

## TD 9 – Complexité en temps

### 1 Problèmes de factorisation

On considère les trois problèmes suivants.

- **FINDSMALLESTFACTOR** : Étant donné  $N \in \mathbb{N}_{>0}$  renvoie le plus petit  $k \in \mathbb{N}$  avec  $k \geq 2$  tel que  $k$  divise  $N$ .
- **FINDGREATESTFACTOR** : Étant donné  $N \in \mathbb{N}_{>0}$  renvoie le plus grand  $k \in \mathbb{N}$  avec  $k < N$  tel que  $k$  divise  $N$ .
- **HASFACTOR** : Étant donné  $(N, M) \in (\mathbb{N}_{>0})^2$  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.

Pour la suite, vous pouvez supposer que tester la primalité d'un nombre est dans P.

**Exercice 2.** Montrer que HASFACTOR est dans NP.

**Exercice 3.** Montrer que HASFACTOR est dans coNP.

### 2 Coloriabilité

Étant donné un graphe non-orienté  $G = (V, E)$ , un  $k$ -coloriage de  $G$ , pour  $k \in \mathbb{N}_{>0}$ , est une application  $c: V \rightarrow \llbracket 1, k \rrbracket$  associant une couleur (un nombre) de 1 à  $k$  à chaque sommet de  $G$ , de telle manière que deux sommets  $x$  et  $y$  adjacents (c'est-à-dire, tels que  $\{x, y\} \in E$ ) n'aient jamais la même couleur ; lorsqu'un tel  $k$ -coloriage existe, on dit que  $G$  est  $k$ -coloriable.

**Exercice 4.** Montrer que le langage  $3\text{COL} = \{\langle G \rangle \mid G \text{ graphe non orienté 3-coloriable}\}$  est dans NP.

**Exercice 5.** Montrer que le langage  $2\text{COL} = \{\langle G \rangle \mid G \text{ graphe non orienté 2-coloriable}\}$  est dans P.

### 3 Propriétés de clôture

**Exercice 6.** Montrer que P est close par intersection, union, complémentation et étoile.

### 4 Quelques propriétés de classes

Étant donné une fonction  $t: \mathbb{N} \rightarrow \mathbb{N}$ , on note  $\text{DTIME}(t(n))$  la classe des langages reconnus par une MT  $\mathcal{M}$  telle qu'il existe une constante  $\alpha \in \mathbb{R}$  pour laquelle, sur toute entrée  $x$ , on a que  $\mathcal{M}(x)$  fonctionne en temps au plus  $\alpha \cdot t(|x|)$ .

On peut alors définir  $\text{P} = \bigcup_{k \in \mathbb{N}} \text{DTIME}(n^k)$  et  $\text{EXP} = \bigcup_{k \in \mathbb{N}} \text{DTIME}(2^{n^k})$ .

De même, étant donné une fonction  $t: \mathbb{N} \rightarrow \mathbb{N}$ , on note  $\text{NTIME}(t(n))$  la classe des langages reconnus par une MTN  $\mathcal{M}$  telle qu'il existe une constante  $\alpha \in \mathbb{R}$  pour laquelle, sur toute entrée  $x$ , on a que  $\mathcal{M}(x)$  fonctionne en temps au plus  $\alpha \cdot t(|x|)$ , quels que soient les choix qu'elle fait lors de son exécution.

On définit alors, de manière similaire,  $\text{NP} = \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)$  et  $\text{NEXP} = \bigcup_{k \in \mathbb{N}} \text{NTIME}(2^{n^k})$ .

Rappelons en outre que, pour toute classe  $C$  de langages, la classe  $\text{co}C$  est donnée par  $\text{co}C = \{\bar{L} \mid L \in C\}$ .

**Exercice 7.** Montrer que si  $P = NP$ , alors  $NP = \text{co}NP$ .

**Exercice 8.** Montrer que si  $P = NP$ , alors  $\text{EXP} = \text{NEXP}$ .

**Exercice 9.** Montrer que si tout langage unaire de  $NP$  est dans  $P$ , alors  $\text{EXP} = \text{NEXP}$ .