



上海市高可信计算重点实验室  
Shanghai Key Laboratory of Trustworthy Computing

# Introduction to Quantum Computing

Yuxin Deng

`yxdeng@sei.ecnu.edu.cn`

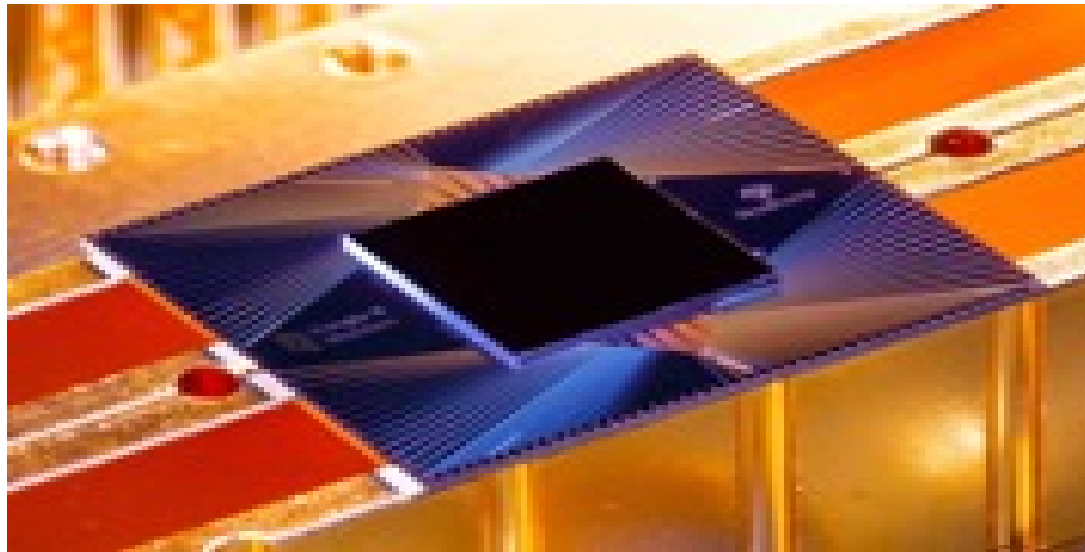
*East China Normal University*



# State of the art

## Quantum processors

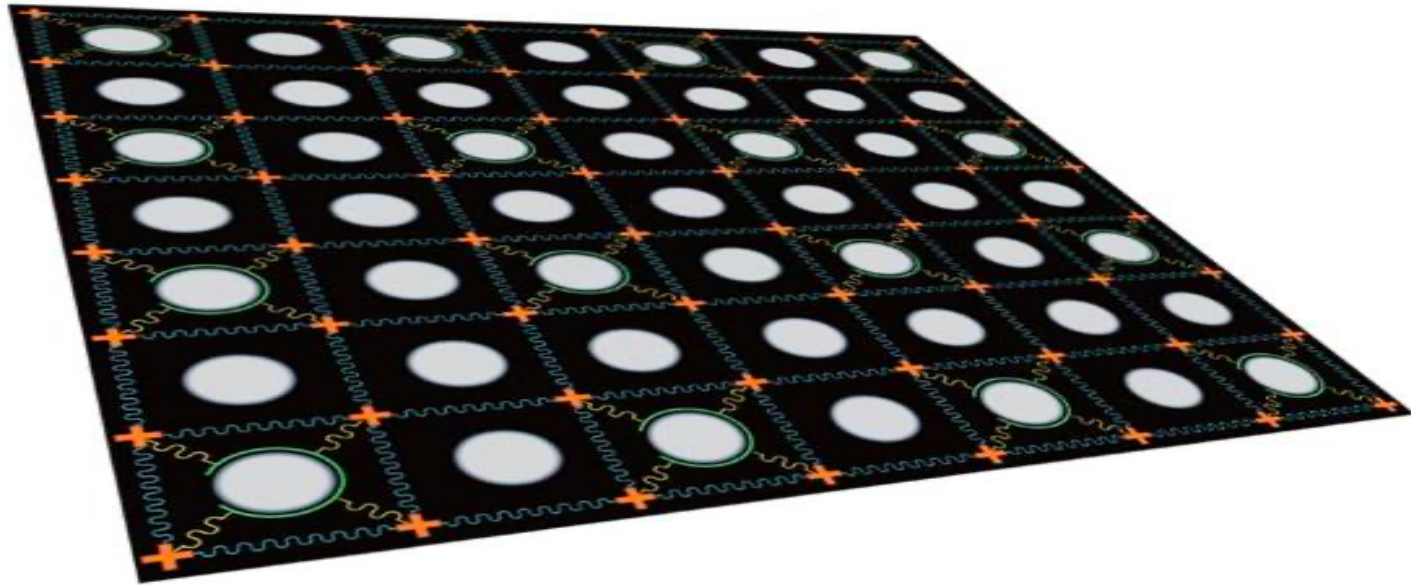
53-qubit superconducting processor “Sycamore” [AAB+19]: 200s for a particular task, which would take a supercomputer 10000 years.



[AAB+19] F. Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature* 574(7779):505-510 (2019).

## Quantum processors

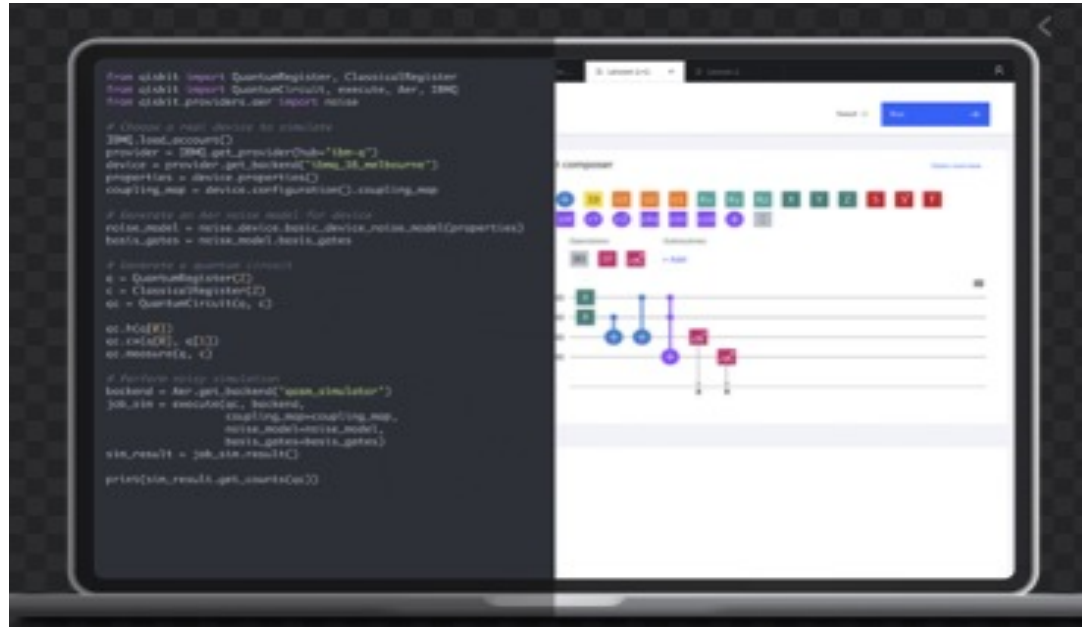
62-qubit superconducting quantum processor “Zu Chongzhi” [GWZ+21]



[GWZ+21] M. Gong et al. Quantum walks on a programmable two-dimensional 62-qubit superconducting processor. *Science* 372, 948-952 (2021).

# Quantum software

Qiskit (IBM), Cirq (Google), Q# (Microsoft) ...



<https://quantum-computing.ibm.com>

## References

- Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2010.
- Mingsheng Ying. Foundations of Quantum Programming. Morgan Kaufmann, 2016.
- Santanu Pattanayak. Quantum Machine Learning with Python. Apress, 2021.

## Outline

- Introduction
- Mathematical Foundations
- Postulates of Quantum Mechanics
- Quantum Circuits
- Quantum Programming
- Quantum Algorithms

# Introduction



## Quantum Bit

- A bit in classical computing is in one of two states: 0 or 1.
- A quantum bit (qubit) can take two fundamental states:  $|0\rangle$  and  $|1\rangle$

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

- Dirac notation: ket  $|0\rangle$  is a column vector, bra  $\langle 0|$  is a row vector  $[1 \ 0]$

## Superposition

- A qubit  $|\psi\rangle$  can exist as a **superposition** of  $|0\rangle$  and  $|1\rangle$ , expressed as a linear combination

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

with  $\alpha, \beta \in \mathbb{C}$ .

- $|0\rangle$  and  $|1\rangle$  are **computational basis states**

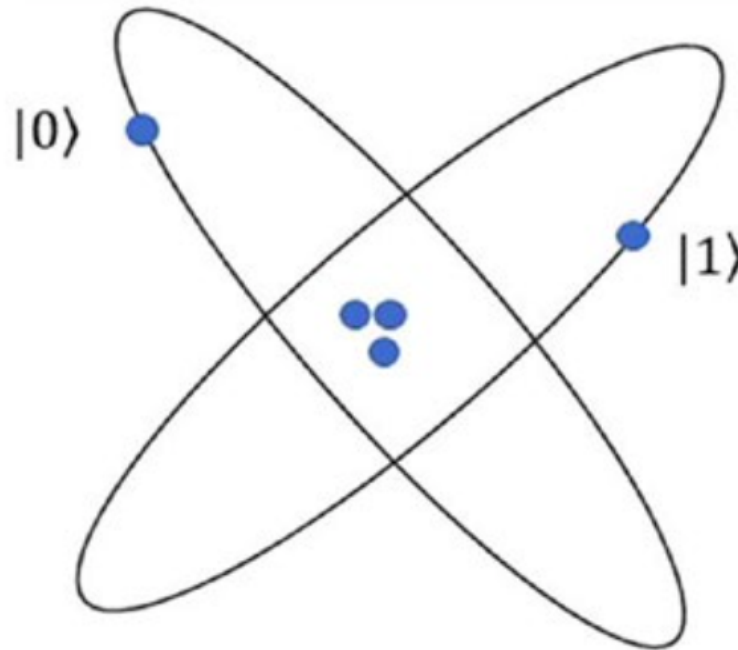
$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

- constraint:  $|\alpha|^2 + |\beta|^2 = 1$
- coefficients  $\alpha, \beta$  are **probability amplitudes**

## Qubit realization

Qubit realization using electron energy states

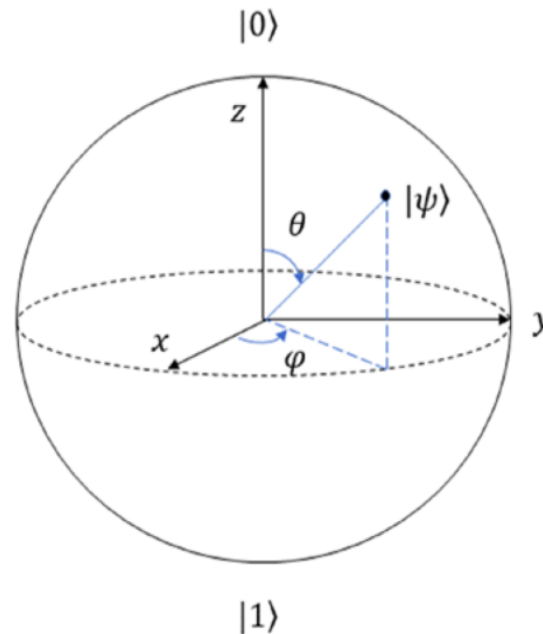
Ground state:  $|0\rangle$ , excited state:  $|1\rangle$



## Bloch sphere representation of qubit

Any point on the surface of the Bloch sphere represents a qubit state.

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle \right)$$



## Bloch sphere representation of qubit

Recall that a complex number  $\alpha = a + ib$  in the Cartesian coordinates can be expressed in polar coordinates as  $\alpha = re^{i\phi}$  with  $r = \sqrt{a^2 + b^2}$ .

Let  $\alpha = r_\alpha e^{i\phi_\alpha}$ ,  $\beta = r_\beta e^{i\phi_\beta}$ .

$$\begin{aligned} |\psi\rangle &= r_\alpha e^{i\phi_\alpha} |0\rangle + r_\beta e^{i\phi_\beta} |1\rangle \\ &= e^{i\phi_\alpha} (r_\alpha |0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)} |1\rangle) \end{aligned}$$

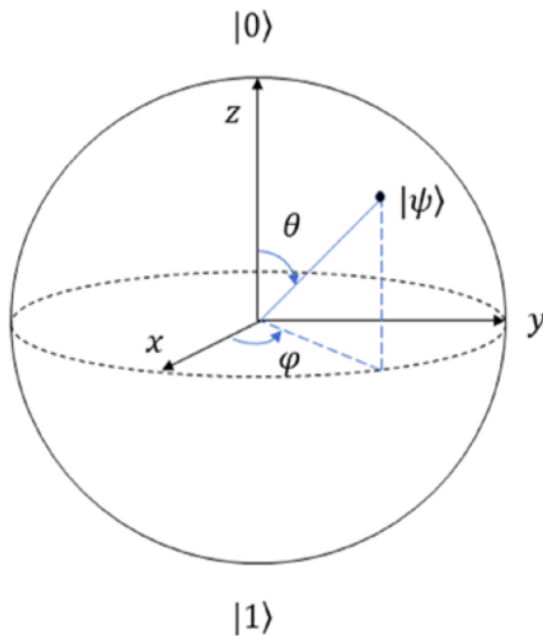
Since  $r_\alpha^2 + r_\beta^2 = |\alpha|^2 + |\beta|^2 = 1$ , take  $r_\alpha = \cos \frac{\theta}{2}$  and  $r_\beta = \sin \frac{\theta}{2}$ .

$$|\psi\rangle = e^{i\phi_\alpha} \left( \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i(\phi_\beta - \phi_\alpha)} |1\rangle \right)$$

Then replace  $\phi_\alpha$  with  $\gamma$  and  $\phi_\beta - \phi_\alpha$  with  $\varphi$  to yield the required form.

## Bloch sphere representation of qubit

Ignore the global phase factor,  $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle$



Axis	Value of $\theta$ and $\varphi$	Qubit State
$ z\rangle$	$\theta = 0; \varphi = 0$	$ 0\rangle$
$ {-z}\rangle$	$\theta = \pi; \varphi = 0$	$ 1\rangle$
$ x\rangle$	$\theta = \frac{\pi}{2}; \varphi = 0$	$\frac{1}{\sqrt{2}} 0\rangle + \frac{1}{\sqrt{2}} 1\rangle$
$ {-x}\rangle$	$\theta = \frac{\pi}{2}; \varphi = \pi$	$\frac{1}{\sqrt{2}} 0\rangle - \frac{1}{\sqrt{2}} 1\rangle$
$ y\rangle$	$\theta = \frac{\pi}{2}; \varphi = \frac{\pi}{2}$	$\frac{1}{\sqrt{2}} 0\rangle + \frac{i}{\sqrt{2}} 1\rangle$
$ {-y}\rangle$	$\theta = \frac{\pi}{2}; \varphi = -\frac{\pi}{2}$	$\frac{1}{\sqrt{2}} 0\rangle - \frac{i}{\sqrt{2}} 1\rangle$

## Multiple qubits

- State of a two-qubit system

$$|\psi\rangle_{AB} = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- Constraint:  $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$

- If we measure qubit A and observe 0, the probability is

$$|\alpha_{00}|^2 + |\alpha_{01}|^2$$

and the post-measurement state is

$$|\phi'\rangle_{AB} = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

## Bell state

- Bell state  $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- If we observe qubit A and observe 0, the two-qubit state collapses to state  $|00\rangle$ . Then if we measure qubit B, we observe outcome 0 with certainty.
- The states of two qubits are perfectly correlated. This phenomenon is quantum entanglement.
- Imagine this Bell state is created using quantum entanglement between two electrons and then we separate the electrons by a large distance. Measuring one electron determines the other electron's state.



## Dirac notation

- Ket vector  $|\psi_1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix}$ ,  $|\psi_2\rangle = \begin{bmatrix} \frac{3}{5} \\ \frac{4i}{5} \end{bmatrix}$
- Bra vector  $\langle\psi_1| = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{bmatrix}$ ,  $\langle\psi_2| = \begin{bmatrix} \frac{3}{5} & -\frac{4i}{5} \end{bmatrix}$
- Inner product of two vectors  $|\psi_1\rangle$  and  $|\psi_2\rangle$  is written

$$\langle\psi_1|\psi_2\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{3}{5} \\ \frac{4i}{5} \end{bmatrix} = \frac{7}{5\sqrt{2}}$$

## Magnitude of a vector

- The magnitude of a vector is the  $l^2$  norm

$$\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle}$$

- $\langle \psi | \psi \rangle = \begin{bmatrix} c_1^* & c_2^* & \dots & c_n^* \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \sum_{i=1}^n c_i^* c_i = \sum_{i=1}^n |c_i|^2.$

- If  $|\psi\rangle$  is a quantum state,  $\langle \psi | \psi \rangle = 1$ . Each  $|c_i|^2$  gives the probability of the state  $|\psi\rangle$  collapsing to the state  $|i\rangle$  on measurement.

## Outer product

The outer product of two vectors  $|\psi_1\rangle \in \mathbb{C}^m$  and  $|\psi_2\rangle \in \mathbb{C}^n$  gives a matrix of dimension  $m \times n$ .

$$|\psi_1\rangle\langle\psi_2| = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix} \begin{bmatrix} d_1^* & d_2^* & \dots & d_n^* \end{bmatrix} = \begin{bmatrix} c_1 d_1^* & c_1 d_2^* & \dots & c_1 d_n^* \\ \vdots & \vdots & \vdots & \vdots \\ c_m d_1^* & c_m d_2^* & \dots & c_m d_n^* \end{bmatrix}$$

## Tensor product

The tensor product of two vectors  $|\psi_1\rangle \in \mathbb{C}^m$  and  $|\psi_2\rangle \in \mathbb{C}^n$  is another vector in  $\mathbb{C}^{m \times n}$ .

