THE UNIVERSITY *of* EDINBURGH
informatics

Quantum Cyber Security
Lecture 5: Quantum Information Part III

Mina Doosti

In this lecture…

We learn about:

- Generalised quantum measurements
  - POVM
  - Projective measurements
- Quantum operations or how quantum states are evolved
  - Unitary (noiseless) quantum operations
  - Quantum gates as unitary operators
- Entangling and non-entangling operations

Measurements (recap)

Measurement is the way to extract (classical) information from a quantum system.

In general, the following rule applies to quantum measurements:

Born Rule:

The measured result for an observable O, on a quantum system $|\psi\rangle$ is given by its eigenvalues λ
The probability of getting a specific eigenvalue λ_i is equal to $\mathrm{p(i)} = \langle\psi|P_i|\psi\rangle$
or more generally for a density matrix ρ is given by $p(i) = Tr[P_i \rho P_i^\dagger]$
Where P_i is the projection onto the eigenspace of O corresponding to λ_i

Now let's learn about more general measurements in QM.

POVM

POVM (Positive Operator-Valued Measurement) is the most general class of measurements in quantum mechanics

Definition: A POVM on $\mathbb{C}^d$ is a set of positive semidefinite ($M_j \geq 0$) matrices $\{M_j\}_j$ such that:

$$\sum_j M_j = \mathbb{I}_d$$

The probability p_j of obtaining the outcome j when performing the measurement $\{M_j\}_j$ is given by:

$$p_j = Tr[M_j \rho]$$

This is the generalisation of the Born rule.

Note that the post measurement state is not directly determined by the POVM formalism. For that we need a new tool!

Kraus Operators

Definition: Let $\{M_j\}_j$ be a POVM on $\mathbb{C}^d$. A Kraus operator representation of M is a set of matrices K_j such that:

$$\forall j \; M_j = K_j^\dagger K_j$$

Also remember that due to POVM condition we have:

$$\sum_j K_j^\dagger K_j = \mathbb{I}_d$$

Now we can write the post-measurement state of a POVM with respect to its Krause operator! Let's say the outcome j is obtained after measuring a density matrix ρ then the post-measurement state is:

$$\rho_j = \frac{K_j \rho K_j^\dagger}{Tr[K_j^\dagger K_j \rho]}$$

Note: If $Tr\left[K_j^\dagger K_j \rho\right] = 0$ the probability of getting outcome j is 0, and hence there is no post-measurement state in that case.

Projective Measurements

Projective measurements, the measurements we have seen so far, are a subclass of POVMs.
Let's see their formal definition:

Definition: A projective measurement (also called von Neumann measurement) is given by a set of orthogonal projector (projection operator) P_j :

$$P_j^2 = P_j \quad \text{and} \quad \sum_j P_j = \mathbb{1}$$

The probability of observing outcome j after applying this measurement to state ρ is given by:

$$p_j = Tr[P_j\rho] \text{ (or } p_j = \langle\psi|P_j|\psi\rangle \text{ for pure states)}$$

And the post measurement state is:

$$\rho_j = \frac{P_j\rho P_j}{Tr[P_j\rho]}$$

As a POVM, the Kraus operators for a projective measurement are specified as: $\mathrm{K_j} = P_j = \sqrt{M_j}$

Examples

$\rho = \sum_x p_x |x\rangle\langle x| \rightarrow$ classical mixture

Measure ρ with POVM $\underbrace{M_x = |x\rangle\langle x|}$

check: $\sum_x M_x = \sum_x |x\rangle\langle x| = I$

$Pr_{\text{get } x} = tr(M_x \rho) = tr(|x\rangle\langle x|\rho) = \langle x|\rho|x\rangle = p_x$

Measuring 2-qubit system

$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$

Let: $M_1 = |\Phi^+\rangle\langle\Phi^+|$ $M_2 = |\Phi^-\rangle\langle\Phi^-|$, $M_3 = |\Psi^+\rangle\langle\Psi^+|$, $M_4 = |\Psi^-\rangle\langle\Psi^-|$

