Solutions to Exam # 1

SSG

P 1.1) Alice is communicating to Bob using quantum states. Eve is wiretapping this through unitary interactions via an ancilla. It is clear that if Eve can distinguish the states, then she can infer the information. Let the states of Alice be $|a\rangle^A, |b\rangle^A$. Let the states of Alice be $\langle a|b\rangle^A \neq 0$ i.e., they need not be orthogonal states. Let the channel action be $\mathcal{U}^{AE\to BE}$ as follows:

$$\mathcal{U}^{AE\to BE}|a\rangle^A|0\rangle^E = |a\rangle^B|\phi\rangle^E \quad \text{—— (1)}$$

$$\mathcal{U}^{AE\to BE}|b\rangle^A|0\rangle^E = |b\rangle^B|\psi\rangle^E \quad \text{—— (2)}$$

Taking the inner products over (1) and (2)

$$\left(\mathcal{U}^{AE\to BE}|a\rangle^A|0\rangle^E\right)^{\dagger}\left(\mathcal{U}^{AE\to BE}|b\rangle^A|0\rangle^E\right)$$

$$= \underbrace{\langle a|b\rangle^A}_{\neq 0}\underbrace{\langle 0|0\rangle^E}_{1} = \underbrace{\langle a|b\rangle^B}_{\neq 0}\langle\phi|\psi\rangle^E$$

$$\langle\phi|\psi\rangle = 1 \quad \text{—— (A)}$$

$\Longrightarrow$ For distinguishability, $\langle\phi|\psi\rangle = 0$, leading to a conclusion that Eve cannot distinguish the states unless she disturbs to violate (A).

Consider $\mathcal{E} = \{(\frac{1}{4}, |0\rangle), (\frac{3}{4}, |+\rangle)\}$

P1.2) Clearly $\langle 0|+\rangle \neq 0$

The Shannon entropy (classically)

is $H_{Sh} = -\frac{1}{4}\log_2\left(\frac{1}{4}\right) - \frac{3}{4}\log_2\left(\frac{3}{4}\right)$

$= 0.811$ bits.

$$\rho = \frac{1}{4}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{3}{4}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{5}{8} & \frac{3}{8} \\ \frac{3}{8} & \frac{3}{8} \end{pmatrix} \quad \text{——— } (1)$$

Solving for the eigenvalues and eigenvectors of (1), we get

$\lambda_+ = 0.8953 \quad |a_+\rangle = [-.811 \; -0.584]^T$

$\lambda_- = 0.1047 \quad |a_-\rangle = [0.584 \; -0.811]^T$

In spectral form

$$\rho = \lambda_+ |a_+\rangle\langle a_+| + \lambda_- |a_-\rangle\langle a_-|$$

The Shannon entropy in spectral form is

$$H_{Sh}^{(\text{spectral})} = -\lambda_+ \log_2(\lambda_+) - \lambda_- \log_2(\lambda_-).$$

$$\cong 0.48 \text{ bits}$$

Clearly $H_{Sh}^{(\text{spectral})} < H_{Sh}^{(\text{non-spectral})}$

$\therefore$ Non-orthogonal states can be compressed further !

P2.1) $\mathcal{E}(\rho) = \frac{1}{2}\left(aI\,tr(\rho) + bX\rho X + cY\rho Y + dZ\rho Z\right)$

$a, b, c, d \geq 0$

To check for linearity property

Consider $\mathcal{E}(\alpha_1 \rho_1 + \alpha_2 \rho_2)$

Clearly,

$\mathcal{E}(\alpha_1 \rho_1 + \alpha_2 \rho_2) = \alpha_1 \mathcal{E}(\rho_1) + \alpha_2 \mathcal{E}(\rho_2)$

So, there are no dependencies of the constraints on a, b, c, d.

