

Outils et algorithmes pour la protection de l'information (I231)
Session 2 (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 appelé 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 .*

- [1.50] Formalisez ces trois définitions à l'aide de la logique des prédicats.
- [4.50] Soit $G := (X, V)$ un graphe. Démontrez que les trois propositions suivantes sont équivalentes :
 - R est un *recouvrement par les sommets* de X .
 - $X \setminus R$ est un *ensemble de sommets indépendants*.
 - $X \setminus R$ est une *clique* du graphe $\bar{G} = (X, \bar{V})$ où $\bar{V} := (X \times X) \setminus V$.

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 ?

- [0.75] Donnez une instance positive (non-triviale) pour chacun de ces trois problèmes de décision (avec des graphes non-orientés).
- [0.50] Démontrez que le problème VC est dans NP.
- [1.00] On suppose que VC est NP-difficile. Dédurre des questions 2 et 4 que INDSET et CL sont NP-complets.

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

- [2.50] Démontrez que la fonction $f : \mathbb{N} \rightarrow \mathbb{N}$ définie par $f(n) := n + 1$ est Turing-calculable.
- [1.25] Calculez les fonctions de complexité en temps $T(n)$ et en espace $E(n)$ de votre algorithme.

Expliquez votre algorithme en français, ou en langage pseudo-algorithmique au préalable et commentez impérativement les blocs d'instructions de votre machine de Turing.