Examen du cours de L3: Calculabilité

3 novembre 2016, durée: 3 heures

Tous les documents sont autorisés, les appareils électroniques sont interdits. Les résultats vus en TD, s'ils sont utilisés, doivent être redémontrés.

1 (16 points)

Pour chacun des problèmes suivants, dire s'ils sont décidables ou non. Justifier.

1. **Donnée:** (Le code d')une machine de Turing M, un mot w et un entier n
   Question: M accepte w après au plus n étapes de calcul
2. **Donnée:** (Le code d')une machine de Turing M dont l'alphabet est $\{0, 1, B, \$\}$
   Question: $L(M) = \{0, 1\}^*$
3. **Donnée:** (Le code d')une machine de Turing M
   Question: il existe un mot w tel que M s'arrête quand elle est exécutée sur la donnée w.
4. **Donnée:** `pas de donnée`
   Question: Le problème de correspondance de Post sur un alphabet à 5 lettres et dans lequel tous les mots sont de longueur au plus 2 est décidable.
5. **Donnée:** Les codes de deux machines de Turing M_1, M_2
   Question: $L(M_1) \subseteq L(M_2)$ ou $L(M_2) \subseteq L(M_1)$.
6. **Donnée:** Une machine de Turing M et un mot w
   Question: M repasse au moins une fois dans une configuration où la tête de lecture est en début de ruban.
7. **Donnée:** Une machine de Turing M qui calcule en temps quadratique.
   Question: $L(M) = \emptyset$
8. **Donnée:** Une fonction récursive primitive à un argument f
   Question: Il existe au moins un entier n tel que $f(n) = 0$

2 (8 points)

Si V est un vecteur de $\mathbb{Z}^n$ et S est un ensemble de matrices $n \times n$ à coefficients dans $\mathbb{Z}$, l'ensemble des *vecteurs accessibles à partir de V, sous l'action de S*, noté $A(V, S)$ est le plus petit ensemble de vecteurs de $\mathbb{Z}^n$ tel que $V \in A(V, S)$ et, si $M \in S$ et $V \in A(V, S)$, alors $M\,V \in A(V, S)$.

Montrer que le problème suivant est indécidable:

Donnée: Un entier n, un vecteur $V \in \mathbb{Z}^n$, un ensemble S de trois matrices $n \times n$ à coefficients dans $\mathbb{Z}$

Question: le vecteur nul est dans $A(V, S)$.

Solution

1

1. Ce problème est décidable: On construit une machine M_0 qui, sur la donnée M, w, n, copie n sur un ruban auxilliaire et simule la machine universelle sur $< M, w >$ en décrémentant à chaque étape simulée le compteur n.

   Si n atteint 0, alors M_0 rejette et si M s'arrête en moins de n étapes, M_0 accepte.

   M_0 s'arrête sur toute donnée et $< M, w >, n) \in L(M_0)$ ssi M s'arrête sur w en moins de n étapes.

   Taux de réussite: 75%.
   La seule erreur significative est de ne pas utiliser explicitement la machine universelle: quand on dit "M' simule M sur w", cela signifie que le code de M est utilisé par M'. Il est ici incorrect de dire qu'on construit une machine M' qui simule M sur w, puisque le code de M' ne dépend pas de celui de M.
   Les copies n'ayant pas fait référence à la machine universelle ont obtenu au maximum 75% des points.

2. C'est indécidable.

   On remarque d'abord que le problème suivant est indécidable:

   Donnée: le code d'une machine de Turing M sur l'alphabet $\{0, 1, \$, B\}$

   Question: M s'arrête sur le mot vide

   En effet, le problème, sans restriction sur l'alphabet, a été montré indécidable en cours. On peut ensuite le réduire au problème ci-dessus en codant un alphabet quelconque sur un alphabet à deux lettres.

   Ensuite, on réduit ce problème de l'arrêt restreint au problème de l'énoncé: Soit M' la machine qui, sur la donnée $x \in \{0, 1\}^*$, ignore x et simule M sur ϵ. Si M s'arrête, M' accepte. $L(M') = \{0, 1\}^*$ ssi M s'arrête sur ϵ.

