TUTORIAL 5

This tutorial contains **bonus** questions. Those question should be worked on **if and only if** the rest of the sheet has been completed.

1 BPP

Definition 1.1. *Let $F : \{0,1\}^* \mapsto \{0,1\}$. F is said to be in $\mathbf{BPP}$ if there exist a polynomial time algorithm such that on input 1^n outputs a classical circuit C_n with input $x \in \{0,1\}^n, r \in \{0,1\}^{p(n)}$ for $p(n)$ a polynomial, such that for all $n > 0,\ x \in \{0,1\}^n, \Pr_r(C_n(x,r) = F(x)) \geq 2/3$, where the probability is taken over the uniform choice of r.*

You can think as C_n as a probabilistic algorithm making a polynomial number of bit flips, the first bitflip outcome being r_1, the second outcome is r_2, etc...

You can freely use the following proposition:

Proposition 1.2 (Chernoff Bound)**.** *Let $X_1, \ldots, X_n$ iid random variables with values in $\{0,1\}$. Let $Z = X_1 + \ldots + X_n$ and let $\mu = \mathrm{E}(Z)$, then for any $1 > \delta > 0$,*

$$\Pr(|Z - \mu| > \delta\mu) < 2 \cdot \exp\left(-\delta^2\mu/3\right)$$

1. Propose a problem solved more efficiently with bounded error than with zero error. *Hint: think about the previous tutorials...*
2. Show that $\mathbf{P} \subseteq \mathbf{BPP}$.
3. Let $\mathbf{BPP}'$ be defined as $\mathbf{BPP}$, with $\Pr(C_n(x,r) = F(x)) \geq 1 - e^{-n^c}$ for $c > 0$ and n the size of the input, instead of $\Pr(C_n(x,r) = F(x)) \geq 2/3$. Show that $\mathbf{BPP}' = \mathbf{BPP}$.
4. Does the same proof works for $1 - e^{-2^n}$? Why?
5. (Bonus, Hard) Let $\mathbf{P/poly}$ be the set of functions $F : \{0,1\}^* \to \{0,1\}$ such that for any $n > 0$ there exists a classical circuit C_n of polynomial size in n with input $x \in \{0,1\}^n$ such that for all $x \in \{0,1\}^n, C_n(x) = F(x)$. What is the difference between $\mathbf{P/poly}$ and $\mathbf{BPP}$? Show that there exists undecidable functions in $\mathbf{P/poly}$.

2 BQP

Definition 2.1. *Let $F : \{0,1\}^* \mapsto \{0,1\}$. F is said to be in $\mathbf{BQP}$ if there exist a polynomial time algorithm A such that on input 1^n outputs a quantum circuit C_n composed of a polynomial number of gates in the set $\{H, K, K^{-1}, CNOT, TOFFOLI\}$, operating on a polynomial number of qubits, such that for all $x \in \{0,1\}^n$, the probability of obtaining $F(x)$ by measuring the first qubit of $C_n \cdot |x\rangle|0^l\rangle$ is $\geq 2/3$.*

1. Prove that $\mathbf{BPP} \subseteq \mathbf{BQP}$.

2. Let $\mathbf{EXP}$ be the set of functions that can be computed in exponential time in the size of their input. We are going to prove that $\mathbf{BQP} \subseteq \mathbf{EXP}$.
   (a) Propose a way to represent a quantum state of n qubits in memory, what amount of memory will you need to represent states during the execution of a circuit of l gates in the set $\{H, K, K^{-1}, CNOT, TOFFOLI\}$?
   (b) Propose an algorithm simulating a quantum circuit, gives its complexity in time and memory. Conclude.

3. Let $\mathbf{PSPACE}$ be the set of functions that can be computed with polynomial memory (but *a priori* unbounded time). We are going to prove that $\mathbf{BQP} \subseteq \mathbf{PSPACE}$.
   (a) Show that $\mathbf{PSPACE} \subseteq \mathbf{EXP}$.
   (b) Let C be a circuit of size m operating on n qubits composed of gates $g_1, g_2, \ldots, g_m$.
   We are going to visualize the evolution of a quantum state in C in the following way:
   The history tree is a complete 2^n-regular tree of depth $m + 1$. Its root is labeled $|x\rangle$ where $x \in \{0, 1\}^n$ is the input of the circuit, and each of the other node are labeled with $|y\rangle$ for $y \in \{0, 1\}^n$ (see Figure 2).
   The weight of the edge $|i\rangle \to |j\rangle$ at level p is defined to be the amplitude of $|j\rangle$ after applying g_p to $|i\rangle$.
      i. Write the history tree of the circuit consisting of H on input $|0\rangle$. Of the circuit $CNOT$ on input $|11\rangle$.
      ii. Write the weight of the edge $|i\rangle \to |j\rangle$ at level p as a function of i, j and g_p.
      iii. Let $x \to u_1 \to \cdots \to u_m$ be a path in the history tree. The weight of this path is the product of the weights of its edges. Show that the weight of a path can be computed in polynomial time and space, given the circuit description and a path.
      iv. Let $y \in \{0, 1\}^n$. Compute the probability of outputting $|y\rangle$ when measuring $C \cdot |x\rangle$ in terms of the weights of the paths starting with $|x\rangle$ and ending with $|y\rangle$ in the history tree.
      v. Conclude that the probability of C to output 0 on input $|x\rangle$ can be computed with a $\mathbf{PSPACE}$ algorithm.

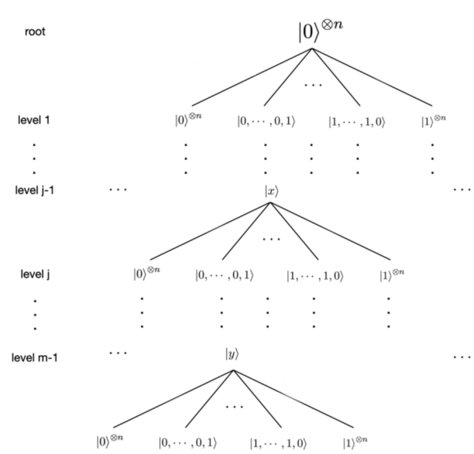

Figure 1: History tree of root $|0^n\rangle$. Source: `https://en.wikipedia.org/wiki/File:Sum_of_histories_tree.png`