To check for trace-preserving property

$$tr(\mathcal{E}(\rho)) = \frac{1}{2}\left[\begin{array}{l} a.\,tr(I\,tr\,\rho) + c\,tr(Y\rho Y) \\ +b\,tr(X\rho X) + d\,tr(Z\rho Z) \end{array}\right]$$

From trace cyclicity property and using $X^2 = Y^2 = Z^2 = I$, we get

$$tr(\mathcal{E}(\rho)) = \frac{1}{2}\left[\begin{array}{l} a.2.\underbrace{tr(\rho)}_{} + b\,\underbrace{tr(X^2\rho)}_{1} \\ + c\,tr^{1}(\underbrace{Y^2}_{I}\rho) + d\,tr(\underbrace{Z^2}_{I}\rho) \end{array}\right]$$

$$= \frac{1}{2}\left[2a + b + c + d\right]$$

$tr(\mathcal{E}(\rho)) = tr(\rho) = 1$ implies

$$\boxed{2a + b + c + d = 2}$$

P2.2) Let the Bloch vector $\underline{r} = (r_x \; r_y \; r_z)$ corresponding to

$$\rho = \frac{1}{2}\left[I + r_x X + r_y Y + r_z Z\right]. \quad (1)$$

Now, we employ the qubit mapping

$$\mathcal{E}(\rho) = \frac{1}{2}\left[a I \, tr(\rho) + b X\rho X + c Y\rho Y + d Z\rho Z\right]. \quad (2)$$

plug in (1) into (2)

$$\begin{aligned}\mathcal{E}(\rho) = \frac{1}{2}\Big[& a I \, tr\left(\frac{1}{2}(I + r_x X + r_y Y + r_z Z)\right)\Big] \\ &+ \frac{b}{2} X \frac{1}{2}\left[I + r_x X + r_y Y + r_z Z\right] X \\ &+ \frac{c}{2} Y \frac{1}{2}\left[I + r_x X + r_y Y + r_z Z\right] Y \\ &+ \frac{d}{2} Z \frac{1}{2}\left[I + r_x X + r_y Y + r_z Z\right] Z \end{aligned} \quad (3)$$

We have

$$\left.\begin{aligned} XY &= -YX \\ YZ &= -ZY \\ ZX &= -XZ \end{aligned}\right\} \quad \begin{aligned} X^2 &= I \\ Y^2 &= I \\ Z^2 &= I \end{aligned} \quad (4)$$

Using (4) in (3),

$$\mathcal{E}(\rho) = \frac{a}{2}\, I\, tr\left(\frac{I}{2} + \frac{r_x X}{2} + \frac{r_y Y}{2} + \frac{r_z Z}{2}\right)$$
$$+ \frac{b}{2} \cdot \frac{1}{2}\left(I + r_x X - r_y Y - r_z Z\right)$$
$$+ \frac{c}{2}\,\frac{1}{2}\left(I - r_x X + r_y Y - r_z Z\right)$$
$$+ \frac{d}{2} \cdot \frac{1}{2}\left(I - r_x X - r_y Y + r_z Z\right) \qquad (5)$$

Grouping the terms in (5), we get

$$\mathcal{E}(\rho) = \frac{I}{2}\left(a + \frac{b+c+d}{2}\right)$$
$$+ \frac{r_x X}{2}\left(\frac{b-c-d}{2}\right)$$
$$+ \frac{r_y Y}{2}\left(\frac{-b+c-d}{2}\right)$$
$$+ \frac{r_z Z}{2}\left(\frac{-b-c+d}{2}\right) \qquad (6)$$

Note: $tr(X) = tr(Y) = tr(Z) = 0$

$tr(I) = 2$

Comparing the terms in 6 in Bloch vector form

$$a + \left(\frac{b+c+d}{2}\right) = 1 \quad \text{— 7a}$$

from trace-preserving condition

$$\left.\begin{aligned} \mu_x &= \frac{b-c-d}{2} \\ \mu_y &= \frac{-b+c-d}{2} \\ \mu_z &= \frac{-b-c+d}{2} \end{aligned}\right\} \text{— 7b}$$

To solve for a, b, c, d, use 7a and 7b, and <u>observe</u> <u>symmetry</u>!

$$\left.\begin{aligned} b &= -\mu_y - \mu_z \\ c &= -\mu_x - \mu_z \\ d &= -\mu_y - \mu_x \\ a &= 1 + \mu_x + \mu_y + \mu_z \end{aligned}\right\} \text{— 8}$$

Eqn 8 determines the necessary constants for the <u>smooth</u> <u>mapping</u>!