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \otimes \begin{bmatrix} d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} c_1 d_1 \\ c_1 d_2 \\ c_1 d_3 \\ c_2 d_1 \\ c_2 d_2 \\ c_2 d_3 \end{bmatrix}$$

## Tensor product

If  $\{|v_1\rangle, \dots, |v_m\rangle\}$  is the basis of one space,  $\{|u_1\rangle, \dots, |u_n\rangle\}$  the basis of another space, then using tensor product can get a larger vector space with basis vectors of the form  $|v_i\rangle \otimes |u_j\rangle$ , written  $|v_i u_j\rangle$ .

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

The Bell state cannot be factored as a tensor product of individual qubit states.

## Single-qubit gates

$$X : \alpha|0\rangle + \beta|1\rangle \rightarrow \beta|0\rangle + \alpha|1\rangle$$

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

$$Z : \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$$

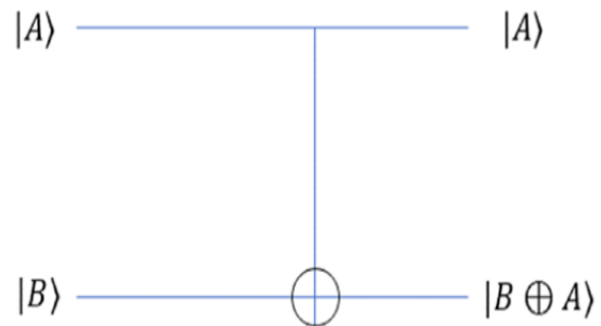
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H : \begin{cases} |0\rangle & \rightarrow & \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |1\rangle & \rightarrow & \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{cases}$$

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

## CNOT gate

$$CNOT : \begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{cases} \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

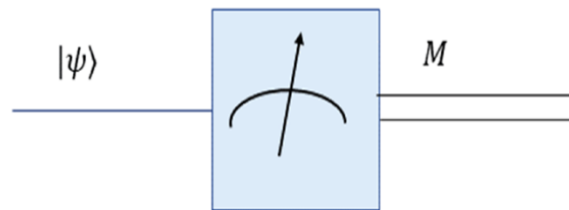


## Measurements in different basis

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

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

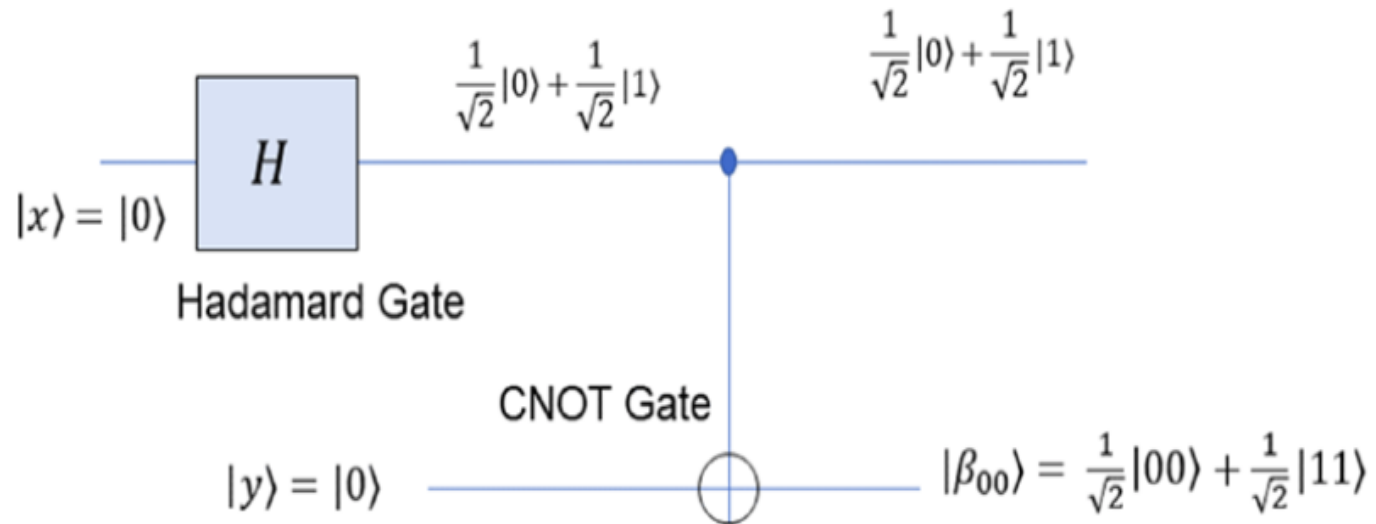
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$



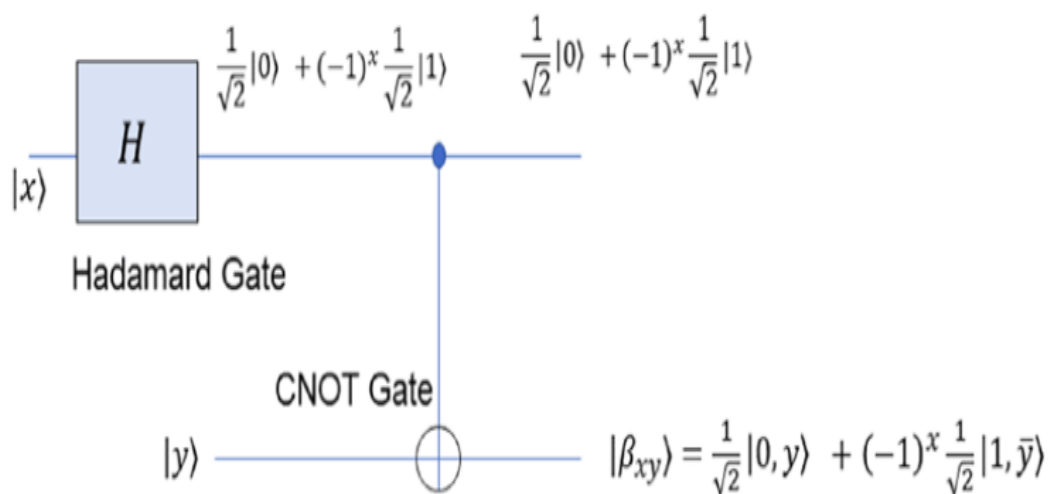


## Preparation of Bell states

$$CNOT : \left( \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes |0\rangle \rightarrow \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$



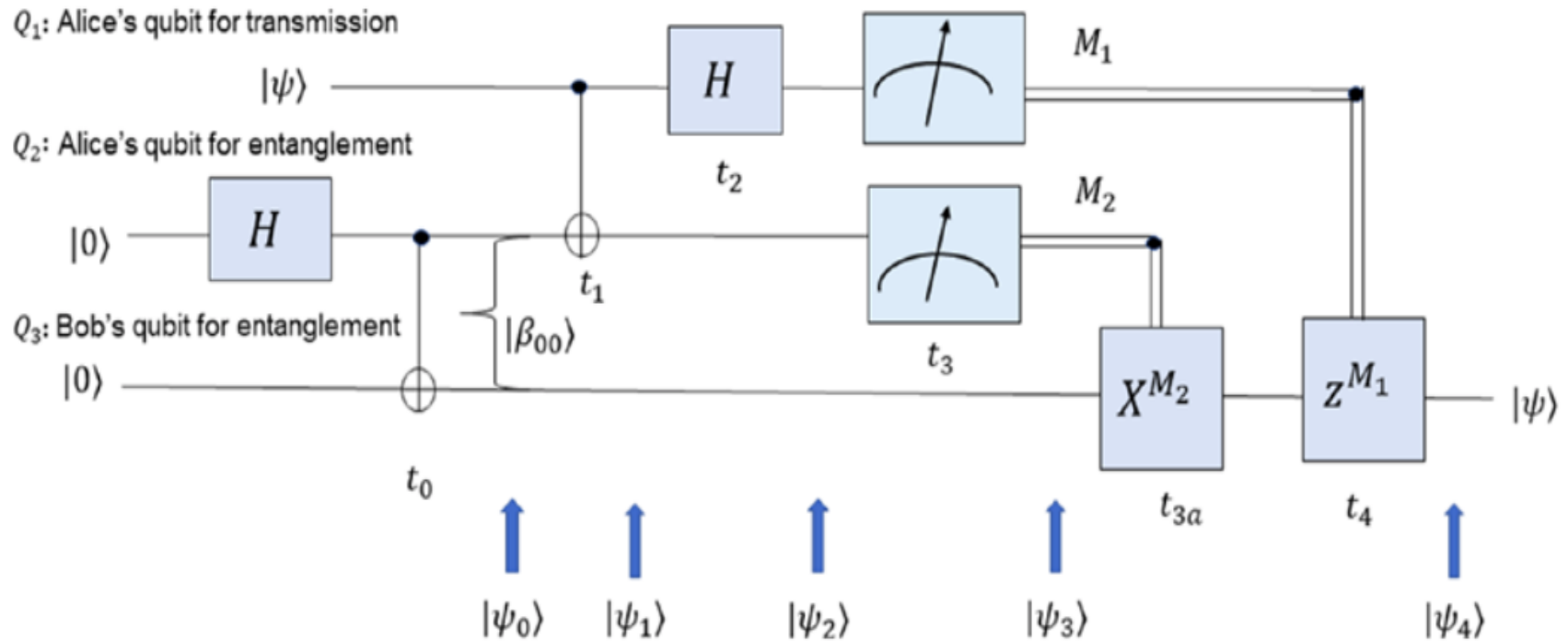
## Generalized Bell states



$x$	$y$	Bell State $ \beta_{xy}\rangle$
0	0	$ \beta_{00}\rangle = \frac{1}{\sqrt{2}} 00\rangle + \frac{1}{\sqrt{2}} 11\rangle$
0	1	$ \beta_{01}\rangle = \frac{1}{\sqrt{2}} 01\rangle + \frac{1}{\sqrt{2}} 10\rangle$
1	0	$ \beta_{10}\rangle = \frac{1}{\sqrt{2}} 00\rangle - \frac{1}{\sqrt{2}} 11\rangle$
1	1	$ \beta_{11}\rangle = \frac{1}{\sqrt{2}} 01\rangle - \frac{1}{\sqrt{2}} 10\rangle$

# Quantum teleportation

Quantum teleportation aims to transmit a qubit by using two bits of classical communication and a Bell pair.

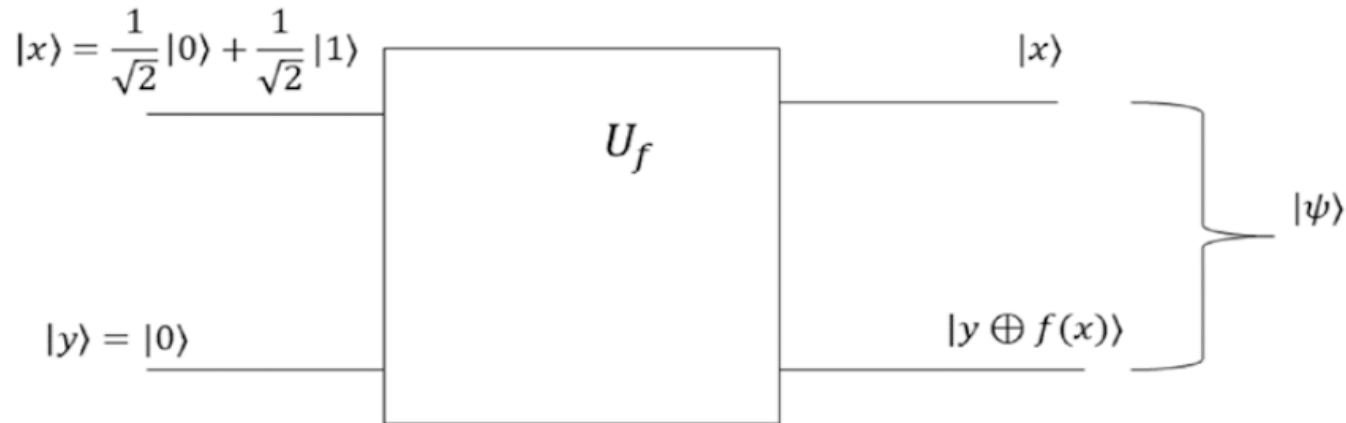


## Quantum teleportation

$$\begin{aligned}
 |\psi_0\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 &= \alpha|0\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) + \beta|1\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 |\psi_1\rangle &= \alpha|0\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) + \beta|1\rangle \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\
 |\psi_2\rangle &= \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\
 &= \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) \\
 &\quad + \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)
 \end{aligned}$$

$M_1$	$M_2$	Bob's Qubit Post Measurement	$X^{M_2}$ , Bob's Qubit State Post $X^{M_2}$	$Z^{M_1}$ , Bob's Qubit State Post $Z^{M_1}$
0	0	$\alpha 0\rangle + \beta 1\rangle$	$I, \alpha 0\rangle + \beta 1\rangle$	$I, \alpha 0\rangle + \beta 1\rangle$
0	1	$\alpha 1\rangle + \beta 0\rangle$	$X, \alpha 0\rangle + \beta 1\rangle$	$I, \alpha 0\rangle + \beta 1\rangle$
1	0	$\alpha 0\rangle - \beta 1\rangle$	$I, \alpha 0\rangle - \beta 1\rangle$	$Z, \alpha 0\rangle + \beta 1\rangle$
1	1	$\alpha 1\rangle - \beta 0\rangle$	$X, \alpha 0\rangle - \beta 1\rangle$	$Z, \alpha 0\rangle + \beta 1\rangle$

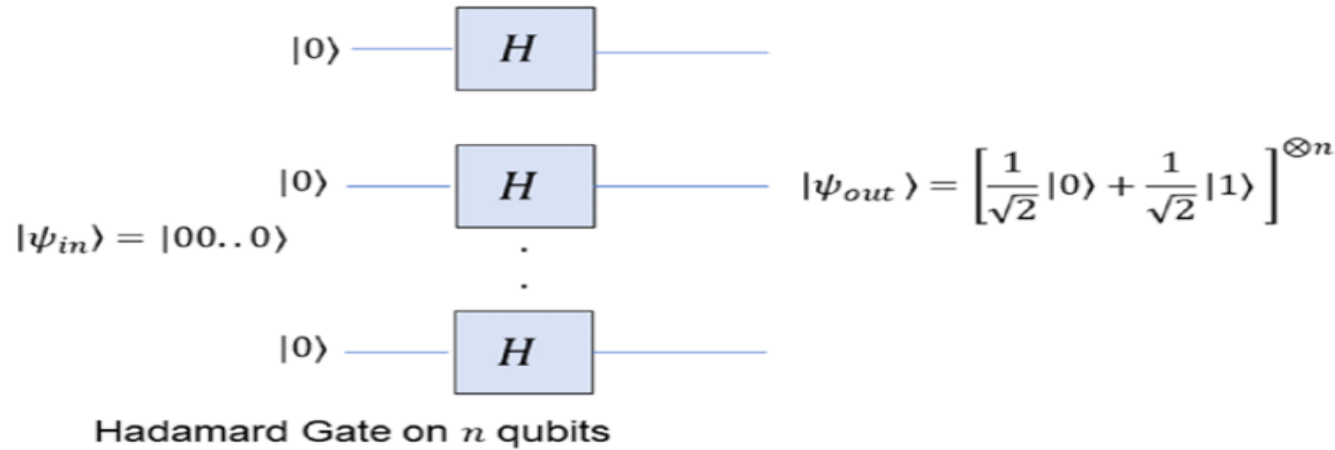
## Quantum parallelism



Start with an equal superposition state  $|x\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ , the output state

$$|\psi\rangle = |x, y \oplus f(x)\rangle = |x, f(x)\rangle = \frac{1}{\sqrt{2}}|0, f(0)\rangle + \frac{1}{\sqrt{2}}|1, f(1)\rangle$$

## Quantum parallelism



$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x_{n-1}=0}^1 \cdots \sum_{x_0=0}^1 |x_{n-1}, \dots, x_0\rangle$$

Treat the binary string as an integer number  $x = x_{n-1}2^{n-1} \dots + x_02^0$ .

$$\text{Then } \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes n} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$$

and the output state  $\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$

## Quantum interference

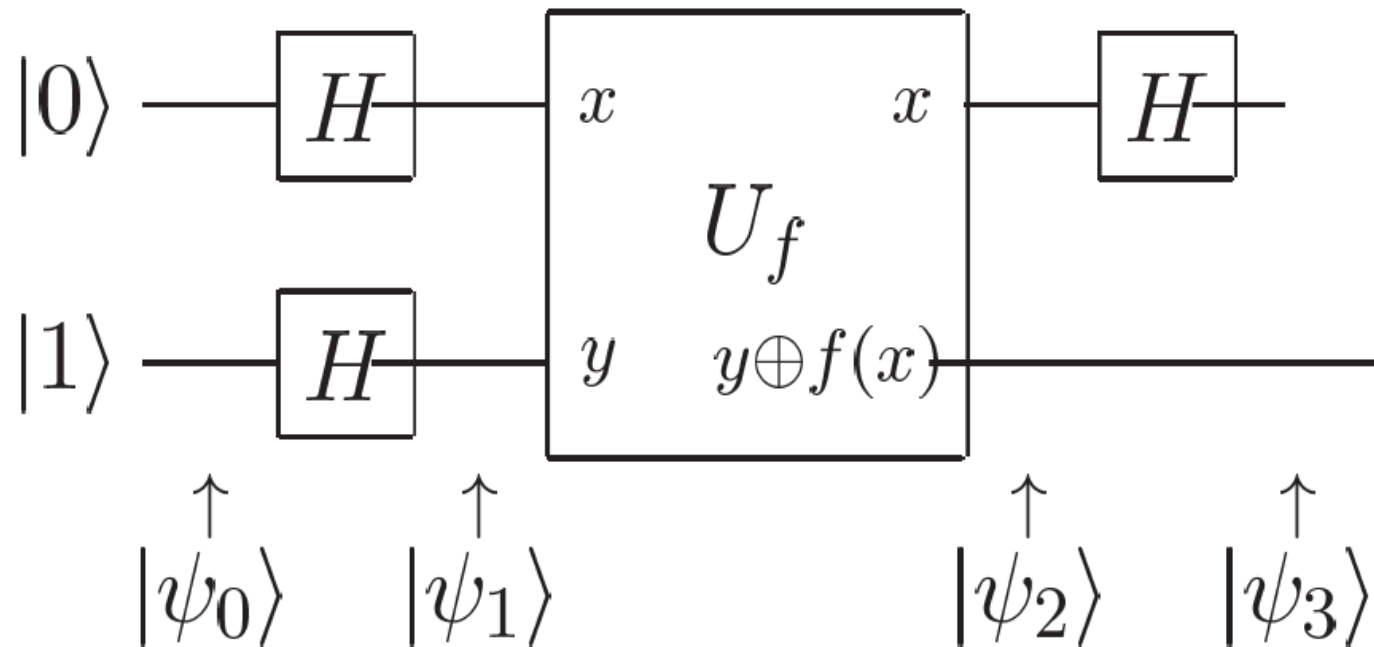
Let  $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

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

After applying  $H$  to  $|\psi\rangle$ , the probability amplitudes of  $|0\rangle$  (resp.  $|1\rangle$ ) undergo constructive (resp. destructive) interference.

