Quantum Communications and Cryptography 24/25

Guillermo Abad

10 Feb, 2025

Exercise 1, CHSH:

Compute the quantum value of each of the four terms $\langle A_x \otimes B_y \rangle$, with $x, y = 1, 2$, in the CHSH expression for the state $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and settings as in Fig.1 and verify that they sum up to $2\sqrt{2}$.

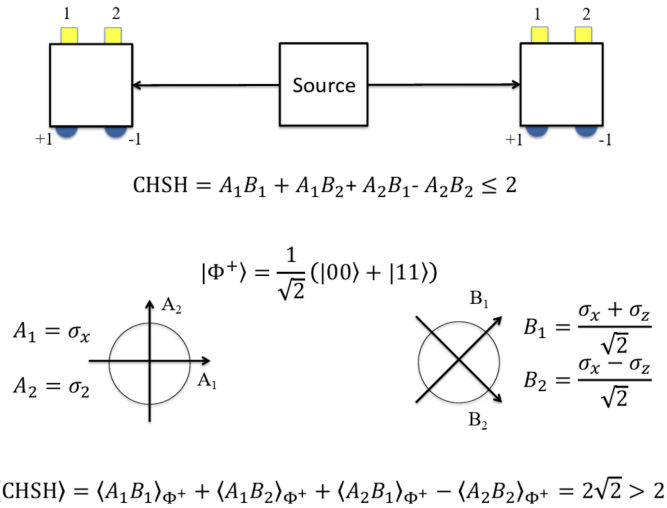

Figure 1: **CHSH Bell inequality**: Two parties measure two two-outcome observables, A_1 and A_2 for Alice,and B_1 and B_2 for Bob. The choice of measurement is represented by a bit, x and y for Alice and Bob. The two possible outcomes are labeled by ± 1. For the quantum violation, observables are replaced by quantum operators and they act on a two-qubit maximally entangled state.

Let's start by generalizing operators $A_{1,2}$ and $B_{1,2}$ from Fig.1, as:

$$A'_\alpha = \cos(\alpha)\sigma_x + \sin(\alpha)\sigma_z \equiv c_\alpha \sigma_x + s_\alpha \sigma_z, \quad B'_\beta = \cos(\beta)\sigma_x + \sin(\beta)\sigma_z \equiv c_\beta \sigma_x + s_\beta \sigma_z \tag{1}$$

where $A_{1,2} = A'_{0,\pi/2}$ and $B_{1,2} = B'_{\pi/4,-\pi/4}$ respectively.

With this, we can compute the general case of the expected value, like:

$$\begin{aligned} \langle A'_\alpha \otimes B'_\beta \rangle_{\Phi^+} \equiv \langle A'_\alpha B'_\beta \rangle_{\Phi^+} &= \langle (c_\alpha \sigma_x + s_\alpha \sigma_z) \otimes (c_\beta \sigma_x + s_\beta \sigma_z) \rangle_{\Phi^+} = \\ &= \langle c_\alpha c_\beta \sigma_x \sigma_x + c_\alpha s_\beta \sigma_x \sigma_z + s_\alpha c_\beta \sigma_z \sigma_x + s_\alpha s_\beta \sigma_z \sigma_z \rangle_{\Phi^+} = \\ &= c_\alpha c_\beta \underbrace{\langle \sigma_x \sigma_x \rangle_{\Phi^+}}_{\to 1} + c_\alpha s_\beta \underbrace{\langle \sigma_x \sigma_z \rangle_{\Phi^+}}_{\to 0} + s_\alpha c_\beta \underbrace{\langle \sigma_z \sigma_x \rangle_{\Phi^+}}_{\to 0} + s_\alpha s_\beta \underbrace{\langle \sigma_z \sigma_z \rangle_{\Phi^+}}_{\to 1} = \\ &= c_\alpha c_\beta + s_\alpha s_\beta = \frac{1}{2}(c_{\alpha-\beta} + c_{\alpha+\beta}) + \frac{1}{2}(c_{\alpha-\beta} - c_{\alpha+\beta}) = c_{\alpha-\beta} = \cos(\alpha - \beta) \end{aligned} \tag{2}$$

and finally the CHSH Bell inequality ends like:

$$\begin{aligned} \langle \text{CHSH} \rangle &= \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle = \\ &= \langle A'_0 B'_{\pi/4} \rangle + \langle A'_0 B'_{-\pi/4} \rangle + \langle A'_{\pi/2} B'_{\pi/4} \rangle - \langle A'_{\pi/2} B'_{-\pi/4} \rangle = \\ &= c_{0-\pi/4} + c_{0+\pi/4} + c_{\pi/2-\pi/4} - c_{\pi/2+\pi/4} = 4 \cdot 1/\sqrt{2} = \boxed{2\sqrt{2}} \end{aligned} \tag{3}$$

Exercise 2, Unambiguous discrimination:

Consider two non-orthogonal pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, with $\langle\psi_0|\psi_1\rangle > 0$. Without loss of generality, the two states can be rotated to be in the XZ plane and with the $+z$ axis as bisector, so that they read:

$$|\psi_0\rangle = \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}, \quad |\psi_1\rangle = \begin{pmatrix}\cos\theta\\ -\sin\theta\end{pmatrix} \tag{4}$$

with $0 \leq \theta \leq \pi/4$. Let $|\psi\rangle$ be an unknown state chosen between these two with equal probability. Consider a three-outcome measurement defined by the operators:

$$M_0 = \mu|\psi_1^\perp\rangle\langle\psi_1^\perp|, \quad M_1 = \mu|\psi_0^\perp\rangle\langle\psi_0^\perp|, \quad M_? = \mathbb{1} - M_0 - M_1, \tag{5}$$

where $|\psi_i^\perp\rangle$ denotes the state orthogonal to $|\psi_i\rangle$.