$\Phi^- \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $\Psi^+ \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $\Psi^- \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

$P_1 = tr(M_1 |EPR\rangle\langle EPR|) = \langle\Phi^+|\overbrace{\Phi^+\rangle\langle\Phi^+}^{\rho_{EPR}}|\Phi^+\rangle = 1$

$P_2 = P_3 = P_4 = 0$

because $\langle\Phi^+|\Phi^-\rangle = \langle\Phi^+|\Psi^+\rangle = \langle\Phi^+|\Psi^-\rangle = 0$

Example: Measuring Parity with POVM

Measuring parity of a 2-qubit system

00 , 11 → even parity   01 , 10 → odd parity

Let's define POVM: $M_{even} = |00\rangle\langle 00| + |11\rangle\langle 11|$ $M_{odd} = |01\rangle\langle 01| + |10\rangle\langle 10|$

↳ should be: $I - M_{even}$ ✓

$$p_{even} = tr(M_{even}\,\rho) = \langle 00|\rho|00\rangle + \langle 11|\rho|11\rangle \qquad p_{odd} = 1 - p_{even} = \langle 01|\rho|01\rangle + \langle 10|\rho|10\rangle$$

Let's try it on EPR state

$$p_{even} = tr(M_{even}|EPR\rangle\langle EPR|) = \langle 00|\tfrac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11| + |11\rangle\langle 00|\right)|00\rangle + \underbrace{\langle 11|EPR\rangle\langle EPR|11\rangle}_{\text{similar}}$$

$$= \tfrac{1}{2}\left[\overbrace{\langle 00|00\rangle}^{1}\langle 00|00\rangle + \cancel{\langle 00|11\rangle}^{0}\cancel{\langle 11|00\rangle}^{0} + \langle 00|00\rangle\cancel{\langle 11|00\rangle}^{0} + \cancel{\langle 00|11\rangle}^{0}\langle 00|00\rangle\right] + \tfrac{1}{2}$$

similar

$$= \tfrac{1}{2} + \tfrac{1}{2} = 1 \qquad p_{odd} = 0 \qquad \rho_{even} = \frac{1}{p_{even}} M_{even}|EPR\rangle\langle EPR|M_{even} = \underbrace{|EPR\rangle\langle EPR|}_{\text{unchanged!}}$$

Example: Partial measurements

Now let's see what happens if we measure one of the qubits of a 2 qubit system

$|EPR\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Let's measure system B in standard basis: $\underbrace{M_0 = I_A \otimes |0\rangle\langle 0|_B, M_1 = I_A \otimes |1\rangle\langle 1|}_{\text{check it's a POVM } \checkmark}$

$$p_0 = tr(M_0 \rho_{EPR}) = \frac{1}{2} tr\left[(I_A \otimes |0\rangle\langle 0|)(|00\rangle\langle 00| + |11\rangle\langle 11| + |00\rangle\langle 11| + |11\rangle\langle 00|)\right]$$

$$= \frac{1}{2} tr\Big[\underbrace{|0\rangle\langle 0| \left(|0\rangle\langle 0|0\rangle\langle 0|\right)}_{tr(|0\rangle\langle 0|) = 1} + \underbrace{|1\rangle\langle 1| \times |0\rangle\cancel{\langle 0|}^{0}1\rangle\langle 1|}_{0} + \underbrace{|0\rangle\langle 1| \times 0}_{0} + \underbrace{|1\rangle\langle 0| \times 0}_{0} \Big] = \frac{1}{2}$$

also $p_1 = \frac{1}{2}$

post-measurement state after getting outcome 0 : $\rho_0^A = |0\rangle\langle 0|$

post-measurement state: $\rho^A = \frac{1}{2}(I \otimes \langle 0|)\rho_{EPR}(I \otimes |0\rangle) + \frac{1}{2}(I \otimes \langle 1|)\rho_{EPR}(I \otimes |1\rangle)$

(for both outcomes)

↓

if Alice doesn't know the outcome $= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ → Maximally mixed state!

Non-orthogonal POVM

Let's define a POVM with 3 possible outcomes!

Imagine we have two possible states, and we want to distinguish them via measurement. We want the following cases:

case 1: It's outcome 1 $|\psi_1\rangle$

case 2: It's outcome 2 $|\psi_2\rangle$

case 3: I don't know!

$$M_1 + M_2 + M_3 = I$$

$$\alpha|\psi_2^\perp\rangle\langle\psi_2^\perp| \qquad \beta|\psi_1^\perp\rangle\langle\psi_1^\perp| \qquad I - M_1 - M_2$$

Let's say $|\psi_1\rangle = |0\rangle$ $\quad |\psi_2\rangle = |+\rangle$ $\quad M_1 = \alpha|-\rangle\langle-|$ $\quad M_2 = \beta|1\rangle\langle 1|$ $\quad M_3 = I - \alpha|-\rangle\langle-| + \beta|1\rangle\langle 1|$

Let's measure state $|+\rangle$

$$p_1 = tr(\alpha|-\rangle\langle-|\,|+\rangle\langle+|) = 0 \qquad p_2 = tr(\beta|1\rangle\langle 1|(|+\rangle\langle+|) = \frac{\beta}{2} \qquad p_3 = 1 - \frac{\beta}{2}$$

You can then optimise the value of α and β to find the measurement that has the least possible "I don't know" error!

A note about the previous example:

From a question during the lecture: Why we don't measure only in Hadamard basis? What's the difference?

if we measure in Hadamard $\{|+\rangle, |-\rangle\}$ basis, our measurement operators are:

$M_1 = |+\rangle\langle+|$ $\quad M_2 = |-\rangle\langle-|$

Remember I have two possible states, $|0\rangle$, $|+\rangle$ and I don't know which one I am measuring!

if it's $|+\rangle \longrightarrow$ $P_1 = 1$ $\quad P_2 = 0 \rightarrow$ so I can tell with certainty it's $|+\rangle$

but if $|0\rangle \longrightarrow$ $P_1 = \frac{1}{2}$ $\quad P_2 = \frac{1}{2} \rightarrow$ so half of the times I am "wrong".

★ The idea with the previous measurement is that no matter which one you get

you can never be wrong, but instead sometimes you "can't distinguish"

Unitary operations

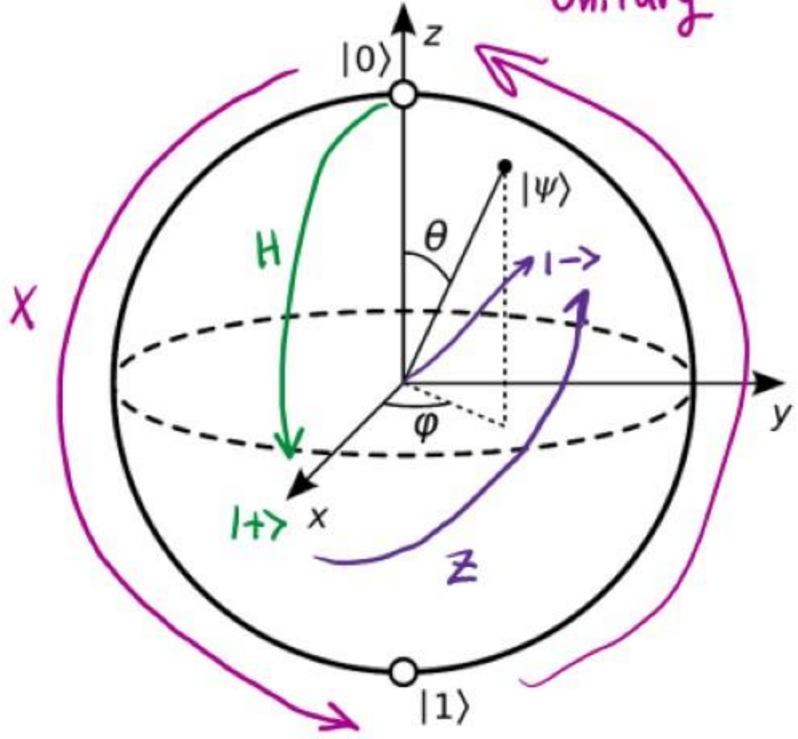
The evolution of pure quantum states is given by a unitary transformation: $U|\psi_{in}\rangle = |\psi_{out}\rangle$ (second postulate)

Unitary operator: Is a linear operator on a Hilbert space that preserves the inner product. $UU^\dagger = U^\dagger U = \mathbb{1}$

Hermitian

Fun (and important) fact: $U = e^{iH}$ try to prove it!