## Deutsch's algorithm

Deutsch's problem: decide if a Boolean function  $f : \{0, 1\} \rightarrow \{0, 1\}$  is constant or not.





## Deutsch's algorithm

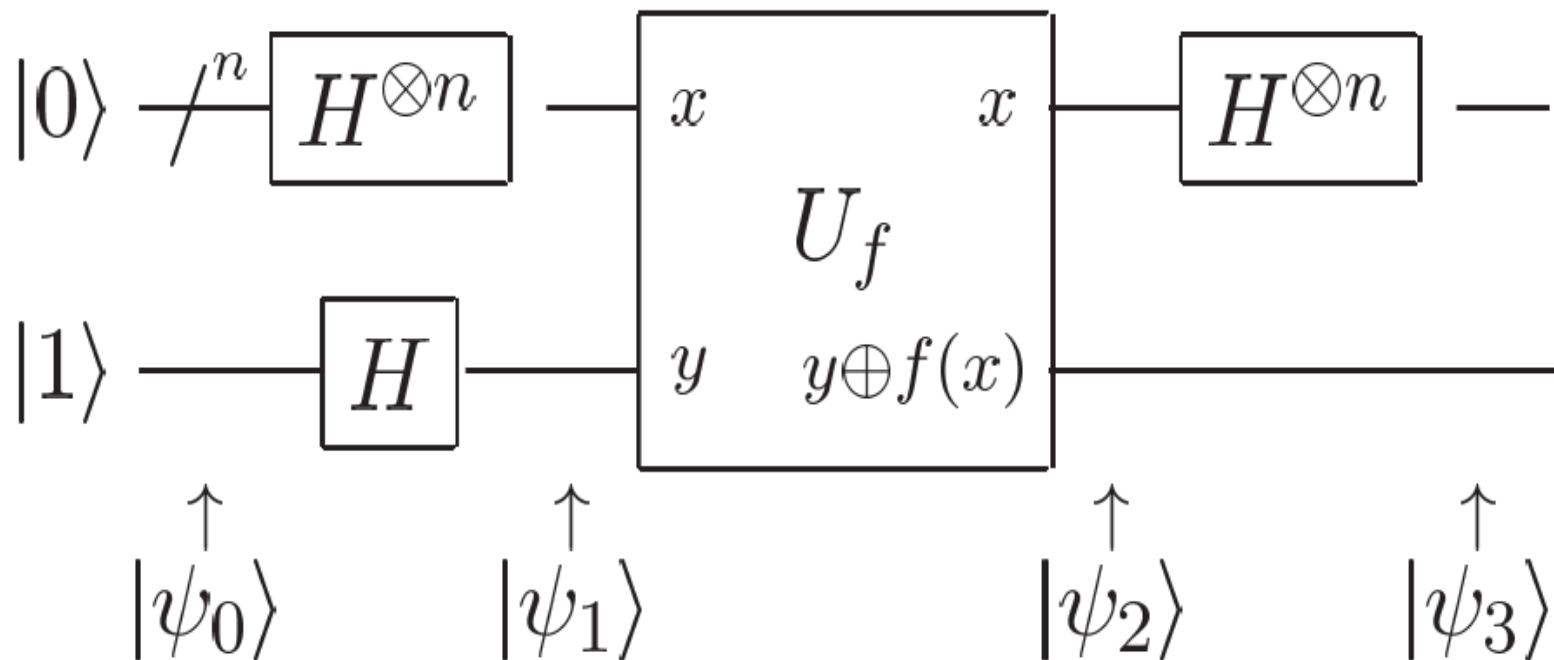
$$\begin{aligned} |\psi_0\rangle &= |01\rangle \\ |\psi_1\rangle &= \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ |\psi_2\rangle &= \begin{cases} \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1). \end{cases} \\ |\psi_3\rangle &= \begin{cases} \pm|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1). \end{cases} \\ &= \pm|f(0) \oplus f(1)\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \end{aligned}$$

The circuit can determine the **global property**  $f(0) \oplus f(1)$  by measuring the first qubit, using only one evaluation of  $f(x)$ !

With a classical apparatus, one would need at least two evaluations.

## The Deutsch-Jozsa algorithm

**Deutsch-Jozsa problem:** given a Boolean function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  that is guaranteed to be either constant or balanced (it returns 0's for exactly half of all inputs and 1's for the other half), determine if it is constant or balanced.



## The Deutsch-Jozsa algorithm

$$\begin{aligned} |\psi_0\rangle &= |0\rangle^{\otimes n} |1\rangle \\ |\psi_1\rangle &= \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ |\psi_2\rangle &= \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

**Phase kickback:** have the function value  $f(x)$  show up in the global phase by applying a unitary transform on the target qubit in superposition.

For  $x = 0$  or  $x = 1$  we have  $H|x\rangle = \sum_z (-1)^{xz} |z\rangle / \sqrt{2}$ , thus

$$H^{\otimes n} |x_1, \dots, x_n\rangle = \frac{\sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle}{\sqrt{2^n}}$$

Write it succinctly,

$$H^{\otimes n} |x\rangle = \frac{\sum_z (-1)^{x \cdot z} |z\rangle}{\sqrt{2^n}}$$

where  $x \cdot z$  is the bitwise inner product of  $x$  and  $z$ , modulo 2.

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^n} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

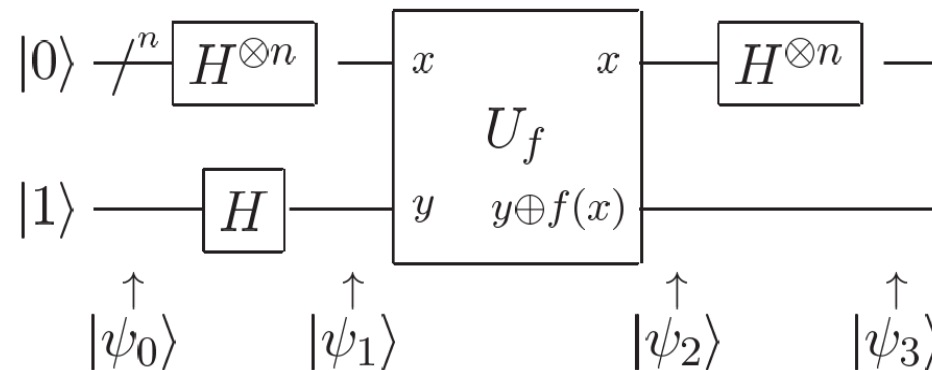
- If  $f$  is constant: the amplitude for  $|0\rangle^{\otimes n}$  is  $\pm 1$ , all other amplitudes must be zero.
- If  $f$  is balanced: the positive and negative contributions to the amplitude for  $|0\rangle^{\otimes n}$  cancel, leaving amplitude zero.

In summary, a measurement of all 0s means  $f$  is constant; otherwise it is balanced.

## The Bernstein-Vazirani Algorithm

The Bernstein-Vazirani Problem: Suppose there is a black-box function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , as in the Deutsch-Jozsa problem. Instead of being balanced or constant, it is guaranteed to return the dot product with some string  $s$ , i.e.  $f_s(x) = s \cdot x \pmod{2}$ . The problem is to find such  $s$ .

Classically, we can reveal  $s$  by querying with the inputs  $100\dots 0, 010\dots 0, 001\dots 0, \dots, 000\dots 1$ , i.e. to call  $f_s$  exactly  $n$  times.



## The Bernstein-Vazirani Algorithm

Use the same quantum circuit as in the Deutsch–Jozsa algorithm,

$$\begin{aligned} |\psi_3\rangle &= \sum_z \sum_x \frac{(-1)^{x \cdot z + f_s(x)} |z\rangle}{2^n} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\ &= \sum_z \sum_x \frac{(-1)^{x \cdot z + s \cdot x} |z\rangle}{2^n} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

The amplitude of any computational basis state  $|z\rangle$  is

$$A(z) = \sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot z + s \cdot x}}{2^n}$$

In particular, when  $z = s$ ,

$$A(s) = \sum_{x \in \{0,1\}^n} \frac{(-1)^{x \cdot s + s \cdot x}}{2^n} = 1$$

That is, we will get state  $|s\rangle$  with 100% probability.

## Simon's Problem

Suppose there is an unknown black-box function  $f$ , which is guaranteed to be either one-to-one or two-to-one. For example,

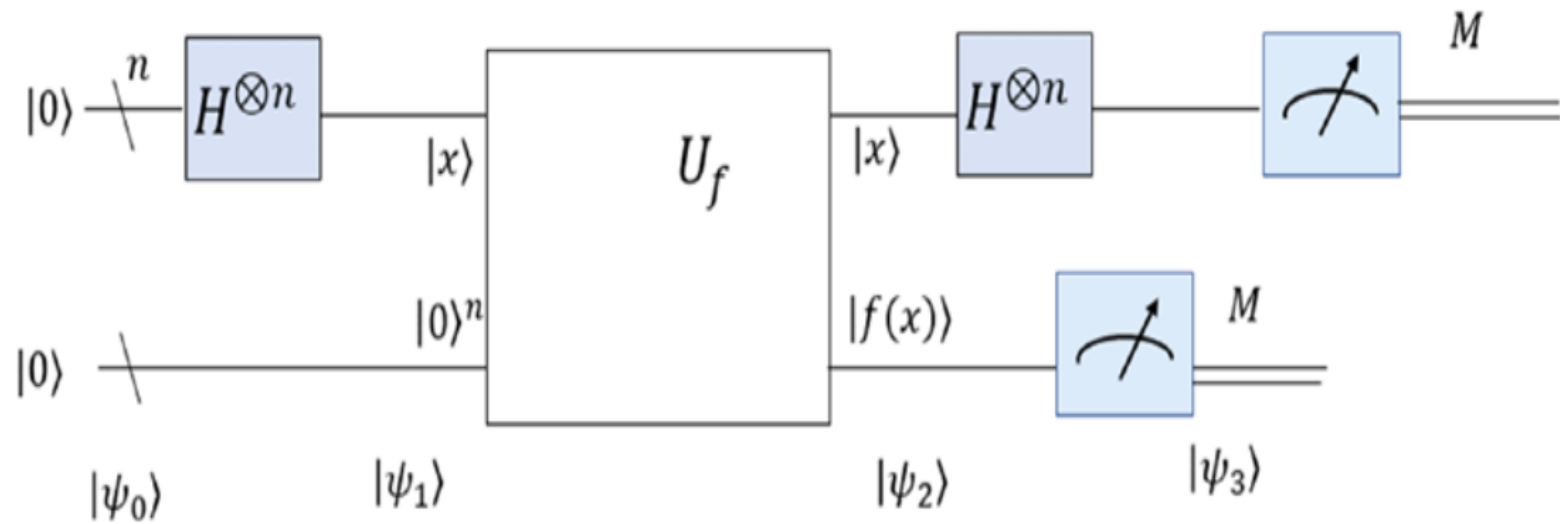
- one-to-one:  $f(i) = i$  for  $i \in \{1, 2, 3, 4\}$
- two-to-one:  $f(1) = f(3) = 1$ ,  $f(2) = f(4) = 2$

When the function is two-to-one, then there is a secret string  $s$  such that  $f(x_1) = f(x_2)$  iff  $x_1 \oplus x_2 = s$ . The string  $s = 000\dots$  represents the one-to-one function  $f$ .

The aim is to determine if  $f$  is one-to-one or two-to-one by finding string  $s$ .

Classically, we have to query  $f$  up to  $2^{n-1} + 1$  inputs, where  $n$  is the number of bits in the inputs.

## Simon's algorithm





## Simon's algorithm

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

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle^{\otimes n}$$

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

$$|\psi_3\rangle = H^{\otimes n} |\psi_2\rangle = \frac{1}{2^n} \sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle |f(x)\rangle$$

- If  $f$  is one-to-one, measuring the target qubits and observe  $|f(x)\rangle$  will get only one corresponding  $x$ . For each input  $|z\rangle$  state, the amplitude is  $A(z) = \frac{1}{2^{n/2}}$  given that the target  $|f(x)\rangle$  is observed. The probability is  $\frac{1}{2^n}$  for all  $z$ , a uniform distribution over the input states  $|z\rangle$ .
- If  $f$  is two-to-one, measuring the target qubits and observe  $|c\rangle$  would corresponds to two values  $x_1, x_2$  with  $f(x_1) = f(x_2) = c$ . The amplitude of each input state  $|z\rangle$  is  $A(z) = \frac{1}{2^{\frac{n+1}{2}}} [(-1)^{x_1 \cdot z} + (-1)^{x_2 \cdot z}]$ .

If  $A(z) \neq 0$  then

$$(-1)^{x_1 \cdot z} = (-1)^{x_2 \cdot z} \quad \Rightarrow \quad x_1 \cdot z = x_2 \cdot z$$

$$s \cdot z = (x_1 \oplus x_2) \cdot z = x_1 \cdot z \oplus x_2 \cdot z = x_1 \cdot z \oplus x_1 \cdot z = 0 \pmod{2}$$

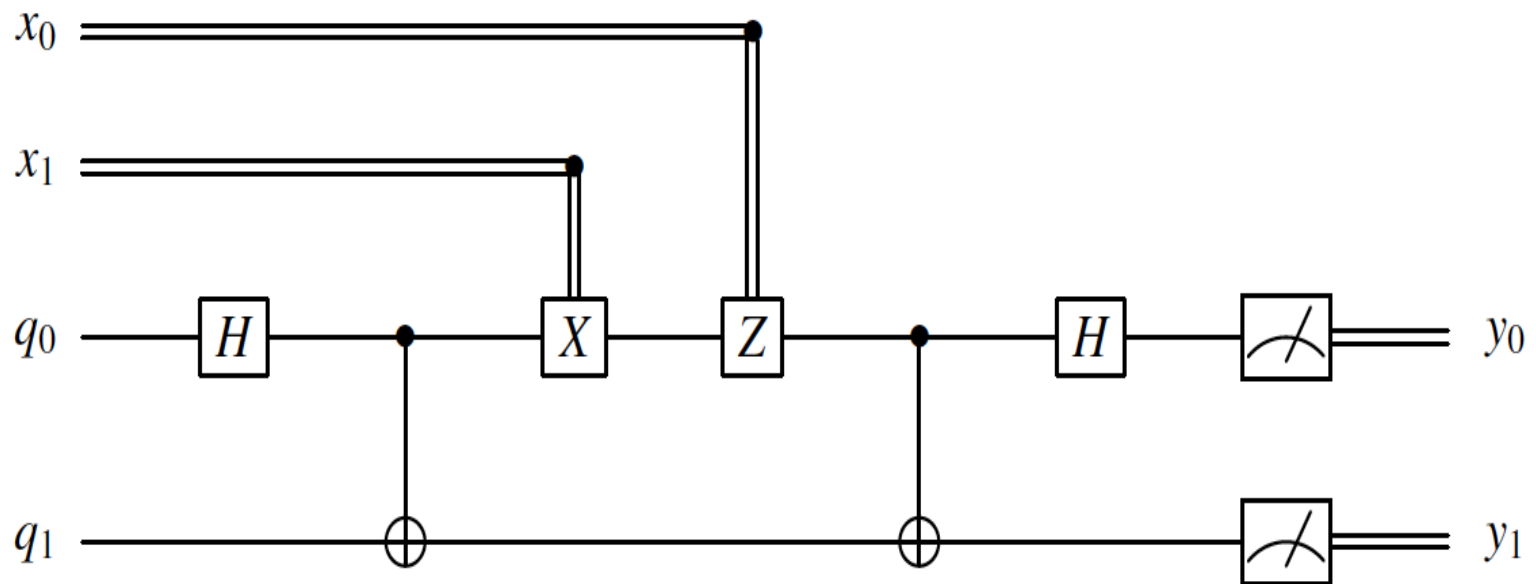
Measure the input qubits and observe  $n$  different  $z$  values to find string  $s$ :

$$\begin{aligned} s \cdot z_1 &= 0 \\ s \cdot z_2 &= 0 \\ &\vdots \\ s \cdot z_n &= 0 \end{aligned}$$

The  $n$  equations can be solved by Gaussian elimination.

## Superdense coding

Superdense coding aims to send two classical bits using just a single qubit of communication.