Before starting with each part, some initial remarks:

- We see that $\theta \in [0, \pi/4)$ defines it correctly, since $\langle\psi_0|\psi_1\rangle = \cos^2(\theta) - \sin^2(\theta) = \cos(2\theta) > 0$
- The orthogonal states $|\psi_i^\perp\rangle$, will correspond to: $|\psi_0^\perp\rangle = \begin{pmatrix}\sin\theta\\ -\cos\theta\end{pmatrix}$, $|\psi_1^\perp\rangle = \begin{pmatrix}\sin\theta\\ \cos\theta\end{pmatrix}$

and all this can be summarized, understanding that these states can be represented as:

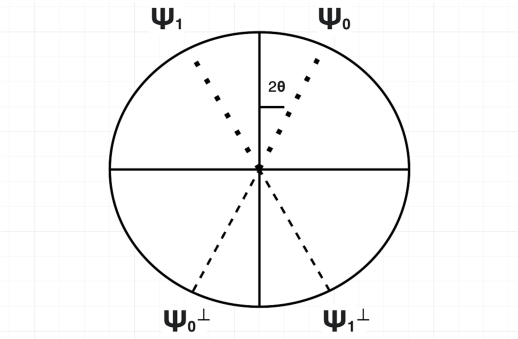

Figure 2: Bloch sphere representation of states $|\psi_i\rangle$ and $\left|\psi_i^\perp\right\rangle$, in the XZ plane.

where for:

- $\theta = 0$, you have both $|\psi_i\rangle$ pointing up, towards $|0\rangle$ (overlap: $1 = \langle 0|0\rangle$),
- $\theta = \pi/4$, you have each $|\psi_i\rangle$ pointing to each side, towards $|\pm\rangle$ (overlap: $\langle +|-\rangle = 0$, not allowed),
- And then for each θ the corresponding orthogonal state, is just the inverse line from the center of the Bloch sphere (always with overlap: $\langle\psi_i^\perp|\psi_i\rangle = 0$).

(a) Find the range of values of μ so that the measurement is well defined, that is, all the three measurement operators are positive semi-definite.

By construction the operators will sum to the identity, so as the excercice asks, we only need to find the μ's such that $M_i \geq 0$ (positive semi-definite) $\forall i \in \{0, 1, ?\}$:

$$\begin{aligned} &M_{0,1} = \mu|\psi_{1,0}^\perp\rangle\langle\psi_{1,0}^\perp| \geq 0 \quad \rightarrow \boxed{\mu \geq 0} \\ &M_? = \mathbb{1} - M_0 - M_1 = \mathbb{1} - \mu\left[\begin{pmatrix}s^2 & sc\\ sc & c^2\end{pmatrix} + \begin{pmatrix}s^2 & -sc\\ -sc & c^2\end{pmatrix}\right] = \mathbb{1} - 2\mu\begin{pmatrix}s^2 & 0\\ 0 & c^2\end{pmatrix} \geq 0 \quad \rightarrow \boxed{\mu \leq \frac{1}{2c^2}} \end{aligned} \tag{6}$$

where $s, c \equiv \sin(\theta), \cos(\theta)$ and in the last step we used that the cosine is always bigger for $\theta \in [0, \pi/4)$.

(b) For this value of μ, compute the probabilities of obtaining the three outputs for each of the two states. What's the operational meaning of this three-outcome measurement?

Let's start with the generalized probability, for the cases $i, j = \{0, 1\}$ (all except those involving $M_?$):

$$Pr(i|\psi_j) = tr(M_i \left|\psi_j\right\rangle\!\left\langle\psi_j\right|) = \langle M_i \rangle_{\psi_j} = \mu \left|\left\langle \psi_{\bar{i}}^{\perp} \middle| \psi_j \right\rangle\right|^2 = \mu (2sc)^2 \delta_{i,j} = \boxed{\mu \sin^2(2\theta)\delta_{i,j}} \tag{7}$$

And now the remaining case, that of $M_?$:

$$\begin{aligned} Pr(?|\psi_j) &= tr(M_? \left|\psi_j\right\rangle\!\left\langle\psi_j\right|) = \langle M_? \rangle_{\psi_j} = \langle \mathbb{1} \rangle_{\psi_j} - \langle M_0 \rangle_{\psi_j} - \langle M_1 \rangle_{\psi_j} = \\ &= 1 - Pr(0|\psi_j) - Pr(1|\psi_j) = 1 - \mu \sin^2(2\theta)\cancelto{1}{(\delta_{0,j} + \delta_{1,j})} = \boxed{1 - \mu \sin^2(2\theta)} \end{aligned} \tag{8}$$

which is independent of i, j, telling us that the probability of not knowing, only depends on θ (and μ).

This can be more understandable by showing all combinations more explicitly:

$$\boxed{|\psi_0\rangle \to \begin{cases} Pr(M_0|\psi_0) = \mu \sin^2(2\theta) \\ Pr(M_1|\psi_0) = 0 \\ Pr(M_?|\psi_0) = 1 - \mu \sin^2(2\theta) \end{cases} \quad ; \quad |\psi_1\rangle \to \begin{cases} Pr(M_0|\psi_1) = 0 \\ Pr(M_1|\psi_1) = \mu \sin^2(2\theta) \\ Pr(M_?|\psi_1) = 1 - \mu \sin^2(2\theta) \end{cases}} \tag{9}$$

which basically tells you, that given a state $|\psi_i\rangle$, you will know its state with 100% confidence, $\mu \sin^2(2\theta)$ of the times, and you will not be able to be 100% sure the rest $(1 - \mu \sin^2(2\theta))$.

(c) Finally, determine the value of μ that minimizes the average probability of obtaining the third outcome, that is:

$$Pr(?) = \frac{1}{2}\left(Pr(?|0) + Pr(?|1)\right) \quad \left(= Pr(M_?) = \sum_i Pr(\psi_i) Pr(M_?|\psi_i)\right) \tag{10}$$

Well since we saw that the $Pr(?|\psi_j)$ is independent of j, we can extract it from the sum and becomes obvious that for any priors $Pr(\psi_j)$:

$$Pr(?) = \sum_j Pr(?|\psi_j) Pr(\psi_j) = \cancelto{1}{\left(\sum_j Pr(\psi_j)\right)} Pr(?|\psi_j) = Pr(?|\psi_j) = 1 - \mu \sin^2(2\theta) \tag{11}$$

Which decreases as μ increases, as one would expect by the construction ($M_? = 1 - \mu \sum_i M_i$). And as we found in part (a), μ has a maximum value of $\frac{1}{2c^2}$, meaning that the minimum probability of $M_?$ is:

$$\begin{aligned} \min_\mu Pr(?) &= \min_\mu \left(1 - \mu \sin^2(2\theta)\right) = 1 - \max_\mu \left(\mu \sin^2(2\theta)\right) = 1 - \max_\mu (\mu) \sin^2(2\theta) = \\ &= 1 - \frac{1}{2c^2} \sin^2(2\theta) = 1 - \frac{1}{2c^2}(2sc)^2 = 1 - 2s^2 = c^2 - s^2 = \boxed{\cos(2\theta) = \langle \psi_0 | \psi_1 \rangle} \end{aligned} \tag{12}$$

where again $c, s = \cos(\theta), \sin(\theta)$.

