Corrections TD 01 – Cardinalité et machines de Turing

Remarques générales : Bien souvent il n'y a pas une seule bonne réponse possible aux questions posées. Pensez à expliquer vos idées et raisonnements dans vos rendus, cela nous aide à comprendre votre démarche dans le cas où vos réponses ne sont pas tout à fait correctes.

Rappel : soient A et B deux ensembles, une fonction $f : A \to B$ est
- injective ssi $\forall\, a, a' \in A : f(a) = f(a') \implies a = a'$ (ou la contraposée),
- surjective ssi $\forall\, b \in B : \exists\, a \in A : b = f(a)$,
- bijective ssi elle est à la fois injective et surjective.

Utile : Théorème de Cantor-Schröder-Bernstein : soient A et B deux ensembles, si il existe une fonction injective de A vers B (intuitivement $|A| \leq |B|$), et une fonction injective de B vers A (intuitivement $|B| \leq |A|$), alors il existe une bijection entre A et B (intuitivement $|A| = |B|$).

Exercice 1. *Ensembles infinis dénombrables*

4. Donner une bijection entre $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$.
Remarquons que toute bijection f possède une inverse f^{-1} qui est également une bijection, on peut donc donner une bijection entre deux ensembles dans n'importe laquelle des deux directions.
Nous allons démontrer que $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par $f(x, y) = \frac{1}{2}(x+y)(x+y+1)+x$ est bijective. Si l'on dessine une grille bidimensionnelle indexée par $\mathbb{N} \times \mathbb{N}$, alors f attribue un entier naturel à chaque point de coordonnées $(x, y) \in \mathbb{N} \times \mathbb{N}$, selon un ordre qui suit les diagonales successives de pente -1. La formule définissant f est obtenue en remarquant que (x, y) est sur une diagonale comportant $x + y + 1$ élements, en utilisant la formule $\frac{n(n-1)}{2}$ pour compter la somme des entiers de 1 à n déjà utilisés sur les diagonales précédentes, et en ajoutant $+x$ pour assigner des nombres successifs sur une même diagonale.
Surjectivité de f : il suffit de remarquer que $\forall n \in \mathbb{N} : \exists (i, j) \in \mathbb{N} \times \mathbb{N} : n = j + \sum_{i=1}^{k} i$ et $0 \leq j \leq k$. En prenant $x = j$ et $y = k - j$ on obtient $(x, y) \in \mathbb{N} \times \mathbb{N}$ tel que

$$f(x, y) = x + \frac{1}{2}(x+y)(x+y+1) = x + \sum_{i=1}^{x+y} i = j + \sum_{i=1}^{j+k-j} i = n.$$

Injectivité de f : on démontre la contraposée. $\forall (x, y), (x', y') \in \mathbb{N} \times \mathbb{N}$. On procède par disjonction de cas, suivant si les deux points sur la même diagonale ou non :
- si $x + y = x' + y'$ (hyp.1) alors $f(x, y) - f(x', y') = x - x'$ (hyp.2) et l'on en déduit que

$$f(x, y) = f(x', y') \overset{\text{(hyp.2)}}{\iff} x = x' \overset{\text{(hyp.1)}}{\iff} (x, y) = (x', y').$$

  Donc en particulier $(x, y) \neq (x', y') \implies f(x, y) \neq f(x', y')$.
- si $x + y > x' + y'$ (le cas $x + y < x' + y'$ est symétrique) alors $x + y \geq x' + y' + 1$ et

$$(x + y)(x + y + 1) > (x' + y' + 1)(x' + y' + 1) = (x' + y')(x' + y' + 1) + x' + y'.$$

  Donc $(x + y)(x + y + 1) + x > (x' + y')(x' + y' + 1) + x'$, d'où $f(x, y) \neq f(x', y')$.

6. Donner une bijection entre $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.
Nous allons réutiliser la bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ de la question 4. Soit $g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par $g(x, y, z) = f(f(x, y), z)$.
Injectivité de g : $\forall(x, y, z), (x', y', z') \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$:

$$\begin{aligned} g(x,y,z) = g(x',y',z') &\overset{\text{définition de } g}{\Longrightarrow} f(f(x,y),z) = f(f(x',y'),z') \\ &\overset{\text{injectivité de } f}{\Longrightarrow} f(x,y) = f(x',y') \text{ et } z = z' \\ &\overset{\text{injectivité de } f}{\Longrightarrow} x = x' \text{ et } y = y' \text{ et } z = z' \end{aligned}$$

Surjectivité de g : $\forall n \in \mathbb{N}$, par la surjectivité de f il existe $(y', z) \in \mathbb{N} \times \mathbb{N}$ tel que $n = f(y', z)$, et pour y' par la surjectivité de f il existe $(x, y) \in \mathbb{N} \times \mathbb{N}$ tel que $y' = f(x, y)$. Nous obtenons $(x, y, z) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ tel que $g(x, y, z) = f(f(x, y), z) = f(y', z) = n$.

