Fondements de l'informatique. Examen
Durée: 3h

Sujet proposé par Olivier Bournez
Version 11
(corrigé)

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".*

Solution : C'est indécidable : il s'agit d'une application directe du théorème de Rice. □

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]*.*

Solution : En utilisant le théorème de récursion, on considère une machine de Turing qui commence par déterminer son propre code $< M >$ puis teste si l'entrée est "je suis la machine de Turing $< M >$". □

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.

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 $< M >$.

Solution : On utilise le théorème de compacité : Par l'absurde, supposons qu'il existe un tel ensemble $\mathcal{F}$. On considère l'ensemble de formules $\mathcal{G}$ obtenu en prenant toutes les formules de $\mathcal{F}$ auxquelles on ajoute les formules $c_{n+1} \leq c_n$, $\neg(c_n = c_{n+1})$ pour tout n, où ces symboles c_n sont de nouveaux symboles. Toute partie finie de $\mathcal{G}$ est consistante, car il y a des relations totales bien fondées dans $\mathbb{N}^*$: en effet $(\mathbb{N}, \leq)$ en est un modèle. Par le théorème de compacité, $\mathcal{G}$ doit être consistante. On obtient une contradiction car l'interprétation des constantes c_n donne une suite infinie strictement décroissante et pourtant toute les formules de $\mathcal{F}$ sont satisfaites. □

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.

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.

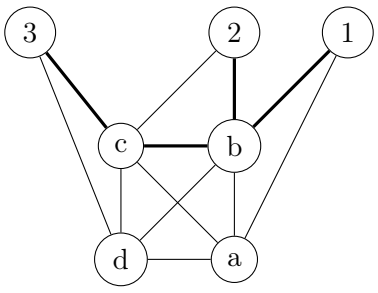
Soit $G = (V_G, E_G)$ un graphe. Nous allons construire un graphe $H = (V_H, E_H)$ à partir de G tel que

— $V_H = V_G \cup E_G$;

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

Solution : Voici une solution. L'arbre est indiqué par ses arêtes en gras.



□

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.*

Solution : Soit S une couverture de sommets du graphe G. Il faut construire un tel arbre.

Pour cela, nous ordonnons les sommets de S : $S = \{s_1, \ldots, s_{|S|}\}$. Nous allons construire l'arbre $T = (V_T, E_T)$ de telle façon suivante :

— $V_T = S \cup E_G$;
— $\{(s_i, s_{i+1}) : 1 \leq i < s_{|S|}\} \subset E_T$;
— $(e, s_i) \in E_T$ si l'arête e de E_G a exactement une extrémité s_i dans S ou si e a deux extrémités s_j et s_i dans S avec $i < j$.

Comme tous les sommets de V_G sont reliés deux à deux dans H, il est clair que $\{(s_i, s_{i+1}) : 1 \leq i < s_{|S|}\}$ forme un chemin dans H. Comme S est une couverture de sommets, pour toute arête e, il existe au moins une extrémité dans S. Donc dans H, le sommet e est voisin d'au moins un sommet de S. T est connexe, et possède $|S| + |E_G| - 1$ arêtes avec $|S| + |E_G|$ sommets : c'est donc un arbre. □

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] *$t - |E_G| + 1$.*

Solution : Considérons l'ensemble de sommets $C = V_T \backslash E_G$. Par définition de H, $C \subset V_G$. Toute arête $e = (u, v)$ de G est un sommet de H, et il est uniquement voisin des sommets u et v. Donc au moins l'un d'entre eux doit être dans C (sinon T ne serait pas connexe). Donc l'ensemble C a pour voisin toutes les arêtes de E, et il constitue une couverture de sommets de G.

Maintenant calculons son nombre d'éléments : $|C| = |V_T| - |E_G|$. Comme T est un arbre, il a $t = |V_T| - 1$ arêtes. On peut conclure que $|C| = t - |E_G| + 1$. □

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.*

Solution : Le problème Arbre de Steiner est dans NP car étant donnée un ensemble d'arêtes, on peut vérifier en temps polynomial

1. si cet ensemble d'arêtes forme un arbre ;
2. si l'ensemble de sommets D est couvert par l'arbre ;
3. si le nombre d'arêtes est inférieur à k.

