Introduction to Quantum Information Processing
Assignment 2
Due: October 29th

1. 3 marks

   Suppose we have a bipartite system in a state described by density matrix

$$\rho = \begin{pmatrix} \frac{1}{2} & \frac{1}{3} & 0 & \frac{1}{6} \\ \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{6} & 0 & 0 & \frac{1}{6} \end{pmatrix}.$$

   What is the result of tracing out the second system?

   Let A be an arbitrary one-qubit operations. What is result the result of tracing out the second system in the state $(I \otimes A)\rho(I \otimes A^{\dagger})$?

   What is the result of tracing out the second system in the state $(A \otimes I)\rho(A^{\dagger} \otimes I)$?

2. 3 marks Exercise 2.11

   Find the eigenvectors, eigenvalues, and diagonal representations of the Pauli matrices X, Y, Z.

3. 4 marks Exercise 4.8, parts 2 and 3.

   Find a vector $\hat{n} = (n_x, n_y, n_z)$, real numbers θ, α, such that the Hadamard gate H equals $e^{i\alpha}R_{\hat{n}}(\theta)$.

   Find a vector $\hat{n} = (n_x, n_y, n_z)$, real numbers θ, α, such that the "phase gate"

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

   equals $e^{i\alpha}R_{\hat{n}}(\theta)$.

4. 4 marks Exercise 2.81.

   Let $|AR_1\rangle$ and $|AR_2\rangle$ be two purifications of a state ρ_A to a composite system AR. Prove that there exists a unitary transformation U_R acting on system R such that $|AR_1\rangle = (I_A \otimes U_R)|AR_2\rangle$.

5. 2 marks Exercise 4.35 (Measurement commutes with controls)

6. 6 marks

   Suppose you are given a 1-qubit gate U_ϕ that takes one unit of time and maps $|0\rangle \to |0\rangle$ and $|1\rangle \to e^{i\phi}|1\rangle$. Suppose $\phi \in \{0, \pi/4, \pi/2, 3\pi/4, \pi, 5\pi/4, 3\pi/2, 7\pi/4\}$. Suppose all other gates take negligible time. Show how to determine ϕ deterministically (i.e. find a procedure that outputs the correct answer with certainty) in only one time step. You can use any finite number of copies of U_ϕ as you wish in that one time step.

7. 4 marks

   Suppose you are given a circuit of size s, consisting only of 1-qubit gates and CNOT gates, that implements an n-qubit unitary operation U. Show how to obtain a circuit of comparable size (i.e. in $O(s)$) consisting only of 1-qubit gates and $CNOT$ gates, that implements the controlled-U operation.

8. 4 marks

   Let $N = pq$, where q and p are large distinct primes. Suppose you know N, and have a circuit for implementing QFT_N^{-1} as well as one copy of the state

$$|\,\psi\rangle = \sum_{x=0}^{q-1} \frac{1}{\sqrt{q}}\,|\,xp + y\rangle$$

   for some random integer $y \in \{0, 1, 2, \ldots, p-1\}$.

   What is the result of applying QFT_N^{-1} to $|\,\psi\rangle$?

   Show how the result will likely allow you to factorize N.

   (N.B. that this is NOT how the famous quantum factoring algorithm works.)

9. 4 marks

   Define the SWAP gate to be the two-qubit gate that swaps the two qubits.

   What are the eigenvalues of the SWAP gate?

   Suppose you are given two qubits in the states $|\,\psi_1\rangle$ and $|\,\psi_2\rangle$ with the promise that the states are either equal or orthogonal. Show how to use the controlled-SWAP gate to test the equality of the two states with probability of error at most 1/3 (regardless of the a priori probabilities of the two possibilities).