Fondements de l'informatique: Examen Durée: 3h

Sujet proposé par Olivier Bournez
Version 1.3
(corrigé)

L'énoncé comporte 5 *parties indépendantes, qui pourront être traitées dans un ordre quelconque. En revanche, dans chaque partie, il peut être utile, dans la réponse à une question, d'utiliser les questions précédentes! On pourra librement admettre le résultat d'une question pour passer aux questions suivantes. La difficulté des questions n'est pas une fonction linéaire ni croissante de leur numérotation.*

Dans tout l'énoncé, et en particulier dans la partie "Machines de Turing", on demande des algorithmes et des solutions à un haut niveau: dans aucune des questions il n'est demandé de décrire complètement une machine de Turing, ni même d'en donner une description graphique; on pourra se contenter pour décrire un algorithme de le décrire par exemple en français ou dans un langage de programmation classique comme JAVA, C ou CAML.

1 Machines de Turing

On rappelle qu'une fonction $f : \mathbb{N} \to \mathbb{N}$ est calculable si il existe une machine de Turing qui partant du codage en binaire de n sur son ruban finit, au bout d'un temps fini, par arriver dans son état d'acceptation avec $f(n)$ écrit en binaire sur son ruban.

Question 1.1. *Montrer que l'inverse d'une fonction $f : \mathbb{N} \to \mathbb{N}$ calculable et bijective est calculable.*

Solution : On peut calculer l'inverse g de f de la façon suivante: sur l'entrée y, on teste pour $x = 0, 1, \cdots$, si $f(x) = y$. On s'arrête dès qu'un a trouvé un tel x. Puisque f est surjective on doit s'arrêter. □

Question 1.2. *Soit C un langage sur un alphabet fini Σ. Montrer que C est récursivement énumérable si et seulement si il existe un langage décidable D tel que*

$$C = \{w | \exists u \ (w, u) \in D\}.$$

Remarque: D est un langage de paires (plus précisément de couples) de mots: (w, u) désigne, comme dans les transparents du cours (par un léger abus de notation) un codage fixé de la paire (du couple) (w, u). Le codage précis n'est pas important à partir du moment où l'on peut retrouver w et u à partir du codage de (w, u), et qu'on peut construire le codage de (w, u) à partir de w et de u. Note: dans le polycopié, on distingue les couples/paires (w, u) et leur codage $< w, u >$ (voir page 114): avec les notations du polycopié, on écrirait $C = \{w | \exists u \ < w, u > \in D\}$.

Solution : Supposons que C soit reconnu par une machine de Turing M. On considère le langage $D = \{(w,u)|u$ code un entier t en binaire et M accepte w en temps $t\}$. D est décidable, car il suffit de simuler M pendant un temps t pour savoir si $(w,u) \in D$. On a bien la propriété que $C = \{w|\exists u\ (w,u) \in D\}$, car tout mot accepté par M l'est en un certain temps t (u est le codage en binaire de t).

Réciproquement, si $C = \{w|\exists u\ (w,u) \in D\}$, alors pour savoir si $w \in C$, il suffit de tester tous les mots u un à un jusqu'à ce qu'on détecte que $(w,u) \in D$. □

Question 1.3. *Parmi les problèmes suivants, lesquels sont décidables, lesquels sont indécidables. Prouver formellement votre réponse.*

1. *Déterminer si le langage accepté par une machine de Turing M ne contient que des palindromes (un palindrome est un mot dont l'ordre des lettres reste le même qu'on le lise de gauche à droite ou de droite à gauche, comme "anna").*
2. *Déterminer si une machine de Turing M et un mot w sont tels que M accepte l'entrée w en n'utilisant (= écrivant) aucune autre case que celles qui contiennent initialement le mot w.*
3. *Déterminer si une machine de Turing M et un mot w sont tels que M accepte l'entrée w en n'utilisant aucune des cases initialement blanches à gauche de celles qui contiennent initialement w.*

Solution : La question 1. est indécidable: il s'agit d'une application directe du théorème de Rice.

La question 2. est décidable: il suffit de simuler M en s'arrêtant en refusant dès que M essaye d'accéder à une case du ruban hors de celles qui contiennent initialement w ou dès que M passe deux fois par la même configuration, et en acceptant si M accepte: une machine qui utilise uniquement les cases du ruban qui contiennent initialement w possède un nombre fini de configurations possibles; si elle passe deux fois par la même configuration, elle le fera indéfiniment; sinon, elle ne peut avoir qu'au plus ce nombre de configurations d'étapes avant de s'arrêter.

