1. **Complete problems for BQP.** We say that a language $L$ is complete for a complexity class $C$ (or that $L$ is $C$-complete) if $L \in C$ and every problem in $C$ can be reduced to $L$ in (classical, deterministic) polynomial time. In class, we discussed the notion of $\text{NP}$-complete problems such as 3SAT. In this problem we explore the notion of complete problems for $\text{BQP}$.

In a promise problem, our goal is to distinguish “yes” from “no” instances subject to a promise about the input. We specify such a problem by a pair of languages $(L_{\text{yes}}, L_{\text{no}}) \subseteq \{0, 1\}^* \times \{0, 1\}^*$ such that $L_{\text{yes}} \cap L_{\text{no}} = \emptyset$ (but we do not require that $L_{\text{yes}} \cup L_{\text{no}} = \{0, 1\}^*$).

(a) [3 points] Let $\text{PromiseBQP}$ be the set of promise problems that can be decided by a $\text{BQP}$ machine. More formally, we say $(L_{\text{yes}}, L_{\text{no}}) \in \text{PromiseBQP}$ if there is a polynomial-time quantum algorithm that, on input $x$, outputs “yes” with probability at least $2/3$ if $x \in L_{\text{yes}}$ and outputs “no” with probability at least $2/3$ if $x \in L_{\text{no}}$. Give an example of a $\text{PromiseBQP}$-complete problem. (It’s okay if your problem is trivial, i.e., its $\text{PromiseBQP}$-completeness may follow straightforwardly from the definition, but you should still prove that the problem is $\text{PromiseBQP}$-complete.)

**Solution:** The trivial $\text{PromiseBQP}$-complete problem is as follows: Given a quantum circuit acting on the $|0\rangle$ state, does a computational-basis measurement of the first qubit of the output give 1 with probability greater than $2/3$ or less than $1/3$? This problem is in $\text{PromiseBQP}$ because we can simply run the circuit to determine which case we are in with bounded error. It is $\text{PromiseBQP}$-complete because any problem in $\text{PromiseBQP}$ can be solved with bounded error by running some quantum circuit. The output of such a circuit can be encoded in the first qubit without loss of generality.

(b) [1 point] Do you think that there are complete problems for the (non-promise) class $\text{BQP}$? Explain why it might be difficult to find such a problem.

**Solution:** Whereas the problem described in the solution of the previous part is trivially $\text{PromiseBQP}$-complete, it is nontrivial to remove the promise since general quantum circuits may output a state such that measuring the first qubit gives 1 with probability between $1/3$ and $2/3$, and it is unclear how to characterize such circuits so they can be excluded without imposing a promise on the input. Indeed, it is plausible that $\text{BQP}$ might not contain complete problems.

2. **Improved upper bound on $\text{BQP}$.** In class, we argued that $\text{BQP} \subseteq \text{PSPACE}$. In this problem we will find a stronger bound.

The class $\text{PP}$ of probabilistic polynomial-time computations (with unbounded error, as opposed to $\text{BPP}$ which has bounded error) is the set of languages $L \subseteq \{0, 1\}^*$ for which there exists a randomized algorithm $A$ satisfying

- $\forall x \in L, A(x) \text{ accepts with probability } > 1/2 \text{ and }$
- $\forall x \notin L, A(x) \text{ rejects with probability } > 1/2 \text{ (i.e., accepts with probability } \leq 1/2).$

(a) [2 points] Prove that $\text{PP} \subseteq \text{PSPACE}$.

**Solution:** To decide a language in $\text{PP}$ using only polynomial space, we sum over all possible assignments of the random bits used by the $\text{PP}$ algorithm to compute the acceptance probability. The $\text{PSPACE}$ machine simply accepts if that probability is above $1/2$. Since we only have to keep a running total, this calculation can be done with only polynomial space.
(b) [3 points] Prove that BQP ⊆ PP.

Solution: We can view a randomized algorithm as a distribution over deterministic algorithms. Specifically, if the algorithm $A(x)$ in the definition of PP uses $k$ bits of randomness, we can view it as a deterministic algorithm $A_r(x)$ where the string $r \in \{0, 1\}^k$ is chosen uniformly at random. Then the acceptance probability of $A(x)$ is simply $\sum_{r \in \{0, 1\}^k} a_r(x)$, where $a_r(x)$ is $1/2^k$ if $A_r(x)$ accepts and 0 if it rejects.

