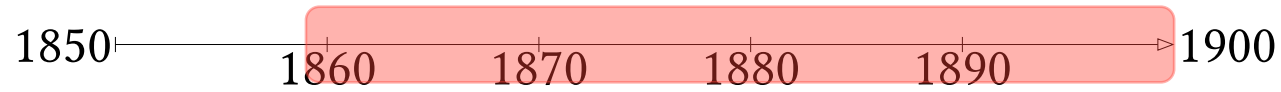


Introduction to quantum cryptography

Alex Bredariol Grilo

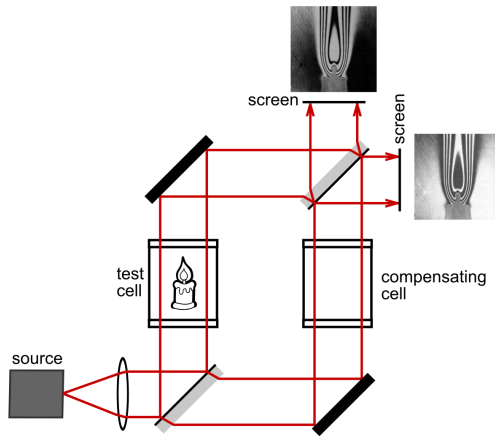


A bit of History

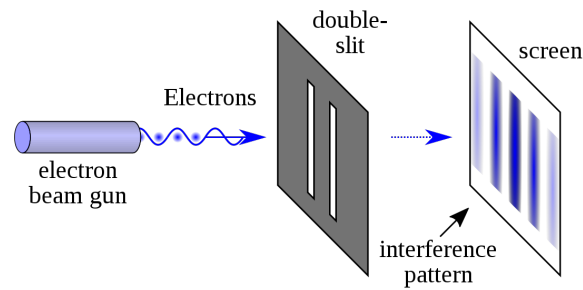


Classical physics is insufficient

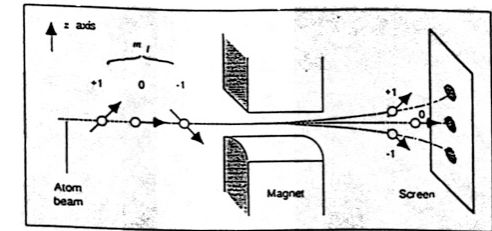
Mach Zehnder interferometer:



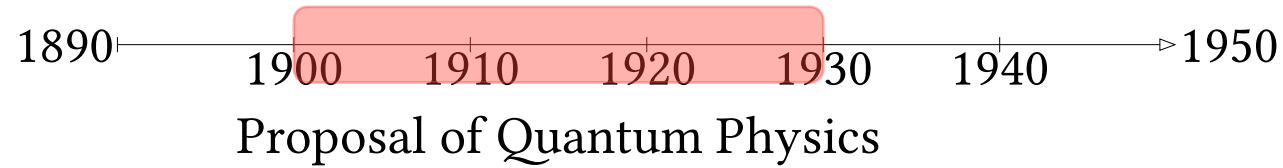
Double-slit experiment:



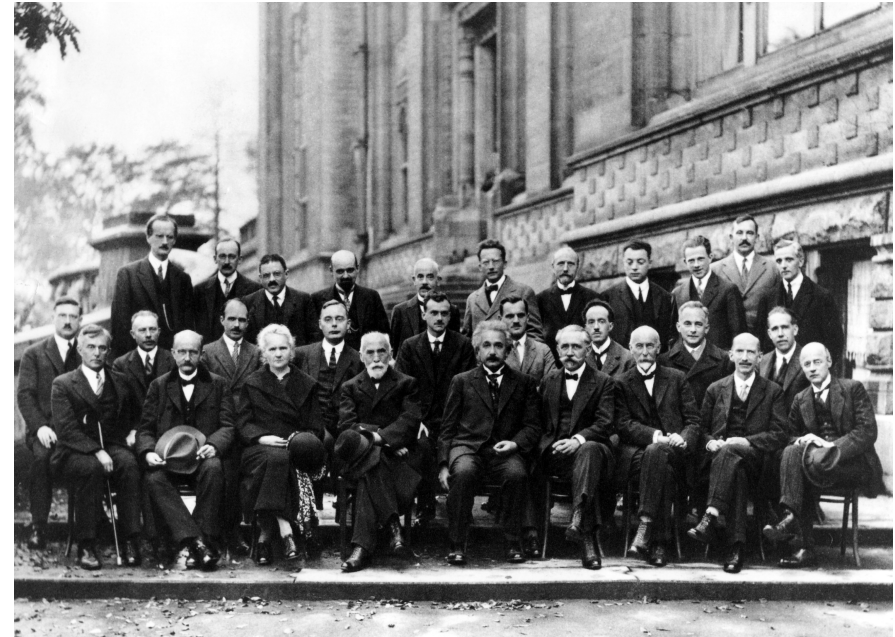
Stern-Gerlach experiment:



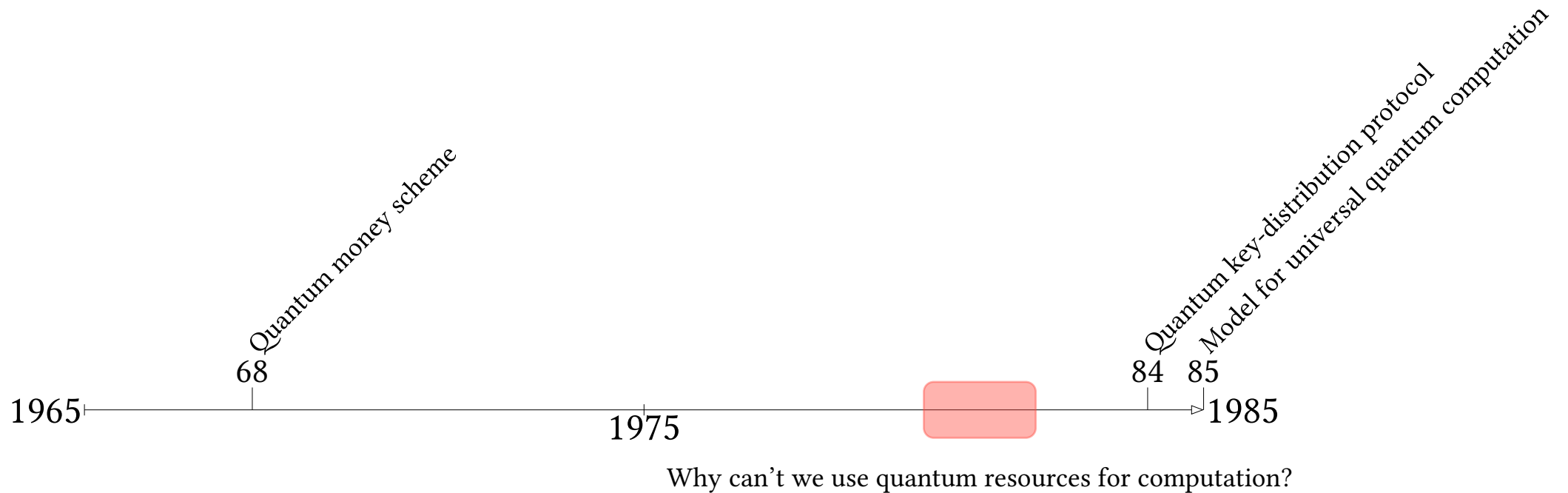
First quantum revolution



- energy quanta
- wave-particle duality
- Heisenberg's uncertainty principle
- ...



Quantum properties as computational resources



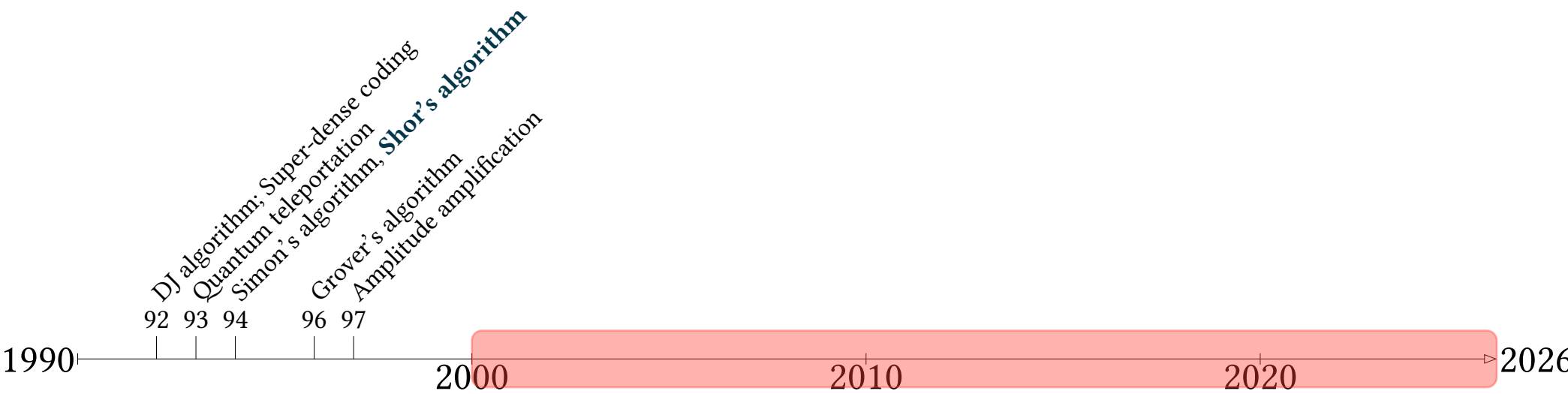
Quantum cryptography

- quantum states cannot be generally copied
- use quantum states as money
- protocols for sharing secret keys

Quantum computation:

- Classical computers do not seem to be able to simulate quantum systems efficiently
- Proposals of quantum devices to perform computation

Boom of quantum computing (theory)

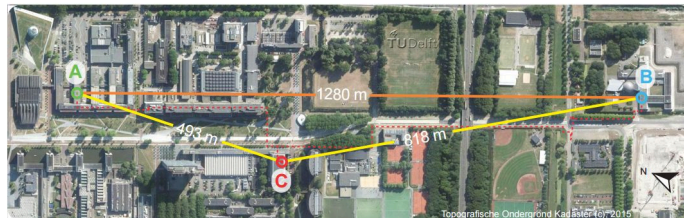


Too many contributions to cite

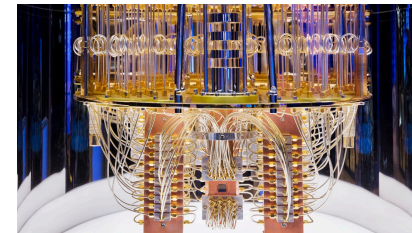
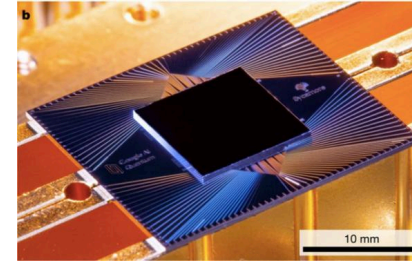


Physical implementation

Quantum crypto is a reality...