P3) We have $\forall k$ and $\varepsilon > 0$

$$\mathrm{tr}\left(\Lambda_k^S \rho_k^S\right) \geq 1 - \varepsilon \, .$$

Let
$$|\phi_k\rangle^{RS} = \sum_i \sqrt{\lambda_i^{(k)}} |\phi_i^{(k)}\rangle^R |\phi_i^{(k)}\rangle^S \quad \text{——— (1)}$$

Construct the coherent instrument

$$U^{S \to SS'} \equiv \sum_k \Lambda_k^S \otimes |k\rangle^{S'} \quad \text{——— (2)}$$

Plugging (1) and (2),
Now, let us evaluate

$$\langle \phi_k |^{RS} \langle k |^{S'} U^{S \to SS'} |\phi_k\rangle^{RS}$$

$$= \sum_i \sqrt{\lambda_i^{(k)}} \langle \phi_i^{(k)} |^R \langle \phi_i^{(k)} |^S \langle k |^{S'} \sum_{k'} \Lambda_{k'}^S \otimes |k'\rangle^{S'} \sum_j \sqrt{\lambda_j^{(k)}} |\phi_j^{(k)}\rangle^R |\phi_j^{(k)}\rangle^S \quad \text{——— (3)}$$

Simplifying (3),

$$\sum_{i,j} \sqrt{\lambda_i^{(k)} \lambda_j^{(k)}} \underbrace{\langle \phi_i^{(k)} | \phi_j^{(k)} \rangle^R}_{\delta_{i,j}} \langle \phi_i^{(k)}|^S \langle k|^{S'} \sum_{k'} \Lambda_{k'}^S \otimes |k'\rangle^{S'} |\phi_j^{(k)}\rangle^S$$

$$= \sum_i \lambda_i^{(k)} \langle \phi_i^{(k)}|^S \underbrace{\langle k|^{S'} \sum_{k'} \Lambda_{k'}^S \otimes |k'\rangle^{S'}}_{\Lambda_k \text{ since } \{|k'\rangle^{S'}\} \text{ form an o.n. basis}} |\phi_i^{(k)}\rangle^S$$

$$= \sum_i \lambda_i^{(k)} \langle \phi_i^{(k)} | \Lambda_k^S | \phi_i^{(k)} \rangle$$

$$= tr \Big(\underbrace{\sum_i \lambda_i^{(k)} |\phi_i^{(k)}\rangle\langle \phi_i^{(k)}|^S}_{\varrho_k^S} \Lambda_k^S \Big)$$

$$= tr \left(\varrho_k^S \Lambda_k^S \right) \geq 1 - \varepsilon$$

by the design of measurements $\{\Lambda_k^S\}$

$\boxtimes$

P4.1) Consider the binary erasure channel.

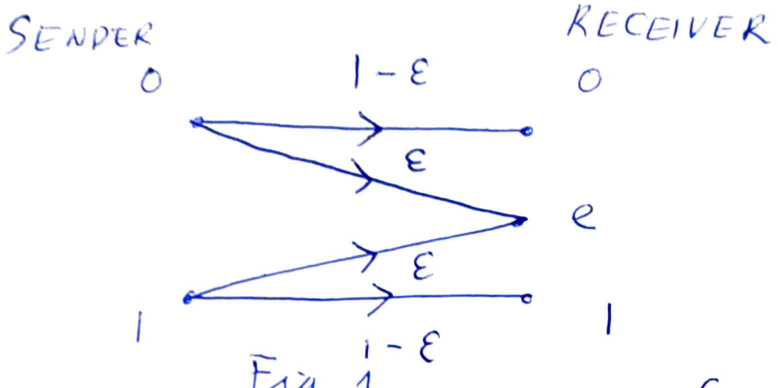

Fig. 1

Let $P(S=0) = 1-p$, $P(S=1) = p$

$p(r=0|s=0) = 1-\varepsilon$ $P(r=1|s=1) = 1-\varepsilon$

$p(r=e|s=0) = \varepsilon$ $P(r=e|s=1) = \varepsilon$

The o/p symbol probabilities are

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

$$= (1-p)(1-\varepsilon) \quad \text{——— } 1(a)$$

$$p(r=1) = p(r=1|s=1)\,P(s=1) = p\cdot(1-\varepsilon) \quad \text{——— } 1(b)$$

$$p(r=e) = \varepsilon \quad \text{——— } 1(c)$$

Using 1(a) − 1(c), compute

$$H(r) = -\sum_{r=\{0,1,e\}} p_r \log_2(p_r)$$

——— (2)

Also

$$H(r|s) = -\sum_{s=\{0,1\}} p(s=s)\, H(r|s=s)$$ (3)

Compute $H(r|s=0) = -(1-\varepsilon)\log_2(1-\varepsilon) - \varepsilon \log_2(\varepsilon)$

i.e., over $r=0$, $r=e$

|||ly $H(r|s=1) = -(1-\varepsilon)\log_2(1-\varepsilon) - \varepsilon\log_2(\varepsilon)$

due to symmetry

(4)

$$C_{erasure} = \max_{p\in[0,1]} H(r) - H(r|s)$$ (5)

Plug (2) and (4) in (5) to get

$$C_{erasure} = \max_{p} \Big[\underbrace{+H(\varepsilon) + (1-\varepsilon) H(p)}_{H(r)} - \underbrace{(H(\varepsilon))}_{H(r|s)} \Big]$$

$$C = \max_{p} (1-\varepsilon) H(p) = \boxed{1-\varepsilon}$$

since $\max_{p} H(p) = 1$ for $p = 1/2$

P4.2) R & S stand for receiver & sender spaces

$$\mathcal{E}(\rho) = (1-\varepsilon)\,\rho + \varepsilon\, |e\rangle^{R} \langle e| \quad \text{since } tr(\rho)=1$$

$$\mathcal{E}(\rho) = (1-\varepsilon)\,\rho + \varepsilon\, |e\rangle^{R} \left[{}^{S}\langle 0|\rho|0\rangle^{S} + {}^{S}\langle 1|\rho|1\rangle^{S} \right] \langle e| \quad (1)$$

From inspection of (1), the Kraus operators are of the form

$$M_0 = \sqrt{1-\varepsilon}\,\left(|0\rangle^{R}\langle 0|^{S} + |1\rangle^{R}\langle 1|^{S} \right)$$

$$M_1 = \sqrt{\varepsilon}\; |e\rangle^{R}\langle 0|^{S}.$$

$$M_2 = \sqrt{\varepsilon}\; |e\rangle^{R}\langle 1|^{S}. \quad (2)$$

Actually, (2) can just written directly from the binary erasure channel schematic description in Fig. 1.

The needed isometric extension is

$$\mathcal{U}^{S\to RE} \equiv \sum_{i=0}^{2} M_i^{S\to R} \otimes |i\rangle^E$$

We introduce a Hilbert space E with o.n. basis $\{|i\rangle^E\}$ that we could couple corresponding to the M_i, $i = 0, 1, 2$ Kraus operators of the erasure channel.

$$\mathcal{U}^{S\to RE} = M_0^{S\to R}|0\rangle^E + M_1^{S\to R}|1\rangle^E + M_2^{S\to R}|2\rangle^E$$

$$= \sqrt{1-\varepsilon}\left(|0\rangle^R|0\rangle^E\langle 0|^S + |1\rangle^R|0\rangle^E\langle 1|^S\right) + \sqrt{\varepsilon}\left(|e\rangle^R|1\rangle^E\langle 0|^S\right) + \sqrt{\varepsilon}\left(|e\rangle^R|2\rangle^E\langle 1|^S\right)$$

In matrix form

$$\mathcal{U}^{S\to RE} = \begin{array}{c} \\ |0\rangle^R|0\rangle^E \\ |0\rangle^R|1\rangle^E \\ |0\rangle^R|2\rangle^E \\ |1\rangle^R|0\rangle^E \\ |1\rangle^R|1\rangle^E \\ |1\rangle^R|2\rangle^E \\ |e\rangle^R|0\rangle^E \\ |e\rangle^R|1\rangle^E \\ |e\rangle^R|2\rangle^E \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle^S & |1\rangle^S \end{array} \\ \begin{bmatrix} \sqrt{1-\varepsilon} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \sqrt{1-\varepsilon} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ \sqrt{\varepsilon} & 0 \\ 0 & \sqrt{\varepsilon} \end{bmatrix} \end{array}$$

P5) Recall from the definition of strong typical sets, for $x^{(n)} \in T_\delta^{X^{(n)}}$

$$-c\delta + H(X) \leq -\frac{1}{n}\log_2\left(P_{X^{(n)}}(x^{(n)})\right) \leq c\delta + H(X)$$

where $c \triangleq -\sum_{x \in \mathcal{X}^+} \log(P_X(x)) \geq 0.$

Now, we are interested in computing $\sum_{x^{(n)}, y^{(n)} \in T_\delta^{X^{(n)} Y^{(n)}}} P_{X^{(n)}}(x^{(n)}) P_{Y^{(n)}}(y^{(n)})$ — 1

since $X^{(n)}$ and $Y^{(n)}$ are statistically independent

Let us upper bound (u.b) 1

$$\sum_{x^{(n)}, y^{(n)} \in T_\delta^{X^{(n)} Y^{(n)}}} P_{X^{(n)}}(x^{(n)}) P_{Y^{(n)}}(y^{(n)}) \leq \left|T_\delta^{X^{(n)} Y^{(n)}}\right|_{u.b} P_{X^{(n)}}(x^{(n)})_{u.b} \cdot P_{Y^{(n)}}(y^{(n)})_{u.b.}$$

— 2

$$P_{X^{(n)}}(x^{(n)}) \leq 2^{-n(H(X) - c\delta)} \quad \text{--- } 3(a)$$

$$P_{Y^{(n)}}(y^{(n)}) \leq 2^{-n(H(Y) - c\delta)} \quad \text{--- } 3(b)$$

$$\left| T_\delta^{X^{(n)} Y^{(n)}} \right| \leq 2^{n(H(X,Y) + c\delta)} \quad \text{--- } 3(c)$$

Plugging 3(a) – 3(c) into 2

$$\Pr\left(x^{(n)}, y^{(n)} \in T_\delta^{X^{(n)} Y^{(n)}}\right) \leq 2^{-n\left(\begin{array}{c} H(X) + H(Y) \\ - H(X,Y) \\ - 3c\delta \end{array}\right)}$$

Now $H(X) + H(Y) - H(X,Y) = I(X;Y)$

$$\therefore \Pr\left(x^{(n)}, y^{(n)} \in T_\delta^{X^{(n)} Y^{(n)}}\right) \leq 2^{-n(I(X;Y) - 3c\delta)}$$

$\boxtimes$

NOTE: You could have also picked c_1, δ_1 for $x^{(n)} \in T_\delta^{X^{(n)}}$, c_2, δ_2 for $y^{(n)} \in T_\delta^{Y^{(n)}}$, c_3, δ_3 for $x^{(n)}, y^{(n)} \in T_\delta^{X^{(n)} Y^{(n)}}$ & an overall $c\delta = \min(c_1\delta_1, c_2\delta_2, c_3\delta_3)$ to get the desired result!