Thus, in the class PP, we have the ability to determine whether the sum of exponentially many numbers is above or below some threshold. If the numbers are either 0 or $1/2^k$ and the threshold is $1/2$, this is precisely the definition of PP (according to the above interpretation). If the numbers take other values, we can simply create an algorithm in which many assignments of the random bits lead to acceptance for a given term of the sum. If we are interested in a threshold other than $1/2$, we can also achieve this by padding the sum with extra 0s (to effectively raise the threshold) or $1/2^k$s (to lower the threshold), but we will not need this below. We can also adjust the range of the values by shifting and/or rescaling the sum.

This ability can be used to simulate a BQP machine. As described in class, we can compute the success probability by summing the amplitudes for all computational paths to determine the value

$$|\langle 0 | U_{t} \ldots U_{2} U_{1} | 0 \rangle|^2 = \sum_{x_1, \ldots, x_{t-1}} \langle 0 | U_{t} | x_{t-1} \rangle \cdots \langle x_2 | U_{2} | x_1 \rangle \langle x_1 | U_{1} | 0 \rangle \langle 0 | U_{1}^\dagger | y_1 \rangle \langle y_1 | U_{2} \rangle \langle y_2 \rangle \cdots \langle y_{t-1} | U_{t} \rangle | 0 \rangle.$$

This is a sum of exponentially many numbers, each of which can be computed efficiently. By combining the terms $(x_1, \ldots, x_{t-1}; y_1, \ldots, y_{t-1})$ and $(y_1, \ldots, y_{t-1}; x_1, \ldots, x_{t-1})$, it is a sum of real numbers. In PP, we can determine whether this sum is above or below $1/2$, which more than suffices to determine whether the BQP machine accepts.

3. Density matrices. Consider the ensemble in which the state $|0\rangle$ occurs with probability $3/5$ and the state $(|0\rangle + |1\rangle) / \sqrt{2}$ occurs with probability $2/5$.

(a) [2 points] What is the density matrix $\rho$ of this ensemble?

Solution:

$$\rho = \frac{3}{5} |0\rangle \langle 0| + \frac{2}{5} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{\langle 0| + \langle 1|}{\sqrt{2}}$$

$$= \frac{4}{5} |0\rangle \langle 0| + \frac{1}{5} |0\rangle \langle 1| + \frac{1}{5} |1\rangle \langle 0| + \frac{1}{5} |1\rangle \langle 1|$$

$$= \frac{1}{5} \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix}$$

(Either of the last two lines is an acceptable answer.)

(b) [2 points] Write $\rho$ in the form $\frac{1}{2} (I + r_x X + r_y Y + r_z Z)$, and plot $\rho$ as a point in the Bloch sphere.

Solution: We have $r_x = \frac{2}{5}$, $r_y = 0$, and $\frac{1}{2} (1 + r_z) = \frac{4}{5} \implies r_z = \frac{3}{5}$. So in the XZ plane, $\rho$
is as follows:

\[ |0\rangle \] 
\[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \] 
\[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \] 
\[ |1\rangle \]

Notice that it is 2/5 of the way along a line from the state |0\rangle to the state |+\rangle.

(c) [3 points] Suppose we measure the state in the computational basis. What is the probability of getting the outcome 0? Compute this both by averaging over the ensemble of pure states and by computing Tr(\(\rho|0\rangle\langle 0|\)), and show that the results are consistent.

**Solution:** With the state |0\rangle, Pr(0) = 1, and with the state |+\rangle, Pr(0) = 1/2. Averaging, we have a probability of \((3/5)(1) + (2/5)(1/2) = 4/5\).

Correspondingly, we have

\[
\text{Tr}(\rho|0\rangle\langle 0|) = \text{Tr}((\frac{4}{5}|0\rangle\langle 0| + \frac{1}{5}|0\rangle\langle 1| + \frac{1}{5}|1\rangle\langle 0| + \frac{1}{5}|1\rangle\langle 1|)(|0\rangle\langle 0|))
\]

\[
= \text{Tr}((\frac{4}{5}|0\rangle\langle 0| + \frac{1}{5}|1\rangle\langle 0|)
\]

\[
= \frac{4}{5}.
\]

(d) [3 points] How does the density matrix change if we apply the Hadamard gate? Compute this both by applying the Hadamard gate to each pure state in the ensemble and finding the corresponding density matrix, and by computing \(H\rho H^\dag\).

**Solution:** We have \(H|0\rangle = |+\rangle\) and \(H|+\rangle = |0\rangle\), so applying the gate to each element of the ensemble gives the density matrix

\[
\frac{3}{5}|+\rangle\langle +| + \frac{2}{5}|0\rangle\langle 0| = \frac{3}{5}|0\rangle + \frac{1}{5}|1\rangle\langle 1| + \frac{1}{5}|1\rangle\langle 0| + \frac{2}{5}|0\rangle\langle 0|
\]

\[
= \frac{3}{10}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) + \frac{2}{5}|0\rangle\langle 0|
\]

\[
= \frac{7}{10}|0\rangle\langle 0| + \frac{3}{10}(|0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|).
\]

On the other hand, conjugating \(\rho\) by \(H\) gives

\[
H\rho H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{5} \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}
\]

\[
= \frac{1}{10} \begin{pmatrix} 5 & 2 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}
\]

\[
= \frac{1}{10} \begin{pmatrix} 7 & 3 \\ 3 & 3 \end{pmatrix}.
\]
in agreement with the previous calculation.