How does it relate to the overlap between the two states?

From this result, we see that the probability of not being sure increases exactly as the overlap. The more the overlap, the more you can't unambiguously discriminate.

Which makes sense, since the more similar the states, the harder it should be to distinguish them.

Exercise 3: Individuals attacks

Consider a cloning individual attack in which Eves action is described by a one parameter family of unitary operations $U(\eta)$. While the no-cloning theorem states that an unknown quantum state cannot be cloned, approximate cloning is always possible. Consider states in the equator of the Bloch sphere, that is,

$$|\theta\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right). \tag{13}$$

Note that if $\theta = 0,\ \pi/2,\ \pi,\ 3\pi/2$ one gets the four states $|\pm x\rangle$ and $|\pm y\rangle$ that can be used for BB84. Take a generic state $|\theta\rangle$ and an ancillary state $|0\rangle$ and apply the global transformation (acting on the two states) $U(\eta)$, or U to simplify the notation:

$$\begin{aligned} U|00\rangle &= |00\rangle, \\ U|10\rangle &= \cos\eta|10\rangle + \sin\eta|01\rangle \equiv c\,|10\rangle + s\,|01\rangle\,. \end{aligned} \tag{14}$$

where I have defined $c, s = \cos\eta, \sin\eta$ for making easier posterior computations.

(a) Briefly explain why U is a valid unitary transformation on the considered quantum states.

For U to be a valid operator we need it to be Unitary in the full space, or equivalently (due to Stinespring dilation) that it behaves as a CPTP map in the subspace of the ancila $|0\rangle$:

$$\Lambda(|\psi\rangle\langle\psi|)\begin{cases} \Lambda\begin{pmatrix} 1 & 0 \\ 0 & \mathbb{0}_{3\times3} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \mathbb{0}_{3\times3} \end{pmatrix} = \Lambda(|00\rangle\langle 00|) = |00\rangle\langle 00| \\ \Lambda\begin{pmatrix} 0&0&0&0 \\ 0&0&0&0 \\ 0&0&1&0 \\ 0&0&0&0 \end{pmatrix} = \begin{pmatrix} 0&0&0&0 \\ 0&s^2&cs&0 \\ 0&cs&c^2&0 \\ 0&0&0&0 \end{pmatrix} = \Lambda(|10\rangle\langle 10|) = \Big(c\,|10\rangle + s\,|01\rangle\Big)\Big(...^\dagger\Big) \end{cases} \tag{15}$$

which for the element $|00\rangle\langle 00|$ is trivial to see that it's trace preserving (TP) and completely positive (CP), since it acts like the identity. And for the second element of the base, we can see it is TP since:

$$tr(\Lambda(|10\rangle\langle 10|)) = s^2 + c^2 = 1 = tr\,|10\rangle\langle 10| \tag{16}$$

and it is also CP, since $\Lambda(|01\rangle\langle 01|)$ can be diagonalized as:

$$\Lambda(|10\rangle\langle 10|) = \frac{s^2+c^2}{2}\begin{pmatrix} 0&0&0 \\ 0&\mathbb{1}_2&0 \\ 0&0&0 \end{pmatrix} + \frac{s^2-c^2}{2}\begin{pmatrix} 0&0&0 \\ 0&\sigma_{z2}&0 \\ 0&0&0 \end{pmatrix} = \frac{\mathbb{1} + (s^2-c^2)\sigma_z}{2} \oplus \mathbb{0}_{2\times2} \tag{17}$$

which has eigenvalues: $\lambda = 0, 0, \frac{1\pm(s^2-c^2)}{2} \geq 0$ making Λ a CPTP map, and its corresponding Stinespring dilation U, unitary (where we have used $\oplus$ as the direct sum).

A more easy way to show this perhaps would have been, to directly fill the rest of the space showing how U acts on it, with an example, proving there is at least a way to do it Unitary. In this case, we can show there exist at least one U unitary if we let it act in the rest of the space like:

$$\begin{cases} U|01\rangle = -c|01\rangle + s|10\rangle \\ U|11\rangle = |11\rangle. \end{cases} \quad \rightarrow \quad U = \begin{pmatrix} 1&0&0&0 \\ 0&-c&s&0 \\ 0&s&c&0 \\ 0&0&0&1 \end{pmatrix} \quad \rightarrow \quad \boxed{UU^\dagger = U^2 = \mathbb{1}} \tag{18}$$

but we don't care how it acts on the rest of this space (outside this proof), since it won't be used.

(b) Compute the final two-qubit state $|\psi(\theta)\rangle_{BE} = U_{BE}|\theta\rangle_B|0\rangle_E$ and the reduced states ρ_B and ρ_E, where $\rho_B = \mathbf{tr}_E|\psi(\theta)\rangle\langle\psi(\theta)|$ and similar for ρ_E.

