Exercise 1. ***Properties of the variational distance***

Given two probability distributions P_X and Q_X with the same alphabet, the variational distance between them is defined as

$$D(P_X, Q_X) = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|. \tag{1}$$

(a) **Operational meaning.** Suppose that you are given one of two dice, P and Q, at random with equal probability. Your task is to guess which die you were given. You know that both dice are biased: the probability of obtaining the different outcomes $X = \{1, \ldots, 6\}$ are given by distributions P_X for die P and Q_X for Q. You are allowed to throw the die only once. Show that your probability of guessing correctly is given by

$$\Pr(\checkmark) = \frac{1}{2}\left(1 + D(P_X, Q_X)\right). \tag{2}$$

Solution. Your best strategy is to say it was the die more likely to outcome the result you obtained, ie. if you define the event $\mathcal{S} = \{x \in \mathcal{X} : P_X(x) \geq Q_X(x)\}$ (the results that are more likely with die P), than you better say that you threw die P if you get an outcome $x \in \mathcal{S}$ and Q if $x \in \bar{\mathcal{S}}$.

The probability that your guess is right is

$$\begin{aligned}\Pr(\checkmark) &= \Pr(\text{die } P)\cdot\Pr(\text{guess } P|\text{die } P) + \Pr(\text{die } Q)\cdot\Pr(\text{guess } Q|\text{die } Q)\\ &= \frac{1}{2}P_X(\mathcal{S}) + \frac{1}{2}Q_X(\bar{\mathcal{S}})\\ &= \frac{1}{2}P_X(\mathcal{S}) + \frac{1}{2}[1 - Q_X(\mathcal{S})]\\ &= \frac{1}{2}\left[1 + P_X(\mathcal{S}) - Q_X(\mathcal{S})\right].\end{aligned}$$

Now we show that we can write the variational distance as $P_X(\mathcal{S}) - Q_X(\mathcal{S})$. We start with

$$\begin{aligned}0 &= \sum_{x\in\mathcal{X}} P_X(x) - Q_X(x)\\ &= \sum_{x\in S}|P_X(x) - Q_X(x)| - \sum_{x\in\bar{\mathcal{S}}}|P_X(x) - Q_X(x)|\end{aligned}$$

The terms $P_X(x) - Q_X(x)$ are positive in the first sum on the right-hand side and negative in the second sum. We can therefore get rid of the absolute values, writing

$$\sum_{x\in S} P_X(x) - Q_X(x) = -\sum_{x\in\bar{\mathcal{S}}} P_X(x) - Q_X(x)$$

$$|\sum_{x\in\mathcal{S}} P_X(x) - Q_X(x)| = \sum_{x\in\bar{\mathcal{S}}}|P_X(x) - Q_X(x)| = \frac{1}{2}\sum_{x\in\mathcal{X}}|P_X(x) - Q_X(x)|.$$

(b) **Triangle inequality.** Show that, for any three probability distributions P_X, Q_X and R_X,

$$D(P_X, Q_X) + D(Q_X, R_X) \geq D(P_X, R_X). \tag{3}$$

Solution. The triangle inequality can be written as

$$\frac{1}{2}\sum_{x\in\mathcal{X}}|P_X(x) - R_X(x)| \leq \frac{1}{2}\sum_{x\in\mathcal{X}}|P_X(x) - Q_X(x)| + |Q_X(x) - R_X(x)|.$$

If the inequality is true for every $x \in \mathcal{X}$, it is also true for the above sum. It is thus sufficient to prove that $|P_X(x) - R_X(x)| \leq |P_X(x) - Q_X(x)| + |Q_X(x) - R_X(x)|$ for all $x \in \mathcal{X}$. We know that $|\alpha + \beta| \leq |\alpha| + |\beta|$ for $\alpha, \beta \in \mathbb{R}$. Hence the inequality follows with $\alpha = P_X(x) - Q_X(x)$ and $\beta = Q_X(x) - R_X(x)$.

(c) **Distance to uniform distribution.** Let $P_X = (p, 1-p)$ be a binary probability distribution. Show that

$$D(P_X, 1 - P_X) = 2D(P_X, U_x), \tag{4}$$

where $U_X = (\frac{1}{2}, \frac{1}{2})$ is the uniform distribution.

Solution. We can write

$$D(P_X, 1-P_X) = \frac{1}{2}\sum_x |P_X(x) - (1-P_X(x))| = \frac{1}{2}\sum_x |2P_X(x)-1| = \sum_x \left|P_X(x) - \frac{1}{2}\right| = 2\,D(P_X, U_X)\ .$$

(d) **Joint distributions.** Let P_{XY} be a joint probability distribution, with marginals P_X and P_Y that have the same alphabet. Show that $D(P_X, P_Y) \leq \Pr[X \neq Y]$.

