

# Partiel-devoir à la maison de calculabilité, 2023

Tous les documents sont autorisés. Les résultats vus en TD ou ailleurs qu'en cours, s'ils sont utilisés, doivent être redémontrés. Ceux vus en cours, même les résultats admis, ne doivent pas être redémontrés, mais seront cités de façon non ambiguë. Seules les notions et notations du cours — de préférence celles des transparents — seront admises dans les réponses.

On rappelle que  $\Sigma^*$  est l'ensemble des mots sur l'alphabet  $\Sigma$ , y compris le mot vide  $\epsilon$ .  $\Sigma^+$  dénote l'ensemble des mots non vides sur  $\Sigma$ .

## 1 Indécidables ou non ?

Pour chacun des problèmes suivants, dire s'ils sont décidables ou non. Justifier. Dans le cas où un problème est indécidable, et chaque fois que ce sera possible, on exhibera une réduction à partir d'un autre problème indécidable, que l'on citera. Si cette réduction a déjà été vue en cours, plutôt que de la redécrire complètement, rappelez cette réduction et dites quelles modifications vous lui apportez.

On note conventionnellement  $n$  ou  $|x|$  la taille de l'entrée  $x$  d'une machine de Turing. On rappelle qu'une machine termine en temps  $f(n)$  si et seulement si toutes ses traces d'exécution, sur toute entrée  $x$ , sont de longueur au plus  $f(n)$ .

**Question 1** **Entrée :** Deux codes de machines de Turing à une bande  $\langle M_1 \rangle^{\text{bin}}$  et  $\langle M_2 \rangle^{\text{bin}}$  ;

**Question :** Existe-t-il un mot accepté à la fois par  $M_1$  et par  $M_2$  ?

**Question 2** **Entrée :** un code de machine de Turing à une bande  $\langle M \rangle^{\text{bin}}$ , un entier  $k$  écrit en binaire ;

**Question :** la machine  $M$  termine-t-elle en temps  $k$  ? (autrement dit, pour toute entrée  $x$ , la machine  $M$ , démarrée sur l'entrée  $x$ , s'arrête-t-elle en au plus  $k$  étapes ?)

**Question 3** **Entrée :** un code de machine de Turing à une bande  $\langle M \rangle^{\text{bin}}$ , un entier  $k$  écrit en binaire ;

**Question :** pour toute entrée  $x$  telle que  $M$  s'arrête sur l'entrée  $x$ , la machine  $M$  termine-t-elle en temps  $k \cdot n^2$  sur  $x$  ? (autrement dit, est-il vrai que

pour toute entrée  $x$ , soit  $M$  ne s'arrête pas sur  $x$  soit  $M$  s'arrête en au plus  $k.n^2$  étapes sur l'entrée  $x$  ?)

**Question 4** **Entrée** : un système de réécriture  $S$  de mots sur un alphabet  $A$ , un mot  $w_0 \in A^*$  et un entier  $k \in \mathbb{N}$  ;

**Question** : existe-il un mot  $w$  de taille  $|w| > k$  tel que  $w_0 \rightarrow^* w$  via  $S$  ?

## 2 Variantes de PCP

On appelle **PCP'** le problème suivant. (Je vous laisse chercher la différence avec **PCP**.)

**Entrée** : Une liste finie de couples  $(u_1, v_1), \dots, (u_n, v_n)$  de mots non vides, sur un alphabet (fini) quelconque.

**Question** : existe-t-il des indices  $i_1, \dots, i_k$  pour un certain  $k \geq 1$  tels que  $u_{i_1}u_{i_2} \cdots u_{i_k} = v_{i_1}v_{i_2} \cdots v_{i_k}$  ?

On notera que la chaîne de réductions vue en cours montre non seulement que **PCP**, mais en fait **PCP'**, est indécidable.

On appelle **binPCP** le problème suivant.

**Entrée** : Une liste finie de couples  $(u_1, v_1), \dots, (u_n, v_n)$  de mots non vides sur l'alphabet  $\{0, 1\}$ .

**Question** : existe-t-il des indices  $i_1, \dots, i_k$  pour un certain  $k \geq 1$  tels que  $u_{i_1}u_{i_2} \cdots u_{i_k} = v_{i_1}v_{i_2} \cdots v_{i_k}$  ?