The final two-qubit state will be given by:

$$|\psi(\theta)\rangle_{BE} = U_{BE}\Big(|\theta\rangle_B|0\rangle_E\Big) = \frac{1}{\sqrt{2}}U_{BE}\Big(\,|00\rangle + e^{i\theta}\,|01\rangle\,\Big) = \frac{1}{\sqrt{2}}\Big(\,|00\rangle + e^{i\theta}(c\,|01\rangle + s\,|10\rangle)\Big) \tag{19}$$

which can also be expressed as:

$$\rho_{BE} = |\psi(\theta)\rangle\langle\psi(\theta)| = \frac{1}{2}\Big(\,|00\rangle + e^{i\theta}(s\,|01\rangle + c\,|10\rangle)\Big)\Big(...^\dagger\Big) = \frac{1}{2}\begin{pmatrix} 1 & e^{-i\theta}s & e^{-i\theta}c & 0 \\ e^{i\theta}s & s^2 & cs & 0 \\ e^{i\theta}c & cs & c^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{20}$$

from where its trivial to find its reduced states by adding the corresponding subspaces of the matrix:

$$\begin{aligned} \rho_E = tr_B(\rho_{BE}) &= \frac{1}{2}\left[\begin{pmatrix} 1 & e^{-i\theta}s \\ e^{i\theta}s & s^2 \end{pmatrix} + \begin{pmatrix} c^2 & 0 \\ 0 & 0 \end{pmatrix}\right] = \boxed{\frac{1}{2}\begin{pmatrix} 1+c^2 & e^{-i\theta}s \\ e^{i\theta}s & s^2 \end{pmatrix}} \\ \rho_B = tr_E(\rho_{BE}) &= \frac{1}{2}\begin{pmatrix} 1+s^2 & e^{-i\theta}c+0 \\ e^{i\theta}c+0 & c^2+0 \end{pmatrix} = \boxed{\frac{1}{2}\begin{pmatrix} 1+s^2 & e^{-i\theta}c \\ e^{i\theta}c & c^2 \end{pmatrix}} \end{aligned} \tag{21}$$

where we see that ρ_b and ρ_E are the same if you change $s \leftrightarrow c$.

(c) Compute the overlap, or fidelity, of these two states with the initial state, that is $F_i = \langle\theta|\rho_i|\theta\rangle$, with $i = B, E$. Do these fidelities depend on θ?

Let's start by computing the general case:

$$F_i = \langle\rho_i\rangle_\theta = \frac{1}{2}\left(\langle 0| + e^{-i\theta}\,\langle 1|\right)\rho_i\left(|0\rangle + e^{i\theta}|1\rangle\right) = \frac{1}{2}(\rho_{i00} + e^{i\theta}\rho_{i01} + e^{-i\theta}\rho_{i10} + \rho_{i11}) \tag{22}$$

where $\rho_{iab} = \langle a|\,\rho_i\,|b\rangle$. From here, its very easy to get each one:

$$\begin{aligned} F_E &= \frac{1}{4}\Big((1+c^2) + e^{i\theta}e^{-i\theta}s + e^{-i\theta}e^{i\theta}s + s^2\Big) = \frac{1}{4}\Big((1+c^2) + s + s + s^2\Big) = \boxed{\frac{1+s}{2}} \\ F_B &= \frac{1}{4}\Big((1+s^2) + e^{i\theta}e^{-i\theta}c + e^{-i\theta}e^{i\theta}c + c^2\Big) = \frac{1}{4}\Big((1+s^2) + c + c + c^2\Big) = \boxed{\frac{1+c}{2}} \end{aligned} \tag{23}$$

which are same result flipping $s \leftrightarrow c$, as we would expect given the previous found symmetry. We also see that the fidelities don't depend on θ, only on η (since $c, s = \cos\eta, \sin\eta$).

To make sense of this, let's study what is the effect of U as a function of η. First of all its obvious that for state $|0\rangle_B$, Eve will always get the correct result, but what about $|1\rangle_B$? Let's see:

$$\begin{aligned} &\eta = 0 \;\rightarrow\; \begin{cases} U|00\rangle = |00\rangle, \\ U|10\rangle = |10\rangle \end{cases} \;\rightarrow\; \text{no attack at all, Eve qubit is always 0, Bob qubit untouched} \\ &\eta = \pi/4 \;\rightarrow\; \begin{cases} U|00\rangle = |00\rangle, \\ U|10\rangle = \frac{|10\rangle+|01\rangle}{\sqrt{2}} \end{cases} \;\rightarrow\; \text{for } |1\rangle_B \text{ Eve and Bob will alter who gets the correct} \\ &\eta = \pi/2 \;\rightarrow\; \begin{cases} U|00\rangle = |00\rangle, \\ U|10\rangle = |01\rangle \end{cases} \;\rightarrow\; \text{totally destr. attack, Eve always gets it correct, and Bob 0} \end{aligned} \tag{24}$$

Find also the value of η for which the two fidelities become equal.

As we can see in Fig.3, the fidelities will be equal for $\pi/4$ and $\pi/4 + \pi = 5\pi/4$ (when $c = s$), with the fidelities being: $F_B = F_E = \frac{1+1/\sqrt{2}}{2} \approx 0.854$, $\frac{1-1/\sqrt{2}}{2} \approx 0.146$ at each point, respectively:

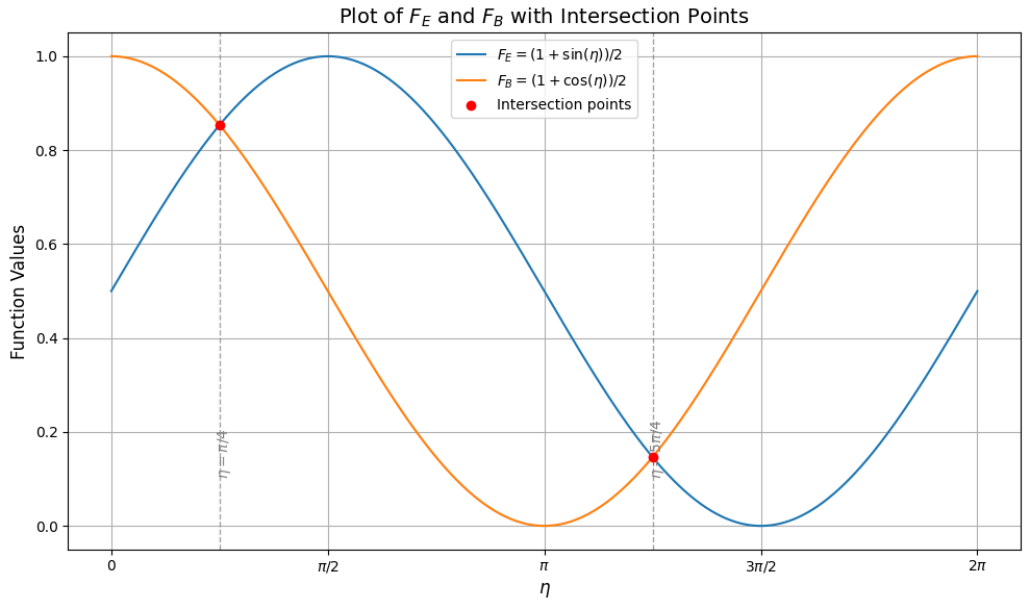

Figure 3: Plot of $F_E = \frac{1+\sin(\eta)}{2}$ (blue) and $F_B = \frac{1+\cos(\eta)}{2}$ (orange) over $\eta \in [0, 2\pi)$. With intersections (red) at $\eta = \frac{\pi}{4}$ and $\eta = \frac{5\pi}{4}$.