Solution.

$$\begin{aligned} D(P_X, P_Y) &= \frac{1}{2}\sum_x \Big|\sum_y P_{XY}(x,y) - \sum_{x'} P_{XY}(x',x)\Big| \\ &\leqslant \frac{1}{2}\sum_x \Big|\sum_y P_{XY}(x,y) - P_{XY}(x,x)\Big| + \frac{1}{2}\sum_x \Big|\sum_{x'} P_{XY}(x',x) - P_{XY}(x,x)\Big| \\ &= \frac{1}{2}\sum_x \sum_{y\neq x} P_{XY}(x,y) + \frac{1}{2}\sum_y \sum_{x\neq y} P_{XY}(x,y) = \sum_{x\neq y} P_{XY}(x,y) = \Pr\left[X \neq Y\right]\ . \end{aligned}$$

Exercise 2. *Playing Eve*

You are Eve, and are trying your best to thwart Alice and Bob's plans to share a secret key using the quantum key distribution protocol BB84. You will hack into their insecure quantum channel, capture the qubit sent by Alice, measure it in some basis, and then send it to Bob. [Note that this is not the most general attack possible.] You are trying to pick the best possible basis to measure Alice's qubit. Remember that you want to minimize the errors that can be detected by Alice and Bob, while trying to maxime the number of bits you guess correctly. Let's try a few different bases. For each case, compute the fraction of bits that you guess correctly, and the error rate induced in Alice and Bob's key, after sifting.

(a) In your first attempt, you will measure all of Alice's qubits in the Z basis.

(b) In your second attempt, you will pick X or Z at random, with equal probability, for each qubit.

(c) More generally, you can measure in an orthonormal basis of the form

$$\left\{\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \cos\frac{\theta+\pi}{2}|0\rangle + \sin\frac{\theta+\pi}{2}|1\rangle\right\}.$$

For instance, picking $\theta = 0$ gives you the Z basis, while $\theta = \frac{\pi}{2}$ results in the X basis. What happens for $\theta = \frac{\pi}{4}$?

Solution. The solution to this exercise is attached on page 4.

Exercise 3. *Chained Bell inequalities*

Consider the following setting. Alice and Bob own one black box each. Alice's box takes an input a from a set $A = \{0, 2, \ldots, 2N-2\}$ and outputs a bit $x \in \{0,1\}$. Similarly, Bob's box takes an input b from a set $B = \{1, 3, \ldots, 2N-1\}$ and outputs $y \in \{0,1\}$.

We define the following measure of correlations,

$$I_N = \Pr(X = Y | A = 0, B = 2N-1) + \sum_{|a-b|=1} \Pr(X \neq Y | A = a, B = b) \tag{5}$$

We want I_N to be small, because then it is possible to show that the outcomes of adjacent inputs a and $b = a \pm 1$ are the same, and unknown to an adversary, with high probability. [This is a generalization of the theorem from the lecture, with $I_2 \mapsto I_N$.]

(a) We will see a physical example of a family of "black boxes" that achieves $I_N \to 0$. Each box corresponds to a quantum measurement device that acts on a single qubit. The qubits to be measured, one in Alice's box and one in Bob's, are maximally entantled.

Let $\{|\uparrow\rangle, |\downarrow\rangle\}$ be an orthonormal basis for a qubit (for instance the Z basis). Suppose that Alice's choices of input a correspond to a POVM $\{E_0^a, E_1^a\}$, on a single qubit, with E_0^a is the projector onto state $|\frac{a}{2N}\pi\rangle$, and E_1^a is the projector onto state $|\left(\frac{a}{2N}+1\right)\pi\rangle$, with $|\theta\rangle = \cos\frac{\theta}{2}|\uparrow\rangle + \sin\frac{\theta}{2}|\downarrow\rangle$. The same holds for Bob's measurements b. Furthermore, suppose that the POVMs on Alice's and Bob's sides act each on a qubit of the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Show that, in these conditions,

