An Introduction to Quantum Computing

Lecture 12: On Measurements and Quantum Key Distribution

Paolo Zuliani

Dipartimento di Informatica
Università di Roma "La Sapienza", Rome, Italy

Agenda

- Principle of Deferred Measurement
- Measurements in Non-Diagonal Bases
- Bell's Inequalities
- The E91 Quantum Key Distribution Protocol

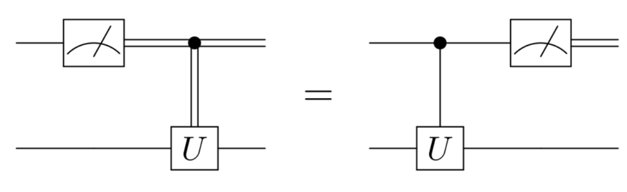
Principle of Deferred Measurement

In a quantum circuit, measurements that control operations can always be moved to the end of the circuit. Any operation conditional on measurements can be replaced by a quantum-conditional operation.

Principle of Deferred Measurement

In a quantum circuit, measurements that control operations can always be moved to the end of the circuit. Any operation conditional on measurements can be replaced by a quantum-conditional operation.

Pictorially:



https://commons.wikimedia.org/wiki/File:Qcircuit_measurement-commute.svg

Principle of Deferred Measurement

In our "programming notation" (assuming two qubits q_0, q_1):

$$\begin{array}{l} b = \text{Measure}(q_0); \\ \text{if } b \text{ then } q_1 = U(q_1) \text{ else skip} \end{array} \quad \equiv \quad \begin{array}{l} \text{ControlledU}(q_0, q_1); \\ b = \text{Measure}(q_0) \end{array}$$

Let's why this is true. We start from the LHS:

Principle of Deferred Measurement

The initial state of our program/circuit is an arbitrary state of two qubits q_0, q_1:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 + |10\rangle + \alpha_3 |11\rangle$$

Principle of Deferred Measurement

The initial state of our program/circuit is an arbitrary state of two qubits q_0, q_1:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 + |10\rangle + \alpha_3 |11\rangle$$

$$\boxed{\text{Execute:} \quad b = \text{Measure}(q_0)}$$

Principle of Deferred Measurement

The initial state of our program/circuit is an arbitrary state of two qubits q_0, q_1:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 + |10\rangle + \alpha_3 |11\rangle$$

$$\boxed{\text{Execute:} \quad b = \text{Measure}(q_0)}$$

$$\begin{cases} b = 0 & |0\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_0|^2 + |\alpha_1|^2 \\ b = 1 & |1\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_1|^2 + |\alpha_3|^2 \end{cases}$$

Principle of Deferred Measurement

The initial state of our program/circuit is an arbitrary state of two qubits q_0, q_1:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 + |10\rangle + \alpha_3 |11\rangle$$

$\boxed{\text{Execute:} \quad b = \text{Measure}(q_0)}$

$$\begin{cases} b = 0 & |0\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_0|^2 + |\alpha_1|^2 \\ b = 1 & |1\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_1|^2 + |\alpha_3|^2 \end{cases}$$

$\boxed{\text{Execute:} \quad \text{if } b \text{ then } q_1 = U(q_1) \text{ else skip}}$

Principle of Deferred Measurement

The initial state of our program/circuit is an arbitrary state of two qubits q_0, q_1:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 + |10\rangle + \alpha_3 |11\rangle$$

$$\boxed{\text{Execute:} \quad b = \text{Measure}(q_0)}$$

$$\begin{cases} b = 0 & |0\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_0|^2 + |\alpha_1|^2 \\ b = 1 & |1\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_1|^2 + |\alpha_3|^2 \end{cases}$$

$$\boxed{\text{Execute:} \quad \text{if } b \text{ then } q_1 = U(q_1) \text{ else skip}}$$

$$\begin{cases} b = 0 & |0\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_0|^2 + |\alpha_1|^2 \\ b = 1 & |1\rangle (U|0\rangle + U|1\rangle) \qquad \text{with probability } |\alpha_1|^2 + |\alpha_3|^2 \end{cases}$$

Principle of Deferred Measurement

The initial state of our program/circuit is an arbitrary state of two qubits q_0, q_1:

$$\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 + |10\rangle + \alpha_3 |11\rangle$$

$$\boxed{\text{Execute:} \quad b = \text{Measure}(q_0)}$$

$$\begin{cases} b = 0 & |0\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_0|^2 + |\alpha_1|^2 \\ b = 1 & |1\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_1|^2 + |\alpha_3|^2 \end{cases}$$

$$\boxed{\text{Execute:} \quad \text{if } b \text{ then } q_1 = U(q_1) \text{ else skip}}$$

$$\begin{cases} b = 0 & |0\rangle (|0\rangle + |1\rangle) \qquad \text{with probability } |\alpha_0|^2 + |\alpha_1|^2 \\ b = 1 & |1\rangle (U|0\rangle + U|1\rangle) \qquad \text{with probability } |\alpha_1|^2 + |\alpha_3|^2 \end{cases}$$

Compute the RHS as an exercise!