the figure shows how at the start the fidelity of Eve increases faster than the fidelity of Bob decreases. For example, for $\eta = \pi/8$, Bob would get almost all results correctly, which might lead to him thinking everything is fine, but Eve is already getting 70% of the information!

And finally, mention, that from our computation and Fig.3, we see that if Eve did this attack, for $\eta < \pi/4$ there will be a positive gap between F_B and F_E, meaning that with error corrections and distilation of privacy, the communication can still be secure.

Finally, compute the reduced states when $F_B = 1$. How do you interpret these results?

Bob fidelity will be one just for $\eta = 0$, which as we saw is the case, where there is no attack at all and Eve always get the 0 state. In such case the reduces states end like:

$$\begin{aligned} \rho_E(\eta = 0) &= \frac{1}{2}\begin{pmatrix} 1+1^2 & e^{-i\theta}0 \\ e^{i\theta}0 & 0^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \boxed{|0\rangle\langle 0| = \frac{\mathbb{1} + \sigma_z}{2}} \\ \rho_B(\eta = 0) &= \frac{1}{2}\begin{pmatrix} 1+0^2 & e^{-i\theta} \\ e^{i\theta} & 1^2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & e^{-i\theta} \\ e^{i\theta} & 1 \end{pmatrix} = \boxed{\frac{1}{2}\left(|0\rangle + e^{i\theta}|1\rangle\right)(...^\dagger) = \frac{\mathbb{1} + O(X,Y)}{2}} \end{aligned} \tag{25}$$

which reflect this, showing that Eve always get the state $|0\rangle$ and Bob, gets the original state $|\theta\rangle_B$.

Also the decomposition in σ's, tells us that the state from Bob only has components on the XY plane, while Alice only on the Z axis, telling us that she has absolutely no information regarding Bob state, in accordance with her Fidelity being 0.

(d) Apply this attack to the BB84 protocol when Alice and Bob use the states $|\pm x\rangle$ and $|\pm y\rangle$ and Eve measures in the same basis as Alice and Bob after basis reconciliation. Compute the distribution of variables $P(abe)$ where a denotes the bit encoded by Alice, and b and e the measurement results by e. Compute also the so-called Quantum Bit Error Rate (QBER) defined by the probability that Bob's result is diferent from Alice's preparation when the bases agree, and the mutual information between Alice and Bob, $I(A:B)$, and between Alice and Eve, $I(A:E)$, where $I(X:Y) = H(A) + H(B) - H(AB)$ and $H(X) = -\sum_x p(x)log(p(x))$.

$$
\begin{aligned}
P(abe) = P(be|a)\cancel{P(a)} \overset{\frac{1}{4}}{=} \frac{1}{4}\,\langle\psi(\theta_a)|\,\overbrace{M_B}^{|b\rangle\langle b|}\otimes\overbrace{M_E}^{|e\rangle\langle e|}\,|\psi(\theta_a)\rangle_{BE} \qquad \text{for} \quad \begin{cases}\theta_a = \{0,\pi/2,\pi,3\pi/2\}\\ \text{when}\\ a = \{+x,+y,-x,-y\}\end{cases}\\
= \frac{1}{4}\Big|\,\langle\psi(\theta_a)|\,(\,|b\rangle\otimes|e\rangle\,)\Big|^2 = \frac{1}{4}\Big|\,\underbrace{\langle\theta_a|\,\langle 0|\,U_E^\dagger}_{\langle\psi(\theta_a)|}\,|b\rangle\,|e\rangle\,\Big|^2
\end{aligned}
\tag{26}
$$

where $|\psi(\theta_a)\rangle_{BE} = \frac{1}{\sqrt{2}}\Big(\,|00\rangle + e^{i\theta_a}(c\,|01\rangle + s\,|10\rangle)\Big)$ as we saw in previous sections.

Substituting all the possible values for $b, e = \{\pm x, \pm y\}$, using the $|\theta\rangle$ representation for them, we get:

$$
\begin{aligned}
P(be|a) = \Big|\,\langle\psi(\theta_a)|\,(\,|b\rangle\otimes|e\rangle\,)\Big|^2 = \left|\frac{1}{2\sqrt{2}}\Big(1,\ e^{i\theta_a}c,\ e^{i\theta_a}s,\ 0\Big)\begin{pmatrix}1\\ e^{i\theta_b}\\ e^{i\theta_e}\\ e^{i\theta_b}e^{i\theta_e}\end{pmatrix}\right|^2 =\\
= \frac{1}{8}\big|1 + e^{i\theta_a}(e^{i\theta_b}c + e^{i\theta_e}s)\big|^2 = \boxed{\frac{1 + \mathrm{Re}(e^{i\theta_a}(e^{i\theta_b}c + e^{i\theta_e}s)) + cs\mathrm{Re}(e^{i(\theta_b-\theta_e)})}{4}}
\end{aligned}
\tag{27}
$$

which for each concrete case give:

