

Partiel-devoir à la maison de calculabilité, 2025

à rendre le 24 novembre 2025 au plus tard, à `jgl@lmf.cnrs.fr`

Correction.

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 Σ^* est l'ensemble des mots sur l'alphabet Σ , y compris le mot vide ϵ .

Je marque la difficulté ou la longueur de chaque question, telle que je la perçois, de $\square\square\square\square$ (trivial) à $\blacksquare\blacksquare\blacksquare\blacksquare$ (très difficile ou très long). Je considère très facile tout résultat qui est une conséquence triviale d'un résultat du cours ou d'une question précédente, aussi difficile que soit ce résultat.

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. Je n'aurai pas besoin de preuve de correction de la réduction, mais cette réduction devra être correcte ; notamment, s'il y a une difficulté à surmonter, vous devrez l'expliquer et dire comment vous la surmontez.

Question 1 $\blacksquare\square\square\square$ **Entrée :** le code $\langle M \rangle^{bin}$ d'une machine de Turing (à une bande), dont l'alphabet d'entrée contient au moins les deux lettres a et b ;

Question : pour tous les mots w acceptés par M , en notant $\#_w(c)$ le nombre d'occurrences d'une lettre c dans w , est-il vrai que $\#_w(a)^3 + 2\#_w(b)^3 \geq 3\#_w(a)\#_w(b) + 5$?

Pour les formalistes : on supposera que les codages des deux lettres a et b sont précisés à des positions fixées dans la table $\text{bin}_{\Sigma'}$, typiquement que ce sont les deux entrées qui suivent les codages de $0, 1, ;, \rightarrow, \downarrow, \leftarrow$, **accept** et **reject**.

Indécidable, par le théorème de Rice. La propriété à tester est extensionnelle, et :

- *il existe des machines de Turing M dont le langage vérifie la propriété ; la plus simple est celle qui ne s'arrête jamais, et dont le langage est vide ;*
- *il existe des machines de Turing M dont le langage ne vérifie pas la propriété ; la plus simple est celle qui n'accepte que le mot vide : dans ce mot $w \stackrel{\text{def}}{=} \epsilon$, $\#_w(a)^3 + 2\#_w(b)^3 = 0$ n'est pas supérieur ou égal à $3\#_w(a)\#_w(b) + 5 = 5$.*

Question 2 ■■■■ Le problème de *bouclage* d'une machine de Turing à deux bandes :

Entrée : Le code d'une machine de Turing $\langle M \rangle^{\text{bin}}$ (à deux bandes) ;

Question : partant de la configuration initiale γ_0 sur le mot d'entrée vide, la machine M boucle-t-elle ?

On dit que M *boucle* en partant de γ_0 s'il existe une configuration γ telle que $\gamma_0 \vdash_M^* \gamma \vdash_M^+ \gamma$. La notation $\gamma \vdash_M^+$ signifie « une suite non vide de transitions $\vdash_M$ ».

*Indécidable, par réduction à partir du problème de l'arrêt **Halt**.*

La réduction prend en entrée le code $\langle M \rangle^{\text{bin}}$ d'une machine de Turing à une bande M .

Dans un premier temps, elle construit une nouvelle machine de Turing M' qui, de façon cruciale, ne boucle jamais. Pour ceci, M' simule M sur sa première bande, et entre deux étapes, incrémente un compteur (en binaire, en unaire, peu importe) sur sa deuxième bande. Ceci garantit que M' ne passe jamais deux fois par la même configuration.

Dans un deuxième temps, on complète M' en une machine M'' qui, lorsque M' arrive en une configuration où M s'arrête, décide de boucler (revenir au même état, laisser la tête en place, réécrire la même lettre sous la bande, pour chacune des deux bandes).

Si M s'arrête sur l'entrée ϵ , alors M'' bouclera.

Si M ne s'arrête pas sur l'entrée ϵ , alors M'' se comporte comme M' et ne boucle donc jamais.

Le fait que le code de M'' soit calculable en fonction de celui de M est considéré comme clair.

Question 3 ■■■■ **Entrée :** une liste de couples de mots $(u_1, v_1), \dots, (u_m, v_m)$ sur un alphabet à deux lettres, où la longueur de u_i égale celle de v_i pour tout $i \in \{1, \dots, m\}$;

Question : y a-t-il des indices $i_1, \dots, i_k$ avec $k \geq 1$ tels que $u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k}$?

Décidable. S'il existe de tels indices, alors u_{i_1} et v_{i_1} sont égaux. Pour décider de la question, il suffit donc de tester s'il existe un $i \in \{1, \dots, m\}$ tel que $u_i = v_i$; on accepte dans ce cas, on rejette sinon.

D'autre part, on peut vérifier le format de l'entrée; notamment vérifier les longueurs des u_i et des v_i est calculable.

2 Présentations de monoïdes

Un *monoïde* est un ensemble M muni d'une opération binaire $\cdot$ associative (le *produit*) et d'un élément neutre 1 pour $\cdot$. On écrira souvent M plutôt que $(M, \cdot, 1)$ pour le monoïde.

Par exemple, Σ^* est un monoïde pour tout alphabet Σ , avec la concaténation pour $\cdot$ et le mot vide ϵ pour élément neutre.

On définit les notions suivantes :

- Un *homomorphisme* de monoïdes $f: M \rightarrow M'$ est une fonction qui préserve le produit (pour tous $m_1, m_2 \in M$, $f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$) et l'élément neutre ($f(1) = 1$).
- Un *isomorphisme* de monoïdes est un homomorphisme bijectif. Son inverse est alors aussi un isomorphisme. On dit que M et M' sont *isomorphes* si et seulement s'il existe un isomorphisme de M vers M' .
- Un *plongement* de monoïdes est un homomorphisme injectif. On dit que M *se plonge dans* M' si et seulement s'il existe un plongement de M dans M' .

