Outils et algorithmes pour la protection de l'information (I231)
Session 1 (2021-2022) - Partie 1 (12pts)

La précision et la clarté de votre rédaction sont ***fondamentales***. Chaque réponse doit être ***justifiée***, les programmes doivent être ***commentés*** et les algorithmes ***expliqués***. Le [barème] est donné à titre indicatif et il est susceptible d'être adapté. Les documents sont interdits. Durée à consacrer à cette partie : 1h45.

EXERCICE 1. [8.25] Un graphe $G = (X, V)$ est constitué d'un ensemble fini X de *sommets* et d'un ensemble $V \subseteq X \times X$ d'*arcs*, ou d'*arêtes* si l'orientation n'a pas d'importance mais on conserve la notation (x, y) pour simplifier.

Déf. 1. *Un sous-ensemble de sommets $R \subseteq X$ est appellé un* recouvrement par les sommets *de G si tout arc de G admet au moins une extrémité dans R.*

Déf. 2. *Un sous-ensemble de sommets $I \subseteq X$ est dit* indépendant *si aucun arc de G ne relie deux sommets quelconques de I.*

Déf. 3. *Un sous-ensemble de sommets $C \subseteq X$ est appelé une* clique *si deux sommets quelconques de C sont reliés par un arc de G.*

1. [1.50] Formalisez ces trois définitions à l'aide de la logique des prédicats.

2. [4.50] Soit $G := (X, V)$ un graphe. Démontrez que les trois propositions suivantes sont équivalentes :

(1) R est un *recouvrement par les sommets* de X.

(2) $X \setminus R$ est un *ensemble de sommets indépendants.*

(3) $X \setminus R$ est une *clique* du graphe $\overline{G} = (X, \overline{V})$ où $\overline{V} := (X \times X) \setminus V$.

On considère les problèmes de décision suivants :

Problème VC [Recouvrement par les sommets]
Instance : Un graphe $G = (X, V)$ et un entier positif $K \leq |X|$.
Question : Existe-t-il un recouvrement R de taille inférieure à K ?

Problème INDSET [Ensemble de sommets indépendants]
Instance : Un graphe $G = (X, V)$ et un entier positif $K \leq |X|$.
Question : Existe-t-il un sous-ensemble I de sommets indépendants de taille supérieure à K ?

Problème CL [Clique]
Instance : Un graphe $G = (X, V)$ et un entier positif $K \leq |X|$.
Question : Existe-t-il une clique C de taille supérieure à K ?

3. [0.75] Donnez une instance positive (non-triviale) pour chacun de ces trois problèmes de décision (avec des graphes non-orientés).

4. [0.50] Démontrez que le problème VC est dans NP.

5. [1.00] On suppose que VC est NP-difficile. Déduire de la question 2 que INDSET et CL sont NP-complets.

EXERCICE 2. [3.75pts] On se fixe l'alphabet $\Sigma := \{0, 1\}$.

1. [2.50] Démontrez que l'opérateur bit-à-bit $\oplus$ vu comme une fonction de $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ est Turing-calculable.

2. [1.25] Calculez les fonctions de complexité en temps $T(n)$ et en espace $E(n)$ de votre algorithme.

NB. Les opérandes en entrée sont de même taille n (en complétant le plus court par des 0 à gauche si nécessaire) et sont séparés par une case vide. Expliquez votre algorithme en français, ou en langage pseudo-algorithmique au préalable et commentez impérativement les blocs d'instructions de votre machine de Turing.