$$
\begin{cases}
P(\pm^b x, \pm^e x \mid a) = \frac{1+\mathrm{Re}(e^{i\theta_a})(\pm^b c \pm^e s)\pm^{b\cdot e}cs}{4} \begin{cases} a = \pm^a x: & \frac{1}{4}\Big(1 \pm^{a\cdot b} c \pm^{a\cdot e} s \pm^{b\cdot e} cs\Big)\\ a = \pm^a y: & \frac{1}{4}\Big(1 \pm^{b\cdot e} cs\Big)\end{cases}\\
P(\pm^b x, \pm^e y \mid a) = \frac{1\pm^b \mathrm{Re}(e^{i\theta_a})c \pm^e \mathrm{Im}(e^{i\theta_a})s}{4} \begin{cases} a = \pm^a x: & \frac{1}{4}\Big(1 \pm^{a\cdot b} c\Big)\\ a = \pm^a y: & \frac{1}{4}\Big(1 \pm^{a\cdot e} s\Big)\end{cases}\\
P(\pm^b y, \pm^e x \mid a) = \frac{1\pm^b \mathrm{Im}(e^{i\theta_a})c \pm^e \mathrm{Re}(e^{i\theta_a})s}{4} \begin{cases} a = \pm^a x: & \frac{1}{4}\Big(1 \pm^{a\cdot e} s\Big)\\ a = \pm^a y: & \frac{1}{4}\Big(1 \pm^{a\cdot b} c\Big)\end{cases}\\
P(\pm^b y, \pm^e y \mid a) = \frac{1+\mathrm{Im}(e^{i\theta_a})(\pm^b c \pm^e s)\pm^{b\cdot e}cs}{4} \begin{cases} a = \pm^a x: & \frac{1}{4}\Big(1 \pm^{b\cdot e} cs\Big)\\ a = \pm^a y: & \frac{1}{4}\Big(1 \pm^{a\cdot b} c \pm^{a\cdot e} s \pm^{b\cdot e} cs\Big)\end{cases}
\end{cases}
\tag{28}
$$

where $\pm^i$ is the sign of e or b, and $\pm^{e\cdot b}$ is the product of both signs.

And therefore the Qubit Error Rate (QBER) will be given by:

$$
\begin{aligned}
\mathrm{QBER} &= \sum_a Pr(b \neq a \mid \text{same basis})P(a) = 1/4\sum_a Pr(b \neq a \mid \text{same basis})\\
&= \frac{1}{4}\Big(Pr(+x_b, -x_a) + Pr(-x_b, +x_a) + Pr(+y_b, -y_a) + Pr(-y_b, +y_a)\Big) =\\
&= \frac{1}{2}\Big(Pr(+x_b, -x_a) + Pr(-x_b, +x_a)\Big) = \frac{1}{2}\Big(\sum_e Pr(+x, e \mid -x) + Pr(-x, e \mid +x)\Big) =\\
&= \frac{1}{2}\Big(\frac{1}{4}(1-c)\cdot 2 + \frac{1}{4}(1-c)\cdot 2\Big) = \frac{2(1-c)}{4} = \boxed{\frac{1-c}{2}} \quad \rightarrow \quad \boxed{QBER + F_B = 1}
\end{aligned}
\tag{29}
$$

which makes sense since, $c = \cos(\eta)$ is the rate at which U leaves Bob qubit invariant, or in other words the overlap between the original state and the transformed one: $\langle 10|\,U\,|10\rangle = \cos(\eta)$.

To end lets compute the mutual information between Alice and Bob: $I(A:B)$ and between Alice and Eve: $I(A:E)$, which are:

$$\begin{cases} I(A:B) = H(A) + H(B) - H(AB) \\ I(A:E) = H(A) + H(E) - H(AE) \end{cases} \quad \text{with} \quad H(x) = \sum_x P(x)\log(P(x)) \tag{30}$$

where the first common factor is easy to compute, since $P(a) = \frac{1}{4}\ \forall a$, giving:

$$H(a) = -\sum_a P(a)\log(P(a)) = -4\Big(\frac{1}{4}\log\frac{1}{4}\Big) = -\log\frac{1}{4} \approx 0.6 \tag{31}$$

the next ones $H(B)$ and $H(E)$ we can extract them from eq.29, giving:

$$\begin{aligned} P(e) &= \sum_{ab} P(be|a)P(a) = \frac{1}{4}\sum_{ab} P(be|a) = \frac{1}{4}\cdot\frac{1}{4}\cdot 4 = \frac{1}{4}\ \forall e \ \rightarrow\ H(e) = -\log\frac{1}{4} \\ P(b) &= \sum_{ae} P(be|a)P(a) = \frac{1}{4}\sum_{ae} P(be|a) = \frac{1}{4}\cdot\frac{1}{4}\cdot 2 = \frac{1}{8}\ \forall b \ \rightarrow\ H(b) = -\log\frac{1}{8} \end{aligned} \tag{32}$$

and we only have the last tems $H(AB)$ and $H(AE)$ remaining, which we can also extract from eq.29:

$$P(AB) = \sum_e P(be|a)P(a) = \frac{1}{4}\sum_e P(be|a) = \begin{cases} P(+x_a,+x_b) = \frac{1+c}{4} = P(-x_a,-x_b) \\ P(+x_a,-x_b) = \frac{1-c}{4} = P(-x_a,+x_b) \\ P(+y_a,+y_b) = \frac{1+c}{4} = P(-y_a,-y_b) \\ P(+y_a,-y_b) = \frac{1-c}{4} = P(-y_a,+y_b) \end{cases}$$

$$P(AE) = \sum_b P(be|a)P(a) = \frac{1}{4}\sum_b P(be|a) = \begin{cases} P(+x_a,+x_e) = \frac{1+s}{8} = P(-x_a,-x_e) \\ P(+x_a,-x_e) = \frac{1-s}{8} = P(-x_a,+x_e) \\ P(+y_a,+y_e) = \frac{1+s}{8} = P(-y_a,-y_e) \\ P(+y_a,-y_e) = \frac{1-s}{8} = P(-y_a,+y_e) \\ P(+x_a,+y_e) = \frac{1+s}{8} = P(-x_a,-y_e) \\ P(+x_a,-y_e) = \frac{1-s}{8} = P(-x_a,+y_e) \\ P(+y_a,+x_e) = \frac{1+s}{8} = P(-y_a,-x_e) \\ P(+y_a,-x_e) = \frac{1-s}{8} = P(-y_a,+x_e) \end{cases} \tag{33}$$

