Technische Universität München (I7)
Prof. J. Křetínský / Dr. M.Raskin

Summer term 2019
14.05.2019

Solution

Computational Complexity – Homework 6

Discussed on 17.05.2019.

Recall that $L \in \mathbf{RP}$ if there exists a polynomial p and a polynomial-time TM $M(x;u)$ using certificates u of length $p(|x|)$ such that for every $x \in \{0,1\}^*$

$$x \in L \Rightarrow Pr[A_{M;x} \geq 3/4 \text{ and } x \notin L \Rightarrow Pr[A_{M;x}] = 0$$

Further $\mathbf{co-RP} = \{\bar{L} \mid L \in \mathbf{RP}\}$ and $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{co-RP}$.

Exercise 6.1

(a) Show that **RP** does not change if we replace in the definition $\geq 3/4$ by $\geq n^{-k}$ or $\geq 1 - 2^{-n^k}$ (with $k > 0$).

(b) Let $L \in \mathbf{NP}$ be decided by a poly-time TM $M(x,u)$ with certificates u of length $p(|x|)$.

Prove or disprove that $x \in L \Rightarrow \Pr[A_{M,x}] \geq n^{-k}$ needs to hold for some $k > 0$ if a polynomial number $r(|x|)$ of reruns should suffice to reduce the probability of false negatives below any given bound $c \in (0,1)$.

Remark: Use that $(1 - 1/k)^k \approx e^{-1}$ for large k.

Exercise 6.2

A cut in a connected non-oriented graph is a set of edges such that their removal makes the graph disconnected.

Consider the following problem: given a graph G and an integer k determine whether the graph G has a cut of size at most k.

Prove that this problem is in **RP**.

Solution: Consider the following random algorithm to find a cut. As long as we have at least three vertices we contract a random edge (declare its ends to be the same vertex and remove all the resulting self-loops; there can be multiple edges between the remaining vertices). Once there are only two vertices, we report all the remaining edges between the vertices as a cut.

This procedure always produces a cut. If the minimal cut has k edges, all vertices have degree at least k (otherwise cutting off a single vertices would be a smaller cut) and there are at least $\frac{kn}{2}$ edges. The same holds at each step.

The probability of not selecting any of the edges in the cut for contraction at the first step is at least $1 - \frac{k}{\frac{kn}{2}} = 1 - \frac{2}{n}$. After each contraction, if we still have all k edges from the minimal cut intact and there are m vertices left, the probability of choosing an edge not from the cut is at least $1\frac{2}{m}$.

The probability to keep all the edges from the cut to the end (and selecting the minimal cut) is at least $\prod_{i=3}^{n}(1 - \frac{2}{i}) = \frac{1}{3}\frac{2}{4}\frac{3}{5}\cdots = \frac{2}{n)(n-1)}$.

We can use amplification to obtain the desired probability of success.

Exercise 6.3

Prove that verifying matrix multiplication (given matrices A, B, C check $AB = C$) is in **coRP**. Show that the verifying algorithm can be made quadratic (for a constant error probability).

Solution: Select a uniformly random vector r with values 0 and 1. If $AB = C$, then $ABr = Cr$. The latter condition can be verified in quadratic time. Let us see why the error will be detected with probability at least $\frac{1}{2}$. (If there is no error, we will always accept).

An equivalent form of the condition is $(AB - C)r = 0$. If $(AB - C)$ contains a nonzero entry at position (i, j), changing j-th coordinate of r changes $(AB - C)r$, and therefore for eavery choice of other coordinates at least one choice of the j-th coordinate leads to the error being discovered.

Exercise 6.4

Show that $L \in \mathbf{ZPP}$ if and only if L is decided by some PTM in expected polynomial time.

Exercise 6.5

For a given $c > 0$ let a language L be in $\mathbf{PP}_{\geq c}$ if $x \in L \Leftrightarrow \Pr[A_{M,x}] \geq c$. Similarly, the class $\mathbf{PP}_{>c}$ is defined.

Show that

(a) $\mathbf{PP}_{>1/2} = \mathbf{PP}_{\geq 1/2}$.

(b) $\mathbf{PP}_{>1/2}$ is closed under complement and symmetric difference.

Remark: The symmetric difference $A\Delta B$ of two sets A, B is defined by $A\Delta B := (A \setminus B) \cup (B \setminus A)$.

(c) MajSat is $\mathbf{PP}_{>1/2}$-complete.

Remark: MajSat is the following problem: Given a Boolean expression with n variables, is it true that the majority of the 2^n truth assignments to its variables, i.e., at least $2^{n-1} + 1$ of them, satisfy it?

*(d) $\mathbf{PP}_{\geq 3/4} = \mathbf{PP}_{\geq 1/2}$.