Montrons maintenant qu'il est complet. Soit $\mathcal{I} =< G = (V_G, E_G, k) >$ une instance du problème RECOUVREMENT DE SOMMETS que l'on sait NP-complet.

Maintenant, nous allons transformer cette instance en une instance $\mathcal{I}'$ du problème Arbre de Steiner $< H = (V_H, E_H), D, k' >$ de la façon suivante :

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

— $V_H = V_G \cup E_G$;
— $E_H = \{(v, u) | v, u \in V_G\} \cup \{(v, a) | v \in V_G, a \in E_G, v$ est extrémité de l'arête a dans $G\}$
— $D = E_G$
— $k' = k + |D| - 1$

Cette transformation peut se faire en temps polynomial : le nombre de sommets du nouveau graphe est $|V_G| + |E_G|$. Construire le graphe H nécessite au plus $\mathcal{O}((|V_G| + |E_G|)^2)$ opérations.

Les questions précédentes ont permis de prouver que le fait suivant : le graphe G admet est une couverture de sommets S de taille k si et seulement si le graphe H admet un arbre ayant moins de k' arêtes passant par tous les sommets de D.

2. Le cardinal d'un ensemble est le nombre de ses éléments.

Donc le problème 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.

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

Solution : Par la question précédente, un réel est calculable si et seulement si $\{q \in \mathbb{Q} | q < \alpha\}$ est décidable. On sait qu'un ensemble est décidable si et seulement s'il est récursivement énumérable et son complémentaire l'est aussi. □

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.*

Solution : On sait que $\{q \in \mathbb{Q} | q < \alpha\}$ est récursivement énumérable. Il y a donc une machine de Turing qui énumère cet ensemble. α est alors la borne supérieure de cette suite.

Réciproquement, pour déterminer si $q < \alpha$, on parcourt la suite calculable de rationnels en acceptant si et seulement si l'on trouve un rationnel dans cette suite plus grand que q. □

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.*

Solution : Etant donné $\epsilon > 0$, on parcourt les couples de rationnels jusqu'à trouver $p < q$ avec $p - q < \epsilon$ avec $p < \alpha$ et $\neg(q < \alpha)$. On retourne alors $a(\epsilon) = (p + q)/2$. □

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

Solution : Si $\alpha \notin \mathbb{Q}$, étant donné q, on teste pour $\epsilon = 1/n$ pour $n = 1, 2, \ldots$ si $a(\epsilon) + \epsilon < q$, auquel cas on répond "vrai", jusqu'à ce que $a(\epsilon) - \epsilon > q$. Si ce dernier cas se produit, on répond "faux".

Nécessairement l'algorithme s'arrête car étant donné q, pour $1/n$ plus petit que $|\alpha - q|$ l'un des deux cas où l'on répond a dû se produire. □

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

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.

Solution : Il reste juste à démontrer que $\{q \in \mathbb{Q} | q < \alpha\}$ est décidable quand $\alpha \in \mathbb{Q}$. Mais ce cas est trivial. □

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 $0.u(1)u(2)\dots u(k)\dots$ avec $u : k \mapsto \{0,1,\dots,9\}$ calculable.*

Solution : Si α est calculable, on peut calculer $u(1), u(2), \dots u(k)$ pour k croissant, en testant si $0.u(1)u(2)\dots u(k-1)i \geq \alpha$ pour $i = 0, 1, \dots, 9$. Dès qu'un trouve $0.u(1)u(2)\dots u(k-1)i < \alpha$ on sait que $u(k)$ vaut $i-1$, puisque $\alpha \in [0.u(1)u(2)\dots u(k-1)(i-1), 0.u(1)u(2)\dots u(k-1)i[$.

Réciproquement, étant donné $\epsilon > 0$, en déterminant k tel que $10^{-k} < \epsilon$, les k premiers chiffres de son écriture en base 10 fournissent une approximation à ϵ près de α. □

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].