... and quantum computing may be not too far



This course

- **Goal:** Overview of the different flavours of topics in quantum cryptography
 1. Introduction: qubits, quantum circuits, entanglement
 2. Private-verification quantum money
 3. QKD
 4. Quantum Oblivious Transfer
 5. Quantum One-time Pad and Authentication
 6. Verification of quantum computations
 7. Pseudorandom-states and beyond
 8. Overview of other topics
- **Lecturers:**

Claude Crépeau (claudio.crepeau@estmtl.ca) and Alex B. Grilo (Alex.Bredariol-Grilo@lip6.fr)
- **Pre-requisites:**

Linear algebra and basic probability. Basic classical cryptography is a big plus.

Basic notions of quantum information theory

Postulates of quantum mechanics

1. **Quantum states:** how to represent physical objects (at the atomic level)?
2. **Evolution:** how do quantum states change in time?
3. **Measurements:** how can we “read” the properties of quantum states?

Our goal: definition of these concepts tailored to their use in Computer Science and Information Theory

Quantum state

Postulate: A quantum state is represented by a unit vector in a complex Hilbert space

Qubits: quantum state with two levels

- Hilbert space: $\mathbb{C}^2$
- Computational basis: $\left\{ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$
- Qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$

Examples in physics:

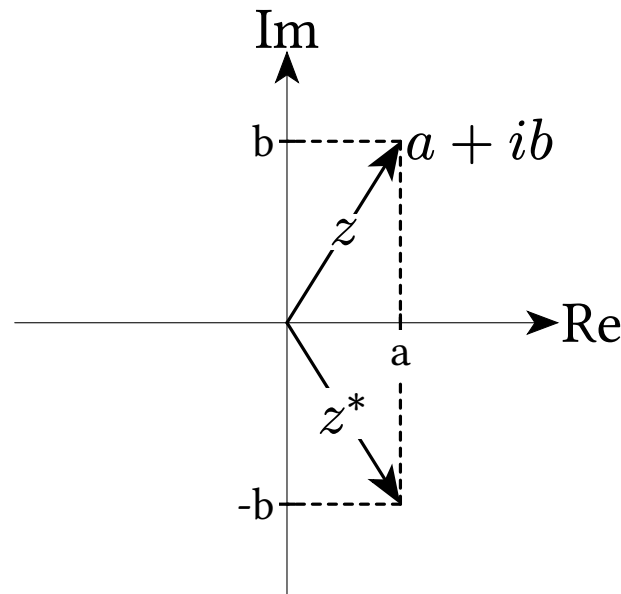
- Energy levels of a trapped ion
- Photon polarization
- ...

Quick recap on complex numbers

A complex number can be written as $z = a + ib$, where $a, b \in \mathbb{R}$ and $i^2 = -1$.

The **complex conjugate** of z is $z^* = a - ib$.

The **norm** of z is its distance from the origin: $|z| = \sqrt{a^2 + b^2} = \sqrt{zz^*}$.



Disclaimer: Most of the time we will only work with states with real amplitudes.

Quizz

Which one of these vectors is not a quantum state?

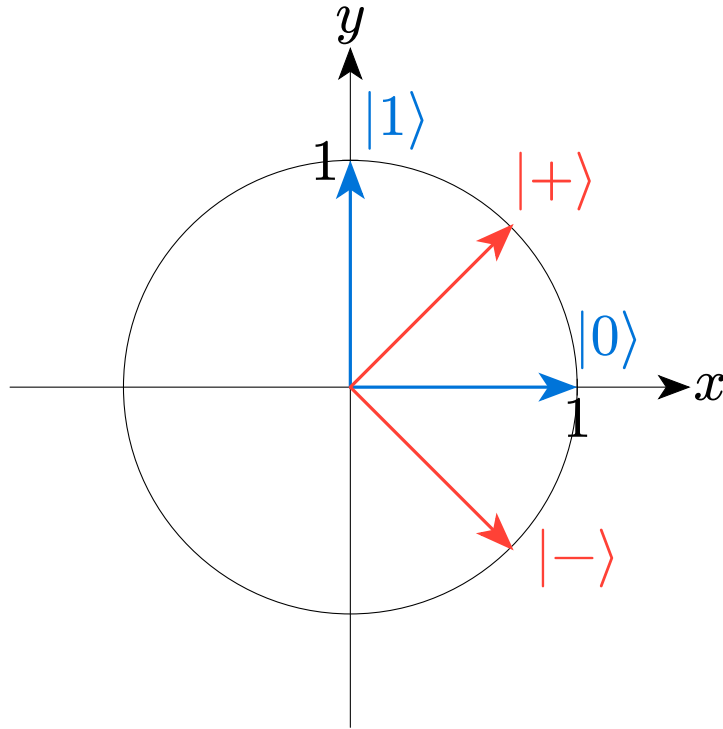
a) $|0\rangle$

b) $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

c) $\frac{1}{3}|0\rangle + \frac{2}{3}|1\rangle$: $\left|\frac{1}{3}\right|^2 + \left|\frac{2}{3}\right|^2 = \frac{5}{9} \neq 1$

d) $\frac{i}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle$

Specially important quantum states



Computational basis

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Hadamard basis

- $|+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Dirac notation

Ket: column vector

$$|\psi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_m \end{pmatrix} \quad |\varphi\rangle = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix}$$

