Modnet, June 2006

Algebraic complexity – Exercise session 3
Boolean parts

We first show that boolean nondeterminism is enough for NP over the structure $(\mathbf{R}, +, -, =)$.

Then we investigate the links between the questions P = NP in algebraic complexity and in boolean complexity thanks to boolean parts.

Let $\mathrm{NDP}_{(\mathbf{R},+,-,=)}$ be the class of languages $A \subseteq \mathbf{R}^\infty$ such that there exist a language $B \in \mathrm{P}_{(\mathbf{R},+,-,=)}$ and a polynomial p satisfying

$$x \in A \iff \exists y \in \{0,1\}^{p(|x|)} (x, y) \in B.$$

Exercise 1 Boolean nondeterminism

1. Let S be a system of linear (dis)equations in $y \in \mathbf{R}^n$ of the form

$$\{\sum_{j=1}^{n} a_{ij} y_j = b_i \ (1 \le i \le p)\} \cup \{\sum_{j=1}^{n} c_{ij} y_j \ne d_i \ (1 \le i \le q)\}$$

   where $a_{ij}, c_{ij} \in \mathbf{N}$ and $b_i, d_i \in \mathbf{R}$. Suppose that a_{ij}, c_{ij} are given in binary, so that they are encoded by a sequence of bits. Show that in $\mathrm{P}_{(\mathbf{R},+,-,=)}$ one can decide whether S has a solution.

2. Show that $\mathrm{NDP}_{(\mathbf{R},+,-,=)} = \mathrm{NP}_{(\mathbf{R},+,-,=)}$.

The boolean part $BP(L)$ of a language $L \subseteq M^\infty$ is $L \cap \{0,1\}^*$. The boolean part of a complexity class is the set of the boolean parts of its languages.
Exercise 2
Prove that $BP(\mathrm{P}_{(\mathbf{R},+,-,=)}) = \mathrm{P}$ and $BP(\mathrm{NP}_{(\mathbf{R},+,-,=)}) = \mathrm{NP}$.

We give the following result concerning the existence of small rational points in a polyhedron.
Theorem. Let S be a polyhedron of $\mathbf{R}^n$ defined by a system of N strict or large inequalities of the form

$$Ax \le b; \ A'x < b'$$

where the coefficients of A, A', b, b' are integers of size L. If $S \ne \emptyset$ then there exists a rational point $x \in S$ of size polynomial in L and n.

Furthermore, as in the case of $(\mathbf{R}, +, -, =)$, the classes $\mathrm{NP}_{(\mathbf{R},+,-,\le)}$ and $\mathrm{NDP}_{(\mathbf{R},+,-,\le)}$ coincide (the proof is slightly more involved because of the order $\le$ but uses the same idea).

Exercise 3

1. Show that the boolean part of $\mathrm{P}_{(\mathbf{R},+,-,\leq)}$ is $\mathbb{P}$ (hint: replace real constants by rationals).
2. Show that the boolean part of $\mathrm{NP}_{(\mathbf{R},+,-,\leq)}$ is $\mathbb{NP}$.
3. Deduce the following implication:

$$\mathrm{P}_{(\mathbf{R},+,-,\leq)} = \mathrm{NP}_{(\mathbf{R},+,-,\leq)} \Longrightarrow \mathbb{P} = \mathbb{NP}.$$