Measurements in Non-Diagonal Bases

So far we have seen *diagonal* measurements (the $|0\rangle, |1\rangle$ basis) and the *non-diagonal* measurements in the $|+\rangle, |-\rangle$ basis in the BB84 protocol.

Measurements in Non-Diagonal Bases

So far we have seen *diagonal* measurements (the $|0\rangle, |1\rangle$ basis) and the *non-diagonal* measurements in the $|+\rangle, |-\rangle$ basis in the BB84 protocol.

However, any self-adjoint operator is a valid quantum-mechanical observable. How to?

Measurements in Non-Diagonal Bases

So far we have seen *diagonal* measurements (the $|0\rangle, |1\rangle$ basis) and the *non-diagonal* measurements in the $|+\rangle, |-\rangle$ basis in the BB84 protocol.

However, any self-adjoint operator is a valid quantum-mechanical observable. How to?

Theorem (Spectral Theorem)

The set of all eigenvectors of a self-adjoint operator acting on a Hilbert space $\mathcal{H}$ is an orthonormal basis for $\mathcal{H}$.

Measurements in Non-Diagonal Bases

So far we have seen *diagonal* measurements (the $|0\rangle, |1\rangle$ basis) and the *non-diagonal* measurements in the $|+\rangle, |-\rangle$ basis in the BB84 protocol.

However, any self-adjoint operator is a valid quantum-mechanical observable. How to?

Theorem (Spectral Theorem)

The set of all eigenvectors of a self-adjoint operator acting on a Hilbert space $\mathcal{H}$ is an orthonormal basis for $\mathcal{H}$.

Therefore:

1. *unitarily* change from a non-diagonal basis to the diagonal basis;
2. measure diagonally.

Measurements in Non-Diagonal Bases

Let $\{e_i\}$ and $\{f_i\}$ be two orthonormal bases.

To change basis from, say $\{f_i\}$ to $\{e_i\}$ we need an operator that satisfies:

$$|f_i\rangle \to |e_i\rangle \quad \text{for all } i$$

Measurements in Non-Diagonal Bases

Let $\{e_i\}$ and $\{f_i\}$ be two orthonormal bases.

To change basis from, say $\{f_i\}$ to $\{e_i\}$ we need an operator that satisfies:

$$|f_i\rangle \rightarrow |e_i\rangle \quad \text{for all } i$$

This can be obtained by the unitary operator (exercise):

$$\sum_i |e_i\rangle \langle f_i|$$

Measurements in Non-Diagonal Bases

Example. Measure a qubit in the basis $\{|+\rangle, |-\rangle\}$:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad\qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Measurements in Non-Diagonal Bases

Example. Measure a qubit in the basis $\{|+\rangle, |-\rangle\}$:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad\qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

We map $|+\rangle$ to $|0\rangle$ and $|-\rangle$ to $|1\rangle$ using the operator U:

$$U = |0\rangle\langle+| \; + \; |1\rangle\langle-|$$

Measurements in Non-Diagonal Bases

Example. Measure a qubit in the basis $\{|+\rangle, |-\rangle\}$:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

We map $|+\rangle$ to $|0\rangle$ and $|-\rangle$ to $|1\rangle$ using the operator U:

$$U = |0\rangle\langle +| \ + \ |1\rangle\langle -|$$

U is unitary since $U^\dagger = (|0\rangle\langle +| \ + \ |1\rangle\langle -|)^\dagger = |+\rangle\langle 0| + |-\rangle\langle 1|$ and thus

$$\begin{aligned} UU^\dagger =& (|0\rangle\langle +| \ + \ |1\rangle\langle -|)(|+\rangle\langle 0| + |-\rangle\langle 1|) \\ =& |0\rangle\langle +|\,|+\rangle\langle 0| + |0\rangle\langle +|\,|-\rangle\langle 1| + |1\rangle\langle -|\,|+\rangle\langle 0| + |1\rangle\langle -|\,|-\rangle\langle 1| \\ =& |0\rangle\langle 0| + |1\rangle\langle 1| = I \end{aligned}$$

Similary for $U^\dagger U$.

