

Exercise 1. Convex Combinations

- (a) Prove that any convex combination of non-signaling systems is a valid non-signaling system. That is, for any two non-signaling systems $P_{AB|XY}^{(1)}$ and $P_{AB|XY}^{(2)}$ and for all $p \in [0, 1]$, consider the system $Q_{AB|XY}$ defined by

$$Q_{AB|XY}(ab|xy) = p \cdot P_{AB|XY}^{(1)}(ab|xy) + (1 - p) \cdot P_{AB|XY}^{(2)}(ab|xy) \quad \forall x, y, a, b.$$

Show that it is a valid conditional probability distribution and that the non-signaling conditions hold:

$$\begin{aligned} \sum_a Q_{AB|XY}(ab|0y) &= \sum_a Q_{AB|XY}(ab|1y) \quad \forall b, y \\ \sum_b Q_{AB|XY}(ab|x0) &= \sum_b Q_{AB|XY}(ab|x1) \quad \forall a, x \end{aligned}$$

Solution. We will show that a convex combination of two non-signaling systems is also a non-signaling system. For every two non-signaling systems $P_{AB|XY}^{(1)}$ and $P_{AB|XY}^{(2)}$ and any $p \in [0, 1]$:

1. for all x, y, a, b , $Q_{AB|XY}(ab|xy) \geq 0$ since $P_{AB|XY}^{(1)}(ab|xy) \geq 0$, $P_{AB|XY}^{(2)}(ab|xy) \geq 0$ and $1 \geq p \geq 0$
2. for all x, y ,

$$\begin{aligned} \sum_{a,b} Q_{AB|XY}(ab|xy) &= \sum_{a,b} \left(p \cdot P_{AB|XY}^{(1)}(ab|xy) + (1 - p) \cdot P_{AB|XY}^{(2)}(ab|xy) \right) \\ &= p \sum_{a,b} P_{AB|XY}^{(1)}(ab|xy) + (1 - p) \sum_{a,b} P_{AB|XY}^{(2)}(ab|xy) \\ &= p \cdot 1 + (1 - p) \cdot 1 \\ &= 1 \end{aligned}$$

3. since the non-signaling conditions are linear, $Q_{AB|XY}$ fulfills the same non-signaling conditions as $P_{AB|XY}^{(1)}$ and $P_{AB|XY}^{(2)}$.

- (b) If for the CHSH game the winning probability using system $P_{AB|XY}^{(1)}$ is w_1 and the winning probability using system $P_{AB|XY}^{(2)}$ is w_2 , what is the winning probability using the system $Q_{AB|XY}$ as defined above?

Solution. One way to think about the convex combination of two systems, is as if Alice and Bob have the first system, $P_{AB|XY}^{(1)}$, with probability p , and the second system, $P_{AB|XY}^{(2)}$, with probability $1 - p$. Therefore, the probability of winning the CHSH game with the system $Q_{AB|XY}$ is the convex combination of the two winning probabilities, i.e., $p \cdot w_1 + (1 - p) \cdot w_2$.

In the exercise class, we have considered the PR-box (left) and the quantum system $Q_{AB|XY}$ (right) which are given by the measurement statistics displayed in the following tables:

Y \ X		0		1	
		A	B	A	B
0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$
	1	$\frac{1}{2}$	0	$\frac{1}{2}$	0
1	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	1	$\frac{1}{2}$	0	0	$\frac{1}{2}$

Y \ X		0		1	
		A	B	A	B
0	0	$\frac{\sin^2(\frac{\pi}{8})}{2}$	$\frac{\cos^2(\frac{\pi}{8})}{2}$	$\frac{\sin^2(\frac{\pi}{8})}{2}$	$\frac{\cos^2(\frac{\pi}{8})}{2}$
	1	$\frac{\cos^2(\frac{\pi}{8})}{2}$	$\frac{\sin^2(\frac{\pi}{8})}{2}$	$\frac{\cos^2(\frac{\pi}{8})}{2}$	$\frac{\sin^2(\frac{\pi}{8})}{2}$
1	0	$\frac{\sin^2(\frac{\pi}{8})}{2}$	$\frac{\cos^2(\frac{\pi}{8})}{2}$	$\frac{\cos^2(\frac{\pi}{8})}{2}$	$\frac{\sin^2(\frac{\pi}{8})}{2}$
	1	$\frac{\cos^2(\frac{\pi}{8})}{2}$	$\frac{\sin^2(\frac{\pi}{8})}{2}$	$\frac{\sin^2(\frac{\pi}{8})}{2}$	$\frac{\cos^2(\frac{\pi}{8})}{2}$

- (c) Denote by $D_{AB|XY}^{(i,j)}$ the deterministic strategy which outputs (i, j) for every input. For example $D_{AB|XY}^{(0,0)}(00|xy) = 1$ for every x, y . Find $p \in [0, 1]$ such that the quantum system above is given by

$$Q_{AB|XY}(ab|xy) = (1 - p) \cdot PR_{AB|XY}(ab|xy) + \sum_{(i,j)} \frac{p}{4} \cdot D_{AB|XY}^{(i,j)}(ab|xy) \quad \forall x, y, a, b$$

where $PR_{AB|XY}$ is the perfect PR-box.