## Superdense coding

$$(x_0 x_1 y_0 y_1, |00\rangle) \xrightarrow{H} \left( *, \frac{|0\rangle+|1\rangle}{\sqrt{2}} |0\rangle \right) \xrightarrow{CNOT} \left( *, \frac{|00\rangle+|11\rangle}{\sqrt{2}} \right)$$

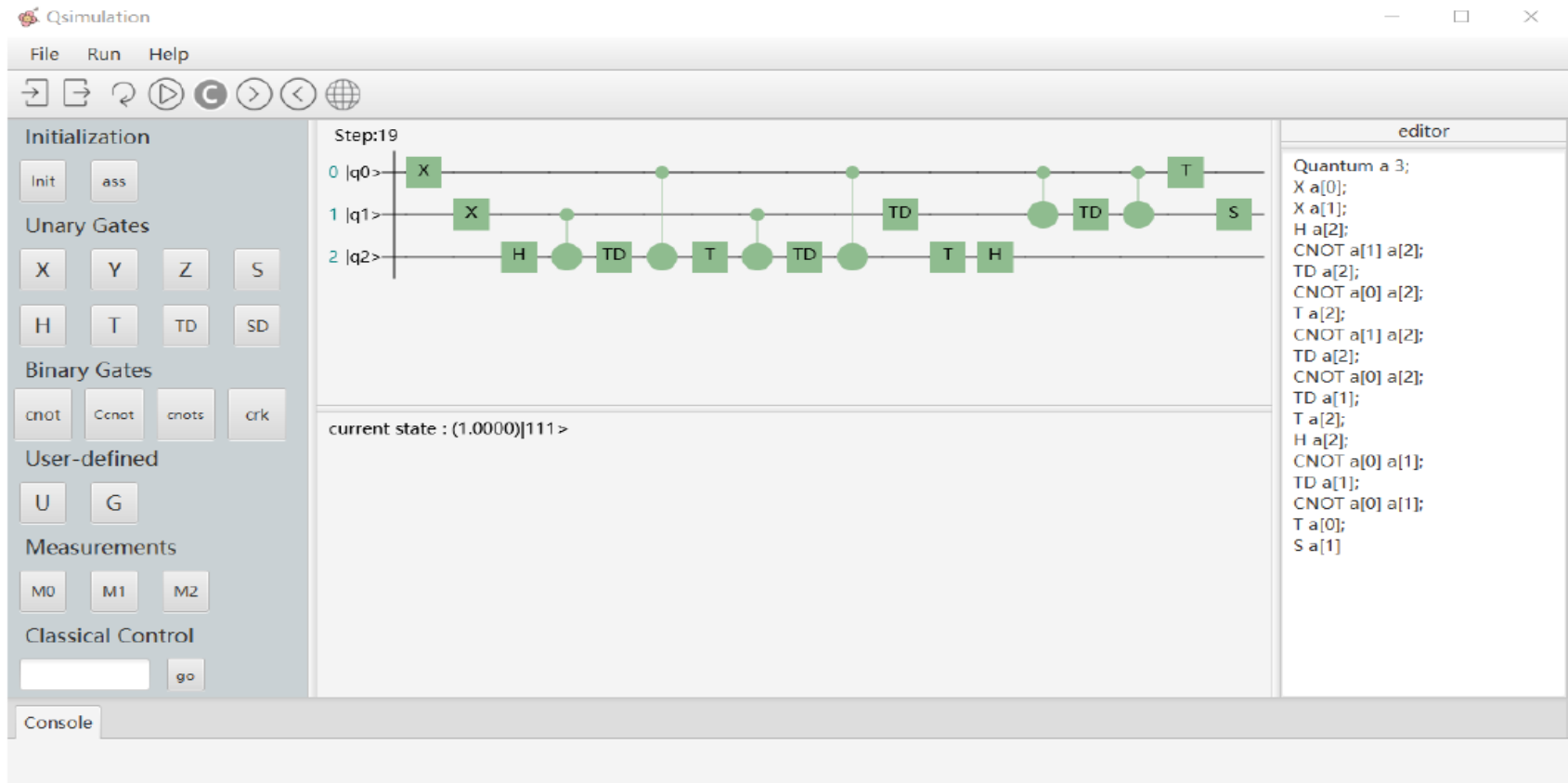
$$\xrightarrow{CX} \left( *, X_0^{x_1} \frac{|00\rangle+|11\rangle}{\sqrt{2}} \right) \xrightarrow{CZ} \left( *, Z_0^{x_0} X_0^{x_1} \frac{|00\rangle+|11\rangle}{\sqrt{2}} \right)$$

$$\equiv \begin{cases} (00y_0y_1, \frac{|00\rangle+|11\rangle}{\sqrt{2}}) & \text{if } x_0 = x_1 = 0 \\ (01y_0y_1, \frac{|10\rangle+|01\rangle}{\sqrt{2}}) & \text{if } x_0 = 0, x_1 = 1 \\ (10y_0y_1, \frac{|00\rangle-|11\rangle}{\sqrt{2}}) & \text{if } x_0 = 1, x_1 = 0 \\ (11y_0y_1, \frac{|10\rangle-|01\rangle}{\sqrt{2}}) & \text{if } x_0 = x_1 = 1 \end{cases}$$

$$\xrightarrow{CNOT} \begin{cases} (00y_0y_1, \frac{|00\rangle+|10\rangle}{\sqrt{2}}) \\ (01y_0y_1, \frac{|11\rangle+|01\rangle}{\sqrt{2}}) \\ (10y_0y_1, \frac{|00\rangle-|10\rangle}{\sqrt{2}}) \\ (11y_0y_1, \frac{|11\rangle-|01\rangle}{\sqrt{2}}) \end{cases} \xrightarrow{H} \begin{cases} (00y_0y_1, |00\rangle) \\ (01y_0y_1, |01\rangle) \\ (10y_0y_1, |10\rangle) \\ (11y_0y_1, |11\rangle) \end{cases} \xrightarrow{Meas} \begin{cases} (0000, |00\rangle) \\ (0101, |01\rangle) \\ (1010, |10\rangle) \\ (1111, |11\rangle) \end{cases}$$

# Qsimulation

Qsimulation is a tool for simulating quantum computation on classical computers.



<https://github.com/coconutoe/quantum>

see also Qiskit <https://qiskit.org>

# Mathematical Foundations

## Vector spaces

A (complex) vector space is a nonempty set  $\mathcal{H}$  with two operations:

- vector addition  $+$  :  $\mathcal{H} \times \mathcal{H} \rightarrow \mathcal{H}$
- scalar multiplication  $\cdot$  :  $\mathbb{C} \times \mathcal{H} \rightarrow \mathcal{H}$

satisfying the following conditions:

1.  $+$  is commutative:  $|u\rangle + |v\rangle = |v\rangle + |u\rangle$ ;
2.  $+$  is associative:  $|u\rangle + (|v\rangle + |w\rangle) = (|u\rangle + |v\rangle) + |w\rangle$ ;
3.  $+$  has the zero element  $0$ , called the zero vector, such that  $0 + |v\rangle = |v\rangle$ ;
4. each  $|v\rangle \in \mathcal{H}$  has its negative vector  $-|v\rangle$  such that  $|v\rangle + (-|v\rangle) = 0$ ;
5.  $1|v\rangle = |v\rangle$ ;
6.  $\alpha(\beta|v\rangle) = (\alpha\beta)|v\rangle$ ;
7.  $(\alpha + \beta)|v\rangle = \alpha|v\rangle + \beta|v\rangle$ ;
8.  $\alpha(|u\rangle + |v\rangle) = \alpha|u\rangle + \alpha|v\rangle$ .

## Inner product spaces

An inner product space is a vector space  $\mathcal{H}$  equipped with an inner product:

$$\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$$

satisfying the conditions:

1.  $\langle u|u \rangle \geq 0$  with equality if and only if  $|u \rangle = 0$ ;
  2.  $\langle u|v \rangle = \langle v|u \rangle^*$ ;
  3.  $\langle u|\alpha v + \beta w \rangle = \alpha \langle u|v \rangle + \beta \langle u|w \rangle$ .
- If  $\langle u|v \rangle = 0$ , then  $|u \rangle$  and  $|v \rangle$  are orthogonal, written  $|u \rangle \perp |v \rangle$ .
  - The length of a vector  $|v \rangle \in \mathcal{H}$  is  $\| |v \rangle \| = \sqrt{\langle v|v \rangle}$ .
  - A vector  $|v \rangle$  is a unit vector if  $\| |v \rangle \| = 1$ .



## Hilbert spaces

Let  $\{|v_n\rangle\}$  be a sequence of vectors in an inner product space  $\mathcal{H}$  and  $|v\rangle \in \mathcal{H}$ .

1. If for any  $\epsilon > 0$ , there exists a positive interger  $N$  such that  $\| |v_m\rangle - |v_n\rangle \| < \epsilon$  for all  $m, n \geq N$ , then  $\{|v_n\rangle\}$  is a **Cauchy sequence**.
2. If for any  $\epsilon > 0$ , there exists a positive interger  $N$  such that  $\| |v_n\rangle - |v\rangle \| < \epsilon$  for all  $n \geq N$ , then  $|v\rangle$  is a limit of  $\{|v_n\rangle\}$ , written  $|v\rangle = \lim_{n \rightarrow \infty} |v_n\rangle$ .

A **Hilbert space** is a complete inner product space, i.e., an inner product space where each Cauchy sequence of vectors has a limit.

## Linear independence of vectors

- A set of vectors  $\{|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle\}$  in  $\mathcal{H}$  is linearly independent if  $c_1|v_1\rangle + c_2|v_2\rangle + \dots + c_n|v_n\rangle = 0$  only when all the coefficients  $c_i$  are zero.
- If a set of  $n$  vectors  $\{|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle\}$  in  $\mathbb{C}^n$  is linearly independent, the vectors span the entire  $n$ -dimensional vector space.
- A set of vectors  $\{|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle\}$  in  $\mathcal{H}$  is orthogonal if  $|v_i\rangle \perp |v_j\rangle$  when  $i \neq j$ .
- An orthogonal set of vectors are linear independent, but the converse is not necessarily true.

## Basis

A **basis**  $B$  of a vector space  $\mathcal{H}$  is a linearly independent subset of  $\mathcal{H}$  that spans  $\mathcal{H}$ . That is,

- (the linear independence property) for every finite subset of vectors  $\{|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle\}$  of  $B$ , if  $c_1|v_1\rangle + \dots + c_n|v_n\rangle = 0$  then all the coefficients  $c_i$  are zero.
- (the spanning property) for every vector  $|v\rangle$  in  $\mathcal{H}$ , there are  $c_1, c_2, \dots, c_n \in \mathbb{C}$  and  $|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle \in B$  such that  $|v\rangle = c_1|v_1\rangle + \dots + c_n|v_n\rangle$ .

## Orthonormal basis

- An orthonormal basis  $B$  of  $\mathcal{H}$  is a basis of  $\mathcal{H}$  such that  $B$  is an orthogonal set of unit vectors.
- The number of vectors in any two orthonormal bases are the same. It is called the dimension of  $\mathcal{H}$ .
- Suppose the dimension of  $\mathcal{H}$  is  $n$  and there is a fixed orthonormal basis  $\{|v_1\rangle, \dots, |v_n\rangle\}$ , then a vector  $|v\rangle = \sum_{i=1}^n c_i |v_i\rangle \in \mathcal{H}$  is represented by the vector in  $\mathbb{C}^n$ :

$$\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

## Closed subspace

Let  $\mathcal{H}$  be a Hilbert space.

- If  $V \subseteq \mathcal{H}$ , and for any  $|u\rangle, |v\rangle \in V$  and  $c \in \mathbb{C}$ .
  - $|u\rangle + |v\rangle \in V$
  - $c|v\rangle \in V$

then  $V$  is called a **subspace** of  $\mathcal{H}$ .

- For any  $V \subseteq \mathcal{H}$ , its closure  $\bar{V}$  is the set of limits  $\lim_{n \rightarrow \infty} |v_n\rangle$  of sequences  $\{|v_n\rangle\}$  in  $V$ .
- A subspace  $V$  of  $\mathcal{H}$  is closed if  $\bar{V} = V$ .
- For any set  $V \subseteq \mathcal{H}$ , the space spanned by  $V$  is written

$$\text{span } X = \left\{ \sum_{i=1}^n c_i |v_i\rangle \mid n \geq 0, c_i \in \mathbb{C} \text{ and } |v_i\rangle \in V (i = 1, \dots, n) \right\}$$

- $\overline{\text{span } V}$  is the closed subspace generated by  $V$ .
- For any  $U, V \subseteq \mathcal{H}$ ,  $U$  and  $V$  are orthogonal, written  $U \perp V$ , if  $|u\rangle \perp |v\rangle$  for all  $|u\rangle \in U, |v\rangle \in V$ .
- The **orthocomplement** of a closed subspace  $V$  of  $\mathcal{H}$  is

$$V^\perp = \{|u\rangle \in \mathcal{H} \mid |u\rangle \perp V\}$$

- The orthocomplement  $V^\perp$  is a closed subspace of  $\mathcal{H}$ ,  $(V^\perp)^\perp = V$ .
- Let  $U, V$  be two subspaces of  $\mathcal{H}$ . Then

$$U \oplus V = \{|u\rangle + |v\rangle \mid |u\rangle \in U \text{ and } |v\rangle \in V\}.$$

## Tensor product of Hilber spaces

- Let  $\mathcal{H}_i$  be a Hilbert spaces with  $\{|\psi_{ij_i}\rangle\}$  as an orthonormal basis for  $i = 1, \dots, n$ .
- Write  $B$  for the set of elements in the form:

$$|\psi_{1j_1}\rangle, \dots, |\psi_{nj_n}\rangle = |\psi_{1j_1}\rangle \otimes \dots \otimes |\psi_{nj_n}\rangle.$$

- The tensor product of  $\mathcal{H}_i$   $i = 1, \dots, n$  is the Hilbert space with  $B$  as an orthonormal basis:

$$\bigotimes_i \mathcal{H}_i = \text{span } B.$$

## Linear operators

Let  $\mathcal{H}$  and  $\mathcal{K}$  be Hilbert spaces. A mapping  $A : \mathcal{H} \rightarrow \mathcal{K}$  is a linear operator if it satisfies the conditions:

1.  $A(|u\rangle + |v\rangle) = A|u\rangle + A|v\rangle$
2.  $A(c|v\rangle) = cA|v\rangle$

Examples:

- Identity operator maps every vector in  $\mathcal{H}$  to itself, denoted by  $I_{\mathcal{H}}$ .
- Zero operator maps every vector in  $\mathcal{H}$  to the zero vector, denoted by  $0_{\mathcal{H}}$ .
- For vectors  $|u\rangle, |v\rangle \in \mathcal{H}$ , their outer product is the linear operator in  $\mathcal{H}$  with

$$(|u\rangle\langle v|)|w\rangle = \langle v|w\rangle|u\rangle.$$



## Projections

- Let  $V$  be a closed subspace of  $\mathcal{H}$  and  $|v\rangle \in \mathcal{H}$ . Then there exists unique  $|v_0\rangle \in V$  and  $|v_1\rangle \in V^\perp$  such that

$$|v\rangle = |v_0\rangle + |v_1\rangle.$$

- Vector  $|v_0\rangle$  is called the projection of  $|v\rangle$  onto  $V$ ,  $|v_0\rangle = P_V|v\rangle$ .
- For closed subspace  $V$  of  $\mathcal{H}$ , the operator

$$P_V : \mathcal{H} \rightarrow V, \quad |v\rangle \mapsto P_V|v\rangle$$

is the **projector** onto  $V$ .

## Linear operator in terms of outer product

- We can define a linear operator  $A$  from a vector space  $V$  to  $W$  as  $|w\rangle\langle v|$ , where  $|v\rangle \in V$ ,  $|w\rangle \in W$ .
- For any vector  $|v'\rangle \in W$ ,

$$A|v'\rangle = |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle$$

- The action of  $A$  is to take  $|v'\rangle$  to the scaled version of  $|w\rangle \in W$ . The scaling is based on how much overlap  $|v'\rangle$  has with  $|v\rangle$ .
- In general, if  $|v_i\rangle \in V$  and  $|w_i\rangle \in W$  are chosen to be linearly independent. Let  $B = \sum_i |w_i\rangle\langle v_i|$ . Then

$$B|v'\rangle = \sum_i |w_i\rangle\langle v_i|v'\rangle = \sum_i \langle v_i|v'\rangle|w_i\rangle$$

The term  $\langle v_i|v'\rangle$  denotes the overlap of  $|v'\rangle$  with each of the  $|v_i\rangle$ .

## Pauli operators

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$\sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |1\rangle\langle 0| + |0\rangle\langle 1|$$

$$\sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i|1\rangle\langle 0| - i|0\rangle\langle 1|$$

$$\sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

## Bounded operators

- An operator  $A$  is **bounded** if there is a constant  $c \geq 0$  such that

$$\|A|v\rangle\| \leq c \cdot \| |v\rangle \|$$

for all  $|v\rangle \in \mathcal{H}$ .

- The norm of  $A$  is

$$\|A\| = \inf\{c \geq 0 \mid \|A|v\rangle\| \leq c \cdot \| |v\rangle \| \text{ for all } |v\rangle \in \mathcal{H}\}$$

- $\mathcal{L}(\mathcal{H})$  stands for the set of bounded operators in  $\mathcal{H}$ .

## Operations of operators

$$(A + B)|v\rangle = A|v\rangle + B|v\rangle$$

$$(cA)|v\rangle = c(A|v\rangle)$$

$$(BA)|v\rangle = B(A|v\rangle)$$

## Löwner order

- An operator  $A \in \mathcal{L}(\mathcal{H})$  is **positive** if for all states  $|v\rangle \in \mathcal{H}$ ,

$$\langle v|A|v\rangle \geq 0.$$

- **Löwner order**:  $A \sqsubseteq B$  if and only if  $B - A$  is positive.
- Distance between operators

$$d(A, B) = \sup_{|v\rangle} \||A|v\rangle - B|v\rangle\|$$

## Matrix representation of operators

- Let the dimension of  $\mathcal{H}$  is  $n$ , fix an orthonormal basis  $\{|v_1\rangle, \dots, |v_n\rangle\}$ . An operator on  $\mathcal{H}$  can be represented by the  $n \times n$  complex matrix

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ & \dots & \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

where  $a_{ij} = \langle v_i | A | v_j \rangle$ .