Bra: row vector

$$\langle\psi| = (a_1^* \ a_2^* \ \dots \ a_m^*)$$

$$\langle\varphi| = (b_1^* \ b_2^* \ \dots \ b_m^*)$$

Bra-ket: inner product (complex number)

$$\langle\varphi|\psi\rangle = (b_1^* \ b_2^* \ \dots \ b_m^*) \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_m \end{pmatrix}$$

$$= \sum_{i \in [m]} b_i^* a_i \in \mathbb{C}$$

Ket-bra: outer product (complex matrix)

$$|\varphi\rangle\langle\psi| = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix} (a_1^* \ a_2^* \ \dots \ a_m^*)$$

$$= \begin{pmatrix} b_1 a_1^* & b_1 a_2^* & \dots & b_1 a_m^* \\ b_2 a_1^* & b_2 a_2^* & \dots & b_2 a_m^* \\ \dots & \dots & \dots & \dots \\ b_m a_1^* & b_m a_2^* & \dots & b_m a_m^* \end{pmatrix} \in \mathbb{C}^{m \times m}$$

Math background: tensor product

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \cdots & \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \text{ and } B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,n'} \\ & \cdots & \\ b_{m',1} & \cdots & b_{m',n'} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ & \cdots & \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix} = \begin{pmatrix} a_{1,1}b_{1,1} & \cdots & a_{1,n}b_{1,n'} \\ & \cdots & \\ a_{m,1}b_{m',1} & \cdots & a_{m,n}b_{m',n'} \end{pmatrix}$$

Tensor product - example

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} := |0\rangle|1\rangle \text{ or } |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} := |1\rangle|0\rangle \text{ or } |10\rangle$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Quantum states - multiple qubits

Register with n qubits: n qubits “side-by-side”

- Hilbert space: $\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}$
- Computational basis: $|i\rangle, i \in \{0, 1\}^n$
- Quantum state: $|\varphi\rangle = \sum_{i \in \{0, 1\}^n} \alpha_i |i\rangle, \alpha_i \in \mathbb{C}$ and $\sum |\alpha_i|^2 = 1$

Example

$$|000\dots 000\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle$$

$$\frac{1}{\sqrt{2}} |000\rangle - \frac{1}{\sqrt{3}} |100\rangle + \frac{i}{\sqrt{6}} |111\rangle$$

Math background: Transpose, conjugate, adjoint and inverse matrices

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \cdots & \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \quad \overline{A} = \begin{pmatrix} a_{1,1}^* & \cdots & a_{1,n}^* \\ \cdots & \cdots & \cdots \\ a_{m,1}^* & \cdots & a_{m,n}^* \end{pmatrix}$$

$$A^T = \begin{pmatrix} a_{1,1} & \cdots & a_{m,1} \\ \cdots & \cdots & \cdots \\ a_{1,n} & \cdots & a_{m,n} \end{pmatrix} \quad A^\dagger = \overline{A^T} = \begin{pmatrix} a_{1,1}^* & \cdots & a_{m,1}^* \\ \cdots & \cdots & \cdots \\ a_{1,n}^* & \cdots & a_{m,n}^* \end{pmatrix}$$

$$A^{-1} : A^{-1}A = A^{-1}A = I \text{ if it exists}$$

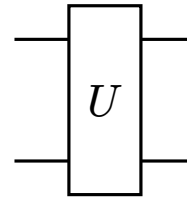
Evolution of quantum states

Postulate: A quantum state evolves according to the Schrödinger equation:

$$i\hbar \frac{\partial}{\partial t} |\psi\rangle = \hat{H} |\psi\rangle$$

Evolution of quantum states is described by **unitary operators**.

- Represented by a matrix
- $UU^\dagger = U^\dagger U = I$, i.e. $U^\dagger = U^{-1}$



Properties:

1. For every vector v : $\|Uv\| = \|v\|$
 $\Rightarrow$ For every valid quantum state $|\psi\rangle$, $U|\psi\rangle$ is also a valid quantum state
2. Reversible: no information loss

Example of quantum unitaries - X

Definition: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Unitary: $X^2 = I$ ($X^\dagger = X$)

Operational:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle$$

X is the NOT operation in the computational basis

$$X|+\rangle = X \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) = |+\rangle$$

$$X|-\rangle = X \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|-\rangle$$

$\{|+\rangle, |-\rangle\}$ are the ± 1 eigenvectors of X , so it is also called as the X -basis.

$$X = |+\rangle\langle+| - |-\rangle\langle-|$$

Example of quantum unitaries - Z

Definition: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Unitary: $Z^2 = I$ ($Z^\dagger = Z$)

Operational:

$$Z|0\rangle = |0\rangle \quad \text{and} \quad Z|1\rangle = -|1\rangle$$

$\{|0\rangle, |1\rangle\}$ are the ± 1 eigenvectors of Z , so so it is also called as the Z -basis.