La question 3. est indécidable. Le problème de l'arrêt se réduit à cette question. En effet, soit M une machine de Turing, et w une entrée. Considérons la machine M' qui simule M en décalant systématiquement vers la droite le contenu du ruban de M dès que M tente d'accéder à une case à gauche de celles initialement occupées par l'entrée. Si M accepte w, alors M' se déplace vers la gauche en écrivant un symbole particulier à jamais. Par construction, M' vérifie la propriété de la question 3. si et seulement si M accepte w.

□

2 Elimination des quantificateurs

Rappels:

- Une théorie T est un ensemble de formules sur une signature Σ.
- Deux formules F et F' sont équivalentes dans une théorie T si et seulement si $F \Leftrightarrow F'$ est une conséquence de T.
- Une formule sans quantificateur est une formule qui ne contient aucun symbole $\exists$ et aucun symbole $\forall$.

On dit qu'une théorie T sur la signature Σ permet l'élimination des quantificateurs dans une formule F (sur Σ) s'il existe une formule F' (sur Σ) sans quantificateur qui lui est équivalente dans la théorie T.

On dit que T permet l'élimination des quantificateurs sur Σ si T permet l'élimination des quantificateurs dans toute formule F sur Σ.

Par exemple, on peut montrer[1] que la théorie T qui correspond aux corps réels clos permet l'élimination des quantificateurs: par exemple, la formule

$$\exists x \ a * x * x + b * x + c = 0$$

(qui possède un quantificateur existentiel) est équivalente à la formule

$$(b * b - 4 * a * c \geq 0 \wedge a \neq 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)$$

(qui n'en possède pas)[2] sur la théorie T.

Le but de cet exercice est de prouver qu'une autre théorie T, la théorie des ordres denses avec premier et dernier élément, permet l'élimination des quantificateurs.

Débutons par quelques généralités, avant de définir cette théorie T.

2.1 Généralités

Question 2.1. *Montrer que si une théorie T sur une signature Σ permet l'élimination des quantificateurs sur une formule F, alors elle permet l'élimination des quantificateurs sur la formule $\neg F$.*

Solution : Si F est équivalente à F' sans quantificateur, alors $\neg F$ est équivalente à $\neg F'$, et donc la théorie permet aussi l'élimination des quantificateurs sur la formule $\neg F$. $\square$

On rappelle que toute formule F est équivalente à une formule en forme normale prénexe (Proposition 5.4 page 68 du polycopié).

Question 2.2. *Montrer que pour qu'une théorie T permette l'élimination des quantificateurs sur la signature Σ, il faut et il suffit que T permette l'élimination des quantificateurs dans toute formule de la forme $\exists x \ H$, où H est sans quantificateur.*

Solution : Clairement la condition est nécessaire, car $\exists x \ H$ est une formule particulière.

Le fait que la condition soit suffisante se prouve par récurrence sur le nombre de quantificateurs de la formule F que l'on peut supposer prénexe: F est de la forme $Q_1 x_1 Q_2 x_2 \dots Q_n x_n F'$ où F' est sans quantificateur, et où chaque Q_i est soit $\exists$ soit $\forall$. On peut même supposer que $Q_1 = \exists$ car $\forall x_1 F''$ est équivalent à la négation de $\exists x_1 \neg F''$, et la négation d'une formule sans quantificateur est une formule sans quantificateur.

La condition permet de prouver la récurrence pour le rang $n = 1$. Pour un rang $n > 1$, par hypothèse de récurrence au rang $n - 1$, $Q_2 x_2 \dots Q_n x_n F'$ est équivalente à une formule F' sans quantificateur, et donc F est équivalente à $Q_1 x_1 F'$. La condition permet de déduire que F est équivalente à une formule sans quantificateur. $\square$

Question 2.3. *Montrer que pour qu'une théorie T permette l'élimination des quantificateurs sur Σ, il faut et il suffit que T permette l'élimination des quantificateurs dans toute formule F sur Σ de la forme $\exists x \ (\alpha_1 \wedge \alpha_2 \wedge \dots \wedge \alpha_r)$, où chaque α_i est soit une formule atomique sur Σ ou la négation d'une telle formule.*

On pourra utiliser le fait que $\exists x (A \vee B)$ est équivalent à $(\exists x A) \vee (\exists x B)$, pour des formules A et B.

