

Quantum Information Theory HW-1

Solutions by Samarth Kashyap

$$1. P(r=1 | s=0) = p$$

$$P(s=0 | s=1) = q$$

$$(2) \text{ let } P(s=0) = a.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$C = \max_a I(r, s)$$

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

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

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

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

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

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

$$- \log [1 - (1-p-q)^{a^*-q}]$$

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

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

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

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

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

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

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

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

$$p_e = p(s=0) p_e(0) + p(s=1) p_e(1)$$

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

(c) With l concatenations,

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

where p_e is as in (b)

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

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

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

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

$$= O\left((a(p^2 - q^2))^{1/2} g^2/2\right)$$

$$E_r(l) \sim O(\sqrt{l})$$

2.

3.5.4

$$H_1 H_2 \text{CNOT} H_1 H_2 = |+\rangle\langle+| \otimes I + |-\rangle\langle-| \otimes Z$$

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

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

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

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

$$H_1 H_2 CNOT H_1 H_2$$

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

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

3.5.5

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

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

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

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

$\therefore$ They commute.

3.5.6

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

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

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

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

We can expand & compare the terms.

3.5.13

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

$$|\hat{\Phi}_{2x}\rangle = (Z^2 X^x \otimes 1) |\hat{\Phi}^+\rangle$$

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

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

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

$$\langle \hat{\Phi}_{2,x_1} | \hat{\Phi}_{2,x_2} \rangle = \frac{1}{2} \left(\langle x_1 | x_2 \rangle + (-1)^{z_1+z_2} \langle \bar{x}_1 | \bar{x}_2 \rangle \right)$$

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

$$\delta_{x_1 x_2} \delta_{z_1 z_2}$$

$$\langle \hat{\Phi}_{2,x_1} | \hat{\Phi}_{2,x_2} \rangle =$$

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.

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

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

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

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

By orthonormality,

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

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

$$\langle n | n \rangle = 1 \quad (\text{Can normalize without consequence})$$

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

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

$$\begin{aligned} \langle \alpha | a^\dagger a | \alpha \rangle &= \langle a \alpha | a \alpha \rangle \\ &= \alpha^* \alpha \langle \alpha | \alpha \rangle \end{aligned}$$

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

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

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

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

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

$$= \alpha \left[\langle \alpha | a^\dagger | \alpha \rangle + \alpha \langle \alpha | a^{\dagger 2} | \alpha \rangle \right]$$

$$= \alpha \left(\alpha + \alpha \alpha^2 \right)$$

$$= |\alpha| + |\alpha|^3$$

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

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

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

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

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

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

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

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

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

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

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

$$a^{\dagger 2} - a a^\dagger - 1 | \alpha \rangle$$

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

$$- 2|\alpha|^2 - 1)$$

$$= - \frac{\hbar m \omega}{2} (\alpha^2 + \alpha^{\dagger 2})$$

$$)^2 - 1]$$

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

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

$$\sigma_x^2$$

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

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

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

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

which satisfies the uncertainty principle.

4.

(a)

$\exists$ a universal deleter D such that

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

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

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

$$= \alpha^2|00b_0\rangle + \beta^2|11b_1\rangle + \alpha\beta|00b_2\rangle + \alpha\beta|10b_3\rangle$$

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

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

Equating,

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

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 $|\alpha|^2 + |\beta|^2 = 1$, $|b_0\rangle \perp |b_2\rangle$, and $|b_1\rangle \perp |b_3\rangle$ 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 $|b_0\rangle \perp |b_1\rangle$ 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 $\frac{1}{2}$.

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

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

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}}$$

$$\frac{|++\rangle + |--\rangle}{\sqrt{2}} \rightarrow \frac{|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B}{\sqrt{2}}$$

Note that

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

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

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

$\Rightarrow$ 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

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

We have

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

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

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

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 entropy rate is maximized by

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

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

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

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

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

$$(1-\epsilon) 2^{n(H^*(x^{(n)}) - \epsilon)} \leq |\mathcal{A}_\epsilon^{(n)}| \leq 2^{n(H^*(x^{(n)}) + \epsilon)}$$

and tends to wards

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

at large n .