Exercise 1. *Eavesdropping quantified*

(a) Consider the following setting.

Alice and Bob are given a choice between two different coins; Alice can toss either coin A_0 or coin A_2 and Bob, either B_1 or B_3. For each toss each party must choose one of the two; tossing both A_0 and A_2 or both B_1 and B_3 is forbidden.

Suppose that Eve wants to manufacture a device that outputs values, Z, designed to tally with A_0. Show that Eve has limited chances to succeed by proving the inequality

$$\Pr(Z = A_0) \leq \frac{1}{2}(1 + I_2), \tag{1}$$

where

$$I_2 = \Pr(A_0 \neq B_1) + \Pr(B_1 \neq A_2) + \Pr(A_2 \neq B_3) + \Pr(B_3 = A_0).$$

Hint. Show and use the following inequality

$$\Pr(A_i = Z) - \Pr(B_j = Z) \leq \Pr(A_i \neq B_j) \quad i \in \{0, 2\}, j \in \{1, 3\}.$$

The scenario can be generalised as follows: Alice has now the choice among $N \geq 2$ different coins A_i indexed by $i \in \{0, 2, \ldots, 2N-2\}$. Similarly, Bob has the choice between N coins B_j labelled by $t\ j \in \{1, 3, \ldots, 2N-1\}$. As before Alice and Bob can only toss one of their coins at the same time.

(b) Show that for N measurements

$$\Pr(Z = A_0) \leq \frac{1}{2}(1 + I_N), \tag{2}$$

where

$$I_N = \Pr(A_0 = B_{2N-1}) + \sum_{|i-j|=1} \Pr(A_i \neq B_i) \tag{3}$$

holds.

(c) We will now see that quantum systems can be used to achieve $I_N \to 0$. Alice and Bob share a qubit in a maximally entangled state

$$\frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle).$$

Alice's coin toss is implemented by a measurement w.r.t. $\{E_0^i, E_1^i\}$ on her qubit, where E_0^a is the projector onto state $|\frac{i}{2N}\pi\rangle$ (corresponding to outcome "0"), and E_1^i is the projector onto state $|\left(\frac{i}{2N}+1\right)\pi\rangle$ (corresponding to outcome "1"), with $|\theta\rangle = \cos\frac{\theta}{2}|\uparrow\rangle + \sin\frac{\theta}{2}|\downarrow\rangle$. The same holds for Bob's measurements B_j.

Show that,

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

Solution.

(a) We have

$$\begin{aligned}\Pr(A_i = Z) &= \Pr(A_i \neq B_j \wedge B_j \neq Z) + \Pr(A_i = B_j \wedge B_j = Z) \\ &\leq \Pr(A_i \neq B_j) + \Pr(B_j = Z)\end{aligned}$$

$$\Rightarrow \Pr(A_i = Z) - \Pr(B_j = Z) \leq \Pr(A_i \neq B_j).$$

This implies a sequence of inequalities:

$$\Pr(A_0 = Z) - \Pr(B_1 = Z) \leq \Pr(A_0 \neq B_1)$$

$$\Pr(B_1 = Z) - \Pr(A_2 = Z) \leq \Pr(A_2 \neq B_1)$$

$$\Pr(A_2 = Z) - \Pr(B_3 = Z) \leq \Pr(A_2 \neq B_3)$$

$$\Pr(B_3 = Z) - \Pr(A_0 \neq Z) \leq \Pr(A_0 = B_3)$$

where the last inequality follows from analogous reasoning as above.
Adding these inequalities together and taking into account that $\Pr(Z \neq A_0) = 1 - \Pr(Z = A_0)$ gives

$$\Pr(Z = A_0) \leq \frac{1}{2}\left(1 + I_2\right).$$

(b) The proof is analogous to part (a).

$$\Pr(A_0 = Z) - \Pr(B_1 = Z) \leq \Pr(A_0 \neq B_1)$$

$$\vdots$$

$$\Pr(B_{2N-1} = Z) - \Pr(A_{2N-2} = Z) \leq \Pr(A_{2N-2} \neq B_{2N-1})$$

$$\Pr(B_{2N-1} = Z) - \Pr(A_1 \neq Z) \leq \Pr(A_0 = B_{2N-1})$$

Adding again yields the desired inequality.

