Quantum Cyber Security
Lecture 5: Quantum Information Basics III

Petros Wallden

University of Edinburgh

27th January 2026

This Lecture

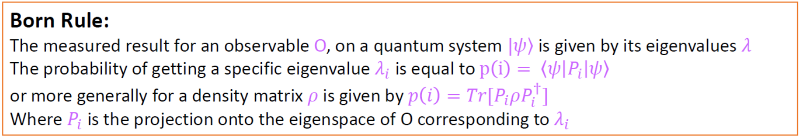
- Generalised quantum measurements
    - POVM (mathematics)
    - Projective and general measurements with examples

This Lecture

- Generalised quantum measurements
  - POVM (mathematics)
  - Projective and general measurements with examples
- Quantum operations
  - unitary operations
  - single qubit and entangling operations (with examples)

Measurements

- We have seen simple one qubit measurements
- It generalises for observable O



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

- P_i is projection to the eigenspace corresp. to eigenvalue λ_i
- Due to trace's cyclic property and $P^2 = P$ (projection):

$$p(i) = \mathrm{Tr}\left(P_i \rho\right)$$

- Can define more general measurements (non-projective)

POVM (Positive Operator-Valued Measure)

It is the basis for general quantum measurements

Definition: POVM

A POVM is defined as a set of Hermitian ($M_j^\dagger = M_j$), positive semi-definite $M_j \geq 0$ 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 $\{M_j\}_j$ on state ρ is given by:

$$p_j = \mathrm{Tr}\left(M_j \rho\right)$$

- Generalises Born's rule
- Post-measurement state not determined by POVM (see next)

Kraus Operators

Definition: Kraus Operators

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

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

- Their existence is guaranteed since M_j positive semi-definite
- From POVMs we have: $\sum_j K_j^\dagger K_j = \mathbb{I}_d$
- The probability of obtaining outcome j:

$$p_j = \mathrm{Tr}\left(K_j \rho K_j^\dagger\right) = \mathrm{Tr}\left(K_j^\dagger K_j \rho\right) = \mathrm{Tr}\left(M_j \rho\right)$$

- The post measurement state after outcome j:

$$\rho_j := \frac{K_j \rho K_j^\dagger}{\mathrm{Tr}\left(K_j \rho K_j^\dagger\right)}$$

- If $\mathrm{Tr}\left(K_j \rho K_j^\dagger\right) = 0$ outcome j never occurs

Projective Measurements

- All measurements we have seen are subclass of POVMs called **projective**

Definition: Projective Measurements

A measurement $\{M_j\}_j$ where all measurement operators are projections $M_j = P_j = P_j^2 \ \ \forall\, j$ is called **projective**

- It follows that $\sum_j P_j = \mathbb{I}$ and that both $M_j = P_j\ ;\ K_j = P_j\ \forall\, j$
- Probability of outcome j on state ρ:

$$p_j = \mathrm{Tr}\left(P_j \rho\right) \quad \text{or for pure states: } p_j = \langle\psi|\, P_j\, |\psi\rangle$$

- State after obtaining outcome j:

$$\rho_j = \frac{P_j \rho P_j}{\mathrm{Tr}\left(P_j \rho\right)}$$

Examples (projective)

- State $\rho = \sum_x p_x |x\rangle \langle x|$ (classical mixture)
- Measure in the computational basis, i.e. $M_x := |x\rangle \langle x|$
- Check: it is a measurement; it gives the intuitive answer p_x

Examples (projective)

- State $\rho = \sum_x p_x |x\rangle\langle x|$ (classical mixture)

- Measure in the computational basis, i.e. $M_x := |x\rangle\langle x|$

- Check: it is a measurement; it gives the intuitive answer p_x

- Two qubit (entangled) measurement

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

- Measure in basis: $M_1 = |\Phi^+\rangle\langle\Phi^+|$; $M_2 = |\Phi^-\rangle\langle\Phi^-|$

  $M_3 = |\Psi^+\rangle\langle\Psi^+|$; $M_4 = |\Psi^-\rangle\langle\Psi^-|$

  where $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$; $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$

- Check: it is a measurement; it gives the intuitive answer

Example (measuring parity)