Unitary



Pauli: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $XX^\dagger = X^\dagger X = I$ Rotate π degree around X axis!

Pauli: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $ZZ^\dagger = Z^\dagger Z = I$ Rotate π degree around Z

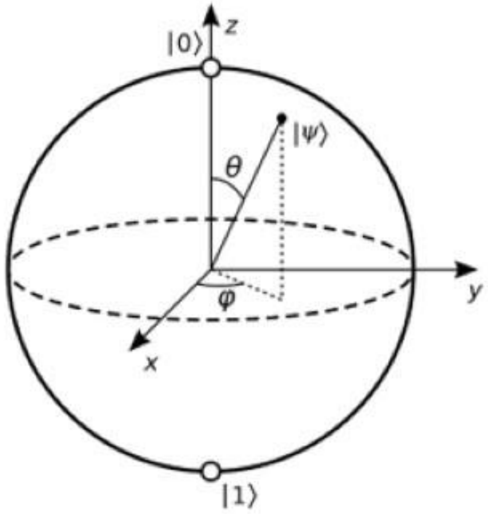
Pauli: $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ around Y axis

Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ Rotate $\frac{\pi}{2}$ degree → change basis!

Any unitary here: $U_{\hat{n}}(\theta) = I \cos\left(\frac{\theta}{2}\right) - i(\hat{n}\cdot\vec{\sigma}) \sin\left(\frac{\theta}{2}\right)$

(X, Y, Z)

All quantum gates are unitaries



Rotation gates:

$$R_x(\theta) = e^{(-i\theta X/2)} = \cos(\theta/2)I - i\sin(\theta/2)X = \begin{bmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

$$R_y(\theta) = e^{(-i\theta Y/2)} = \cos(\theta/2)I - i\sin(\theta/2)Y = \begin{bmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{bmatrix}$$

$$R_z(\theta) = e^{(-i\theta Z/2)} = \cos(\theta/2)I - i\sin(\theta/2)Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

Any rotation is a combination of these.

$$R_{\hat{n}}(\theta) = e^{-i\theta\hat{n}\cdot\frac{1}{2}\vec{\sigma}}$$

More math-y nerdy stuff: Bloch sphere shows Lie algebra for the group of unitary matrices on qubit that is SU(2) is isomorphic to the Lie algebra of the group of three-dimensional rotations SO(3)

Unitary evolution of a density matrix: $\rho_{out} = U\rho_{in}U^\dagger$

$U = X \qquad \rho_{in} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|-\rangle\langle -|$

$$\rho_{out} = \frac{1}{2}\underbrace{X|0\rangle}_{|1\rangle}\underbrace{\langle 0|X}_{\langle 1|} + \frac{1}{2}\underbrace{X|-\rangle}_{-|-\rangle}\underbrace{\langle -|X}_{-\langle -|} = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|-\rangle\langle -|$$

$U = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad U^\dagger = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \rho_{in} = \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$

$$\rho_{out} = \frac{1}{4}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & -3i \\ i & -i \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 3 \end{pmatrix}$$

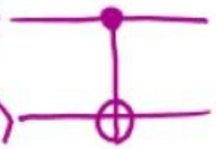
Unitaries on more qubits

By composition (tensor product):

$$U_1 \otimes U_2 \otimes U_3 \quad |q_1 q_2 q_3\rangle = U_1|q_1\rangle \otimes U_2|q_2\rangle \otimes U_3|q_3\rangle = |q_1^{out}\rangle \otimes |q_2^{out}\rangle \otimes |q_3^{out}\rangle$$

