Quantum description of the universe

- Plank's Quantum theory of Radiation
- Photo-Electric Effect
- Bhor's hypothesis of discrete orbits for electron

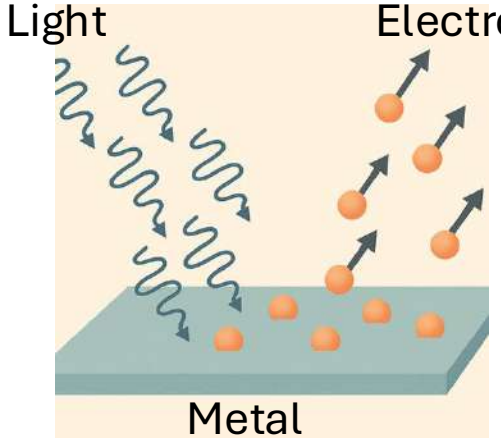
$$E = h\nu$$

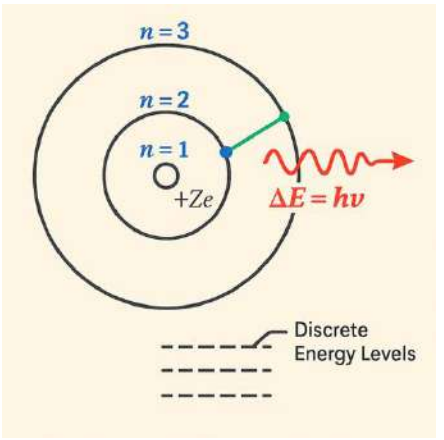
INTERNATIONAL YEAR OF Quantum Science and Technology

Photo-Electric Effect

Is light a wave or a particle?

This theory says it's a particle - and won Einstein his Nobel Prize !



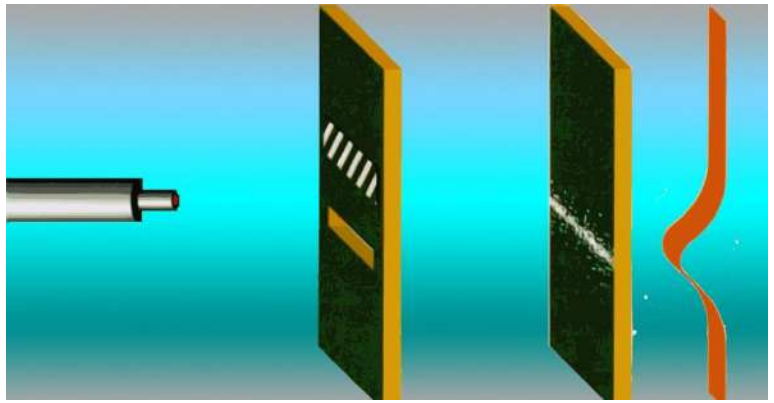


The idea that light exists as tiny packets, or particles, that we now call photons. Alongside Max Planck's work on quanta of heat, and Niels Bohr's later work on quanta of matter, Einstein's work anchors the most building block of 20th-century physics: we live in a quantum universe, one built out of tiny, discrete chunks of energy and matter.

1925 - Heisenberg's paper, "**On quantum-theoretical reinterpretation of kinematic and mechanical relationships**"
1926 - Schrodinger's paper, "**An undulatory theory of the mechanics of atoms and molecules**"