(c)

$$\begin{aligned}&\Pr[A_0 = B_{2N-1}] \\ &= \Pr[A_0 = B_{2N-1} = 0] + \Pr[A_0 = B_{2N-1} = 1] \\ &= \left|\langle 0| \otimes \langle \left(1 - \frac{1}{2N}\right)\pi| \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)\right|^2 + \left|\langle \pi| \otimes \langle \left(2 - \frac{1}{2N}\right)\pi| \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)\right|^2 \\ &= \frac{1}{2}\left|\left(\cos((1 - \frac{1}{2N})\frac{\pi}{2})\langle\uparrow\uparrow| + \sin((1 - \frac{1}{2N})\frac{\pi}{2})\langle\uparrow\downarrow| + \langle\right) \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)\right|^2 \\ &+ \frac{1}{2}\left|\left(\cos((2 - \frac{1}{2N})\frac{\pi}{2})\langle\downarrow\uparrow| + \sin((2 - \frac{1}{2N})\frac{\pi}{2})\langle\downarrow\downarrow| + \langle\right) \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)\right|^2 \\ &= \frac{1}{2}\cos^2((1 - \frac{1}{2N})\frac{\pi}{2})^2 + \frac{1}{2}\sin^2((2 - \frac{1}{2N})\frac{\pi}{2})^2 \qquad \text{(S.1)}\end{aligned}$$

Use

$$\cos(\frac{\pi}{2} - \frac{1}{2N}\frac{\pi}{2}) = \sin(\frac{\pi}{4N})$$

$$\sin(\pi - \frac{1}{2N}\frac{\pi}{2}) = \sin(\frac{\pi}{4N})$$

$$\Rightarrow (??) = \frac{1}{2}(\sin^2(\frac{\pi}{4N}) + \sin^2(\frac{\pi}{4N})) = \sin^2(\frac{\pi}{4N}).$$

$$\begin{aligned}
&\Pr[A_i \neq B_j] \\
&= \Pr[A_i = 0, B_j = 1] + \Pr[A_i = 1, B_j = 0] \\
&= \left| \langle \frac{i}{2N}\pi| \otimes \langle (\frac{j}{2N}+1)\pi| \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2 + \left| \langle (\frac{i}{2N}+1)\pi| \otimes \langle \frac{j}{2N}\pi| \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle) \right|^2 \\
&= \frac{1}{2}\left| \left(\cos(\frac{i}{2N}\frac{\pi}{2}) \cos((\frac{j}{2N}+1)\frac{\pi}{2}) + \sin(\frac{i}{2N}\frac{\pi}{2}) \sin((\frac{j}{2N}+1)\frac{\pi}{2}) \right) \right|^2 \\
&+ \frac{1}{2}\left| \left(\cos((\frac{i}{2N}+1)\frac{\pi}{2}) \cos(\frac{j}{2N}\frac{\pi}{2}) + \sin((\frac{i}{2N}+1)\frac{\pi}{2}) \sin(\frac{j}{2N}\frac{\pi}{2}) \right) \right|^2 \qquad \text{(S.2)}
\end{aligned}$$

Use

$$\cos(x + \frac{\pi}{2}) = -\sin(x) \quad \sin(x + \frac{\pi}{2}) = \cos(x) \Rightarrow$$

$$(??) = \frac{1}{2}\left(-\cos(\frac{i\pi}{2N}) \sin(\frac{j\pi}{2N}) + \sin(\frac{i\pi}{2N}) \cos(\frac{j\pi}{2N}) \right)^2 + \frac{1}{2}\left(-\sin(\frac{i\pi}{2N}) \cos(\frac{j\pi}{2N}) + \cos(\frac{i\pi}{2N}) \sin(\frac{j\pi}{2N}) \right)^2$$

$$= \frac{1}{2}\sin^2(\underbrace{(i-j)}_{\pm 1}\frac{\pi}{4N}) + \frac{1}{2}\sin^2((i-j)\frac{\pi}{4N}) = \sin^2(\frac{\pi}{4N})$$

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

where we used $\sin(x) \leq x$ for $x > 0$.

Exercise 2. ***Stronger than quantum correlations: The PR-Box***

Let us consider again the case of two coins with correlations summarised by the following table.

Alice		A_0		A_2	
Bob		0	1	0	1
B_1	0	$\frac{1}{2}-\epsilon$	ϵ	$\frac{1}{2}-\epsilon$	ϵ
	1	ϵ	$\frac{1}{2}-\epsilon$	ϵ	$\frac{1}{2}-\epsilon$
B_3	0	ϵ	$\frac{1}{2}-\epsilon$	$\frac{1}{2}-\epsilon$	ϵ
	1	$\frac{1}{2}-\epsilon$	ϵ	ϵ	$\frac{1}{2}-\epsilon$

The entries in the tables correspond to the conditional probabilities of the joint outcomes, e.g. he first entry means $P_{XY|A_0B_1}((x,y) = (0,0)) = \frac{1}{2} - \epsilon$.