Two-qubit gates:

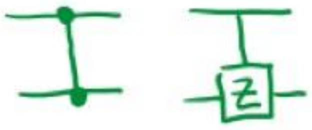
* CNOT $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$



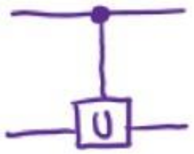
if $|q_1\rangle = |0\rangle \to$ do nothing

if $|q_1\rangle = |1\rangle \to$ apply X on $|q_2\rangle$

* CZ $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$



CU (general U) $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$, U



$|q_1\rangle = |1\rangle$
$\downarrow$
apply U

* SWAP $= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

swap them!

$$\text{SWAP}\,|q_1\rangle|q_2\rangle = |q_2\rangle|q_1\rangle$$

* Toffoli

CCNOT

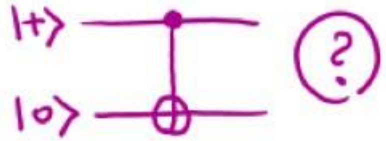
$\}\to$ 2 controls

$$\text{Toffoli}\,|abc\rangle \to |ab\; c \oplus (a \wedge b)\rangle$$

Entangling operators

Some unitary operators entangle separate systems. How?

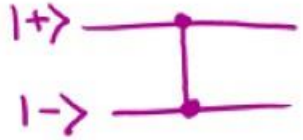
$$\mathrm{CNOT}\,(|+\rangle \otimes |0\rangle) = \mathrm{CNOT}\left[\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|10\rangle\right]$$



$$= \tfrac{1}{\sqrt{2}}\left[\mathrm{CNOT}\,|\underset{\text{Apply } I}{\underline{0}\,0}\rangle + \mathrm{CNOT}\,|\underset{\text{Apply } X}{\underline{1}\,0}\rangle\right] = \tfrac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

Entangled!

$$CZ\,(|+\rangle|-\rangle) = \tfrac{1}{\sqrt{2}}\left[CZ|0\rangle|-\rangle + CZ|1\rangle|-\rangle\right]$$



$$= \tfrac{1}{\sqrt{2}}\left[|0\rangle|-\rangle + |1\rangle Z\left(\tfrac{1}{\sqrt{2}}|0\rangle - \underbrace{|1\rangle}_{-|1\rangle}\right)\right]$$

$$= \tfrac{1}{\sqrt{2}}\left[|0\rangle|-\rangle + |1\rangle|+\rangle\right]$$

$$= \tfrac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle + |11\rangle\right]$$

→ also entangled!

Entanglement as a resource

In quantum information entanglement is a resource.

Non-entangling operators are the ones that consume this resource or don't change it.

For instance, if you are only allowed to do Local Operation and Classical Communication, you cannot create or increase entanglement. This class is called "LOCC".

Alice

$$\frac{1}{\sqrt{2}}\left[|0_A 0_B\rangle + |1_A 1_B\rangle\right]$$

Bob

Alice measures her state in comp. basis $\rightarrow$ gets $|0\rangle_A$ $\longrightarrow$ Bob's state collapses to $|0\rangle_B$

$$\underbrace{|0\rangle_A \otimes |0\rangle_B}_{\text{separable}}$$

Alice applies H

Bob applies H

$$H_A \otimes H_B \left[\tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right] = \frac{1}{\sqrt{2}}\left[|{+}{+}\rangle + |{-}{-}\rangle\right] \rightarrow \text{same state!}$$

Formally defining the LOCC operations helps us to "quantify" the amount of entanglement.

If you are super interested: Chitambar, Eric, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. "Everything you always wanted to know about LOCC (but were afraid to ask)." *Communications in Mathematical Physics* 328 (2014): 303-326.

Resources

1. Quantum Computation and Quantum Information by *Nielsen & Chuang*: 2.2

2. Introduction to Quantum Cryptography by *Thomas Vidick and Stephanie Wehner*: chapter 2: 2.3

3. Quantum Information Theory by *Mark M. Wilde*: chapter 4: 4.1, 4.2, 4.3