Introduction to Quantum Algorithms

Krishnamoorthy Dinesh (IIT Palakkad)

Workshop on Quantum Algorithms and Cryptography
Pre-conference workshop, FSTTCS 2025, BITS Goa

December 14, 2025

Qubit (Quantum Bit)

States - $|0\rangle$, $|1\rangle$ ("Ket 0", "Ket 1")

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \alpha, \beta \in \mathbb{C} \qquad \psi \text{ ("Psi")}$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

- Examples of 1-qubit: $|\psi_1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$, $|\psi_2\rangle = \frac{1}{\sqrt{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle$.

- Non-example: $\frac{1}{2}\,|0\rangle + \frac{1}{2}\,|1\rangle$. (Why ?)

Qubits and Quantum Gates

What is a k-qubit ?

2-qubit

- Basis states are $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
- **Form**: $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad a, b, c, d \in \mathbb{C}$ and $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.
- Example: $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$ (Valid ?)

k-qubit

- 2^k basis states: $\overbrace{0\ldots0}^{k}, \overbrace{0\ldots0}^{k-1}1, \ldots, \overbrace{1\ldots1}^{k}$.
- **Form**: $\sum_{x\in\{0,1\}^k} a_x|x\rangle \qquad$ every $a_k \in \mathbb{C}$ $\sum_x |a_x|^2 = 1$.
- Each state viewed as a vector in $\mathbb{C}^{2^k}$.

- Measuring a qubit causes $\rightarrow$ "collapse" to a basis state.
- Which basis state ? Dictated by the amplitude of the state.

Example: Suppose $|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$.

Measuring $|\psi\rangle$ gives

$$\begin{cases} |00\rangle & \text{with probability } \left|\frac{1}{2}\right|^2 \\ |01\rangle & \text{with probability } \left|\frac{1}{2}\right|^2 \\ |10\rangle & \text{with probability } \left|\frac{1}{2}\right|^2 \\ |11\rangle & \text{with probability } \left|-\frac{1}{2}\right|^2 \end{cases}$$

- Measuring a state destroys it ! (not reversible).
- All measurements in **standard basis**.

> Take away: Measure a k-qubit $\sum_x a_x |x\rangle$,
> ... Gets $|x\rangle$ with probability $|a_x|^2$.

Unitary matrix U

U is a matrix over $\mathbb{C}$ with $UU^* = U^*U = I$

Easy to remember: "Inverse is (conjugate) transpose".

- Example:

$$H = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \text{(Why ?)}$$

- Non-example:

$$\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

Why Unitary ?

Quantum physics: all quantum operations must be

1. linear, and
2. maps qubits to qubits (length preserving)

Linear algebra: Maps that are linear and length preserving is *exactly* Unitary.

- Unitary maps are invertible. Inverse of U is U^*.

Examples

Qubits and Quantum Gates

More examples of quantum gates - 1

Qubits and Quantum Gates

Putting everything together: an example

CHSH Game

Setup

- Does quantum gives us any advantage over classical ?
- CHSH = Clauser, Horne, Shimony and Holt (1970s)

Game setup

- **Input**: Alice gets $x \in \{0, 1\}$ alone.
  Bob gets $y \in \{0, 1\}$ alone.
- **Output**: Alice output $a \in \{0, 1\}$ (depending on x).
  Bob must output $b \in \{0, 1\}$ (depending on y) such that ...

$$x \wedge y = a(x) \oplus b(y)$$

$$\begin{array}{ccc} a(x) & & b(y) \\ \uparrow & & \uparrow \\ \text{Alice} & || & \text{Bob} \\ \uparrow & & \uparrow \\ x & & y \end{array}$$

- **Obs**: Cannot be correct always !
- **Goal**: Find a strategy s.t. equality holds for as many inputs as possible.

.

CHSH Game

Classical strategies and its limitations

Strategy 1: $a(x) = 1,\ b(y) = y$

x	y	$a(x)$	$b(y)$	$x \wedge y$	$a(x) \oplus b(y)$
0	0	1	0	0	1
0	1	1	1	0	0
1	0	1	0	0	1
1	1	1	1	1	0

Success $= 1/4 = 25\% = 0.25$

Strategy 2: $a(x) = \neg x,\ b(y) = y$

x	y	$a(x)$	$b(y)$	$x \wedge y$	$a(x) \oplus b(y)$
0	0	1	0	0	1
0	1	1	1	0	0
1	0	0	0	0	0
1	1	0	1	1	1

Success $= 3/4 = 75\% = 0.75$

Take away: No classical strategy succeed with probability more than 0.75
(Why ? Just enumerate and check !)

Quantum strategy Use EPR pair !