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$Z|+\rangle = \frac{1}{\sqrt{2}}(Z|0\rangle + Z|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$

$$Z|-\rangle = \frac{1}{\sqrt{2}}(Z|0\rangle - Z|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

Z is the NOT operation in the Hadamard basis

Example of quantum unitaries - H

Definition: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Unitary: $H^2 = I$ ($H^\dagger = H$)

Operational:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \quad \text{and} \quad H|1\rangle = |-\rangle$$

$$H|+\rangle = |0\rangle \quad \text{and} \quad H|-\rangle = |1\rangle$$

H allows us to move from computational to Hadamard basis (and vice-versa)

Quizz

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. What is $X|\psi\rangle$, $Z|\psi\rangle$ and $H|\psi\rangle$?

$$X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \beta|0\rangle + \alpha|1\rangle$$

$$Z|\psi\rangle = Z(\alpha|0\rangle + \beta|1\rangle) = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$$

$$\begin{aligned} H|\psi\rangle &= H(\alpha|0\rangle + \beta|1\rangle) = \alpha H|0\rangle + \beta H|1\rangle = \alpha|+\rangle + \beta|-\rangle \\ &= \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle \end{aligned}$$

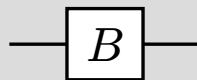
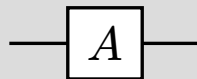
Remember that $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Composing unitaries

If $A \in \mathbb{C}^{n \otimes n}$ and $B \in \mathbb{C}^{n \otimes n}$ are unitary, then AB is also unitary.

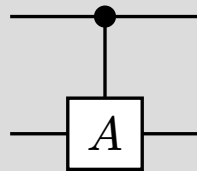


If $A \in \mathbb{C}^{n \otimes n}$ and $B \in \mathbb{C}^{m \otimes m}$ are unitary, then $A \otimes B$ is also unitary.



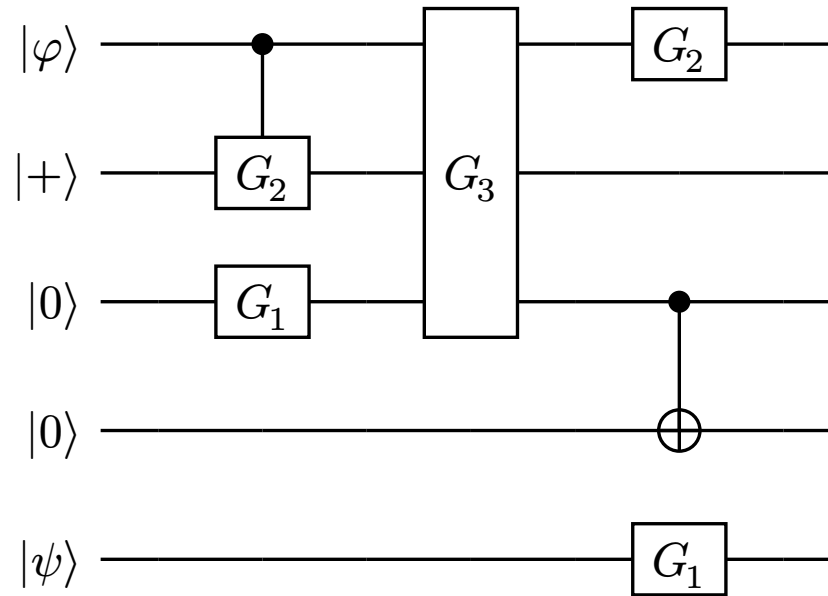
Let $A \in \mathbb{C}^{2^n \otimes 2^n}$. The unitary $cA \in \mathbb{C}^{2^{n+1} \otimes 2^{n+1}}$ is the unitary that:

$$cA \sum_{b \in \{0,1\}, y \in \{0,1\}^n} \alpha_{by} |b\rangle |y\rangle \mapsto \sum_{y \in \{0,1\}^n} \alpha_{0y} |0\rangle |y\rangle + \alpha_{1y} |1\rangle A|y\rangle$$



Quantum circuits

1. Fix a gateset $\mathcal{G} = \{G_1, G_2, \dots\}$ (usually on a constant number of qubits)
2. Fix the number of qubits
3. Compose gates from $\mathcal{G}$ on those qubits



$$(G_2 \otimes I \otimes c(X) \otimes G_1)(G_3 \otimes I_{45})(c(G_2) \otimes G_1 \otimes I_{45})|\varphi\rangle|+\rangle|00\rangle|\psi\rangle$$

$c(X)$ is also known as CNOT

Measuring quantum states - computational basis

Measure $|\psi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$ in the computational basis

- Output i with probability $|\alpha_i|^2$
- Quantum state collapses to $|i\rangle$