which then give and entropy:

$$\begin{aligned} H(AB) &= -\sum_{AB} P(AB)\log(P(AB)) = 4\left(\frac{1+c}{4}\log\frac{1+c}{4} + \frac{1-c}{4}\log\frac{1-c}{4}\right) = \\ &= \left((1+c)\log\frac{1+c}{4} + (1-c)\log\frac{1-c}{4}\right) = 2\log\frac{1}{4} + (1+c)\log(1+c) + (1-c)\log(1-c) \\ H(AE) &= -\sum_{AB} P(AB)\log(P(AB)) = 8\left(\frac{1+s}{8}\log\frac{1+s}{8} + \frac{1-s}{8}\log\frac{1-s}{8}\right) \\ &= \left((1+s)\log\frac{1+s}{8} + (1-s)\log\frac{1-s}{8}\right) = 2\log\frac{1}{8} + (1+s)\log(1+s) + (1-s)\log(1-s) \end{aligned} \tag{34}$$

to finally, after expressing $\log\frac{1}{4} = \log 2 + \log\frac{1}{8}$, get:

$$\boxed{\begin{aligned} I(A:B) &= H(A) + H(B) - H(AB) = (1+c)\log(1+c) + (1-c)\log(1-c) \\ I(A:E) &= H(A) + H(E) - H(AE) = (1+s)\log(1+s) + (1-s)\log(1-s) - \log 2 \end{aligned}} \tag{35}$$

which tell us that there is a positive gap in the mutual information and therefore possible security (after error correction and destilation) for $\cos(\eta) > \sin(\eta) + \text{Ct}$, as one would have expected from the original transformation of Eve $U(\eta)$.

Exercise 4: Computation of key rates

In the six-state protocol, Alice prepares the eigenstates of σ_x, σ_y and σ_z, and sends them to Bob, who measures these observables. After basis reconciliation, Alice and Bob keep only those cases in which they use the same basis. In the entanglement-based picture, the protocol is basically equivalent to the preparation of the two-qubit maximally entangled state on which Alice and Bob measure the three Pauli operators. Consider now that Alice and Bob are connected by the so-called qubit depolarizing channel defined as

$$\mathcal{D}_p(X) = pX + (1-p)\frac{\mathbb{1}}{2}\mathrm{tr}(X). \tag{36}$$

(a) Compute the state between Alice and Bob resulting from applying this channel to half of the maximally entangled state

$$\begin{aligned}\rho_{AB} &= (\mathbb{1}_A \otimes \mathcal{D}_p(|\Phi\rangle\langle\Phi|_{AB}) = p\,|\Phi\rangle\langle\Phi|_{AB} + (1-p)\Big(\mathbb{1}_A \otimes \frac{\mathbb{1}_B}{2} tr_B\Big)(|\Phi\rangle\langle\Phi|)_{AB} = \\ &= p\,|\Phi\rangle\langle\Phi|_{AB} + (1-p)\frac{1}{2}\Big(\,|0\rangle\langle 0|_A \frac{\mathbb{1}_B}{2} + |0\rangle\langle 1|_A \cancelto{\mathbb{1}_B}{tr(|0\rangle\langle 1|)}\cancelto{0}{\frac{\mathbb{1}_B}{2}} + \cancelto{0}{(\ldots)^\dagger} + |1\rangle\langle 1|_A \frac{\mathbb{1}_B}{2}\Big) = \\ &= \boxed{p\,|\Phi\rangle\langle\Phi|_{AB} + (1-p)\frac{\mathbb{1}_{AB}}{4}} = \frac{1}{2}\begin{pmatrix} p & 0 & 0 & p \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ p & 0 & 0 & p \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 1-p & 0 & 0 & 0 \\ 0 & 1-p & 0 & 0 \\ 0 & 0 & 1-p & 0 \\ 0 & 0 & 0 & 1-p \end{pmatrix}\end{aligned} \tag{37}$$

(b) Compute the probabilities of the results by Alice and Bob when they both measure in the z basis

$$P(\pm,\pm) = \langle \pm z|\langle \pm z|\rho_{AB}|\pm z\rangle|\pm z\rangle. \tag{38}$$

From the matrix representation in eq.37 its trivial, since we are just asked to get the diagonal elements:

$$\boxed{\begin{cases} P(+,+) = P(-,-) = \frac{p}{2} + \frac{1-p}{4} = \frac{1+p}{4} \\ P(+,-) = P(-,+) = 0 + \frac{1-p}{4} = \frac{1-p}{4} \end{cases}} \tag{39}$$

(c) Include Eve in the picture by providing a purification of the state ρ_{AB}, that is, a pure state $|\psi\rangle_{ABE}$ such that $\mathrm{tr}_E|\Psi\rangle\langle\Psi|_{ABE} = \rho_{AB}$.

To include Eve in the picture, we just need to diagonalize our state ρ_{AB} and then we can use that for $\rho_S = \sum_i \lambda_i\,|i\rangle\langle i|$ we can purify the state with $|\psi\rangle_{SE} = \sum_i \sqrt{(}\lambda_i)\,|i\rangle\,|e_i\rangle$ using any basis $|e_i\rangle$ (There are infinitely many possible purifications all a Unitary/change of basis away).

So first from matrix representation we can see that we have a p component of $|\Phi^+\rangle\langle\Phi^+|$, plus an identity ($\mathbb{1}$) of $\frac{1-p}{4}$, and since the identity can be expanded as a sum of:

$$\mathbb{1} = \Big|\Phi^+\Big\rangle\Big\langle\Phi^+\Big| + |\Phi^-\rangle\langle\Phi^-| + \Big|\Psi^+\Big\rangle\Big\langle\Psi^+\Big| + |\Psi^-\rangle\langle\Psi^-| \tag{40}$$

then our state ends up in diagonal form like:

$$\begin{aligned}\rho_{AB} &= p\Big|\Phi^+\Big\rangle\Big\langle\Phi^+\Big| + \frac{1-p}{4}\Big(\Big|\Phi^+\Big\rangle\Big\langle\Phi^+\Big| + |\Phi^-\rangle\langle\Phi^-| + \Big|\Psi^+\Big\rangle\Big\langle\Psi^+\Big| + |\Psi^-\rangle\langle\Psi^-|\Big) \\ &= \frac{1+3p}{4}\Big|\Phi^+\Big\rangle\Big\langle\Phi^+\Big| + \frac{1-p}{4}\Big(|\Phi^-\rangle\langle\Phi^-| + \Big|\Psi^+\Big\rangle\Big\langle\Psi^+\Big| + |\Psi^-\rangle\langle\Psi^-|\Big)\end{aligned} \tag{41}$$

and its purification is:

$$\boxed{|\Psi\rangle_{ABE} = \sqrt{\frac{1+3p}{4}}\Big|\phi^+\Big\rangle|1\rangle + \sqrt{\frac{1-p}{4}}\Big(\,|\phi^-\rangle|2\rangle + \Big|\psi^+\Big\rangle|3\rangle + |\psi^-\rangle|4\rangle\Big)} \tag{42}$$

