Introduction to Quantum Information Processing
Assignment 5
Due at 11:59pm on Friday March 25th 2013 using the LEARN dropbox, or the dropbox located outside the tutorial centre, MC 4066, BOX 2, Slot 11 (please submit a confirmation of submission online in this case)
(will constitute 10% out of the 50% assignment marks)

1. **8 marks** *Energy conservation and maintaining coherence*

   Consider a qubit where $|0\rangle$ and $|1\rangle$ have different energies E_0 and E_1, and one-qubit gates are effected using light fields containing photons with energy (roughly) equal to $E_1 - E_0$. If the light field interacting with the qubit consists of exactly n photons, then a transition from $|1\rangle$ to $|0\rangle$ will leave $n+1$ photons in the light field; a transition from $|0\rangle$ to $|1\rangle$ will leave $n-1$ photons in the light field, $|0\rangle \mapsto |0\rangle$ or $|1\rangle \mapsto |1\rangle$ leaves n photons in the light field. In other words, if we try to map $|0\rangle$ to $|0\rangle + |1\rangle$ starting with a light field with exactly n photons, the light field will be entangled with the qubit (i.e. $|0\rangle|n\rangle + |1\rangle|n-1\rangle$), preventing quantum interference in the qubit if the light is discarded.

   We generally model the light field used as being in a "coherent state", which is a special superposition of different numbers of photons. For simplicity ("coherent states" have coefficients proportional to $\alpha^n/\sqrt{n!}$), suppose our light field, before the interaction with the qubit, is in the state

   $$|\psi_k\rangle = \sum_{n=1}^{k} \frac{1}{\sqrt{k}} |n\rangle$$

   where $|n\rangle$ denotes the state with n identical photons.

   Let $\overline{H}$ be the (hypothetical) interaction (the natural interaction would have amplitudes that depend on n) between the light field and qubit that maps $|0\rangle|n\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle|n\rangle + \frac{1}{\sqrt{2}}|1\rangle|n-1\rangle$ and $|1\rangle|n\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle|n+1\rangle - \frac{1}{\sqrt{2}}|1\rangle|n\rangle$.

   (a) **3 marks** *Approximating the Hadamard gate*

   Suppose the qubit and light field start in the state $|0\rangle|\Psi_k\rangle$ and then they interact according to $\overline{H}$. Compute the density matrix of the qubit after discarding the light field. In other words, compute

   $$\rho = Tr_2(\overline{H}(|0\rangle\langle 0| \otimes |\psi_k\rangle\langle\psi_k|)\overline{H}^{\dagger})$$

   (i.e. trace out the light field register after the interaction that maps $|0\rangle|\psi_k\rangle \mapsto \overline{H}|0\rangle|\psi_k\rangle$).
   Thus show that

   $$1 - \langle +|\rho|+\rangle \in O\left(\frac{1}{k}\right)$$

where $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = H|0\rangle$ is the desired output (call this difference the "error").

(*Hint: Note that when you compute* $\overline{H}|0\rangle|\psi_k\rangle$, *the state can be written in the form* $\alpha|+\rangle|$ *something* $\rangle + \beta|junk\rangle$ *where* $|\alpha|^2 \in 1 - O(1/k)$.)

It can similarly be shown that for any one-qubit state ρ_1, *the map* $\rho_1 \mapsto \rho_2 = Tr_2(\overline{H}(\rho_1 \otimes |\psi_k\rangle\langle\psi_k|)\overline{H}^\dagger)$ *implements the ideal Hadamard gate with error in* $O(\frac{1}{k})$. *Thus if one has a large supply of copies of the state* $|\psi_k\rangle$, *for large* k, *one can perform many Hadamard gates with high precision.*

(b) **3 marks** *Phase reference*

Suppose that instead of $|\psi_k\rangle$ we are given a state we can denote by $|e^{i\phi}\psi_k\rangle$ and define as

$$|e^{i\phi}\psi_k\rangle = \frac{1}{\sqrt{k}}\sum_{n=1}^{k} e^{in\phi}|n\rangle.$$

Show that the map

$$\rho_1 \mapsto \rho_2 = Tr_2(\overline{H}(\rho_1 \otimes |e^{i\phi}\psi_k\rangle\langle e^{i\phi}\psi_k|)\overline{H}^\dagger)$$

approximates the map

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\phi}}{\sqrt{2}}|1\rangle$$
$$e^{i\phi}|1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{e^{i\phi}}{\sqrt{2}}|1\rangle$$

with error in $O(\frac{1}{k})$ on inputs $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$.

(Again, let "error" denote the difference between 1 *and* $\langle$ *ideal state*$|$ *actual state* $|$ *ideal state*

(This error bound can be shown to be the case on arbitrary one-qubit inputs.)

(c) **2 marks** *Picking a random phase reference*

Prove that

$$\sum_j |e^{i\phi_j}\psi_k\rangle\langle e^{i\phi_j}\psi_k| = \sum_{n=1}^{k}|n\rangle\langle n|$$

where the first sum is over values $\phi_j \in \{0, 2\pi/k, 2\pi 2/k, \ldots, 2\pi(k-1)/k\}$, the kth roots of 1.

In other words, one can obtain a random $|e^{i\phi_j}\psi_k\rangle$ *by simply picking a random* $|n\rangle$. *This also works if we integrate equally over all* $\phi_k \in [0, 2\pi)$.