- If  $|v\rangle = \sum_{i=1}^n \alpha_i |v_i\rangle$ , then

$$A|v\rangle = A \begin{bmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \dots \\ \beta_n \end{bmatrix}$$

where  $\beta_i = \sum_{j=1}^n a_{ij} \alpha_j$ .

## Eigenvectors

- An **eigenvector** of an operator  $A$  is a non-zero vector  $|\psi\rangle \in \mathcal{H}$  such that  $A|\psi\rangle = \lambda|\psi\rangle$  for some  $\lambda \in \mathbb{C} \Rightarrow (A - \lambda I)|\psi\rangle = 0$ . If  $|\psi\rangle \neq 0$  then  $\det(A - \lambda I) = 0$ .
- $\lambda$  is called the **eigenvalue** of  $A$  corresponding to  $|\psi\rangle$ .
- The set of eigenvalues of  $A$  is called the **spectrum** of  $A$  and denoted by  $\text{spec}(A)$ .
- For each eigenvalue  $\lambda \in \text{spec}(A)$ , the set

$$\{|\psi\rangle \in \mathcal{H} \mid A|\psi\rangle = \lambda|\psi\rangle\}$$

is a closed subspace of  $\mathcal{H}$  and called the **eigenspace** of  $A$  corresponding to  $\lambda$ .

- the eigenspaces corresponding to different eigenvalues  $\lambda_1 \neq \lambda_2$  are orthogonal.



## Diagonal representation

- If the eigenvectors of the operator  $A$  denoted by  $|k\rangle$  are orthonormal and their corresponding eigenvalues are  $\lambda_k$ , then

$$A = \sum_k \lambda_k |k\rangle\langle k|$$

which is called a **diagonal representation** of the operator  $A$ .

- Take the Pauli matrix  $X$ . From  $\det(X - \lambda I) = 0$  we obtain two eigenvalues  $\lambda_1 = 1$ ,  $\lambda_2 = -1$ . The corresponding eigenvectors are  $|\lambda_1\rangle = \left[ \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \right]^T$  and  $|\lambda_2\rangle = \left[ \frac{1}{\sqrt{2}} \quad -\frac{1}{\sqrt{2}} \right]^T$ , which are orthonormal to each other. The matrix  $X$  itself is not diagonal; however, it can be represented as the diagonal matrix wrt the basis vectors  $|\lambda_1\rangle$  and  $|\lambda_2\rangle$ .

## Adjoint of an operator

- For any operator  $A \in \mathcal{L}(\mathcal{H})$ , there exists a unique operator  $A^\dagger$  such that

$$(A|u\rangle, |v\rangle) = (|u\rangle, A^\dagger|v\rangle).$$

- Operator  $A^\dagger$  is called the **adjoint** of  $A$ .
- If  $A = (a_{ij})_{n \times n}$  then  $A^\dagger = (b_{ij})_{n \times n}$  with  $b_{ij} = a_{ji}^*$ .
- For two operators  $A, B$ ,  $(AB)^\dagger = B^\dagger A^\dagger$
- $(A^\dagger)^\dagger = A$

## Normal operators

- An operator  $A$  is **normal** if it commutes with its adjoint  $A^\dagger$ , i.e.,  $AA^\dagger = A^\dagger A$ .
- Normal operators admit a **spectral decomposition**:

$$A = \sum_k \lambda_k |k\rangle\langle k|$$

where  $\lambda_k$  stands for the eigenvalue corresponding to the eigenvector  $|k\rangle$ .

## Example

- The matrix representation of the Hadamard operator is

$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  has eigenvalues  $\lambda_1 = 1$ ,  $\lambda_2 = -1$ . The corresponding

eigenvectors are  $|\lambda_1\rangle = \begin{bmatrix} \frac{1}{\sqrt{4-2\sqrt{2}}} \\ \frac{1}{\sqrt{2\sqrt{2}}} \end{bmatrix}$  and  $|\lambda_2\rangle = \begin{bmatrix} \frac{1}{\sqrt{4+2\sqrt{2}}} \\ -\frac{1}{\sqrt{2\sqrt{2}}} \end{bmatrix}$

- Verify that

$$\lambda_1|\lambda_1\rangle\langle\lambda_1| + \lambda_2|\lambda_2\rangle\langle\lambda_2| = H$$

## Hermitian operators

- An operator  $M \in \mathcal{L}(\mathcal{H})$  is **Hermitian** if it is self-adjoint:  $M^\dagger = M$ . In physics, a Hermitian operator is called an **observable**.
- If a Hermitian operator is not a degenerate i.e. each eigenvalue corresponds to only one eigenvector, its eigenvectors are orthogonal to each other.
- An operator  $P$  is a **projector**:  $P = P_V$  for some closed subspace  $V$  of  $\mathcal{H}$ , if and only if  $P$  is Hermitian and  $P^2 = P$ .
- All eigenvalues of an observable (i.e. a Hermitian operator)  $M$  are real numbers.

$$M = \sum_{\lambda \in \text{spec}(M)} \lambda P_\lambda$$

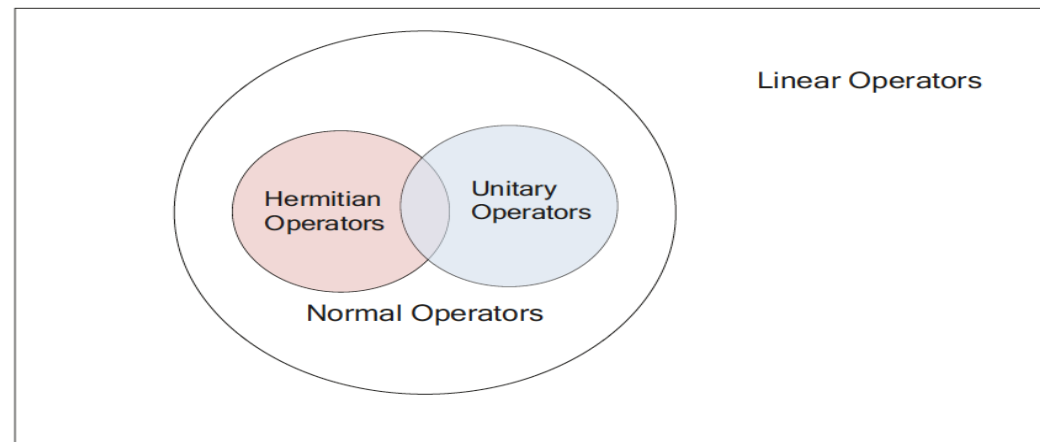
where  $P_\lambda$  is the projector onto the eigenspace corresponding to  $\lambda$ .

## Unitary transformation

- An operator  $U \in \mathcal{L}(\mathcal{H})$  is **unitary** if  $U^\dagger U = U U^\dagger = I_{\mathcal{H}}$ .
- All unitary transformations preserve inner product:

$$(U|u\rangle, U|v\rangle) = \langle u|v\rangle.$$

- If the dimension of  $\mathcal{H}$  is  $n$ , then a unitary operator is represented by an  $n \times n$  unitary matrix  $U$  with  $U^\dagger U = I_n$ .



## Trace of linear operators

The **trace** of a linear operator is the sum of its diagonal entries.

- The sum of the eigenvalues of a linear operator equals its trace.
- $tr(AB) = tr(BA)$
- $tr(A + B) = tr(A) + tr(B)$
- For a linear operator  $A$  and a scalar  $c \in \mathbb{C}$ ,  $tr(cA) = c \times tr(A)$
- The trace of a linear operator is invariant to a unitary similarity transform,  $tr(UAU^\dagger) = tr(A)$

## Tensor product of operators

- Let  $A_i \in \mathcal{L}(\mathcal{H}_i)$  for  $i = 1, \dots, n$ . Their tensor product  $\bigotimes_{i=1}^n A_i = A_1 \otimes \dots \otimes A_n \in \mathcal{L}(\bigotimes_{i=1}^n \mathcal{H}_i)$ :

$$(A_1 \otimes \dots \otimes A_n)|\psi_1, \dots, \psi_n\rangle = A_1|\psi_1\rangle \otimes \dots \otimes A_n|\psi_n\rangle$$

- The tensor product of two matrices

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \vdots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}$$

- $(A \otimes B)^* = A^* \otimes B^*$
- $(A \otimes B)^T = A^T \otimes B^T$
- $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$



## Functions of normal operators

- A normal operator has a spectral decomposition  $A = \sum_i \lambda_i |i\rangle\langle i|$ , where  $\lambda_i$  represents the eigenvalues and  $|i\rangle$  the corresponding eigenvectors.
- A function  $f$  on  $A$  can be defined as  $f(A) = \sum_i f(\lambda_i) |i\rangle\langle i|$
- Example:  $\exp(cA) = \sum_i e^{c\lambda_i} |i\rangle\langle i|$
- Alternatively, if  $A$  is not normal, we use the exponential expansion

$$\exp(cA) = I + cA + \frac{(cA)^2}{2!} + \frac{(cA)^3}{3!} + \dots$$

- If  $A$  is normal,  $(cA)^k = \sum_i (c\lambda_i)^k |i\rangle\langle i|$  and  
 $\exp(cA) = \sum_i (1 + c\lambda_i + \frac{c^2\lambda_i^2}{2!} + \dots) |i\rangle\langle i| = \sum_i e^{c\lambda_i} |i\rangle\langle i|$

## Commutator and anti-commutator operators

- The **commutator** of two linear operators  $M$ ,  $N$  is

$$[M, N] = MN - NM$$

- The **anti-commutator** of two linear operators  $M$ ,  $N$  is

$$\{M, N\} = MN + NM$$

- 

$$MN = \frac{[M, N] + \{M, N\}}{2}$$

# Postulates of Quantum Mechanics

## Postulate 1: Quantum state

- The state space of a closed quantum system is represented by a Hilbert space.
- A pure state of the system is described by a unit vector in its state space.
- Example: 2-dimensional Hilbert space

$$\mathcal{H}_2 = \mathbb{C}^2 = \{\alpha|0\rangle + \beta|1\rangle \mid \alpha, \beta \in \mathbb{C}\}.$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

## Example: Square summable sequences

- The space of square summable sequences:

$$\mathcal{H}_\infty = \left\{ \sum_{n=-\infty}^{\infty} \alpha_n |n\rangle \mid \alpha_n \in \mathbb{C} \text{ for all } n \in \mathbb{Z} \text{ and } \sum_{n=-\infty}^{\infty} |\alpha_n|^2 < \infty \right\}$$

- Inner product:

$$\left( \sum_{n=-\infty}^{\infty} \alpha_n |n\rangle, \sum_{n=-\infty}^{\infty} \beta_n |n\rangle \right) = \sum_{n=-\infty}^{\infty} \alpha_n^* \beta_n.$$

- $\{|n\rangle \mid n \in \mathbb{Z}\}$  is an orthonormal basis,  $\mathcal{H}_\infty$  is infinite-dimensional.

## Postulate 2: Quantum evolution

- Suppose that the states of a closed quantum system at times  $t_0$  and  $t_1$  are  $|\psi_0\rangle$  and  $|\psi_1\rangle$ , respectively. Then there is a unitary operator  $U$  such that

$$|\psi_1\rangle = U|\psi_0\rangle$$

## Schrödinger's equation

- The quantum state of a closed system evolves according to Schrödinger's equation

$$\frac{i\hbar}{2\pi} \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$$

where  $\hbar$  is the Plank's constant and  $H$  is the Hamiltonian of the closed quantum system.

- The Hamiltonian is a Hermitian operator and hence has a spectral decomposition

$$H = \sum_k E_k |E_k\rangle\langle E_k|$$

- The solution to Schrödinger's equation is

$$|\psi(t)\rangle = e^{\frac{-i2\pi H(t-t_0)}{h}} |\psi(t_0)\rangle$$

- The expression  $U(t, t_0) = e^{\frac{-i2\pi H(t-t_0)}{h}}$  is the unitary operator

- If the spectral decomposition of the Hamiltonian operator is

$H = \sum_i E_i |E_i\rangle\langle E_i|$ , then the spectral decomposition of  $U(t, t_0)$  is

$$U(t, t_0) = \sum_k e^{\frac{-i2\pi H(t-t_0)}{h}} |E_k\rangle\langle E_k|$$



## Example: Hadamard transformation

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

$$H|0\rangle = H \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle$$

$$H|1\rangle = H \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = |-\rangle$$

## Example: Translation

- Let  $k$  be an integer. The  $k$ -translation operator  $T_k$  in  $\mathcal{H}_\infty$  is defined by

$$T_k|n\rangle = |n + k\rangle$$

for all  $n \in \mathbb{Z}$ .

- $T_{-1}$  and  $T_1$  move a particle on the line one position to the left and to the right, respectively.

### Postulate 3: Quantum measurement

- A quantum measurement on a system with state Hilbert space  $\mathcal{H}$  is described by a collection  $\{M_m\} \subseteq \mathcal{L}(\mathcal{H})$  of measurement operators satisfying the completeness equation:  $\sum_m M_m^\dagger M_m = I_{\mathcal{H}}$
- The index  $m$  stands for the measurement outcomes that may occur in the experiment.
- If the state of a quantum system is  $|\psi\rangle$  immediately before the measurement, then for each  $m$ ,
  - the probability that result  $m$  occurs in the measurement is

$$p(m) = \|M_m|\psi\rangle\|^2 = \langle\psi|M_m^\dagger M_m|\psi\rangle \quad \text{Born rule}$$

- the state of the system after the measurement with outcome  $m$  is
$$|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}$$

## Completeness equation

- The completeness equation comes from the fact that the sum of the probabilities pertaining to the different measurement operators should sum to 1.

$$\sum_m p(m) = 1$$

$$\Rightarrow \sum_m \langle m | M_m^\dagger M_m | m \rangle = 1$$

$$\Rightarrow \langle m | \sum_m M_m^\dagger M_m | m \rangle = 1$$

The last equation holds only if  $\sum_m M_m^\dagger M_m = I_{\mathcal{H}}$

## Example

- The measurement of a qubit in the computational basis:

$$M_0 = |0\rangle\langle 0|, \quad M_1 = |1\rangle\langle 1|.$$

- If the qubit was in state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  before the measurement, then
  - the probability of obtaining outcome 0 is

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | M_0 | \psi \rangle = |\alpha|^2,$$

the state of the system after the measurement is  $\frac{M_0|\psi\rangle}{\sqrt{p(0)}} = |0\rangle$ .

- the probability of outcome 1 is  $p(1) = |\beta|^2$ , the state after the measurement is  $|1\rangle$ .

## Projective measurements

- An observable  $M$  defines a measurement  $\{P_\lambda \mid \lambda \in \text{spec}(M)\}$ , called a projective measurement.
- Upon measuring a system in state  $|\psi\rangle$ , the probability of obtaining result  $\lambda$

$$p(\lambda) = \langle \psi | P_\lambda | \psi \rangle$$

the state of the system after the measurement is

$$\frac{P_\lambda |\psi\rangle}{\sqrt{p(\lambda)}}$$

- The expectation, i.e. average value, of  $M$  in state  $|\psi\rangle$  is

$$\langle M \rangle_\psi = \sum_{\lambda \in \text{spec}(M)} p(\lambda) \cdot \lambda = \langle \psi | M | \psi \rangle.$$

## General Heisenberg uncertainty principle

- The standard deviation  $\Delta M$  of  $M$  in state  $|\psi\rangle$ :

$$(\Delta M)^2 = \langle M^2 \rangle_\psi - \langle M \rangle_\psi^2$$

- For two measurement operators  $M$  and  $N$ , the standard deviation of their outcomes follows the relation

$$\Delta M \Delta N \geq \frac{1}{2} \| \langle \psi | [M, N] | \psi \rangle \|$$

See P. 71-74 of S. Pattanayak's book for a detailed proof.

## Postulate 4: Composite quantum systems

The state space of a composite quantum system is the tensor product of the state spaces of its components.

- Suppose  $S$  is a quantum system composed by subsystems  $S_1, \dots, S_n$  with state Hilbert space  $\mathcal{H}_1, \dots, \mathcal{H}_n$ .
- If for each  $1 \leq i \leq n$ ,  $S_i$  is in state  $|\psi_i\rangle \in \mathcal{H}_i$ , then  $S$  is in the **product state**  $|\psi_1, \dots, \psi_n\rangle$ .
- A state of the composite system is **entangled** if it is not a product of states of its component systems.



## Examples

- The state space of the system of  $n$  qubits

$$\mathcal{H}_2^{\otimes n} = \mathbb{C}^{2^n} = \left\{ \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \mid \alpha_x \in \mathbb{C} \text{ for all } x \in \{0,1\}^n \right\}.$$

- A two-qubit system can be in a product state like  $|00\rangle, |0\rangle|+\rangle$ .
- It may also be in an entangled state like the Bell states or the EPR (Einstein-Podolsky-Rosen) pairs.

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), & |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

## Implementing a general measurement by a projective measurement

- Let  $M = \{M_m\}$  be a quantum measurement in Hilbert space  $\mathcal{H}$ .
- Introduce a new Hilbert space  $\mathcal{H}_M = \text{span} \{|m\rangle\}$  used to record the possible outcomes of  $M$ .
- Choose a fixed state  $|0\rangle \in \mathcal{H}_M$ . Define unitary operator in  $\mathcal{H}_M \otimes \mathcal{H}$ :

$$U_m(|0\rangle|\psi\rangle) = \sum_m |m\rangle|\psi\rangle$$

- Define a projective measurement  $\bar{M} = \{|m\rangle\langle m| \otimes I_{\mathcal{H}}\}$  in  $\mathcal{H}_M \otimes \mathcal{H}$ .