4. Local operations and the partial trace.

(a) [4 points] Let \( |\psi\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle \). Let \( \rho \) denote the density matrix of \( |\psi\rangle \) and let \( \rho' \) denote the density matrix of \( (I \otimes H)|\psi\rangle \). Compute \( \rho \) and \( \rho' \).

**Solution:** The density matrix of \( |\psi\rangle \) is

\[
\rho = |\psi\rangle\langle\psi| = \left( \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle \right)\left( \frac{\sqrt{3}}{2}\langle00| + \frac{1}{2}\langle11| \right) = \frac{3}{4}|00\rangle\langle00| + \frac{\sqrt{3}}{4}(|00\rangle\langle11| + |11\rangle\langle00|) + \frac{1}{4}|11\rangle\langle11|.
\]

We have

\[
(I \otimes H)|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle|+\rangle + \frac{1}{2}|1\rangle|-\rangle = \frac{\sqrt{3}}{2\sqrt{2}}(|00\rangle + |01\rangle) + \frac{1}{2\sqrt{2}}(|10\rangle - |11\rangle),
\]

so

\[
\rho' = (I \otimes H)|\psi\rangle\langle\psi|(I \otimes H) = \frac{1}{8} \left[ \sqrt{3}(|00\rangle + |01\rangle) + |10\rangle - |11\rangle \right] \left[ \sqrt{3}(\langle00| + \langle01|) + \langle10| - \langle11| \right]
\]

\[
= \frac{1}{8} \begin{pmatrix}
3 & 3 & \sqrt{3} & -\sqrt{3} \\
3 & 3 & \sqrt{3} & -\sqrt{3} \\
\sqrt{3} & \sqrt{3} & 1 & -1 \\
-\sqrt{3} & -\sqrt{3} & -1 & 1
\end{pmatrix}.
\]

(Either answer can be given using either Dirac notation or in matrix form.)

(b) [3 points] Compute \( \text{Tr}_B(\rho) \) and \( \text{Tr}_B(\rho') \), where \( B \) refers to the second qubit.

**Solution:** This is a direct computation. For \( \rho \), using the Dirac form above

\[
\text{Tr}_B(\rho) = \frac{3}{4}|0\rangle\langle0| + \frac{1}{4}|1\rangle\langle1|.
\]

For \( \rho' \), in matrix form we have

\[
\text{Tr}_B(\rho') = \frac{1}{8} \begin{pmatrix}
3 + 3 & \sqrt{3} - \sqrt{3} \\
\sqrt{3} - \sqrt{3} & 1 + 1
\end{pmatrix}
\]

\[
= \frac{1}{4} \begin{pmatrix}
3 & 0 \\
0 & 1
\end{pmatrix},
\]

so that \( \text{Tr}_B(\rho) = \text{Tr}_B(\rho') \).

(c) [4 points] Let \( \rho \) be a density matrix for a quantum system with a bipartite state space \( A \otimes B \). Let \( I \) denote the identity operation on system \( A \), and let \( U \) be a unitary operation on system \( B \). Prove that \( \text{Tr}_B(\rho) = \text{Tr}_B((I \otimes U)^\dagger \rho (I \otimes U)) \).
Solution: Let $\rho = \sum_{ij} a_{ijkl} |\psi_i\rangle\langle \psi_j| \otimes |\phi_k\rangle\langle \phi_l|$ for some orthonormal bases $\{|\psi_i\rangle\}$ and $\{|\phi_j\rangle\}$. Then

$$\text{Tr}_B(\rho) = \text{Tr}_B \left( \sum_{ijkl} a_{ijkl} |\psi_i\rangle\langle \psi_j| \otimes |\phi_k\rangle\langle \phi_l| \right)$$

$$= \sum_{ijkl} a_{ijkl} \text{Tr}_B( |\psi_i\rangle\langle \psi_j| \otimes |\phi_k\rangle\langle \phi_l| )$$

$$= \sum_{ijkl} a_{ijkl} \text{Tr}( |\phi_k\rangle\langle \phi_l| ) |\psi_i\rangle\langle \psi_j|$$