Measurements in Non-Diagonal Bases

Recall that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, and that $H = H^\dagger$.

Measurements in Non-Diagonal Bases

Recall that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, and that $H = H^\dagger$.

Hence, we have that $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, and thus $U = H$. In fact, let us write the matrix representation of U:

$$\begin{aligned} U &= |0\rangle\langle +| \;+\; |1\rangle\langle -| \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}^T + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix}^T \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0\\1 & -1\end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = H \end{aligned}$$

Bell's Inequalities

Also known as Bell's Theorem, after physicist John Bell (1928-1990).
Result first presented in "On the Einstein Podolsky Rosen Paradox", 1964.

Bell's Inequalities

Also known as Bell's Theorem, after physicist John Bell (1928-1990).
Result first presented in "On the Einstein Podolsky Rosen Paradox", 1964.

The EPR thought experiment:

$$\text{Alice} \xleftarrow{\textit{one particle}} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xrightarrow{\textit{one particle}} \text{Bob}$$

EPR's "paradox": Alice's and Bob's measurement results (in the *diagonal* basis) are always <u>anticorrelated</u>!

Bell's Inequalities

Also known as Bell's Theorem, after physicist John Bell (1928-1990).
Result first presented in "On the Einstein Podolsky Rosen Paradox", 1964.

The EPR thought experiment:

$$\text{Alice} \xleftarrow{\textit{one particle}} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xrightarrow{\textit{one particle}} \text{Bob}$$

EPR's "paradox": Alice's and Bob's measurement results (in the *diagonal* basis) are always anticorrelated!

Suppose now that Alice measures one of two different observables (say Q and R), and Bob one of another pair of observables (say S and T, not necessarily the same as Alice's). What happens?

Bell's Inequalities

Suppose the four observables (Alice's + Bob's) always return ± 1, *i.e.*, the eigenvalues of the four self-adjoint operators are ± 1.

Bell's Inequalities

Suppose the four observables (Alice's + Bob's) always return ± 1, *i.e.*, the eigenvalues of the four self-adjoint operators are ± 1.

Assumptions:

1. neither Alice nor Bob decide which observables they will measure before they receive their particle;
2. both Alice and Bob measure their particle at the same time (to avoid causal interference between their measurements)

Bell's Inequalities

Suppose the four observables (Alice's + Bob's) always return ± 1, *i.e.*, the eigenvalues of the four self-adjoint operators are ± 1.

Assumptions:

1. neither Alice nor Bob decide which observables they will measure before they receive their particle;
2. both Alice and Bob measure their particle at the same time (to avoid causal interference between their measurements)

Hence, we can say that Alice's particle has two "properties" that describe the result of measuring either of the two possible measurements, say, $Q = \pm 1$ and $R = \pm 1$. Similarly for Bob's particle with, say, $S = \pm 1$ and $T = \pm 1$.

Bell's Inequalities

Graphically:

Alice's particle values:		Bob's particle values:
$Q = \pm 1$ $R = \pm 1$	$\xleftarrow{\textit{one particle}}\xrightarrow{\textit{one particle}}$	$S = \pm 1$ $T = \pm 1$

Bell's Inequalities

Graphically:

Alice's particle values:		Bob's particle values:
$Q = \pm 1$ $R = \pm 1$	$\xleftarrow{\textit{one particle}}\quad\xrightarrow{\textit{one particle}}$	$S = \pm 1$ $T = \pm 1$

Let us consider the quantity: $QS + RS + RT - QT$. It is easy to see that:

$$QS + RS + RT - QT \leqslant 2.$$

Bell's Inequalities

Now suppose we perform repeated experiments in which EPR particles are sent to Alice and Bob, who will randomly and independently decide which observable to measure, while respecting the two previous assumptions.

Bell's Inequalities

Now suppose we perform repeated experiments in which EPR particles are sent to Alice and Bob, who will randomly and independently decide which observable to measure, while respecting the two previous assumptions.

We compute the *expected value* $\mathcal{A}$ (or average) of $QS + RS + RT - QT$:

$$\mathcal{A} = E[QS + RS + RT - QT] \leqslant 2$$

Bell's Inequalities

Now suppose we perform repeated experiments in which EPR particles are sent to Alice and Bob, who will randomly and independently decide which observable to measure, while respecting the two previous assumptions.

We compute the *expected value* $\mathcal{A}$ (or average) of $QS + RS + RT - QT$:

$$\mathcal{A} = E[QS + RS + RT - QT] \leqslant 2$$

and since $E[\cdot]$ is a linear operator:

$$\boxed{\mathcal{A} = E[QS] + E[RS] + E[RT] - E[QT] \leqslant 2 \qquad \textbf{(Bell's inequality)}}$$

Bell's Inequalities

Now suppose we perform repeated experiments in which EPR particles are sent to Alice and Bob, who will randomly and independently decide which observable to measure, while respecting the two previous assumptions.

