UNM Physics 452/581: Introduction to Quantum Information, Problem Set 3, Fall 2007

Instructor: Dr. Landahl
Issued: September 12, 2007
Due: September 18, 2007

Do all of the problems listed below. Hand in your problem set at the beginning of class on the desk at the front of the classroom or after class in the box in the Physics and Astronomy main office by 5 p.m. **Please put your name and/or IQI number number on your assignment**, as well as the course number (Physics 452/581). Please show all your work and write clearly. Credit will be awarded for clear explanations as much, if not more so, than numerical answers. Avoid the temptation to simply write down an equation and move symbols around or plug in numbers. Explain what you are doing, draw pictures, and check your results using common sense, limits, and/or dimensional analysis.

3.1. Quantum safecracker

Your reputation as a world-class safecracker has brought you to the ultimate challenge: a safe with a quantum lock! The safe is in someone's office and the locking mechanism is connected rather elaborately to a single spin-1/2 qubit that has "tumblers" that allow the qubit to be rotated around the x, y, and z directions. After performing one or more rotations about these axes, pulling a lever makes a loud "click" and if the combination was correct, the safe opens. If not, the qubit gets replaced with a qubit prepared in the same initial configuration. (Suppose that the safe manufacturer has supplied the safe with an essentially inexhaustible supply of these qubits so that you couldn't use them all up in a human lifetime.)

(a) Your first guess at the combination is that it is a single rotation about one of the axes. Because the Pauli matrices X, Y, and Z are so central to spin-1/2 quantum mechanics, you try each of these first. (Who knows, maybe the safe owner chose a really easy combination!) What rotations $U(\hat{n}, \theta)$ do each of the Pauli matrices correspond to? In other words, find the angle and axis for the rotation matrix corresponding to each Pauli matrix. (*Hint*: Remember that since states are equivalent up to an overall phase, so are the rotation matrices $U(\hat{n}, \theta)$. In particular, note that U and iU correspond to the same rotation.)

(b) The simple guesses failed. Your next guess is that the combination involves just one x rotation followed by one y rotation. You try rotating about each axis by various simple angles like π, $\pi/2$, etc. One of the combinations you try is a rotation about the x axis by $\pi/2$ followed by a rotation about the y axis by $\pi/2$. (i) Write down the 2×2 unitary matrix corresponding to the net rotation this generates. (ii) What axis and angle are associated with this net rotation? [Note: there are actually two solutions, because $(\hat{n}, \theta)$ and $(-\hat{n}, -\theta)$ correspond to the same rotation matrix.] (*Hint*: First write out the 2×2 matrix for a general rotation in terms of $\hat{n}$ and θ and match its matrix components with what you got in part (i) to solve for the components of $\hat{n}$ and for θ.)

(c) You've been at this x-y rotation guessing for a while and you are starting to guess rotations that are really tiny. One of your guesses is a rotation about the x axis by ϵ followed by a rotation about the y axis by ϵ, where ϵ is a very small angle. Before you have a chance to pull the lever, you hear the footsteps of a security guard down the hall whom you know checks the safe regularly. Did I mention that your safecracking activity was illicit? Rather than pull the lever to reset the qubit, which would make a very loud "click," you opt instead to try to reset the lock by rotating the tumblers back, first about the x axis by $-\epsilon$ and then about the y axis by $-\epsilon$. After doing so and hiding under a desk, you realize that you rotated the tumblers back in the wrong order! (i) Modeling the angle ϵ as infinitesimal, use a Taylor expansion for each rotation involved and write down the 2×2 unitary gate that resulted from all four rotations you performed, to lowest nonzero order in ϵ. (ii) This net unitary gate is itself an infinitesimal rotation. About what axis is the rotation and by how much? [Note: As in part (b)(ii), there are actually two solutions.]

(d) The security guard checks the lock and doesn't notice any problems. The rotations you did were infinitesimal, after all! Deciding that the whole x-y plan is going nowhere, you decide to try some old-fashioned techniques. You open up the desk drawer in the office and you see a piece of paper with the phrase "$x + y + z$" on it. That must be the combination! What could it mean? You guess that it means that the net rotation generated by the correct combination is about the axis $\hat{n} = (\hat{x} + \hat{y} + \hat{z})/\sqrt{3}$. With a pencil and paper, you set to work figuring out rotation matrices for various angles about this axis. (i) Write down the 2×2 rotation matrix corresponding to a rotation by the angle $2\pi/3$ about this axis. (ii) Verify that this acts as the Bloch sphere rotation one would expect by showing what it does to the spin-up states in the x, y, and z directions. (iii) How could you achieve this rotation using the tumblers? (*Hint*: Compare your answer in part (i) to what you got in part (b)(i).)

