Quantum Information Theory HW-1

Solutions by Samarth Kashyap

1. $P(r=1 \mid s=0) = p$

$P(r=0 \mid s=1) = q$

(a) Let $P(s=0) = a$.

$$P(r=0) = q(1-a) + (1-p)a = (1-p-q)a + q$$

$$P(r=1) = pa + (1-q)(1-a) = (p+q-1)a + 1 - q$$

$$P(r=0, s=0) = (1-p)a \qquad P(r=0, s=1) = q(1-a)$$

$$P(r=1, s=0) = pa \qquad P(r=1, s=1) = (1-q)(1-a)$$

$$H(r|s) = P(s=0)\, H(r|s=0) + P(s=1)\, H(r|s=1)$$

$$= a\left[-p\log p - (1-p)\log(1-p)\right] + (1-a)\left[-q\log q - (1-q)\log(1-q)\right]$$

$$= a \log \frac{q^q (1-q)^{1-q}}{p^p (1-p)^{1-p}} - \log q^q (1-q)^{1-q}$$

$$H(r) = -\left[(1-p-q)a + q\right] \log \left[(1-p-q)a + q\right]$$

$$+ \left[(1-p-q)a + q - 1\right] \log \left[(p+q-1)a + 1 - q\right]$$

$$= \left[(1-p-q)a + q\right] \log \left[\frac{1}{(1-p-q)a+q} - 1\right]$$

$$- \log\left[1 - (1-p-q)a - q\right]$$

$$I(r;s) = H(r) - H(r|s)$$

$$= \left[(1-p-q)a + q\right] \log \left[\frac{1}{(1-p-q)a+q} - 1\right]$$

$$- \log\left[1 - (1-p-q)a - q\right]$$

$$- a \log \frac{q^q (1-q)^{1-q}}{p^p (1-p)^{1-p}} + \log q^q (1-q)^{1-q}$$

$$C = \max_{a} I(r;s)$$

$$\frac{dI(r;s)}{da} = (1-p-q)\log\left[\frac{1}{(1-p-q)a+q} - 1\right]$$

$$- \log \frac{q^q(1-q)^{1-q}}{p^p(1-p)^{1-p}} = 0$$

Writing $\gamma = \left(\frac{q^q(1-q)^{1-q}}{p^p(1-p)^{1-p}}\right)^{\frac{1}{1-p-q}}$

$$\frac{1}{(1-p-q)a+q} = 1+\gamma$$

$$a^* = \left(\frac{1}{1+\gamma} - q\right)\frac{1}{(1-p-q)}$$

$$C = \left[(1-p-q)a^* + q\right] \log\left[\frac{1}{(1-p-q)a^* + q} - 1\right]$$

$$- \log\left[1 - (1-p-q)a^* - q\right]$$

$$- a^* \log \frac{q^q (1-q)^{1-q}}{p^p (1-p)^{1-p}} + \log q^q (1-q)^{1-q}$$

$$= \frac{1}{1+\gamma} \log \gamma - \log \frac{\gamma}{1+\gamma}$$

$$- \left(\frac{1}{1+\gamma} - q\right) \log \gamma + \log q^q (1-q)^{1-q}$$

$$= (q-1) \log \gamma + \log(1+\gamma) + \log q^q (1-q)^{1-q}$$

$$= \log\left[\gamma^{q-1} (1+\gamma) q^q (1-q)^{1-q}\right]$$

$$C = \log(1+\gamma) - \frac{1-q}{1-p-q}\left(h(p) - h(q)\right) - h(q)$$

(b) $P_e(0) = 3p^2(1-p) + p^3$

$P_e(1) = 3q^2(1-q) + q^3$

$P_e = p(s=0)\,P_e(0) + p(s=1)\,P_e(1)$

$P_e = a(3p^2 - 2p^3) + (1-a)(3q^2 - 2q^3)$

(c) With 2 concatenations,

$P_e^{(2)} = 3P_e^2(1-P_e) + P_e^3$

where P_e is as in (b)

$P_e^{(2)} \sim O\left(a^2(p^2-q^2)^2\right)$

$P_e^{(n)} \sim O\left(a^{2^{n-1}}(p^2-q^2)^{2^{n-1}}\right)$

w.r.t block length $l = 3^n$,

$P_e(l) \sim O\left(a^{2^{\log_3 l - 1}}(p^2-q^2)^{2^{\log_3 l - 1}}\right)$

$$= \mathcal{O}\left(\left(a(p^2-q^2)\right)^{l^{\log_3 2}/2} \right)$$

$$E_r(l) \sim \mathcal{O}\left(\sqrt{l}\right)$$

2.