Example

- Measure $|0\rangle$, the outcome is 0 with probability 1 and state collapses to $|0\rangle$
- Measure $|1\rangle$, the outcome is 1 with probability 1 and state collapses to $|1\rangle$
- Measure $|+\rangle$
 - The outcome is 0 with probability $\frac{1}{2}$ and state collapses to $|0\rangle$
 - The outcome is 1 with probability $\frac{1}{2}$ and state collapses to $|1\rangle$
- Measure $|-\rangle$
 - The outcome is 0 with probability $\frac{1}{2}$ and state collapses to $|0\rangle$
 - The outcome is 1 with probability $\frac{1}{2}$ and state collapses to $|1\rangle$

Measuring quantum states - arbitrary basis

Measure $|\psi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$ in basis $\{|\varphi_i\rangle\}_{i \in \{0,1\}^n}$

- Output i with probability $|\langle\psi|\varphi_i\rangle|^2$
- Quantum state collapses to $|\varphi_i\rangle$

Notice that we can also write $|\psi\rangle = \sum_{i \in \{0,1\}^n} \beta_i |\varphi_i\rangle$, and $\beta_i = \langle\psi|\varphi_i\rangle$



Measure $|\psi\rangle = \sum_{i \in \{0,1\}^n} \beta_i |\varphi_i\rangle$ in basis $\{|\varphi_i\rangle\}_{i \in \{0,1\}^n}$

- Output i with probability $|\beta_i|^2$
- Quantum state collapses to $|\varphi_i\rangle$

Measuring quantum states - arbitrary basis

Let us consider measurements in the $\{|\varphi_0\rangle = |+\rangle, |\varphi_1\rangle = |-\rangle\}$ basis

Example

- Measure $|+\rangle$, the outcome is 0 with probability 1 and state collapses to $|+\rangle$
- Measure $|-\rangle$, the outcome is 1 with probability 1 and state collapses to $|-\rangle$
- Measure $|0\rangle$
 - The outcome is 0 with probability $\frac{1}{2}$ and state collapses to $|+\rangle$
 - The outcome is 1 with probability $\frac{1}{2}$ and state collapses to $|-\rangle$
- Measure $|1\rangle$
 - The outcome is 0 with probability $\frac{1}{2}$ and state collapses to $|+\rangle$
 - The outcome is 1 with probability $\frac{1}{2}$ and state collapses to $|-\rangle$

Partial measurement

Measure the first qubit of $|\psi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$ in the computational basis

- Output is b with probability $p_b = \sum_{j \in \{0,1\}^{n-1}} |\alpha_{bj}|^2$
- Quantum state collapses to $\frac{1}{\sqrt{p_b}} \sum_{j \in \{0,1\}^{n-1}} \alpha_{bj} |bj\rangle$

Exercise: Show that $\frac{1}{\sqrt{p_b}} \sum_{j \in \{0,1\}^{n-1}} \alpha_{bj} |bj\rangle$ is normalized.

Example Measure the first qubit of $\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$ in the computational basis.

- Output is 0 with probability $\frac{2}{3}$, post-measurement state is $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$
- Output is 1 with probability $\frac{1}{3}$, post-measurement state is $|10\rangle$

Remark: I described it with the first qubit, but if we had any other set of qubits, it would follow the same principle.

Projective measurements

Measure the state $|\psi\rangle$ according to the projectors $\Pi_1, \dots, \Pi_k$, s.t. $\sum_{i=1}^k \Pi_i = I$:

- Output is $i \in [k]$ with probability $|\Pi_i|\psi\rangle|^2$
- Quantum state collapses to $\frac{\Pi_i|\psi\rangle}{|\Pi_i|\psi\rangle|}$

Exercise: Show that if $\sum_{i=1}^k \Pi_i = I$, then $i \neq j \Rightarrow \Pi_i$ and Π_j are orthogonal, i.e., $\text{tr}(\Pi_i \Pi_j) = 0$.

Exercise: Show that all of the previous measurements that we discussed can be written as projective measurements.

Entanglement

Product states

A bipartite state $|\psi\rangle_{AB}$ is said to be a product state if there exists $|\psi_1\rangle_A$ and $|\psi_2\rangle_B$ such that $|\psi\rangle_{AB} = |\psi_1\rangle_A \otimes |\psi_2\rangle_B$

Theorem: Not all states are product.

Proof: Let us consider the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Suppose that $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\varphi_0\rangle|\varphi_1\rangle$, for some $|\varphi_b\rangle = \alpha_b|0\rangle + \beta_b|1\rangle$.

$$|\varphi_0\rangle|\varphi_1\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle)(\alpha_1|0\rangle + \beta_1|1\rangle) = \alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle$$

We have that

1. $\alpha_0\alpha_1 = \frac{1}{\sqrt{2}}$
2. $\alpha_0\beta_1 = 0$
3. $\beta_0\alpha_1 = 0$
4. $\beta_0\beta_1 = \frac{1}{\sqrt{2}}$

Item 2 implies that $\alpha_0 = 0$ or $\beta_1 = 0 \Rightarrow \alpha_0\alpha_1 = 0$, or $\beta_0\beta_1 = 0$. **Contradiction.**

Entangled states

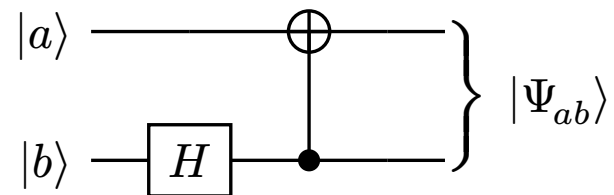
If a quantum state is not a product state, it is **entangled**.

