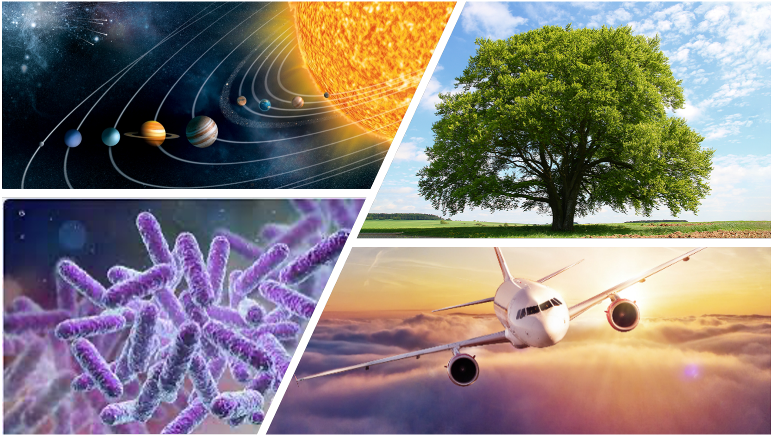
CS6846 – Quantum Algorithms and Cryptography

Basics of Quantum Information

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

The Model

The universe is complex, strange and fascinating. Full of diversity – bacteria to airplanes to trees to planets.



The Model

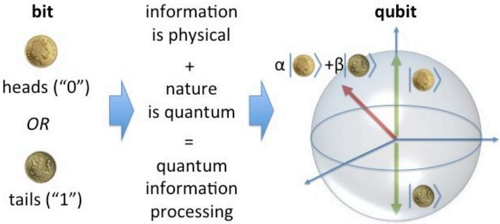
- Science wants to understand the universe by abstracting out the principles of observed phenomena in the simplest form.

The Model

- Science wants to understand the universe by abstracting out the principles of observed phenomena in the simplest form.
- Achieved by discovering models that help to understand and predict behaviour.

The Model

- Science wants to understand the universe by abstracting out the principles of observed phenomena in the simplest form.
- Achieved by discovering models that help to understand and predict behaviour.
- Information is physical and subject to quantum laws – we start with a clean mathematical model for quantum information.



Basic Formalism: Complex Numbers

- A complex number is a number of the form $a + bi$ for $a, b \in \mathbb{R}$, where i is the imaginary root of -1, i.e. $i = \sqrt{-1}$.
- Real and Imaginary parts:

$$z = a + ib$$

Real Part : a

Imaginary part : b.

- Polar Co-ordinates:

$$z = (|z| \cos\theta) + i(|z| \sin\theta) = |z| e^{i\theta}$$

$$|z| = \sqrt{a^2 + b^2}$$

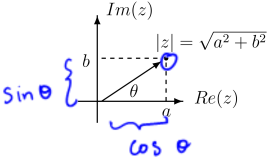


Figure: Geometric Representation of $z = a + bi$, image courtesy: OW lecture notes.

Basic Formalism: Complex Numbers

- The complex conjugate of a complex number z is denoted by z^* or $z^\dagger$.
- For $z = a + bi$, z^* is defined as $a - bi$. Note that $|z^*| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$.

Basic Formalism: Complex Numbers

- The complex conjugate of a complex number z is denoted by z^* or $z^\dagger$.
- For $z = a + bi$, z^* is defined as $a - bi$. Note that $|z^*| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$.
- Product of two complex numbers $z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$ is:

Basic Formalism: Complex Numbers

- The complex conjugate of a complex number z is denoted by z^* or $z^\dagger$.
- For $z = a + bi$, z^* is defined as $a - bi$. Note that $|z^*| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$.
- Product of two complex numbers $z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$ is:

$$(a_1 + b_1 i)(a_2 + b_2 i) = a_1 a_2 - b_1 b_2 + i(b_1 a_2 + a_1 b_2).$$

- The product of any complex number $z = a + bi$ with its complex conjugate $z^* = a - bi$ is

$$(a + ib)(a - ib) = a^2 - i^2 b^2 + iba - iba = a^2 + b^2 = |z|^2.$$

- A complex vector is an $m \times 1$ complex matrix. What is the conjugate transpose $A^\dagger$ of the following complex vector?

$$A = \begin{bmatrix} \alpha \\ \beta \\ \vdots \\ \eta \end{bmatrix}$$

Two vectors A and B are **orthonormal** if $A^\dagger B = 0$.

Basic Formalism: Complex Numbers

- A complex vector is an $m \times 1$ complex matrix. What is the conjugate transpose $A^\dagger$ of the following complex vector?

$$A = \begin{bmatrix} \alpha \\ \beta \\ \vdots \\ \eta \end{bmatrix} \qquad A^\dagger = [\alpha^* \ \beta^* \ \cdots \ \eta^*].$$

  Two vectors A and B are **orthonormal** if $A^\dagger B = 0$.

- For any $m \times n$ complex matrix M, the conjugate transpose of M denoted by $M^\dagger$ is the matrix obtained by first taking the transpose of matrix M and then replacing each entry in the resulting matrix by its complex conjugate.