We have seen in the lecture that these correlations can be created within quantum mechanics for $\epsilon = \frac{1}{2}\sin^2(\pi/8) \approx 0.07$.

In the following we will denote by $X \in \{0,1\}$ *the outcome of Alice's coin toss and by* $Y \in \{0,1\}$ *the outcome of Bob's coin toss.*

(a) Correlations of the above form that exist within quantum theory cannot be created classically. However, they are not the most general distributions we could consider if we are only constrained by the

no-signalling principle: there are in fact other joint distributions that cannot be obtained by measurements on a quantum state, but that nonetheless would not allow for instantaneous information transmission over distance (signalling)

$$P_{X|A_iB_1}(x) = P_{X|A_i}(x), \text{ for } i \in \{0,2\}, x \in \{0,1\}.$$

To see this, look at the following joint probability distribution for $\epsilon = 0$, a so-called PR box:

Alice		A_0		A_2	
Bob		0	1	0	1
B_1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$
B_3	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	1	$\frac{1}{2}$	0	0	$\frac{1}{2}$

Show that the PR box

(i) is non-signalling

(ii) is non-local: $P_{XY|A_iB_j} \neq P_{X|A_i}P_{Y|B_j}$;

(iii) yields $I_N = 0$.

(b) We shall now see how the above quantum correlation (coming from the Bell state) can be simulated using such a PR box combined with deterministic strategies. Imagine that Alice and Bob apply the following strategy:

- *with probability $1-p$ a PR-box;*
- *with probability $p/4$, one of four deterministic boxes, that always outcome 00, 01, 10 and 11 respectively.*

Find p so that the final joint probability distribution equals the one of the Bell state given above.

Solution.

(a) The PR-box is

(i) *non-signalling:*

Alice		A_0		A_2	
Bob		$+$	$-$	$+$	$-$
B_1	$+$	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	$-$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
B_3	$+$	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	$-$	$\frac{1}{2}$	0	0	$\frac{1}{2}$

$$\begin{aligned} P_{X|A_iB_1}(x) = P_{X|A_i}(x), \ \forall i, x \Leftrightarrow \\ \Leftrightarrow \sum_y P_{XY|A_iB_1}(x,y) = \sum_y P_{XY|A_i}(x,y), \ \forall i, x \Leftrightarrow \\ \Leftrightarrow \sum \text{red terms} = \sum \text{orange terms}, \ \forall \text{ columns} \Leftrightarrow \\ \Leftrightarrow \frac{1}{2} = \frac{1}{2} \ \checkmark \end{aligned}$$

The other non-signalling conditions, can be checked similarly.

(ii) *non-local:*

$$P_{XY|A_i,B_j}(x,y) \neq P_{X|A_i}(x)\ P_{Y|B_j}(y),\ \forall i,j,x,y \Leftrightarrow$$

$$\Leftrightarrow P_{XY|A_i,B_j}(x,y) \neq \left[\sum_{y'} P_{XY|A_i,B'_j}(x,y')\right]\left[\sum_{x'} P_{XY|A'_i,B_j}(x',y)\right] \quad \forall i',j',\ \forall i,j,x,y \Leftrightarrow$$

$$\Leftrightarrow \{\text{table cell}\} \neq \left[\sum \{\text{column of the cell}\}\right]\left[\sum \text{row of the cell}\right],\ \forall \text{ cells} \Leftrightarrow$$

$$\Leftrightarrow 0 \text{ or } \frac{1}{2} \neq \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}\ \checkmark$$

(iii) *and yields* $I_N(P_{XY|AB}) = 0$.

Alice		A_0		A_2	
Bob		$+$	$-$	$+$	$-$
B_1	$+$	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	$-$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
B_3	$+$	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	$-$	$\frac{1}{2}$	0	0	$\frac{1}{2}$

$$I_N = \sum \text{red terms} = 0$$

(b) If we look at the first entry in the table (top left), it is straightforward to see that we need

$$(1-p) * \frac{1}{2} + p * \frac{1}{4} = \frac{1}{2} - \epsilon, \tag{S.3}$$

which implies that $p = 4\epsilon$. One can easily verify that this result also works for the other entries in the table.