- $00, 11$ even parity; $01, 10$ odd parity
- Define POVM (check condition; projects to even/odd subspace)

  $$M_{\text{even}} = |00\rangle\langle 00| + |11\rangle\langle 11| \;\; ; \;\; M_{\text{odd}} = |01\rangle\langle 01| + |10\rangle\langle 10|$$

- $\cdots$ after calculation gets:
  $$p_{\text{even}} = \langle 00|\,\rho\,|00\rangle + \langle 11|\,\rho\,|11\rangle \;\; ; \;\; p_{\text{odd}} = \langle 01|\,\rho\,|01\rangle + \langle 10|\,\rho\,|10\rangle$$
- Check on $\rho = |\Phi^+\rangle\langle\Phi^+|$

  (expected outcome prob 1 for even parity and state unchanged!)

Example (partial measurement)

- 2-qubit state $|\Phi^+\rangle_{AB}$, measure system B only in comp basis
- $M_0 := \mathbb{I}_A \otimes |0\rangle\langle 0|_B$; $M_1 := \mathbb{I}_A \otimes |1\rangle\langle 1|_B$
- Check it is a measurement (POVM condition satisfied)
- Compute p_0, p_1 (each with prob 0.5)
- Compute the corresponding post-measurement states ($\rho_0^A = |0\rangle\langle 0|$; $\rho_1^A = |1\rangle\langle 1|$)
- What is the state of A if we measure system B but "forget" the outcome? (totally mixed state: property of maximally entangled states)

Non-projective POVM

- We can measure a single qubit with more than two outcomes!
  - Prob 0.5 measure in $\{\left|0\right\rangle, \left|1\right\rangle\}$ and prob 0.5 in $\{\left|+\right\rangle, \left|-\right\rangle\}$

$$M_0 = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| \; ; \; M_1 = \frac{1}{2}\left|1\right\rangle\left\langle 1\right| \; ; M_2 = \frac{1}{2}\left|+\right\rangle\left\langle +\right| \; ; M_3 = \frac{1}{2}\left|-\right\rangle\left\langle -\right|$$

Check it is measurement and probs on state $\rho = \left|0\right\rangle\left\langle 0\right|$

Non-projective POVM

- We can measure a single qubit with more than two outcomes!

- Prob 0.5 measure in $\{|0\rangle, |1\rangle\}$ and prob 0.5 in $\{|+\rangle, |-\rangle\}$

  $M_0 = \frac{1}{2}|0\rangle\langle 0|$; $M_1 = \frac{1}{2}|1\rangle\langle 1|$; $M_2 = \frac{1}{2}|+\rangle\langle +|$; $M_3 = \frac{1}{2}|-\rangle\langle -|$

  Check it is measurement and probs on state $\rho = |0\rangle\langle 0|$

- Consider

  $M_0 = \alpha|-\rangle\langle -|$; $M_1 = \beta|1\rangle\langle 1|$; $M_2 = \mathbb{I} - \alpha|-\rangle\langle -| - \beta|1\rangle\langle 1|$

  Is it a measurement? (for $\alpha = \beta = 1/2$: yes)

  What are the probs on state $\rho = |+\rangle\langle +|$?

Non-projective POVM

- We can measure a single qubit with more than two outcomes!
  - Prob 0.5 measure in $\{|0\rangle, |1\rangle\}$ and prob 0.5 in $\{|+\rangle, |-\rangle\}$

    $$M_0 = \frac{1}{2}|0\rangle\langle 0| \;;\; M_1 = \frac{1}{2}|1\rangle\langle 1| \;; M_2 = \frac{1}{2}|+\rangle\langle +| \;; M_3 = \frac{1}{2}|-\rangle\langle -|$$

    Check it is measurement and probs on state $\rho = |0\rangle\langle 0|$
  - Consider

    $$M_0 = \alpha|-\rangle\langle -| \;;\; M_1 = \beta|1\rangle\langle 1| \;; M_2 = \mathbb{I} - \alpha|-\rangle\langle -| - \beta|1\rangle\langle 1|$$

    Is it a measurement? (for $\alpha = \beta = 1/2$: yes)

    What are the probs on state $\rho = |+\rangle\langle +|$?
- This can be used to distinguish "with no errors", between non-orthogonal states $|0\rangle, |+\rangle$, while allowing the "I don't know" answer!