Quantum description: wave–particle nature

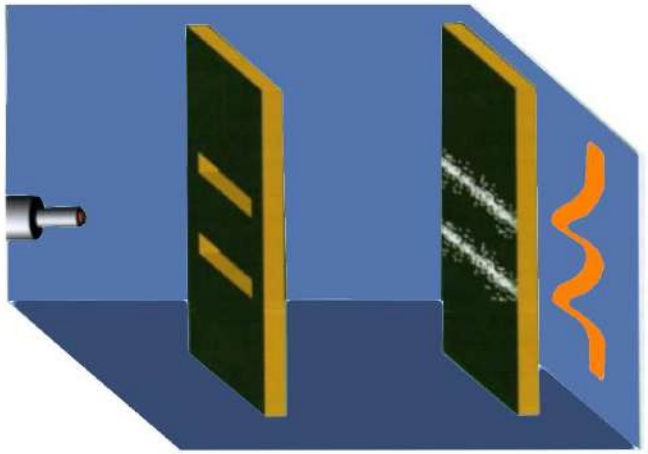
When only one slit is open



When both slits are open

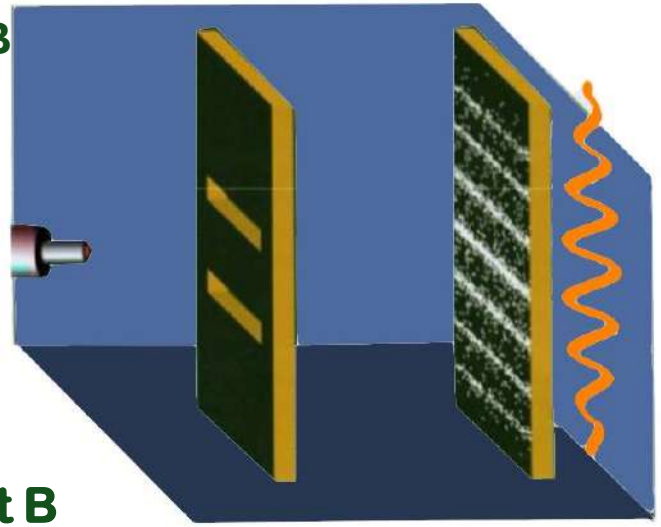
If light behaves as particle we should get

A



If light behaves as waves we should get

B



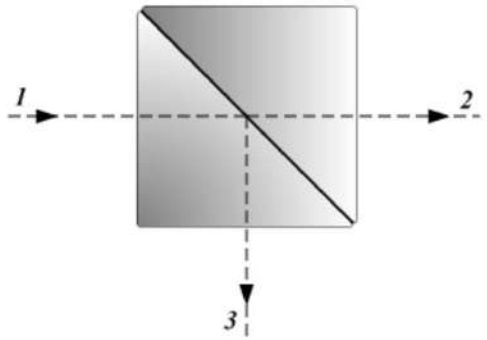
What we get ?

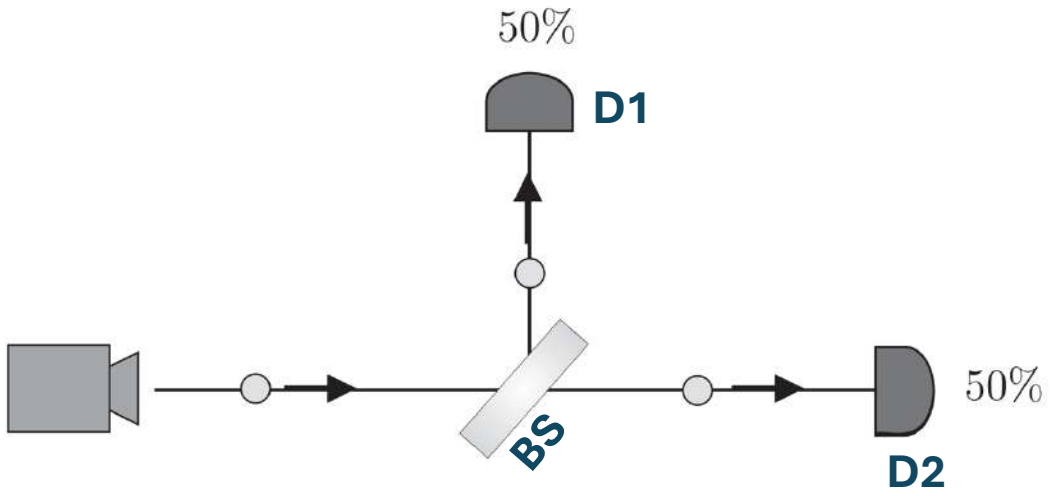
- When we track the photon path, we get A
- When we don't observer which path the photon travelled, we get B

Beam splitter and single photon

Classical light splits into two paths. What will happen to single photon ?