Solution. Consider for example the first entry in the table $Q_{AB|XY}(00|00)$. The only deterministic system which affects this entry in the convex combination is the system $D_{AB|XY}^{(0,0)}$. Therefore we must have

$$(1 - p) \cdot 0 + \frac{p}{4} = \frac{\sin^2(\frac{\pi}{8})}{2}$$

which means that $p = 2\sin^2(\frac{\pi}{8})$. You can verify that this choice of p is also good for all the other entries of the table.

Exercise 2. IP Game

Consider the following game. Alice gets a bit string $x \in \{0, 1\}^n$ of length n and Bob gets a bit string $y \in \{0, 1\}^n$ of the same length. Alice and Bob can share as many PR-boxes as they wish and can communicate classically. The goal of the game is to calculate the following function

$$IP^*(x, y) = (\overline{x_1 \cdot y_1}) \oplus (\overline{x_2 \cdot y_2}) \oplus \dots \oplus (\overline{x_n \cdot y_n})$$

where $\overline{x \cdot y}$ is the negation of $x \cdot y$, with as little communication as possible (measured in classical bits). Only one of the parties needs to know the result of the calculation. Give a strategy for this game which allows Alice and Bob to win the game with just one bit of communication.

Remark: The amount of communication needed for such a distributed calculation of a function is called the communication complexity of the function. There is a classical result which shows that the distributed calculation of any binary function can be reduced to a calculation of some inner product function. Together with what you prove here, this implies that the communication complexity of any binary function is at most one bit if Alice and Bob are allowed to share PR-boxes.

Solution. For every $i \in \{1, 2, \dots, n\}$ Alice and Bob will use one PR-box. Using the i 'th box, Alice and Bob will insert the input bits x_i and y_i and get outputs bits a_i and b_i such that $a_i \oplus b_i = \overline{x_i \cdot y_i}$. Now note that

$$\begin{aligned} \text{IP}^*(x, y) &= (\overline{x_1 \cdot y_1}) \oplus (\overline{x_2 \cdot y_2}) \oplus \dots \oplus (\overline{x_n \cdot y_n}) \\ &= (a_1 \oplus b_1) \oplus (a_2 \oplus b_2) \oplus \dots \oplus (a_n \oplus b_n) \\ &= (a_1 \oplus a_2 \oplus \dots \oplus a_n) \oplus (b_1 \oplus b_2 \oplus \dots \oplus b_n) \end{aligned}$$

and therefore Alice can calculate on her side $a' = a_1 \oplus a_2 \oplus \dots \oplus a_n$ and send only this one bit to Bob. With this bit Bob can now calculate the rest on his side by calculating $a' \oplus (b_1 \oplus b_2 \oplus \dots \oplus b_n)$.

Exercise 3. Mermin-GHZ Game

In this game, Alice, Bob and Charlie receive input bits x , y and z , with the promise that $x \oplus y \oplus z = 0$. Their goal is to output bits a , b and c , respectively, such that

$$a \oplus b \oplus c = x \vee y \vee z.$$

- (a) Show that there is no classical winning strategy (i.e., no classical strategy that wins with probability one). What is the maximal probability of winning using a classical strategy assuming that all valid inputs are equally likely?

Solution. The desired functionality is given by the following table:

x	y	z	$x \vee y \vee z \stackrel{!}{=} a \oplus b \oplus c$
0	0	0	0
1	1	0	1
1	0	1	1
0	1	1	1

Clearly we can achieve 75% winning probability by setting $a \equiv b \equiv c \equiv 1$. Now suppose that we could do better. Then there would exist a *deterministic* classical winning strategy, i.e. functions $a(x)$, $b(y)$, $c(z)$ such that $a(x) \oplus b(y) \oplus c(z) = x \vee y \vee z$ for all valid inputs. This leads to a contradiction:

$$1 = \bigoplus_{x \oplus y \oplus z = 0} x \vee y \vee z = \bigoplus_{x \oplus y \oplus z = 0} a(x) \oplus b(y) \oplus c(z) = 0. \quad \zeta$$

The first equality is obtained by summing the last column in the table, while the last equality follows from observing that each of the input bits x , y and z (and hence the corresponding output) attains the same value twice as we vary over all allowed inputs.