[1] Ce qui est hors de l'ambition de ce sujet.

[2] Bien entendu, ici 4 désigne $1 + 1 + 1 + 1$. De même, $a \neq 0$, par exemple, représente $\neg(a = 0)$.

Solution : Chaque formule sans quantificateur H équivaut à une formule de la forme $H_1 \vee \cdots \vee H_k$ où H_i est lui-même de la forme $\alpha_1 \wedge \cdots \wedge \alpha_r$, chaque α_i est soit une formule atomique sur Σ ou la négation d'une telle formule (forme normale disjonctive).

Il suffit alors d'observer que $\exists x\ (H_1 \vee \cdots \vee H_k)$ est équivalent à $(\exists x H_1) \vee \cdots \vee (\exists x H_k)$. $\square$

2.2 Ordres denses avec premier et dernier élément

On considère la signature Σ suivante: 2 symboles de constantes 0 et 1; 2 symboles de relations $<$ et $=$ d'arité 2.

La théorie T des *ordres denses avec premier et dernier élément* est la théorie sur la signature Σ qui contient les formules suivantes:

1. $\forall x \neg(x < x)$; (ordre strict)
2. $\forall x \forall y \forall z((x < y \wedge y < z) \Rightarrow x < z)$ (ordre transitif)
3. $\forall x \forall y(x = y \vee x < y \vee y < x)$ (axiome de relation d'ordre total)
4. $\forall x \forall y \exists z(x < y \Rightarrow (x < z \wedge z < y))$ (axiome de densité)
5. $\forall x(x = 0 \vee 0 < x)$ (axiome du 1ier élément)
6. $\forall x(x = 1 \vee x < 1)$ (axiome du dernier élément)

On suppose la théorie égalitaire[3]: cela revient soit à considérer qu'on impose que le symbole $=$ est nécessairement interprété par l'égalité, soit à supposer que T contient aussi les axiomes de l'égalité: $\forall x\ x = x$, $\forall x \forall y\ (x = y \Rightarrow y = x)$ et $\forall x \forall y \forall z(((x = y) \wedge (y = z)) \Rightarrow x = z)$, $\forall x \forall x' \forall y, (x = x') \Rightarrow ((x < y) \Leftrightarrow (x' < y))$, $\forall x \forall y \forall y', (y = y') \Rightarrow ((x < y) \Leftrightarrow (x < y'))$.

Comme annoncé, on veut montrer que T permet l'élimination des quantificateurs sur Σ.

Question 2.4. *Montrer qu'on est ramené à prouver l'élimination des quantificateurs dans une formule de la forme $\exists x(\alpha_1 \wedge \cdots \wedge \alpha_r)$, où chaque α_i est de la forme $t_1 < t_2$ ou $t_1 = t_2$.*

Solution : Par les axiomes $\neg(t_1 < t_2)$ est équivalent à $(t_2 < t_1) \vee (t_1 = t_2)$, et $\neg(t_1 = t_2)$ est équivalent à $(t_1 < t_2) \vee (t_2 < t_1)$. Il suffit alors d'utiliser le fait que $A \wedge (B \vee C)$ équivaut à $(A \wedge B) \vee (A \wedge C)$ et que $\exists x(A \vee B)$ équivaut à $(\exists x A) \vee (\exists x B)$. $\square$

Question 2.5. *Prouver que T permet l'élimination des quantificateurs sur Σ.*

Solution : Par récurrence sur r. Pour $r = 1$, la formule est $\exists x(t_1 < t_2)$ ou t_1 et t_2 sont 0, 1 ou une variable. L'élimination est immédiate.

Supposons l'élimination effectuée au rang $r - 1$ et considérons la formule $\exists x(\alpha_1 \wedge \cdots \wedge \alpha_r)$. Chaque α_i doit contenir x. Sinon, si par exemple α_1 ne le contient pas, la formule équivaut à $\alpha_1 \wedge \exists x(\alpha_2 \wedge \cdots \wedge \alpha_r)$ et on est ramené à l'hypothèse au rang $r - 1$.

Par conséquent, la formule s'écrit $\exists x(x < t_1 \wedge \cdots \wedge x < t_k \wedge u_1 < x \wedge \cdots \wedge u_l < x \wedge x = v_1 \wedge \ldots x = v_m)$, où les t, u, v sont des termes que l'on peut supposer différents de x (si par exemple t_1 ou u_1 est x, la formule est équivalente à faux; si v_1 est x on est ramené au rang $r - 1$).

