Tutorial 11 – Probabilistic classes

Definition. Let RP be the class[1] of languages L s.t. there exits a polytime Probabilistic Turing Machine M s.t. for every $x \in \{0,1\}^*$,

$$x \in L \implies \mathbb{P}[M(x) = 1] \geq 2/3,$$
$$x \notin L \implies \mathbb{P}[M(x) = 0] = 1.$$

Equivalently, the class PP is defined by $x \in L \iff \mathbb{P}[M(x) = 1] > 1/2$.

Exercise 1. *Polynomial Identity Testing*

An *arithmetic circuit* is a directed acyclic graph whose inputs are indeterminates x_i and the constant 1, and whose gates are $+$, $\times$ and $-$. Thus an arithmetic circuit computes a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$. The problem PolyNonNul is the set of arithmetic circuits computing a nonzero polynomial.

1. What is the maximal degree of a size-m circuit?

2. Show the following lemma:

   Lemma (Schwartz-Zippel)**.** *Let $p(x_1, \ldots, x_n)$ be a nonzero polynomial of degree at most d, and S a finite set of integers. If $a_1, \ldots, a_n$ are randomly chose (with replacement) in S, then*

   $$\mathbb{P}[p(a_1, \ldots, a_n) = 0] \leq d/|S|.$$

3. Propose a probabilistic algorithm deciding PolyNonNul which errs with probability at most $1/3$. What is its complexity?

4. Show that PolyNonNul $\in$ RP. **Hint.** On can compute *modulo* an integer n, and use the fact that there are $\pi(n) = O(n/\log n)$ prime numbers not greater than n.

Exercise 2.

Let us consider vairant of the Sat:

$$\text{MajSat} = \{\phi : \phi \text{ is satisfied by } > 1/2 \text{ of its assignments}\}$$
$$\#\text{Sat} = \{(\phi, k) : \phi \text{ is satisfied by } > k \text{ assignments}\}$$

1. Show that MajSat $\in$ PP.

2. Show that #Sat $\leq_p$ MajSat.

3. Show that #Sat and MajSat are PP-complete.

[1] Remember how BPP is defined, and compare.

Exercise 3. *Let us have fun with definitions...*

1. Show that in the definition of BPP, the constant $2/3$ can be replaced by $f(|x|)$ where f is any function verifying $1/2 + n^{-c} \leq f(n) \leq 1 - 2^{-n^d}$ with $c, d > 0$.
2. Do those bounds still hold in the case of RP?
3. Let $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$. Show that ZPP is the class of languages s.t. there exists a polytime PTM which gives than right answer with probability at most $1/2$, and answers "I don't know" otherwise. Show that the same class can also be defined with PTM which always give the right answer and which stop in expected polynomial time.
4. Show that $\mathsf{RP} \subseteq \mathsf{NP}$.
5. And $\mathsf{RP} \subseteq \mathsf{P/poly}$?

Exercise 4. *Let's draw!*

Justify everything: