EPR, Bell’s Inequality, and the E91 Protocol

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- C. Bernhardt: Chapter 5
- M. Nielsen and I. Chuang: Section 2.6

Copenhagen Interpretation

- Named after city where Neils Bohr lived
- According to Copenhagen interpretation:
  - Before a measurement is made, a quantum system exists in a superposition of multiple states
    - e.g., particle might be considered to be in multiple locations simultaneously
  - The act of measuring forces the system to "collapse" into a single, definite state
    - Specific state it collapses into is probabilistic, i.e., it is governed by probabilities, not determined with certainty
  - Observer or measuring apparatus plays crucial role in determining outcome of quantum event
    - Observer not merely passively observing, but actively influencing system's state
- Some physicists, e.g., Einstein and Schrodinger did not subscribe to this model, in particular, to:
  - interpretation of states jumping with given probabilities to basis states, and
  - concept of action at a distance in entanglement
- They thought there should be a better model using:
  - hidden variables and local realism (details later)
- John Stewart Bell devised an ingenious test, which could distinguish between above two models
- Later, several experiments based on Bell's result were conducted, which showed that:
  - Einstein and Schrodinger's view was wrong and Copenhagen interpretation is correct

Local Realism

- A concept in physics that combines two ideas:
  - ❑ locality
  - ❑ realism
- Locality:
  - ❑ an object's properties are determined only by its immediate environment
  - ❑ any influence on that object can only travel at or below speed of light
  - ❑ distant objects cannot instantaneously affect each other
- Realism:
  - ❑ objects have definite, pre-existing properties, regardless of whether they are being observed or measured
- Einstein, Boris Podolsky, and Nathan Rosen (EPR) published a paper, which stated that:
  - ❑ special theory of relativity implied that information could not travel faster than speed of light,
  - ❑ but instantaneous action at a distance (as in entangled particles) would mean that information could be sent from Alice to Bob instantaneously
- This problem known as *EPR paradox*

Hidden Variables

- Hidden variables:
  - properties of particles, to which we do not have access, which determine the outcomes of quantum measurements even before the measurements are actually made
- EPR proposed that:
  - quantum mechanics might be incomplete because it does not account for these hidden variables,
  - quantum mechanics only provides probabilistic predictions, while a more complete theory (including hidden variables) could offer deterministic outcomes

Versions of Bell’s Inequality

- There are several versions of Bell’s inequality
- We discuss two versions

Bell’s Inequality: Version 1
Clauser, Horne, Shimony, and Holt (CHSH Inequality)

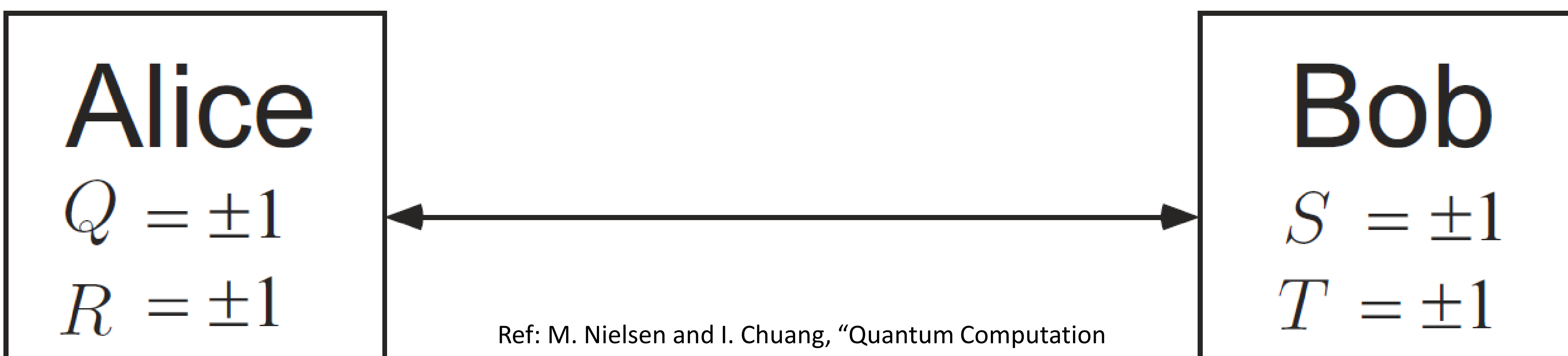
CHSH Inequality

- Imagine we perform following experiment, illustrated in Fig.
- Charlie prepares two particles:
  - sends one particle to Alice, and second particle to Bob
- Once Alice receives her particle, she performs a measurement on it
- She has available two different measurement apparatuses, so she could choose to do one of two different measurements
- These measurements are of physical properties which we shall label:
  - P_Q and P_R, respectively
- Alice doesn't know in advance which measurement she will choose to perform:
  - when she receives particle, she randomly decides which measurement to perform
- For simplicity, assume that the measurements can each have one of two outcomes, $+1$ or -1
- Suppose Alice's particle has a value:
  - Q for the property P_Q
  - R for the property P_R

Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"

CHSH Inequality (contd.)

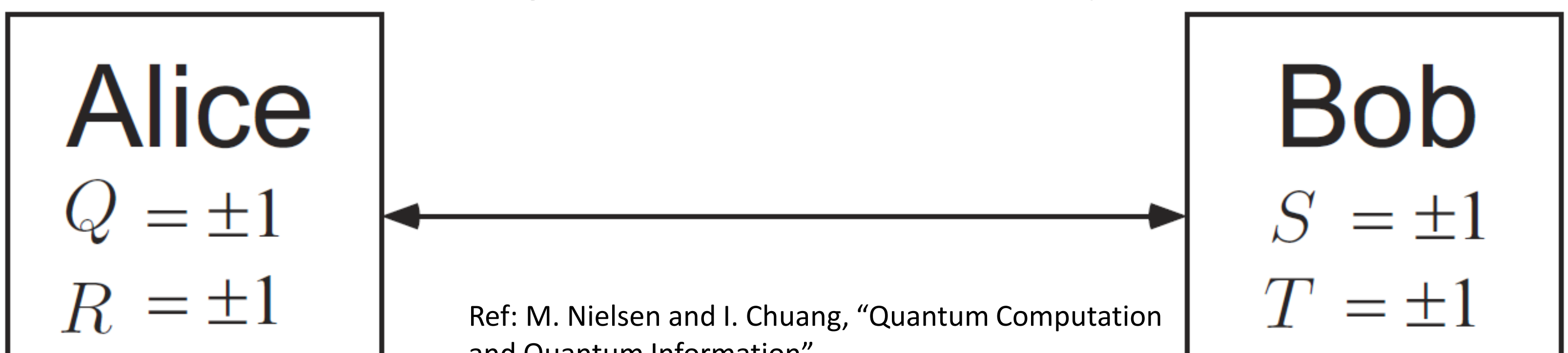
- Similarly, Bob is capable of measuring one of two properties, P_S or P_T, each taking value $+1$ or -1
- Bob waits until he has received the particle and then:
  - ❑randomly decides which measurement to perform
- Timing of experiment arranged so that Alice and Bob do their measurements *at the same time*
- Therefore, according to classical model, measurement which Alice performs cannot disturb result of Bob's measurement (or vice versa):
  - ❑since physical influences cannot propagate faster than light



Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"

CHSH Inequality (contd.)

- Note that:
  1) $QS + RS + RT - QT = (Q + R)S + (R - Q)T$
- Since $R, Q \in \{-1, +1\}$, it follows that:
  - ❑ $(Q + R)S = 0$ or $(R - Q)T = 0$
- In either case, from 1), we get that:
  2) $QS + RS + RT - QT = \pm 2$
- Let $p(q, r, s, t)$ be probability that, before the measurements are performed, system is in state where $Q = q, R = r, S = s, T = t$
  - ❑ these probabilities may depend on how Charlie performs his preparation, and on experimental noise
- By 2), we get:
  3) $E(QS) + E(RS) + E(RT) - E(QT) = \sum_{q,r,s,t} p(q, r, s, t)\,(qs + rs + rt - qt) \leq 2$
- Inequality in 3) known as CHSH inequality
- Note that we derived 3) using classical model (assumption of realism)



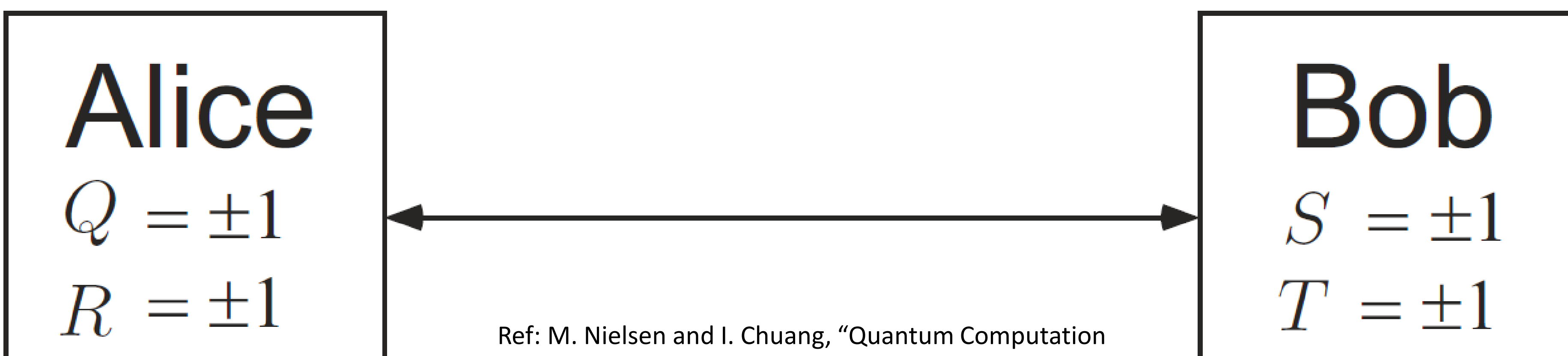
Ref: M. Nielsen and I. Chuang, “Quantum Computation and Quantum Information”

CHSH Inequality (contd.)

- Recall: CHSH inequality:

  3) $E(QS) + E(RS) + E(RT) - E(QT) \leq 2$

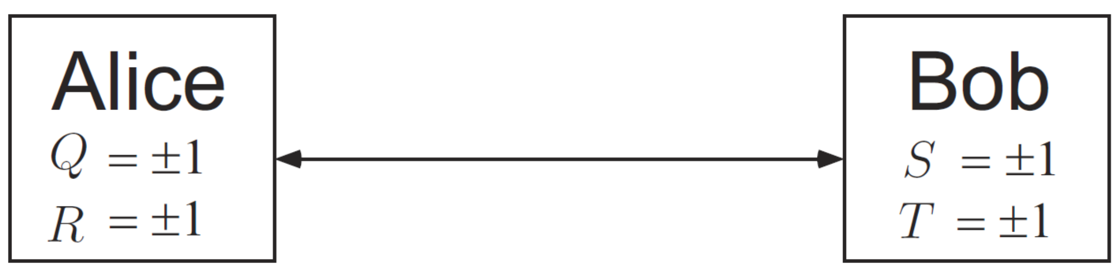
- By repeating experiment many times, Alice and Bob can determine each quantity on LHS of 3)
- Thus, they can check to see whether it is obeyed in a real experiment
- Next, we calculate LHS of 3) using quantum mechanical model



Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"

CHSH Inequality (contd.)

- Recall: CHSH inequality:
  3) $E(QS) + E(RS) + E(RT) - E(QT) \leq 2$
- Suppose Charlie prepares a quantum system of two qubits in state:
  - $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$
- He passes:
  - first qubit to Alice, and
  - second qubit to Bob
- They perform measurements of following observables:
  - $Q = Z_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}$
  - $R = X_1, T = \frac{Z_2 - X_2}{\sqrt{2}}$
  - (**Note**: subscript 1 (respectively, 2) denotes qubit of Alice (respectively, Bob))
- **Exercise**: Show that eigenvalues of each of the above observables Q, R, S, and T are ± 1
  - recall: eigenvalues of observables are measurement outcomes; hence, the possible outcomes are ± 1 for each observable
- **Exercise:** Show that average values of above observables are:
  - $\langle QS \rangle = \frac{1}{\sqrt{2}}; \langle RS \rangle = \frac{1}{\sqrt{2}}; \langle RT \rangle = \frac{1}{\sqrt{2}}; \langle QT \rangle = -\frac{1}{\sqrt{2}}$
  - (use the fact that $\langle M \rangle \equiv \langle \psi | M | \psi \rangle$)
- Thus:
  4) $\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}$
- Note that 3) and 4), which were obtained using classical and quantum mechanical model, respectively, contradict each other

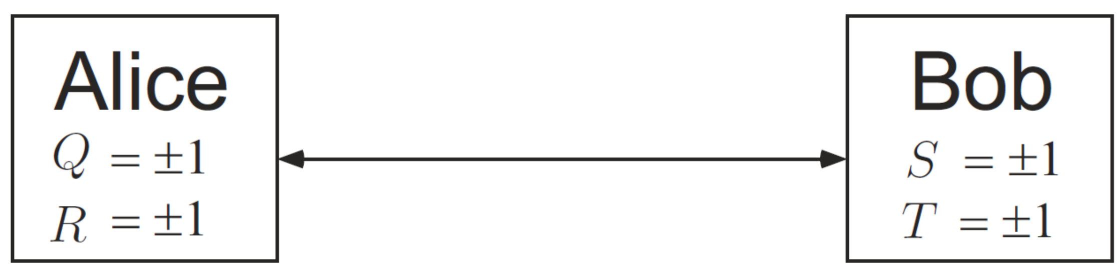


Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"

CHSH Inequality (contd.)

- Recall:
  - ❑ $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$
  - ❑ $Q = Z_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}$
  - ❑ $R = X_1, T = \frac{Z_2 - X_2}{\sqrt{2}}$
- We now outline the proof of $\langle QS \rangle = \frac{1}{\sqrt{2}}$, which is part of above exercise
- $Q|0\rangle = Z|0\rangle = |0\rangle$ and $Q|1\rangle = Z|1\rangle = -|1\rangle$
- It can be shown that: $S|0\rangle = \frac{-|0\rangle - |1\rangle}{\sqrt{2}}$ and $S|1\rangle = \frac{-|0\rangle + |1\rangle}{\sqrt{2}}$
- Hence: $QS|\psi\rangle = QS\left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right) = \frac{Q|0\rangle \otimes S|1\rangle - Q|1\rangle \otimes S|0\rangle}{\sqrt{2}}$, which simplifies to: $QS|\psi\rangle = \frac{-1}{2}[|00\rangle - |01\rangle + |10\rangle + |11\rangle]$
- So $\langle QS \rangle = \langle \psi | QS | \psi \rangle = -\left(\frac{\langle 01| - \langle 10|}{2\sqrt{2}}\right)[|00\rangle - |01\rangle + |10\rangle + |11\rangle] = \frac{1}{\sqrt{2}}$

Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"



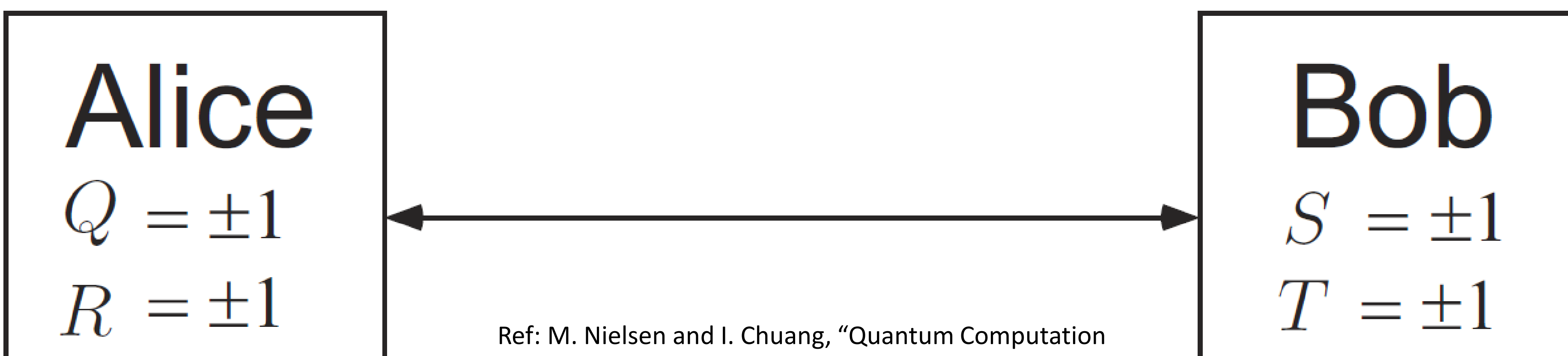
CHSH Inequality (contd.)

- Recall:
  - ❑ $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$
  - ❑ $Q = Z_1, S = \frac{-Z_2 - X_2}{\sqrt{2}}$
  - ❑ $R = X_1, T = \frac{Z_2 - X_2}{\sqrt{2}}$
- Note that we need to calculate $E(QS)$, which is the average value of the product of two scalars
- But we equated it to $\langle QS \rangle = \langle \psi | QS | \psi \rangle = \langle \psi | Q \otimes S | \psi \rangle$
- Why does the tensor product $Q \otimes S$ correspond to the measurement outcome qs, which is a product of two scalars?
- Recall the spectral decompositions:
  - ❑ $Q = \sum_q qP_q$ and
  - ❑ $S = \sum_s sP_s$
  - ❑ where P_q is projector onto eigenspace of Q with eigenvalue q
- So:
  - ❑ $Q \otimes S = \left(\sum_q qP_q\right) \otimes \left(\sum_s sP_s\right) = \sum_{q,s} (qs)\left(P_q \otimes P_s\right)$
- Hence, $Q \otimes S$ is an observable with corresponding measurement outcomes qs

Ref: M. Nielsen and I. Chuang, “Quantum Computation and Quantum Information”

CHSH Inequality (contd.)

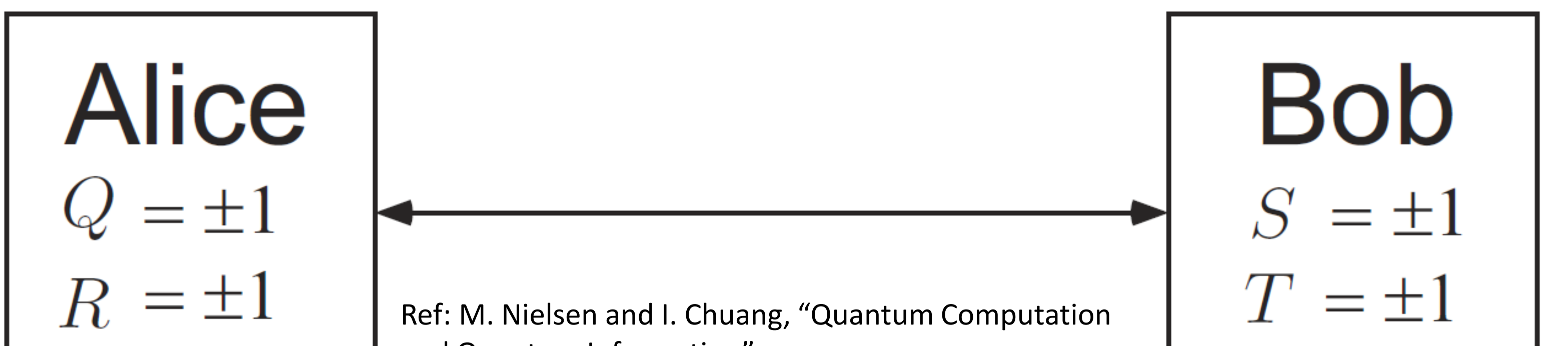
- Recall:
  3) $E(QS) + E(RS) + E(RT) - E(QT) \leq 2$
     - obtained using classical model
  4) $\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}$
     - obtained using quantum mechanical model
- Several experiments have been conducted to check as to which one of 3) and 4) is true
- Results were strongly in favor of quantum mechanical prediction 4)
- So the CHSH inequality 3) is *not* obeyed by Nature
- It means that assumptions that went into the derivation of the CHSH inequality must be incorrect



Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"

CHSH Inequality (contd.)

- Recall:
  - *3)* $E(QS) + E(RS) + E(RT) - E(QT) \leq 2$
    - obtained using classical model
  - 4) $\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}$
    - obtained using quantum mechanical model
- There are two assumptions made in various proofs of 3) which are questionable: realism and locality
- *Realism:*
  - assumption that the physical properties P_Q, P_R, P_S, and P_T have definite values, Q, R, S, and T, which exist independent of observation
  - We used this in above derivation to write $E(QS) + E(RS) + E(RT) - E(QT) = \sum_{q,r,s,t} p(q,r,s,t)\,(qs + rs + rt - qt)$, where $p(q,r,s,t)$ is probability that before the measurements are performed, system is in state where $Q = q, R = r, S = s, T = t$
  - **Note**: If we try to define $p(q,r,s,t)$ to be probability that *after* measurements are performed, the outcomes will be $Q = q, R = r, S = s, T = t$, then such a joint distribution does not exist in general since either P_Q or P_R (respectively, P_S or P_T) is measured, but not both
- *Locality*:
  - assumption that Alice performing her measurement does not influence the result of Bob's measurement
  - If this assumption holds, then we can write:
    - $E(QS) = E(Q)E(S)$, $E(RS) = E(R)E(S)$, $E(RT) = E(R)E(T)$, and $E(QT) = E(Q)E(T)$
    - So $E(QS) + E(RS) + E(RT) - E(QT) = E(S)\big(E(Q) + E(R)\big) + E(T)\big(E(R) - E(Q)\big) \leq |E(Q) + E(R)| + |E(Q) - E(R)| \leq 2\max(|E(Q)|, |E(R)|) \leq 2$
- These two assumptions together constitute assumption of local realism*:*
  - must be dropped



Ref: M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information"

Bell’s Inequality: Version 2

Entangled Qubits in Different Bases

- Consider two entangled qubits in state:
  - ❑ $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix}$
- Now, consider a new orthonormal basis $(|b_0\rangle, |b_1\rangle)$:
  - ❑ where the components of $|b_0\rangle$ and $|b_1\rangle$ are *real numbers*
- **Claim**:
  - ❑ $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}|b_0\rangle \otimes |b_0\rangle + \frac{1}{\sqrt{2}}|b_1\rangle \otimes |b_1\rangle$
- **Proof:**
  - ❑ Let $|b_0\rangle = \begin{bmatrix}a\\b\end{bmatrix}$ and $|b_1\rangle = \begin{bmatrix}c\\d\end{bmatrix}$, where $a, b, c, d \in \boldsymbol{R}$
  - ❑ Then $\begin{bmatrix}1\\0\end{bmatrix} = a\begin{bmatrix}a\\b\end{bmatrix} + c\begin{bmatrix}c\\d\end{bmatrix}$

  1) So $\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \left(a\begin{bmatrix}a\\b\end{bmatrix} + c\begin{bmatrix}c\\d\end{bmatrix}\right) \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix} \otimes \begin{bmatrix}a\\0\end{bmatrix} + \begin{bmatrix}c\\d\end{bmatrix} \otimes \begin{bmatrix}c\\0\end{bmatrix}$
  2) Similarly, $\begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix} \otimes \begin{bmatrix}0\\b\end{bmatrix} + \begin{bmatrix}c\\d\end{bmatrix} \otimes \begin{bmatrix}0\\d\end{bmatrix}$

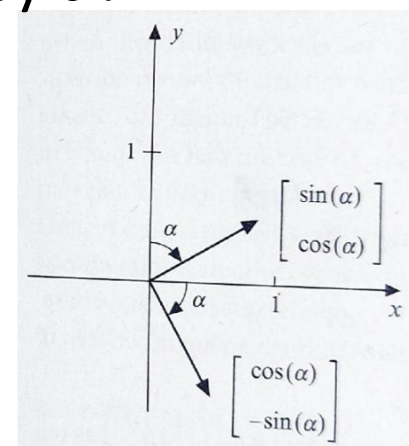
  - ❑ Adding 1) and 2), we get: $\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix} \otimes \begin{bmatrix}a\\b\end{bmatrix} + \begin{bmatrix}c\\d\end{bmatrix} \otimes \begin{bmatrix}c\\d\end{bmatrix} = |b_0\rangle \otimes |b_0\rangle + |b_1\rangle \otimes |b_1\rangle$