Origins: Double Slit Experiment

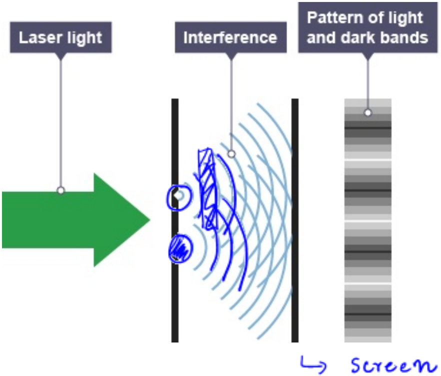


Figure: Double Slit Experiment, image courtesy Medium.com

A photon beam is passed through two slits – constructive and destructive interference is demonstrated, suggesting wave like behaviour.

Origins: Double Slit Experiment

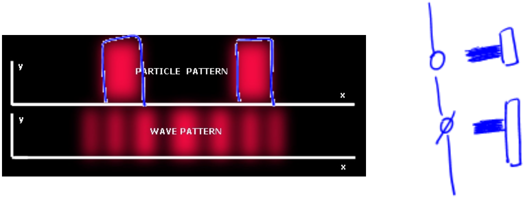


Figure: Double Slit Experiment, image courtesy Medium.com

When passed through one slit at a time, or observed using detectors in front of each slit, there is no interference pattern. Without observation, photon was in position of two states "top" and "bottom", going through both at same time. Quantum computing uses this "superposition".

Origins: Double Slit Experiment

- When passed through one slit at a time, or observed using detectors in front of each slit, light behaves as particle (i.e. no interference pattern). Observation "collapses" wave function of particle.

Origins: Double Slit Experiment

- When passed through one slit at a time, or observed using detectors in front of each slit, light behaves as particle (i.e. no interference pattern). Observation "collapses" wave function of particle.
- Without observation, photon was in position of two states "top" and "bottom", going through both at same time.

Origins: Double Slit Experiment

- When passed through one slit at a time, or observed using detectors in front of each slit, light behaves as particle (i.e. no interference pattern). Observation "collapses" wave function of particle.
- Without observation, photon was in position of two states "top" and "bottom", going through both at same time.
- Quantum computing seeks to use this "superposition" to generate "parallelism".

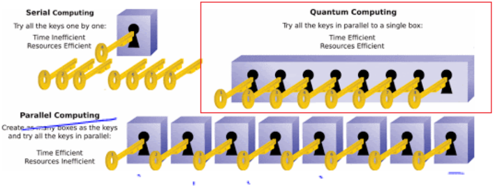


Figure: Quantum Parallelism, image courtesy: Medium.com

What's the Catch?

- Say that each register simultaneously stores both bits, 0 and 1.

What's the Catch?

- Say that each register simultaneously stores both bits, 0 and 1.
- How many bits do n registers store?

What's the Catch?

- Say that each register simultaneously stores both bits, 0 and 1.
- How many bits do n registers store?
- Can we run exponentially many threads of computation in parallel? Then, can we solve NP-complete problems?

What's the Catch?

- Say that each register simultaneously stores both bits, 0 and 1.
- How many bits do n registers store?
- Can we run exponentially many threads of computation in parallel? Then, can we solve NP-complete problems?
- Possibly can simultaneously try all possible solutions, but must quickly concentrate probability on "correct" solution!

Figure: Concentrate Probability, image courtesy: Physics World

Defining a Qubit

- Ket and Bra notation

$|\cdot\rangle$

Ket is a d-dimensional column vector $\in \mathbb{C}^d$.

Bra $\langle\cdot|$ is a d-dimensional row vector which is the complex conjugate of corres. ket.

$$|v_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \qquad |v_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} \qquad a_i, b_i \in \mathbb{C}.$$

- Inner Product

$$\langle v_1 | v_2 \rangle = \sum_{i=1}^{d} a_i^* b_i .$$

Defining a Qubit

- Start by writing classical bits as vectors $|0\rangle$ and $|1\rangle$.

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

- A qubit can be in a 'superposition' state

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where $|\alpha|^2 + |\beta|^2 = 1$, and $\alpha, \beta \in \mathbb{C}^2$ are called the amplitudes on each of the basis states $|0\rangle$ and $|1\rangle$.

Defining a Qubit

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

Measure $|\psi\rangle$:

- Probability of finding $|\Psi\rangle$ in either state $|0\rangle$ or $|1\rangle$ is:

$$|\alpha|^2 \text{ or } |\beta|^2$$
$$\downarrow \qquad \downarrow$$
$$|0\rangle \qquad |1\rangle.$$

- Every two-state quantum system can be written as a linear combination of the basis states.

eg: $|\psi\rangle = 0.8|0\rangle + 0.6|1\rangle$

Can write $|\psi\rangle$ as $\begin{bmatrix} 0.8 \\ 0.6 \end{bmatrix}$

Examples of qubits.