## Implementing a general measurement by a projective measurement

- Then  $M$  is realized by the projective measurement  $\overline{M}$  together with the unitary operator  $U_M$ .
- For any pure state  $|\psi\rangle \in \mathcal{H}$ ,
  - When we perform measurement  $M$  on  $|\psi\rangle$ , the probability of outcome  $m$  is denoted by  $p_M(m)$ , the post-measurement state corresponding to  $m$  is  $|\psi_m\rangle$ .
  - When we perform measurement  $\overline{M}$  on  $|\overline{\psi}\rangle = U_M(|0\rangle|\psi\rangle)$ , the probability of outcome  $m$  is denoted by  $p_{\overline{M}}(m)$ , the post-measurement state corresponding to  $m$  is  $|\overline{\psi}_m\rangle$ .
- For each  $m$ , we have

$$\begin{aligned} p_{\overline{M}}(m) &= p_M(m) \\ |\overline{\psi}_m\rangle &= |m\rangle|\psi_m\rangle \end{aligned}$$

## Ensembles

- The state of a quantum system is not completely known: it is in one of a number of pure states  $|\psi_i\rangle$ , with respective probabilities  $p_i$ , where  $|\psi_i\rangle \in \mathcal{H}$ ,  $p_i \geq 0$  for each  $i$ ,  $\sum_i p_i = 1$ .
- We call  $\{(|\psi_i\rangle, p_i)\}$  an ensemble of pure states or a mixed state
- It can be represented by the density operator

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$$

- A pure state  $|\psi\rangle$  may be seen as a special mixed state  $\{(|\psi\rangle, 1)\}$ . Its density operator is  $\rho = |\psi\rangle \langle \psi|$ .

## Density operators

- The trace  $tr(A)$  of operator  $A \in \mathcal{L}(\mathcal{H})$ :

$$tr(A) = \sum_i \langle \psi_i | A | \psi_i \rangle$$

where  $\{|\psi_i\rangle\}$  is an orthonormal basis of  $\mathcal{H}$ .

- A density operator  $\rho$  is a positive operator with  $tr(\rho) = 1$ .
- The operator  $\rho$  defined by any ensemble  $\{(|\psi_i\rangle, p_i)\}$  is a density operator. Conversely, any density operator  $\rho$  is defined by an (but unnecessarily unique) ensemble  $\{(|\psi_i\rangle, p_i)\}$ .
- If  $\rho$  is a pure state,  $tr(\rho^2) = 1$ ; if it is a mixed state,  $tr(\rho^2) < 1$ .
- The density operator of  $n$  quantum systems with density operators  $\rho_1, \dots, \rho_n$  can be expressed as  $\rho = \rho_1 \otimes \dots \otimes \rho_n$ .

## Postulates of quantum mechanics in the language of density operators

- A closed quantum system from time  $t_0$  to  $t$  is described by unitary operator  $U$  depending on  $t_0$  and  $t$ :  $|\psi\rangle = U|\psi_0\rangle$ .
- If the system is in mixed state  $\rho_0, \rho$  at times  $t_0$  and  $t$ , respectively, then  $\rho = U\rho_0U^\dagger$ .
- If the state of a quantum system was  $\rho$  before measurement  $M_m$  is performed, then the probability that result  $m$  occurs is

$$p(m) = \text{tr}(M_m^\dagger M_m \rho)$$

and the system after the measurement is

$$\rho_m = \frac{M_m \rho M_m^\dagger}{p(m)}$$

## Reduced density operators

- We often need to characterize the state of a subsystem of a quantum system.
- It is possible that a composite system is in a pure state, but some of its subsystems must be seen as in a mixed state.
- Let  $S$  and  $T$  be quantum systems whose state Hilbert spaces are  $\mathcal{H}_S$  and  $\mathcal{H}_T$ , respectively.
- The partial trace over system  $T$ :

$$\begin{aligned} \text{tr}_T &: \mathcal{L}(\mathcal{H}_S \otimes \mathcal{H}_T) \rightarrow \mathcal{L}(\mathcal{H}_S) \\ \text{tr}_T(|\psi\rangle\langle\phi| \otimes |\theta\rangle\langle\xi|) &= \langle\xi|\theta\rangle \cdot |\psi\rangle\langle\phi| \end{aligned}$$

- Let  $\rho$  be a density operator in  $\mathcal{H}_S \otimes \mathcal{H}_T$ . Its reduced density operator for system  $S$ :  $\rho_S = \text{tr}_T(\rho)$ .

## The Bell state

- The density operator of the Bell state  $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  is

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

- $\rho_A = \text{tr}_B(\rho_{AB}) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2}$
- $\text{tr}(\rho_A^2) = \text{tr}(\frac{I}{4}) = \frac{1}{2} < 1$
- Thus qubit A is in the mixed state, so is qubit B. The joint state of the two qubits is in a pure state, while the individual qubits are in a mixed state!



## Super-operators

- Unitary transformations are suited to describe the dynamics of closed quantum systems.
- For open quantum systems that interact with the outside environment, we need a general notion of quantum operation.
- A linear operator in vector space  $\mathcal{L}(\mathcal{H})$  is called a **super-operator** in  $\mathcal{H}$ .
- Let  $\mathcal{H}$  and  $\mathcal{K}$  be Hilbert spaces. For any super-operators  $\mathcal{E}$  in  $\mathcal{H}$  and  $\mathcal{F}$  in  $\mathcal{K}$ , their tensor product  $\mathcal{E} \otimes \mathcal{F}$  is the super-operator in  $\mathcal{H} \otimes \mathcal{K}$ : for each  $C = \sum_i \alpha_i (A_i \otimes B_i)$ ,  $A_i \in \mathcal{L}(\mathcal{H})$ ,  $B_i \in \mathcal{L}(\mathcal{K})$ ,

$$(\mathcal{E} \otimes \mathcal{F})(C) = \sum_i \alpha_i (\mathcal{E}(A_i) \otimes \mathcal{F}(B_i))$$

## Quantum operations

- A quantum operation in a Hilbert space  $\mathcal{H}$  is a super-operator in  $\mathcal{H}$  satisfying:
  1.  $tr(\mathcal{E}(\rho)) \leq tr(\rho) = 1$  for each density operator  $\rho$  in  $\mathcal{H}$ ;
  2. (Complete positivity) For any extra Hilbert space  $\mathcal{H}_R$ ,  $(\mathcal{I}_R \otimes \mathcal{E})(A)$  is positive provided  $A$  is a positive operator on  $\mathcal{H}_R \otimes \mathcal{H}$ , where  $\mathcal{I}_R$  is the identity operator in  $\mathcal{L}(\mathcal{H}_R)$ .
  3. Let the states of a system at times  $t_0$  and  $t$  are  $\rho_0$  and  $\rho$ , respectively. Then they must be related to each other by a super-operator  $\mathcal{E}$  depending only on the times  $t_0$  and  $t$ :

$$\rho = \mathcal{E}(\rho_0)$$

## Examples

- Let  $U$  be a unitary transformation in a Hilbert space  $\mathcal{H}$ . Define  $\mathcal{E}(\rho) = U\rho U^\dagger$  for every density operator  $\rho$ . Then  $\mathcal{E}$  is a quantum operation.
- Let  $M = \{M_m\}$  be a quantum measurement in  $\mathcal{H}$ .
  1. For each  $m$ , if for any system state  $\rho$  before measurement, define  $\mathcal{E}_m(\rho) = p_m\rho_m = M_m\rho M_m^\dagger$  where  $p_m$  is the probability of outcome  $m$  and  $\rho_m$  is the post-measurement state corresponding to  $m$ , then  $\mathcal{E}_m$  is a quantum operation.
  2. For any system  $\rho$  before measurement, the post-measurement state is

$$\mathcal{E}(\rho) = \sum_m \mathcal{E}_m(\rho) = \sum_m M_m\rho M_m^\dagger$$

whenever the measurement outcomes are ignored. Then  $\mathcal{E}$  is a quantum operation.

## Kraus Theorem

The following statements are equivalent:

1.  $\mathcal{E}$  is a quantum operation in a Hilbert space  $\mathcal{H}$ ;
2. (System-environment model) There is an environment system  $E$  with state Hilbert space  $\mathcal{H}_E$ , and a unitary transformation  $U$  in  $\mathcal{H}_E \otimes \mathcal{H}$  and a projector  $P$  onto some closed subspace of  $\mathcal{H}_E \otimes \mathcal{H}$  such that

$$\mathcal{E}(\rho) = \text{tr}_E [PU(|e_0\rangle\langle e_0| \otimes \rho)U^\dagger P]$$

for all density operator  $\rho$  in  $\mathcal{H}$ , where  $|e_0\rangle$  is a fixed state in  $\mathcal{H}_E$ ;

3. (Kraus operator-sum representation) There exists a finite or countably infinite set of operators  $\{E_i\}$  in  $\mathcal{H}$  such that  $\sum_i E_i^\dagger E_i \subseteq I$  and







$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

for all density operators  $\rho$  in  $\mathcal{H}$ . We write  $\mathcal{E} = \sum_i E_i \circ E_i^\dagger$ .

# Quantum Circuits

## Single qubit gates

Some common single qubit gates

Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli- $X$		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli- $Y$		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli- $Z$		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

## Rotation operators

Rotation operators about the  $\hat{x}$ ,  $\hat{y}$  and  $\hat{z}$  axes.

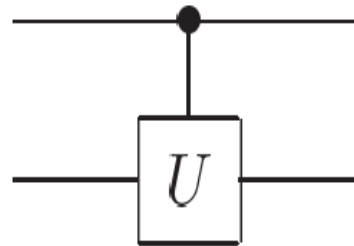
$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} X = \begin{bmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Y = \begin{bmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}$$

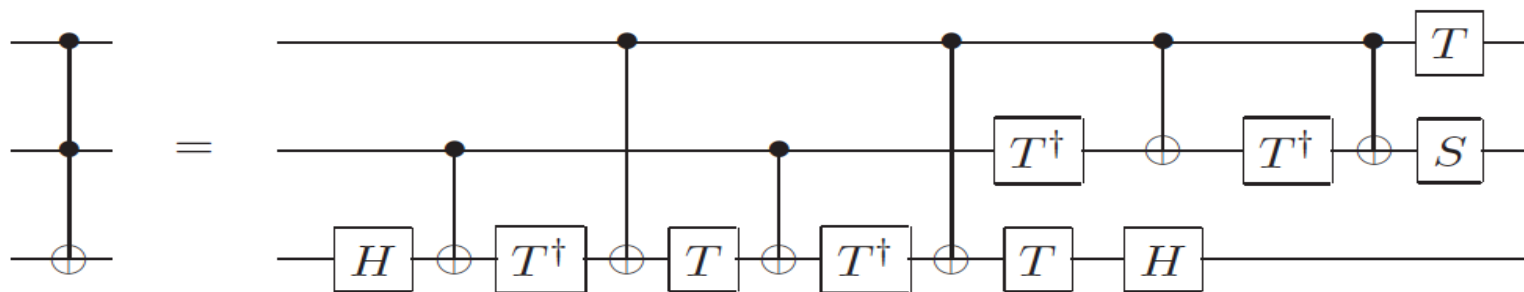
$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

## Controlled gates

- A controlled-U operation:  $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$

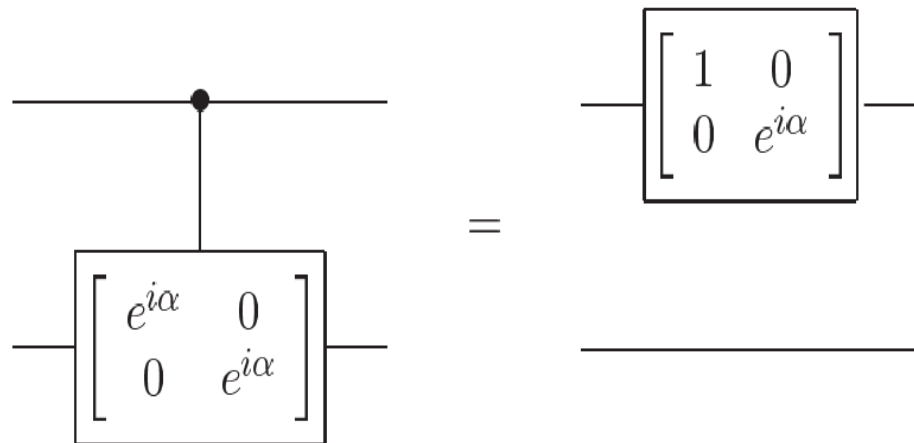
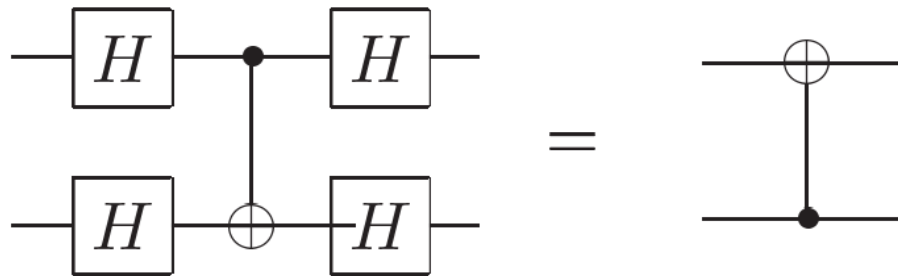


- Toffoli gate





## Circuit equivalence

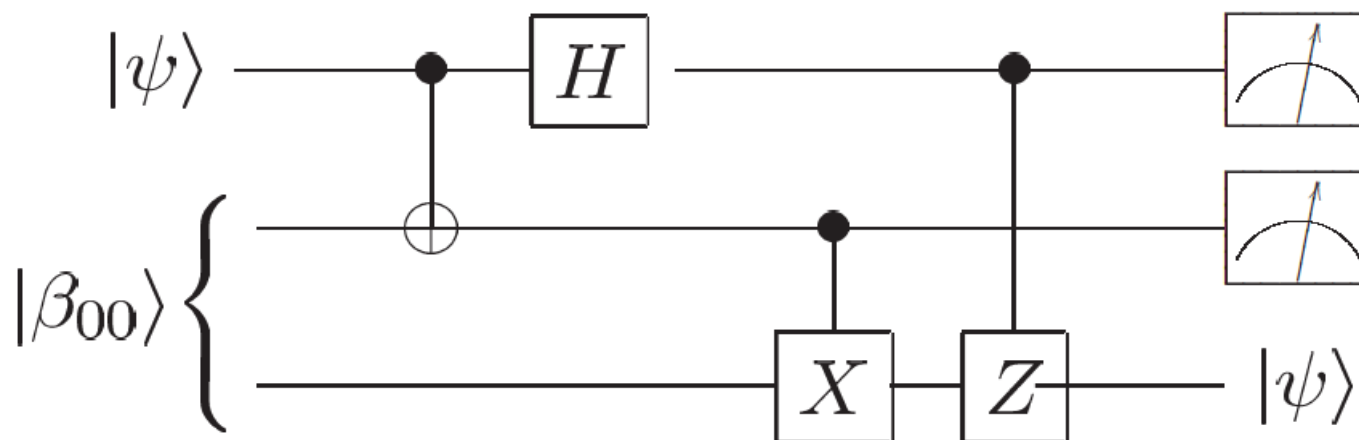


## Universal gate sets

- Single qubit and CNOT gates can be used to implement an arbitrary unitary operation on  $n$  qubits, and therefore are universal for quantum computation.
- The *standard set* of universal gates:  $\{H, S, T, CNOT\}$
- Another universal gate set:  $\{H, S, CNOT, Toffoli\}$
- Approximating arbitrary unitary gates is generically hard: an arbitrary unitary operation  $U$  on  $n$  qubits may be approximated to within a distance  $\epsilon$  using  $O(n^2 4^n \log^c(n^2 4^n / \epsilon))$  gates.

## Principle of deferred measurement

- **Principle of deferred measurement:** Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.
- Teleportation with measurements at the end:



# Quantum Programming

## Syntax of a purely quantum language

1. Assume a countably infinite set  $qVar$  of quantum variables, ranged over by  $q, q', q_0$  etc.
2. Each quantum variable  $q \in qVar$  has a type  $\mathcal{H}_q$  (a Hilbert space).
3. For simplicity, we consider two basic types:

$$\mathbf{Bool} = \mathcal{H}_2, \quad \mathbf{Int} = \mathcal{H}_\infty$$

4. A quantum register is a finite sequence  $\bar{q} = q_1, \dots, q_n$  of quantum variables. Its state Hilbert space:

$$\mathcal{H}_{\bar{q}} = \bigotimes_{i=1}^n \mathcal{H}_{q_i}$$

## Syntax of a purely quantum language

$$\begin{aligned} S \quad ::= & \quad \mathbf{skip} \mid q := |0\rangle \mid U[\bar{q}] \mid S_1; S_2 \\ & \mid \mathbf{if} (\square m \cdot M[\bar{q}] = m \rightarrow S_m) \\ & \mid \mathbf{while} M[\bar{q}] = 1 \mathbf{do} S \end{aligned}$$

## Notations

- A positive operator  $\rho$  is a **partial density operator** if  $tr(\rho) \leq 1$ .
- Write  $\mathcal{D}(\mathcal{H})$  for the set of partial density operators in  $\mathcal{H}$ .
- Write  $\mathcal{H}_{all}$  for the tensor product of the state Hilbert space of all quantum variables:  $\mathcal{H}_{all} = \otimes_{q \in qVar} \mathcal{H}_q$
- Let  $\bar{q} = q_1, \dots, q_n$  be a quantum register. An operator in the state Hilbert space  $\mathcal{H}_{\bar{q}}$  has a cylindrical extension  $A \otimes I$  in  $\mathcal{H}_{all}$ .
- Write **nil** for the empty program, i.e., successful termination.
- A configuration is a pair  $\langle S, \rho \rangle$ , where
  1.  $S$  is a quantum program or **nil**;
  2.  $\rho \in \mathcal{D}(\mathcal{H}_{all})$  denotes the (global) state of quantum variables.
- Transition between quantum configurations:  $\langle S, \rho \rangle \rightarrow \langle S', \rho' \rangle$

## Operational semantics

$$\frac{}{\langle \mathbf{skip}, \rho \rangle \rightarrow \langle \mathbf{nil}, \rho \rangle}$$

$$\frac{}{\langle q := |0\rangle, \rho \rangle \rightarrow \langle \mathbf{nil}, \rho' \rangle}$$

$$\text{where } \rho' = \begin{cases} |0\rangle_q \langle 0| \rho |0\rangle_q \langle 0| + |0\rangle_q \langle 1| \rho |1\rangle_q \langle 0| & \text{if } \text{type}(q) = \mathbf{Bool} \\ \sum_{n=-\infty}^{\infty} |0\rangle \langle n| \rho |n\rangle_q \langle 0| & \text{if } \text{type}(q) = \mathbf{Int} \end{cases}$$

$$\frac{}{\langle U[\bar{q}], \rho \rangle \rightarrow \langle \mathbf{nil}, U \rho U^\dagger \rangle}$$

$$\frac{}{\langle S_1, \rho \rangle \rightarrow \langle S'_1, \rho' \rangle}$$

$$\frac{}{\langle S_2, \rho \rangle \rightarrow \langle S'_2, \rho' \rangle}$$

$$\frac{}{\langle S_1; S_2, \rho \rangle \rightarrow \langle S'_1; S_2, \rho' \rangle}$$

$$\frac{}{\langle \mathbf{nil}; S_2, \rho \rangle \rightarrow \langle S'_2, \rho' \rangle}$$



## Operational semantics

---

$$\langle \mathbf{if} (\square m \cdot M[\bar{q}] = m \rightarrow S_m), \rho \rangle \rightarrow \langle S_m, M_m \rho M_m^\dagger \rangle$$

for each possible outcome  $m$  of measurement  $M = \{M_m\}$

---

$$\langle \mathbf{while} M[\bar{q}] = 1 \mathbf{do} S, \rho \rangle \rightarrow \langle \mathbf{nil}, M_0 \rho M_0^\dagger \rangle$$

---

$$\langle \mathbf{while} M[\bar{q}] = 1 \mathbf{do} S, \rho \rangle \rightarrow \langle S; (\mathbf{while} M[\bar{q}] = 1 \mathbf{do} S), M_1 \rho M_1^\dagger \rangle$$

## Computation

Let  $S$  be a quantum program and  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ .

1. A transition sequence of  $S$  starting in  $\rho$  is a finite or infinite sequence of configurations

$$\langle S, \rho \rangle \rightarrow \langle S_1, \rho_1 \rangle \rightarrow \dots \rightarrow \langle S_n, \rho_n \rangle \rightarrow \dots$$

such that  $\rho_n \neq 0$  for all  $n$  except for the last  $n$  if the sequence is finite.

2. If a sequence cannot be extended, then it is a **computation** of  $S$  starting in  $\rho$ .
  - If a computation is finite with the last configuration  $\langle \mathbf{nil}, \rho' \rangle$ , then it terminates in  $\rho'$ .
  - If it is infinite, then it diverges.

## Denotational semantics

1. If a configuration  $\langle S', \rho' \rangle$  can be reached from  $\langle S, \rho \rangle$  in  $n$  steps, then we write  $\langle S, \rho \rangle \rightarrow^n \langle S', \rho' \rangle$ .
2. Write  $\rightarrow^*$  for the reflexive and transitive closure of  $\rightarrow$ .
3. Let  $S$  be a quantum program. Its semantic function

$$\llbracket S \rrbracket : \mathcal{D}(\mathcal{H}_{all}) \rightarrow \mathcal{D}(\mathcal{H}_{all})$$

$$\llbracket S \rrbracket(\rho) = \sum \{ |\rho' \rangle \mid \langle S, \rho \rangle \rightarrow^* \langle \mathbf{nil}, \rho' \rangle \}$$

## Structural definition

1.  $\llbracket \mathbf{skip} \rrbracket(\rho) = \rho$

2. If  $type(q) = \mathbf{Bool}$ , then

$$\llbracket q := |0\rangle \rrbracket(\rho) = |0\rangle_q \langle 0| \rho |0\rangle_q \langle 0| + |0\rangle_q \langle 1| \rho |1\rangle_q \langle 0|$$

3. If  $type(q) = \mathbf{Int}$ , then

$$\llbracket q := |0\rangle \rrbracket(\rho) = \sum_{n=-\infty}^{\infty} |0\rangle \langle n| \rho |n\rangle_q \langle 0|$$

4.  $\llbracket U[\bar{q}] \rrbracket(\rho) = U \rho U^\dagger$

5.  $\llbracket S_1; S_2 \rrbracket(\rho) = \llbracket S_2 \rrbracket(\llbracket S_1 \rrbracket(\rho))$

6.  $\llbracket \mathbf{if} (\square m \cdot M[\bar{q}] = m \rightarrow S_m) \rrbracket(\rho) = \sum_m \llbracket S_m \rrbracket(M_m \rho M_m^\dagger)$

## Basic lattice theory

1. A **partial order** is a pair  $(X, \sqsubseteq)$ , where  $X$  is a nonempty set and  $\sqsubseteq$  is a binary relation on  $X$  satisfying
  - Reflexivity:  $x \sqsubseteq x$  for all  $x \in X$ ;
  - Antisymmetry:  $x \sqsubseteq y$  and  $y \sqsubseteq x$  imply  $x = y$  for all  $x, y \in X$ ;
  - Transitivity:  $x \sqsubseteq y$  and  $y \sqsubseteq z$  imply  $x \sqsubseteq z$  for all  $x, y, z \in X$ .
2. Let  $(X, \sqsubseteq)$  be a partial order.
  - An element  $x \in X$  is the least element of  $X$  if  $x \sqsubseteq y$  for all  $y \in X$ .  
The least element is denoted by  $0$ .
  - An element  $x \in X$  is an upper bound of a subset  $Y \subseteq X$  if  $y \sqsubseteq x$  for all  $y \in Y$ .
  - $x$  is the least upper bound of  $Y$ , written  $x = \bigsqcup Y$  if
    - $x$  is an upper bound of  $Y$
    - for any upper bound  $x'$  of  $Y$ ,  $x \sqsubseteq x'$ .

## Basic lattice theory

1. A complete partial order (CPO) is a partial order  $(X, \sqsubseteq)$  if for any increasing sequence  $\{x_n\}$

$$x_0 \sqsubseteq x_1 \sqsubseteq \dots$$

its least upper bound  $\bigsqcup_{n=0}^{\infty} x_n$  exists. A CPO with bottom is a CPO with a least element.

2. Let  $(X, \sqsubseteq)$  be a CPO. A function  $f$  on  $X$  is continuous if

$$f\left(\bigsqcup_n x_n\right) = \bigsqcup_n f(x_n)$$

for any increasing sequence  $\{x_n\}$  in  $X$ .

## Knaster-Tarski Theorem

Let  $(X, \sqsubseteq)$  be a CPO with bottom and function  $f : X \rightarrow X$  is continuous.  
Then  $f$  has the least fixed point

$$\mu.f = \bigsqcup_{n=0}^{\infty} f^n(0)$$

where  $f^0 = 0$  and  $f^{n+1}(0) = f(f^n(0))$  for  $n \geq 0$ .

## Domain of quantum operations

- Domain of partial density operators:  $(\mathcal{D}(\mathcal{H}), \sqsubseteq)$  is a CPO with the zero operator  $0_{\mathcal{H}}$  as its least element.
- Domain of quantum operations:
  - Each quantum operation in a Hilbert space  $\mathcal{H}$  is a continuous function on  $(\mathcal{D}(\mathcal{H}), \sqsubseteq)$ .
  - Write  $\mathcal{QO}(\mathcal{H})$  for the set of quantum operations in Hilbert space  $\mathcal{H}$ .
  - The Löner order between operators induces a partial order between quantum operations: for any  $\mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$ ,

$$\mathcal{E} \sqsubseteq \mathcal{F} \Leftrightarrow \mathcal{E}(\rho) \sqsubseteq \mathcal{F}(\rho) \text{ for all } \rho \in \mathcal{D}(\mathcal{H})$$

- $(\mathcal{QO}(\mathcal{H}), \sqsubseteq)$  is a CPO.



## Syntactic approximation

- **abort** denotes a quantum program such that

$$\llbracket \mathbf{abort} \rrbracket(\rho) = 0_{\mathcal{H}_{all}} \text{ for all } \rho \in \mathcal{D}(\mathcal{H})$$

- Consider a quantum loop

$$\mathit{While} \equiv \mathbf{while} \ M[\bar{q}] = 1 \ \mathbf{do} \ S.$$

- For any integer  $k \geq 0$ , the  $k$ -th syntactic approximation  $\mathit{while}^k$  of  $\mathit{while}$ :

$$\mathit{while}^0 = \mathbf{abort}$$

$$\mathit{while}^{k+1} = \mathbf{if} \ (M[\bar{q}] = 0 \rightarrow \mathbf{skip} \\ \square \ M[\bar{q}] = 1 \rightarrow S; \mathit{while}^k)$$

## Denotation of loops

- Semantic function of loops:

$$\llbracket while \rrbracket = \bigsqcup_{k=0}^{\infty} \llbracket while^k \rrbracket,$$

where  $\bigsqcup$  stands for the supremum of a sequence of quantum operations in the CPO  $(\mathcal{QO}(\mathcal{H}_{all}), \sqsubseteq)$ .

- For any  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ :

$$\llbracket while \rrbracket(\rho) = M_0 \rho M_0^\dagger + \llbracket while \rrbracket(\llbracket S \rrbracket(M_1 \rho M_1^\dagger)).$$

## Termination probabilities

- For any quantum program  $S$  and all partial density operators  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ ,

$$tr(\llbracket S \rrbracket(\rho)) \leq tr(\rho).$$

- $tr(\llbracket S \rrbracket(\rho))$  is the probability that program  $S$  terminates when starting in state  $\rho$ .

## Quantum predicates

- A quantum predicate should be a physical observable.
- A quantum predicate in a Hilbert space  $\mathcal{H}$  is a Hermitian operator  $M$  in  $\mathcal{H}$  with all its eigenvalues lying within the unit interval  $[0, 1]$ .
- The set of predicates in  $\mathcal{H}$  is denoted  $\mathcal{P}(\mathcal{H})$ .
- Satisfaction of quantum predicates:  $\text{tr}(M\rho)$  may be interpreted as the degree to which quantum state  $\rho$  satisfies quantum predicate  $M$ .
- Let  $M$  be a Hermitian operator in  $\mathcal{H}$ . The following statements are equivalent:
  1.  $M \in \mathcal{P}(\mathcal{H})$  is a quantum predicate
  2.  $0_{\mathcal{H}} \sqsubseteq M \sqsubseteq I_{\mathcal{H}}$
  3.  $0 \leq \text{tr}(M\rho) \leq 1$  for all density operators  $\rho \in \mathcal{H}$

## Quantum predicates

**Lemma** For any observables  $M, N$ , the following two statements are equivalent:

1.  $M \sqsubseteq N$
2.  $\text{tr}(M\rho) \leq \text{tr}(N\rho)$  for all density operators  $\rho \in \mathcal{H}$

**Lemma** The set  $\mathcal{P}(\mathcal{H}), \sqsubseteq$  of quantum predicates with the Löwner partial order is a CPO.

## Quantum preconditions

- Let  $M, N \in \mathcal{P}(\mathcal{H})$  be quantum predicates,  $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$  a quantum operation. Then  $M$  is a **precondition** of  $N$  w.r.t.  $\mathcal{E}$ , written  $\{M\}\mathcal{E}\{N\}$ , if

$$\text{tr}(M\rho) \leq \text{tr}(N\mathcal{E}(\rho))$$

for all density operators  $\rho \in \mathcal{H}$ .

- Intuition: a probabilistic version of implication relation — if state  $\rho$  satisfies predicate  $M$ , then the state after transformation  $\mathcal{E}$  from  $\rho$  satisfies predicate  $N$ .

## Quantum weakest preconditions

Let  $M \in \mathcal{P}(\mathcal{H})$  be a quantum predicate,  $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$  a quantum operation. The weakest precondition of  $M$  w.r.t.  $\mathcal{E}$  is a quantum predicate  $wp(\mathcal{E})(M)$  satisfying

1.  $\{wp(\mathcal{E})(M)\}\mathcal{E}\{M\}$
2. for all quantum predicates  $N$ ,  $\{N\}\mathcal{E}\{M\}$  implies  $N \sqsubseteq wp(\mathcal{E})(M)$ .

## Characterisation of quantum weakest preconditions

Using Kraus operators:

Let  $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$  be represented by the set  $\{E_i\}$  of operators

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

Then for each predicate  $M \in \mathcal{P}(\mathcal{H})$ :

$$wp(\mathcal{E})(M) = \sum_i E_i^\dagger M E_i.$$



## Characterisation of quantum weakest preconditions

Using system-environment model:

If quantum operation  $\mathcal{E}$  is given by

$$\mathcal{E}(\rho) = \text{tr}_E(PU(|e_0\rangle\langle e_0| \otimes \rho)U^\dagger P)$$

then

$$wp(\mathcal{E})(M) = \langle e_0|U^\dagger P(M \otimes I_E)PU|e_0\rangle$$

## Schrödinger-Heisenberg duality

- Denotationally, a quantum program is a forward state transformer  $\mathcal{E}$ :

$$\begin{aligned}\mathcal{E} & : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}), \\ & \rho \mapsto \mathcal{E}(\rho) \text{ for each } \rho \in \mathcal{D}(\mathcal{H})\end{aligned}$$

- A weakest precondition defines a backward quantum predicate transformer:

$$\begin{aligned}wp(\mathcal{E}) & : \mathcal{P}(\mathcal{H}) \rightarrow \mathcal{P}\mathcal{H}, \\ & M \mapsto wp(\mathcal{E})(M) \text{ for each } M \in \mathcal{P}(\mathcal{H})\end{aligned}$$

## Schrödinger-Heisenberg duality

Let  $\mathcal{E}$  be a quantum operation mapping density operators to themselves,  $\mathcal{E}^*$  an operator mapping Hermitian operators to themselves. If for each density operator  $\rho$ , Hermitian operator  $M$ ,

$$(Duality) \quad tr(M\mathcal{E}(\rho)) = tr(\mathcal{E}^*(M)\rho)$$

then  $\mathcal{E}$  and  $\mathcal{E}^*$  are (Schrödinger-Heisenberg dual).

$$\begin{array}{ccc} \rho & \models & \mathcal{E}^*(M) \\ \mathcal{E} \downarrow & & \uparrow \mathcal{E}^* \\ \mathcal{E}(\rho) & \models & M \end{array}$$

Any quantum operation  $\mathcal{E} \in \mathcal{QO}(\mathcal{H})$  and its weakest precondition  $wp(\mathcal{E})$  are dual to each other.

## Basic properties of quantum weakest preconditions

Let  $\lambda \geq 0$ ,  $\mathcal{E}, \mathcal{F} \in \mathcal{QO}(\mathcal{H})$ , let  $\{\mathcal{E}_n\}$  be an increasing sequence in  $\mathcal{QO}(\mathcal{H})$ .

1.  $wp(\lambda \cdot \mathcal{E}) = \lambda \cdot wp(\mathcal{E})$  provided  $\lambda \cdot \mathcal{E} \in \mathcal{QO}(\mathcal{H})$ ;
2.  $wp(\mathcal{E} + \mathcal{F}) = wp(\mathcal{E}) + \wp(\mathcal{F})$  provided  $\mathcal{E} + \mathcal{F} \in \mathcal{QO}(\mathcal{H})$ ;
3.  $wp(\mathcal{E} \circ \mathcal{F}) = wp(\mathcal{F}) \circ wp(\mathcal{E})$ ;
4.  $wp(\bigsqcup_{n=0}^{\infty} \mathcal{E}_n) = \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)$ , with the later being defined as follows:

$$\left( \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n) \right)(M) := \bigsqcup_{n=0}^{\infty} wp(\mathcal{E}_n)(M)$$

## Floyd-Hoare logic

A correctness formulas is a statement of the form

$$\{P\}S\{Q\}$$

where

- $S$  is a quantum program
- $P, Q \in \mathcal{P}(\mathcal{H}_{all})$  are quantum predicates in  $\mathcal{H}_{all}$
- $P$  is called the precondition,  $Q$  the postcondition.

## Partial and total correctness

- **Partial correctness:** If a state satisfies precondition  $P$ , by executing  $S$ , either the program does not terminate, or it terminates in a state satisfying the postcondition  $Q$ .
- **Total correctness:** If a state satisfies precondition  $P$ , by executing  $S$ , the program must terminate and it terminates in a state satisfying the postcondition  $Q$ .

## Partial and total correctness

- The Hoare triple  $\{P\}S\{Q\}$  is valid in the sense of total correctness, written

$$\models_{tot} \{P\}S\{Q\}$$

if

$$tr(P\rho) \leq tr(Q\llbracket S \rrbracket(\rho))$$

for all  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ , where  $\llbracket S \rrbracket$  is the semantics of  $S$ .

- The Hoare triple  $\{P\}S\{Q\}$  is valid in the sense of partial correctness, written

$$\models_{par} \{P\}S\{Q\}$$

if

$$tr(P\rho) \leq tr(Q\llbracket S \rrbracket(\rho)) + (tr(\rho) - tr(\llbracket S \rrbracket(\rho)))$$

for all  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ .

## Basic properties of correctness

- If  $\models_{tot} \{P\}S\{Q\}$  then  $\models_{par} \{P\}S\{Q\}$ .
- For any quantum program  $S$ , and predicates  $P, Q \in \mathcal{P}(\mathcal{H}_{all})$ ,

$$\models_{tot} \{0_{\mathcal{H}_{all}}\}S\{Q\}, \quad \models_{par} \{P\}S\{I_{\mathcal{H}_{all}}\}.$$

- (Linearity) For any  $P_1, P_2, Q_1, Q_2 \in \mathcal{P}(\mathcal{H}_{all})$  and  $\lambda_1, \lambda_2 \geq 0$  with  $\lambda_1 P_1 + \lambda_2 P_2, \lambda_1 Q_1 + \lambda_2 Q_2 \in \mathcal{P}(\mathcal{H}_{all})$ , if

$$\models_{tot} \{P_i\}S\{Q_i\} \quad (i = 1, 2)$$

then

$$\models_{tot} \{\lambda_1 P_1 + \lambda_2 P_2\}S\{\lambda_1 Q_1 + \lambda_2 Q_2\}$$

The same holds for partial correctness if  $\lambda_1 + \lambda_2 = 1$ .



