

Problem 1 (*Properties of probabilistic Computation*)

Prove the following statements.

- $ZPP = RP \cap \text{co-RP}$.
- $BPP^{BPP} = BPP$.

Problem 2 (*Probabilistic algorithms for SAT*)

Show that if SAT is in **BPP**, then there is a probabilistic polynomial time algorithm that given a satisfiable CNF formula as input produces a satisfying assignment with probability at least $1/2$.

Next, show that $NP \subseteq BPP$ implies that $NP = RP$.

Problem 3 (*Approximation method over the reals*)

Let y_1, \dots, y_m be Boolean variables. Denote by y the vector (y_1, \dots, y_m) . Let $k = \log_2(m) + 1$ and $S_0 = \{1, \dots, m\}$. For $i = 0, \dots, k-1$, define S_{i+1} to be the set obtained from S_i by including every element of S_i with probability $1/2$.

Define real valued polynomials $P_i(y) = \sum_{j \in S_i} y_j$, for $i = 0, \dots, k$ and let $P(y) = 1 - \prod_{i=0}^k (1 - P_i(y))$.

Let $y \neq 0$ be fixed and prove the following statements.

- $\Pr[P_i(y) > 1 \text{ for all } i] \leq 1/2$.
- Conclude that $\Pr[P_0(y) = 1 \vee (\exists i : P_{i+1}(y) \leq 1 \wedge P_i(y) > 1)] \geq 1/2$.
- $\Pr[P_{i+1}(y) = 0] = 2^{-P_i(y)}$.
- $\Pr[P_{i+1}(y) = 1] = P_i(y)2^{-P_i(y)}$.
- $\Pr[P_{i+1}(y) = 1 \mid P_{i+1}(y) \leq 1 \wedge P_i(y) > 1] = P_i(y)/(P_i(y) + 1) \geq 2/3$.
- Conclude that $\Pr[\exists i : P_i(y) = 1] \geq 1/3$ and hence $\Pr[P(y) = 1] \geq 1/3$.

Finally, prove the following results.

Proposition 1 Let t be a positive integer and let y_1, \dots, y_m be Boolean variables. Then there is a family of real valued polynomials P of degree at most $t \cdot (\log_2(m) + 2)$ such that for all fixed $y \in \{0, 1\}^m$

$$\Pr[P(y) = \text{OR}(y)] \geq 1 - (2/3)^t .$$

Theorem 2 Let C be a depth d circuit with AND and OR gates of size S . Then there is a real valued probabilistic polynomials P of degree at most $(t \cdot (\log_2(S) + 2))^d$ and a set $T \subseteq \{0, 1\}^n$ of size at least $(1 - S(2/3)^t)2^n$ such that for all $x \in T$ we have $P(x) = C(x)$.

Problem 4 Define the class \mathbf{MA} to be the class of languages L having an interactive proof system as follows. The only communication is a single message from the prover (Merlin) to the probabilistic polynomial time verifier (Arthur). If $x \in L$ then Arthur accepts with probability 1. If $x \notin L$ then Arthur accepts with probability at most $1/2$.

Prove that $\mathbf{BPP} \subseteq \mathbf{MA}$. (Hint: Use the technique of the proof showing that $\mathbf{BPP} \subseteq \Sigma_2^p$.)

Give a definition of a version of \mathbf{MA} with two sided error \mathbf{MA}_2 , and extend the proof of $\mathbf{BPP} \subseteq \mathbf{MA}$ to show that in fact $\mathbf{MA}_2 \subseteq \mathbf{MA}$.

Problem 5 (Bonus Problem)

Use the results of Problem 3 to derive another proof of the result that \mathbf{AC}^0 circuits require exponential size to compute the parity function. You may find the following steps useful.

- Let $E \subseteq \{0, 1\}^n$ such that $|E| \leq \sum_{i=0}^k \binom{n}{i}$. Then there is a nonzero and positive polynomial $Q(x)$ of degree at most $2k$ such that $Q(x) = 0$ for all $x \in E$.
- Let $R(x)$ be a multilinear polynomial of degree k . Then there is a univariate polynomial R' of degree at most k such that $R'(x_1 + \dots + x_n) = \sum_{\pi \in S_n} R(x_{\pi(1)}, \dots, x_{\pi(n)})$ for all x .