18.435/2.111 Homework # 3

Due Thursday, October 16

The first three problems relate to the factoring algorithm. Recall that we factored N by constructing the unitary transformation U which takes $U\,|\,a\rangle = |\,ax \bmod N\rangle$ for $0 \le a < N$ and $\gcd(x, N) = 1$. We found the minimum $r > 0$ for which $U^r\,|\,1\rangle = |\,1\rangle$ and used it to factor N. Note that for some of these problems, Theorem A4.10 on page 632 of N&C may come in handy. This theorem says that the multiplicative group of residues mod p^α is cyclic for odd primes p.

1. For $N = 15$, what fraction of the residues $1 \le x < N$ with $\gcd(x, N) = 1$ will result in a factorization? How about for $N = 63$? (While testing all these residues is one way to solve this problem, there are much more efficient ones.)

2. Suppose we try to apply the factoring algorithm to a number $N = p^\alpha$ which is a power of p. Will it work? If not, what goes wrong?

3. Suppose we try to apply the factoring algorithm, but we forget to check whether $\gcd(x, N) = 1$ and accidentally choose an x with $1 < x < N$ and $\gcd(x, N) > 1$. Will the algorithm still work? If not, what goes wrong?

The next two problems deal with the period-finding algorithm on p. 236 of N&C. This was not covered in class, but is quite similar to the order-finding algorithm (p. 232) which was. The difference is that the order-finding algorithm operates on a black box U which performs $U\,|\,a\rangle = |\,f(a)\rangle$ where f is a classical one-to-one function, and finds the minimum value of r such that $U^r\,|\,b\rangle = |\,b\rangle$, whereas the period-finding algorithm operates on a black box U such that $U\,|\,x\rangle\,|\,y\rangle = |\,x\rangle\,|\,y \oplus f(x)\rangle$. Also note that the value of t is given using big-O notation, but for the algorithm to work, you actually need $t \ge 2L$.

4. Do Exercise 5.20 in N&C.

5. Suppose we apply this period-finding algorithm to the function

$$\begin{aligned} f(x) &= 1 \qquad \text{if } r \text{ divides } x \\ f(x) &= 0 \qquad \text{if } x \text{ is not a multiple of } r. \end{aligned}$$

Approximately what is the probability that we learn the period r?

6. For Grover's search algorithm, assume that we have M target states out of N total states, so the black box O takes

$$\begin{aligned} O\,|\,x\rangle &= -\,|\,x\rangle \qquad \text{if } x \text{ is a target state,} \\ O\,|\,x\rangle &= |\,x\rangle \qquad \text{otherwise.} \end{aligned}$$

Suppose we find a target state with probability 1 after one iteration of the algorithm. What can you say about the ratio M/N?

7. Consider the modification to Grover's algorithm so that the oracle now performs

$$\begin{aligned} O\,|\,x\rangle &= e^{i\phi}\,|\,x\rangle \qquad \text{if } x \text{ is a target state,} \\ O\,|\,x\rangle &= |\,x\rangle \qquad\quad \text{otherwise.} \end{aligned}$$

Show that if you use the transformation

$$\tilde{G} = H^{\otimes n}\left[(1-e^{i\phi})\,|\,0\rangle\,\langle 0\,|\,-I\right]H^{\otimes n}O$$

instead of the standard Grover iteration, for any state with M/N sufficiently large you can choose ϕ so that the algorithm finds a target state with probability 1 after one iteration. For what values of M/N is there such a ϕ?

18.435/2.111 Homework # 5

Due Tuesday, November 25

1. What is the density matrix obtained if you have a qubit which is in state

$$\begin{array}{rll} |\,0\rangle & \text{with probability} & \frac{1}{3}, \\ -\frac{1}{2}\,|\,0\rangle + \frac{\sqrt{3}}{2}\,|\,1\rangle & \text{with probability} & \frac{1}{3}, \\ -\frac{1}{2}\,|\,0\rangle - \frac{\sqrt{3}}{2u}\,|\,1\rangle & \text{with probability} & \frac{1}{3}. \end{array}$$

2. What is the density matrix obtained if you take the partial trace over the second qubit of the following state; i.e., what is

$$\mathrm{Tr}_2 \frac{1}{\sqrt{3}}(|\,00\rangle + |\,01\rangle + |\,10\rangle).$$

3. One way to obtain a noisy quantum operation is to have the input quantum state interact with another "environment" quantum system, and then take a partial trace that removes the "environment" system.

Suppose we start with a qubit in state $|\,\psi\rangle$, and an "environment qubit" $|\,e\rangle$ in state $\frac{\sqrt{3}}{2}\,|\,0\rangle + \frac{1}{2}\,|\,1\rangle$. We then apply the quantum gate controlled σ_z

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

to the state $|\,\psi\rangle \otimes |\,e\rangle$, and take the partial trace to remove $|\,e\rangle$. Express the resulting quantum operation in operator sum notation,

$$\rho \to \sum_i A_i \rho A_i^\dagger.$$

4. Suppose we start with a qubit and first apply the dephasing operation

$$\rho \to (1-p)\rho + p\sigma_z \rho \sigma_z^\dagger$$

and then apply the amplitude damping operation

$$\rho \to \sum_{i=1}^{2} A_i \rho A_i^\dagger$$

where

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-q} \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & \sqrt{q} \\ 0 & 0 \end{pmatrix}.$$