7. Donner une bijection entre Σ^* et $\mathbb{N}$, pour Σ un alphabet fini.
Notre idée pour mettre en correspondance les entiers et les mots consiste intuitivement à « compter en base $m = |\Sigma|$ ». Soit une bijection $\vartheta : \Sigma \to \{1, \ldots, m\}$ (ce sont deux ensembles finis de même taille), qui correspond à attribuer une valeur à chaque lettre. Soit $f : \Sigma^* \to \mathbb{N}$ definie pour tout mot $w = w_k \ldots w_2 w_1 w_0 \in \Sigma^*$ par

$$f(w_k \ldots w_2 w_1 w_0) = \sum_{i=0}^{k} \vartheta(w_i)\, m^i,$$

et avec la convention $f(\epsilon) = 0$. Par exemple pour $\Sigma = \{a, b, c\}$ et $\vartheta(a) = 1, \vartheta(b) = 2, \vartheta(c) = 3$, on aura $f(\epsilon) = 0$, $f(a) = 1$, $f(b) = 2$, $f(c) = 3$, $f(aa) = 4$, $f(ab) = 5$, $f(ac) = 6$, $f(ba) = 7$, $f(bb) = 8$, $f(bc) = 9$, $f(ca) = 10$, $f(cb) = 11$, $f(cc) = 12$, $f(aaa) = 13$, etc, $f(acc) = 21$ puis $f(baa) = 22$.
Injectivité de f : $\forall w, w' \in \Sigma^*$, si $f(w) = f(w')$ alors par définition de f nous avons $\sum_{i=0}^{k} \vartheta(w_i)\, m^i = \sum_{i=0}^{k'} \vartheta(w'_i)\, m^i$ et pouvons alors en déduire inductivement que :

— $\left(\sum_{i=0}^{k} \vartheta(w_i)\, m^i\right) \mod m \equiv \left(\sum_{i=0}^{k} \vartheta(w'_i)\, m^i\right) \mod m$, ce qui se réduit à $\vartheta(w_0) = \vartheta(w'_0)$, donc $w_0 = w'_0$ car ϑ est injective.
— Il s'ensuit que $\sum_{i=1}^{k} \vartheta(w_i)\, m^i = \sum_{i=1}^{k} \vartheta(w'_i)\, m^i$ donc $\left(\sum_{i=1}^{k} \vartheta(w_i)\, m^i\right) \mod m^2 \equiv \left(\sum_{i=1}^{k} \vartheta(w'_i)\, m^i\right) \mod m^2$, ce qui se réduit à $\vartheta(w_1) = \vartheta(w'_1)$, donc $w_1 = w'_1$ car ϑ est injective.
— etc jusqu'à $w_k = w'_k$ et $k = k'$ qui épuisent w et w' simultanément (pour qu'il s'ensuive que $0 = 0$).

Surjectivité de f : étant donné $n \in \mathbb{N}$, pour trouver $w \in \Sigma^*$ tel que $f(w) = n$ nous pouvons adapter l'algorithme de calcul de la représentation en base m de l'entier n. L'adaptation consiste à utiliser le symbole $\vartheta^{-1}(m)$ à la place du 0. En reprenant notre exemple de $\Sigma = \{a, b, c\}$ et $m = 3$, pour $n = 1234$ nous aurons :

$$\begin{array}{rrl} & 1234 \mod 3 \equiv 1 & \Longrightarrow w_0 = \vartheta^{-1}(1) = a \\ \frac{1234-1}{3} = 411 & 411 \mod 3 \equiv 0 & \Longrightarrow w_1 = \vartheta^{-1}(3) = c \\ \frac{411-3}{3} = 136 & 136 \mod 3 \equiv 1 & \Longrightarrow w_2 = \vartheta^{-1}(1) = a \\ \frac{136-1}{3} = 45 & 45 \mod 3 \equiv 0 & \Longrightarrow w_3 = \vartheta^{-1}(3) = c \\ \frac{45-3}{3} = 14 & 14 \mod 3 \equiv 2 & \Longrightarrow w_4 = \vartheta^{-1}(2) = b \\ \frac{14-2}{3} = 4 & 4 \mod 3 \equiv 1 & \Longrightarrow w_5 = \vartheta^{-1}(1) = a \\ \frac{4-1}{3} = 1 & & \Longrightarrow w_6 = \vartheta^{-1}(1) = a \end{array}$$

Et l'on peut vérifier que $f(aabcaca) = 1234$.