**Question 5** Exhiber une réduction de **PCP'** vers **binPCP**, et en déduire que **binPCP** est indécidable.

On appelle **bin1PCP** le problème suivant.

**Entrée** : Une liste finie de couples  $(u_1, v_1), \dots, (u_n, v_n)$  de mots sur l'alphabet  $\{0, 1\}$ , où chaque  $u_i$  et chaque  $v_i$  se termine par un 1.

**Question** : existe-t-il des indices  $i_1, \dots, i_k$  pour un certain  $k \geq 1$  tels que  $u_{i_1}u_{i_2} \cdots u_{i_k} = v_{i_1}v_{i_2} \cdots v_{i_k}$  ?

**Question 6** Montrer par une réduction appropriée que **bin1PCP** est indécidable.

## 3 Automates probabilistes

Un automate probabiliste est, grosso modo, un automate fini usuel, mais avec des probabilités de transition. Formellement, un *automate probabiliste* est un quintuplet  $\mathcal{A} \stackrel{\text{def}}{=} (Q, \Sigma, q_0, \Delta, F)$ , où :

- $Q$  est un ensemble fini, dit d'*états* ;
- $\Sigma$  est un ensemble fini, l'*alphabet* ;

- $q_0 \in Q$  (l'état initial) ;
- $F \subseteq Q$  (l'ensemble des états finaux) ;
- $\Delta: Q \times \Sigma \rightarrow \mathcal{D}(Q)$  est la *fonction de transition* ;  $\mathcal{D}(Q)$  est l'ensemble des *distributions* sur  $Q$ , c'est-à-dire l'ensemble des fonctions  $\mu: Q \rightarrow [0, 1]$  telles que  $\sum_{q \in Q} \mu(q) = 1$  ( $\mu(q)$  est la *probabilité* de  $q$  pour cette distribution).

On peut calculer sur des automates probabilistes  $\mathcal{A}$ , comme sur des automates usuels, à un détail près : on doit pouvoir représenter les probabilités, et calculer dessus. On appellera automate probabiliste *rationnel* tout automate probabiliste dont les probabilités  $\Delta(q, a)(q')$  sont des rationnels dans  $[0, 1]$ .

La représentation utilisée d'un automate probabiliste rationnel  $\mathcal{A}$  sur une machine de Turing consiste typiquement à numéroter les états de  $Q$ , et écrire les composantes de  $\mathcal{A}$  les unes après les autres, séparés par un caractère frais ;  $\Delta$  est représenté par une liste de toutes les valeurs  $\Delta(q, a)(q')$  dans un ordre quelconque, ces valeurs (rationnelles)  $p/q$  étant écrites comme un couple de deux entiers naturels.

Étant donné un automate probabiliste  $\mathcal{A}$  comme plus haut, on définit la fonction  $\overline{\Delta}: Q \times \Sigma^* \rightarrow \mathcal{D}(Q)$  en posant, pour tout  $q \in Q$  :

- $\overline{\Delta}(q, \epsilon) \stackrel{\text{def}}{=} \delta_q$ , où  $\delta_q$  est la *distribution de Dirac* :  $\delta_q(q) \stackrel{\text{def}}{=} 1$ ,  $\delta_q(q') \stackrel{\text{def}}{=} 0$  pour tout  $q' \in Q \setminus \{q\}$  ;
- pour tout  $a \in \Sigma$ , pour tout  $w \in \Sigma^*$ , pour tout  $p \in Q$ ,  $\overline{\Delta}(q, aw)(p) \stackrel{\text{def}}{=} \sum_{q' \in Q} \Delta(q, a)(q') \cdot \overline{\Delta}(q', w)(p)$ .

