Math 410 Intro to Quantum Computing Homework 8

Sample Solution

$\in \mathbb{C}^N$ $\quad N = 2^n$

6.1 Let $N = 2^n$, $\tilde{f} = (\tilde{f}(0), \ldots, \tilde{f}(N-1))^t$ and $f = (f(0), \ldots, f(N-1))^t$. Then

$$\Sigma_y |\tilde{f}(y)|^2 = \langle \tilde{f}|\tilde{f}\rangle = \langle \tilde{f}(y)|\underbrace{K^\dagger(x,y)\overset{I_N}{K}(x,y)}|\tilde{f}(y)\rangle = \langle f|f\rangle = \Sigma_x |f(x)|^2 \text{ as } K \text{ is unitary.}$$

6.2 (1) To get $\langle x|x\rangle = 1$, note that $\langle\psi|\psi\rangle = \mathcal{N}^2 \Sigma_x \cos^2 \frac{2\pi x}{N}$. Thus, $\Sigma_x cos^2 \frac{2\pi x}{N} = \Sigma_x \frac{\cos(\frac{4\pi x}{N})+1}{2} = \frac{N}{2}$, and hence, $\mathcal{N} = 2^{-\frac{n-1}{2}}$

$\sum_{x=0}^{N-1} w_x |x\rangle$

(2) The coefficient of $|x\rangle$ in $U_{QFT_n}|\psi\rangle$ equals $\frac{1}{\sqrt{N}\sqrt{N/2}} \Sigma_y e^{-2\pi i x y/N} \cos \frac{2\pi y}{N}$

$= \frac{1}{\sqrt{2N}} e^{-2\pi i x y/N}(e^{2\pi i y/N} + e^{-2\pi i y/N}) = \frac{1}{\sqrt{2N}}(\boxed{e^{-2\pi i(x+1)y/N} + e^{-2\pi i(x-1)y/N}})$, ✓

$\begin{bmatrix} w_0 \\ \vdots \\ w_{N-1} \end{bmatrix}$

which is nonzero if and only if $x = 1$ or $N-1$. So, the expression reduces to $\frac{1}{\sqrt{2N}} N(\delta_{x,1} + \delta_{x,N-1}) = \frac{1}{\sqrt{2}}(\delta_{x,1} + \delta_{x,N-1})$. Therefore, $U_{QFT_n}|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |N-1\rangle)$.

6.3 Let $\frac{2^n}{P} = m \in \mathbb{N}$. Apply QFT, we obtain $|\Psi'\rangle = \frac{1}{2^n}\Sigma_{x,y} e^{-2\pi i x y/2^n}|y\rangle|f(x)\rangle$.

Separating the summation over x using a arbitrary function $h(x)$, we let

$$\boxed{\Sigma_{x=0}^{2^n-1} h(x) = \Sigma_{l=0}^{P-1}\Sigma_{k=0}^{m-1} h(kP+l).}$$

Substituting, we have $|\Psi'\rangle = \frac{1}{2^n}\Sigma_{l=0}^{P-1}\Sigma_{k=0}^{m-1}\Sigma_y e^{-2\pi i l y/2^n} e^{-2\pi i k y/m}|y\rangle|f(kP+l)\rangle$

As f has period P, $f(kP+l) = f(l)$, $|\Psi'\rangle = \frac{1}{2^n}\Sigma_y \Sigma_{k=0}^{m-1} e^{-2\pi i k y/m}\Sigma_{l=0}^{P-1} e^{-2\pi i l y/2^n}|y\rangle|f(l)\rangle$.

When $y = qm, 0 \le q \le P-1$, then $\boxed{\Sigma_{k=0}^{m-1} e^{-2\pi i k y/m} = \Sigma_{k=0}^{m-1} e^{-2\pi i k q} = m;}$

When $y \ne qm$, then $\boxed{\Sigma_{k=0}^{m-1} e^{-2\pi i k y/m} = \frac{1-e^{-2\pi i y}}{1-e^{-2\pi i y/m}} = 0.}$ $\quad 1 + a + \cdots + a^k = \frac{1-a^{k+1}}{1-a}$

With that, we have $|\Psi'\rangle = \frac{m}{2^n}\Sigma_{l=0}^{P-1}\Sigma_{q=0}^{P-1} e^{-2\pi i l q/P}|qm\rangle|f(l)\rangle$.

Therefore, we can obtain $qm = \frac{q(2^n)}{P}$ for some $q \in \mathbb{Z}, 0 \le q \le P-1$.

7.1 Similar to Proposition 7.1, we have

$U_f|\phi\rangle = DR_f|\phi\rangle = D(\Sigma_{x\ne z}\omega_x|x\rangle - \Sigma_{z\in A}\omega_z|z\rangle) = \Sigma_{x\notin A}(2\bar{\omega} - \omega_x)|x\rangle + \Sigma_{z\in A}(2\bar{\omega} + \omega_z)|z\rangle$.