   Taux de réussite: 97%

   Commentaire: L'idée était d'appliquer le théorème de Rice, mais l'énoncé est mal fait (il fallait ne pas restreindre l'alphabet de la machine). On ne peut pas, en toute rigueur, appliquer le théorème de Rice tel que vu en cours puisque, si M est une machine sur l'alphabet $\{0, 1, \$, B\}$, il existe des machines sur un autre alphabet qui acceptent le même langage. Il ne s'agit donc pas d'une propriété "des langages récursivement énumérables" mais "des langages récursivement énumérables sur un alphabet fixé, de cardinal au moins 3". Les élèves ayant appliqué le théorème de Rice ont eu les points. Ceux qui ont fait une réduction correcte ont eu, en plus, un bonus.

3. C'est indécidable. On réduit le problème de l'arrêt. À la donnée M, w du problème de l'arrêt, on associe la machine M' qui ignore son entrée et simule M sur w. Cette réduction est calculable: il suffit d'effacer le ruban d'écire w, puis ajouter le code de M.

De plus, M s'arrête sur w ssi M' s'arrête sur toute entrée ssi M' s'arrête sur au moins une entrée.

Taux de réussite: 87%

4. Ce problème est décidable: la machine qui renvoie toujours oui ou toujours non résoud la question.

   Taux de réussite: 88%

5. Le problème est indécidable. Tout d'abord on remarque que, par le théorème de Rice, le problème, étant donnée une machine M_1, est ce que $L(M_1) \subseteq \{\epsilon\}$ ou $\{\epsilon\} \subseteq L(M_1)$ est indécidable. En effet, il s'agit d'une propriété des langages récursivement énumérables et elle est satisfaite par la machine qui accepte le mot vide et aucun autre mot et n'est pas satisfaite par une machine qui accepte le langage $\{a\}$ où $a \neq \epsilon$.

   On réduit ensuite ce problème à celui de l'énoncé en choisissant pour M_2 une machine telle que $L(M_2) = \{\epsilon\}$. ($L(M_1) \subseteq L(M_2)$ ou $L(M_2) \subseteq L(M_1)$) ssi $L(M_1) \subseteq \{\epsilon\}$ ou $\{\epsilon\} \subseteq L(M_1)$.

   Taux de réussite: 80%
   Commentaire: on ne peut pas appliquer directement le théorème de Rice à une propriété de paires de langages récursivement énumérables. Ceux qui ont fait cette erreur n'ont obtenu que la moitié des points.

6. C'est indécidable. On réduit le problème de l'arrêt. Soit M_1, w la donnée du problème de l'arrêt.

   On construit d'abord une machine M_2 sur un alphabet augmenté du symbole \$′, les transitions à partir de \$′ étant les mêmes que celles à partir de \$, en écrivant \$′ à la place d'écrire \$. L'application qui à $< M_1, w >$ associe $< M_2, w >$ est calculable.

   On construit ensuite une machine M qui commence par écrire le mot $\$'w$ sur son ruban (en ignorant son entrée). On place ensuite la tête de lecture de M devant \$′. M simule ensuite M_2. Si M_2 est sur le point de s'arrêter, alors M revient en tout début de ruban et s'arrête.

   La réduction est calculable et, de plus, comme, dans la table de transition de M_1, la lecture de \$ entraine un déplacement à droite, dans la table de M_2, la lecture de \$′ entraine aussi un déplacement à droite. M ne se déplacera donc jamais à gauche en lisant \$′, excepté si M_1 s'arrête sur w. Dans ce dernier cas, par construction, la tête de lecture de M revient en début de ruban: M_1 s'arrête sur w ssi M revient au moins une fois en tête de ruban (quelle que soit la donnée).

   Taux de réussite: 67%. Principale erreur: la réduction est incorrecte; on n'a pas l'équivalence entre $f(< M, w >) \in P_6$ et M s'arrête sur w.

7. C'est indécidable. On réduit le complémentaire du problème de l'arrêt. Soient M, w les données du problème de l'arrêt.