Ceci définit  $\overline{\Delta}(q, w)$  par récurrence sur la longueur de mot  $w$  ;  $\overline{\Delta}(q, w)(p)$  est la probabilité, partant de l'état  $q$ , d'arriver à l'état  $p$  en lisant le mot  $w$ . La formule  $\overline{\Delta}(q, aw)(p) \stackrel{\text{def}}{=} \sum_{q' \in Q} \Delta(q, a)(q') \cdot \overline{\Delta}(q', w)(p)$  se lit : la probabilité d'aller de  $q$  à  $p$  en lisant  $w$  est la somme sur tous les états intermédiaires  $q'$  de la probabilité d'aller de  $q$  à  $q'$  en lisant  $a$ , multipliée par la probabilité d'aller de  $q'$  à  $p$  en lisant  $w$ .

La *probabilité d'acceptation*  $Pr_{\mathcal{A}}(w)$  (par l'automate probabiliste  $\mathcal{A}$ ) d'un mot  $w$  est, par définition, la somme  $\sum_{p \in F} \overline{\Delta}(q_0, w)(p)$ .

On notera les automates probabilistes sous forme graphique. Par exemple, l'automate probabiliste de la figure 1 est composé de :

- $Q \stackrel{\text{def}}{=} \{q_0, q_{\perp}, q_{\top}\}$  ;
- $\Sigma \stackrel{\text{def}}{=} \{0, 1\}$  ;
- l'état initial  $q_0$  est repéré par une flèche entrante isolée (complètement à gauche) ;
- l'unique état final (de  $F$ ) est repéré par une flèche sortant isolée, c'est  $q_{\top}$  ;

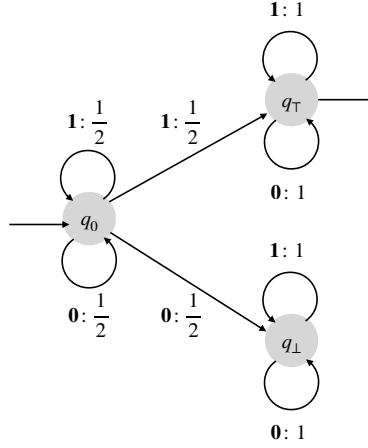


FIGURE 1 – L'automate probabiliste  $\mathcal{A}_{\text{bin}}$

- $\Delta(q_0, 0) \stackrel{\text{def}}{=} \{q_0 \mapsto \frac{1}{2}, q_\perp \mapsto \frac{1}{2}, q_\top \mapsto 0\}$  ;
- $\Delta(q_0, 1) \stackrel{\text{def}}{=} \{q_0 \mapsto \frac{1}{2}, q_\perp \mapsto 0, q_\top \mapsto \frac{1}{2}\}$  ;
- $\Delta(q, a) \stackrel{\text{def}}{=} \delta_q$  pour tout  $q \in \{q_\top, q_\perp\}$  et pour tout  $a \in \Sigma$ .

On notera que seules les probabilités strictement positives sont représentées dans la figure.

**Question 7** Étant donné un mot  $a_1 \cdots a_n$  sur l'alphabet  $\{0, 1\}$ , donner une formule explicite pour  $Pr_{\mathcal{A}_{\text{bin}}}(a_1 \cdots a_n)$ , et la justifier.

**Question 8** Soit  $\Sigma$  un alphabet. Pour toute fonction  $\varphi: \Sigma \rightarrow \{0, 1\}^*$ , on étend  $\varphi$  aux mots par  $\widehat{\varphi}(a_1 \cdots a_n) \stackrel{\text{def}}{=} \varphi(a_1) \cdots \varphi(a_n)$ . Construire un automate probabiliste  $\mathcal{A}_\varphi$  sur l'alphabet  $\Sigma$  tel que, pour tout  $w \in \Sigma^*$ ,  $Pr_{\mathcal{A}_\varphi}(w) = \text{bin}(\widehat{\varphi}(w))$ . La fonction  $\text{bin}$  envoie tout mot  $b_1 \cdots b_m$  sur l'alphabet  $\{0, n\}$  vers le réel  $0, b_1 \cdots b_m = \sum_{i=1}^m \frac{1}{2^i} b_i$ . Par « construire », on entend en particulier que l'on peut calculer  $\mathcal{A}_\varphi$  — qui devra en particulier être un automate probabiliste rationnel — à partir d'une table décrivant  $\varphi$  ; on n'aura pas besoin de justifier que  $\mathcal{A}_\varphi$  est calculable, mais ceci devra être intuitivement évident.

