Partiel – Lundi 7 novembre 2011

Durée : 2h. Notes de cours et documents non autorisés. Le sujet comprend 5 exercices indépendants, puis un exercice bonus : les deux premiers exercices sont du cours, ou en sont très proches. Les trois exercices suivants sont sans doute de difficulté croissante.
La notation tiendra compte de la qualité de la rédaction et du soin apporté à la copie.
Si vous bloquez sur une question d'un exercice, vous pouvez admettre le résultat et passer à la suite.

Exercice 1. *Cours de dessin*

Donner toutes les inclusions connues entre les classes de complexité suivantes, en précisant les inclusions strictes et les égalités : AP, PH, P, NP, coNP, L, NL, coNL, PSPACE, NPSPACE, coNPSPACE, EXP, NEXP, Σ_1^p, Π_1^p, Σ_2^p, Π_2^p, Σ_i^p et Π_i^p pour $i > 2$, P/poly. Justifier les inclusions strictes et les égalités par un théorème du cours, *en citant l'énoncé complet*.
Vous pouvez par exemple représenter les inclusions sous forme de graphe orienté, et utiliser la transitivité de l'inclusion pour limiter le nombre d'arcs.

Exercice 2. *Oracles*

Soit $\mathcal{C}$, $\mathcal{C}_1$ et $\mathcal{C}_2$ trois classes de complexité. On note $\mathcal{C}_1^{\mathcal{C}_2} = \bigcup_{L\in\mathcal{C}_2} \mathcal{C}_1^L$.

1. A-t-on toujours $\mathcal{C}_1 = \mathcal{C}_2 \implies \mathcal{C}^{\mathcal{C}_1} = \mathcal{C}^{\mathcal{C}_2}$?
2. A-t-on toujours $\mathcal{C}_1 = \mathcal{C}_2 \implies \mathcal{C}_1^{\mathcal{C}} = \mathcal{C}_2^{\mathcal{C}}$?
3. Montrer que pour tout langage A, $\mathsf{P}^A = \mathsf{NP}^A \implies \mathsf{P}^A = \mathsf{PH}^A$.
4. Exhiber un langage A tel que $\mathsf{P}^A = \mathsf{NP}^A$.

Définition. On dit qu'un langage $L \subseteq \Sigma^\star$ est *creux* lorsqu'il existe un polynôme p tel que $L \cap \Sigma^n$ est de cardinal au plus $p(n)$ pour tout n.

Exercice 3. *Conseil : c'est creux*

1. Montrer que tout langage creux appartient à P/poly.
2. Montrer que $\mathsf{P/poly} = \bigcup_{L \text{ creux}} P^L$.

Exercice 4. *Rembourrage*

On note $\mathsf{E} = \bigcup_c \mathsf{DTIME}(2^{cn})$, à ne pas confondre avec EXP.

1. Montrer que si $\mathsf{E} = \mathsf{PSPACE}$, alors $\mathsf{DTIME}(2^{n^2}) \subseteq \mathsf{PSPACE}$.
2. Donc ?

Exercice 5. *Théorème de Mahaney*

On souhaite démontrer le théorème suivant, en utilisant un preuve due à Ogihara et Watanabe.

Théorème (Mahaney, 1982)**.** *S'il existe un langage creux* NP*-difficile, alors* P = NP.

Soit L un langage creux NP-difficile, et soit $X \in \mathsf{NP}$ défini par

$$x \in X \iff \exists y \in \Sigma^{q(|x|)}, \langle x, y\rangle \in Y,$$

où q est un polynôme et $Y \in \mathsf{P}$.
On définit $G(X) = \{\langle x, w\rangle : \exists y \in \Sigma^{q(|x|)}, y \geq w \text{ et } \langle x, y\rangle \in Y\}$ où $y \geq w$ signifie que y est plus grand que x dans l'ordre lexicographique.

1. Montrer que $G(X) \in \mathsf{NP}$.
2. Soit f une réduction polynomiale de $G(X)$ à L, et soit $x \in \Sigma^n$. Que peut-on dire du cardinal de $\{f(\langle x, w\rangle) : \langle x, w\rangle \in G(X)\}$?
3. Soit $w_1, w_2 \in \Sigma^\star$ avec $w_1 \leq w_2$. On note $E_x(w_1, w_2)$ l'ensemble des couples $\langle x, w\rangle$ tels que $w_1 \leq w \leq w_2$ et $\chi_{G(X)}$ la fonction indicatrice de $G(X)$. Si $\chi_{G(X)}(\langle x, w_1\rangle) = \chi_{G(X)}(\langle x, w_2\rangle)$, que peut-on dire des couples $\langle x, w\rangle \in E_x(w_1, w_2)$?
4. Donner un algorithme décidant X en temps polynomial. **Indication.** Sur l'entrée x, l'algorithme trouvera le plus grand w tel que $\langle x, w\rangle \in G(X)$ si un tel w existe.

Exercice bonus

La cryptographie (moderne) est basée sur l'idée suivante : il existe des fonctions qu'on sait facilement calculer, mais qu'il est difficile d'inverser. On va s'intéresser ici à un type de telles fonctions, qu'on appellera *fonction à sens unique* [1].

Définition. Une fonction f est dite *honnête* si pour tout y dans l'image de f, y admet un antécédent de taille polynomiale. Autrement dit, il existe un polynôme q tel que pour tout x, il existe x' tel que $f(x') = f(x)$ et $|x'| \leq q(|f(x')|)$.
On dit qu'une fonction f est *inversible en temps polynomial* si pour tout y dans l'image de f, on peut trouver *un* antécédent de y en temps polynomial : il existe une fonction g, calculable en temps polynomial, telle que $f(g(y)) = y$ pour tout y dans l'image de f.
Une *fonction à sens unique* est une fonction f, calculable en temps polynomial, honnête, et qui n'est pas inversible en temps polynomial.

1. Soit f une fonction calculable en temps polynomial et honnête. Montrer qu'elle est inversible *en temps non déterministe polynomial*.
2. Supposons qu'il existe une fonction à sens unique f. On définit $\textsc{Pref-Inv}(f) = \{\langle y, t\rangle : \exists x, |t \cdot x| \leq q(|y|) \text{ et } f(t \cdot x) = y\}$, où q est le polynôme témoin de l'honnêteté de f, et $t \cdot x$ est la concaténation de t et x. Montrer que $\textsc{Pref-Inv}(f) \in \mathsf{NP} \setminus \mathsf{P}$.
3. Soit X un problème de NP, et $Y \in \mathsf{P}$ et un polynôme p tels que $x \in X \iff \exists y \in \Sigma^{p(|x|)}, \langle x, y\rangle \in Y$. Considérons f définie sur les entrées de la forme $\langle x, w\rangle$, et telle que $f(\langle x, w\rangle) = 0x$ si $\langle x, w\rangle \in Y$, et $1x$ sinon. Montrer que si f est inversible en temps polynomial, alors X peut être accepté en temps polynomial (c'est-à-dire qu'il existe une machine déterministe M qui accepte en temps polynomial si $x \in X$, et qui rejette ou boucle si $x \notin X$).

1. La définition donnée ici n'est pas la définition utilisée actuellement, mais celle utilisée dans les années 1980.