1 Problèmes de factorisation

On considère les trois problèmes suivants :
— FINDSMALLESTFACTOR Étant donné $N \in \mathbb{N}^*$ renvoie le plus petit $k \in \mathbb{N}$ avec $k \geq 2$ tel que k divise N.
— FINDGREATESTFACTOR Étant donné $N \in \mathbb{N}^*$ renvoie le plus grand $k \in \mathbb{N}$ avec $k < N$ tel que k divise N.
— HASFACTOR Étant donné $(N, M) \in \mathbb{N}^{*2}$ décide s'il existe un facteur non trivial de N plus petit que M.

Exercice 1. Montrer que si l'on sait résoudre un de ces problèmes en temps polynomial, alors on sait résoudre les trois. Attention le temps polynomial se réfère à la taille de l'entrée qui est logarithmique en les nombres représentés.

Exercice 2. Montrer que HASFACTOR est dans $\mathcal{NP}$. *Vous pouvez supposer que tester la primalité d'un nombre est dans $\mathcal{P}$.*

Exercice 3. Montrer que HASFACTOR est dans co-$\mathcal{NP}$.

2 Propriétés de clôture

Exercice 4. Montrer que les langages décidables en temps polynomial sont stables par intersection, union, complémentation et étoile (i.e. le langage L^*).

3 Fonctions à sens unique

Supposons que :
— on a une bijection f des entiers sur n bits vers les entiers sur n bits, pour tout n (i.e., sur une entrée x de n bits, $f(x)$ est un entier sur n bits tel que $f(x) = f(y) \Rightarrow x = y$).
— la fonction f se calcule en temps polynomial.
— la fonction inverse de f ne peut pas se calculer en temps polynomial. (On dit que c'est une fonction à sens unique.)

Exercice 5. Montrer que si une telle bijection existe, alors $\mathcal{P} \neq \mathcal{NP}$.
Suggestion : Montrer que le langage $L = \{(x, f(y)) : x \leq y\}$ appartient à $\mathcal{NP} \setminus \mathcal{P}$.

Exercice 6. Montrer de plus, que si elle existe, alors $\mathcal{NP} \cap$ co-$\mathcal{NP} \neq \mathcal{P}$.

4 Quines

Pour deux MT A et B on note $A \cdot B$ une MT qui exécute B après avoir exécuté A.
Pour chaque mot $w \in \Sigma^*$, soit $P(w)$ un MT sur Σ qui écrit le mot w sur le ruban.

Exercice 7. Expliquer pourquoi la fonction $q : \mathbb{N} \to \mathbb{N}$ est récursive (i.e. calculable).

$$q(n) = \begin{cases} \langle P(w) \rangle & \text{s'il existe } w \in \Sigma^* \text{ tel que } n = \langle w \rangle \\ \bot & \text{sinon} \end{cases}$$

Exercice 8. Expliquer pourquoi la fonction $s_2(m, n) : \mathbb{N}^2 \to \mathbb{N}$ est récursive.

$$s_2(m, n) = \begin{cases} \langle A \cdot B \rangle & \text{s'il existe } A, B \text{ telles que } \langle A \rangle = m \wedge \langle B \rangle = n \\ \bot & \text{sinon} \end{cases}$$

Exercice 9. En déduire qu'il existe une MT M qui termine en affichant $\langle M \rangle$ sur la bande.