Algebraic complexity – Exercise session 3

Boolean parts

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

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

Let \(\text{NDP}(\mathbb{R}, +, -, =)\) be the class of languages \(A \subseteq \mathbb{R}^{\infty}\) such that there exist a language \(B \in \text{P}(\mathbb{R}, +, -, =)\) 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 \(y \in \mathbb{R}^n\) of the form

\[
\{ \sum_{j=1}^{n} a_{ij} y_j = b_i (1 \leq i \leq p) \} \cup \{ \sum_{j=1}^{n} c_{ij} y_j \neq d_i (1 \leq i \leq q) \}
\]

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

2. Show that \(\text{NDP}(\mathbb{R}, +, -, =) = \text{NP}(\mathbb{R}, +, -, =)\).

---

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 \(BP(\text{P}(\mathbb{R}, +, -, =)) = \text{P}\) and \(BP(\text{NP}(\mathbb{R}, +, -, =)) = \text{NP}\).

We give the following result concerning the existence of small rational points in a polyhedron.

**Theorem.** Let \(S\) be a polyhedron of \(\mathbb{R}^n\) defined by a system of \(N\) strict or large inequalities of the form

\[
Ax \leq b; \quad A' x < b'
\]

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

Furthermore, as in the case of \((\mathbb{R}, +, -, =)\), the classes \(\text{NP}(\mathbb{R}, +, -, \leq)\) and \(\text{NDP}(\mathbb{R}, +, -, \leq)\) coincide (the proof is slightly more involved because of the order \(\leq\) but uses the same idea).
Exercise 3

1. Show that the boolean part of $P_{(\mathbb{R},+,\cdot,\leq)}$ is $\mathbb{P}$ (hint: replace real constants by rationals).

2. Show that the boolean part of $NP_{(\mathbb{R},+,\cdot,\leq)}$ is $\mathbb{NP}$.

3. Deduce the following implication:

$$P_{(\mathbb{R},+,\cdot,\leq)} = NP_{(\mathbb{R},+,\cdot,\leq)} \implies \mathbb{P} = \mathbb{NP}.$$