Schedule A2, (Computer Science, CS and Philosophy, Maths and CS)
Hilary Term 2023

Computational Complexity

Exercise class 6: circuit complexity, BPP, RP

1. Prove that the complexity classes BPP and RP are closed under union. That is, for languages $\mathcal{L}_1$ and $\mathcal{L}_2$ in BPP, $\mathcal{L}_1 \cup \mathcal{L}_2$ is also in BPP, and similarly for RP.

2. Recall the definition of the complexity class P/poly: A language $\mathcal{L}$ over the binary alphabet belongs to P/poly if there exists a sequence of boolean circuits $C_1, C_2, \ldots$ where C_i has i inputs, is of size polynomial in i, and for all natural numbers i, C_i accepts words in $\mathcal{L}$ of length i (and does not accept words not in $\mathcal{L}$).

   Prove that the complexity class BPP is a subset of P/poly. You may like to start by proving RP$\subseteq$P/poly.

3. A 3-Horn-formula is a propositional logic formula of the form $\phi := \bigwedge_{i=1}^{n} C_i$, where $C_i := \bigvee_{j=1}^{n_i}$ is a clause with at most 3 literals (i.e. $n_i \leq 3$) of which at most one is positive.

   The problem 3-Horn-Sat is defined as the problem, given a 3-Horn formula ϕ, to decide if ϕ is satisfiable.

   Show that 3-Horn-Sat is P-complete (under LOGSPACE reductions). To prove hardness, use the fact that Monotone-CVP is P-complete.

4. Show that BPP and RP are closed under polynomial-time reductions in the sense that if $P \leq_p Q$ and $Q \in$ BPP (or RP) then $P \in$ BPP (or RP).

5. The aim of this question is to show that if NP $\subseteq$ BPP then NP=RP. We pursue this question in several steps.

   (a) Show that if there is a (deterministic) polynomial-time algorithm for deciding whether a SAT-instance is satisfiable then there is also a (deterministic) polynomial-time algorithm for computing a satisfying assignment.

   (b) Show that the same is true for BPP algorithms. That is, if there is a bounded error polynomial time algorithm for deciding whether an instance to SAT is satisfiable then there is also such an algorithm which constructs a satisfying assignment with bounded error probability.

   Hint. Use probability amplification.

   (c) Show that if NP $\subseteq$ BPP then NP $\subseteq$ RP.

   (d) Show that RP $\subseteq$ NP.