Alternatively, one can look at the vectors with components $|w\rangle = (w_0, \ldots, w_{N-1})^t$ and see that $|\tilde{w}\rangle = R_f(|w\rangle)$ will change the entries of $|w\rangle$ with labels in A to negative, and then $D|\tilde{w}\rangle = \frac{2}{N}\tilde{w}\sum_x |x\rangle - \tilde{w}$. Thus, the entries of $U_f|w\rangle$ has the asserted form.

$\left(\frac{2}{N}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{bmatrix} - I\right)|\hat{w}\rangle$

$x \in A \longleftrightarrow$ $\begin{bmatrix} w_0 \\ w \\ \vdots \\ w_{N-1} \end{bmatrix}$

Ref: Nov 1, 7 Class notes

7.2 By induction on $k \geq 0$. When $k = 0$, the result holds. Assume that the result holds for $k-1$. Then $U_f^k|\varphi_0\rangle = U_f|\varphi_{k-1}\rangle$. By induction assumption $|\varphi_{k-1}\rangle = (w_0, \ldots, w_{N-1})^t$, where $w_x = a_{k-1}$ if $x \in A$ and $w_x = b_{k-1}$ if $x \notin A$. Hence, $|\varphi_k\rangle = U_f(|\varphi_{k-1}\rangle)$ has two types of entries depending on whether the entries have label in A or not:

$$a_k = \frac{2}{N}((N-d)b_{k-1} - da_{k-1}) + a_{k-1} = \frac{1}{N}((N - 2d)a_{k-1} + 2(N-d)b_{k-1}),$$

$$b_k = \frac{2}{N}((N-d)b_{k-1} - da_{k-1}) - b_{k-1} = \frac{1}{N}(-2da_{k-1} + (N-2d)b_{k-1}).$$

Check:

$\begin{pmatrix} a_0 \\ b_0 \end{pmatrix} = \frac{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}{\sqrt{N}}$

Remark Note the typo in the book. We should have $a_k = \frac{1}{N}((N-2d)a_{k-1} - 2(N-d)b_{k-1})$.

7.3 Similar to proposition 7.3, we have

Let $p_k = \sqrt{d}a_k, q_k = \sqrt{N-d}b_k$. Then $\begin{bmatrix} p_k \\ q_k \end{bmatrix} = M \begin{bmatrix} p_{k-1} \\ q_{k-1} \end{bmatrix}$, where

$\begin{pmatrix} p_0 \\ q_0 \end{pmatrix} = \frac{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}{\sqrt{N}}$

$$M = \begin{bmatrix} (N-2d)/N & 2\sqrt{N-d}/N \\ -2\sqrt{N-d}/N & (N-2d)/N \end{bmatrix} = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{bmatrix}.$$

$\begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix}^k = \begin{pmatrix} \cos k\varphi & \sin k\varphi \\ -\sin k\varphi & \cos k\varphi \end{pmatrix}$

Then $\begin{bmatrix} p_k \\ q_k \end{bmatrix} = M^k \begin{bmatrix} p_0 \\ q_0 \end{bmatrix} = \begin{bmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{bmatrix} \begin{bmatrix} \sin\theta \\ \cos\theta \end{bmatrix} = \begin{bmatrix} \sin[(2k+1)\theta] \\ \cos[(2k+1)\theta] \end{bmatrix}$

As $a_k = \frac{1}{\sqrt{d}}p_k, b_k = \frac{1}{\sqrt{N-d}}q_k$ we have $a_k = \frac{1}{\sqrt{d}}\sin[(2k+1)\theta], b_k = \frac{1}{\sqrt{N-d}}\cos[(2k+1)\theta]$.

will yield the correct correspondence $\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ to $\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}$

7.4 Similar to proposition 7.4, we have

Define $\tilde{m}$ by $(2\tilde{m}+1)\theta = \frac{\pi}{2} \to \tilde{m} = \frac{\pi}{4\theta} - \frac{1}{2}$. We see $|\tilde{m} - m| \leq \frac{1}{2}$ as $m = \lfloor \frac{\pi}{4\theta} \rfloor$.

Then $|(2m+1)\theta - (2\tilde{m}+1)\theta| = |(2m+1)\theta - \frac{\pi}{2} \leq \theta$.

Note that $\theta \sim \frac{d}{\sqrt{N}}$ is small when $N \gg 1$ and $\sin x$ is monotonically increasing in neighborhood of $x = 0$. Thus, $0 < \sin|(2m+1)\theta - \frac{\pi}{2}| < \sin\theta$ or $\cos^2|(2m+1)\theta| \leq \sin^2\theta = \frac{d}{N}$.

