TD 05 – Prophéties spatiales

Exercice 1. *...jusqu'à Agrawal et al.*

PRIMES est dans NP [1].

1. PRIMES est-il dans coNP ? dans P ?

On admettra [2] dans la suite qu'un entier n est premier si et seulement si il existe un nombre a dans $[1, n-1]$ tel que
– $a^{n-1} \equiv 1 \mod n$
– $\forall q \in \mathbb{P} : q|(n-1), a^{n-1/q} \not\equiv 1 \mod n$

2. Avec cette définition, montrer que PRIMES est dans NP.

Exercice 2. *Poisson cuisiné au menu*

On définit les deux réductions suivantes :
– *many-one* ou *Karp* : $A \leq_m^p B \iff \exists f \in \mathsf{FP}, (x \in A \iff f(x) \in B)$
– *par oracle* ou *Cook-Turing* : $A \leq_T^p B \iff A \in \mathsf{P}^B$

1. Quelle est la réduction vue en cours ?
2. Montrer que TAUTOLOGIE $\in \mathsf{P}^{\mathrm{SAT}}$, et plus généralement que pour tout A, $\bar{A} \leq_T^p A$.
3. Montrer que pour tout $A \in \mathsf{P}$, $\mathsf{P}^A = \mathsf{P}$.
4. Montrer que $\leq_T^p$ est transitive ($A \leq_T^p B$ et $B \leq_T^p C$ impliquent $A \leq_T^p C$).
5. Montrer que si TAUTOLOGIE $\leq_m^p$ SAT alors NP = coNP.
6. Montrer que NP = coNP ssi NP est close pour $\leq_T^p$ ($A \leq_T^p B$ et $B \in \mathsf{NP} \implies A \in \mathsf{NP}$).
7. Quelles relations existent entre $\leq_m^p$ et $\leq_T^p$?

Exercice 3. *Langage* L

1. Montrer que les fonctions $n \mapsto \lfloor \log n \rfloor$ et $n \mapsto n^k$ ($k \geq 1$) sont constructibles en espace, et que si f est constructible en espace, alors 2^f également.
2. Montrer que les langages PAIR $= \{x : x$ contient un nombre pair de $1\}$ et MULT $= \{\langle \overline{n}, \overline{m}, \overline{n \cdot m} \rangle : n, m \in \mathbb{N}\}$ sont dans L.
3. Montrer que 3-SAT $\in$ PSPACE, et plus généralement que NP $\subseteq$ PSPACE.

Exercice 4. *Théorème de Berman (1978)*

1. Donner un algorithme récursif pour résoudre SAT.
2. Soit S un langage unaire NP-complet. En utilisant une réduction polynomiale de SAT à S, améliorer l'algorithme précédent pour qu'il devienne polynomial.
3. Donc ?

1. On n'utilisera pas l'algorithme AKS pour répondre aux questions suivantes...
2. Il s'agit du test de primalité de Lucas connu depuis la fin du XIX$^{\mathrm{e}}$ siècle. (cf. wikipedia si vous voulez des détails).