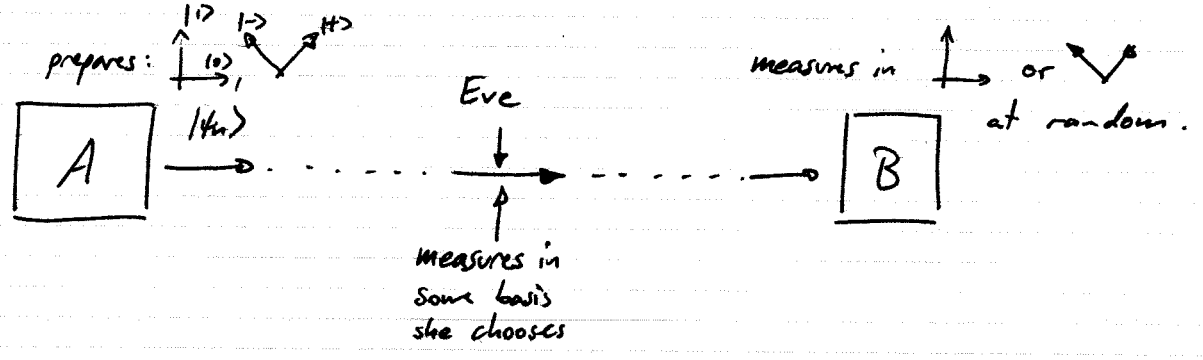
$$I_N = 2N \sin^2 \frac{\pi}{4N} \leq \frac{\pi^2}{8N}. \tag{6}$$

Solution. The solution to this exercise is attached on page 7.

(b) How would you adapt the protocol from the lecture to take advantge of this Bell inequality?

Solution. By measuring in such a basis, Alice and Bob can achieve a lower "secrecy" value $I_N \to 0$ (for large N) instead of I_2, and the two key bits will differ with lower probability.

Solution to Exercise 2.



Note that it is only important to look at the bits that are kept after sifting, ie. those where B measured in the same basis as Alice prepared.

(a) Eve measures in the Z basis.

if A prepared $|0\rangle$ or $|1\rangle$, ($\frac{1}{2}$ of the time), Eve gets full information about the bit, and introduces no error.

if A prepared $|+\rangle$ or $|-\rangle$, ($\frac{1}{2}$ of the time), Eve gets a completely random outcome, independent of the bit value. When B measures in the X basis, Eve's post-meas. state will again collapse randomly onto $|+\rangle$ or $|-\rangle$, introducing an error with probability $\frac{1}{2}$.

In total: * $\frac{1}{2}$ of the bits are fully known to Eve
$+\frac{1}{4}$ guessed correctly by chance $= \frac{3}{4}$

* $\frac{1}{4}$ of the sifted key will differ between A & B.

(b) Eve measures randomly in X or Z.

Eve will measure in the "wrong" basis $\frac{1}{2}$ of the time, so the same conclusions hold as in part (a).

(c) Let $|\vartheta_0\rangle = \cos\frac{\vartheta}{2}|0\rangle + \sin\frac{\vartheta}{2}|1\rangle$
$|\vartheta_1\rangle = -\sin\frac{\vartheta}{2}|0\rangle + \cos\frac{\vartheta}{2}|1\rangle$.

Then, if Alice prepares $|0\rangle$ or $|1\rangle$, the measurement probabilities for Eve are

$\langle\vartheta_0|0\rangle = \cos\frac{\vartheta}{2} \rightarrow |\langle\vartheta_0|0\rangle|^2 = \cos^2\frac{\vartheta}{2} = \frac{1}{2}(1+\cos\vartheta)$
$\langle\vartheta_0|1\rangle = \sin\frac{\vartheta}{2} \rightarrow |\langle\vartheta_0|1\rangle|^2 = \sin^2\frac{\vartheta}{2} = \frac{1}{2}(1-\cos\vartheta)$
$\langle\vartheta_1|0\rangle = -\sin\frac{\vartheta}{2} \rightarrow |\langle\vartheta_1|0\rangle|^2 = \sin^2\frac{\vartheta}{2} = \frac{1}{2}(1-\cos\vartheta)$
$\langle\vartheta_1|1\rangle = \cos\frac{\vartheta}{2} \rightarrow |\langle\vartheta_1|1\rangle|^2 = \cos^2\frac{\vartheta}{2} = \frac{1}{2}(1+\cos\vartheta)$

Likewise, in the $|+\rangle/|-\rangle$ basis we have:

$\langle\vartheta_0|+\rangle = \frac{1}{\sqrt{2}}(\cos\frac{\vartheta}{2}+\sin\frac{\vartheta}{2}) \rightarrow |\langle\vartheta_0|+\rangle|^2 = \frac{1}{2}(1+\sin\vartheta)$
$\langle\vartheta_0|-\rangle = \frac{1}{\sqrt{2}}(\cos\frac{\vartheta}{2}-\sin\frac{\vartheta}{2}) \rightarrow |\langle\vartheta_0|-\rangle|^2 = \frac{1}{2}(1-\sin\vartheta)$
$\langle\vartheta_1|+\rangle = \frac{1}{\sqrt{2}}(\cos\frac{\vartheta}{2}-\sin\frac{\vartheta}{2}) \rightarrow |\langle\vartheta_1|+\rangle|^2 = \frac{1}{2}(1-\sin\vartheta)$
$\langle\vartheta_1|-\rangle = \frac{1}{\sqrt{2}}(\cos\frac{\vartheta}{2}-\sin\frac{\vartheta}{2}) \rightarrow |\langle\vartheta_1|-\rangle|^2 = \frac{1}{2}(1+\sin\vartheta)$

Let's say Eve guesses the bit value "0" whenever she gets $|\vartheta_0\rangle$.
Then her total probability of guessing correctly is:

$$\Pr(\text{correct guess}) = \underbrace{\frac{1}{2}}_{\Pr[\text{Alice uses } Z]} \cdot \underbrace{\frac{1}{2}(1+\cos\vartheta)}_{\Pr[\text{guess correctly if Alice encoded in } Z]} + \underbrace{\frac{1}{2}\cdot\frac{1}{2}(1+\sin\vartheta)}_{\text{same, for } X} = \frac{1}{2}+\frac{1}{4}(\sin\vartheta+\cos\vartheta)$$

for $\vartheta = \frac{\pi}{4}$, $\Pr[\text{correct guess}] = \frac{1}{2}+\frac{1}{2\sqrt{2}} \approx 85\%$.

Eve will introduce an error if, for example, Alice prepared $|0\rangle$, which collapsed to $|\vartheta_0\rangle$, but then failed to collapse back to $|0\rangle$ at Bob's side.
The total probability of introducing an error is:

Solution to Exercise 2.

Alice can prepare $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ each prob $= 1/4$.

collapse to $|0\rangle$ or $|1\rangle$

Alice $|0\rangle$

collapses back to $|0\rangle$

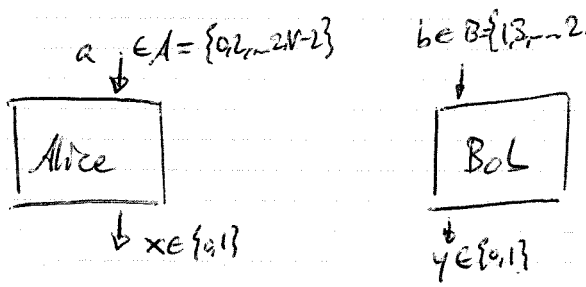
$$\Pr[\text{error}] = \frac{1}{4}\Big[|\langle \delta_0|0\rangle|^2 |\langle \delta_0|1\rangle|^2 + |\langle \delta_0|1\rangle|^2 |\langle \delta_0|0\rangle|^2 + |\langle \delta_1|0\rangle|^2 |\langle \delta_1|1\rangle|^2 + |\langle \delta_1|1\rangle|^2 |\langle \delta_1|0\rangle|^2$$

$$+ |\langle \delta_0|+\rangle|^2 |\langle \delta_0|-\rangle|^2 + |\langle \delta_0|-\rangle|^2 |\langle \delta_0|+\rangle|^2 + |\langle \delta_1|+\rangle|^2 |\langle \delta_1|-\rangle|^2 + |\langle \delta_1|-\rangle|^2 |\langle \delta_1|-\rangle|^2 \Big]$$

$$= \frac{1}{4}\Big[\left(\tfrac{1}{4} - \tfrac{1}{4}\cos^2\theta\right) + \left(\tfrac{1}{4} - \tfrac{1}{4}\cos^2\theta\right) + (\quad - \quad) + (\quad - \quad)$$

$$+ \left(\tfrac{1}{4} - \tfrac{1}{4}\sin^2\theta\right) + \left(\tfrac{1}{4} - \tfrac{1}{4}\sin^2\theta\right) + (\quad - \quad) + (\quad - \quad) \Big]$$

$$= \frac{1}{4}(2 - 1) = \frac{1}{4} \qquad \text{(independent of } \theta\text{!)}$$



(thanks D. Esteves for your solutions.)