Hence, $P_{m,z} = \sin^2[(2m+1)\theta] = 1 - \cos^2[(2m+1)\theta] \geq 1 - \frac{d}{N}$ asserted in (7.47)

Eventually, $m = \lfloor \frac{\pi}{4\theta} \rfloor \leq \frac{\pi}{4\theta} \leq \frac{\pi}{4}\sqrt{\frac{N}{d}}$; so, the operation time of m is $O(\sqrt{\frac{N}{d}})$.

$\rho = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \\ \phi & \phi \end{bmatrix} = \frac{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}{2}$

$\rho_S = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \rightarrow \frac{I_2}{2} = \frac{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}{2}$

$L(\rho) = \left(\frac{tr \rho}{2}\right) I_2$

Depolarizing Channel

The depolarizing channel is defined by

$$\mathcal{E}(\rho_S) = (1-p)\rho_S + pI/2, \qquad 0 \le p \le 1.$$

The input state ρ_S is sent to a maximally mixed state $I/2$ with a probability p, remains unchanged with a probability $1-p$. The Choi/Kraus operators are: $E_0 = \sqrt{1-3p/4}I$ and $E_k = \sqrt{p/4}\sigma_k$ for $k = x, y, z$. Let $p' = 3p/4$. Then

$$\boxed{\mathcal{E}(\rho_S) = \underbrace{(1-p')}_{I \cdot I}\rho_S + (p'/3)\sum_k \sigma_k \rho_S \sigma_k^{\dagger}.}$$

$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

This can be modeled by $\quad = (\sqrt{1-p'} \cdot I)\rho_S(\sqrt{1-p'}\, I)^{\dagger}$

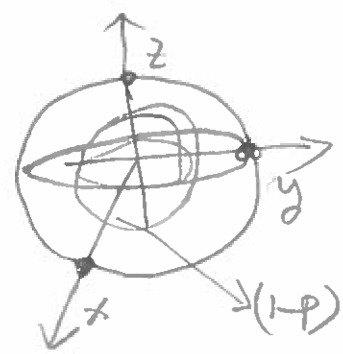
$$\rho_S \mapsto V(\rho_S \otimes I/2 \otimes [(1-p)|0\rangle\langle 0| + p|1\rangle\langle 1|])V^t = (1-p)\rho_S \otimes (I/2) \otimes |0\rangle\langle 0| + p\,(I/2) \otimes \rho_S |1\rangle\langle 1|$$

with $V = I_4 \otimes |0\rangle\langle 0| + U_{SWAP}|1\rangle\langle 1|$.

Use the block sphere representation:

$$\boxed{\mathcal{E}(\rho_S) = \frac{1}{2}\left(I + (1-p)\sum_k c_k \sigma_k\right).}$$

So, the block sphere shrinks in the $1x, y, z$ directions by a factor of $1-p$.



$\mathcal{E}\left(\frac{I}{2} + c_x\sigma_x + c_y\sigma_y + c_z\sigma_z\right)$

ϕ

$= \left(\qquad \right)$

$\mathcal{E}\left(\frac{I}{2} + \frac{\sigma_x}{2}\right)$

$\mathcal{E}\left(\frac{I}{2} + \frac{\sigma_y}{2}\right)$

$\mathcal{E}\left(\frac{I}{2} + \frac{\sigma_z}{2}\right).$

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

$$\| $$

$$E_0^\dagger E_0 + E_1^\dagger E_1 = I_2$$

Amplitude-Damping Channel

The amplitude-damping channel is defined by

$$\boxed{\mathcal{E}(\rho_S) = E_0 \rho_S E_0^\dagger + E_1 \rho_S E_1^\dagger, \qquad E_0 = \begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{pmatrix}, \; E_1 = \sqrt{p}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}.}$$

It describes the decay of the qubit from $|1\rangle$ to $|0\rangle$ with probability p.

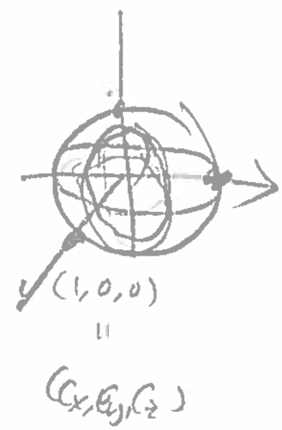
Use the block sphere representation:

$$\mathcal{E}(\rho_S) = \frac{1}{2}\left(I + \sqrt{1-p}c_x\sigma_x\sqrt{1-p}c_y\sigma_y + (p + (1-p)c_z)\sigma_z\right).$$

So, the block sphere shrinks in the x and y directions by a factor of $\sqrt{1-p}$, and shrinks in the z direction by a factor of $1-p$ and then shift to the north pole by p.

