Foundations of Interactive Proofs
Tutorial 1 – Wednesday, December 17

Recall that BPP_α is the class of languages $\mathcal{L}$ for which there is a probabilistic polynomial-time Turing machine M such that:

- If $x \in \mathcal{L}$, $\Pr[M(x) = 1] \geq \alpha(|x|)$, and
- If $x \notin \mathcal{L}$, $\Pr[M(x) = 0] \geq \alpha(|x|)$

In class, we defined $\mathsf{BPP} := \mathsf{BPP}_{2/3}$

Warm-up

Question 0. Show that $\mathsf{NP} \subseteq \mathsf{EXP} = \cup_{c>1}\mathsf{DTIME}(2^{n^c})$.

Randomized complexity

Question 1. Show that for any polynomial p, $\mathsf{BPP} = \mathsf{BPP}_{1/2+1/p(|x|)}$.

Question 2. Show that $\mathsf{BPP} = \mathsf{BPP}_{1-2^{-|x|^2}}$.

Question 3 (hard). Recall that $\mathsf{AM}[k]$ is the class of languages $\mathcal{L}$ that admit a public coin $k(|x|)$-round interactive proof system. As for BPP, we denote by $\mathsf{AM}_\alpha[k]$ the class of languages with an $\mathsf{AM}[k]$ protocol with completeness and soundness error bounded by $\alpha(|x|)$. Again, using the latter notation, in class, we defined $\mathsf{AM} = \mathsf{AM}_{2/3}$. Show that for any polynomial k,

$$\mathsf{AM}[k] = \mathsf{AM}_{1-2^{-|x|^2}}[k]$$

Hint: use the protocol tree representation, associate a valuation to each node corresponding to the probability of acceptance using an optimal prover strategy. Formulate the goal over such trees, and proceed by induction over the nodes.

Non-uniform complexity

Question 4. Show that $\mathsf{P}/1$ contains undecidable languages.
Hint: use an uncomputable function $f : \mathbb{N} \to \{0, 1\}$, and define $f' : x \mapsto f(|x|)$. Use this to build an undecidable set S where $x \in S$ iff $1^{|x|} \in S$.

Question 5. Show that $\mathsf{BPP} \subset \mathsf{P/poly}$.
Hint: use a characterization of BPP with acceptance and rejection exponentially close to 1, and use an averaging argument to find a random coin that works correctly on all inputs.

Space complexity

Question 6. Show that $\mathsf{DTIME}(s(n)) \subseteq \mathsf{SPACE}(s(n)) \subseteq \mathsf{DTIME}(2^{O(s(n))})$ and $\mathsf{NP} \subseteq \mathsf{PSPACE}$.

Question 7. Prove that TQBF is in PSPACE.
Hint: proceed by recursion on the number of variables in φ. Peel off variables by setting them to 0 or 1, and evaluate an AND or an OR depending on the quantifier. Reuse the same space for evaluating both branches.

Question 8 (hard). Prove that TQBF is PSPACE-complete.
Hint: fix a language L and write the configuration graph of the machine M deciding L in space $s(n)$. Reduce the acceptance problem to finding out whether a directed path from a start node to an end node exists in the graph. Write the task of checking for an edge as a CNF. Build a QBF that is true iff a path exist.

Tutorial 2 – Space Complexity

Question 1. Show that $\mathsf{DTIME}(s(n)) \subseteq \mathsf{SPACE}(s(n)) \subseteq \mathsf{DTIME}(2^{O(s(n))})$ and $\mathsf{NP} \subseteq \mathsf{PSPACE}$.

Question 2. Prove that TQBF is in PSPACE.
Hint: proceed by recursion on the number of variables in φ. Peel off variables by setting them to 0 or 1, and evaluate an AND or an OR depending on the quantifier. Reuse the same space for evaluating both branches.

Question 3 (hard). Prove that TQBF is PSPACE-complete.
Hint: write the configuration graph $G_{M,x}$ of a Turing machine M on input x (definition given in class).

■ **Question 3.1.** Assume that M is an $s(n)$-space TM. Prove that $G_{M,x}$ has at most $2^{c \cdot s(n)}$ nodes (c is a constant).

■ **Question 3.2.** Assume that there exists an $O(s(n))$-size CNF $\phi_{M,x}$ such that for all C, C', $\phi_{M,x}(C, C') = 1$ iff C and C' are neighbors in $G_{M,x}$ (this follows by Cook-Levin). Formulate the goal: what QBF ψ are we trying to construct? What should this QBF verify?

■ **Question 3.3.** define intermediate QBF with two unquantified inputs (by their property – we will construct them afterwards) $\psi_i(C, C')$ such that $\psi = \psi_{c \cdot s(n)}(C_{\mathsf{start}}, C_{\mathsf{end}})$. Formulate the induction hypothesis.

■ **Question 3.4.** Prove the induction hypothesis.
Hint: write a QBF for $\psi_i(C, C')$ assuming a QBF for $\psi_{i-1}(C_0, C_1)$ for any (C_0, C_1). Make sure to avoid an exponential blowup!

Question 4. How would you extend the approach above to $\mathsf{NPSPACE}$? Conclude.