Problem Set #1

CMSC 858L
Instructor: Daniel Gottesman

Due on Gradescope Feb. 16, 2023, noon

The late deadline to turn the problem set in without penalty is Feb. 19, 2023, noon.

Problem #1. Different error cutoffs (50 pts.)

Define BPP_ϵ the same way as BPP, but with an error cutoff of $1/2 + \epsilon$ instead of $2/3$. That is, for BPP_ϵ,

1. If $x \in L$, then $\mathrm{Prob}(A(x) = 1) \geq 1/2 + \epsilon$.
2. If $x \notin L$, then $\mathrm{Prob}(A(x) = 0) \geq 1/2 + \epsilon$.

In this problem, we will consider ϵ to be a function of $|x|$, although in part a, it is a constant function.

Results in this problem should be unconditional (that is, not depending on additional complexity-theoretic assumptions, such as the assumption that P = BPP.

Hint: For parts of this problem, you may want to consider that a randomized algorithm can be thought of as a deterministic algorithm that reads from a pre-determined string of uniformly random bits as well as from its usual input.

You may also want to use some statistical tail bounds. If you are not very familiar with these, let me suggest Hoeffding's inequality: When $X_1, \ldots, X_n$ are independent random variables with values in the interval $[a, b]$, let X be their sum and let μ be the mean value of X. Then $\forall\, \delta > 0$,

$$\mathrm{Prob}(X \geq (1+\delta)\mu) < \exp\left(-\frac{2\delta^2\mu^2}{n(a-b)^2}\right) \tag{1}$$

a) (10 pts.) Prove that for any constant ϵ, $0 < \epsilon < 1/2$, $\mathrm{BPP}_\epsilon = \mathrm{BPP}$.

b) (10 pts.) Prove that if $\epsilon = 1/f(|x|)$, with $f(|x|) = O(\mathrm{poly}(|x|))$, then $\mathrm{BPP}_\epsilon = \mathrm{BPP}$.

c) (15 pts.) Prove that if $\epsilon = 2^{-|x|}$, then $\mathrm{BPP}_\epsilon \subseteq \mathrm{PSPACE}$.

d) (15 pts.) Find a value for ϵ (which again will be a function of $|x|$) such that you can prove that $\mathrm{BPP}_\epsilon = \mathrm{P}$.

Problem #2. Variations of BQP(50 pts.)

The purpose of this problem is to study variations in the definition of BQP. In order to avoid having to deal with Turing machines, we will instead consider the circuits for BQP to be given as the output of another circuit.

In this problem "with no input" means that the circuit starts with all bits or qubits in a standard state (typically 0 or $|0\rangle$).

Let G_n^c be a family of classical circuits of size $O(\mathrm{poly}(n))$ with no input that outputs a family of quantum circuits Q_n^c that take an input x and output a single bit (after measurement) with outcome 1 with probability P_x^c. Let S^c be the set of quantum circuit families that can be generated in this way.

Note that since the circuit G_n^c has polynomial size, the output circuit Q_n^c must as well.

a) (25 pts.) Let G_n^q be a family of *quantum* circuits of size $O(\text{poly}(n))$ with no input that outputs a family of quantum circuits Q_n^q that take an input x and output a single bit (after measurement) with outcome 1 with probability P_x^q. Show that for any such family Q_n^q, there exists a quantum circuit family in S^c with $P_x^c = P_x^q$.

   Note: This fact is the main idea in showing that if you define BQP by referring to circuits generated uniformly by a *quantum* Turing machine rather than a classical Turing machine, the class doesn't change.

b) (25 pts.) Let $G_n^0(x)$ be a family of classical circuits of size $O(\text{poly}(n))$ with input x such that $|x| = n$ and that output a quantum circuit Q_x^0 that depends on x but takes no input. The circuit Q_x^0 outputs a single bit with outcome 1 with probability P_x^0. Show that the set of probability distributions P_x^0 that can be generated this way is the same as the set of probability distributions P_x^c that are the outcome probabilities for some quantum circuit family in S^c.

   Note: The point here is that we have a choice between defining BQP circuits as taking a classical input for the instance and defining the class to consist of quantum circuits with no input but that are designed with the specific instance in mind. In either case, we get the same complexity class.