$$\rho_S = \frac{1}{2}\left(I + c_x\sigma_x + c_y\sigma_y + c_z\sigma_z\right)$$

$$\mathcal{E}(\rho_S) = \frac{1}{2}\left(I + \sqrt{1-p}\, c_x\sigma_x + \sqrt{1-p}\, c_y\sigma_y + [p + (1-p)c_z]\,\sigma_z\right)$$



9.4 Lindblad Equation

Recall the Lioville-von Neumann equation for a closed system

$$\frac{\partial \rho_S}{\partial t} = \frac{1}{i}[H, \rho_S].$$

For an open system, it becomes

$$\boxed{\rho_S(t) = \mathrm{Tr}_E(U(t)(\rho_S \otimes \rho_E)U(t)^\dagger].}$$

Thus,

$$\frac{\partial \rho_S}{\partial t} = \frac{\partial \rho_S}{\partial t}\mathrm{Tr}_E(U(t)(\rho_S \otimes \rho_E)U(t)^\dagger] = \frac{1}{i}\mathrm{Tr}_E[H, U(t)(\rho_S \otimes \rho_E)U(t)^\dagger].$$

Assume that the system relies very little about previous history, the we use the **Markovian approximation**, and the equation will be of the form

$$\boxed{\frac{\partial \rho_S}{\partial t}} = \mathcal{L}\rho_S(t) = \frac{1}{i}[\tilde{H}, \rho_S] + \sum_{K=1}^{N} \gamma_K \left(L_k \rho_S L_k^\dagger - \frac{1}{2} L_k^\dagger L_k \rho_S - \frac{1}{2} \rho_S L_k^\dagger L_k \right).$$

This is known as the Lindblad equation; the operators L_k are known as the Lindblad operators.

Quantum error correction

10.1 Classical quantum error correction

In classical communication, suppose a noisy channel will change x to $x \oplus 1$ for $x = 0, 1$ with a probability $p < 1/2$. One may send xxx instead of x and use maximum likelihood decoding so that the probability of correct transmission for one bit is the sum of the probabilities of x sent to xxx, $xx\hat{x}$, $x\hat{x}x$, $\hat{x}xx$:

$$\boxed{(1-p)^3 + 3p(1-p)^2} = (1-p)^2(1+2p) >> \overset{1-p}{\cancel{p}}$$

If Alice send XXX, then Bob decodes the message as XXX using the above scheme. i.e. $(1-p)^3 + 3p(1-p)^2 = (1-p)^2(1+2p)$

Without encoding, Bob will correctly decode with a prob. $1-p$

$(1-p)(1+2p)$
$= 1 + p - 2p^2 > 1$
$\therefore (1-p)^2(1+2p)$
$> (1-p)$

0, 1

$C = \{(000), (111)\}$
$\subseteq \mathbb{Z}_2^3$ with 8 elements

10.2 Quantum error correction

10.2.1 Bit-Flip QECC

We cannot copy qubit because of no-cloning.

not a copy of $|\psi\rangle = a|0\rangle + b|1\rangle$.

"copy" means $|\psi\rangle|00\rangle = |\psi\rangle|\psi\rangle|\psi\rangle$

$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix}$

But, we can encode $|\psi\rangle = a|0\rangle + b|1\rangle$ as $|\psi\rangle_L = a|000\rangle + b|111\rangle$ using $CNOT$ gates on $|\psi\rangle|00\rangle$.

Then the set of **code words** is

$$\mathbf{C} = \{a|000\rangle + b|111\rangle : a, b \in \mathbf{C}, |a|^2 + |b|^2\}.$$

$a|000\rangle + b|111\rangle$

The QECC scheme can be done in the following steps.

- Encode $|\psi\rangle = a|0\rangle + b|1\rangle$ as $|\psi\rangle_L = a|000\rangle + b|111\rangle \in \mathbf{C}$.
- Transmit via the quantum channel.

  $\mathcal{E}(\rho) = (1-3p)\rho + p(X \otimes I \otimes I)\rho(X \otimes I \otimes I)^\dagger + p(I \otimes X \otimes I)\rho(I \otimes X \otimes I)^\dagger + p(I \otimes I \otimes X)\rho(I \otimes I \otimes X)^\dagger + p^2(\cdots) + p^3$

  $\left\{ \rho = \begin{bmatrix} a \\ 0 \\ \vdots \\ 0 \\ b \end{bmatrix} : a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1 \right\}$
- Apply error syndrome detection and correction

  * Suppose $|x_1x_2x_3\rangle$ is received.

  * Add two ancillas $|AB\rangle$ with $A = |x_1 \oplus x_2\rangle$ and $B = |x_1 + x_3\rangle$ to detect the **(error) syndrome**.

  * Apply correction to correct $|\psi\rangle_L$ accordingly.
- Reversing the encoding step, one gets $|\psi\rangle$.

Bit-flip Channel.

$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto X\begin{pmatrix} a \\ b \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$