Si $k > 1$, la formule équivaut à $[t_1 < t_2 \wedge \exists x(x < t_1 \wedge x < t_3 \wedge \ldots)] \vee [\neg(t_1 < t_2) \wedge \exists x(x < t_2 \wedge x < t_3 \wedge \ldots)]$ et on est ramené au rang $r - 1$. De même si $l > 1$.

Si $k = l = 1$, la formule s'écrit $\exists x(x < t_1 \wedge u_1 < x \wedge x = v_1 \wedge \cdots \wedge x = v_m)$ qui pour $m \neq 0$ équivaut à $(v_1 = v_2 = \cdots = v_m) \wedge (u_1 < v_1 < t_1)$, et pour $m = 0$ à $u_1 < t_1$.

Pour $k = 0$, la formule est $\exists x(u_1 < x \wedge x = v_1 \wedge \cdots \wedge x = v_m)$ qui, pour $m = 0$ équivaut à $u_1 \neq 1$. De même pour $l = 0$, la formule équivaut à $t_1 \neq 0$. $\square$

[3]Voir le polycopié page 72.

3 Spectres

Soit Σ une signature, et F une formule close sur Σ. On appelle *spectre* de F, et on note $Sp(F)$ l'ensemble des entiers naturels n tels que F admette au moins un modèle dont l'ensemble de base possède exactement n éléments.

Question 3.1. *Proposer une signature Σ et une formule close F dont le spectre est l'ensemble des entiers naturels pairs.*

Solution : On considère la signature Σ réduite à un symbole de fonction d'arité 1 f, et le symbole de relation $=$. On considère la formule F suivante $\forall x(f(f(x)) = x \wedge \neg(x = f(x)))$.

Un modèle de cette formule impose que f soit une involution $f(f(x)) = x$. La relation binaire définie par $a \equiv b$ si $f(a) = b$ ou $f(b) = a$ est une relation d'équivalence dont chaque classe possède exactement deux éléments. Comme les classes constituent une partition, le cardinal d'un modèle doit être pair.

Réciproquement, pour $n = 2 * p$, on peut prendre le modèle dont l'ensemble de base est $\{1, 2, \cdots, n\}$, avec l'application f qui à k associe $k + p$ pour $1 \leq k \leq p$ et $k - p$ pour $p + 1 \leq k \leq n$. $\square$

Question 3.2. *Montrer que toute théorie dont le spectre est infini possède au moins un modèle dont l'ensemble de base est infini. (indication: on pourra utiliser le théorème de compacité et et une famille de formules bien choisie).*

Solution : Soit G une formule close dont le spectre est infini sur un signature Σ. Pour chaque entier $k \geq 1$, on note F_k la formule $\exists v_0 \exists v_1 \ldots \exists v_k \bigwedge_{0 \leq i < j \leq k} \neg(v_i = v_j)$.

Soit T la théorie $\{G\} \cup \{F_k | k \in \mathbb{N}\}$. Pour un entier N quelconque, G admet au moins un modèle de cardinal supérieur ou égal à $N + 1$, puisque le spectre de G est infini. Un tel modèle est un modèle aussi de la théorie $\{G\} \cup \{F_1, F_2, \ldots, F_N\}$. Cela prouve que toute partie finie de T admet un modèle. Par le théorème de compacité, T en possède un également.

Or un modèle de T n'est rien d'autre qu'un modèle infini de G. $\square$

4 NP-complétude

On a vu en cours que le problème de décision 3-COLORABILITE*:*

- ***Donnée**: Un graphe (fini) $G = (V, E)$.*
- ***Réponse**: Décider s'il existe un coloriage du graphe utilisant au plus* 3 *couleurs*

est NP-complet (On rappelle que le coloriage d'un graphe est un façon de colorer les sommets du graphe de telle sorte qu'aucune arête possède deux extrémités de la même couleur).

On s'intéresse à prouver la NP-complétude de différentes variantes du problème 3-COLORABILITE dans cet exercice: on utilisera (ou pourra utiliser) à chaque fois la NP-complétude du problème 3-COLORABILITE.

Question 4.1. *Montrer que le problème de décision* 4-COLORABILITE*:*

- ***Donnée**: Un graphe (fini) $G = (V, E)$.*
- ***Réponse**: Décider s'il existe un coloriage du graphe utilisant au plus* 4 *couleurs.*

est NP-complet.