Example $\text{GHZ}_n = \frac{1}{\sqrt{2}}(|0\dots 0\rangle + |1\dots 1\rangle)$

$$W_n = \frac{1}{\sqrt{n}}(|10\dots 0\rangle + |01\dots 0\rangle + \dots + |00\dots 1\rangle)$$

Bell basis

$$\left\{ \underbrace{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)}_{|\Psi_{00}\rangle/\text{EPR pair}}, \underbrace{\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)}_{|\Psi_{01}\rangle}, \underbrace{\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)}_{|\Psi_{10}\rangle}, \underbrace{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)}_{|\Psi_{11}\rangle} \right\}$$

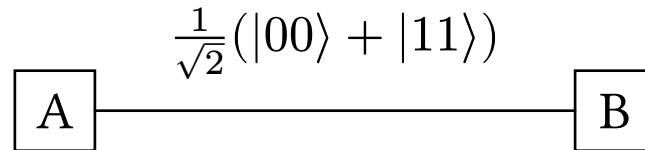


Exercise: Show that this circuit indeed create the Bell basis when the inputs are the computational basis.

Spooky action at a distance

Theorem: For every real basis $\{|\varphi_0\rangle, |\varphi_1\rangle\}$, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|\varphi_0\rangle|\varphi_0\rangle + |\varphi_1\rangle|\varphi_1\rangle)$

Proof: Exercise.



1. A and B share an EPR pair, and move very, very far apart
2. If A measures in some basis and has outcome b , and Bob measures in the same basis he also gets bit b

Full agreement. They are able to share a random bit without communication.

Communication faster than speed of light? **NO!**

To agree on a basis, there must be communication.

Source of quantum power/weirdness

1. Non-local games/Bell inequalities (Tuesday)
2. Quantum teleportation (today)
3. Super-dense coding (today)
4. ...

Communicating classical bits

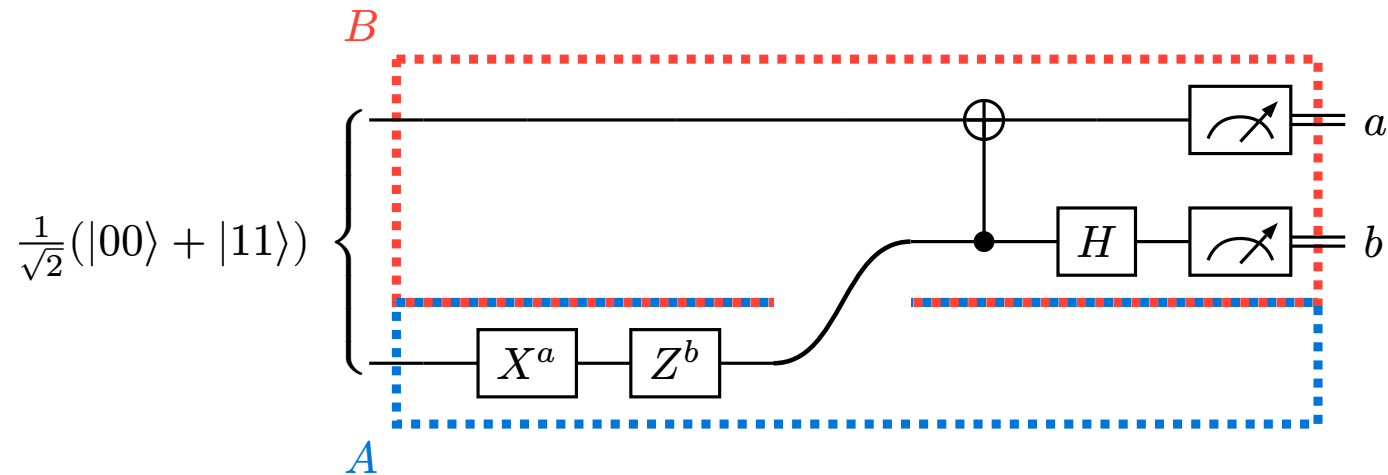


A wants to transmit two bits a, b to B.

Theorem. If communication is classical, A needs to send two bits to B. Even if they share previous resource that is independent of a, b , e.g. infinite random tape or even infinite quantum state.

Super-dense coding

What happens if A has quantum communication to B?



1. A and B share an EPR pair
2. A applies $X^a Z^b$ on her half
3. A sends her qubit to B
4. B measures in the Bell basis $\{|\Psi_{ab}\rangle\}$

Theorem: The output of B's measurements are a and b .