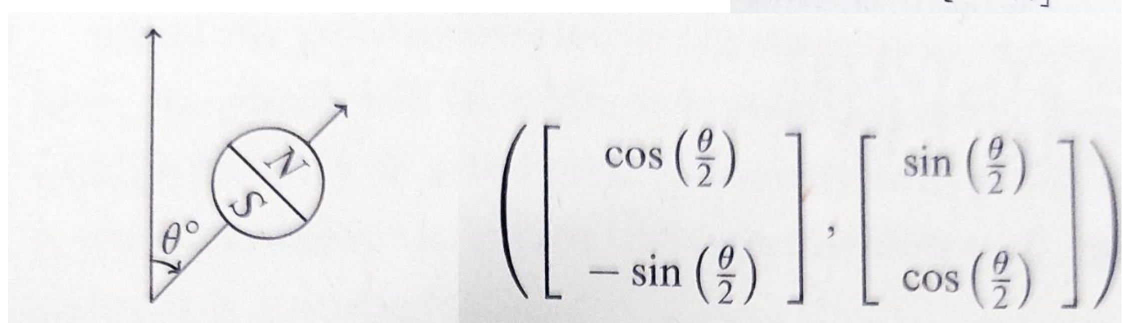
Bases Used for Bell's Inequality

- For proving Bell's inequality, we use three different bases
- These correspond to rotating our measuring device through 0°, 120°, and 240°
- Above three bases denoted by:
  - ❑ $(|\uparrow\rangle, |\downarrow\rangle)$, $(|\searrow\rangle, |\nwarrow\rangle)$, and $(|\swarrow\rangle, |\nearrow\rangle)$, respectively
- Assume that qubits are encoded in spin of particles
- Recall: basis associated with rotating our apparatus by θ:

$$\left(\begin{bmatrix} \cos(\theta/2) \\ -\sin(\theta/2) \end{bmatrix}, \begin{bmatrix} \sin(\theta/2) \\ \cos(\theta/2) \end{bmatrix}\right)$$

- Hence:
  - ❑ $|\searrow\rangle = \begin{bmatrix} \frac{1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix}, |\nwarrow\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$
  - ❑ $|\swarrow\rangle = \begin{bmatrix} \frac{-1}{2} \\ \frac{-\sqrt{3}}{2} \end{bmatrix}, |\nearrow\rangle = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{-1}{2} \end{bmatrix}$





(a) Measurement angle (b) Basis

Ref: "Quantum Computing for Everyone" by C. Bernhardt

Classical Explanation of Entanglement

- Consider two entangled qubits:
  - one with Alice and other with Bob
  - state of the qubits is $\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$
- Recall:
  - when Alice and Bob perform a measurement of their qubits in basis $(|\uparrow\rangle, |\downarrow\rangle)$, both get same answer (either 0 or 1)
- Recall: for proving Bell's inequality:
  - we rotate our measuring device through 0°, 120°, and 240°
  - we measure spin of particles in the bases $(|\uparrow\rangle, |\downarrow\rangle)$, $(|\searrow\rangle, |\nwarrow\rangle)$, and $(|\swarrow\rangle, |\nearrow\rangle)$
- Classical theory states:
  - there is a definite outcome of the measurement in each basis that is already determined before we perform the measurement (realism)
- Quantum theory states:
  - outcome of measurement not determined until the time we perform the measurement

Bell's Inequality

- We generate a stream of n pairs of qubits:
  - from each pair, one sent to Alice and other to Bob
- Each pair of qubits is in state:
  - $\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$
- Alice:
  - measures each qubit in direction 0°, 120°, or 240°
    - for each qubit, direction of measurement selected uniformly at random, independently of other qubits
  - does not keep track of direction she chose for a qubit
  - records the outcome (0 or 1) of each measurement
- Subsequently, Bob does the same for his qubits:
  - his directions of measurements selected independently of Alice
- In this way, Alice and Bob generate strings of length n each of 0s and 1s
- What is the fraction of bits of these strings in which Alice and Bob are in agreement?
- Bell realized that quantum mechanics model and classical model gave different numbers for the answer