Une *présentation* est la donnée (Σ, E) d'un ensemble Σ (l'*alphabet*) et d'un ensemble E de couples de mots de Σ^* . On ne suppose ni Σ ni E fini en général. Un couple $(u, v) \in E$ sera appelé une *relation*. Un tel ensemble *engendre* une congruence $\sim_E$, c'est-à-dire une relation d'équivalence compatible à la concaténation, définie comme suit. D'abord, E engendre une relation de réécriture $\rightarrow_E$, comme définie en cours : on a $w \rightarrow_E w'$ si et seulement si w s'écrit $w_1 u w_2$, w' s'écrit $w_1 v w_2$ pour un certain mot $w_1 \in \Sigma^*$, un mot $w_2 \in \Sigma^*$ et une relation $(u, v) \in E$. On symétrise cette relation et l'on définit $w \leftrightarrow_E w'$ si et seulement si $w \rightarrow_E w'$ ou $w' \rightarrow_E w$. Enfin, $\sim_E$ est la clôture réflexive transitive $\leftrightarrow_E^*$ de $\leftrightarrow_E$.

Étant donnée une présentation (Σ, E) , on peut former le monoïde quotient $\Sigma^*/\sim_E$. Ses éléments sont les classes d'équivalences $[w]_E$ de mots w de Σ^* pour $\sim_E$, le produit est défini par $[w]_E \cdot [w']_E \stackrel{\text{def}}{=} [ww']_E$, et l'élément neutre est $1_E \stackrel{\text{def}}{=} [\epsilon]_E$.

Une *présentation finie* est une présentation (Σ, E) telle que Σ et E sont finis.

On dit que (Σ, E) est une présentation d'un monoïde M si et seulement si M est isomorphe à $\Sigma^*/\sim_E$. Tout monoïde M a une présentation, par exemple la présentation triviale $(M, \{(m_1 m_2, m_1 \cdot m_2) \mid m_1, m_2 \in M\})$ (ici, m_1, m_2 sont juste deux lettres de M , de même que $m_1 \cdot m_2$), mais elle n'est pas finie en général. Un monoïde est à *présentation finie* si et seulement s'il existe une présentation finie (Σ, E) de M .

Question 4 ■■■■ Soit (Σ, E) une présentation. Supposons qu'il existe deux mots *init* et *end* dans Σ^* tels que :

- (a) pour tout $w \in \Sigma^*$ avec $\text{init} \leftrightarrow_E^* w$, il existe au plus un mot $w' \in \Sigma^*$ tel que $w \rightarrow_E w'$;
- (b) et il n'existe pas de mot $w' \in \Sigma^*$ tel que $\text{end} \rightarrow_E w'$.

Montrer que pour tout $w \in \Sigma^*$ tel que $\text{init} \leftrightarrow_E^* w$, $w \leftrightarrow_E^* \text{end}$ si et seulement si $w \rightarrow_E^* \text{end}$.

La direction seulement si est évidente : si $w = w_0 \rightarrow_E w_1 \rightarrow_E \dots \rightarrow_E w_n = \text{end}$ alors $w = w_0 \leftrightarrow_E w_1 \leftrightarrow_E \dots \leftrightarrow_E w_n = \text{end}$.

Supposons donc $w \leftrightarrow_E^* \text{end}$, par une suite $w = w_0 \leftrightarrow_E w_1 \leftrightarrow_E \dots \leftrightarrow_E w_n = \text{end}$.

On va démontrer que $w_k \rightarrow_E^* \text{end}$ pour tout $k \in \{0, 1, \dots, n\}$ par récurrence descendante (forte) sur k .

Si $k = n$, c'est évident.

Si $0 \leq k \leq n - 1$, alors par hypothèse de récurrence $w_{k+1} \rightarrow_E^* \text{end}$.

Si $w_k \rightarrow_E w_{k+1}$, on obtient $w_k \rightarrow_E w_{k+1} \rightarrow_E^* \text{end}$. Si $w_{k+1} \rightarrow_E w_k$, alors d'abord on ne peut pas avoir $w_{k+1} = \text{end}$ par l'hypothèse (b).

En particulier, $k + 1 \neq n$, donc $k \leq n - 2$. Il y a donc une étape de réécriture $w_{k+1} \rightarrow_E w_{k+2}$. L'hypothèse (a), que l'on peut utiliser car $\text{init} \leftrightarrow_E^* w_{k+1}$, implique alors que $w_k = w_{k+2}$. Par hypothèse de récurrence (forte) on a $w_{k+2} \rightarrow_E^* \text{end}$, donc $w_k \rightarrow_E^* \text{end}$. (Une autre possibilité est de partir d'une suite $w = w_0 \leftrightarrow_E w_1 \leftrightarrow_E \dots \leftrightarrow_E w_n = \text{end}$ de longueur n minimale, et alors ce dernière cas de figure ne peut pas avoir lieu.)

On conclut en prenant $k = 0$.

Question 5 ■■■■ Montrer que le problème suivant est indécidable :

Entrée : une présentation finie (Σ, E) , deux mots *init*, *end* $\in \Sigma^*$;

Question : $init \sim_E end$?

On reprend la réduction de **RHalt** vers **semiThue**_ε du cours (voir les transparents). En partant d'un code $\langle M \rangle^{bin}$ d'une machine de Turing M , cette réduction produit un système (A, R, w_0) . De R , on ne garde que les six (schémas de) règles codant les transitions de M , plus les règles $\llbracket qa \rightarrow \llbracket q$ avec $q \in \{\text{accept}, \text{reject}\}$ et $a \in \Sigma \cup Q^+$, mais sans les règles $\llbracket q \rrbracket \rightarrow \epsilon$. (On voit les règles $\ell \rightarrow r$ comme des relations (ℓ, r) , ici.) Ajoutons finalement la règle $\llbracket \text{reject} \rrbracket \rightarrow \llbracket \text{accept} \rrbracket$, et posons $end \stackrel{def}{=} \llbracket \text{accept} \rrbracket$.

Appelons l'ensemble résultant de règles E , et posons $\Sigma \stackrel{def}{=} E$. il a les propriétés suivantes :

- En posant $init \stackrel{def}{=} \llbracket q_0 \$ \rrbracket$, $init$ contient exactement une lettre du sous-alphabet Q^+ des états étendus, et chaque relation (u, v) de E a exactement une lettre de Q^+ dans u et une dans v . Donc les mots w tels que $init \leftrightarrow_E^* w$ ont exactement une occurrence d'un symbole de Q^+ , et alors il existe au plus une règle (u, v) de E qui s'applique pour réécrire w via $u \rightarrow v$, et elle ne s'applique qu'à une seule position. Ceci montre que (A, E) a la propriété (a) de la **Question 4**.
- Le mot end ne se réécrit (de gauche à droite) par aucune des règles de E . Donc la propriété (b) est vraie aussi.