We compute the *expected value* $\mathcal{A}$ (or average) of $QS + RS + RT - QT$:

$$\mathcal{A} = E[QS + RS + RT - QT] \leqslant 2$$

and since $E[\cdot]$ is a linear operator:

$$\boxed{\mathcal{A} = E[QS] + E[RS] + E[RT] - E[QT] \leqslant 2 \qquad \textbf{(Bell's inequality)}}$$

Let us test this inequality in quantum mechanics!

Bell's Inequalities

Try this "experimental setting":

Alice measures one of $\begin{cases} Q = Z \\ R = X \end{cases}$ Bob measures one of $\begin{cases} S = \frac{-Z-X}{\sqrt{2}} \\ T = \frac{Z-X}{\sqrt{2}} \end{cases}$

Bell's Inequalities

Try this "experimental setting":

Alice measures one of $\begin{cases} Q = Z \\ R = X \end{cases}$ Bob measures one of $\begin{cases} S = \frac{-Z-X}{\sqrt{2}} \\ T = \frac{Z-X}{\sqrt{2}} \end{cases}$

One can show (Rule 3 of Quantum Mechanics) that

$$E[QS] = \langle QS \rangle = \frac{1}{\sqrt{2}}; \quad \langle RS \rangle = \frac{1}{\sqrt{2}}; \quad \langle RT \rangle = \frac{1}{\sqrt{2}}; \quad \langle QT \rangle = -\frac{1}{\sqrt{2}}$$

Bell's Inequalities

Try this "experimental setting":

Alice measures one of $\begin{cases} Q = Z \\ R = X \end{cases}$ Bob measures one of $\begin{cases} S = \frac{-Z-X}{\sqrt{2}} \\ T = \frac{Z-X}{\sqrt{2}} \end{cases}$

One can show (Rule 3 of Quantum Mechanics) that

$$E[QS] = \langle QS \rangle = \frac{1}{\sqrt{2}}; \quad \langle RS \rangle = \frac{1}{\sqrt{2}}; \quad \langle RT \rangle = \frac{1}{\sqrt{2}}; \quad \langle QT \rangle = -\frac{1}{\sqrt{2}}$$

and thus

$$\mathcal{A} = \langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}$$

The Bell inequality is **violated** by quantum mechanics!!!!

Bell's Inequalities

$$\mathcal{A} = \langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}$$

Does this actually happen?

Bell's Inequalities

$$\mathcal{A} = \langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}$$

Does this actually happen?

YES!!

The 2022 Nobel Prize in Physics was given to Aspect, Clauser, and Zeilinger for "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".

The E91 Protocol

After Artur Ekert, 1991.

Quantum key distribution protocol similar to BB84, except that eavesdropping is tested with the Bell inequality.

The E91 Protocol

After Artur Ekert, 1991.

Quantum key distribution protocol similar to BB84, except that eavesdropping is tested with the Bell inequality.

Say, Alice and Bob take a random portion of their qubits and use them for computing the value of $\mathcal{A} = \langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle$:

- if $\mathcal{A} \approx 2\sqrt{2}$ then all fine (distil and generate key as BB84);
- else `abort` (too much eavesdropping or noise).

Coda

Since Bell's inequality is empirically violated, some of its assumptions must be **wrong**.

Coda

Since Bell's inequality is empirically violated, some of its assumptions must be **wrong**.

Assumptions:

1. neither Alice nor Bob decide which observables they will measure before they receive their particle; [**Realism**]
2. both Alice and Bob measure their particle at the same time (to avoid causal interference between their measurements). [**Locality**]

Coda

Since Bell's inequality is empirically violated, some of its assumptions must be **wrong**.

Assumptions:

1. neither Alice nor Bob decide which observables they will measure before they receive their particle; [**Realism**]
2. both Alice and Bob measure their particle at the same time (to avoid causal interference between their measurements). [**Locality**]

Experiments tell us that either realism or locality (or both!) must be wrong.

Coda

Since Bell's inequality is empirically violated, some of its assumptions must be **wrong**.

Assumptions:

1. neither Alice nor Bob decide which observables they will measure before they receive their particle; [**Realism**]
2. both Alice and Bob measure their particle at the same time (to avoid causal interference between their measurements). [**Locality**]

Experiments tell us that either realism or locality (or both!) must be wrong.

Research: can you find other uses of the Bell inequalities?