1 On the class BQP

The class BQP (Bounded-error Quantum Polynomial time) captures all decision problems that are computable, with high probability, in polynomial time. Since we prefer to use quantum circuits, rather than quantum Turing Machines, we model polynomial time by polynomial circuit size. That is, a quantum circuit C_n for n-qubit inputs is said to run in polynomial time if it has at most poly(n) gates. To capture algorithms that behave uniformly on all input lengths, we restrict our attention to polynomial-time uniform circuits; that is, families of circuits $\{C_n\}_{n\in\mathbb{N}}$ whose classical description can be generated by a polynomial-time classical Turing machine (put differently, a Turing Machine, that given an integer n, outputs the description of the circuit C_n).

With the above in mind, we are ready to formally define BQP.

Definition 1. *A language L is in the class BQP if there exists a family of polynomial-time uniform circuits $\{C_n\}_{n\in\mathbb{N}}$ of polynomial size, such that on input $x \in \{0,1\}^n$:*

- *if $x \in L$, then $\Pr[C_n(x) = 1] \geq 2/3$, and*
- *if $x \notin L$, then $\Pr[C_n(x) = 0] \geq 2/3$.*

It is important to note that the choice of probability $2/3$ is arbitrary and could have also been any number that is bounded away from above from $1/2$ (i.e., does better, by a constant factor, than a random guess). This is because we can amplify the success probability of a quantum algorithm to $1-\epsilon$ by repeating it $O(\log(1/\epsilon))$ times and ruling according to the majority answer.

To make the above argument precise, we shall need the Chernoff bound.

Claim 1 (Chernoff bound)**.** *Let $A_1, \ldots, A_t$ be independent random variables taking values in $\{0,1\}$. Denote $A = \Sigma_i A_i/t$. Then,*

$$\Pr\left[|A - \mathbb{E}[A]| \geq \delta\right] \leq 2e^{-t\delta^2/2} .$$

Fix input $x \in \{0,1\}^n$. Run $C_n(x)$ (independently) k times. Denote by $A_i(x)$ the output of $C_n(x)$ in its i'th invocation. As before, denote by $A = \Sigma_i A_i/t$ the average value of the algorithm over the t different invocations. Our amplified algorithm rules by majority, i.e., outputs 1 (accepts) if $A > 1/2$.

Now, suppose that $x \in L$. Since our algorithm accepts x with probability at least $2/3$, the average value over the invocations is $\mathbb{E}[A] = 2/3$. By the Chernoff bound,

$$\Pr[|A - 2/3| \geq 1/6] \leq 2e^{-t(1/6)^2/2}] = \exp(-t) .$$

Hence, fixing the number of invocations to $t = O(\log(1/\epsilon))$, the probability of mistake is at most ϵ, as we wanted. The case that $x \notin L$ is completely symmetric.

Finally, a prominent example of a problem in BQP, which is not known to be in P (only in NP and coNP), is the Factor problem, discussed in previous lectures.