## Weakest (liberal) preconditions

- Let  $S$  be a quantum program,  $P \in \mathcal{P}(\mathcal{H}_{all})$  a quantum predicate in  $\mathcal{H}_{all}$ .
  1. The **weakest precondition** of  $S$  w.r.t.  $P$  is the quantum predicate  $wp.S.P \in \mathcal{P}(\mathcal{H}_{all})$  satisfying:
    - $\models_{tot} \{wp.S.P\}S\{P\}$ ;
    - if quantum predicate  $Q \in \mathcal{P}(\mathcal{H}_{all})$  satisfies  $\models_{tot} \{Q\}S\{P\}$  then  $Q \sqsubseteq wp.S.P$ .
  2. The **weakest liberal precondition** of  $S$  w.r.t.  $P$  is the quantum predicate  $wlp.S.P \in \mathcal{P}(\mathcal{H}_{all})$  satisfying:
    - $\models_{par} \{wlp.S.P\}S\{P\}$ ;
    - if quantum predicate  $Q \in \mathcal{P}(\mathcal{H}_{all})$  satisfies  $\models_{par} \{Q\}S\{P\}$  then  $Q \sqsubseteq wp.S.P$ .
- Equivalence of semantic and syntactic definitions  
 $wp.S.P = wp(\llbracket S \rrbracket)(P)$ .

## Structural representation of weakest liberal preconditions

- $wlp.\text{skip}.P = P$ .
- If  $\text{type}(q) = \mathbf{Bool}$ , then

$$wlp.(q := |0\rangle).P = |0\rangle_q \langle 0|P|0\rangle_q \langle 0| + |1\rangle_q \langle 0|P|0\rangle_q \langle 1|$$

If  $\text{type}(q) = \mathbf{Int}$ , then  $wlp.(q := |0\rangle).P = \sum_{n=-\infty}^{\infty} |n\rangle_q \langle 0|P|0\rangle_q \langle n|$

- $wlp.(U[\bar{q}]).P = U^\dagger P U$ .
- $wlp.(S_1; S_2).P = wlp.S_1.(wlp.S_2.P)$ .
- $wlp.(\mathbf{if} \square m \cdot M[\bar{q}] = m \rightarrow S_m).P = \sum_m M_m^\dagger (wlp.S_m.P) M_m$ .
- $wlp.(\mathbf{while} M[\bar{q}] = 1 \mathbf{do} S).P = \sqcap_{n=0}^{\infty} P_n$ , where  $P_0 = I_{\mathcal{H}_{all}}$ ,

$$P_{n+1} = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.P_n) M_1 \text{ for all } n \geq 0.$$

## Trace-preserving property

- For any quantum program  $S$ , quantum predicate  $P \in \mathcal{P}(\mathcal{H}_{all})$ , and any partial density operator  $\rho \in \mathcal{D}(\mathcal{H}_{qll})$ :

$$tr((wp.S.P)\rho) = tr(P\llbracket S \rrbracket(\rho))$$

$$tr((wlp.S.P)\rho) = tr(P\llbracket S \rrbracket(\rho)) + (tr(\rho) - tr(\llbracket S \rrbracket\rho)).$$

- Fixed point characterisation. Write *while* for the quantum loop “**while**  $M[\bar{q}] = 1$  **do**  $S$ ”. Then for any  $P \in \mathcal{P}(\mathcal{H}_{all})$ 
  - $wp.\textit{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wp.S.(wp.\textit{while}.P)) M_1$ .
  - $wlp.\textit{while}.P = M_0^\dagger P M_0 + M_1^\dagger (wlp.S.(wlp.\textit{while}.P)) M_1$ .

## Proof system for partial correctness

- $\{P\} \text{ skip } \{P\}$

- If  $\text{type}(q) = \mathbf{Bool}$ , then

$$\{|0\rangle_q \langle 0|P|0\rangle_q \langle 0| + |1\rangle_q \langle 0|P|0\rangle_q \langle 1|\} q := |0\rangle \{P\}$$

If  $\text{type}(q) = \mathbf{Int}$ , then

$$\left\{ \sum_{n=-\infty}^{\infty} |n\rangle_q \langle 0|P|0\rangle_q \langle n| \right\} q := |0\rangle \{P\}$$

- $\{U^\dagger P U\} U[\bar{q}] \{P\}$

## Proof system for partial correctness

- $$\frac{\{P\} S_1 \{Q\} \quad \{Q\} S_2 \{R\}}{\{P\} S_1; S_2 \{R\}}$$
- $$\frac{\{P_m\} S \{Q\} \text{ for all } m}{\{\sum_m M_m^\dagger P_m M_m\} \text{ if } (\Box m \cdot M[\bar{q}] = m \rightarrow S_m) \{Q\}}$$
- $$\frac{\{Q\} S \{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\} \text{ while } M[\bar{q}] = 1 \text{ do } S \{P\}}$$
- $$\frac{P \sqsubseteq P' \quad \{P'\} S \{Q'\} \quad Q' \sqsubseteq Q}{\{P\} S \{Q\}}$$

## Proof system for partial correctness

If  $\{P\}S\{Q\}$  is derivable in the previous proof system, we write  $\vdash_{par} \{P\}S\{Q\}$ .

- **Soundness** For any program  $S$  and predicates  $P, Q \in \mathcal{P}(\mathcal{H}_{all})$

$$\vdash_{par} \{P\}S\{Q\} \text{ implies } \models_{par} \{P\}S\{Q\}$$

- **Completeness** For any program  $S$  and predicates  $P, Q \in \mathcal{P}(\mathcal{H}_{all})$

$$\models_{par} \{P\}S\{Q\} \text{ implies } \vdash_{par} \{P\}S\{Q\}$$

## Bound (ranking) functions

Let  $P \in \mathcal{P}(\mathcal{H}_{all})$  be a quantum predicate,  $\epsilon > 0$  be a real number.

A function

$$t : \mathcal{D}(\mathcal{H}_{all}) \rightarrow \omega$$

is a  $(P, \epsilon)$ -bound function of quantum loop

**while**  $M[\bar{q}] = 1$  **do**  $S$

if for all  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ ,

1.  $t(\llbracket S \rrbracket(M_1 \rho M_1^\dagger)) \leq t(\rho)$ ;
2.  $\text{tr}(P\rho) \geq \epsilon$  implies

$$t(\llbracket S \rrbracket(M_1 \rho M_1^\dagger)) < t(\rho)$$

## Characterisation of bound functions

The following two statements are equivalent:

1. for any  $\epsilon > 0$ , there exists a  $(P, \epsilon)$ -bound function  $t_\epsilon$  of the loop **while**  $M[\bar{q}] = 1$  **do**  $S$ ;
2.  $\lim_{n \rightarrow \infty} \text{tr}(P(\llbracket S \rrbracket \circ \mathcal{E}_1)^n(\rho)) = 0$  for all  $\rho \in \mathcal{D}(\mathcal{H}_{all})$ .



## Proof system for total correctness

Rule for while loop: if

- $\{Q\} S \{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}$
- for any  $\epsilon > 0$ ,  $t_\epsilon$  is a  $(M_1^\dagger Q M_1, \epsilon)$ -bound function of loop  
**while**  $M[\bar{q}] = 1$  **do**  $S$

then  $\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}$  **while**  $M[\bar{q}] = 1$  **do**  $S \{P\}$

## Proof system for total correctness

If  $\{P\}S\{Q\}$  is derivable in the previous proof system for total correctness, we write  $\vdash_{tot} \{P\}S\{Q\}$ .

- **Soundness** For any program  $S$  and predicates  $P, Q \in \mathcal{P}(\mathcal{H}_{all})$

$$\vdash_{tot} \{P\}S\{Q\} \text{ implies } \models_{tot} \{P\}S\{Q\}$$

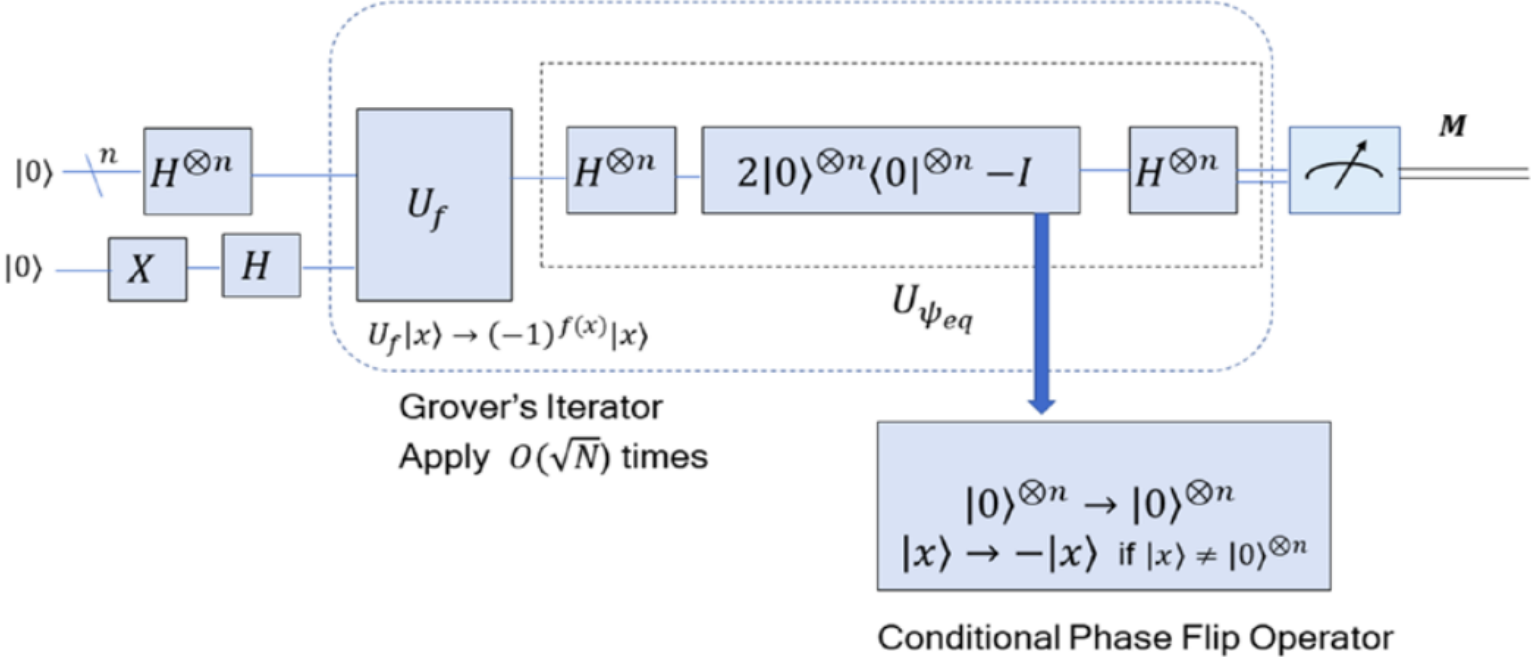
- **Relative completeness** For any program  $S$  and predicates  $P, Q \in \mathcal{P}(\mathcal{H}_{all})$

$$\models_{tot} \{P\}S\{Q\} \text{ implies } \vdash_{tot} \{P\}S\{Q\}$$

# Quantum Algorithms

# Grover's algorithm

Suppose there are  $N = 2^n$  items in a database. The aim is to search the item indexed by  $k$ . Assume the existence of a function  $f$  with  $f(x) = 1$  if  $x = k$  and 0 otherwise.



## Grover's algorithm

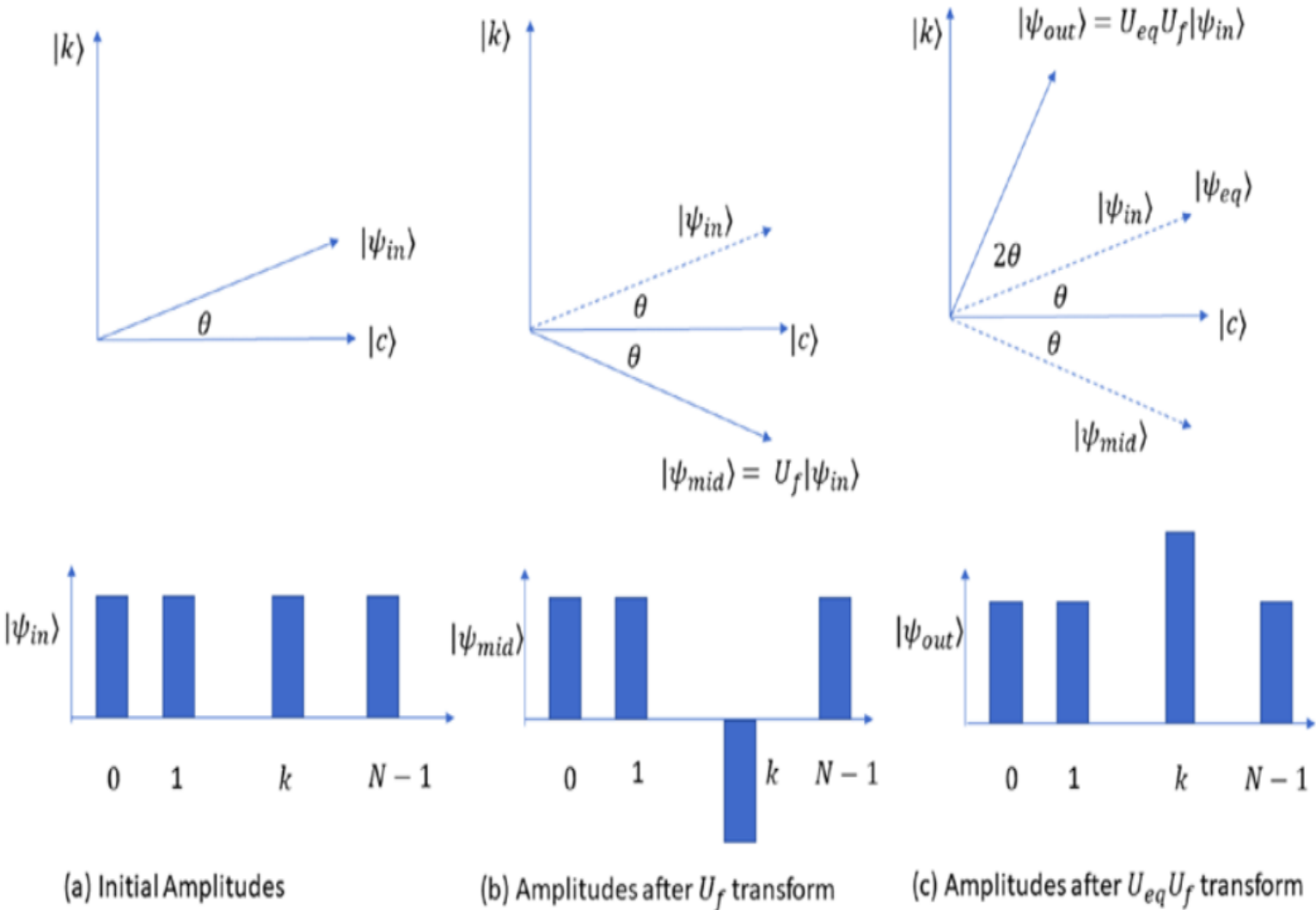
1.  $|\psi_0\rangle = |0\rangle^{\otimes n} |0\rangle$
2.  $|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
3. Phase kickback:  $|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
4. View the equal superposition state  $|\psi_{in}\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle$  as a linear combination of two vectors.

$$|\psi_{in}\rangle = \cos \theta |c\rangle + \sin \theta |k\rangle$$

with  $\theta = \arcsin \frac{1}{\sqrt{N}}$ .

5. Apply  $U_f$  on  $|\psi_{in}\rangle$  gives  $|\psi_{mid}\rangle = \cos \theta |c\rangle - \sin \theta |k\rangle$ . It is a reflection about vector  $|c\rangle$ .

# Grover's algorithm



## Grover's algorithm

6. Reflect vector  $|\psi_{mid}\rangle$  over the equal superposition state vector  $|\psi_{eq}\rangle$ .

Let

$$U_{eq} = 2|\psi_{eq}\rangle\langle\psi_{eq}| - I = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}$$

$$\begin{aligned} |\psi_{out}\rangle &= U_{eq}|\psi_{mid}\rangle = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} \cos \theta \\ -\sin \theta \end{bmatrix} \\ &= \begin{bmatrix} \cos 2\theta \cos \theta - \sin 2\theta \sin \theta \\ \sin 2\theta \cos \theta + \cos 2\theta \sin \theta \end{bmatrix} = \begin{bmatrix} \cos 3\theta \\ \sin 3\theta \end{bmatrix} = \cos 3\theta|c\rangle + \sin 3\theta|k\rangle \end{aligned}$$

7. Apply  $U_f$  followed by  $U_{eq}$  for  $m$  iterations, the final output state  $(U_{eq}U_f)^m|\psi_{in}\rangle$  will be close to  $|k\rangle$ .

8. The  $U_f$  transformation is the same as in the Deutsch-Jozsa and

Bernstein-Vajirani algorithms.  $U_{eq}$  can be slightly simplified as:

$$U_{eq} = H^{\otimes n} (2|0\rangle^{\otimes n} \langle 0|^{\otimes n} - I) H^{\otimes n}$$

The unitary transformation  $(2|0\rangle^{\otimes n} \langle 0|^{\otimes n} - I)$  maps  $|x\rangle$  to  $|x\rangle$  if  $|x\rangle = |0\rangle^{\otimes n}$ , and to  $-|x\rangle$  otherwise.