Answer of Quantum Mechanics

- Consider a pair of qubits, which is in state:
  - ❑ $\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$
- Recall: if Alice and Bob select same direction of measurement (i.e., same basis), their outcomes are same
- Consider case where they select different directions of measurement
- E.g.: suppose:
  - ❑ Alice chooses $(|\searrow\rangle, |\nwarrow\rangle)$
  - ❑ Bob chooses $(|\swarrow\rangle, |\nearrow\rangle)$
- Entangled state can be written as:
  - ❑ $\frac{1}{\sqrt{2}}|\searrow\rangle|\searrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle\,|\nwarrow\rangle$
- When Alice performs measurement:
  - ❑ she gets 0 and state jumps to $|\searrow\rangle|\searrow\rangle$ w.p. $\frac{1}{2}$
  - ❑ she gets 1 and state jumps to $|\nwarrow\rangle\,|\nwarrow\rangle$ w.p. $\frac{1}{2}$
- Suppose Alice gets 0 and state jumps to $|\searrow\rangle|\searrow\rangle$
- Now:
  - ❑ $|\searrow\rangle = \frac{1}{2}|\swarrow\rangle + \frac{\sqrt{3}}{2}|\nearrow\rangle$
- So when Bob performs measurement:
  - ❑ gets 0 w.p. $\frac{1}{4}$ and 1 w.p. $\frac{3}{4}$
- Thus, when Alice gets 0, states of Alice and Bob agree w.p. $\frac{1}{4}$
- **Exercise**: Show that even when Alice gets 1, states of Alice and Bob agree w.p. $\frac{1}{4}$
- In summary:
  - ❑ when Alice chooses $(|\searrow\rangle, |\nwarrow\rangle)$ and Bob chooses $(|\swarrow\rangle, |\nearrow\rangle)$, their bits agree w.p. $\frac{1}{4}$ and disagree w.p. $\frac{3}{4}$
- **Exercise**: Show that in all other cases in which Alice and Bob choose different bases, their bits agree w.p. $\frac{1}{4}$ and disagree w.p. $\frac{3}{4}$
- In summary, for a given pair of qubits:
  - ❑ w.p. $\frac{1}{3}$, Alice and Bob choose same basis and their bits agree w.p. 1
  - ❑ w.p. $\frac{2}{3}$, Alice and Bob choose different bases and their bits agree w.p. $\frac{1}{4}$
- According to quantum mechanics model, what is the fraction of bits of the strings of Alice and Bob for which the bits are in agreement?
  - ❑ $\frac{1}{2}$

Classical Answer

- Classical view:
  - Measurements in all directions determined right from the start
- There are eight possible configurations:
  - $000, 001, 010, 011, 100, 101, 110, 111$
  - where the three bits in each configuration give the answer (0 or 1) if we measure a qubit in bases $(|\uparrow\rangle, |\downarrow\rangle)$, $(|\searrow\rangle, |\nwarrow\rangle)$, and $(|\swarrow\rangle, |\nearrow\rangle)$, respectively
- Due to the entanglement between qubits of Alice and Bob:
  - for each pair of qubits, configurations of Alice and Bob are identical
- Table shows all possible outcomes of measurement, where:
  - a, b, and c denote $(|\uparrow\rangle, |\downarrow\rangle)$, $(|\searrow\rangle, |\nwarrow\rangle)$, and $(|\swarrow\rangle, |\nearrow\rangle)$, respectively
  - (x, y), where $x, y \in \{a, b, c\}$, denotes that Alice (respectively, Bob) measures qubit in basis x (respectively, y)
  - Entries in table show whether measurements agree (A) or disagree (D)
- Probabilities that should be assigned to different configurations unknown
- Since Alice and Bob choose each of their three bases with equal probabilities, each of the nine pairs of bases occurs w.p. $\frac{1}{9}$
- Note that each row contains at least five As
- Hence, overall probability that measurements of Alice and Bob result in same outcome is at least $\frac{5}{9}$
- According to classical model, what is the fraction of bits of the strings of Alice and Bob for which the bits are in agreement?
  - at least $\frac{5}{9}$

	Measurement directions								
Config.	(a,a)	(a,b)	(a,c)	(b,a)	(b,b)	(b,c)	(c,a)	(c,b)	(c,c)
000	A	A	A	A	A	A	A	A	A
001	A	A	D	A	A	D	D	D	A
010	A	D	A	D	A	D	A	D	A
011	A	D	D	D	A	A	D	A	A
100	A	D	D	D	A	A	D	A	A
101	A	D	A	D	A	D	A	D	A
110	A	A	D	A	A	D	D	D	A
111	A	A	A	A	A	A	A	A	A

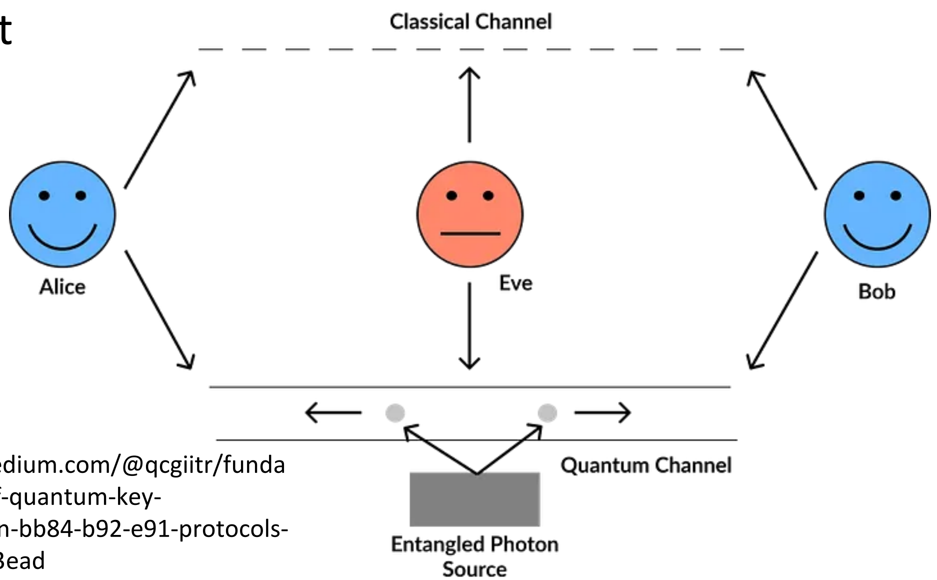
Ref: "Quantum Computing for Everyone" by C. Bernhardt