3.5.4

$$H_1 H_2 \,\mathrm{CNOT}\, H_1 H_2 = |+\rangle\langle +| \otimes \mathbb{1} + |-\rangle\langle -| \otimes Z$$

$$H = |0\rangle\langle +| + |1\rangle\langle -|$$

$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$

$$H_1 H_2 \,\mathrm{CNOT} = |+\rangle\langle 0| \otimes H + |-\rangle\langle 1| \otimes H X$$

with $XH = |1\rangle\langle +| + |0\rangle\langle -|$,

$H_1 H_2 \, CNOT \, H_1 H_2$

$$= |+\rangle\langle+| \otimes \mathbb{1} + |-\rangle\langle-| \otimes \left(|-\rangle\langle+| + |+\rangle\langle-| \right)$$

$|-\rangle\langle+| + |+\rangle\langle-|$ is the Z gate as it flips the $|+\rangle$, $\langle-|$ basis.

3.5.5

$$CNOT_{10} = \left(\mathbb{1} \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| \right) \otimes \mathbb{1}$$

$$CNOT_{12} = \mathbb{1} \otimes \left(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X \right)$$

$$CNOT_{10}\, CNOT_{12} = \mathbb{1} \otimes |0\rangle\langle 0| \otimes \mathbb{1} + X \otimes |1\rangle\langle 1| \otimes X$$

$$CNOT_{12}\, CNOT_{10} = \mathbb{1} \otimes |0\rangle\langle 0| \otimes \mathbb{1} + X \otimes |1\rangle\langle 1| \otimes X$$

$\therefore$ They commute.

3.5.6

$$CNOT_{01} = \left(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X\right) \otimes \mathbb{1}$$

$$CNOT_{21} = \mathbb{1} \otimes \left(\mathbb{1} \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|\right)$$

$$CNOT_{01}\, CNOT_{21} = |0\rangle\langle 0| \otimes \left(\mathbb{1} \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|\right)$$

$$+ |1\rangle\langle 1| \otimes \left(X \otimes |0\rangle\langle 0| + \mathbb{1} \otimes |1\rangle\langle 1|\right)$$

$$CNOT_{21}\, CNOT_{01} = \left(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X\right) \otimes |0\rangle\langle 0|$$

$$+ \left(|0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes \mathbb{1}\right) \otimes |1\rangle\langle 1|$$

We can expand & compare the terms.

3.5.13

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\Phi_{zx}\rangle = (Z^z X^x \otimes \mathbb{1})|\Phi^+\rangle$$

$$= \frac{Z^z}{\sqrt{2}}\left(|x0\rangle + |\bar{x}1\rangle\right)$$

$$= \frac{Z^z}{\sqrt{2}}\left(|0x\rangle + |1\bar{x}\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0x\rangle + (-1)^z|1\bar{x}\rangle\right)$$

$$\langle\Phi_{z_1x_1}|\Phi_{z_2x_2}\rangle = \frac{1}{2}\left(\langle x_1|x_2\rangle + (-1)^{z_1+z_2}\langle\bar{x}_1|\bar{x}_2\rangle\right)$$

$$= \delta_{x_1,x_2}\ \frac{1+(-1)^{z_1+z_2}}{2}$$

$$\langle\Phi_{z_1x_1}|\Phi_{z_2x_2}\rangle = \delta_{x_1,x_2}\,\delta_{z_1,z_2}$$

3.

(2) $$\langle \alpha | \beta \rangle = e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n=0}^{\infty} \frac{(\alpha^* \beta)^n}{n!}$$

$$= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} e^{\alpha^* \beta}$$

$$\langle \alpha | \beta \rangle = \exp\left(\frac{2\alpha^* \beta - |\alpha|^2 - |\beta|^2}{2} \right)$$

$\therefore$ They are not orthogonal.

(1) $$a|\alpha\rangle = \alpha|\alpha\rangle$$

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

$$\langle m a^\dagger | \alpha \rangle = \langle m | a \alpha \rangle$$ where $m \in \mathbb{Z}^+$

$$\sqrt{m+1}\,\langle m+1|\alpha\rangle = \alpha\,\langle m|\alpha\rangle$$

By orthogonality,

$$\sqrt{m+1}\;\frac{\alpha^{m+1}}{\sqrt{(m+1)!}}\langle m+1|m+1\rangle = \alpha.\;\frac{\alpha^{m}}{\sqrt{m!}}\langle m|m\rangle$$

$$\langle m+1|m+1\rangle = \langle m|m\rangle$$

$\langle n|n\rangle = 1$ (Can normalize without consequence)

