BQP/qpoly $\subseteq$ PP/poly

Daniel Tobias

University of California, Davis

January 10, 2023

BQP/qpoly $\subseteq$ PP/poly means that we can simulate a quantum computer with access to quantum advice with a classical machine that has access to short classical advice.

Recall the **Group Non-Membership Problem (GNP)**. Given group G_n and some subgroup $H_n \leq G_n$ is $x \notin H_n$? We start with a quantum advice state

$$|H_n\rangle = \frac{1}{\sqrt{|H_n|}} \sum_{y \in H_n} |y\rangle$$

which can be sent to

$$|xH_n\rangle = \frac{1}{\sqrt{|H_n|}} \sum_{y \in H_n} |xy\rangle$$

Map $|H_n\rangle$ **to** $|xH_n\rangle$ **by**:
$|y\rangle|0\rangle \to |y\rangle|xy\rangle \to |y \oplus x^{-1}xy\rangle|xy\rangle = |0\rangle|xy\rangle$ for each $y \in H_n$.

Next we prepare a state with $\left(|0\rangle|H_n\rangle + |1\rangle|H_n\rangle\right)/\sqrt{2}$, apply Hadamard to the first qubit, and measure it in the computational basis to distinguish the cases $|H_n\rangle = |xH_n\rangle$ (which means $x \in H_n$) and $\langle H_n|xH_n\rangle = 0$ (which means $x \notin H_n$).

After applying the hadamard we're in state

$$\frac{1}{2}\left[(|0\rangle|H_n\rangle + |xH_n\rangle) + |1\rangle(|H_n\rangle - |xH_n\rangle)\right]$$

Notice that if $|H_n\rangle = |xH_n\rangle$ that (ignoring renormalization) this state is really just $|0\rangle|H_n\rangle$ otherwise we'll have a state like $|0\rangle\left(|H_n\rangle + |xH_n\rangle\right) + |1\rangle\left(|H_n\rangle - |xH_n\rangle\right)$. The remaining registers besides the first one don't really matter, since repeated experiments will be enough to tell you if this is a superposition or not, which then tells you the status of $|xH_n\rangle$.

As we saw, the quantum advice $|H_n\rangle$ acts like additional input and does not depend on x, the group element which we're asking about. The advice only depends on size of the input, since by definition G_n is a group whose members can be uniquely labeled by n-bit strings. Advice acts like initializing your quantum computer in a state that is more favorable than just the all $|0\rangle$ state.

PP/poly (probabilistic polynomial time)

The class of decision problems in NP such that if the answer is 'yes' then $\geq 2/3$ of the computation paths accept and if the answer is 'no' then $\leq 1/3$ of the computation paths accept with polynomial sized classical advice.

BQP/qpoly

There exists a polynomial sized quantum circuit with a polynomial sized family of quantum advice states $|\psi_n\rangle$ such that a 'yes' instance accepts with probability $\geq 2/3$ and a 'no' instead accepts with a probability $\leq 2/3$.

Sketch of simulation BQP/qpoly $\subseteq$ PP/poly. For convenience say $L_n(x) = 1$ if the input x is in the language L and 0 otherwise. $L_n(x)$ is computed by a BQP machine with polynomial sized quantum advice. Then all we need is a PP machine that computes $L_n(x)$ using poly sized classical advice.

What is the classical advice? The adviser (who has access to the BQP machine) provides inputs $x_1, ..., x_T$ (where $T \leq O(p(n) \log p(n))$ and $p(n)$ is the length of the quantum advice) along with $L_n(x_1), ..., L_n(x_T)$ which is the "acceptance status" of the input x_t. Notice that this already solves half the puzzle, for if $x \in \{x_1, ..., x_T\}$ then we simply can return $L_n(x)$.

Continued.
If x is not in our list of inputs, we we pick the largest t such that $x_t < x$ (where $<$ is lexicographical ordering) and prepare the maximally mixed state I. We then condition I to I_t by running the quantum algorithm A (the one which decides $L_n(x)$ for input x) on $x_1, ..., x_t$ in this order and postselect on A correctly outputting $L_n(x_1), ..., L_n(x_t)$. If $P_x(\rho)$ is the probability that A outputs 1 with advice state ρ then we will return round$(P_x(I_t))$.

An interesting improvement on the theorem is BQP/qpoly $\subseteq$ QMA/poly meaning we can assume a quantum advice state is simply just a witness state in QMA.

The end!