Par une modification simple de la construction du cours, M s'arrête sur l'entrée ϵ si et seulement si $init \rightarrow_E^* end$. Or la **Question 4** nous dit que $init \rightarrow_E^* end$ est équivalent à $init \sim_E end$.

Finalement, Σ et E sont clairement calculables en fonction de $\langle M \rangle^{bin}$.

Question 6 ■■■ Raffiner la construction de la **Question 5** et montrer qu'il existe une présentation finie (Σ_U, E_U) et un mot end_U tels que le problème suivant est indécidable :

Entrée : un mot $init \in \Sigma_U^*$;

Question : $init \sim_{E_U} end_U$?

(Désolé, cette question n'est pas indépendante de la précédente. De plus, et même si vous pouvez déduire facilement la **Question 5** de la **Question 6**, vous devez répondre à la **Question 5** sans faire appel à la **Question 6**.)

Au lieu de prendre en entrée le code $\langle M \rangle^{bin}$ d'une machine de Turing M , on fixe pour M une machine de Turing universelle.

On construit $E_U \stackrel{def}{=} E$ comme à la **Question 5** (on n'a pas besoin de le calculer), et sans la règle $\llbracket \text{reject} \rrbracket \rightarrow \llbracket \text{accept} \rrbracket$, et l'on pose $end_U \stackrel{def}{=} \llbracket \text{accept} \rrbracket$.

La réduction transforme maintenant un mot $w \in \Sigma_U^*$ (dont on cherche à savoir s'il est accepté par la machine universelle) en $\text{init} \stackrel{\text{def}}{=} \llbracket q_0 \$ w \rrbracket$. Ceci est clairement calculable.

On notera $P(\Sigma, E)$ pour dire qu'une propriété P est vraie d'une présentation finie (Σ, E) . On dira aussi que (Σ, E) *satisfait* la propriété P , ou *vérifie* la propriété P . On notera $\neg P(\Sigma, E)$ pour dire que P est fausse de (Σ, E) .

Définition 1 (Propriété de Markov) Une propriété de Markov est une propriété P de présentations finies telle que :

- (A) P est extensionnelle : étant données deux présentations finies (Σ, E) et (Σ', E') de deux monoïdes isomorphes, $P(\Sigma, E)$ si et seulement si $P(\Sigma', E')$;
- (B) il existe une présentation finie (Σ_1, E_1) telle que $P(\Sigma_1, E_1)$;
- (C) il existe une présentation finie (Σ_2, E_2) telle que pour toute présentation finie (Σ, E) telle que $\Sigma_2^* / \sim_{E_2}$ se plonge dans $\Sigma^* / \sim_E$, $\neg P(\Sigma, E)$.

On dit parfois, par abus de langage, qu'une propriété de Markov est une propriété de monoïdes à présentations finies qui est invariante par isomorphismes, qui est vraie d'au moins un monoïde à présentation finie, et telle qu'il existe un monoïde à présentation finie qui ne se plonge dans aucun monoïde à présentation finie qui vérifie P .

Étant données deux présentations (Σ, E) et (Σ', E') , on définit leur *produit libre* $(\Sigma, E) * (\Sigma', E')$ comme suit. Informellement, et sous l'hypothèse simplificatrice que Σ et Σ' sont disjoints, le produit libre est $(\Sigma \cup \Sigma', E \cup E')$. Comme on ne peut pas supposer que Σ et Σ' sont disjoints en général, on forme des unions disjointes. En détail :

- pour tout $a \in \Sigma$, on note $\bar{a}$ le couple $(0, a)$; on étend la notation aux mots $w \in \Sigma^*$ (si $w = a_1 \cdots a_n$, alors $\bar{w} \stackrel{\text{def}}{=} \bar{a}_1 \cdots \bar{a}_n$), aux relations (u, v) ($\overline{(u, v)} \stackrel{\text{def}}{=} (\bar{u}, \bar{v})$), aux ensembles de relations ($\bar{E} \stackrel{\text{def}}{=} \{\overline{(u, v)} \mid (u, v) \in E\}$), et aux alphabets ($\bar{\Sigma} \stackrel{\text{def}}{=} \{\bar{a} \mid a \in \Sigma\}$) ;
- pour tout $a' \in \Sigma'$, on note $\overline{\overline{a'}}$ le couple $(1, a')$; on étend la notation aux mots $w' \in \Sigma'^*$ (si $w' = a'_1 \cdots a'_n$, alors $\overline{\overline{w'}} \stackrel{\text{def}}{=} \overline{\overline{a'_1}} \cdots \overline{\overline{a'_n}}$), aux relations (u', v') ($\overline{\overline{(u', v')}} \stackrel{\text{def}}{=} (\overline{\overline{u'}}, \overline{\overline{v'}})$), aux ensembles de relations ($\overline{\overline{E'}} \stackrel{\text{def}}{=} \{\overline{\overline{(u', v')}} \mid (u', v') \in E'\}$), et aux alphabets ($\overline{\overline{\Sigma'}} \stackrel{\text{def}}{=} \{\overline{\overline{a'}} \mid a' \in \Sigma'\}$) ;
- le produit libre $(\Sigma, E) * (\Sigma', E')$ est $(\bar{\Sigma} \cup \overline{\overline{\Sigma'}}, \bar{E} \cup \overline{\overline{E'}})$.

Le fait que $\bar{a}$ soit codé comme $(0, a)$ et $\overline{\overline{a'}}$ comme $(1, a')$ n'a aucune importance. Le seul intérêt est que $\bar{\Sigma}$ et $\overline{\overline{\Sigma'}}$ sont toujours disjoints, quels que soient Σ et Σ' . On ne

fera donc plus mention à l'avenir de la façon particulière dont $\bar{a}$ et $\overline{\bar{a}}$ sont codés (y compris dans les réponses aux questions.)

On admettra le résultat suivant.

