18.435/2.111 Homework 11

Due Thursday, December 14.

1: Those wacky aliens from Cor Leonis are back. This time, they give you one of seven states in a three-dimensional space. These states are

$$\sqrt{\frac{2}{3}}\cos\frac{2k\pi}{7}\,|\,0\rangle + \sqrt{\frac{2}{3}}\sin\frac{2k\pi}{7}\,|\,1\rangle + \frac{1}{\sqrt{3}}\,|\,2\rangle\,,$$

where k ranges from 0 to 6. Your task is to figure out which of these states they've given you. This time, they won't give you a replacement if you drop the qutrit, but they will give you some help. They are willing to narrow down the choice to two possibilities. You can ask them to do this in one of two ways (called choices A, B, and C). If you take choice A, they will give you two possibilities where k differs by 1 (mod 7). If you take choice B, they will give you two possibilites where k differs by 2 (mod 7), and if you take choice C, they will give you two possibilites where k differs by 3 (mod 7). How can you accomplish the aliens' task with probability 1?

2: In the previous problem, you find that the quantum apparatus the aliens lent you is defective, and you can only make POVM measurements which have all rank 1 outcomes. Prove that you cannot always identify the correct vector.

3: A purification of a state ρ on a quantum system A is a pure state $|\,\psi\rangle$ on the joint system $A \otimes B$ so that $\mathrm{Tr}_{\,B}\,|\,\psi\rangle\langle\psi\,| = \rho$. Do problem 2.81 in Nielsen and Chuang

4: Suppose we have a CSS code encoding k qubits into n qubits that corresponds to two binary classical linear codes on n bits, $S \subset C$. The dual quantum code corresponds to $C^\perp \subset S^\perp$. Now, recall in the proof of the security of quantum key distribution, we took a translate of this code. The codewords after translation by t in bit space were, for $v \in C$,

$$|\,v + S\rangle = \frac{1}{\sqrt{|S|}}\sum_{s\in S}|\,v + s + t\rangle\,.$$

Show that when you take $H^{\otimes n}\,|\,v + S\rangle$, you get a state in the dual code translated in phase space. That is, you get a state which is in the subspace spanned by codewords

$$\left|\,w + C^\perp\right\rangle = \frac{1}{\sqrt{|C^\perp|}}\sum_{c\in C^\perp}(-1)^{c\cdot t}\,|\,w + c\rangle\,.$$

for $w \in S^\perp$.

5: In this exercise, we show that if we have a function with an irrational period, the quantum Fourier transform can still find the period of it. This is how quantum computers can find the solution to Pell's equation. Here, we use the floor and ceiling functions: $\lfloor x \rfloor$ is the largest integer $\leq x$ and $\lceil x \rceil$ is the smallest integer $\geq x$.

5a: Suppose there is a large irrational number r, with $\log_2 r \approx n$. Let P be a permutation of the numbers between 0 and $\lfloor r \rfloor$, We are given an efficiently computable function f which takes an integer x to

$$f(x) = P(\lfloor x - dr \rfloor),$$

where d is the largest integer such that $x > dr$. Show that with high probability you can obtain a state

$$\frac{1}{\sqrt{T}} \sum_{y=0}^{T-1} |\lceil ry \rceil + S\rangle$$

for some integers T and S, (here S and T may be randomly chosen during the quantum algorithm, rather than determined beforehand, although T should be large). The quantum computation should be polynomial in n.

5b: Show how to take the quantum Fourier transform of the state from 5a to obtain the first $3n$ bits of r. Some hints (I hope they are helpful): Show the states you want have high probability (rather than showing the states you don't want have low probability), and consider whether the the Fourier transform is large or small.

6: Give a quantum circuit which encodes a qubit using the quantum Hamming code given in Eqs. 10.78 and 10.79 in Nielsen and Chuang.

7a: Suppose you have three qubits. You measure their total spin in the x direction, given by the observable

$$J_x = \frac{1}{2} (\sigma_x \otimes \mathrm{id} \otimes \mathrm{id} + \mathrm{id} \otimes \sigma_x \otimes \mathrm{id} + \mathrm{id} \otimes \mathrm{id} \otimes \sigma_x)$$

and find that it is $\frac{3}{2}$. Show that the expected value of the total spin in the z direction is now 0.

7b: Suppose you have three qubits, as in 7a. You measure their total spin in the x direction and find that it is $\frac{1}{2}$. What is now the maximum possible expected value of the total spin in the z direction?

7c: Suppose you have three qubits. You project onto the 4-dimensional subspace where the total spin in the x direction is either $\frac{1}{2}$ or $\frac{3}{2}$. Show that the expected value of the total spin in the z direction can be larger than the value you found in 7b.

7d: (extra credit) What is the maximum expected value of the total spin in the z direction that you could have obtained in problem 7c.