Solution : Ce problème est clairement dans NP: la donnée d'une coloriage des sommets constitue un certificat vérifiable en temps polynomial: il suffit de vérifier qu'aucune arête possède deux extrémités de la même couleur.

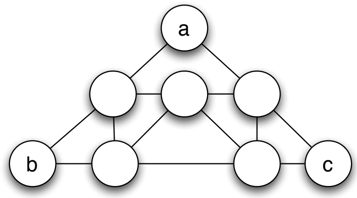
La réduction à partir de 3-COLORABILITE est la suivante.

Considérons une instance du problème 3-COLORABILITE composée du graphe $G = (V, E)$. Nous allons construire une instance du problème 4-COLORABILITE correspondant au graphe G' telle que $G' = (V \cup \{u\}, E \cup \{(u, v) : v \in V\})$ avec u un sommet d'appartenant pas à V. En effet G' est une copie du graphe G avec un sommet supplémentaire u qui est voisin de tous les sommets de G.

Cette réduction est clairement polynomiale puisqu'on rajoute un sommet et $|V|$ arêtes.

Il est facile de voir que G possède une coloration de k couleurs si et seulement si G' possède une coloration de $k + 1$ couleurs. □

On considère dans les questions qui suivent le graphe H suivant:



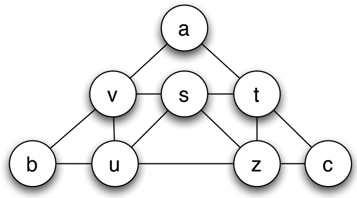
Question 4.2. *Montrer que ce graphe ne possède pas de coloration du graphe utilisant au plus* 2 *couleurs.*

Solution : Le graphe H a comme sous-graphe une clique de 3 sommets (triangle). Il est impossible de colorier une clique de 3 sommets en 2 couleurs.

□

Question 4.3. *Montrer que dans toute coloration du graphe utilisant au plus* 3 *couleurs, a, b et c sont de même couleur.*

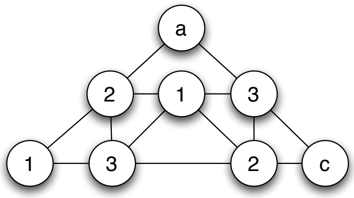
Solution : Commençons tout d'abord par nommer tous les sommets de graphe H de la façon suivante:



Soit C une coloration utilisant au plus 3 couleurs que l'on notera 1, 2, 3. Nous notons par $C(v)$ la couleur du noeud v. Sans perte de généralité, nous supposerons que $C(b) = 1$.

- Comme les sommets b, u, v forment un triangle, ils sont tous de couleurs différentes. Sans perte de généralité, nous supposerons que $C(v) = 2$ et $C(u) = 3$.
- Les sommets u, v, s forment un triangle et donc ils sont tous de couleurs différentes. Comme $C(v) = 2$ et $C(u) = 3$, on a $C(s) = 1$.
- Comme les sommets s, u, z forment un triangle et comme $C(s) = 1$ et $C(u) = 3$, on a $C(z) = 2$.

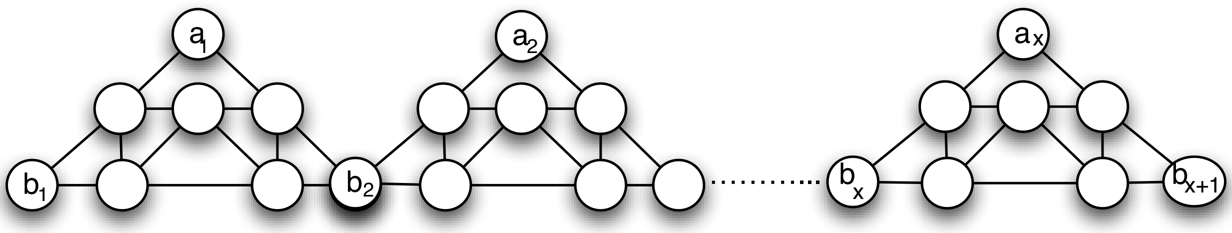
- Comme les sommets s, t, z forment un triangle et comme $C(s) = 1$ et $C(z) = 2$, on a $C(t) = 3$.
- Comme les sommets c, t, z forment un triangle et comme $C(t) = 3$ et $C(z) = 2$, on a $C(c) = 1$.
- Comme le sommet a est incident aux sommets v et au sommet t, on a $C(a) = 1$.