Summary of Bell's Result

- Recall above question:
  - What is the fraction of bits of the strings in which Alice and Bob are in agreement?
- Answer of quantum mechanics: $\frac{1}{2}$
- Classical answer: at least $\frac{5}{9}$
- Thus, Bell's test gives us a way to distinguish between the two theories
- Above experiment has been performed by several researchers
- Outcomes have always been in agreement with quantum mechanics

E91 QKD Protocol

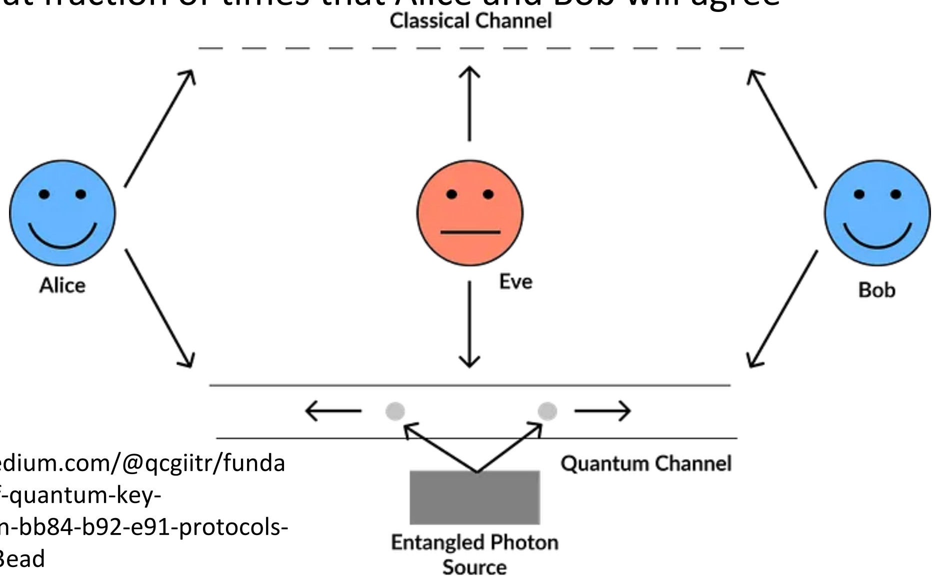
- In 1991, Artur Ekert proposed QKD protocol based on entangled qubits used in Bell's test
- We generate a stream of $3n$ pairs of qubits:
  - ❑ from each pair, one sent to Alice and other to Bob
- Each pair of qubits is in state:
  - ❑ $\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$
- Alice and Bob measure each qubit using a random choice of three bases:
  - ❑ as in Bell test
- As in BB84 protocol, for each measurement:
  - ❑ Alice and Bob record both outcome and basis that they chose
- After Alice and Bob have made $3n$ measurements:
  - ❑ They compare the sequences of bases that they chose
  - ❑ This can be done on insecure channel:
    - ○ Note that they only reveal bases, but not measurement outcomes
  - ❑ They will agree on approximately n of the sequence of bases



Ref: https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead

E91 QKD Protocol (contd.)

- For the n pairs of qubits for which Alice and Bob selected same basis:
  - Alice and Bob get same measurement outcome (0 or 1)
- This string of n bits will be their key if an eavesdropper Eve is not listening in
- Now Alice and Bob test to find if Eve is present
- If Eve is eavesdropping, she will have to measure the qubits:
  - When she measures them, the entangled states of Alice and Bob become unentangled
- Alice and Bob look at their bits strings of length $2n$ each that correspond to times when they chose different bases
- From above Bell inequality calculation, they know that if their states are entangled, in each place, they should agree w.p. $\frac{1}{4}$
- However, if Eve is measuring one of the qubits, the fraction of bits for which they agree changes
- E.g., if Eve measures a qubit before Alice and Bob have made their measurements:
  - by checking all the possibilities, it can be shown that fraction of times that Alice and Bob will agree increases to $\frac{3}{8}$
- Hence, Alice and Bob can use following test to check for presence of Eve:
  - They calculate fraction of the $2n$ qubits for which their measurement outcomes agree
  - If it is close to $\frac{1}{4}$, they can conclude that nobody has interfered and use the key



Ref: https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead