Calculabilité
Cours 4 : réductions

Kévin Perrot – Aix Marseille Université – printemps 2022

Table des matières

4.3 Réductions (many-one) 1
4.4 Théorème de Rice 3
4.5 Réductions (oracle) 4

4.3 Réductions (many-one)

Une des formulations les plus populaires du résultat de Turing en 1936 est donnée par le théorème de l'arrêt. Voyons maintenant une façon plus épurée de formuler ces idées, qui nous permettront d'aller plus loin de façon élégante.

Théorème 1. *Le langage* $L_d = \{\langle M\rangle \mid M \text{ n'accepte pas le mot } \langle M\rangle\}$ *n'est pas semi-décidable.*

Démonstration. Par l'absurde, supposons qu'une machine M_d reconnaisse L_d. Considérons alors l'entrée $\langle M_d\rangle$ donnée à la machine M_d. Deux cas sont possibles.

— Si M_d n'accepte pas $\langle M_d\rangle$ alors, par définition du langage L_d, le mot $\langle M_d\rangle$ est dans L_d. Or M_d reconnait L_d, donc M_d accepte $\langle M_d\rangle$, une contradiction.

— Si M_d accepte $\langle M_d\rangle$ alors, par définition du langage L_d, le mot $\langle M_d\rangle$ n'est pas dans L_d. Or M_d reconnait L_d, donc M_d n'accepte pas $\langle M_d\rangle$, une contradiction.

Dans les deux cas nous arrivons à une contradiction. □

La preuve est cette fois encore plus simple ! Ce résultat nous dit qu'il n'existe pas de MT M_d (un seul et même algorithme qui répond oui/non correctement pour chaque instance) pour décider si une machine M reconnait le mot $\langle M\rangle$ (même si la machine M_d a le droit de ne pas s'arrêter si M ne reconnait pas $\langle M\rangle$). Ce problème peut sembler artificiel, mais il sert de *graine* pour dériver la non récursivité d'autres problèmes (plus naturels), via une méthode qui s'appelle une **réduction**.

Intuitivement, un problème A se réduit à un problème B si connaissant un algorithme pour décider/calculer B, on peut obtenir un algorithme pour décider/calculer A.

Définition 2. *Une* **réduction many-one** [1]**Turing** *du langage A au langage B est une fonction calculable $f : \Sigma_A^* \to \Sigma_B^*$ telle que $w \in A \iff f(w) \in B$. On note $A \leq_m^T B$.*

On appelle *instance* de L un mot $w \in \Sigma_L^*$ dont on se demande s'il appartient au langage L. Une réduction montre que si le langage B est décidable alors il en est de même du langage A. On utilise ensuite l'idée suivante : pour montrer qu'un langage B est indécidable, on choisit un langage A bien connu pour être indécidable, et l'on réduit A

à B. On aura alors

$$B \text{ décidable} \implies A \text{ décidable} \qquad \text{et} \qquad A \text{ indécidable}$$

et l'on peut en déduire (règle de *résolution* en logique !) que par conséquent B est indécidable. On notera que le raisonnement est tout aussi valide en remplaçant *décidable* par *semi-décidable*.

Corollaire 3. *Le langage $L_u = \{\langle M\rangle \# w \mid M \text{ accepte le mot } w\}$ n'est pas décidable. Plus précisément, son complément $L_{\bar{u}}$ n'est pas semi-décidable.*

Démonstration. Nous allons réduire L_d à $L_{\bar{u}}$ en décrivant une procédure algorithmique pour transformer les instances de L_d en des instances de $L_{\bar{u}}$. Soit w' une instance de L_d.

1. la machine vérifie $w' \in L_{enc}$, si w' n'est pas un encodage valide alors on retourne l'instance $\langle M_{palindrome}\rangle \# abba$ (on a bien $w' \notin L_d$ et $\langle M_{palindrome}\rangle \# abba \notin L_{\bar{u}}$) ;
2. si $w' = \langle M\rangle$ est un encodage valide, alors on retourne l'instance $w' \# w' = \langle M\rangle \# \langle M\rangle$ (on a bien $w' \in L_d$ si et seulement si $\langle M\rangle \# \langle M\rangle \in L_{\bar{u}}$).

Cette réduction montre que si $L_{\bar{u}}$ est semi-décidable alors L_d l'est également, or le théorème 1 nous dit que L_d n'est pas semi-décidable, donc $L_{\bar{u}}$ non plus, et par conséquent L_u n'est pas décidable (propriété de clôture). □

Corollaire 4. *Le langage $L_{halt\epsilon} = \{\langle M\rangle \mid M \text{ s'arrête quand on la lance sur l'entrée vide}\}$ n'est pas décidable.*

Démonstration. Nous allons réduire L_u à $L_{halt\epsilon}$. Etant donnée $\langle M\rangle \# w$ une instance de L_u, nous construisons l'instance $\langle M'\rangle$ suivante pour $L_{halt\epsilon}$:

1. on vérifie $\langle M\rangle \in L_{enc}$, si $\langle M\rangle$ n'est pas un encodage valide alors on retourne l'instance $\langle M'\rangle = \langle M\rangle$;
2. sinon on construit $\langle M'\rangle$ avec M' la machine qui commence par écrire w sur le ruban (cela est possible en utilisant $|w|$ états), puis entre dans l'état initial de M (M' va alors se comporter comme M), et nous rajoutons également à M' des transitions, depuis tous les états non finaux où M s'arrête (transition indéfinie), vers un état qui boucle à l'infini [2].

Dans tous les cas, nous avons bien $\langle M\rangle \# w \in L_u \iff \langle M'\rangle \in L_{halt\epsilon}$, donc si $L_{halt\epsilon}$ est décidable alors L_u est décidable, or le théorème 3 nous dit que L_u n'est pas décidable, donc $L_{halt\epsilon}$ n'est pas décidable. □

Voyez-vous la réduction utilisant le théorème 4 pour démontrer le théorème de l'arrêt ?

1. Navré pour l'anglicisme, *many-one* qualifie la fonction f (de plusieurs vers un, il faut comprendre par là que ni l'injectivité ni la surjectivité ne sont imposées).

2. Pour les fous de formalisme : soit $\langle M\rangle \# w$ une instance de L_u avec $M = (Q, \Sigma, \Gamma, \delta, q_0, B, q_F)$ et $w = w_0 \dots w_k$, dans le second cas nous construisons $\langle M'\rangle$ avec $M' = (Q \cup \{q'_0, \dots, q'_{k+1}\} \cup \{q'_{loop}\}, \Sigma, \Gamma, \delta', q'_0, q_F)$ avec $\delta'(q,a) = \delta(q,a)$ pour tout q et a où $\delta(q,a)$ est définie, et $\delta'(q'_i, B) = (q'_{i+1}, w_{k-i}, L)$ pour tout $0 \le i \le k$ afin d'écrire w sur le ruban initiallement vide, et $\delta'(q'_{k+1}, B) = (q_0, B, R)$ pour aller dans l'état initial de M sur le début du mot w, et $\delta'(q,a) = (q'_{loop}, B, R)$ pour tout $q \in Q$ et $a \in \Gamma$ pour lesquels $\delta(q,a)$ est indéfinie, et enfin $\delta'(q'_{loop}, a) = (q'_{loop}, B, R)$ pour tout $a \in \Gamma$.

4.4 Théorème de Rice

Nous avons vu que de nombreuses questions sur les MT sont indécidables. Certaines questions sont clairement décidables, comme par exemple : est-ce qu'une MT donnée a 5 états ? Il s'avère cependant que **toute question non triviale qui concerne uniquement le langage reconnu par une MT (plutôt que la machine elle-même) est indécidable**. Une question non triviale étant une question qui n'est ni toujours vraie, ni toujours fausse.

Définition 5. *Soit P une famille de langages. On appelle P une* **propriété non triviale** *si il existe deux machines de Turing M_1 et M_2 telles que $L(M_1) \in P$ et $L(M_2) \notin P$.*

Théorème 6 (Rice)**.** *Pour toute propriété non triviale P, il n'existe aucun algorithme pour décider si une MT M vérifie $L(M) \in P$. Autrement dit, $L_P = \{\langle M \rangle \mid L(M) \in P\}$ n'est pas décidable.*

Démonstration. Nous utilisons une réduction depuis L_u. Sans perte de généralité, nous pouvons supposer $\emptyset \notin P$ (sinon on considère le complément de P au lieu de P). Puisque P est non triviale, il existe une MT M_{P^+} telle que $L(M_{P^+}) \in P$.

Etant donnée $\langle M \rangle \# w$ une instance de L_u, nous allons constuire l'instance $\langle M' \rangle$ (pour le problème d'appartenance de $L(M')$ à P) avec M' la machine qui :

1. copie son entrée u sur un ruban séparé pour l'utiliser plus tard ;
2. écrit w sur le ruban et place la tête sur la première lettre de w ;
3. entre dans l'état initial de M. À partir de là M' simule M, en ignorant u, jusqu'à ce que (éventuellement) M entre dans son état final ;
4. si M entre dans son état final, alors le mot u est recopié sur un ruban blanc (que des symboles B) et la machine M_{P^+} est simulée sur u. On entre dans un état final si M_{P^+} accepte u.

Etant donné n'importe quels $\langle M \rangle$ et w, la machine M' (et donc son code $\langle M' \rangle$) peut effectivement être construite algorithmiquement.

La correction de la réduction ($\langle M \rangle \# w \in L_u \iff \langle M' \rangle \in L_P$) est assurée par les observations :

— si M accepte w, alors M' acceptera exactement les mots u que M_{P^+} accepte, donc dans ce cas $L(M') = L(M_{P^+}) \in P$ et $\langle M' \rangle \in L_P$;
— si M n'accepte pas w, alors M' n'accepte aucun mot u, donc dans ce cas $L(M') = \emptyset \notin P$ et $\langle M' \rangle \notin L_P$.

On en conclut que si la propriété P est décidable alors L_u est décidable, or le théorème 3 nous dit que L_u n'est pas décidable, donc la propriété P n'est pas décidable. □

Remarque 7. M_1 **simule** M_2 = *M_1 se comporte comme M_2* = *M_1 suit la table de transition de M_2.*

Par application du théorème de Rice, on peut déduire immédiatement que les problèmes suivants sont indécidables : étant donnée une MT M,

— *est-ce M accepte tous les mots ?*
— *est-ce que $L(M)$ est un langage régulier ?*
— *est-ce M accepte tous les palindromes ?*

4.5 Réductions (oracle)

Les réductions Turing que nous avons définies dans la section 4.3 ont une définition simple, mais sont en fait assez restraintes. Nous proposons maintenant une définition plus générale de la notion de réduction, qui correspond exactement à l'idée d'imaginer que nous puissions résoudre un problème B, et de s'intéresser alors à la résolution d'un problème A.

Définition 8. *Un langage A est* **Turing-réductible** *à un langage B si il existe une machine de Turing avec* **oracle** *B, qui décide le langage A. On note $A \leq^T B$.*

Une machine de Turing avec oracle B est une machine qui peut, au cours de son calcul, obtenir autant de réponses qu'elle souhaite sur des questions d'appartenance au langage B : est-ce que tel $w \in B$? est-ce que tel autre $w' \in B$? Et l'oracle pour le langage B lui donne des réponses oui/non, instantanément. La définition suivante explique comment implémenter formellement cette idée dans le modèle des machines de Turing.

Définition 9. *Une machine de Turing M avec* **oracle** *B possède un ruban supplémentaire appelé ruban d'oracle, et trois états spéciaux $q_{question}$, q_{oui} et q_{non}. À chaque fois que M entre dans l'état $q_{question}$, la machine va dans l'état q_{oui} si $w \in B$, ou dans l'état q_{non} si $w \notin B$, avec w le contenu du ruban d'oracle. Les réponses aux questions d'appartenance à B sont données instantanément, et comptent comme une seule étape de calcul.*

Grâce aux machines avec oracle, on peut définir la *calculabilité relative*. C'est l'idée d'une machine branchée à une source d'information (comme par exemple un ordinateur branché à une base donnée, ou au world wide web...) qui est décrite par le langage de l'oracle. Le modèle des machines de Turing sans oracle peut être vu comme un modèle *offline*, alors que le modèle des machines de Turing avec oracle peut être vu comme un modèle *online*.

Définition 10. *L'ensemble des langages décidables avec oracle B est $\{A \mid A \leq^T B\}$.*

Remarque 11. *Une machine de Turing avec oracle, dont l'oracle est un langage décidable, décide un langage qui est également décidable.*

Remarque 12. *Les réductions Turing many-one et Turing (avec oracle) ne sont pas strictement équivalentes :*

- *si A est Turing many-one réductible à B, alors A est Turing réductible à B ;*
- *tout langage décidable est Turing réductible à n'importe quel langage (puisque l'oracle est inutile), mais un langage décidable non vide ne peut pas être Turing many-one réduit au langage $B = \emptyset$ (puisque quels que soient f at w on aura toujours $f(w) \notin B$). Donc par exemple, le langage Σ^* est Turing réductible au langage $\emptyset$, mais pas Turing many-one réductible ;*
- *tout langage est Turing réductible à son complément, mais si A est Turing many-one réductible à B et B est semi-décidable, alors A est également semi-décidable. Par conséquent, le complément du problème de l'arrêt (qui n'est pas semi-décidable) n'est pas Turing many-one réductible à son complément (le problème de l'arrêt, qui est semi-décidable).*

Références

[1] M. Sipser. *Introduction to the theory of computation.* Course Technology, 2006.