   On construit d'abord une machine M' à plusieurs rubans: la donnée x est sur le premier ruban. M' commence par écrire w sur le second ruban.

Sur la donnée x, la machine M' effectue au plus $|x|$ étapes du calcul de M sur w. Si M s'arrête, alorsM' accepte.

Le deuxième ruban est donc utilisé ici pour simuler M.

Si M s'arrête sur w après n étapes de calcul, alors M' accepte tous les mots de longueur au moins n. Si M ne s'arrête pas sur w, alors $L(M') = \emptyset$. Donc $L(M') = \emptyset$ ssi M ne s'arrête pas sur w.

M' calcule en temps linéaire avec deux rubans, donc en temps quadratique avec un seul ruban.

Taux de réussite: 37%
Erreurs courantes: 1) On ne peut pas appliquer le théorème de Rice car ce n'est pas une propriété des langages récursivement énumérables. 2) Le temps de calcul d'une machine de Turing s'apprécie sur une machine à un seul ruban; 90% des points à ceux qui dont c'est la seule erreur 3) Simuler n^2 étapes de calcul n'est pas évident en temps quadratique, même avec deux rubans.

8. C'est indécidable. On réduit le problème de l'arrêt.

   On a vu en cours que, en codant les configurations des machines de Turing par des entiers, pour toute machine de Turing M, la fonction g qui à n, γ où γ est le code d'une configuration de M associe le code γ' de la configuration obtenue après n mouvements de M à partir de γ, ou bien 0 si M s'arrête en moins de n étapes à partir de γ, est une fonction primitive récursive.

   Si γ_0 est le code de la configuration initiale de M sur w, $f(n) = g(n, \gamma_0)$ s'annule si et seulement si M s'arrête sur w.

   Taux de réussite: 20%. Principale erreur: réductions dans le mauvais sens !

2

On code le problème de correspondance de Post modifié. Soient $u_1, \ldots, u_n, v_1, \ldots, v_n$ une instance de PCP modifié.

Les mots sont vus comme des entiers en base $b > |\Sigma|$. On note $\overline{w}$ l'entier dénoté par w.

On construit d'abord le vercteur $V \in \mathbb{Z}^{3n+1}$ comme suit: $V_1 = \overline{u_1}, V_2 = \overline{u_2}, V_3 = 1$, $V_i = 0$ pour $4 \leq i \leq 3n$, $V_{3n+1} = 1$.

On construit ensuite les matrice P, M, G comme suit:

- $P_{i,i+3} = 1$ pour $i = 1, \ldots, 3n-3$, $P_{3n-2,1} = P_{3n-1,2} = P_{3n,3} = 1$ et $P_{3n-2,,j} = 0$ pour $j \neq 1$, $P_{3n-1,j} = 0$ pour $j \neq 2$, $P_{3n,j} = 0$ pour $j \neq 3$. Enfin $P_{3n+1,j} = 1$ ssi $j = 3n+1$.

  Autrement dit, si on note I_3 la matrice identité 3×3

$$P = \begin{pmatrix} \mathbf{0} & I_3 & \mathbf{0} & \ldots & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & I_3 & \ldots & \mathbf{0} & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \ldots & I_3 & 0 \\ I_3 & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

P effectue une permutation circulaire des $3n$ premières lignes, par blocs de 3 lignes.

- $$M = \begin{pmatrix} b^{|u_1|} & 0 & \overline{u_1} & b^{|u_2|} & 0 & \overline{u_2} & \cdots & b^{|u_n|} & 0 & \overline{u_n} & 0 \\ 0 & b^{|v_1|} & \overline{v_1} & 0 & b^{|v_2|} & \overline{v_2} & \cdots & 0 & b^{|v_n|} & \overline{v_n} & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & \cdots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix}$$

  Autrement dit, seules les 3 premières et la dernière lignes de M sont non nulles et $M_{1,3i+1} = b^{|u_i|}, M_{1,3i+2} = 0, M_{1,3i+3} = \overline{u_i}$ et $M_{1,3n+1} = 0$, $M_{2,3i+1} = 0, , M_{2,3i+2} = b^{|v_i|}, M_{2,3i+3} = \overline{v_i}$ et $M_{1,3n+1} = 0$, $M_{3,3i+2} = 1$ et $M_{3,j} = 0$ si $j \neq 2 \mod 3$.