2. *Error correction*

7 marks

Suppose we are using the 3-qubit phase-flip code and recovery operator, with error operation $\mathcal{E} : \rho \mapsto U_\theta \otimes U_\theta \otimes U_\theta \rho U_\theta^\dagger \otimes U_\theta^\dagger \otimes U_\theta^\dagger$, where $U_\theta = R_z(\theta)$ and $\sin^2(\theta/2) = p$. (In other words, a U_θ operation is applied to each qubit.)

(a) **1.5 marks**

Suppose we start with the encoded state $|+\rangle|+\rangle|+\rangle$, and then the above error occurs.

Express the resulting state $U_\theta \otimes U_\theta \otimes U_\theta|+\rangle|+\rangle|+\rangle$ as a superposition of $|+\rangle|+\rangle|+\rangle, |+\rangle|+\rangle|-\rangle, |+\rangle|-\rangle|+\rangle, |-\rangle|+\rangle|+\rangle, |+\rangle|-\rangle|-\rangle, |-\rangle|+\rangle|-\rangle, |-\rangle|-\rangle|+\rangle, |-\rangle|-\rangle|-\rangle$.

(b) **1.5 marks** Show that the probability of being in a state that will not be corrected by "majority voting" in the $\{|+\rangle, |-\rangle\}$ basis is in $O(p^2)$.

(c) Suppose we measure the stabilizers XXI and XIX.

i. **0.5 marks each**
Show that the probability of obtaining $+1$ and $+1$ is in $1 - O(p)$.
What is the resulting state of the encoded qubit in this case?
What is the resulting state of the encoded qubit after the appropriate correction is done?
Show that the resulting error probability in this case is in $O(p^3)$.

ii. **0.5 marks each**
Show that the probability of obtaining $+1$ and -1 is in $O(p)$.
What is the resulting state of the encoded qubit in this case?
What is the resulting state of the encoded qubit after the appropriate correction is done?
Show that the resulting error probability in this case is in $O(p)$.

3. *Decoherence-free subspace* **1 marks**

Find a basis for a two-dimensional subspace of two qubits that is not affected by the phase noise operation $\rho \mapsto U_\theta \otimes U_\theta \rho U_\theta^\dagger \otimes U_\theta^\dagger$, where $U_\theta = R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$.

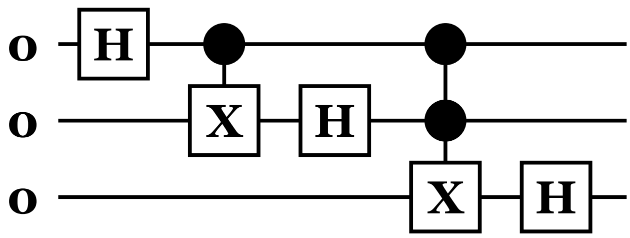
In other words, find two orthogonal 2-qubit states $|\phi_0\rangle$ and $|\phi_1\rangle$ such that, for $i = 0, 1$,

$$U_\theta \otimes U_\theta |\phi_i\rangle = e^{i\alpha}|\phi_i\rangle$$

where α is a constant.

4. $BQP \subseteq P^{\sharp P}$ **4 marks**

Consider the following circuit, with input state $|000\rangle$.



Note that, with respect to the computational basis, there are 8 computational paths taken, each with amplitude $\pm\frac{1}{\sqrt{8}}$.

For example, the path

$$|000\rangle \mapsto |100\rangle \mapsto |110\rangle \mapsto |100\rangle \mapsto |100\rangle \mapsto |101\rangle$$

is taken with amplitude $\frac{1}{\sqrt{8}}$, since the first Hadamard maps $|000\rangle$ to $|100\rangle$ with amplitude $\frac{1}{\sqrt{2}}$. Then the CNOT maps $|100\rangle$ to $|110\rangle$ with amplitude 1. Then the second Hadamard maps $|110\rangle$ to $|100\rangle$ with amplitude $\frac{1}{\sqrt{2}}$, and so on. The product of these transition amplitudes is $\frac{1}{\sqrt{8}}$.

(a) Write down the other 7 paths and the amplitude of each path.

(b) NP-hard problems can be reduced to a question of the form: Given a function $f : \{0,1\}^n \to \{0,1\}$ (computable in time polynomial in n), does there exist an input string x such that $f(x) = 1$.

The counting version of this decision problem is to output the number of inputs x such that $f(x) = 1$. The class of problems of this form is denoted $\sharp P$. These are function problems (i.e. the output is not just 'accept' or 'reject'). The class of decision problems solvable in polynomial time given an oracle for solving any $\sharp P$ problem is denoted $P^{\sharp P}$.

Note that the class BQP is equivalent to the class of languages L for which there exists a family of polynomial sized quantum circuits A_n consisting of $CNOT$, Toffoli and Hadamard gates (and each A_n can be constructed in polynomial time by a classical computer) where A_n has n input qubits and with the property that for any positive integer n and any string x of length n

- if $x \in L$ then $|\langle 00\ldots0|A_n|x\rangle|^2 \geq \frac{2}{3}$
- if $x \notin L$ then $|\langle 00\ldots0|A_n|x\rangle|^2 \leq \frac{1}{3}$

Prove that $BQP \subseteq P^{\sharp P}$. In other words, for any language $L \in BQP$, show how to decide membership in L in polynomial time using an oracle for some $\sharp P$ language.