$\mathrm{QMA}^A \neq \mathrm{QCMA}^A$?

Daniel Tobias

University of California, Davis

November 22, 2022

Last week in Sanchyan's talk: definitions of QMA and QCMA as quantum analogues of NP.

- **QMA (Quantum Merlin Arthur)** - Languages L in which positive instances can in polynomial time be verified by a quantum verifier with a polynomial sized quantum proof (taken to be a quantum state $|\psi\rangle$).
- **QCMA (Quantum Classical Merlin Arthur)** - Languages L in which positive instances can in polynomial time be verified by a quantum verifier with a polynomial sized classical proof string.

We can consider a similar complexity class but instead of a witness string we now consider an advice string. It differs from a witness string in that it doesn't have to be verified (so we can trust it) and it cannot depend on the input string, only the size of the input string. An analogy is to think of a graduate adviser who is very busy and so can only give advice to graduate students based on which year they are in.

Definition. P/poly is the class of languages L decidable by a polynomial time Turing machine which receives a polynomial size advice string a_n which only depends on the length n of the input.

To see the power of advice consider P/exp which instead receives an exponentially sized advice string. This could decide any language whatsoever by giving a large lookup table as advice. That is, it can map each 2^n possible length n inputs to a specific advice string. Now a fully quantum analog is BQP/qpoly.

Definition. BQP/qpoly is the class of languages L decidable by poly-time quantum algorithm Q and a set of poly-size quantum advice states $\{|\psi_n\rangle\}$ such that $Q\left(|x\rangle \mid |\psi_n\rangle \mid |0\cdots 0\rangle\right)$ accepts with with probability $\geq \frac{2}{3}$ if $x \in L$ and rejects with probability $\geq \frac{2}{3}$ for every $x \notin L$.

We can always switch to classical advice and notate it BQP/poly.

Theorem. There exists a classical oracle U for which $\mathrm{BQP}^{u}/\mathrm{qpoly} \neq \mathrm{BQP}^{U}/\mathrm{poly}$.

Last week the **Group Non-Membership** problem was discussed: Given $g_1, ..., g_n, h \in G$ is $h \notin \langle g_1, ..., g_n \rangle$? This problem is in QMA. However it was shown by Watrous this problem lies in $\mathrm{BQP}^{U}/\mathrm{qpoly}$ but is not known to lie in $\mathrm{BQP}^{U}/\mathrm{poly}$ where U is some quantum oracle.

How powerful is BQP/qpoly? Is BQP/qpoly = ALL (the class of all languages)? Deciding a language is computing an n-input boolean function $L_n : \{0,1\}^n \to \{0,1\}$, so perhaps we could have a quantum adviser encode the entire truth table of L_n as

$$|\psi_n\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \, |L_n(x)\rangle$$

But what would we even do with this advice? Measuring this would result in a very small probability of getting the correct answer associated to input x.

This introduces the question if poly-sized quantum advice is really more useful than poly-sized classical advice. Aaronson showed that BQP/qpoly $\subseteq$ PostBQP/poly. Meaning whatever you can do with a quantum advice string, you can do with a classical advice string given you are willing to spend possibly exponentially computational effort trying to understand the classical advice.

Theorem. BQP/qpoly $\subseteq$ PostBQP/poly.

Proof. Suppose $|\varphi_n\rangle$ is our quantum advice state and let $|\varphi\rangle = |\varphi_n\rangle^{\otimes n}$ be n copies of this advice state. Since we don't have quantum access to this advice state $|\varphi\rangle$, we will have to guess it which we can do to exponentially low probability $\frac{1}{\exp(n)}$.

The strategy will be to show that we can simulate an algorithm $Q(x, |\varphi\rangle) \in$ BQP/qpoly by an algorithm in PostBQP/poly. To guess $|\varphi\rangle$, it makes sense to start with the maximally mixed state ρ_0. The adviser provides classical advice $x_1 \in \{0,1\}^n$ such that

$$P[Q(x_1, \rho_1) = L_n(x)] < 2/3$$

Then we run $Q(x_1, \rho_1)$ and postselect on obtaining the correct answer and we leave ρ_2 in the advice register. The adviser then sends x_2 such that

$$P[Q(x_2, \rho_2) = L_n(x)] < 2/3$$

Now we just need a bound on k, the number of iterations we need to condition ρ properly. We want to choose an orthonomal basis containing the advice state $|\varphi\rangle$ and expand the maximally mixed state in this basis. But the maximally mixed state can be written as an equal mixture in any orthonormal basis

$$\frac{1}{2^m} \sum_{x \in \{0,1\}^n} |x\rangle\langle x| = \frac{1}{2^m} \sum_{x \in \{0,1\}^n} |\varphi_i\rangle\langle \varphi_i|$$

where say $|\varphi_1\rangle = |\varphi\rangle$. Then

$$P[Q(|\varphi\rangle) \text{ succeeds on } x_1, ..., x_k] > 0.9$$

so

$$\left(\frac{2}{3}\right)^k \geq P\left[Q\left(\frac{I}{2^m}\right) \text{ succeeds on } x_1, ..., x_k\right] > \frac{0.9}{2^m}$$

which implies $k = O(m)$.

So far we've discussed the difference between quantum and classical advice, but what about quantum vs classical oracles. Let A, B two complexity classes. Is there an oracle $\mathcal{O}$ such that $A^{\mathcal{O}} \neq B^{\mathcal{O}}$?

Definition. A quantum oracle is an infinite sequence of unitaries $\{U_n\}_{n\geq 1}$. If the quantum computer is in state

$$|\Phi\rangle = \sum_z \alpha_z |z\rangle |\phi_z\rangle$$

where $|z\rangle$ is the work register and $|\phi_z\rangle$ is the answer register then querying the oracle maps this state to

$$|\Phi'\rangle = \sum_z \alpha_z |z\rangle U_n |\phi_z\rangle$$

If $\mathcal{O}$ is a classical oracle, then this immediately implies there exists quantum oracle U with $A^U \neq B^U$ but the reverse might not be true since the space of quantum oracles is larger.

Finally, we have a result that there exists a quantum oracle U with $\text{QMA}^U \neq \text{QCMA}^U$ from Kuperberg & Aaronson however whether there exists a classical oracle which also separates the classes is an open problem (but conjectured to be true).

The end!