Donc on a bien que dans toute coloration du graphe utilisant au plus 3 couleurs, a, b et c sont de même couleur.

□

Question 4.4. *On considère le graphe H_x correspondant à x copies de H de la façon suivante :*



Montrer que dans toute coloration du graphe H utilisant au plus 3 couleurs, les sommets $(a_i)_{1 \leq i \leq x}$, $(b_i)_{1 \leq i \leq x+1}$ sont de même couleur.

Solution : Le graphe H_x est x copies de H. Par la question précédente : les sommets $(a_i)_{1 \leq i \leq x}$ et $(b_i)_{1 \leq i \leq x+1}$ sont de même couleur. □

Question 4.5. *Prouver que le problème de décision* 4DEG-3-COLORABILITE*:*

- ***Donnée**: Un graphe (fini) $G = (V, E)$ dont tous les sommets sont de degré au plus* 4
- ***Réponse**: Décider s'il existe un coloriage du graphe utilisant au plus* 3 *couleurs.*

est NP-complet.

(Rappel: on admet la NP-complétude du problème 3-COLORABILITE*).*

Solution : On peut remarquer que 4DEG-3-COLORABILITE est un sous-problème de 3-COLORABILITE.

Comme 3-COLORABILITE est dans NP, cela implique que 4DEG-3-COLORABILITE l'est aussi.

La réduction est la suivante. Considérons une instance du problème 3-COLORABILITE composée du graphe $G = (V, E)$. Pour tout sommet v, nous allons introduire tout d'abord une numérotation arbitraire des arêtes incidentes à v. Notons par $f_v(e)$ le numéro de l'arête e incidente en v.

Nous allons construire une instance du problème 4DEG-3-COLORABILITE correspondant au graphe G'.

- pour chaque sommet v de G, nous lui associons un graphe H_d dans G' où d est le degré de v. Par souci de simplification, nous renommerons les sommets a_i en les sommets v_i pour tout entier i compris entre 1 et d.

- pour chaque arête $e = (v, u)$ de G, nous lui associons une arête dans G' qui relie le sommet $v_{f_v(e)}$ avec $u_{f_u(e)}$

Le graphe G' est bien un graphe de degré au plus 4.

Cette réduction est clairement polynomiale puisqu'on rajoute deux graphes de type H par arête de G.

Nous allons prouver que si G possède une coloration de 3 couleurs, alors G' possède une coloration de 3 couleurs.

Supposons que G possède une coloration C de 3 couleurs. Nous allons construire une coloration C' de 3 couleurs pour le graphe G'.

Pour chaque sommet v de G, $C'(v_i) = C(v)$ pour tout entier i compris entre 1 et le degré de v. Le graphe associé au sommet v est ensuite coloré en reprenant le résultat de la question précédente.

Maintenant, il suffit de vérifier que C' est bien une coloration. Pour cela il suffit de vérifier que chaque arête correspondant à une arête $e = (u, v)$ de G possède deux extrémités de couleurs différentes. L'arête $(v_{f_v(e)}, u_{f_u(e)})$ a deux extrémités ayant comme couleur $C'(v_{f_v(e)})$ et $C'(u_{f_u(e)})$ respectivement. Nous avons par construction $C'(u_{f_u(e)}) = C(u)$ et $C'(v_{f_v(e)}) = C(v)$. Comme C est une coloration de trois couleurs, et que v et u sont voisins, on a $C(u) \neq C(v)$. On peut en déduire que l'arête $(v_{f_v(e)}, u_{f_u(e)})$ a deux extrémités de couleur différentes.

Donc G' possède une coloration de 3 couleurs.

Maintenant, nous allons prouver la contraposée.

Supposons que G' possède une coloration C' de 3 couleurs. Nous allons construire une coloration C de 3 couleurs pour le graphe G.

Pour chaque sommet v de G, est associé un graphe de type H. La couleur $C(v)$ du sommet v pour la coloration C sera la même que la coloration de $C'(v_1)$. Il faut maintenant vérifier que C est bien une coloration du graphe G.

D'après la question précédente $C'(v_i) = C'(v_1)$ pour tout entier i compris entre 1 et le degré de v dans G.