Description of A_x, B_y

x	A_x
0	I
1	$R_{\pi/4}$

y	B_y
0	$R_{\pi/8}$
1	$R_{-\pi/8}$

Analysis

- Suppose $x = 0, \; y = 0$.
- When do we succeed ? Succeed if outcome is $|0\rangle_A |0\rangle_B$ or $|1\rangle_A |1\rangle_B$.
- What is the probability ? Sum of probabilities of measuring

Before: $\frac{1}{\sqrt{2}} |0\rangle_A |0\rangle_B + \frac{1}{\sqrt{2}} |1\rangle_A |1\rangle_B$

After: $\frac{1}{\sqrt{2}} |0\rangle_A (R_{\pi/8} |0\rangle_B) + \frac{1}{\sqrt{2}} |1\rangle_A (R_{\pi/8} |1\rangle_B)$

- Simplify:

$$\begin{aligned} &\frac{1}{\sqrt{2}} \cos(\pi/8) |0\rangle_A |0\rangle_B + \frac{1}{\sqrt{2}} \sin(\pi/8) |0\rangle_A |1\rangle_B \\ -&\frac{1}{\sqrt{2}} \sin(\pi/8) |1\rangle_A |0\rangle_B + \frac{1}{\sqrt{2}} \cos(\pi/8) |1\rangle_A |1\rangle_B \end{aligned}$$

- Succees probability - $\frac{1}{2}\cos^2(\pi/8) + \frac{1}{2}\cos^2(\pi/8) = \cos^2(\pi/8)$.

CHSH Game

Quantum strategy can succeed with probability 0.853

- Similar analysis for other cases ($x = 0, y = 1$; $x = 1, y = 0$; $x = 1, y = 1$): success probability is $\cos^2(\pi/8) \approx 0.853$.
- Stategy succeeds with probability $0.853 > 0.75$ (for all inputs).

> Take away: Quantum strategy can succeed with probability 0.853

- **Surprise !** No quantum strategy can do better than $\cos^2(\pi/8)$

Quantum Queries

Exploiting states in superposition

- Toffoli gate can compute $\wedge$ and $\neg$.

- Any Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be computed using $\wedge, \neg$.
- Compute any Boolean function $\to$ Use Toffoli gates.
- $U_f : \ket{x}\ket{b} \mapsto \ket{x}\ket{b \oplus f(x)}$
- Give an address, get value at the address.

U_f

Quantum Queries

Computing AND of 3 bits using Toffoli

Quantum Query Model

Significance

$$U_f\left(\sum_x a_x |x\rangle |b\rangle\right) = \sum_x a_x |x\rangle |b \oplus f(x)\rangle$$

Benfit: Ability to evaluate a Boolean function in superposition of inputs.

Query Model

We assume that

1. **Given an f, U_f is available**
2. **Each application of U_f ("quantum query") is unit cost**
3. **Only the number of times U_f is applied matters**

- Why (1) ? f is usually a verification and is easy.
- Why (2), (3) ? Reads to input (in superposition) is a resource
- Called as the **quantum query model**. U_f is often called as oracle.

Let f be an n-bit Boolean function.

- Given a U_f, consider the following circuit
- What is its behaviour ? Recall $U_f : \ket{x}\ket{b} \mapsto \ket{x}\ket{b \oplus f(x)}$

$$U_f\left(\ket{x} \otimes \frac{1}{\sqrt{2}}(\ket{0} - \ket{1})\right) = \ket{x} \otimes \left(\frac{1}{\sqrt{2}}\ket{0 \oplus f(x)} - \frac{1}{\sqrt{2}}\ket{1 \oplus f(x)}\right)$$

Quantum Query Model

Phased Oracle

$$U_f\left(|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}|1 \oplus f(x)\rangle\right)$$

- $f(x) = 0 \to |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = |x\rangle|-\rangle.$
- $f(x) = 1 \to |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle\right) = -|x\rangle|-\rangle.$

Take away: $U_f(|x\rangle|-\rangle) = (-1)^{f(x)}|x\rangle|-\rangle$

- Ancilla dropped. This gives a **phased oracle** (value appears in phase).
- $U_f^{\pm}$: $|x\rangle \mapsto (-1)^{f(x)}|x\rangle.$

Given an f, from now on assume, U_f and $U_f^{\pm}$ are available.

Summary so far

- Saw what is ...
  - a qubit, k-qubit (states in superposition)
  - a quantum gates/operators (unitary)
  - a measurement
- CHSH games – quantum beats classical !
- Perform operation in superposition: U_f – oracle for a Boolean function f.
- Quantum query model
- $U_f^{\pm}$ – phased oracle.

Plan for the rest of the talk

Understand couple of quantum algorithms and how they work

Compute parity of two bits

Warm up

- **Given**: two bits a_0, a_1 via an oracle U_a.
- **Task**: compute $a_0 \oplus a_1$.

What is U_a ?

- $U_a |0\rangle |0\rangle = |0\rangle |a_0\rangle$
- $U_a |1\rangle |0\rangle = |1\rangle |a_1\rangle$

- **Issue**: Need to use U_a twice (Two queries).
- Any classical algorithm must read twice ! (Why ?)