(d)Compute now the state between Alice, Bob and Eve after Alice and Bob measure in the z basis

$$\rho_{ABE} = \sum_{a,b=\pm} P(a,b)|a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |e^{ab}\rangle\langle e^{ab}|_E, \tag{43}$$

where $|e_E^{\pm\pm}\rangle$ is given by $\langle \pm z|_A \otimes \langle \pm z|_B \otimes \mathbb{1}_E|\Psi\rangle_{ABE}$ after normalization.

We can do this quicker if we take into account that the normalization is the square root of the probability, there defining:

$$|\bar{e}_E^{\pm\pm}\rangle = \langle \pm z|_A \otimes \langle \pm z|_B \otimes \mathbb{1}_E|\Psi\rangle_{ABE} \quad \boxed{\begin{cases} |\bar{e}_E^{++/--}\rangle = \left(\sqrt{\frac{1+3p}{4}}\,|1\rangle \pm \sqrt{\frac{1-p}{4}}\,|2\rangle\right)/\sqrt{2} \\ |\bar{e}_E^{+-/-+}\rangle = \sqrt{\frac{1-p}{4}}\frac{|3\rangle \pm |4\rangle}{\sqrt{2}} \end{cases}} \tag{44}$$

we will have that the state after Alice and Bob measure is:

$$\boxed{\rho_{ABE} = \sum_{a,b=\pm} |a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |\bar{e}^{ab}\rangle\langle \bar{e}^{ab}|_E} \tag{45}$$

for which we need to compute $|\bar{e}^{ab}\rangle\langle \bar{e}^{ab}|_E$:

$$|\bar{e}^{ab}\rangle\langle \bar{e}^{ab}|_E = \begin{cases} |\bar{e}_E^{++/--}\rangle\langle \bar{e}_E^{++/--}| = \frac{1}{2}\Big(\frac{1+3p}{4}\,|1\rangle\langle 1| + \frac{1-p}{4}\,|2\rangle\langle 2| \pm \sqrt{\frac{1+3p}{4}}\sqrt{\frac{1-p}{4}}(|1\rangle\langle 2| + |2\rangle\langle 1|)\Big) \\ |\bar{e}_E^{+-/-+}\rangle\langle \bar{e}_E^{+-/-+}| = \frac{1-p}{8}\Big(\,|3\rangle\langle 3| + |4\rangle\langle 4| \pm (|3\rangle\langle 4| + |4\rangle\langle 3|)\Big) \end{cases} \tag{46}$$

which give a final expression for the state:

$$\begin{aligned} \boxed{\rho_{ABE} = \frac{1}{8}\Big[} & |+\rangle\langle +| \otimes |+\rangle\langle +| \otimes \Big((1+3p)\,|1\rangle\langle 1| + (1-p)\,|2\rangle\langle 2| + \sqrt{1+3p}\sqrt{1-p}(|1\rangle\langle 2| + |2\rangle\langle 1|)\Big) \\ & + |+\rangle\langle +| \otimes |-\rangle\langle -| \otimes (1-p)\Big(\,|3\rangle\langle 3| + |4\rangle\langle 4| + (|3\rangle\langle 4| + |4\rangle\langle 3|)\Big) + \\ & + |-\rangle\langle -| \otimes |+\rangle\langle +| \otimes (1-p)\Big(\,|3\rangle\langle 3| + |4\rangle\langle 4| - (|3\rangle\langle 4| + |4\rangle\langle 3|)\Big) + \\ & + |-\rangle\langle -| \otimes |-\rangle\langle -| \otimes \Big((1+3p)\,|1\rangle\langle 1| + (1-p)\,|2\rangle\langle 2| - \sqrt{1+3p}\sqrt{1-p}(|1\rangle\langle 2| + |2\rangle\langle 1|)\Big)\Big] = \\ & = \frac{1}{8}\begin{pmatrix} \begin{pmatrix} 1+3p & \sqrt{1+3p}\sqrt{1-p} \\ \sqrt{1+3p}\sqrt{1-p} & 1-p \end{pmatrix} & \begin{pmatrix} 1-p & 1-p \\ 1-p & 1-p \end{pmatrix} \\ \begin{pmatrix} 1-p & -(1-p) \\ -(1-p) & 1-p \end{pmatrix} & \begin{pmatrix} 1+3p & -\sqrt{1+3p}\sqrt{1-p} \\ -\sqrt{1+3p}\sqrt{1-p} & 1-p \end{pmatrix} \end{pmatrix} \end{aligned} \tag{47}$$

(e) Compute the two terms appearing in the Devetak-Winter bound, $I(A:B)$ and $\chi(A:E)$, where

$$\chi(A:E) = S(\rho_E) - \sum_{a=\pm} p(a)S(\rho_E^a), \tag{48}$$

$S(\rho) = -\mathbf{tr}(\rho\log\rho)$ is the standard von Neumann entropy, $\rho_E^a = \sum_{b=\pm} p(b|a)|e^{ab}\rangle\langle e^{ab}|_E$ and $\rho_E = \sum_a p(a)\rho_E^a = \mathbf{tr}_{AB}|\Psi\rangle\langle\Psi|_{ABE}$. Calculate the value of p for which the Devetak-Winter bound becomes equal to zero.

(Don't have time for this part)