Pour cela il suffit de vérifier que chaque arête correspondant à une arête $e = (u, v)$ de G possède deux extrémités de couleurs différentes. Il faut prouver que $C(u) \neq C(v)$. Par construction nous avons $C'(v_{f_v(e)}) = C(v)$ et $C'(u_{f_u(e)}) = C(u)$. Comme $(v_{f_v(e)}, u_{f_u(e)})$ est une arête de G', par définition d'une coloration nous avons $C'(v_{f_v(e)}) \neq C'(u_{f_u(e)})$ et donc par conséquence $C(u) \neq C(v)$. Donc C est bien une coloration de 3 couleurs de G.

$\square$

5 Fonctions affines par morceaux

La configuration d'une machine de Turing (à 1 ruban) peut se coder par un triplet (q, u, v) comme dans le transparent 16 du cours 4: $q \in Q$ désigne l'état de la machine, et u, v désignent le contenu respectivement à gauche et à droite de la tête de lecture du ruban, la tête de lecture étant sur la première lettre de v. On suppose que v est écrit de gauche à droite, et u de droite à gauche.

On peut supposer sans perte de généralité que l'alphabet d'entrée et de travail (hormis le caractère B de blanc) est l'alphabet $\Sigma = \{0, 1\}$. On peut aussi supposer que $Q = \{0, 1, \dots, m-1\}$.

Un mot $u = u_1 u_2 \dots u_n \in \Sigma^*$ sur l'alphabet $\Sigma = \{0, 1\}$ peut se coder par le rationnel

$$\gamma(u) = \sum_{i=1}^{n} \frac{2u_i}{4^i}.$$

La configuration $C = (q, u, v)$ peut alors se coder par $(q, \gamma(u), \gamma(v)) \in [0, m] \times [0, 1]^2$.

Question 5.1. *Supposons que le programme de la machine de Turing ordonne, dans la configuration C, d'écrire le symbole $a \in \{0, 1\}$, de se déplacer vers la gauche et d'aller dans l'état q'.*

Montrer que le codage de la nouvelle configuration C' à partir de celle de C s'obtient en appliquant une fonction affine par morceaux à chaque composante de celle de C. Montrer que l'on peut supposer la fonction affine par morceaux continue.

Solution : On a $C' = (q', u', v')$, avec $\gamma(v') = \gamma(v)/4 + 2a/4$, $\gamma(u') = 4 * \gamma(u) - b$, avec $b = 0$ si $\gamma(u) \in [0, 1/4]$ et $b = 2$ si $\gamma(u) \in [1/2, 3/4]$ (peut importe la valeur de b pour $\gamma(u)$ hors de ces intervalles).

Puisque la valeur de b n'importe pas en dehors de ces intervalles, on peut compléter la fonction pour qu'elle soit continue. □

Question 5.2. *Prouver que pour toute machine de Turing M, on peut construire une fonction continue affine par morceaux $f : \mathbb{R}^3 \to \mathbb{R}^3$ dont les itérations simulent l'évolution de M.*

Solution : On peut voir la fonction affine par morceaux $4 * \gamma(u) - b$ précédente comme une fonction affine avec deux morceaux: le morceau correspondant à $b = 0$ correspond au fait qu'on lit un 0 en face de la tête de lecture, et celui à $b = 1$ au fait qu'on lit un 1.

Selon le même principe, on peut construire une fonction affine par morceaux qui permet d'obtenir la configuration suivante à partir de la configuration courante: chaque morceau correspond à un état possible q + un lettre en face de la tête de lecture, et a pour effet de produire la nouvelle configuration par des décalages vers la droite ou vers la gauche à coup de multiplications et divisions par 4. □

Question 5.3. *Prouver que le problème suivant est indécidable: on se donne une fonction continue affine par morceaux $f : \mathbb{R}^3 \to \mathbb{R}^3$, un point de départ $x_0 \in \mathbb{R}^3$, un rectangle[4] R, et on veut savoir si la suite définie par $x_{t+1} = f(x_t)$ est telle que $x_t \in R$ pour un certain entier t.*

Solution : Par la construction précédente, le problème de l'arrêt se réduit à se problème. Etant donnée une machine M et une entrée w, on peut considérer la fonction continue affine par morceaux correspondante f_M, l'entrée x_0 codant la configuration initiale correspondante, et $R = \{q_a\} \times [0, 1]^2$ où q_a est l'état d'acceptation de M. (f_M, x_0, R) est une instance positive du problème si et seulement si M accepte w. □

[4]sous-ensemble rectangulaire d'un hyperplan.