# Quantum Computing, an Introduction with Grover's Search

Yan-Tong Lin Advisor: Ming-Hsuan Kang

Department of Computer Science, National Chiao Tung University, Taiwan

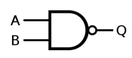
## Introduction

Quantum computation differs from its classical counterpart in a fundamental way. With proper algorithm design, it is known that exponential speedups can be acquired in certain problems. With the advance of quantum hardware technology, the need for efficient quantum algorithms is rising.

In this poster, we aim to introduce some fundamental concepts in quantum computing with the quantum circuit model and some examples. We start by walking through circuit model for classical computation. Then the mathematical formulation of quantum mechanics related to quantum computing is explained, which is used to present the quantum circuit model. Followed by an example showing the power of quantum parallelism — Deutsch-Jozsa Algorithm. Finally, Grover's search algorithm is introduced to show a quadratic speedup on unstructured search problems.

## Classical Circuit Model

- Bits are used to store information
  - e.g. **0001** as **1**, **0101** as **5**
- Gates are used to manipulate them
  - e.g. ***NAND*** gate
  - one can show that ***NAND*** can achieve universal computation
- We model physical phenomenon to do these




Q = A NAND B

Truth Table

| Input A | Input B | Output Q |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Figure: NAND gate and its truth table

## Postulates of Quantum Mechanics

In the past decades, physicists discover that Nature is "quantum".

- States of Systems are Unit Vectors in Hilbert Spaces
- Evolutions are linear transforms on the Hilbert space which map states to states.
- Measurements are Collections of Operators
- States of a Compositional System are Tensor Products of States of Component Systems

## Qubit

- States of Systems are Unit Vectors in Hilbert Spaces
- qubit: $|\mathbf{0}\rangle, |\mathbf{1}\rangle$
- superpostion: $\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle, |\alpha|^2 + |\beta|^2 = \mathbf{1}$

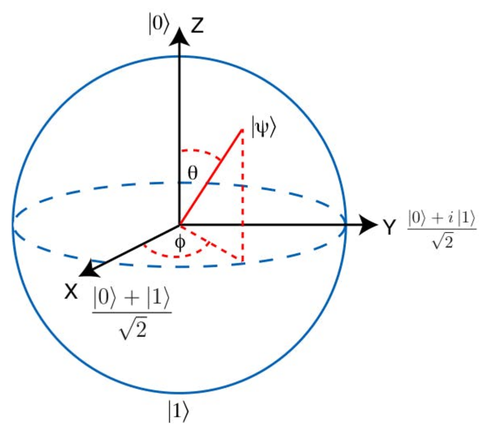



Figure: Bloch Sphere: $|\psi\rangle = \boldsymbol{e}^{i\delta}(\cos\frac{\theta}{2}|\mathbf{0}\rangle + \boldsymbol{e}^{i\phi}\sin\frac{\theta}{2}|\mathbf{1}\rangle)$

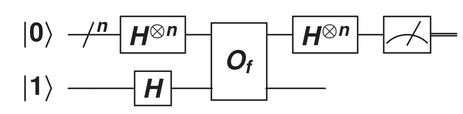
## Quantum Gates

- Evolutions are linear transforms on the Hilbert space which map states to states.
- Norm-Preserving + Linear $\Longrightarrow$ Unitary
- Functions on one qubit: Members of $\boldsymbol{SU}(\mathbf{2}) \cong \boldsymbol{SO}(\mathbf{3})$
- Like in classical computation, it can be shown that there exists finite universal gate sets.

## Deutsch-Jozsa Algorithm

$\boldsymbol{f} : \{\mathbf{0},\mathbf{1}\}^n \to \{\mathbf{0},\mathbf{1}\}$ is either balanced or constant. Given $\boldsymbol{O_f}(|\boldsymbol{x},\boldsymbol{y}\rangle) = |\boldsymbol{x},\boldsymbol{y}\oplus\boldsymbol{f}(\boldsymbol{x})\rangle$ as black boxes, judge if $\boldsymbol{f}$ is constant.

- It requires $\boldsymbol{O}(\mathbf{2}^n)$ queries of $\boldsymbol{f}$ for a classical circuit to judge
- quantum: $\boldsymbol{O}(\mathbf{1})$ query of $\boldsymbol{O_f}$




$$|\psi_0\rangle = |\mathbf{0}\rangle^{\otimes n}|\mathbf{1}\rangle$$

$$|\psi_1\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}^{n+1}}}\sum_{\boldsymbol{x}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}|\boldsymbol{x}\rangle\left(|\mathbf{0}\rangle - |\mathbf{1}\rangle\right)$$

$$|\psi_2\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}^{n+1}}}\sum_{\boldsymbol{x}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}|\boldsymbol{x}\rangle(|\boldsymbol{f}(\boldsymbol{x})\rangle - |\mathbf{1}\oplus\boldsymbol{f}(\boldsymbol{x})\rangle)$$

$$= \frac{\mathbf{1}}{\sqrt{\mathbf{2}^{n+1}}}\sum_{\boldsymbol{x}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}(-\mathbf{1})^{\boldsymbol{f}(\boldsymbol{x})}|\boldsymbol{x}\rangle(|\mathbf{0}\rangle - |\mathbf{1}\rangle)$$