Lemme 2 *Étant données deux présentations (Σ, E) et (Σ', E') , et leur produit libre $(\Sigma'', E'') \stackrel{\text{def}}{=} (\Sigma, E) * (\Sigma', E')$, et en écrivant M, M', M'' pour les monoïdes ainsi présentés, il existe deux plongements de monoïdes $\iota: M \rightarrow M''$ et $\iota': M' \rightarrow M''$.*

Démonstration. (Sketch.) Soit e (« effacement ») la fonction qui à tout mot de Σ''^* associe le même mot, dans lequel on n'a gardé que les lettres de $\overline{\Sigma}$, dans le même ordre ; on a donc effacé les lettres de $\overline{\Sigma'}$. Pour tous mots $w_1'', w_2'' \in \Sigma''^*$, si $w_1'' \leftrightarrow_{\overline{E'}} w_2''$ alors $e(w_1'') = e(w_2'')$, et si $w_1'' \leftrightarrow_{\overline{E}} w_2''$ alors $e(w_1'') \leftrightarrow_{\overline{E}} e(w_2'')$. Par récurrence sur le nombre d'étapes $\leftrightarrow_{E''}$, et en distinguant selon que ces étapes sont de type $\leftrightarrow_{\overline{E}}$ ou $\leftrightarrow_{\overline{E'}}$, on en déduit que si $w_1'' \leftrightarrow_{E''}^* w_2''$, alors $e(w_1'') \leftrightarrow_{\overline{E}} e(w_2'')$.

En particulier, si w_1'' est de la forme $\overline{w_1}$ avec $w_1 \in \Sigma^*$ et si w_2'' est de la forme $\overline{w_2}$ avec $w_2 \in \Sigma^*$, auquel cas $e(w_1'') = \overline{w_1}$ et $e(w_2'') = \overline{w_2}$, on a que $\overline{w_1} \leftrightarrow_{E''}^* \overline{w_2}$ implique $\overline{w_1} \leftrightarrow_{\overline{E}} \overline{w_2}$. L'implication réciproque est évidente puisque $\overline{E} \subseteq E''$. Or $w_1 \leftrightarrow_E^* w_2$ si et seulement si $\overline{w_1} \leftrightarrow_{\overline{E}}^* \overline{w_2}$, par une récurrence immédiate sur le nombre d'étapes $\leftrightarrow_E^*$ dans un sens, sur le nombre d'étapes $\leftrightarrow_{\overline{E}}^*$ dans l'autre sens.

Nous venons donc de démontrer que : (1) pour tous mots $w_1, w_2 \in \Sigma^*$, $w_1 \leftrightarrow_E^* w_2$ si et seulement si $\overline{w_1} \leftrightarrow_{E''}^* \overline{w_2}$. Par symétrie, on démontre de même que : (2) pour tous mots $w_1', w_2' \in \Sigma'^*$, $w_1' \leftrightarrow_{E'}^* w_2'$ si et seulement si $\overline{\overline{w_1'}} \leftrightarrow_{E''}^* \overline{\overline{w_2'}}$.

Nous posons $\iota([w]_E) \stackrel{\text{def}}{=} [\overline{w}]_{E''}$ pour tout $w \in \Sigma$. Ceci est bien défini par (1), qui démontre aussi que ι est injective. Par construction, ι est un homomorphisme de monoïdes, c'est donc un plongement.

On définit de même ι' par $\iota'([w']_{E'}) \stackrel{\text{def}}{=} [\overline{\overline{w'}}]_{E''}$ pour tout $w' \in \Sigma'$, et il s'agit aussi d'un plongement. $\square$

Soit P une propriété de Markov, que l'on fixera à partir de maintenant et jusqu'à la **Question 11**. On fixera de même, et pour la même durée, des présentations finies (Σ_1, E_1) et (Σ_2, E_2) telles que données à la définition 1, et l'on pose :

$$(\Sigma'', E'') \stackrel{\text{def}}{=} (\Sigma_U, E_U) * (\Sigma_2, E_2),$$

où (Σ_U, E_U) est donné à la **Question 6**. Finalement, on fixe deux mots $u, v \in \Sigma''^*$.

On définit la présentation $(\Sigma_{u,v}, E_{u,v})$ par :

- $\Sigma_{u,v} \stackrel{\text{def}}{=} \Sigma'' \cup \{\#, \$\}$, où $\#$ et $\$$ sont deux lettres distinctes et hors de Σ'' ;
- $E_{u,v} \stackrel{\text{def}}{=} E'' \cup \{(a\#v\$, \#v\$) \mid a \in \Sigma_{u,v}\} \cup \{(\#u\$, \epsilon)\}$.

On pose de plus :

$$(\Sigma'_{u,v}, E'_{u,v}) \stackrel{\text{def}}{=} (\Sigma_1, E_1) * (\Sigma_{u,v}, E_{u,v}).$$

On notera aussi $M_1 \stackrel{\text{def}}{=} \Sigma_1^* / \sim_{E_1}$ le monoïde présenté par (Σ_1, E_1) , M_2 le monoïde présenté par (Σ_2, E_2) , M'' le monoïde présenté par (Σ'', E'') , $M_{u,v}$ le monoïde présenté par $(\Sigma_{u,v}, E_{u,v})$ et $M'_{u,v}$ le monoïde présenté par $(\Sigma'_{u,v}, E'_{u,v})$.

Dans la suite, on pourra utiliser (en y faisant référence explicitement) les faits suivants :

- (1) pour tous mots $u_1, v_1 \in \Sigma_1^*$, $u_1 \sim_{E_1} v_1$ si et seulement si $\overline{u_1} \sim_{E'_{u,v}} \overline{v_1}$;
- (2) pour tous mots $u_2, v_2 \in \Sigma_{u,v}^*$, $u_2 \sim_{E_{u,v}} v_2$ si et seulement si $\overline{u_2} \sim_{E'_{u,v}} \overline{v_2}$.

Ce sont les propriétés (1) et (2) démontrées au cours de la preuve du lemme 2, adaptées au cas présent. On pourra aussi, si on le souhaite, utiliser les notations ι et ι' pour les plongements de M_1 dans $M'_{u,v}$ et de $M_{u,v}$ dans $M'_{u,v}$ respectivement, ou de M_U et de M_2 dans M'' respectivement.

Question 7 ■■■■ Montrer que si $u \sim_{E''} v$ alors pour tout $a \in \Sigma_{u,v}$, $\overline{a} \sim_{E'_{u,v}} \epsilon$.

Par hypothèse, on a $u \sim_{E''} v$, donc $u \sim_{E_{u,v}} v$ puisque $E'' \subseteq E_{u,v}$. Pour tout $a \in \Sigma_{u,v}$,

$$\begin{array}{ll} a \leftrightarrow_{E_{u,v}} a \# u \$ & \text{par la règle } (\# u \$, \epsilon) \\ \leftrightarrow_{E_{u,v}} a \# v \$ & \text{car } u \sim_{E_{u,v}} v \\ \leftrightarrow_{E_{u,v}} \# v \$ & \text{par la règle } (a \# v \$, \# v \$) \\ \leftrightarrow_{E_{u,v}} \# u \$ & \text{car } u \sim_{E_{u,v}} v \\ \leftrightarrow_{E_{u,v}} \epsilon & \text{par la règle } (\# u \$, \epsilon). \end{array}$$

On a donc $a \leftrightarrow_{E_{u,v}} \epsilon$, d'où le résultat en utilisant (2).

Question 8 ■■■■ En déduire que si $u \sim_{E''} v$ alors $(\Sigma'_{u,v}, E'_{u,v})$ satisfait la propriété P.

*Par la **Question 7**, on a $\overline{a} \sim_{E'_{u,v}} \epsilon$ pour tout $a \in \Sigma_{u,v}$, donc : $(*) \overline{w} \sim_{E'_{u,v}} \epsilon$ pour tout mot $w \in \Sigma_{u,v}^*$ (récurrence immédiate sur la longueur de w).*

On en déduit que M_1 et $M'_{u,v}$ sont isomorphes. L'isomorphisme est simplement ι . On sait déjà que c'est un plongement par le lemme 2, il ne reste qu'à démontrer qu'il est surjectif. Pour tout mot $w \in \Sigma_{u,v}^*$, on écrit w comme une concaténation $\overline{u_1} \overline{v_1} \cdots \overline{u_n} \overline{v_n}$ où les u_i sont des mots de Σ_1^* et les v_i sont des mots de $\Sigma_{u,v}^*$ (possiblement vides). Par $(*)$, $w \sim_{E'_{u,v}} \overline{u_1 \cdots u_n}$. Mais ceci signifie que $[w]_{E'_{u,v}} = \iota([u_1 \cdots u_n]_{E_1})$. Donc ι est surjective.

Comme P est **extensionnelle** (condition (A) de la définition 1) et que (Σ_1, E_1) satisfait P (condition (B)), P doit aussi être vraie de $(\Sigma'_{u,v}, E'_{u,v})$.

Dans la suite, on pourra utiliser le lemme suivant, en le référençant explicitement.

Lemme 3 Si $u \not\sim_{E''} v$, alors pour tous mots $w, w' \in \Sigma''^*$, si $w \sim_{E_{u,v}} w'$ alors $w \sim_{E''} w'$.

Démonstration. (Sketch — de nombreux détails omis.) Pour tout mot $w \in \Sigma''^*$, soit S_w le plus petit ensemble des mots de $\Sigma_{u,v}^*$ contenant $[w]_{E''}$ et stable par insertion de mots de la forme $\#u'\$$ avec $u' \in [u]_{E''}$. Cette dernière propriété signifie que si $u \sim_{E''} u'$ alors pour tous mots $w_1 w_2 \in S_w$, $w_1 \#u' \$ w_2$ est aussi dans S_w . On vérifie que : (*) pour tout $w \in S_w$, w ne peut pas s'écrire $w_1 \#v \$ w_2$ pour aucun couple de mots w_1, w_2 . Ceci est dû au fait que $u \not\sim_{E''} v$.

Par une analyse de cas assez fastidieuse, on vérifie que pour tout mot $w' \in S_w$, pour tout mot $w'' \in \Sigma_{u,v}^*$ tel que $w' \leftrightarrow_{E_{u,v}} w''$, w'' est encore dans S_w . Le point important est qu'on ne peut pas avoir $w' \leftrightarrow_{E_{u,v}} w''$ via l'usage d'une relation $(a \#v \$, \#v \$)$, dans un sens ou dans l'autre, par (*).

Donc S_w est un *invariant* pour $\leftrightarrow_{E_{u,v}}$: en partant de w et en appliquant autant de réécritures via $\leftrightarrow_{E_{u,v}}$ que l'on veut, on obtient toujours des mots qui sont dans S_w . Plus formellement, pour tout mot $w' \in [w]_{E_{u,v}}$, w' est dans S_w . En particulier, pour tout mot $w' \in \Sigma''^*$ tel que $w \sim_{E_{u,v}} w'$, alors $w' \in S_w$. Mais comme w' est dans Σ''^* et ne contient donc ni $\#$ ni $\$$, c'est qu'il a été obtenu sans utiliser l'opération d'insertion d'un mot de la forme $\#u' \$$ avec $u' \in [u]_{E''}$. Par définition de S_w , on a donc $w' \in [w]_{E''}$, ce qui est ce que l'on voulait démontrer. $\square$

Question 9 ■■■■ Montrer que si $u \not\sim_{E''} v$, alors M'' se plonge dans $M_{u,v}$, via un plongement que nous nommerons π , et que vous explicitez.

Posons $\pi([w]_{E''}) \stackrel{\text{def}}{=} [w]_{E_{u,v}}$ pour tout mot $w \in \Sigma''^*$. Ceci est bien défini car si $w \sim_{E''} w'$ alors $w \sim_{E_{u,v}} w'$, puisque $E'' \subseteq E_{u,v}$.

Il est clair que π est un homomorphisme de monoïdes.

Supposons que $w \sim_{E_{u,v}} w'$, avec $w, w' \in \Sigma''^*$. Par le lemme 3, $w \sim_{E''} w'$. Autrement dit, si $\pi([w]_{E''}) = \pi([w']_{E''})$, alors $[w]_{E''} = [w']_{E''}$, donc π est injective.

Question 10 ■■■■ En déduire que si $u \not\sim_{E'_{u,v}} v$, alors $\neg P(\Sigma'_{u,v}, E'_{u,v})$.

Si on avait $u \sim_{E''} v$, on aurait $u \sim_{E'_{u,v}} v$ parce que $E'' \subseteq E'_{u,v}$. Donc $u \not\sim_{E''} v$.

Nous démontrons donc que sous l'hypothèse $u \not\sim_{E''} v$, alors $\neg P(\Sigma'_{u,v}, E'_{u,v})$. C'est ce qui sera utile à la question suivante. Comme $u \sim_{E''} v$, on peut appliquer la **Question 9**, et donc obtenir un plongement π de M'' dans $M_{u,v}$.

Par le lemme 2, on a un plongement ι' de M_2 dans M'' , que l'on compose avec le plongement π , puis avec le plongement ι' de $M_{u,v}$ dans $M'_{u,v}$. Ainsi, M_2 se plonge dans $M'_{u,v}$.

Par la condition (C) de la définition 1, $\neg P(\Sigma'_{u,v}, E'_{u,v})$.

Question 11 ■■■■ Conclure que toute propriété de Markov P de présentations finies de monoïdes est indécidable. On explicitera la réduction (comme d'habitude).

On forme la réduction suivante depuis le problème indécidable de la **Question 6** vers P . Partant de $\text{init} \in \Sigma_U^*$, on forme $(\Sigma'_{u,v}, E'_{u,v})$ avec $u \stackrel{\text{def}}{=} \overline{\text{init}}$, $v \stackrel{\text{def}}{=} \overline{\text{end}_U}$. Par le lemme 2 (ou plutôt la propriété (1) de sa preuve, avec $(\Sigma, E) \stackrel{\text{def}}{=} (\Sigma_U, E_U)$ et $(\Sigma', E') \stackrel{\text{def}}{=} (\Sigma_2, E_2)$), $\text{init} \sim_{E_U} \text{end}_U$ si et seulement si $u \sim_{E''} v$. Si $u \sim_{E''} v$, alors la **Question 8** nous dit que $P(\Sigma'_{u,v}, E'_{u,v})$. Sinon, la **Question 10** (ou plutôt sa démonstration, qui n'a besoin que de l'hypothèse $u \not\sim_{E''} v$) nous dit que $\neg P(\Sigma'_{u,v}, E'_{u,v})$.

On note que le produit libre de deux présentations finies est fini, et que l'on a rajouté un nombre fini de lettres pour passer de Σ'' à $\Sigma_{u,v}$ et un nombre fini de relations pour passer de E'' à $E_{u,v}$. On observe que la construction de $\Sigma_{u,v}$ (que l'on peut se donner à l'avance, vu qu'il ne dépend en fait pas de u ni de v), et surtout de $E_{u,v}$, est calculable en fonction de u et de v . On observe aussi que la construction du produit libre final $(\Sigma'_{u,v}, E'_{u,v})$ est elle aussi calculable en fonction de (Σ_1, E_1) (une constante) et $(\Sigma_{u,v}, E_{u,v})$.

Donc P est indécidable.

Question 12 ■■■■ Parmi les problèmes suivants, prenant en entrée une présentation finie (Σ, E) d'un monoïde M , lesquels sont décidables et lesquels sont indécidables ? Justifier.

- (a) **Question** : M est-il fini ?
- (b) **Question** : M est-il un groupe, autrement dit tout élément $m \in M$ a-t-il un inverse à gauche et à droite ?
- (c) **Question** : peut-on séparer Σ comme l'union disjointe de deux ensembles Σ^+ et Σ^- , avec une bijection ${}^{-1}: \Sigma^+ \rightarrow \Sigma^-$, de sorte que E contienne toutes les relations (aa^{-1}, ϵ) et $(a^{-1}a, \epsilon)$, $a \in \Sigma^+$?
- (d) **Question** : existe-t-il une présentation finie (Σ', E') de M sur un alphabet Σ' à deux lettres ?

- (e) **Question :** existe-t-il une présentation finie (Σ', E') de M telle que l'on peut séparer Σ' comme l'union disjointe de deux ensembles Σ'^+ et Σ'^- , avec une bijection ${}_{-}^{-1} : \Sigma'^+ \rightarrow \Sigma'^-$, de sorte que E' contienne toutes les relations (aa^{-1}, ϵ) et $(a^{-1}a, \epsilon)$, $a \in \Sigma'^+$?
- (f) **Question :** la présentation (Σ, E) est-elle *redondante*, au sens où il existe des relations $(u_1, v_1), \dots, (u_n, v_n) \in E$ (pas nécessairement distinctes), avec $n \geq 1$, telles que $u_1 \cdots u_n$ et $v_1 \cdots v_n$ sont des mots identiques ?
- (g) **Question :** M est-il apériodique ? (Un monoïde est *apériodique* si et seulement si pour tout $m \in M$, il existe un entier $n \in \mathbb{N}$ tel que $m^n = m^{n+1}$.)

Ce sont toutes des propriétés extensionnelles, à part la **Question 12c** et la **Question 12f**.

Question 12a Indécidable par la **Question 11**. On prend $\Sigma_1 \stackrel{\text{def}}{=} \{a\}$ et $E_1 \stackrel{\text{def}}{=} \{(a, \epsilon)\}$, qui présente le monoïde contenant juste un élément : il est donc fini, et vérifie la propriété. On prend $\Sigma_2 \stackrel{\text{def}}{=} \{a\}$, $E_2 \stackrel{\text{def}}{=} \emptyset$. Le monoïde présenté est Σ_2^* (à isomorphisme près, $\mathbb{N}$ muni de l'addition et de 0 comme élément neutre), qui est infini, et tout monoïde dans lequel il se plongera sera donc nécessairement infini.

Question 12b Indécidable par la **Question 11**. On prend Σ_1 et E_1 comme en **Question 12a** : le monoïde présenté est le groupe trivial. On prend $\Sigma_2 \stackrel{\text{def}}{=} \{a\}$ et $E_2 \stackrel{\text{def}}{=} \{(aa, a)\}$ (pas comme en **Question 12a** : le monoïde $\{a\}^*$ est isomorphe à $\mathbb{N}$, qui n'est pas un groupe mais se plonge dans le groupe $\mathbb{Z}$, présenté par $(\{a, \bar{a}\}, \{(a\bar{a}, \epsilon), (\bar{a}a, \epsilon)\})$). Le monoïde ainsi présenté est $\{0, 1\}$ avec 1 la classe d'équivalence de ϵ et 0 la classe d'équivalence de tous les autres mots : la loi est le produit. Quel que soit le monoïde G dans lequel se plonge ce monoïde, l'élément 0 y sera un idempotent différent de 1, ce qui n'est pas possible si G est un groupe. Explicitement, si 0 a un inverse x , on a $1 = 0x$ dans G ; donc $0 = 01 = 00x = 0x = 1$, contradiction.

Question 12c Décidable (même si cette propriété implique d'être un groupe). Il suffit d'énumérer les ensembles Σ^+ et Σ^- et les bijections ${}_{-}^{-1}$ possibles, et de tester l'appartenance des relations indiquées à E .

Question 12d Erratum. Désolé, j'ai fait une erreur. Je pensais à une solution, qui se trouve être à un problème différent de celui que j'ai finalement énoncé en **Question 12d**. Voir l'annexe A, où je présente d'abord le problème que j'avais résolu, avec sa solution ; ceci montre notamment que **Question 12d** n'est pas une propriété de Markov : elle vérifie (A) et

(B) mais pas (C). Je présente ensuite des solutions que j'ai vu dans les copies, après les avoir un peu nettoyées.

Question 12e. Indécidable. La question est équivalente à la **Question 12b**. En effet, s'il existe une telle présentation finie, alors M est un groupe. Réciproquement, si M est un groupe, on peut construire Σ' comme l'union disjointe $\overline{\Sigma} \cup \overline{\overline{\Sigma}}$ et E' comme $\overline{E} \cup \{(\overline{a\overline{a}}, \epsilon) \mid a \in \Sigma\} \cup \{(\overline{\overline{a\overline{a}}}, \epsilon) \mid a \in \Sigma\}$.

Question 12f. Indécidable, mais pas par la **Question 11**, la propriété n'étant pas (clairement, en tout cas) extensionnelle. Mais il s'agit d'une simple reformulation du problème de correspondance de Post.

Question 12g. Indécidable par la **Question 11**. On prend Σ_1 et E_1 comme en **Question 12a** : l'unique élément est l'unité 1, qui vérifie $1^n = 1^{n+1}$ pour tout $n \in \mathbb{N}$. On prend Σ_2 et E_2 comme en **Question 12a**. Dans tout monoïde dans lequel se plonge Σ_2^* , l'élément a est tel que $a^n \neq a^{n+1}$ pour tout $n \in \mathbb{N}$;

A Solutions de la Question 12d

A.1 Ma solution erronée

La solution que j'avais en tête était à la question suivante : M se plonge-t-il dans un monoïde ayant une présentation finie à deux lettres ? Cette question est décidable, car : (*) tout monoïde ayant une présentation finie se plonge dans un monoïde ayant une présentation finie à deux lettres.

Esquisse de preuve de (*). Étant donnée une présentation finie (Σ, E) , on énumère les lettres de Σ : $a_1, \dots, a_n$. On code ensuite chaque lettre sur $\{0, 1\}$, par exemple en codant a_i par $f(a_i) \stackrel{\text{def}}{=} 110^i 10^{n-i}$ pour tout $i \in \{1, \dots, n\}$. La longueur de $f(a_i)$ est $n + 3$, indépendante de i . Le « 11 » en début de $f(a_i)$ sert à reconnaître le début du code de a_i . On étend f à Σ^* de l'unique façon qui en fait un homomorphisme de monoïdes. Chaque règle (u, v) est compilée en $(f(u), f(v))$. Notons $f(E)$ l'ensemble des règles ainsi obtenues. Il est clair que si $w \leftrightarrow_E w'$, alors $f(w) \leftrightarrow_{f(E)} f(w')$. Ceci implique que la fonction $\hat{f}$ qui à $[w]_E$ associe $[f(w)]_{f(E)}$ est bien définie ; c'est un homomorphisme, comme on le vérifie aisément. De plus, $f(w)$ est dans le langage F^* , où $F = \{f(a_1), \dots, f(a_n)\}$. Réciproquement, pour tous $s, t \in F^*$, on peut écrire s et t comme $f(w)$ et $f(w')$ pour des mots $w, w' \in \Sigma^*$ uniques (découper s et t en blocs en $n + 3$ bits), et si $s \leftrightarrow_{f(E)} t$, alors c'est par une règle $(f(u), f(v))$ qui s'applique à une position multiple de $n + 3$, à cause du 11 en début de code de chaque lettre ; et donc $w \leftrightarrow_E w'$, via la règle $(u, v) \in E$. Ceci montre que $\hat{f}$ est injective, et définit donc

un plongement de monoïdes.

Notons que (*) montre que **Question 12d** ne vérifie pas la propriété (C) d'une propriété de Markov. Elle vérifie cependant (A) et (B).

A.2 Solution

Cette solution a été trouvée par Eva Coquerel et par Elliott Ranvier. Bravo à eux deux !

Dans un premier temps, on considère la propriété P_1 vérifiée par un monoïde M si et seulement si M a un générateur g . Un *générateur* g est un élément de M tel que tout élément de M s'écrit comme un produit g^n de g avec lui-même n fois pour au moins un $n \in \mathbb{N}$. (Souvent, en mathématiques, on demande qu'un générateur soit différent de 1, mais ceci ne servirait qu'à compliquer la démonstration. Si 1 est un générateur, M est le monoïde trivial $\{1\}$.) La propriété P_1 est de Markov. Elle est extensionnelle par définition, la présentation finie $(\{a\}, \emptyset)$ définit un monoïde avec un générateur (a) , et la présentation finie $(\{a, b\}, \emptyset)$ définit un monoïde $(\{a, b\}^*)$ tel que tout monoïde M dans lequel il se plonge est non-commutatif (car $ab \neq ba$ dans $\{a, b\}^*$, et donc dans M) ; or tout monoïde avec un générateur est commutatif. Comme P_1 est une propriété de Markov, elle est indécidable.