$$\therefore \sum_{n=0}^{\infty}|n\rangle\langle n| = \mathbb{1}$$

(3) $$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

$$\langle\alpha|a^{\dagger}a|\alpha\rangle = \langle a\alpha|a\alpha\rangle$$

$$= \alpha^{*}\alpha\,\langle\alpha|\alpha\rangle$$

$$\langle\alpha|\alpha\rangle = e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{(\alpha^*\alpha)^n}{n!} = 1.$$

$$\therefore \langle\alpha|N|\alpha\rangle = |\alpha|^2$$

$$\langle\alpha|(a^\dagger a)^2|\alpha\rangle = \langle\alpha|a^\dagger a a^\dagger a|\alpha\rangle$$

$$= \alpha\langle\alpha|a^\dagger(1+a^\dagger a)|\alpha\rangle$$

$$= \alpha\langle\alpha|a^\dagger + a^{\dagger 2} a|\alpha\rangle$$

$$= \alpha\left[\langle a\alpha|\alpha\rangle + \alpha\langle a\alpha|a^\dagger|\alpha\rangle\right]$$

$$= \alpha(\alpha^* + \alpha\alpha^{*2})$$

$$= |\alpha|^2 + |\alpha|^4$$

$$\sigma_N^2 = \langle\alpha|N^2|\alpha\rangle - \langle\alpha|N|\alpha\rangle^2$$

$$\sigma_N^2 = |\alpha|^2$$

(d) $\hat{x} = \sqrt{\frac{\hbar}{2m\omega}}\left(a + a^\dagger\right)$

$$\hat{p} = -i\sqrt{\frac{\hbar m\omega}{2}}\left(a - a^\dagger\right)$$

$$\langle \alpha | x | \alpha \rangle = \sqrt{\frac{\hbar}{2m\omega}}\left(\alpha + \alpha^*\right)$$

$$\langle \alpha | p | \alpha \rangle = -i\sqrt{\frac{\hbar m\omega}{2}}\left(\alpha - \alpha^*\right)$$

$$\langle \alpha | x^2 | \alpha \rangle = \frac{\hbar}{2m\omega}\langle \alpha | a^2 + a^{\dagger 2} + a a^\dagger + a^\dagger a | \alpha \rangle$$

$$= \frac{\hbar}{2m\omega}\langle \alpha | a^2 + a^{\dagger 2} + 2a^\dagger a + 1 | \alpha \rangle$$

$$= \frac{\hbar}{2m\omega}\left(\alpha^2 + \alpha^{*2} + 2|\alpha|^2 + 1\right)$$

$$= \frac{\hbar}{2m\omega}\left[(\alpha+\alpha^*)^2+1\right]$$

$$\langle\alpha|p^2|\alpha\rangle = -\frac{\hbar m\omega}{2}\langle\alpha|a^2+a^{\dagger 2}-aa^\dagger-a^\dagger a|\alpha\rangle$$

$$= \frac{-\hbar m\omega}{2}\langle\alpha|a^2+a^{\dagger 2}-2a^\dagger a-1|\alpha\rangle$$

$$= -\frac{\hbar m\omega}{2}\left(\alpha^2+\alpha^{*2}-2|\alpha|^2-1\right)$$

$$= -\frac{\hbar m\omega}{2}\left[(\alpha-\alpha^*)^2-1\right]$$

$$\sigma_x^2 = \langle\alpha|x^2|\alpha\rangle - \langle\alpha|x|\alpha\rangle^2$$

$$= \frac{\hbar}{2m\omega}$$

$$\sigma_p^2 = \frac{\hbar m\omega}{2}$$

$$\sigma_x^2 \sigma_p^2 = \frac{\hbar^2}{4}$$

which satisfies the uncertainty principle.

4.

(a)

If $\exists$ a universal deleter D such that

$$D|\psi\rangle|\psi\rangle|a\rangle = |\psi\rangle|0\rangle|b\rangle$$

writing $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

$$D|\psi\rangle|\psi\rangle|a\rangle = D\left(\alpha^2|00\rangle + \beta^2|11\rangle + \alpha\beta\left(|01\rangle + |10\rangle\right)\right)|a\rangle$$

$$= \alpha^2|00b_0\rangle + \beta^2|10b_1\rangle + \alpha\beta|00b_2\rangle + \alpha\beta|10b_3\rangle$$

$$= \alpha|00\rangle\left(\alpha|b_0\rangle + \beta|b_2\rangle\right) + \beta|10\rangle\left(\beta|b_1\rangle + \alpha|b_3\rangle\right)$$

$$D|\psi\rangle|\psi\rangle|a\rangle = |\psi\rangle|0\rangle|b\rangle$$

Equating,

$$|\psi\rangle|b\rangle = \alpha|0\rangle\left(\alpha|b_0\rangle + \beta|b_2\rangle\right) + \beta|1\rangle\left(\beta|b_1\rangle + \alpha|b_3\rangle\right)$$