(a) Let us calculate the quantity I_N:

$$I_N = Pr[X=Y \mid A=a,\ B=2N-1] + \sum_{|a-b|=1} Pr[X \neq Y \mid A=a,\ B=b]$$

$$Pr[X=Y \mid A=0,\ B=2N-1] = Pr[X=Y=0 \mid A=0, B=2N-1] + Pr[X=Y=1 \mid A=0, B=2N-1]$$

$$= \left| \left(\langle 0| \otimes \langle (1-\tfrac{1}{2N})\pi| \right) \tfrac{1}{\sqrt{2}} (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2 + \left| \left(\langle \pi| \otimes \langle (2-\tfrac{1}{2N})\pi| \right) \tfrac{1}{\sqrt{2}} (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2$$

($a=0$, $x=0$; $b=2N-1$, $y=0$; $a=0$, $x=1$; $b=2N-1$, $y=1$)

$$= \tfrac{1}{2} \left| \left(\cos\left(1-\tfrac{1}{2N}\right)\tfrac{\pi}{2} \right) \langle\uparrow\uparrow| + \sin\left(1-\tfrac{1}{2N}\right)\tfrac{\pi}{2} \langle\downarrow\downarrow| \right) (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2 +$$

$$\tfrac{1}{2} \left| \left(\cos\left(2-\tfrac{1}{2N}\right)\tfrac{\pi}{2} \right) \langle\downarrow\uparrow| + \sin\left(2-\tfrac{1}{2N}\right)\tfrac{\pi}{2} \langle\downarrow\downarrow| \right) (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2$$

$$= \tfrac{1}{2} \cos^2\left(1-\tfrac{1}{2N}\right)\tfrac{\pi}{2} + \tfrac{1}{2} \sin^2\left(2-\tfrac{1}{2N}\right)\tfrac{\pi}{2}$$

$$\cos\left(\tfrac{\pi}{2} - \tfrac{1}{2N}\tfrac{\pi}{2}\right) = -\sin\left(-\tfrac{1}{2N}\tfrac{\pi}{2}\right) = \sin\tfrac{\pi}{4N}$$

$$\sin\left(\pi - \tfrac{1}{2N}\tfrac{\pi}{2}\right) = -\sin\left(-\tfrac{1}{2N}\tfrac{\pi}{2}\right) = \sin\tfrac{\pi}{4N}$$

$$= \tfrac{1}{2} \left[\sin^2\tfrac{\pi}{4N} + \sin^2\tfrac{\pi}{4N} \right] = \sin^2\tfrac{\pi}{4N}$$

$$Pr[X \neq Y \mid A=a, B=b] = Pr[X=0, Y=1 \mid A=a, B=b] + Pr[X=1, Y=0 \mid A=a, B=b]$$

$$= \left| \left\langle \left(\tfrac{a}{2N}\pi\right) \right| \otimes \left\langle \left(\tfrac{b}{2N}+1\right) \right| \cdot \tfrac{1}{\sqrt{2}} (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2 + \left| \left\langle \left(\tfrac{a}{2N}+1\right)\pi \right| \otimes \left\langle \tfrac{b}{2N}\pi \right| \tfrac{1}{\sqrt{2}} (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \right|^2$$

$$= \tfrac{1}{2} \left| \cos\tfrac{a}{2N}\tfrac{\pi}{2} \cos\left(\left(\tfrac{b}{2N}+1\right)\tfrac{\pi}{2}\right) + \sin\tfrac{a}{2N}\tfrac{\pi}{2} \sin\left(\left(\tfrac{b}{2N}+1\right)\tfrac{\pi}{2}\right) \right|^2$$

$$+ \tfrac{1}{2} \left| \cos\left(\left(\tfrac{a}{2N}+1\right)\tfrac{\pi}{2}\right) \cos\left(\tfrac{b}{2N}\tfrac{\pi}{2}\right) + \sin\left(\left(\tfrac{a}{2N}+1\right)\tfrac{\pi}{2}\right) \cos\tfrac{b}{2N}\tfrac{\pi}{2} \right|^2$$

$$\cos\left(x+\tfrac{\pi}{2}\right) = -\sin x$$

$$\sin\left(x+\tfrac{\pi}{2}\right) = \cos x$$

$$= \tfrac{1}{2} \left(\underbrace{-\cos\tfrac{a\pi}{2N} \sin\tfrac{b\pi}{2N} + \sin\tfrac{a\pi}{2N} \cos\tfrac{b\pi}{2N}}_{= \sin\left[(a-b)\cdot\frac{\pi}{4N}\right]} \right)^2 + \tfrac{1}{2} \left(\underbrace{-\sin\tfrac{a\pi}{2N} \cos\tfrac{b\pi}{2N} + \cos\tfrac{a\pi}{2N} \sin\tfrac{b\pi}{2N}}_{\text{Same}} \right)^2$$

$|a-b| = \pm 1$

$$= \sin^2\tfrac{\pi}{4N}.$$

$\sin x \leq x$ ($x \geq 0$)

$$\Rightarrow I_N = \left[1 + (2N-1)\right] \sin^2\tfrac{\pi}{4N} = 2N \cdot \sin^2\tfrac{\pi}{4N} \leq \tfrac{\pi^2}{8N}$$