You try the tumbler combination indicated in part (d)(iii) and the safe door opens. Your reputation as a master safecracker remains intact!

3.2. Bloch sphere

(a) Use the Bloch sphere representation of a qubit to show that the outer product of any qubit state $|\psi\rangle$ with itself can be expressed in the form

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + \vec{\mathbf{p}} \cdot \vec{\boldsymbol{\sigma}}),$$

where $\vec{\mathbf{p}}$ is a 3-component real vector whose length is 1, *i.e.*, $|\vec{\mathbf{p}}| = 1$. Explicitly state the components of $\vec{\mathbf{p}}$ in terms of the angles θ and φ on the Bloch sphere.

(b) After a spin-1/2 rotation $U(\hat{n}, \theta)$, the vector $\vec{\mathbf{p}}$ from part (a) gets mapped to a new vector $\vec{\mathbf{p}}'$. What is this vector in terms of $\vec{\mathbf{p}}$, $\hat{n}$ and θ? Give a geometric interpretation of the action of U on $\vec{\mathbf{p}}$. (*Hint*: It might be helpful to work out $UXU^\dagger$, $UYU^\dagger$, and $UZU^\dagger$ first.)

(c) Show that no unitary gate on a spin-1/2 particle can fix spin up and down in both the x and y directions and also interchange spin up and down in the z direction. [Note: This is an example of a spatial parity inversion transformation of the Bloch sphere.] (*Hint*: Such a gate U would act like $U|\pm\rangle_j = e^{i\theta_j^{(\pm)}}|\pm\rangle_j$ for $j = x$ and $j = y$ but like $U|\pm\rangle_j = e^{i\theta_j^{(\pm)}}|\mp\rangle_j$ for $j = z$, where $|\pm\rangle_j$ denotes the spin up and down states in the j-direction. Work out what conditions these angles would have to satisfy for consistency when all states are expressed in a single basis.)

3.3. Simon Says

Recall that the objective of Simon's problem is to evaluate the function $g : X \to Y$ with as few queries to the input as possible, where g, X, and Y are defined as follows:

$$n \in \mathbb{N}, \qquad N := 2^n, \qquad \Sigma := \mathbb{B}^n, \qquad Y := \mathbb{B}, \tag{1}$$

$$X := \{x = (x_0, \ldots, x_{N-1}) \in \Sigma^N \mid x_i = x_j \text{ iff } i = j \oplus s\} \tag{2}$$

$$g(x) := \begin{cases} 0 & s = 0^n \\ 1 & s \neq 0^n. \end{cases} \tag{3}$$

We saw in class that the deterministic query complexity of this problem is

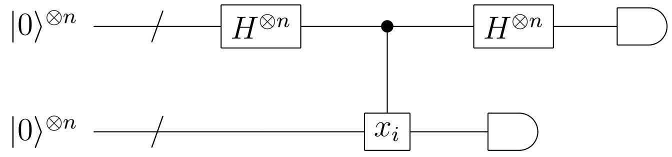
$$D(g) = \left\lceil \frac{1}{2}\sqrt{8N+1} + \frac{1}{2} \right\rceil .$$

In 1994, Daniel Simon constructed a *quantum* Monte Carlo query algorithm for this problem that uses only $\mathcal{O}(\log N)$ quantum queries, demonstrating that the quantum Monte Carlo query complexity of this problem is

$$Q_2(g) = \mathcal{O}(\log N).$$

This algorithm is now known as *Simon's algorithm*. Let's see what Simon says.

The core of Simon's algorithm is described by the following quantum circuit.



To understand Simon's algorithm, let's trace through Simon's circuit step-by-step and go over the post-processing that needs to be done to evaluate g in a Monte Carlo way.

(a) The first step of Simon's circuit is a Walsh-Hadamard transform applied to the upper "index register," initially prepared in the n-qubit state $|0\rangle^{\otimes n}$. What is the quantum state of these n qubits after this gate is applied? (*Hint*: Review your solution to problem 2.2 (h).)

(b) The next step of Simon's circuit is a quantum query. Recall that a quantum query acts jointly on the index register and the lower "letter register" as $|i\rangle|j\rangle \mapsto |i\rangle|j \oplus x_i\rangle$. What is the combined quantum state of both registers after this query?