For this to hold,

$$\alpha|b_0\rangle + \beta|b_2\rangle = \beta|b_1\rangle + \alpha|b_3\rangle = |b\rangle$$

Since $|b\rangle$ is normalized and $|\alpha|^2 + |\beta|^2 = 1$, $|b_0\rangle$ & $|b_2\rangle$, and $|b_1\rangle$ & $|b_3\rangle$ are orthogonal.

$$\therefore |b_0\rangle = |b_3\rangle, \quad |b_1\rangle = |b_2\rangle$$

$$|b\rangle = \alpha|b_0\rangle + \beta|b_1\rangle$$

Thus the state $|\psi\rangle$ can be obtained from $|b\rangle$ via the operator $|0\rangle\langle b_0| + |1\rangle\langle b_1|$ and the states $|b_0\rangle$ & $|b_1\rangle$ can be known by applying D on $|00a\rangle$ and $|11a\rangle$ respectively.

(2)

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

But also,

$$|\Phi^+\rangle = \frac{|++\rangle + |--\rangle}{\sqrt{2}}$$

If A measures in computational basis, the state collapses to either $|00\rangle$ or $|11\rangle$. If B measures in the computational basis, he gets either $|0\rangle$ with probability 1 or $|1\rangle$ with probability 1.

If A measures in X-basis, the state collapses to either $|++\rangle$ or $|--\rangle$. If B measures in the computational basis, he gets $|0\rangle$ or $|1\rangle$, each with probability $1/2$.

However, B can only make one measurement on the single ebit he has access to.

If B has a cloner, he can clone his ebit:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \to \frac{|0\rangle_A |0\rangle_B^{\otimes n} + |1\rangle_A |1\rangle_B^{\otimes n}}{\sqrt{2}}$$

$$\frac{|++\rangle + |--\rangle}{\sqrt{2}} \to \frac{|+\rangle_A |+\rangle_B^{\otimes n} + |-\rangle_A |-\rangle_B^{\otimes n}}{\sqrt{2}}$$

Note that

$$\frac{|0\rangle_A |0\rangle_B^{\otimes n} + |1\rangle_A |1\rangle_B^{\otimes n}}{\sqrt{2}} \neq \frac{|+\rangle_A |+\rangle_B^{\otimes n} + |-\rangle_A |-\rangle_B^{\otimes n}}{\sqrt{2}}$$

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{\sum_{k=0}^{2^n} |k\rangle}{2^{n/2}}$$

$$\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{\sum_{k=0}^{2^n} (-1)^k |k\rangle}{2^{n/2}}$$

$\Rightarrow$ Violates linearity of quantum ops. But we will continue.

Now, after A measures her ebit in the X/Z basis, B can measure his register. If he gets $|0\rangle^{\otimes n}$ or $|1\rangle^{\otimes n}$ he instantly knows A measured in Z basis. If he measures anything else, A measured in X basis.

5. Let

$$P(x_{i+1} = 1 \mid x_i = 0) = p.$$

We have

$$P(x_{i+1} = 0 \mid x_i = 1) = 1 - p$$

$$P(x_{i+1} = 0 \mid x_i = 1) = 1$$

$$P(x_{i+1} = 1 \mid x_i = 1) = 0$$

We can model this as a Markov chain with transition matrix

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

This has stationary distribution

$$\begin{pmatrix} \frac{1}{2-p} & \frac{1-p}{2-p} \end{pmatrix}$$

Which leads to the entropy rate

$$H(x^{(n)}) = \frac{1}{2-p} H(p)$$

The entropyrate is maximized by

$$\frac{dH(x^{(n)})}{dp} = 0 \Rightarrow \frac{1}{2-p} \log\left(\frac{1-p}{p}\right) + \frac{H(p)}{(2-p)^2} = 0$$

$$\left(\frac{1-p}{p}\right)^{2-p} = p^{p}(1-p)^{1-p}$$

$$p^2 + p - 1 = 0$$

$$p^* = \frac{-1+\sqrt{5}}{2}$$

And the maximum entropy rate is

$$H^*(x^{(n)}) = \frac{1}{2-p^*} H(p^*)$$

$$\approx 0.694$$

So, the typical set size is bounded by

$$(1-\varepsilon)\, 2^{n(H^*(x^{(n)})-\varepsilon)} \le |T_\varepsilon^{(n)}| \le 2^{n(H^*(x^{(n)})+\varepsilon)}$$

and tends towards

$$2^{nH^*(x^{(n)})} = 1.618^n$$

at large n.