Question: Is it possible to use **only once** and correctly compute $a_0 \oplus a_1$?

- Will use $U_a^{\pm}$: phased U_a
- Consider the following circuit:

Recall $U_a^{\pm}$.

- $U_a^{\pm}|0\rangle = (-1)^{a_0}|0\rangle$
- $U_a^{\pm}|1\rangle = (-1)^{a_1}|1\rangle$

State before measurement:

$$H\left(\frac{(-1)^{a_0}}{\sqrt{2}}|0\rangle + \frac{(-1)^{a_1}}{\sqrt{2}}|1\rangle\right)$$

Quantum algorithm to compute parity of two bits

One query quantum algorithm

State before measurement:

$$H\left(\frac{(-1)^{a_0}}{\sqrt{2}}|0\rangle + \frac{(-1)^{a_1}}{\sqrt{2}}|1\rangle\right) = \frac{(-1)^{a_0}}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \frac{(-1)^{a_1}}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\left(\frac{(-1)^{a_0} + (-1)^{a_1}}{2}\right)|0\rangle + \left(\frac{(-1)^{a_0} - (-1)^{a_1}}{2}\right)|1\rangle$$

- $a_0 = a_1 \implies$ Output $\pm|0\rangle$. Measure, always gets $|0\rangle$
- $a_0 \neq a_1 \implies$ Output $\pm|1\rangle$. Measure, always gets $|1\rangle$

Take away: Parity of 2 bits can be computed with 1 oracle query.

- Argument generalizes. Parity of n bits can be computed in $n/2$ queries.
- Want to be always correct? Then, $n/2$ queries necessary !

Deutsch's Problem

Statement

- Consider a function $f : \{0,1\} \to \{0,1\}$.
- Four possible Truth tables: $\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.
- Either constant or balanced.

Deutsch's Problem

Let $f : \{0,1\} \to \{0,1\}$. Is $f(0) = f(1)$?

- Classically: two queries are sufficient and necessary (Why ?).
- Can we do with only one query ? Classically: correct only half of time.
- Solution: Suffices to compute $f(0) \oplus f(1)$!
- Doable in 1 quantum query to $U_f^{\pm}$ (Warm up).

Final state value:

$$\left(\frac{(-1)^{f(0)} + (-1)^{f(1)}}{2}\right)|0\rangle + \left(\frac{(-1)^{f(0)} - (-1)^{f(1)}}{2}\right)|1\rangle$$

- $f(0) = f(1) \implies$ Output $\pm|0\rangle$. Measure, always gets $|0\rangle$
- $f(0) \neq f(1) \implies$ Output $\pm|1\rangle$. Measure, always gets $|1\rangle$

Deutsch-Josza problem

Given a function $f\colon \{0,1\}^n \to \{0,1\}$ with the **promise** that either

1. f is constant, or
2. f is always balanced (half zeros, half ones).

Example: $n = 3$

$\begin{bmatrix} 0\\0\\0\\0\\0\\0\\0\\0 \end{bmatrix}$ – "Constant" $\begin{bmatrix} 1\\0\\1\\0\\1\\0\\1\\0 \end{bmatrix}$ – "Balanced" $\begin{bmatrix} 1\\1\\1\\0\\1\\1\\1\\0 \end{bmatrix}$ – Output ?

Deutsch-Josza problem

Classical and Quantum solutions

- Generalization of Deutsch's problem.
- Classical solution ($n = 3$): Do all 8 lookups. Can we do better ?
- 5 lookups suffices. Can we do in 4 ?

Take away: There is a deterministic solution making $2^{n-1} + 1$ queries. (Why ?)
Also, this is necessary (Why ?)

Surprise !

Deutsch-Josza problem can be solved with only **one** quantum query.

Algorithm:

Walsh-Hadmard Transform

- $H^{\otimes n}|0^n\rangle$ produces a state where all n bit strings are in equal superposition.
- $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- $H \otimes H|00\rangle = H|0\rangle \otimes H|0\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
- $\overbrace{H \otimes \ldots \otimes H}^{n}|0\ldots 0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x \in \{0,1\}^n}|x\rangle$.

Deutsch-Josza problem

Sketch of how and why it works

Why it works ?

- Suppose $|\psi\rangle$ is final state before measurement
- f constant$\rightarrow \pm|0\dots0\rangle$ in $|\psi\rangle$. Will *always* give $|0\dots0\rangle$ on measure.
- f is balanced $\rightarrow 0\,|0\dots0\rangle$ in $|\psi\rangle$. Will *never* give $|0\dots0\rangle$.
- Doable in 1 quantum query to $U_f^{\pm}$. Makes no mistakes !

How it works ? Understand what is $|\psi\rangle$!

$$|\psi\rangle = H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\right)$$

1. **HW**: For $x \in \{0,1\}^n$, Show that $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$
2. Use this to understand $|\psi\rangle$ and amplitude of $|0\dots0\rangle$.

Summary