Quantum Computing 2019 Set 2

Due October 10th October 3rd

Instructions: Solutions should be legibly handwritten or typset. Sets are to be returned in the mailbox outside 615 Soda Hall.

Problem 1. (2 points) In the proof of $\text{BQP} \subseteq \text{GapP}$, we assumed that we can find a complete gate set where every gate can be expressed as a unitary matrix with only real entries. i.e. quantum computing with real amplitudes is just as powerful as allowing complex amplitudes. Show this is possible.

Problem 2. Consider a device that ideally produces the state $|\psi_0\rangle$ but due to manufacturing defects produces the state $|\psi_1\rangle$. We will show that if $|\psi_0\rangle$ and $|\psi_1\rangle$ have large overlap $|\langle\psi_0|\psi_1\rangle|$, then no quantum process can distinguish these two devices with high probability. For any process $P$, quantify how well it distinguishes $|\psi_0\rangle$ and $|\psi_1\rangle$ by:

$$
\Delta \overset{\text{def}}{=} |\Pr(P(|\psi_0\rangle \text{ outputs 0}) - \Pr(P(|\psi_1\rangle \text{ outputs 0})|)
$$

1. (2 points) Consider the simplest strategy: measure in a basis for which $|\psi_0\rangle$ is a basis vector and guess 0 if the measurement is $|\psi_0\rangle$ and 1 otherwise. Show that then

$$
\Delta = 1 - |\langle\psi_0|\psi_1\rangle|^2.
$$

2. (2 points) This strategy is not optimal. Find a better measurement for which

$$
\Delta = \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2}, \quad (\star)
$$

(Hint: There is a 2-dimensional space containing $|\psi_0\rangle$ and $|\psi_1\rangle$. It may be useful to remember the trigonometric identities of $2 \sin x \sin y = \cos(x - y) - \cos(x + y)$ and $\cos 2x = 2 \cos^2 x - 1$.)
We will show that this second strategy is indeed optimal. To show the upper bound of \( (\star) \), we will first introduce a generalized form of measurement called a *positive-operator valued measurement* (POVM). A POVM is a set of Hermitian positive semidefinite operators \( \{M_i\} \) on a Hilbert space \( \mathcal{H} \) that sum up to identity
\[
\sum_{i=1}^{n} M_i = \mathbb{I}_{\mathcal{H}}.
\]
The probability of measuring outcome \( i \) is given by \( \Pr(i) = \langle \psi | M_i | \psi \rangle \). This generalizes a basis measurement as we can consider \( M_i = |b_i\rangle\langle b_i| \) for any basis \( \{ |b_i\rangle \} \). An important difference between basis measurements and POVMs are that the element of a POVM are not necessarily orthogonal and, therefore, the number of elements can be larger than the dimension of the Hilbert space \( \mathcal{H} \).

Instead, POVMs are exactly as descriptive as as applying a unitary \( U \) to the state and ancilla \( |\psi\rangle \otimes |0\ldots0\rangle \) followed by a measurement of some of the qubits.

3. **(2 points)** For any POVM \( \{M_i\} \), let \( A_i = \sqrt{M_i} \), consider the following partial transformation:
\[
U : |\psi\rangle |0\rangle_{\text{ancilla}} \mapsto \sum_{i=1}^{n} A_i |\psi\rangle |i\rangle_{\text{ancilla}}.
\]
Conclude that \( U \) followed by a measurement of the ancilla register gives the same statistics as the POVM.

4. **(2 points)** Given a unitary \( U \) acting on the state and some ancilla of dimension \( n \) initialized to zero, construct a POVM equivalent to applying \( U \) and measuring the ancilla in the standard basis.

Returning to the problem at hand, we can generalize the distinguishing measurement as a POVM with two elements \( M \) and \( \mathbb{I} - M \), with the two outcomes corresponding to answering 0 and 1, respectively. Attempt the next four parts if you are able to – if not, you will get another chance to return to them when we will have covered some more background material in class.

5. **(2 points)** Show that then the optimal value of \( \Delta \) is
\[
\Delta_{\text{opt}} = \max_{0 \leq M \leq \mathbb{I}} \text{Tr} (M \rho)
\]
where \( \rho = |\psi_0\rangle\langle \psi_0 | - |\psi_1\rangle\langle \psi_1 |. \)
6. **(2 points)** Conclude that

\[
\max_{0 \leq M \leq \mathbb{I}} \text{Tr}(M\rho) = \frac{1}{2} \text{Tr} \sqrt{\rho^2}.
\]

(Hint: Consider an optimal \(M\) in the basis where \(\rho\) is diagonal).

7. **(2 points)** Finish by showing

\[
\text{Tr} \sqrt{\rho^2} = 2 \sqrt{1 - |\langle \psi_0 | \psi_1 \rangle|^2}.
\]

(Hint: \(\rho\) is a rank 2 matrix; therefore it has only 2 non-zero eigenvalues. Now express \(\text{tr}(\rho^2)\) in two ways.)

8. **(1 point)** Give a justification as to why the maximizing \(M\) and the measurement you gave in Part 2 are the same.

**Problem 3. (6 points)** Show that \(\text{BQP}^{\text{BQP}} = \text{BQP}\). More formally, let \(f\) be a language \(\in \text{BQP}\) and let \(g\) be a language \(\in \text{BQP}^f\), a language decidable by a BQP device with access to \(f\). Then show that \(g \in \text{BQP}\).

(Hint: it might help to prove a rigorous version of the statement: If a binary measurement on a quantum state outputs 0 with high probability, then the post-measurement state on output 0 has high overlap with the pre-measurement state.)

**Problem 4. (2 points)** Raz and Tal showed that \(\exists \) an oracle \(A\) such that \(\text{BQP}^A \not\subset \text{PH}^A\). The oracle they used to show this result is the “forrelation” oracle. The oracle consists of two functions \(f, g : \{0, 1\}^n \rightarrow \{\pm 1\}\) with the promise\(^1\) that either \(\Phi_{f, g} \geq 3/5\) or \(|\Phi_{f, g}| \leq 1/100\) for

\[
\Phi_{f, g} \overset{\text{def}}{=} 2^{-3n/2} \sum_{x, y \in \{0, 1\}^n} f(x)(-1)^{x \cdot y} g(y).
\]

Show that these two cases can be distinguished with high probability given quantum access to \(f\) and \(g\).

\(^1\)The reason for the asymmetry in one promise being for \(\Phi_{f, g}\) while other for its absolute value is technical and if interested, one should look at the paper of Aaronson and Ambainis introducing the problem.