  Known as **Unambiguous State Discriminations**

Unitary operations

- Unitary operations: $U^\dagger U = UU^\dagger = \mathbb{I}$
- Also $U = e^{iH}$ for H a Hermitian matrix
- In quantum computing, gates are unitaries (see below)
- However, there are more general operations (see next lecture)

Single Qubit Gates

- For a single classical bit there is only one non-trivial gate: NOT: takes $0 \rightarrow 1$ and $1 \rightarrow 0$, i.e. $\neg a = a \oplus 1$
- For qubits all unitary operators are allowed gates

  Even for single qubit, there exist **infinite** different gates

Single Qubit Gates

- For a single classical bit there is only one non-trivial gate: NOT: takes $0 \to 1$ and $1 \to 0$, i.e. $\neg a = a \oplus 1$
- For qubits all unitary operators are allowed gates

  Even for single qubit, there exist **infinite** different gates
- The quantum NOT-gate is the Pauli X:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

  Acts as the NOT-gate to computational basis vectors: $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$

  For a general qubit: $\alpha|0\rangle + \beta|1\rangle \to \alpha|1\rangle + \beta|0\rangle$

$$\alpha|0\rangle + \beta|1\rangle \quad \text{———}\boxed{X}\text{———} \qquad \alpha|1\rangle + \beta|0\rangle$$

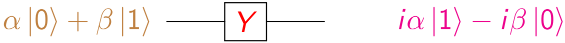
Single Qubit Gates

- We give some gates. Using a suitable finite collection of gates we can approximate all (see later).
- Pauli Y-gate:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

On computational basis vectors: $|0\rangle \rightarrow i\,|1\rangle$ and $|1\rangle \rightarrow -i\,|0\rangle$.

Acting on a general state: $\alpha\,|0\rangle + \beta\,|1\rangle \rightarrow i\alpha\,|1\rangle - i\beta\,|0\rangle$



$\alpha\,|0\rangle + \beta\,|1\rangle$ $\qquad$ $i\alpha\,|1\rangle - i\beta\,|0\rangle$

Single Qubit Gates

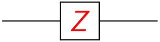
- We give some gates. Using a suitable finite collection of gates we can approximate all (see later).
- Pauli Z-gate:

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

On computational basis vectors: $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow -|1\rangle$.

Acting on a general state: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$

$\alpha|0\rangle + \beta|1\rangle$



$\alpha|0\rangle - \beta|1\rangle$

E.g. $Z|+\rangle = |-\rangle$

Single Qubit Gates

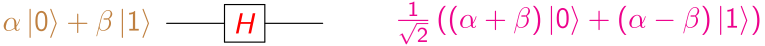
- We give some gates. Using a suitable finite collection of gates we can approximate all (see later).
- Hadamard H-gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

On computational basis vectors: $|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Acting on a general state:

$$\alpha\,|0\rangle + \beta\,|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left((\alpha+\beta)\,|0\rangle + (\alpha-\beta)\,|1\rangle\right)$$



$\alpha\,|0\rangle + \beta\,|1\rangle$ —$\boxed{H}$— $\frac{1}{\sqrt{2}}\left((\alpha+\beta)\,|0\rangle + (\alpha-\beta)\,|1\rangle\right)$

E.g. $H|0\rangle = |+\rangle$

Single Qubit Gates

- We give some gates. Using a suitable finite collection of gates we can approximate all (see later).
- Phase gate R_θ-gate:

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

On computational basis vectors: $|0\rangle \to |0\rangle$ and $|1\rangle \to e^{i\theta}|1\rangle$.

Acting on a general state:

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|0\rangle + e^{i\theta}|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \quad \text{———}\boxed{R_\theta}\text{———} \qquad \alpha|0\rangle + e^{i\theta}\beta|1\rangle$$

Single Qubit Gates

Some examples of phase gates R_θ:

1. $R_\pi = Z$
2. $R_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ Some authors call this gate as **the** phase gate
3. $R_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix}$ This gate is also called the $\pi/8$-gate

   Note: This is not a typo! Historically is called this way even though it corresponds to $\theta = \pi/4$ due to different conventions!

Two Qubits Gates

Notation: "Control" gates are denoted as $\mathrm{CU} = \wedge U$

Two Qubits Gates

Notation: "Control" gates are denoted as $\mathrm{CU} = \wedge U$

The first qubit acts as a control for the second qubit (target).