- (b) Show that there exists a quantum winning strategy in which Alice, Bob and Charlie share a GHZ state, $|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} (|000\rangle_{ABC} + |111\rangle_{ABC})$.

Solution. We consider the following strategy, which is performed by each of the players: On receiving input 0, the player measures in the σ_x -eigenbasis,

$$|\phi_{0,1}^x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix},$$

and outputs i if the the outcome was $|\phi_i^x\rangle$. On receiving input 1, she measures in the σ_y -eigenbasis,

$$|\phi_{0,1}^y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm i \end{pmatrix},$$

and outputs j if the the outcome was $|\phi_j^y\rangle$.

We now show that this strategy allows the players to win with certainty. To see this, note that at least one of the players will receive a zero input bit. Without loss of generality, we can take this to be Alice, i.e. $x = 0$. The following table displays the post-measurement reduced state on Bob and Charlie's side corresponding to each measurement outcome:

a	post-measurement state of Bob and Charlie
0	$\frac{1}{\sqrt{2}} (00\rangle_{BC} + 11\rangle_{BC}) = \frac{1}{\sqrt{2}} (\phi_0^x \phi_0^x\rangle_{BC} + \phi_1^x \phi_1^x\rangle_{BC}) = \frac{1}{\sqrt{2}} (\phi_0^y \phi_1^y\rangle_{BC} + \phi_1^y \phi_0^y\rangle_{BC})$
1	$\frac{1}{\sqrt{2}} (00\rangle_{BC} - 11\rangle_{BC}) = \frac{1}{\sqrt{2}} (\phi_0^x \phi_1^x\rangle_{BC} + \phi_1^x \phi_0^x\rangle_{BC}) = \frac{1}{\sqrt{2}} (\phi_0^y \phi_0^y\rangle_{BC} + \phi_1^y \phi_1^y\rangle_{BC})$

(This follows from the $U \otimes U^*$ -invariance of the triplet state.)

As is apparent from the table, the post-measurement state for $a = 0$ is correlated for measurements in the σ_x -eigenbasis, but anti-correlated for measurements in the σ_y -eigenbasis. For $a = 1$, the opposite is true.

On the other hand, since $x \oplus y \oplus z = 0$ and $x = 0$ by assumption, we necessarily have that $y = z = 0$ or $y = z = 1$. That is, both Bob and Charlie will always measure in the same basis (in the σ_x -eigenbasis in the first case, the σ_y -eigenbasis in the second case). Therefore, we get the second-to-last column in the following table:

x	y	z	$x \vee y \vee z$	a	$\mathbf{b} \oplus \mathbf{c}$	$a \oplus b \oplus c$
0	0	0	0	0	$\mathbf{0}$	0
0	1	1	1	1	$\mathbf{1}$	0
1	0	1	1	0	$\mathbf{1}$	1
1	1	0	1	1	$\mathbf{0}$	1

The players win the game with 100% success.

- (c) Find a non-signaling winning strategy in which Alice and Bob share a PR-box.

Solution. Alice and Bob simply use the PR-box, which gives them outputs a and b satisfying $a \oplus b = \overline{xy}$. Charlie outputs the negation of his input, $c = \bar{z}$. Then:

x	y	z	$x \vee y \vee z$	$a \oplus b = \overline{xy}$	$c = \bar{z}$	$a \oplus b \oplus c$
0	0	0	0	1	1	0
1	1	0	1	0	1	1
1	0	1	1	1	0	1
0	1	1	1	1	0	1

In fact, there exists a strategy in which Charlie always outputs a constant! This is because $x \oplus y \oplus z = 0$, so that $x \oplus y \oplus 1 = \bar{z} = c$. It follows that if Alice and Bob add their input x, y to the respective output of the PR-box then Charlie may simply always output 1. Indeed:

x	y	z	$x \vee y \vee z$	$a \oplus b = \overline{xy} \oplus x \oplus y$	$c = 1$	$a \oplus b \oplus c$
0	0	0	0	1	1	0
1	1	0	1	0	1	1
1	0	1	1	0	1	1
0	1	1	1	0	1	1

(Here, a and b denotes the output of Alice and Bob, i.e. $a = a' \oplus x$ and $b = b' \oplus y$, where a' and b' are the outputs of the PR-box.)

- (d) Is there a quantum winning strategy in which only Alice and Bob share a quantum state?

