Complexité avancée - TD 10

Benjamin Bordais

December 16, 2020

Exercise 1 A little come back to P and RP

We define a random language A by setting that each word $x \in \{0,1\}^*$ is in A with probability $1/2$. Show that almost surely (on the probabilistic choice on the language A) we have $\mathsf{P}^A = \mathsf{RP}^A$.

Hint: *Fix an $\epsilon > 0$ and an enumeration $(M_i)_{i \in \mathbb{N}}$ of probabilistic Turing machine running in polynomial time with an oracle. Exhibit deterministic polynomial time Turing machines $(N_i)_{i \in \mathbb{N}}$ such that the probability (over the random language considered) that there is one i such that M_i and N_i do not coincide is lower than $C \cdot \epsilon$ for a constant C. You may use the language A as a random bit generator.*

Exercise 2 Multi-Prover Protocol

Definition 1 *Let $P_1, \dots, P_k$ be infinitely powerful machines whose output is polynomially bounded. Let V be a probabilistic polynomial-time machine. V is called the* verifier*, and $P_1, \dots, P_k$ are called the* provers*.*

A round of a multi-prover interactive protocol on input x consists of an exchange of messages (i.e. words over a given alphabet) between the verifier and the provers, and works as follows:

- *The verifier V is executed on an input consisting of x, the history of all previous messages exchanged with all provers (both sent and received messages), and a random tape content of size polynomial in $|x|$. The output of the verifier is computed in time polynomial in $|x|$, and consists of messages to some or all of the provers.*
- *Each message q_i sent from the verifier to prover P_i is followed by an answer a_i, of size polynomial in $|x|$, sent from the prover P_i to the verifier. The answer a_i is computed by P_i on input consisting of x and the history of all messages previously exchanged between the verifier and the prover P_i (and only P_i).*
- *Alternatively the verifier may decide not to produce messages, and terminates the protocol by either accepting or rejecting, based on the input x and the history of all previous messages exchanged with all provers.*

You can view the protocol as executed by the verifier sharing communication tapes with each P_i, where different provers P_i and P_j (for $i \neq j$) have no tapes they can both access, besides the input tape. In a round the verifier stores each message q_i to prover P_i on the i-th communication tape, shared between the prover and P_i. The answer of P_i is put on tape i as well. The verifier has access to the input and all communication tapes, while each prover P_i has access only to the input and tape i.

$P_1, \ldots, P_k$ and V form a multi-prover interactive protocol *for a language L if the execution of the protocol between V and $P_1, \ldots P_k$ terminates after a polynomial number of rounds (in the size of the input x) and:*

- *if $x \in L$, then $Pr[(V, P_1, \ldots, P_k)$ accepts $x] > 1 - 2^{-n}$;*
- *if $x \notin L$, then for all provers $P'_1, \ldots, P'_k$, $\quad Pr[(V, P'_1, \ldots, P'_k)$ accepts $x] < 2^{-n}$;*

where q is a polynomial and the probability is computed over all possible random choices of V.

In this case, we denote $L \in \mathsf{MIP}_k$. The number of provers k need not be fixed and may be a polynomial in the size of the input x. We say that $L \in \mathsf{MIP}$ if $L \in \mathsf{MIP}_{p(n)}$ for some polynomial p. Clearly $\mathsf{MIP}_1 = \mathsf{IP} = \mathsf{PSPACE}$ (as you will see in the lecture), but allowing more provers makes the interactive protocol model potentially more powerful.

1. Let M be a probabilistic polynomial-time Turing machine with access to an oracle. A language L is accepted by M iff:
   - if $x \in L$, then there exists an oracle O s.t. M^O accepts x with probability greater than $1 - 2^{-n}$;
   - if $x \notin L$, then for any oracle O', $M^{O'}$ accepts x with probability lower than 2^{-n}.

   Show that $L \in \mathsf{MIP}$ if and only if L is accepted by a probabilistic polynomial time oracle machine.

2. Show that $\mathsf{MIP} = \mathsf{MIP}_2$ (assuming we can use error-reduction).

3. Show that $\mathsf{MIP} \subseteq \mathsf{NEXP}$ (this is, in fact, an equality. It can be shown by using the same kind of idea (but more involved) that was used to prove that $\mathsf{IP} = \mathsf{PSPACE}$).

Exercise 3 Polynomial Identity Testing

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.

This can be seen with an array $(s_1, \ldots, s_n, g_1, \ldots, g_m)$ (the number of nodes), with first the n sources and then the m internal nodes (or gates) where an input of a gate g_i can either be a source s_j or another gate g_k with $k < i$.

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

- Ouput: C is identically zero

1. Show that if the variables x may range from 0 to $X \in \mathbb{N}$, then the maximum (absolute) value of a cricuit with m internal gates is X^{2^m} and show that this maximum value can achieved (this justifies the sentence "Algebraic circuits are more compact than polynomials").

2. 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 statements

- **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 $d \cdot |S|^{n-1}$.

- **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 $\frac{2^X}{X}$.