Exercice 2. *Ensembles infinis indénombrables*

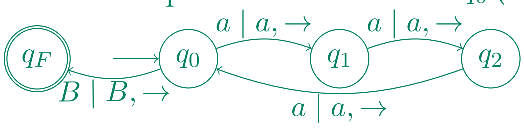
1. Donner une bijection entre $\mathcal{P}(\mathbb{N})$ (l'ensemble des parties de $\mathbb{N}$) et $[0,1]$.
Réels binaires : pour répondre à cette question nous allons écrire tout réel $r \in [0,1]$ en binaire, sous la forme $0.x_0x_1x_2x_3\dots$ avec $r = \sum_{i\geq 0} x_i\, 2^{-i-1}$ (rappelons que les réels peuvent avoir une infinité de décimales/bits après la virgule, comme par exemple $\frac{1}{3} = 0.33333333\dots$ en décimal, et $\frac{1}{3} = 0.01010101\dots$ en binaire). Il y a une petite subtilité : la représentation de certains réels n'est pas unique (comme par exemple en binaire $\frac{1}{2} = 0.10000000\dots = 0.01111111\dots$), mais nous allons ignorer cette subtilité et considérer que deux réels x, x' dont les représentations diffèrent sur au moins un $x_i \neq x'_i$ sont différents.

Notre bijection est $f : \begin{array}{ccl} \mathcal{P}(\mathbb{N}) & \to & [0,1] \\ X & \mapsto & 0.x_0x_1x_2x_3\dots \text{ avec } \mathrm{x}_i = 1 \iff i \in X. \end{array}$
Injectivité de f : $\forall X, X' \in \mathcal{P}(\mathbb{N})$, si $f(X) = 0.x_0x_1x_2x_3\dots = 0.x'_0x'_1x'_2x'_3 = f(X')$ alors $\forall i \in$: $x_i = x'_i$ donc par définition de f on a $i \in X \iff i' \in X'$, c'est-à-dire $X = X'$.
Surjectivité de f : $\forall r = 0.x_0x_1x_2x_3\dots \in [0,1]$ on peut construire l'ensemble $X = \{i \in \mathbb{N} \mid x_i = 1\}$ qui nous donne $f(X) = r$ par définition de f.

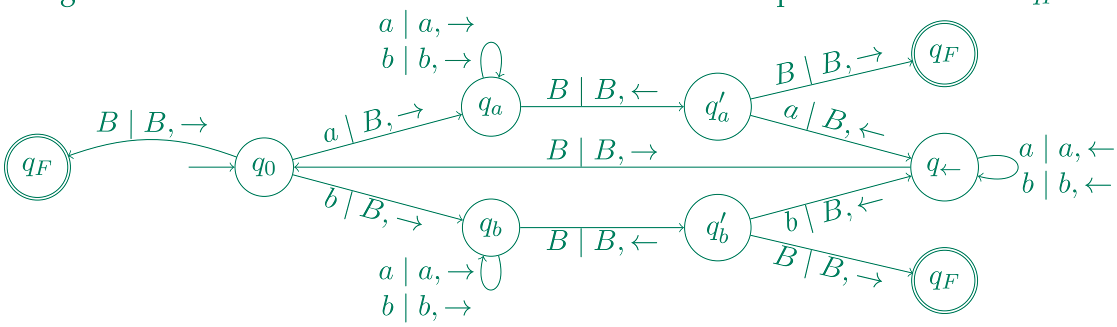
Exercice 5. *MT*

Nous vous invitons à vérifier ces machines sur des exemples de mots dans, et en dehors de, L.

2. $L = \{w \in \Sigma^* \mid |w| \equiv 0 \mod 3\}$ avec $\Sigma = \{a\}$.
Rappelons que $|w| \equiv 0 \mod 3$ signifie que le reste de la division euclidienne de $|w|$ par 3 vaut 0, en d'autres termes la taille de w est un multiple de 3. Notre idée consiste à avoir trois états q_0, q_1, q_2 tels que quand on est dans l'état q_i cela signifie que le mot lu jusqu'ici comporte un nombre de lettres qui, modulo 3, vaut i. Au moment où on lit le symbole B, il faut donc que l'on soit dans l'état q_0 (sinon la machine s'arrête dans un état non final).



3. $L = \{w \in \Sigma^* \mid w \text{ est un palindrome}\}$ avec $\Sigma = \{a, b\}$.
Rappelons qu'un palindrome est un mot qui se lit identiquement de gauche à droite, et de droite à gauche. Notre idée consiste à effacer les lettres du mot d'entrée de la gauche vers la droite, en vérifiant à chaque fois que la lettre correspondante à l'opposée du mot est identique (et en l'effaçant également). Nous avons un palindrome si et seulement si nous atteignons le mot vide. Par soucis de lisibilité nous écrivons plusieurs fois l'état q_F.



Les états q_a et q_b servent à parcourir le mot de gauche à droire jusqu'à la lettre correspondante. Les états q'_a et q'_b vérifient l'identité des lettres en début et fin du mot d'entrée (s'il comporte un nombre impair de lettres, alors la dernière lettre est comparée avec B). L'état $q_\leftarrow$ sert à revenir au début du mot.