Solution : Si $a(\epsilon)$ et $b(\epsilon)$ sont des fonctions calculables qui approximent p et q à ϵ près, alors $c(\epsilon) = a(\epsilon/2) + b(\epsilon/2)$ (respectivement : $a(\epsilon/2) - b(\epsilon/2)$) approximent $p+q$ (resp. $p-q$) à ϵ près. Elles sont bien calculables par composition de fonctions calculables.

Pour le produit

$$\begin{aligned} |pq - a(\epsilon)b(\epsilon)| &\leq |p| \cdot |q - b(\epsilon)| + |b(\epsilon)||p - a(\epsilon)| && (1)\\ &\leq a(1)\epsilon + b(1)\epsilon && (2)\\ &= (a(1) + b(1))\epsilon && (3) \end{aligned}$$

Donc $a(\frac{\epsilon}{a(1)+b(1)})b(\frac{\epsilon}{a(1)+b(1)})$ donne une approximation de pq à ϵ près.
On fait une majoration similaire pour le quotient. □

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.*

Solution : Un polynôme P possède un nombre fini de racines. Pour chacune d'entre elle, on peut donc trouver un intervalle $[c,d]$ avec c et d rationnels qui l'isole : P possède une unique racine α sur $]c,d[$. P ne change pas de signe sur $[c,\alpha]$ et sur $[\alpha,d]$. Quitte à raisonner sur la dérivée de P (ou une dérivée suffisante de P) on peut supposer que $P(c)$ change de signe en α sur $[c,d]$. En remplaçant P par $-P$ si besoin, supposons $P(c) > 0$. Si α est rationnel, alors α est calculable. Si α n'est pas rationnel, alors il est aussi calculable car pour déterminer si un rationnel q satisfait $q < \alpha$, il suffit de tester si $q \leq c$ ou si ($q > c$ et $P(q) > 0$). Pour déterminer si $P(q) > 0$ ou $P(q) < 0$ (on ne peut pas avoir $P(q) = 0$), il suffit de faire pour $\epsilon = 1/n$ pour n croissant si $P(q) + \epsilon < 0$ alors répondre vrai, et si $P(q) - \epsilon > 0$ alors répondre faux. Cette boucle termine nécessairement, car $P(q) \neq 0$. □

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

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.

Solution : $\forall x \exists y (x < y)$ est un interpolant. □

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.

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

Solution : Si T_1 n'était pas cohérent, cela signifierait que $T_1 \vdash F$ et $T_1 \vdash \neg F$ pour une formule F, et donc T_1 prouve une formule toujours fausse $(F \wedge \neg F)$. Par conséquent, il prouve aussi n'importe quelle formule F' toujours fausse sur la signature commune. Maintenant, T_2 prouve sa négation $\neg F'$ (toujours vraie). Et donc cette formule séparerait T_1 de T_2 contrairement à l'hypothèse.

On fait un argument symétrique pour T_2. □

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.*

Solution :

Si $\theta(c_1, \ldots, c_k)$ les sépare, alors $T_1 \vdash \theta(c_1, \ldots, c_k)$ et $T_2 \vdash \neg\theta(c_1, \ldots, c_k)$. Puisque $c_1, \ldots, c_k$ n'apparaissent pas dans φ, $\varphi \vdash \forall x_1 \ldots \forall x_n \theta(x_1, \ldots, x_n)$ (formule de généralisation, voir cours).

On doit avoir par ailleurs $\psi \vdash \neg\forall x_1 \ldots \forall x_n \theta(x_1, \ldots, x_n)$. Par conséquent, on obtient $\forall x_1 \ldots \forall x_n \theta(x_1, \ldots, x_n) \vdash \psi$. Donc $\forall x_1 \ldots \forall x_n \theta(x_1, \ldots, x_n)$ est un interpolant entre 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.*

Solution : Par contradiction. Supposons que $\varphi \vdash \psi$ et qu'il n'existe pas d'interpolant. Cela veut dire par la question précédente que $T_1 = \{\varphi\}$ et $T_2 = \{\neg\psi\}$ sont inséparables. Par le résultat admis, la théorie $T_1 \cup T_2$ est cohérente. Par le théorème de complétude, elle doit posséder un modèle, et donc on obtient une contradiction avec $\varphi \vdash \psi$. □