Show the resulting transformation can be expressed in the operator-sum notation with just three matrices A_i:

$$\rho \to \sum_{i=1}^{3} A_i \rho A_i^\dagger.$$

5. Consider the depolarizing quantum operation $\mathcal{D}$:

$$\mathcal{D}(\rho) = (1-p)\rho + \frac{p}{3} \sum_{a=x,y,z} \sigma_a \rho \sigma_a^\dagger,$$

with $p < 3/4$. Suppose we apply $\mathcal{D}$ to a density matrix ρ_{in} to obtain $\rho_{\text{out}} = \mathcal{D}(\rho_{\text{in}})$. Show that the minimum possible eigenvalue of a density matrix output from this operation is $2p/3$.
Hint: use the identity

$$\frac{1}{4}\rho + \frac{1}{4} \sum_{a=x,y,z} \sigma_a \rho \sigma_a^\dagger = \frac{I}{2},$$

where I is the identity matrix.

6. Do Exercise 10.27 in Nielsen and Chuang.
Hint: one way to do this is to show directly that it has equivalent error-correcting properties for bit errors, and then take the Hadamard transform of the code and show that this works well for phase errors. Another approach is to follow the proof that Nielsen and Chuang use to derive the phase error-correcting properties of a CSS code.

18.435/2.111 Homework # 4

Due Thursday, November 6

1. In the teleportation protocol, show that the probability distribution for the values of the two qubits that Alice sends to Bob is independent of the state $|\psi\rangle$ of the qubit being transmitted. In other words, an eavesdropper can infer nothing about the value of $|\psi\rangle$ by knowing the values of the two classical bits transmitted.

2. Show that Alice can teleport two qubits $|\phi\rangle\,|\psi\rangle$ "through" the gate

$$S = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

so that Bob obtains two qubits in the state $S\,|\phi\rangle\,|\psi\rangle$.

More specifically, suppose Alice and Bob share four qubits in the state

$$\frac{1}{2}\Big(\,|\,0000\rangle + |\,0101\rangle + |1010\rangle - |\,1111\rangle\,\Big),$$

with Alice holding the first pair of qubits and Bob holding the second pair. Alice measures $|\phi\rangle$ and her first qubit in the Bell basis, and measures $|\psi\rangle$ and her second qubit in the Bell basis. Alice sends the results of these measurements to Bob over a classical channel, and Bob applies some unitary transformations, which depend on the classical information he receives from Alice, to his two qubits to obtain the state $S\,|\phi\rangle\,|\psi\rangle$. Explain how the transformations Bob applies depend on the results of Alice's measurements.

3. Generalize the superdense coding procedure to three-dimensional quantum states (qutrits). Let $|\,0\rangle\,,|\,1\rangle\,,|\,2\rangle$ be an orthonormal basis for the qutrits. Now, suppose Alice and Bob share a pair of qutrits in the state

$$|\,\mathrm{EPR}_3\rangle = \frac{1}{\sqrt{3}}\Big(\,|\,00\rangle + |\,11\rangle + |\,22\rangle\,\Big)$$

Show that there are 9 unitary operations so that if Alice performs one of these unitary operations on her half of the state $|\,\mathrm{EPR}_3\rangle$, and sends the resulting qubit to Bob, he can then make a measurement on the two qutrits that he now holds which deterministically tells him which operation Alice performed. This shows that superdense coding can encode $\log_2 9$ bits in one qutrit.

Hint: Define the two matrices

$$T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}.$$

Powers of these of the form $R^a T^b$ with $0 \leq a, b \leq 2$ will play the role of the Pauli matrices in this superdense coding procedure, with the Bell basis replaced by the states $R^a T^b \,|\, \mathrm{EPR}_3\rangle$. You will need to show that these states form an orthonormal basis of the space of two qutrits.

4. Suppose that we have four parties, Alice, Bob, Cathy, and David. Alice and Cathy share a pair of qubits which are in one of the four Bell basis states,

$$\frac{1}{\sqrt{2}}(|\,01\rangle \pm |\,10\rangle), \qquad\qquad \frac{1}{\sqrt{2}}(|\,00\rangle \pm |\,11\rangle),$$

but they don't know which state it's in. Bob and David share a pair of qubits in the same Bell state. Suppose further that Alice and Bob share a pair of qubits in the state $\frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle)$. Show that there is a protocol that lets Cathy and David end up sharing a pair of qubits in the state $\frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle)$.
Hint: Let Alice teleport her half of the Alice-Bob pair to Cathy, and Bob teleport his half of this pair to David. Show that even though Cathy and David don't know which Bell state they had, they can still apply Pauli transformations to their teleported qubits to end up with the state $\frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle)$.

5. (Extra Credit) Show that in the model for quantum computation using measurement on cluster states, a SWAP gate can be implemented by bringing two transmission lines together for three qubits, and measuring every qubit using the observable σ_x (i.e., in the basis $\frac{1}{2}(|\,0\rangle \pm |\,1\rangle)$). For example, the following cluster

$$\begin{array}{ccccccc} \sigma_x & \sigma_x & \sigma_x & \sigma_x & \sigma_x & \sigma_x & \sigma_x \\ & & \sigma_x & \sigma_x & \sigma_x & & \\ \sigma_x & \sigma_x & \sigma_x & & \sigma_x & \sigma_x & \sigma_x \end{array}$$

would implement a SWAP gate.