**Question 9** Pour chaque automate probabiliste rationnel  $\mathcal{A}$  sur un alphabet quelconque  $\Sigma$ , construire un automate probabiliste rationnel  $\neg \mathcal{A}$  sur  $\Sigma$  tel que  $Pr_{\neg \mathcal{A}}(w) = 1 - Pr_{\mathcal{A}}(w)$  pour tout mot  $w \in \Sigma^*$ .

**Question 10** Pour tout automate probabiliste  $\mathcal{A} \stackrel{\text{def}}{=} (Q, \Sigma, q_0, \Delta, F)$ , soit  $\bullet \mathcal{A}$  l'automate probabiliste  $(Q \cup \{\bullet\}, \Sigma, \bullet, \bullet \Delta, F)$ , où  $\bullet$  est un état frais (hors de  $Q$ ), et :

- pour tout  $a \in \Sigma$ , pour tout  $q' \in Q \cup \{\bullet\}$ ,  $\bullet \Delta(\bullet, a)(q') \stackrel{\text{def}}{=} \Delta(\bullet, q_0)(q')$  si  $q' \neq \bullet$ , 0 si  $q' = \bullet$  ;

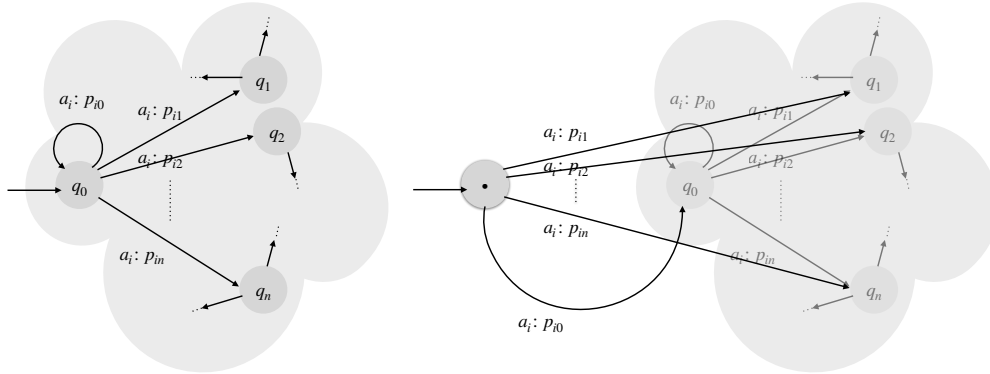


FIGURE 2 – La transformation de la **Question 10** : à gauche, l’automate probabiliste  $\mathcal{A}$ ; à droite, l’automate  $\bullet\mathcal{A}$ . Les lettres  $a_i$  parcourent l’alphabet  $\Sigma$ . On n’a détaillé que les transitions sortant de  $q_0$  pour une lettre  $a_i$  donnée.

— pour tout  $a \in \Sigma$ , pour tout  $q \in Q$ , pour tout  $q' \in Q \cup \{\bullet\}$ ,  $\bullet\Delta(q, a)(q') \stackrel{\text{def}}{=} \Delta(q, a)(q')$  si  $q' \neq \bullet$ , 0 sinon.

Voir la figure 2 pour une illustration. (Les probabilités  $p_{ij}$  sont égales à  $\Delta(q_0, a_i)(q_i)$ .) Que vaut  $Pr_{\bullet\mathcal{A}}(w)$ , pour tout  $w \in \Sigma^*$  ? Donner une preuve complète, en faisant attention aux cas limites.

**Question 11** Pour chaque couple d’automates probabilistes rationnels  $\mathcal{A}$  and  $\mathcal{A}'$  sur un même alphabet  $\Sigma$ , et pour chaque nombre rationnel  $\alpha$  dans  $[0, 1]$ , construire un automate probabiliste rationnel  $\mathcal{A} +_{\alpha} \mathcal{A}'$  sur  $\Sigma$  tel que pour tout mot non vide  $w \in \Sigma^+$ ,  $Pr_{\mathcal{A} +_{\alpha} \mathcal{A}'}(w) = \alpha \cdot Pr_{\mathcal{A}}(w) + (1 - \alpha) \cdot Pr_{\mathcal{A}'}(w)$ . Une description suffisamment claire (par exemple avec un dessin) de l’automate suffira, pas besoin d’une preuve pleine de symboles.