I.e. depending on the value of the first qubit we either do nothing $\mathbb{I}$ to the second qubit, or we apply the (single qubit) gate U to the second qubit

Two Qubits Gates

Notation: "Control" gates are denoted as $\mathrm{CU} = \wedge U$

The first qubit acts as a control for the second qubit (target).

I.e. depending on the value of the first qubit we either do nothing $\mathbb{I}$ to the second qubit, or we apply the (single qubit) gate U to the second qubit

Solid dot, signifies control qubit

Two Qubits Gates

- The most important two-qubit gate is CNOT (Controlled-NOT)

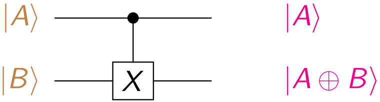
$$\wedge X = \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Two Qubits Gates

- The most important two-qubit gate is CNOT (Controlled-NOT)

$$\wedge X = \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- A general state: $a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \rightarrow a\,|00\rangle + b\,|01\rangle + c\,|11\rangle + d\,|10\rangle$

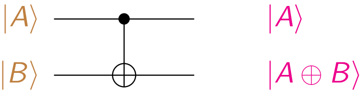


Two Qubits Gates

- The most important two-qubit gate is CNOT (Controlled-NOT)

$$\wedge X = \mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- A general state (alternative diagrammatic notation): $a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \rightarrow a\,|00\rangle + b\,|01\rangle + c\,|11\rangle + d\,|10\rangle$

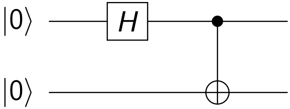


Example: entangling gate

- Consider $\wedge X(|+\rangle \otimes |0\rangle)$
- It gives: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$

Example: entangling gate

- Consider $\wedge X(|+\rangle \otimes |0\rangle)$
- It gives: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$
- From no entanglement, $\wedge X$ gives maximal entanglement
- The circuit for preparing the Bell state:



Two Qubits Gates

- Given $U = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix}$ the controlled U gate:

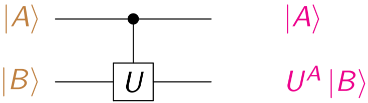
$$\wedge U = \mathrm{C}U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix}$$

Two Qubits Gates

- Given $U = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix}$ the controlled U gate:

$$\wedge U = \mathrm{C}U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{00} & U_{01} \\ 0 & 0 & U_{10} & U_{11} \end{bmatrix}$$

- A general state:
$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \rightarrow a|00\rangle + b|01\rangle +$
$+ |1\rangle U(c|0\rangle + d|1\rangle)$

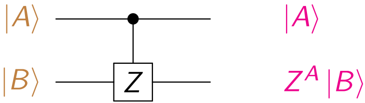


Two Qubits Gates

- E.g. the controlled Z gate:

$$\wedge Z = \mathrm{C}Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

- A general state:
$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \to a\,|00\rangle + b\,|01\rangle + c\,|10\rangle - d\,|11\rangle$



A Three Qubits Gate

- **The Toffoli gate:** Has two control qubits that are left unaffected, and a target qubit.

  Notation: $\wedge \wedge X$.

  Action: It acts as identity except when both controlled qubits are $|1\rangle$ where we apply X to the target qubit:

$$|A\rangle\,|B\rangle\,|C\rangle \rightarrow |A\rangle\,|B\rangle\,X^{AB}\,|C\rangle = |A\rangle\,|B\rangle\,|C \oplus AB\rangle$$

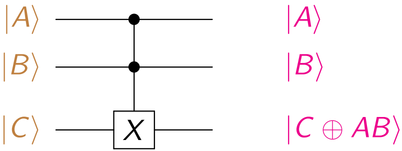
A Three Qubits Gate

- **The Toffoli gate:** Has two control qubits that are left unaffected, and a target qubit.

  Notation: $\wedge \wedge X$.

  Action: It acts as identity except when both controlled qubits are $|1\rangle$ where we apply X to the target qubit:

$$|A\rangle\,|B\rangle\,|C\rangle \rightarrow |A\rangle\,|B\rangle\,X^{AB}\,|C\rangle = |A\rangle\,|B\rangle\,|C \oplus AB\rangle$$


$|A\rangle$
$|B\rangle$
$|C\rangle$
X
$|A\rangle$
$|B\rangle$
$|C \oplus AB\rangle$