Dans un deuxième temps, on montre que P_1 se réduit à la **Question 12d**. La réduction prend en entrée une présentation finie (Σ, E) , et construit $(\Sigma \cup \{b\}, E)$, où b est une lettre hors de Σ . On montre que le monoïde $M \stackrel{\text{def}}{=} \Sigma / \sim_E$ vérifie P_1 si et seulement si $M^+ \stackrel{\text{def}}{=} (\Sigma \cup \{a\}) / \sim_E$ a une présentation finie à deux lettres, où a est une lettre fraîche, c'est-à-dire hors de Σ .

On démontre que : (**) M^+ est (à isomorphisme près) le monoïde des mots $m_0 a m_1 a \cdots a m_k$ où chaque m_i est dans M , et $k \in \mathbb{N}$ (si $k = 0$, il n'y a pas de a), avec l'élément neutre 1 de M comme élément neutre et le produit défini par

$$(m_0 a m_1 a \cdots a m_k)(m'_0 a m'_1 a \cdots a m'_{k'}) \stackrel{\text{def}}{=} m_0 a m_1 a \cdots a (m_k m'_0) a m'_1 a \cdots a m'_{k'}.$$

Je ne ferai qu'une esquisse de preuve. Les éléments de M^+ sont les classes d'équivalence de mots $w_0 a w_1 a \cdots a w_k$ modulo $\sim_E$, où chaque w_i est dans Σ^* . Les réécritures par $\leftrightarrow_E$ ne peuvent être effectuées qu'à l'intérieur de chaque w_i , et l'on en déduit que M^+ est isomorphe au monoïde des mots $m_0 a m_1 a \cdots a m_k$ où chaque m_i est dans M . En particulier, chaque élément de M^+ s'écrit de façon unique sous cette forme.

— Supposons que M vérifie P_1 , et soit g un générateur de M . On prétend que M est alors soit $\mathbb{N}$ (à isomorphisme près—présenté par $(\{g\}, \emptyset)$, l'isomorphisme envoyant n sur g^n) soit un monoïde fini. En effet, si M satisfait ne

serait-ce qu'une relation non-triviale, c'est-à-dire de la forme $g^m = g^n$ avec $m \neq n$ (disons $m < n$ sans perte de généralité, et posons $k \stackrel{\text{def}}{=} n - m$), alors on a $g^{m+qk} = g^{n+(q-1)k} = g^{m+(q-1)k}$ pour tout $q \geq 1$, donc $g^{m+qk} = g^m$ par récurrence sur q ; il s'ensuit que pour tout $j \geq m$, en écrivant $j = m + qk + r$ avec $0 \leq r < k$ (division euclidienne), $g^j = g^{m+r}$. Les seuls éléments distincts de M sont parmi $g^0, g^1, \dots, g^{m+k-1}$ et $g^{m+k} = g^m$: M est un *lasso* de base m et de période k . Un tel lasso a comme présentation finie $(\{g\}, \{(g^{m+k}, g^m)\})$.

Si $M = \mathbb{N}$ (à isomorphisme $k \mapsto g^n$ près), alors M^+ est le monoïde des mots $g^{n_0} a g^{n_1} a \dots a g^{n_k}$, avec les lois décrites plus haut ; c'est donc le monoïde présenté par $(\{g, a\}, \emptyset)$, et il a donc une présentation finie à deux lettres.

Si M est un lasso de base m et de période k , alors M^+ est présenté par $(\{g, a\}, \{(g^{m+k}, g^m)\})$.

- Réciproquement, supposons que M^+ a une présentation finie à deux lettres, disons $(\{b, c\}, E')$. Nous évacuons d'abord le cas où M est le monoïde trivial $\{1\}$: dans ce cas, M vérifie P_1 , car 1 est un générateur (avec la définition que j'ai prise). Supposons donc M non trivial.

Comme $[b]_{E'} \in M^+$, on a $[b]_{E'} = [w_b]_E$ pour un mot w_b de $(\Sigma \cup \{a\})^*$, et de façon similaire, $[c]_{E'} = [w_c]_E$ pour un mot w_c de $(\Sigma \cup \{a\})^*$.

Nous allons utiliser plusieurs fois la propriété $(**)$ démontrée plus haut, définissant complètement M^+ .

Au moins un des deux mots w_b, w_c contient un a . Sinon w_b et w_c seraient dans Σ^* , et tout élément de M^+ , qui est produit de copies de $[b]_{E'}$ et de $[c]_{E'}$, donc de copies de $[w_b]_E$ et de $[w_c]_E$, serait de la forme $[w]_E$ avec $w \in \Sigma^*$, donc dans M . C'est impossible car parmi les éléments de M^+ , on trouve a (vu comme un mot—grâce à $(**)$), qui n'est pas dans M .

Il n'est pas possible que w_b et w_c contiennent tous les deux un a . Sinon l'écriture unique de $[w_b]_{E'}$ sous la forme $m_0 a m_1 a \dots a m_k$ (grâce à $(**)$) contiendrait au moins un a (autrement dit, $k \geq 1$) et pareil pour $[w_c]_{E'}$. Ceci impliquerait que tout élément de M^+ , qui s'écrit comme un produit de copies de $[w_b]_{E'}$ et de $[w_c]_{E'}$, serait soit l'élément unité 1 soit contiendrait au moins un a . Pour tout $m \in M$, le mot m vu comme élément de M^+ est sa propre décomposition sous la forme unique donnée par $(**)$, et ceci impliquerait que $m = 1$, donc que M serait trivial.

Supposons, à symétrie près entre b et c , que w_b contienne au moins un a , et w_c n'en contienne pas. Pour tout $m' \in M'$, si m' s'écrit comme un produit de copies de $[w_b]_{E'}$ et de $[w_c]_{E'}$ avec au moins une occurrence de $[w_b]_{E'}$, alors la décomposition unique $m_0 a m_1 a \dots a m_k$ donnée en $(**)$ contient au

moins un a (i.e., $k \geq 1$); donc $m' \notin M$. Par contraposée, tout $m \in M$ s'écrit comme un produit de copies de $[w_b]_{E'}$. Autrement dit, $[w_b]_{E'}$ est un générateur de M . Donc M vérifie P_1 .