graphe, et E ses arêtes. On suppose les graphes non-orientés.

1. Bien entendu, "je suis la machine de Turing $< M >$" designe la concaténation du mot "je suis la machine de Turing" et du mot correspondant à $< M >$.

On rappelle les définitions et faits suivants : un graphe est *connexe* s'il existe un chemin entre toute paire de sommets. C'est un *arbre* s'il ne possède aucun cycle. On pourra utiliser le fait suivants : un arbre avec $t+1$ sommets possède nécessairement t arêtes. Réciproquement, un graphe connexe ayant $t+1$ sommets et t arêtes est un arbre.

Etant donné un graphe G, on appellera *arbre de G* tout sous-graphe de G qui est un arbre. On dira qu'un tel arbre *passe par un sommet s* (de G) si ce sommet s est dans le sous-graphe.

L'objectif de cet algorithme est de prouver que le problème suivant est NP-complet.

Arbre de Steiner:

— **Donnée**: Un graphe non-orienté $G = (V, E)$, un ensemble D de sommets, un entier k.

— **Réponse**: Décider s'il existe un arbre de G qui a moins de k arêtes et qui passe par tous les sommets de D.

Soit $G = (V_G, E_G)$ un graphe. Nous allons construire un graphe $H = (V_H, E_H)$ à partir de G tel que

— $V_H = V_G \cup E_G$;

— $E_H = \{(v, u) | v, u \in V_G\} \cup \{(v, a) | v \in V_G, a \in E_G, v \text{ est extrémité de l'arête } a \text{ dans } G\}$.

Question 4. *On considère le cas où $V_G = \{a, b, c, d\}$, et $E_G = \{(a, b), (b, c), (c, d)\}$. Dessiner le graphe H correspondant. Proposer un arbre de H qui possède 4 arêtes et qui passe par tous les sommets de H qui sont dans E_G.*

Rappelons la définition suivante : une *couverture de sommets* S d'un graphe G est un sous-ensemble de sommets tel que toutes les arêtes de G ont au moins une de leurs extrémités dans S.

Question 5. *Démontrer que si S est une couverture de sommets du graphe G, alors il existe un arbre de H qui passe par tous les sommets dans E_G et qui possède $|S| + |E_G| - 1$ arêtes.*

Question 6. *Montrer que si $T = (V_T, E_T)$ est un arbre qui passe par tous les sommets dans E_G et qui possède t arêtes, alors il existe une couverture de sommets S du graphe G de cardinal*[2] *$t - |E_G| + 1$.*

On rappelle que le problème RECOUVREMENT DE SOMMETS:

— **Donnée**: Un graphe $G = (V_G, E_G)$ non-orienté et un entier k.

— **Réponse**: Décider s'il existe une couverture S de G avec le cardinal de S qui vaut k.

est NP-complet.

Question 7. *Montrer que le problème* Arbre de Steiner *est NP-complet.*

4 Le corps des réels calculables

Les définitions suivantes ne font rien que de formaliser ce à quoi on s'attend : $\mathbb{Q}$ désigne l'ensemble des rationnels, et $\mathbb{Q}_*^+$ l'ensemble des rationnels strictement positifs. On suppose fixé un codage des rationnels tel que les opérations habituelles[3] sont calculables sur ce codage[4]. On dira qu'une fonction $f : \mathbb{Q}_*^+ \to \mathbb{Q}$ est *calculable* si elle est calculable avec ce codage (et définie sur tout $\mathbb{Q}_*^+$). De même un ensemble de rationnels est dit *décidable* si l'ensemble des codages des rationnels de cet ensemble l'est. Un ensemble de rationnels est dit *récursivement énumérable* si l'ensemble des codages des rationnels de cet ensemble l'est.

Un nombre réel α est dit *calculable* si $\{q \in \mathbb{Q} | q < \alpha\}$ est décidable.

On dit qu'un réel α est *énumérable par le bas* si $\{q \in \mathbb{Q} | q < \alpha\}$ est récursivement énumérable.

On dit qu'un réel α est *énumérable par le haut* si $\{q \in \mathbb{Q} | q \geq \alpha\}$ est récursivement énumérable.

2. Le cardinal d'un ensemble est le nombre de ses éléments.
3. Exemple : somme, produit, ...
4. Par exemple on peut coder le rationnel $r = p/q$ par le couple p, q où p et q sont écrits en binaire.

