Complexité avancée - TD 11

Benjamin Bordais

January 6, 2021

Definition 1 (Probabilitically Checkable Proofs (PCP)) *A Turing machine with direct access is a Turing machine with:*

- *a special state, called the* reading state*,*
- *a reading oracle,*
- *two special working tapes, called the* direct access tape*, and the* address tape*.*

The machine never reads directly the content of the direct access tape (in the sense that the normal transitions of the machine are independent of the content of the direct access tape). This tape is only accessed via the reading oracle in the following way: when the machine goes in the reading state, the content of the address tape is interpreted as the binary representation of a position i of the direct access tape. The reading oracle then provides in one step, the symbol in position i of the direct access tape. (You can assume this symbol is stored in the control state, or in a special output tape of the reading oracle.)

A $\mathsf{PCP}(R(n), Q(n), T(n))$-verifier *is a probabilistic Turing machine with direct access to a tape called the* proof tape *over alphabet* $\{0,1\}$*. On input x of size n and proof tape content π, the machine uses $R(n)$ random bits and works in the following three phases:*

1. *It first computes $Q(n)$ positions $p_1, \dots p_{Q(n)}$ (in binary) in polynomial time in n, and with no calls to the reading oracle (i.e. these positions are only a function of x and the random tape content).*
2. *Then it makes $Q(n)$ calls to the reading oracle, to retrieve the symbols of the proof tape π in positions $p_1, \dots p_{Q(n)}$.*
3. *Finally, it computes a boolean value (either accept or reject) in time $T(n)$ and with no calls to the reading oracle (i.e. the answer computed in this phase is only a function of x, the random tape content, and the symbols $\pi[p_1], \dots \pi[p_{Q(n)}]$).*

The class $\mathsf{PCP}(R(n), Q(n), T(n))$ *is the set of languages L such that there exists a* $\mathsf{PCP}(R(n), Q(n), T(n))$*-verifier V such that:*

- *if $x \in L$, there exists a proof $\pi \in \{0,1\}^*$ such that $Pr_r[V(x, \pi, r)$ rejects $] = 0$;*
- *if $x \notin L$, then for all $\pi \in \{0,1\}^*$ $Pr_r[V(x, \pi, r)$ accepts $] \leq 1/2$.*

Where the probability is computed over all random tape contents r of size $R(n)$.

Exercise 1 PCP witnessing

Let $\mathsf{PCP}'(k \cdot \log\ n, Q(n), T(n))$ be defined as $\mathsf{PCP}(k \cdot \log\ n, Q(n), T(n))$ except that only proofs π of size $n^k \cdot Q(n)$ are considered, and addresses computed by the verifier have $\log(n^k \cdot Q(n))$ bits. Prove that $\mathsf{PCP}(k \cdot \log\ n, Q(n), T(n)) = \mathsf{PCP}'(k \cdot \log\ n, Q(n), T(n))$.

Exercise 2 PCP and non-deterministic classes

Prove that, with $R(n) = \Omega(log\ n)$, we have $\mathsf{PCP}(R(n), Q(n), T(n)) \subseteq \mathbf{NTIME}(2^{O(R(n))} \cdot Q(n) \cdot (T(n) + poly(n)))$.

Exercise 3 Known classes

Prove the following statements:

$$\bigcup_{c\in\mathbb{N},\ T(n) \text{ a polynomial}} \mathsf{PCP}(0, c \cdot \log\ n, T(n)) = \mathsf{P}$$

$$\bigcup_{R(n),\ T(n) \text{ polynomials}} \mathsf{PCP}(R(n), 0, T(n)) = \mathsf{coRP}$$

$$\bigcup_{Q(n),\ T(n) \text{ polynomials}} \mathsf{PCP}(0, Q(n), T(n)) = \mathsf{NP}$$

(In fact $\bigcup_{T(n) \text{ a polynomial}} \mathsf{PCP}(O(\log n), O(1), T(n)) = \mathsf{NP}$ (this is known as the PCP theorem).)

Exercise 4 Graph non-ismorphism

Show that $\overline{\mathbf{ISO}} \in \mathsf{PCP}(p(n), 1, c)$ for some polynomial p and constant c.

Exercise 5 PCP, MIP and NEXPTIME

Recall the definition of MIP from the previous exercise sheet (where we can assume that the probability of acceptance is equal to 1 when $x \in L$).

Prove that

$$\bigcup_{R(n),Q(n),T(n) \text{ polynomials}} \mathsf{PCP}(R(n), Q(n), T(n)) \subseteq \mathbf{MIP} \subseteq \mathbf{NEXPTIME}$$

(The last inclusion was proved in the previous exercise sheet. In fact, we have an equality.)

Remark. Indeed **MIP** and this version of PCP *coincide* with **NEXPTIME**, but you are not required to prove the opposite inclusions.

Exercise 6 Polynomial Identity Testing

This was already given in the previous exercise sheet.

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

Exercise 7 A general note on self-reducibility

Define a language L to be *downward-self-reducible* if there is a polynomial-time Turing Machine R such that for any x of length n, $R^{L_{n-1}}(x) = L(x)$, where L_k denotes an oracle that decides L on input of size at most k. Prove that if L is such a language, then $L \in$ PSPACE.