Problem 1: Non-binary coins

Our definition of PTM gives the machine the possibility to pick random bits (i.e., do something with probability 1/2. But what if we want to do something with a different probability, say, 1/3? The definition of PTM should not depend on what kind of random numbers we use!

(a) Show that there is a polynomial-time PTM that, given input $x$ outputs 1 with probability $1/3 \pm 2^{-|x|}$ (but not more or less).

Note: This gives us a subroutine that we can use to simulate 1/3-random bits with high enough precision not to influence the overall output distribution of the PTM too much.

(b) Show that there is not polynomial-time PTM that, given input $n$, outputs 1 with probability exactly 1/3.

Hint: You can assume that the PTM runs exactly $T(n)$ steps for some function $T$ (i.e., the runtime does not depend on the random choices). Let $R$ be the number of random choices that lead to output 1. Show that the probability of output 1 is a fraction whose denominator is a power of two.

Problem 2: Amplification

We have defined the class $\text{BPP}$ as the set of all languages that can be solved in probabilistic polynomial time with probability at least 2/3. We have seen that the arbitrary number 2/3 does not matter much: if we can decide $L$ in probabilistic polynomial time with probability 2/3, then we can decide $L$ in probabilistic polynomial time with probability $\alpha$ for any constant $\alpha < 1$.

We showed this by simply constructing a new algorithm $\hat{M}$ that runs the original algorithm $M$ $t$ times (for suitable $t$), and then outputs the most common output.

A search problem is a relation $S$ between bitstrings (i.e., $S$ is a set of pairs $(x,y)$ where $y$ is a solution for $x$). We say we can “solve $S$ in probabilistic polynomial time with probability $\alpha$” iff there is a PTM $M$ such that for all $x$, $\Pr[(x,y) \in R : y \leftarrow M(x)] \geq \alpha$.

Is amplification also possible for search problems? That is, is the following fact true?

---

For simplicity, we consider only search problems where every $x$ has a solution.
Lemma 1 (Wrong!) If we can solve a search problem $S$ in probabilistic polynomial time with probability $2/3$, then we can solve $S$ in probabilistic polynomial time with probability $\alpha$.

We will consider the prime search problem. Given $N$, the problem is to find a prime $p \in [N, 2N]$. Assume that we have a PTM $M_{\text{prime}}$ that solves the prime search problem with probability $2/3$.

(a) Show that amplification by majority decision does not work for constructing a PTM $M_{\text{prime}}$ that solves the prime search problem in probabilistic polynomial time with probability, say, $3/4$.

(b) Show how to solve the prime search problem probabilistic polynomial time with probability $3/4$ using $M_{\text{prime}}$.

Note: Here you may use the fact that it can be decided in deterministic polynomial time whether a given number is a prime.

(c) (Bonus points) Show that Lemma 1 is not true.

Hint: That is, you should show that there is a search problem that can be solved in probabilistic polynomial time with probability $2/3$, but not with probability, say, $3/4$. For example, you could use a random search problem $S$ where for each $x$, a bitstring $y$ is a solution with probability $0.7$.

Note: A complete proof will be quite elaborate. A proof sketch is sufficient.