IF228 CALCULABILITÉ ET COMPLEXITÉ	DS 2	2025-2026

Indications : Les exercices sont indépendants. La note finale est la somme des points obtenus aux deux exercices. Dans l'exercice 2, chaque partie dépend des parties précédentes. Les questions précédées d'une étoile sont difficiles ; elles rapportent des points hors-barème.

Exercice 1 [sur 10] On examine, dans cet exercice, des variantes du Problème de Correspondance de Post.
On appelle homomorphisme du monoide libre A^* dans le monoide libre B^*, toute application $\varphi : A^* \to B^*$ telle que

$$\varphi(\varepsilon) = \varepsilon \text{ et } \forall u, v \in A^*, \ \ \varphi(u \cdot v) = \varphi(u) \cdot \varphi(v).$$

Le problème PCP peut se reformuler comme suit :

- **Instance :** Deux alphabets finis A, B et deux homomorphismes $\varphi, \psi : A^* \to B^*$.
- **Question :** Existe-t-il un mot $w \in A^+$ tel que $\varphi(w) = \psi(w)$?

1- Rappeler (sans justification) le résultat vu en cours concernant le problème PCP : est-il décidable ? ou indécidable ?
2- Pour chacun des problèmes de décision suivants, dire s'il est décidable ? ou indécidable ? et justifiez votre réponse par un algorithme (informel) ou une réduction (many-one ou de Turing).
Problème PCP*

- **Instance :** Deux alphabets finis A, B et deux homomorphismes $\varphi, \psi : A^* \to B^*$.
- **Question :** Existe-t-il un mot $w \in A^*$ tel que $\varphi(w) = \psi(w)$?

Problème PCP-RAT

- **Instance :** Deux alphabets finis A, B, un automate fini $\mathcal{A}$ et deux homomorphismes $\varphi, \psi : A^* \to B^*$.
- **Question :** Existe-t-il un mot $w \in \mathrm{L}(\mathcal{A})$ tel que $\varphi(w) = \psi(w)$?

(on dénote par $\mathrm{L}(\mathcal{A})$ le langage reconnu par l'automate $\mathcal{A}$).
Problème PCP-PROD

- **Instance :** Deux alphabets finis A, B, deux homomorphismes $\varphi, \psi : A^* \to B^*$.
- **Question :** Existe-t-il des mots $u, v \in A^+$ tel que $\varphi(u \cdot v) = \psi(u \cdot v)$?

Problème PCP-IND

- **Instance :** Deux alphabets finis A, B, deux homomorphismes $\varphi, \psi : A^* \to B^*$.
- **Question :** Existe-t-il des mots $u, v \in A^+$ tel que $\varphi(u) = \psi(v)$?

Exercice 2 [sur 20]

Partie 1

Fonctions à sens unique.

Dans tout cet exercice X désigne un ensemble fini.
1- Soit $f : X^* \to X^*$ une fonction totale calculable, bijective. L'inverse de f, notée f^{-1}, est une fonction totale. Est-elle calculable, en général ?
2- Soit $f : X^* \to X^*$ une fonction totale. Montrer qu'il existe une fonction totale $\bar{f} : X^* \to X^*$ telle que

$$\forall x \in X^*, f(\bar{f}(f(x))) = f(x). \tag{1}$$

Nous nommons *pseudo-inverse* de f, toute fonction totale $\bar{f}$ qui vérifie la condition (1).
*3- Est-ce que, toute fonction totale calculable $f : X^* \to X^*$ admet un pseudo-inverse *calculable* ? Aide : construire une fonction totale calculable f dont l'image n'est pas récursive.

Définition Une fonction $f : X^* \to X^*$ (où X est un alphabet fini de cardinal ≥ 2) est dite "à sens unique" ssi elle vérifie les trois conditions :
(C1) f est totale, calculable en temps déterministe polynomial (classe **FP**)
(C2) Il existe des polynomes p, q à coefficients dans $\mathbb{N}$ tels que :

$$\forall u \in X^*, |f(u)| \leq p(|u|) \text{ et } |u| \leq q(|f(u)|).$$

(C3) Pour toute fonction totale $\bar{f} : X^* \to X^*$, si $f \circ \bar{f} \circ f = f$ alors $\bar{f} \notin \mathbf{FP}$.
On examine, dans les parties 2,3 la question de savoir s'il existe des fonctions à sens unique.

Partie 2

Considérons une fonction $f : X^* \to X^*$ telle que

$$f \text{ est à sens unique} \tag{2}$$

Considérons le problème de décision (PREFIX-INVERSE) suivant :

- **Instance :** Des mots $u, w \in X^*$
- **Question :** Existe-t-il un mot $v \in X^*$ tel que $f(uv) = w$?

4- Montrer que le problème (PREFIX-INVERSE) est dans **NP**.
5- Montrer que, si A est un algorithme (déterministe) qui résout le problème (PREFIX-INVERSE) en temps polynômial alors f a un pseudo-inverse $\bar{f}$ dans la classe **FP**.
*6- Montrer que, si il existe une fonction à sens unique, alors $\mathbf{NP} \neq \mathbf{P}$.

Partie 3

Considérons maintenant un langage $L \subseteq X^*$ tel que

$$L \text{ appartient à la classe de complexité } \mathbf{NP} \setminus \mathbf{P}. \tag{3}$$

Alors il existe une fonction totale $V : X^* \times X^* \to \{0,1\}$ et des polynômes $p_1, p_2 \in \mathbb{N}[z]$ tels que

$$L = \{u \in X^* \mid \exists v \in X^*, V(u,v) = 1 \text{ et } |v| \leq p_1(|u|)\},$$

et V est calculable en temps $\leq p_2(|u| + |v|)$.
On suppose que les symboles $\#, 0, 1$ n'appartiennent pas à X et on considère l'alphabet :

$$Y := X \cup \{\#, 0, 1\}.$$

Nous construisons une fonction $f : Y^* \to Y^*$ par :

$$\forall u, v \in X^*, \text{ si } |v| \leq p_1(|u|), f(u\#v) := u\#V(u,v); \quad \text{si } |v| > p_1(|u|), f(u\#v) := \#\#u\#v,$$

$$\forall w \in Y^* \setminus (X^*\#X^*), f(w) := \#\#w.$$

7- Montrer que f vérifie la condition (C1).
8- Montrer que f vérifie la condition (C2).
*9- Montrer que f vérifie la condition (C3).
10- Montrer que si $\mathbf{NP} \neq \mathbf{P}$ alors il existe une fonction à sens unique.