Question 8. *Montrer que α est calculable si et seulement s'il est énumérable par le bas et énumérable par le haut.*

Question 9. *Montrer qu'un réel α est énumérable par le bas si et seulement si c'est la borne supérieure d'une suite $u_0, u_1, \ldots, u_i, \ldots$ de rationnels telle que la fonction $i \mapsto u_i$ est calculable.*

Un nombre réel α est dit *effectivement approximable* s'il existe une fonction calculable $a : \mathbb{Q}_*^+ \to \mathbb{Q}$ telle que pour tout rationnel $\epsilon > 0$, $a(\epsilon)$ fournit une approximation de α à ϵ-près : autrement dit : $|\alpha - a(\epsilon)| \leq \epsilon$ pour tout $\epsilon > 0$.

Question 10. *Démontrer que si α est calculable alors il est effectivement approximable.*

Question 11. *Soit α un réel avec $\alpha \notin \mathbb{Q}$. Démontrer que si α est effectivement approximable, alors il est calculable.*

Question 12. *En déduire que α est calculable si et seulement s'il est effectivement approximable.*

Question 13. *Montrer qu'un réel $\alpha \in [0, 1]$ est calculable*[5] *si et seulement s'il possède une écriture*[6] *en base 10 de la forme $0.u(1)u(2)\ldots u(k)\ldots$ avec $u : k \mapsto \{0, 1, \ldots, 9\}$ calculable.*

L'ensemble des réels calculables est un sous-corps du corps des réels : en raison du fait que $\mathbb{R}$ est un corps, il suffit de démontrer les faits suivants.

Question 14. *Démontrer que la somme, le produit, la différence et le quotient de deux nombres calculables est calculable*[7].

C'est même un corps réel clos. En raison du fait que $\mathbb{R}$ est un corps réel clos, il suffit de démontrer le fait suivant :

Question 15. *Démontrer que toute racine α d'un polynôme à coefficients calculables est un réel calculable. On pourra utiliser le fait que, quitte à raisonner sur une dérivée suffisante du polynôme, on peut supposer que le polynôme change de signe en α.*

5 Théorème d'interpolation de Craig

Dans ce qui suit, on considère deux formules φ et ψ construites sur deux signatures, Σ_1 pour φ et Σ_2 pour ψ. La signature Σ_0 est la signature dont les symboles (de constantes, relations et fonctions) sont ceux communs à Σ_1 et Σ_2.

Une formule θ est appelée un interpolant des formules φ et ψ avec $\varphi \vdash \psi$ si l'on a $\varphi \vdash \theta$ et $\theta \vdash \psi$, et si θ est construite sur la signature commune Σ_0.

Le théorème de Craig affirme que si l'on a deux formules φ et ψ avec $\varphi \vdash \psi$, alors il existe toujours un interpolant.

Question 16. *Soit φ la formule $\forall x\ (x < f(x))$ sur la signature $(\emptyset, \{f\}, \{<\})$ et ψ la formule $\exists y\ (c < y)$ sur la signature $(\{c\}, \emptyset, \{<\})$.*

Proposer un interpolant entre φ et ψ.

Soit C un ensemble dénombrable de constantes qui n'apparaissent ni dans Σ_1 ni dans Σ_2. Soit $\Sigma_i' = \Sigma_i \cup C$ pour $i = 0, 1, 2$.

Soit T_1 une théorie sur la signature Σ_1' et T_2 une théorie sur la signature Σ_2'. Une formule θ sur la signature Σ_0' sépare T_1 de T_2 si $T_1 \vdash \theta$ et $T_2 \vdash \neg\theta$. Deux théories sont dîtes *inséparables* s'il n'existe aucune telle formule θ.

5. On rappelle que 1 peut aussi s'écrire $1 = 0.99999\ldots$.
6. Possiblement infinie.
7. Le second étant non-nul pour le quotient, évidemment.

Question 17. *Montrer que si T_1 et T_2 sont inséparables alors T_1 est cohérent et T_2 est cohérent.*

Question 18. *Soient les théories $T_1 = \{\varphi\}$ sur la signature Σ'_1 et $T_2 = \{\neg\psi\}$ sur la signature Σ'_2. Montrer que si T_1 et T_2 sont séparables alors il existe toujours un interpolant des formules φ et ψ.*

On admettra le résultat suivant : si T_1 et T_2 sont inséparables alors $T_1 \cup T_2$ est aussi cohérent (la preuve de ce résultat peut être vue comme une généralisation de la preuve du théorème de complétude).

Question 19. *En déduire le théorème de Craig.*