1. $\cos\theta|0\rangle + \sin\theta|1\rangle$

$$\cos^2\theta + \sin^2\theta = 1.$$

2. $0.8|0\rangle - 0.6|1\rangle$

$$|0.8|^2 + |-0.6|^2 = 1.$$

Amplitude can be complex.

$$|\psi\rangle = i|0\rangle + 0|1\rangle$$

or $\frac{1}{\sqrt{2}}\left(i|0\rangle + 1|1\rangle\right).$

$$\left|\frac{i}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1.$$

Useful Bases

Any quantum state can be expressed in terms of an **orthonormal basis**.

Standard Basis:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Useful Bases

Any quantum state can be expressed in terms of an **orthonormal basis**.

Standard Basis:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Hadamard Basis:

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

Useful Bases

Any quantum state can be expressed in terms of an **orthonormal basis**.

Standard Basis:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

Hadamard Basis:

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

Exercise: represent $|0\rangle$ and $|1\rangle$ in terms of the Hadamard basis.

Multiple Qubits

Say we have two qubits, A and B – how can we write these?
Construct a basis: perform a mapping from strings to orthonormal vectors.

$$|00\rangle \to \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |01\rangle \to \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle \to \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle \to \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

eg: $|\Psi_{AB}\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

When considering n qubits, consider vector space $\mathbb{C}^{2^n}$ where each basis vector is labelled by an n bit string. A quantum state of n qubits can be written as:

$$|\Psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle, \quad \text{where} \quad \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1.$$

$\sum_{x \in \{0,1\}^2} |\frac{1}{2}|^2 = 4\left(\frac{1}{2}\right)^2 = 1.$

Multiple Qubits

Example EPR pair:

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

Later, we will show that this state is entangled.

Multiple Qubits

Example EPR pair:

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

Later, we will show that this state is entangled.

How to combine qubits: Given two arbitrary qubits $|\psi_A\rangle = \begin{bmatrix}\alpha_A \\ \beta_A\end{bmatrix}$ and $|\phi_B\rangle = \begin{bmatrix}\alpha_B \\ \beta_B\end{bmatrix}$, how to express their combined state?

Multiple Qubits

Example EPR pair:

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

Later, we will show that this state is entangled.

How to combine qubits: Given two arbitrary qubits $|\psi_A\rangle = \begin{bmatrix}\alpha_A \\ \beta_A\end{bmatrix}$ and $|\phi_B\rangle = \begin{bmatrix}\alpha_B \\ \beta_B\end{bmatrix}$, how to express their combined state?

Tensor Product:

$$|\psi_A\rangle \otimes |\phi_B\rangle = \begin{pmatrix}\alpha_A \\ \beta_A\end{pmatrix} \otimes \begin{pmatrix}\alpha_B \\ \beta_B\end{pmatrix}$$

$$= \begin{pmatrix}\alpha_A \begin{pmatrix}\alpha_B \\ \beta_B\end{pmatrix} \\ \beta_A \begin{pmatrix}\alpha_B \\ \beta_B\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_A\alpha_B \\ \alpha_A\beta_B \\ \beta_A\alpha_B \\ \beta_A\beta_B\end{pmatrix}.$$

Notation.

$|\psi_A\rangle \otimes |\phi_B\rangle$

$|\psi_A\rangle|\phi_B\rangle$ or $|\psi_A\phi_B\rangle$.

Examples

- Establish that the tensor product is distributive, associative but not commutative.

Examples

- Establish that the tensor product is distributive, associative but not commutative.
- Application: generate true randomness!

Examples

- Establish that the tensor product is distributive, associative but not commutative.
- Application: generate true randomness!

$\langle 0| = (1\ 0)$

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

Prepare Hadamard state

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

$\langle 0|1\rangle = (1\ 0)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0.$

Measure in the standard basis. $|0\rangle$, $|1\rangle$

$$\Pr(|0\rangle) = |\langle 0|+\rangle|^2 = \Big|\underbrace{\langle 0|0\rangle}_{1}\frac{1}{\sqrt{2}} + \langle 0|1\rangle\frac{1}{\sqrt{2}}\Big|^2 = \frac{1}{2}.$$

- If we want to measure $|\psi\rangle$ in orthonormal basis $\{|b_j\rangle\}_j$, the probability of observing the outcome $|b_j\rangle$ is $|\langle b_j|\psi\rangle|^2$.

Measurement

- Measurement of a quantum system collapses the wave function and results in the state being found in one of the bases states.
  In a circuit diagram, a measurement is depicted as

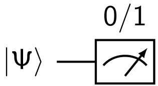


Figure: A measurement of $|\Psi\rangle$ will yield either $|0\rangle$ ("0") or $|1\rangle$ ("1").

- A measurement will result in a basis state with probability according to the square of the 2-norm of the associated amplitude. But once a measurement collapses a wave function, any subsequent measurement will obtain the same result with probability 1.

Acknowledgements

- Slides for the course are based on material in courses offered at UIUC and Princeton (see webpage). & CMU.
- All images – courtesy Google Images.
- This applies for all slides throughout the course.

Thanks!