$$|\psi_3\rangle = \frac{\mathbf{1}}{\mathbf{2}^n}\sum_{\boldsymbol{x}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}(-\mathbf{1})^{\boldsymbol{f}(\boldsymbol{x})}\left[\sum_{\boldsymbol{y}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}(-\mathbf{1})^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{y}\rangle\right]$$

$$= \frac{\mathbf{1}}{\mathbf{2}^n}\sum_{\boldsymbol{y}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}\left[\sum_{\boldsymbol{x}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}(-\mathbf{1})^{\boldsymbol{f}(\boldsymbol{x})}(-\mathbf{1})^{\boldsymbol{x}\cdot\boldsymbol{y}}\right]|\boldsymbol{y}\rangle$$

Now consider $|\boldsymbol{y}\rangle = |\mathbf{0}\rangle$

$$\frac{\mathbf{1}}{\mathbf{2}^n}\sum_{\boldsymbol{x}=\mathbf{0}}^{\mathbf{2}^n-\mathbf{1}}(-\mathbf{1})^{\boldsymbol{f}(\boldsymbol{x})}(-\mathbf{1})^{\boldsymbol{x}\cdot\mathbf{0}}|\mathbf{0}\rangle$$

We get the first register measures $|\mathbf{0}\rangle^{\otimes n} \iff \boldsymbol{f}$ is constant

## Grover's Search

Given a set $\boldsymbol{X}$ of $\boldsymbol{N}$ items and a function $\boldsymbol{f} : \boldsymbol{X} \to \{\mathbf{0},\mathbf{1}\}$,
suppose there are $\boldsymbol{M} = \epsilon\boldsymbol{N}$ out of $\boldsymbol{N}$ items satisfy $\boldsymbol{f}(\boldsymbol{x}) = \mathbf{1}$.
Find an instance $\boldsymbol{x} \in \boldsymbol{S}$ such that $\boldsymbol{f}(\boldsymbol{x}) = \mathbf{1}$.

- For classical algorithms, $\boldsymbol{O}(\boldsymbol{N})$-time is required to get an instance with high probability.
- For quantum algorithms, assume an oracle $\boldsymbol{U_\omega}$ is given such that

$$\boldsymbol{U_\omega}|\boldsymbol{x}\rangle = (-\mathbf{1})^{\boldsymbol{f}(\boldsymbol{x})}|\boldsymbol{x}\rangle.$$

With Grover's Search, $\boldsymbol{O}(\sqrt{\boldsymbol{N}})$-time is suffice.

Represent uniform state vector by l.c. of uniform "good" and uniform "bad" vectors.

$|\boldsymbol{s}\rangle = \sqrt{\frac{1}{N}}\sum_{\boldsymbol{x}}|\boldsymbol{x}\rangle$

$|\omega\rangle = \sqrt{\frac{M}{N}}\sum_{\boldsymbol{x}\in\boldsymbol{f}^{-1}(1)}|\boldsymbol{x}\rangle$

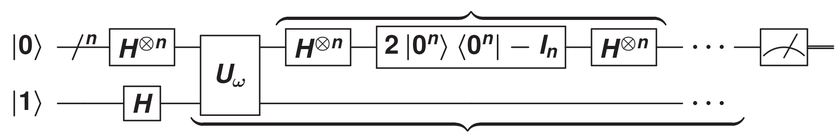
$|\boldsymbol{s}'\rangle = \sqrt{\frac{N-M}{N}}\sum_{\boldsymbol{x}\notin\boldsymbol{f}^{-1}(1)}|\boldsymbol{x}\rangle$

then $|\boldsymbol{s}\rangle = \sin\frac{\theta}{2}|\omega\rangle + \cos\frac{\theta}{2}|\boldsymbol{s}'\rangle$ where $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$

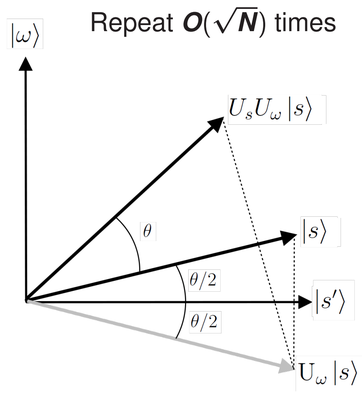
$$\boldsymbol{U_\omega} = \boldsymbol{I} - \mathbf{2}|\omega\rangle\langle\omega|$$

$$\boldsymbol{U_s} = \mathbf{2}\,|\boldsymbol{s}\rangle\,\langle\boldsymbol{s}| - \boldsymbol{I}$$

Grover diffusion operator $\boldsymbol{U_s}$




Repeat $\boldsymbol{O}(\sqrt{\boldsymbol{N}})$ times




We want to stop when the state vector passes close to $|\omega\rangle$. $\boldsymbol{r} = \#\text{round} \approx \pi\sqrt{\boldsymbol{N}}/\mathbf{4}$ is the first $\boldsymbol{r}$ we can get a high probability.