M1, 2005–2006

Complexité structurelle – TD 4
Diagonalisation

1 Utilisation des théorèmes de hiérarchie

Exercice 1

1. Soit $c > 0$. Montrer que si DSPACE(n^c) $\subseteq$ NP alors NP = PSPACE.
2. En déduire que pour tout $c > 0$ on a DSPACE(n^c) $\neq$ NP, et également NSPACE(n^c) $\neq$ NP.
3. Montrer de même que pour tout $c > 0$, DTIME(2^{cn}) $\neq$ NP.

2 Diagonalisation retardée

Nous allons utiliser la même méthode que dans la preuve du théorème de Ladner (*delayed diagonalization*) pour montrer un résultat un peu plus fort :
Théorème – Si P $\neq$ NP, alors il existe deux langages $A, B \in$ NP tels que $A \not\leq_T B$ et $B \not\leq_T A$.

Nous allons prendre A de la forme $A = \mathrm{SAT} \cap S$ où

$$S = \{x; |x| \in \cup[a_{2i}, a_{2i+1}[\} \in \mathrm{P}$$

pour une certaine suite (a_i) strictement croissante à construire, et $B = \mathrm{SAT} \setminus A$.

Exercice 2

1. Grâce à une énumération des machines de Turing polynomiales à horloge et à oracle, reformuler la conclusion du théorème.
2. Construire la suite (a_i) afin de satisfaire les conditions du 1 tout en maintenant S dans P.
3. En déduire le théorème.
4. Montrer que cela implique le théorème de Ladner : si P $\neq$ NP alors il existe des problèmes dans NP $\setminus$ P qui ne sont pas NP-complets.

3 Borne inférieure non uniforme

EXPSPACE est la classe des langages décidables en espace $2^{O(n)}$:

$$\mathrm{EXPSPACE} = \bigcup_{c>0} \mathrm{DSPACE}(2^{cn}).$$

Exercice 3

1. Donner un majorant évident du nombre de circuits booléens dont le code est de taille $\leq n^{\log n}$.
2. On travaille à n fixé. On veut définir $L^{=n}$ tel qu'il ne soit reconnu par aucun circuit à n entrées de taille $\leq n^{\log n}$. Définir $\{0^n\} \cap L$ de façon à ce qu'au moins la moitié des circuits se trompent sur 0^n.
3. Définir complètement le langage $L^{=n}$, montrer qu'il n'est pas reconnu par des circuits de taille polynomiale.
4. En déduire que EXPSPACE $\not\subseteq$ P/poly.