Proof: Exercise: Check that $|\Psi_{ab}\rangle = (Z^b X^a \otimes I)|\Psi_{00}\rangle$

Quantum teleportation

$$|\psi\rangle \in \mathbb{C}^2 \quad \boxed{A} \quad \boxed{B}$$

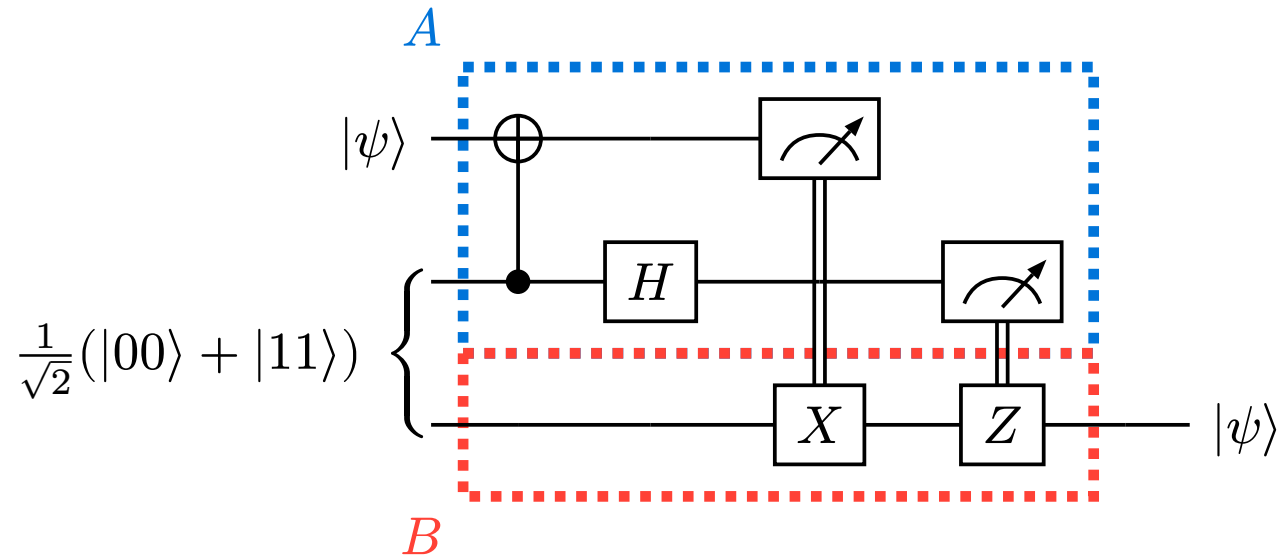
A wants to transmit a qubit $|\psi\rangle$ to B, but she can only transmits classical messages.

Difficulties:

- No cloning theorem (next class)
- Infinite amount of communication

Quantum teleportation

What happens if they can pre-share entanglement?



Theorem: The output of the previous circuit is $|\psi\rangle$.

Proof: Exercise

Mixed states

Mixed states

I kind of lied... what we have seen so far are not the general type of quantum states.

In particular:

- They don't model parts of entangled quantum states
What is the state that A has when she shares half of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?
- They don't model distributions of quantum states
 $|0\rangle$ w.p. $\frac{1}{2}$, $|1\rangle$ w.p. $\frac{1}{2}$

Pure states: what we have seen so far

Mixed states: probabilistic distribution over pure states

Density matrices

Mathematical representation of mixed states

- Density matrix of $|\psi\rangle$ is $|\psi\rangle\langle\psi|$
- Density matrix of a distribution $((p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), \dots, (p_k, |\psi_k\rangle))$ is

$$\rho = \sum_{i=1}^k p_i |\psi_i\rangle\langle\psi_i|$$

Properties of density matrices:

- Trace is 1 (The trace of a square matrix is $\sum_i a_{i,i}$)
- Positive semi-definitive (all its eigenvalues are non-negative)

Density matrices - examples

Example

- $|\Psi_{00}\rangle\langle\Psi_{00}| = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$

- Distribution $(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

- Distribution $(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)$

$$\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|+\rangle\langle +| = \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

- Distribution $(\frac{2}{3}, |+\rangle), (\frac{1}{3}, |0\rangle)$

$$\frac{2}{3}|+\rangle\langle +| + \frac{1}{3}|0\rangle\langle 0| = \frac{1}{3}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} + \frac{1}{3}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

Partial Trace

Bipartite quantum state $\rho_{AB} = \sum_{i,j,k,l} \rho_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ on $\mathcal{H}_A \otimes \mathcal{H}_B$.

The **partial trace** over system B gives the reduced state of system A :

$$\rho_A = \text{tr}_B(\rho_{AB}) = \sum_{i,j,k} \rho_{ijkk} |i\rangle\langle j|$$

Remark:

- $\text{tr}(\rho_A) = 1$.
- ρ_A contains all information accessible by measurements performed only on A .
- Information about correlations with B is generally lost.

Example

$$|\Psi_{00}\rangle\langle\Psi_{00}| = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

Trace out the second qubit:

$$\rho_A = \text{tr}_B(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, subsystem A is **maximally mixed**.

$$\rho_{AB} = \sum_{i,j,k,l} \rho_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|$$

$$\text{Trace out: } \rho_A = \text{tr}_B(\rho_{AB}) = \sum_{i,j,k} \rho_{ijkk} |i\rangle\langle j|$$

Evolution and measurements of mixed states

- Apply unitary U on a mixed state $\rho \mapsto U\rho U^\dagger$
- Measure the state ρ according to the projectors $\Pi_1, \dots, \Pi_k$, s.t. $\sum_{i=1}^k \Pi_i = I$:
 - Output is $i \in [k]$ with probability $\text{tr}(\Pi_i \rho)$
 - Quantum state collapses to $\frac{\Pi_i \rho \Pi_i}{\sqrt{\text{tr}(\Pi_i \rho)}}$

Exercise: Show that we have the same states as described before if ρ is a pure state.

Questions?

We will see next how to use these basic concepts to construct cryptographic primitives