Solution. (Sketch) Suppose that there exists such a strategy. We may assume without loss of generality that Charlie performs a deterministic strategy, $c = f(z)$. Then, using $z = x \oplus y$, one finds that the resulting correlations can be used to win the CHSH game with probability one (e.g., for $c = z$ we find that $a \oplus b = xy$). This is of course impossible by Tsirelson's bound.

Exercise 4. Mermin–Peres Magic Square Game

A *magic square* is a three-by-three grid with entries in ± 1 , such that the product of each row is equal to $+1$ while the product of each column is equal to -1 . The *magic square game* now is the following game of two players, Alice and Bob. Alice receives the index x of a row and has to output three numbers in ± 1 which look like the row of a magic square (i.e., their product is equal to $+1$). Bob receives the index y of a column and has to output three numbers in ± 1 which look like the column of a magic square (i.e., their product is equal to -1). Crucially, their output has to agree on the intersection, as in the following example:

	y	1	2	3	
x					
1				1	
2		-1	-1	1	$\prod = 1$
3				-1	
					$\prod = -1$

- (a) Show that there is no classical strategy that wins with probability one. *Hint: Do magic squares exist?*

Solution. Suppose that there exists a (without loss of generality) deterministic classical strategy that is successful with 100% probability. Then we can construct a magic square: Define $m_{x,y}$ as the number in the intersection of the x -th row and the y -column as returned by Alice and Bob, respectively. But such magic squares do not exist, for

$$1 = 1^3 = \prod_x \prod_y m_{x,y} = \prod_y \prod_x m_{x,y} = (-1)^3 = -1. \quad \zeta \tag{S.1}$$

- (b) Find a quantum winning strategy. *Hint: Let Alice and Bob share two entangled pairs of qubits and consider products of Pauli operators.*

Solution. We have seen above that the system of equations

$$\begin{aligned} \prod_y m_{x,y} &= 1 \quad (\forall x) \\ \prod_x m_{x,y} &= -1 \quad (\forall y) \end{aligned} \tag{S.2}$$

has no solution over $\{\pm 1\}$. In fact, the argument above shows that it has no solution as long as the variables $m_{x,y}$ commute with each other (so that we can do the same re-ordering as in (S.1)).

We are therefore lead to search for *non-commutative* solutions of (S.2)! That is, we would like to find operators $M_{x,y}$ that satisfy (S.2). The operators $M_{x,y}$ should be Hermitian, so that we can interpret them as observables. We shall furthermore require that the operators in each row commute with each other, and likewise for the operators in each column (so that they can be jointly measured). Following the hint, we find that the following products of Pauli operators does the job:

	y	1	2	3
x				
1		$\sigma_x \otimes \sigma_x$	$\sigma_x \otimes \mathbf{1}$	$\mathbf{1} \otimes \sigma_x$
2		$\sigma_y \otimes \sigma_y$	$-\sigma_x \otimes \sigma_z$	$-\sigma_z \otimes \sigma_x$
3		$\sigma_z \otimes \sigma_z$	$\mathbf{1} \otimes \sigma_z$	$\sigma_z \otimes \mathbf{1}$

(To see that the operators in the second row commute with each other, use that $\sigma_x \sigma_y = i \sigma_z$ etc.)

Now the idea is that Alice, given a row index x as input, will output the result of measuring all observables $M_{x,y}$ for the row (on her part of the state), while Bob, given a column index y as input, will output the result of measuring all observables $M_{x,y}$ for the column (on his part of the state). Since the operators $M_{x,y}$ satisfy (S.2), the product of Alice's output is $+1$, while the product of Bob's output is -1 .

Thus we only have to satisfy compatibility condition, which requires that Alice and Bob should get the same measurement output on the intersection. This we will do by choosing a suitable state: Following the hint, we consider *two* maximally entangled states shared between Alice and Bob:

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} (|00\rangle_{A_1 B_1} + |11\rangle_{A_1 B_1}) \otimes \frac{1}{\sqrt{2}} (|00\rangle_{A_2 B_2} + |11\rangle_{A_2 B_2}).$$

It is then easy to check by using

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|\phi_0^x \phi_0^x\rangle + |\phi_1^x \phi_1^x\rangle) = \frac{1}{\sqrt{2}} (|\phi_0^y \phi_1^y\rangle + |\phi_1^y \phi_0^y\rangle),$$

where $|0,1\rangle$ are the eigenvectors of σ_z and where $|\phi_j^{x,y}\rangle$ denote the eigenvectors of σ_x and σ_y as in the solution to the last exercise (with eigenvalues ± 1 each), that the compatibility condition is indeed satisfied.