$$= \sum_{ijkl} a_{ijkl} |\psi_i\rangle\langle \psi_j| .$$

Similarly,

$$\text{Tr}_B((I \otimes U)\rho(I \otimes U^\dagger)) = \text{Tr}_B \left( \sum_{ijkl} a_{ijkl} |\psi_i\rangle\langle \psi_j| \otimes U|\phi_k\rangle\langle \phi_l| U^\dagger \right)$$

$$= \sum_{ijkl} a_{ijkl} \text{Tr}_B( |\psi_i\rangle\langle \psi_j| \otimes U|\phi_k\rangle\langle \phi_l| U^\dagger )$$

$$= \sum_{ijkl} a_{ijkl} \text{Tr}(U|\phi_k\rangle\langle \phi_l| U^\dagger ) |\psi_i\rangle\langle \psi_j|$$

$$= \sum_{ijkl} a_{ijkl} \text{Tr}(U^\dagger U|\phi_k\rangle\langle \phi_l| ) |\psi_i\rangle\langle \psi_j|$$

$$= \sum_{ijkl} a_{ijkl} \text{Tr}( |\phi_k\rangle\langle \phi_l| ) |\psi_i\rangle\langle \psi_j|$$

$$= \sum_{ijkl} a_{ijkl} |\psi_i\rangle\langle \psi_j|$$

$$= \text{Tr}_B(\rho)$$

as claimed.

(d) [4 points] Show that the converse of part (c) holds for pure states. In other words, show that if $|\psi\rangle$ and $|\phi\rangle$ are bipartite pure states, and $\text{Tr}_B(|\psi\rangle\langle \psi|) = \text{Tr}_B(|\phi\rangle\langle \phi|)$, then there is a unitary operation $U$ acting on system $B$ such that $|\phi\rangle = (I \otimes U)|\psi\rangle$.

Solution: By the Schmidt decomposition (Theorem 2.7.1 in KLM), we can write

$$|\psi\rangle = \sum_i \sqrt{p_i} |\alpha_i\rangle |\beta_i\rangle$$

for some orthonormal basis $\{|\alpha_i\rangle\}$ for system $A$ and $\{|\beta_i\rangle\}$ for system $B$, and probability distribution $\{p_i\}$. Expand the first register of $|\phi\rangle$ in the basis $\{|\alpha_i\rangle\}$, giving

$$|\phi\rangle = \sum_i |\alpha_i\rangle |\tilde{\gamma}_i\rangle$$
where \{\ket{\tilde{\gamma}_i}\} are some (non-normalized) vectors. Then we have
\[
\text{Tr}_B(\ketbra{\psi}) = \sum_{i,j} \sqrt{p_i p_j} \ketbra{\alpha_i} \text{Tr}(\ketbra{\beta_i})
\]
\[
= \sum_{i,j} \sqrt{p_i p_j} \delta_{ij} \ketbra{\alpha_i},
\]
and
\[
\text{Tr}_B(\ketbra{\phi}) = \sum_{i,j} \ketbra{\alpha_i} \text{Tr}(\ketbra{\tilde{\gamma}_i})
\]
\[
= \sum_{i,j} \langle \tilde{\gamma}_j \rangle \tilde{\gamma}_i \ketbra{\alpha_i}.
\]

Both partial traces are equal by assumption and \{\ket{\alpha_i}\} is an orthonormal basis, so the coefficients in both cases are the same: \(\sqrt{p_i p_j} \delta_{ij} = \langle \tilde{\gamma}_j \rangle \tilde{\gamma}_i\). This means that the states \{\ket{\tilde{\gamma}_i}\} are pairwise orthogonal and \(\|\ket{\tilde{\gamma}_i}\| = \sqrt{p_i}\) (it is possible that \(p_i = 0\) for some \(i\)). Equivalently, we can find an orthonormal basis \{\ket{\gamma_i}\} such that \(\ket{\tilde{\gamma}_i} = \sqrt{p_i} \ket{\gamma_i}\). Then we see that \(\ket{\phi} = (I \otimes U) \ket{\psi}\), where \(U = \sum_i \ket{\gamma_i} \bra{\beta_i}\) is the unitary change of basis from \{\ket{\beta_i}\} to \{\ket{\gamma_i}\}.

(e) [2 points] Does the converse of part (c) hold for general density matrices? Prove or provide a counterexample.

**Solution:** The converse is false in general; here is a counterexample. Consider the states
\[
\rho = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}, \quad \rho' = \begin{pmatrix}
1/2 & 0 & 0 & 0 \\
0 & 1/2 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix}.
\]

These states have \(\text{Tr}_B(\rho) = \text{Tr}_B(\rho') = \ketbra{0}\ket{0}\), but since they have different eigenvalues, there is no unitary transformation mapping one to the other.

Total points: 36