In the next step of Simon's circuit, two steps occur in parallel: the index register undergoes another Walsh-Hadamard transform and the letter register qubits are measured. Because these operations are independent, it doesn't matter if they are performed exactly in parallel—one can happen before the other. In fact, the letter register measurement can even be deferred until the very end of the circuit. (Even better, it can be omitted entirely, but we'll keep it in for pedagogical clarity.)

(*c*) Suppose the letter register measurement happens first. This measurement is described by the projectors

$$\mathit{\Pi}_j = I^{\otimes n} \otimes |j\rangle\langle j|, \qquad j = 0, \ldots, N-1.$$

Use the Born rule to show that the post-measurement state is

$$|\psi\rangle \mapsto \begin{cases} |j\rangle|x_j\rangle, \ \text{prob}(j) = 2^{-n} & \text{if } s = 0^n, \\ \\ \frac{1}{\sqrt{2}}(|j\rangle + |j \oplus s\rangle)|x_j\rangle, \ \text{prob}(j) = 2^{-n+1} & \text{if } s \neq 0^n. \end{cases}$$

(*d*) After the measurement in part (*c*), another Walsh-Hadamard transform is applied to the index register. Show that the resulting state is

$$|\psi\rangle \mapsto \begin{cases} \dfrac{1}{2^{n/2}} \displaystyle\sum_{i=0}^{N-1} (-1)^{i \cdot j} |i\rangle|x_j\rangle & \text{if } s = 0^n, \\ \dfrac{1}{2^{(n-1)/2}} \displaystyle\sum_{s \cdot i = 0} (-1)^{i \cdot j} |i\rangle|x_j\rangle & \text{if } s \neq 0^n. \end{cases}$$

where the dot product denotes the bitwise dot product encountered in the previous problem set's problem 2.2(*g*) and j labels the outcome obtained from the measurement in part (*c*).

The final step of Simon's circuit is a measurement of the index register by the projectors $\mathit{\Pi}_i = |i\rangle\langle i| \otimes I^{\otimes n}$. From part (*c*), one can see that the outcome will be some index i that obeys $s \cdot i = 0$. (Note that when $s = 0^n$, this is automatically satisfied.) Is having such an i enough information to evaluate g? Not quite. But it turns out that if one is able to gather $n-1$ linearly independent such indices, then one *can* evaluate g. By linearly independent, I mean that none of the indices can be expressed as a bitwise sum of any combination of the other indices. If this is the case, then one has $n-1$ linear equations in n unknowns (the bits of s) that one can solve to obtain s:

$$\begin{aligned} s \cdot i_0 &= 0 \\ s \cdot i_1 &= 0 \\ &\vdots \\ s \cdot i_{n-2} &= 0. \end{aligned}$$

[Note: one might think that n equations are needed to solve for n unknowns, but the fact that this is linear algebra over $\mathbb{B}$ rather than $\mathbb{R}$ makes this not true—work out a small example to convince yourself of this if you aren't convinced.]

At least two more queries, one at $i = 0$ and one at $i = s$, are needed to verify that the s obtained by solving this set of linear equations is indeed the s defined by the problem. If

$x_0 \neq x_s$, then $s = 0^n$—the seemingly unique solution to the set of linear equations wasn't unique at all because any set of indices will satisfy them. On the other hand, if $x_0 = x_s$, then the solution to the set of linear equations is indeed unique and $s \neq 0^n$.

The upshot of these considerations is that the query complexity of Simon's algorithm hinges on how many times Simon's circuit must to be run to yield $n-1$ linearly independent indices with high confidence.

(e) Show that if Simon's circuit is run $n-1$ times, yielding indices $i_0, \ldots, i_{n-2}$ the probability that the indices are linearly independent is at least as large as

$$\prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) = 0.2887880950866\ldots > \frac{1}{4}.$$

You only have to show that it is greater than the product above, not that the product has this weird value.

Conclusion. The results of this problem show that $n+1$ calls to Simon's circuit, which corresponds to making $n+1$ quantum queries, will evaluate g with a probability greater than 25%. Not a great success rate! However, it can be boosted by repetition. For example, if the entire procedure described in parts (a) through (e) are repeated r times, the probability of not finding a linearly independent set of indices during one of the repetitions is less than $(3/4)^r$. If one chooses $r = 4$, then the overall success probability of Simon's algorithm is $0.68359\ldots$, which is greater than the $2/3$ value we used to define what it means to evaluate a function in a Monte Carlo (*i.e.*, two-sided error) way.