Complexité avancée
TD 9&10

Cristina Sirangelo - LSV, ENS-Cachan

December 3rd, 2014

Exercise 1. PP vs #P A *polynomially balanced relation* is a binary relation R between words of Σ^* for which there exist two polynomials p and q such that :
- if $R(x, y)$ holds then $|y| < p(|x|)$, and
- for all words $x, y \in \Sigma^*$, whether $R(x, y)$ holds can be verified in time $q(|x|)$.

A function $f : \Sigma^* \to \mathbb{N}$ is in the class $\#\mathbf{P}$ if there exists a polynomially balanced relation R over words of Σ^* such that for all $x \in \Sigma^*$,

$$f(x) = |\ \{y \mid R(x, y)\}\ |$$

1. Prove that a function $f : \Sigma^* \to \mathbb{N}$ is in the class $\#\mathbf{P}$ iff there exists a non-deterministic polynomial time Turing machine M such that for all $x \in \Sigma^*$

$$f(x) = |\ \{\rho \mid \rho \text{ is an accepting run of } M \text{ on input } x\}\ |$$

2. Prove that a function $f : \Sigma^* \to \mathbb{N}$ is in the class $\#\mathbf{P}$ iff there exists a probabilistic Turing machine M running in time $t(n)$ and having random tape of size $t(n)$, for some polynomial t, such that for all $x \in \Sigma^*$

$$f(x) = |\ \{r \text{ of size } t(n) \mid M(x, r) \text{ accepts }\}\ |$$

3. Oracle machines with a function oracle $f : \Sigma^* \to \mathbb{N}$ are defined in the same way as usual oracle machines with language oracles, except that the oracle returns its output $f(x)$ in binary on a dedicated tape (as opposed to just checking membership in a language).

   Recall from TD 8 that **PP** is the class of languages L for which there exists a polynomial time probabilistic Turing machine M such that :

   if $x \in L$ then $Pr[M(x, r) \text{ accepts }] \geq \frac{1}{2}$
   if $x \notin L$ then $Pr[M(x, r) \text{ accepts }] < \frac{1}{2}$

   Prove that $\mathbf{P}^{\mathbf{PP}} = \mathbf{P}^{\#\mathbf{P}}$.

Exercise 2. 2SAT and RP Let φ be a 2CNF formula and let ρ_0 be an arbitrary assignment of variables of φ. Consider the following randomized algorithm for 2SAT on input φ :

$\rho \leftarrow \rho_0$;
repeat r times
    if ρ satisfies all clauses of φ **accept** (φ is satisfiable) ;
    otherwise let $C = L_1 \vee L_2$ be the first clause of φ which is false under ρ ;
    pick one of the two literals at random (with probability $\frac{1}{2}$ each) ;
    flip the truth value of the corresponding variable in ρ (so that C is true) ;
end repeat
reject ; (φ is probably not satisfiable)

Find a value of r such that the above is an **RP** algorithm for 2SAT.

Exercise 3. Polynomial identity An n-variable *algebraic circuit* is a directed acyclic graph having exactly one node with out-degree zero, and exactly n nodes with in-degree zero. The latter are called *sources*, and are labelled by variables $x_1, \ldots x_n$; the former is called the *output* of the circuit. Moreover each non-source node is labelled by an operator in the set $\{+, -, \times\}$, and has in-degree two.

An algebraic circuit defines a function from $\mathbb{Z}^n$ to $\mathbb{Z}$, associating to each integer assignment of the sources the value of the output node, computed through the circuit. It is easy to show that this function can be described by a polynomial in the variables $x_1, \ldots x_n$. Algebraic circuits are indeed a form of implicit representation of multivariate polynomials. Nevertheless algebraic circuits are more compact than polynomials.

An algebraic circuit C is said to be *identically zero* if it evaluates to zero for all possible integer assignments of the sources.

The **Polynomial identity** problem is as follows :

INPUT : An algebraic circuit C
QUESTION : is C identically zero ?

Show that **Polynomial identity** is in **coRP** (note that it is not known whether Polynomial identity is in **P**).

Hint : you may need the following known facts :

Fact (Schwartz-Zippel lemma) If $p(x_1, \ldots x_n)$ is a nonzero polynomial with coefficients in $\mathbb{Z}$ and total degree at most d, and $S \subseteq \mathbb{Z}$, then the number of roots of p belonging to S^n is at most $d \cdot |S|^{n-1}$.

Fact (Prime number theorem) There exists a known integer $X_0 \geq 0$ such that, for all integers $X \geq X_0$, the number of prime numbers in the set $[1..2^X]$ is at least $\frac{2^X}{X}$.

Exercise 4. BPP and oracle machines. Prove that $\mathbf{P}^{\mathbf{BPP}} = \mathbf{BPP}$.

Exercise 5. Arthur-Merlin protocols. Prove the following statements, directly from definition of Arthur-Merlin games :

- $\mathbf{M} = \mathbf{NP}$;
- $\mathbf{A} = \mathbf{BPP}$;
- $\mathbf{NP}^{\mathbf{BPP}} \subseteq \mathbf{MA}$;
- $\mathbf{AM} \subseteq \mathbf{BPP}^{\mathbf{NP}}$.

Exercise 6. Prove that if $\mathbf{NP} \subseteq \mathbf{BPP}$ then $\mathbf{AM} = \mathbf{MA}$.