**Question 12** Soit  $\Sigma$  un alphabet. On se donne deux fonctions  $\varphi, \varphi' : \Sigma \rightarrow \{0, 1\}^*$  telles que  $\varphi(a)$  et  $\varphi'(a)$  sont des mots binaires se terminant par un 1, pour toute lettre  $a \in \Sigma$ . Montrer que pour tout mot non vide  $w \in \Sigma^+$ ,  $Pr_{\mathcal{A}_{\varphi+1/2} \neg \mathcal{A}_{\varphi'}}(w) = \frac{1}{2}$  si et seulement si  $\widehat{\varphi}(w) = \widehat{\varphi'}(w)$ .

**Question 13** Par réduction depuis **bin1PCP**, montrer que le problème suivant dit de *non-vacuité avec probabilité 1/2* :

**Entrée** : un automate probabiliste rationnel  $\mathcal{A} = (Q, \Sigma, q_0, \Delta, F)$  ;

**Question** :  $\mathcal{A}$  accepte-t-il un mot avec probabilité  $\frac{1}{2}$  ? (autrement dit, existe-t-il un mot  $w \in \Sigma^*$  tel que  $Pr_{\mathcal{A}}(w) = \frac{1}{2}$  ?) est indécidable.

Étant donnés deux automates probabilistes  $\mathcal{A} \stackrel{\text{def}}{=} (Q, \Sigma, q_0, \Delta, F)$  et  $\mathcal{A}' \stackrel{\text{def}}{=} (Q', \Sigma, q'_0, \Delta', F')$  sur le même alphabet  $\Sigma$ , on forme l’*automate probabiliste produit*  $\mathcal{A} \cdot \mathcal{A}'$  comme suit :

- son ensemble d'états est  $Q \times Q'$  ;
- son alphabet est  $\Sigma$  ;
- son état initial est  $(q_0, q'_0)$  ;
- sa fonction de transition envoie  $((q, q'), a)$  vers la distribution produit  $(p, p') \in Q \times Q' \mapsto \Delta(q, a)(p) \cdot \Delta'(q', a)(p')$  ;
- son ensemble d'états finaux est  $F \times F'$ .

On admettra que  $Pr_{\mathcal{A} \cdot \mathcal{A}'}(w) = Pr_{\mathcal{A}}(w) \cdot Pr_{\mathcal{A}'}(w)$  pour tout mot  $w \in \Sigma^*$ .

**Question 14** Montrer que le problème suivant, dit de *non-vacuité* d'un automate probabiliste, est indécidable.

**Entrée :** un automate probabiliste rationnel  $\mathcal{A} = (Q, \Sigma, q_0, \Delta, F)$ , un seuil  $\theta \in ]0, 1[$  ;

**Question :**  $\mathcal{A}$  accepte-t-il un mot avec probabilité  $\geq \theta$  ?

Il est conseillé de montrer que le problème reste indécidable si  $\theta$  est une constante fixée dans  $]0, 1[$ , que l'on précisera. (Si vous êtes curieux, le problème est en fait indécidable pour n'importe quelle constante  $\theta$  fixée dans  $]0, 1]$ . Le cas  $\theta < 1$  a été traité par Bertoni, Mauri et Torelli en 1977, et il a fallu attendre Gimbert et Oualhadj en 2010 pour obtenir la réponse dans le cas  $\theta = 1$ . Le problème est trivialement décidable si  $\theta = 0$ .)

**Question 15** Le problème suivant est-il décidable ?

**Entrée :** un automate probabiliste rationnel  $\mathcal{A} = (Q, \Sigma, q_0, \Delta, F)$  ;

**Question :**  $\mathcal{A}$  accepte-t-il un mot avec probabilité  $> 0$  ?