- $$G = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 1 & -1 & -1 & 1 & -1 & -1 & \cdots & 1 \end{pmatrix}$$

  Autrement dit: seule la dernière ligne de G est non nulle et $g_{3n+1,3i+1} = 1$, $g_{3n+1,j} = -1$, pour $j \neq 1 \mod 3$.

On montre d'abord, par récurrence sur k, que le vecteur

$$V_{i_1,\ldots,i_k} = \begin{pmatrix} \overline{u_{i_1} \cdots u_{i_k}} \\ \overline{v_{i_1} \cdots v_{i_k}} \\ 1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

est dans $A(V_1, S)$ si $i_1 = 1$: c'est le cas pour $k = 1$ puisque $V_{i_1} = V$.

$$V_{i_1 \cdots, i_{k+1}} = M\ P^{i_{k+1}-1}\ V_{i_1,\ldots,i_k}$$

En effet, les seules lignes non nulles de $P^{i_{k+1}-1}\ V_{i_1,\ldots,i_k}$ sont les lignes d'indice $i_{k+1}, i_{k+1} + 1, i_{k+1} + 2, 3n + 1$ qui contiennent respectivement $\overline{u_{i_1} \cdots u_{i_k}}, \overline{v_{i_1} \cdots v_{i_k}}, 1$. $MP^{i_{k+1}-1}\ V_{i_1,\ldots,i_k}$ est un vecteur dont toutes les composantes sont nulles, sauf les 3 premières et la dernière, qui valent respectivement:

- $b^{|u_{i_{k+1}}|} \times \overline{u_{i_1} \cdots u_{i_k}} + \overline{u_{i_{k+1}}} \times 1 = \overline{u_{i_1} \cdots u_{i_{k+1}}}$
- $b^{|v_{i_{k+1}}|} \times \overline{v_{i_1} \cdots v_{i_k}} + \overline{v_{i_{k+1}}} \times 1 = \overline{v_{i_1} \cdots v_{i_{k+1}}}$
- 1, 1.

Si PCP modifié a une solution: $u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k}$, alors $\overline{u_{i_1} \cdots u_{i_k}} = \overline{v_{i_1} \cdots v_{i_k}}$ et donc $G\, V_{i_1,\ldots,i_k} = 0 \in A(V,S)$.

Réciproquement, montrons que tous les vecteurs de $A(V,S)$ sont de l'une des formes suivantes:

- $P^j V_{i_1,\ldots,i_k}$
- $W_\alpha = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \alpha \end{pmatrix}$

Pour cela, il suffit de calculer l'action de P, M, G sur les vecteurs d'une de ces deux formes:

- $P \cdot P^j V_{i_1,\ldots,i_k} = P^{j+1} V_{i_1,\ldots,i_k}$
- $P \cdot W_\alpha = W_\alpha$
- $M \cdot P^j V_{i_1,\ldots,i_k} = V_{i_1,\ldots,i_k,i_j}$
- $M \cdot W_\alpha = W_\alpha$
- $G \cdot P^j V_{i_1,\ldots,i_k} = W_{\overline{u_{i_1}\cdots u_{i_k}} - \overline{v_{i_1}\cdots v_{i_k}}}$
- $G \cdot W_\alpha = W_\alpha$

ll en résulte que $W_0 \in A(V,S)$ ssi il existe $i_1, \ldots, i_k$ tels que $\overline{u_{i_1} \cdots u_{i_k}} - \overline{v_{i_1} \cdots v_{i_k}} = 0$

Taux de réussite: 13%
Commentaire: le problème est encore indécidable si on prend 2 matrices au lieu de 3. C'est un problème ouvert célèbre de savoir si, étant donnés une seule matrice M et un vecteur V, il existe dans $A(M,V)$ un vecteur dont la première composante est nulle. (Problème des récurrences linéaires)