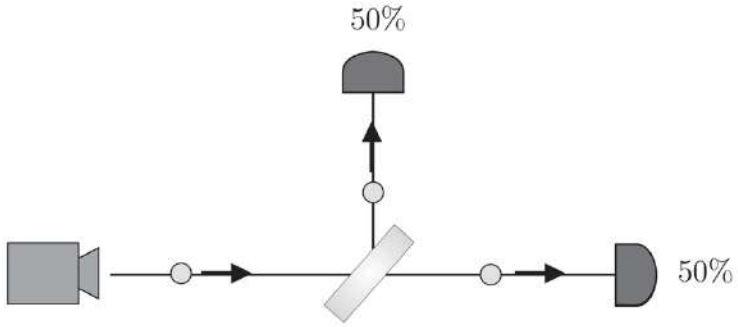
Beam Splitter (BS)



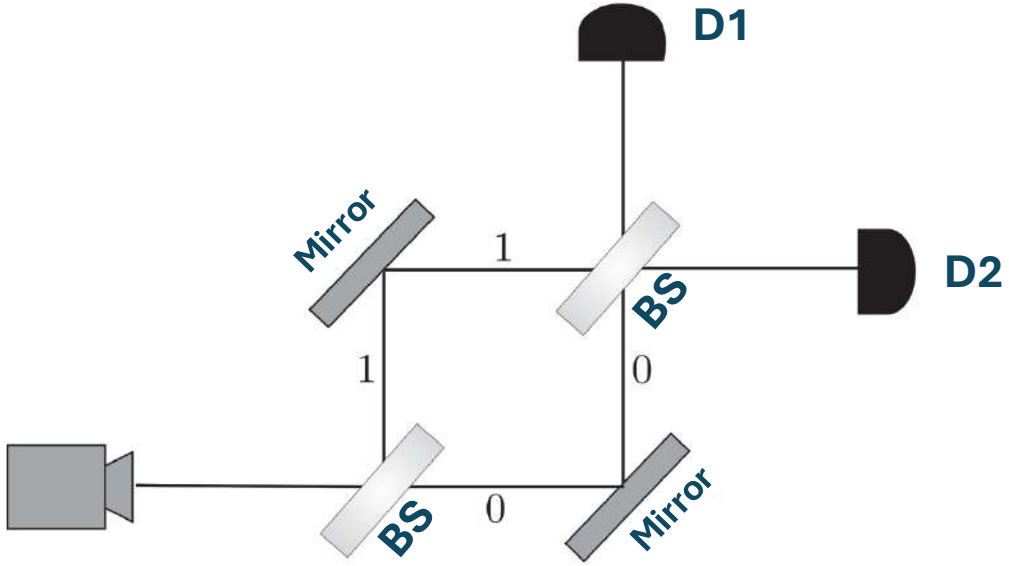


- **Demonstrates existence of photons as single particles**
- **Photons don't split**

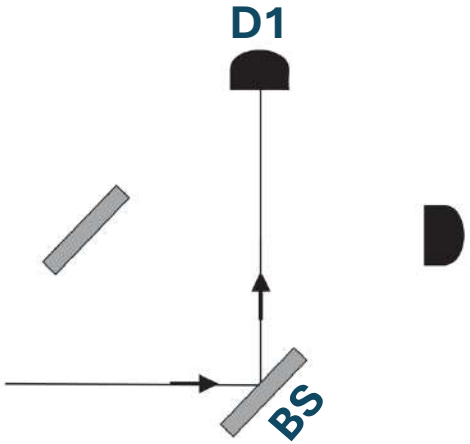
Beam splitters and single photon



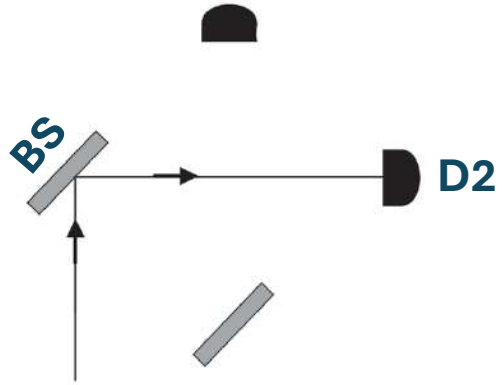
Single beam splitter setting



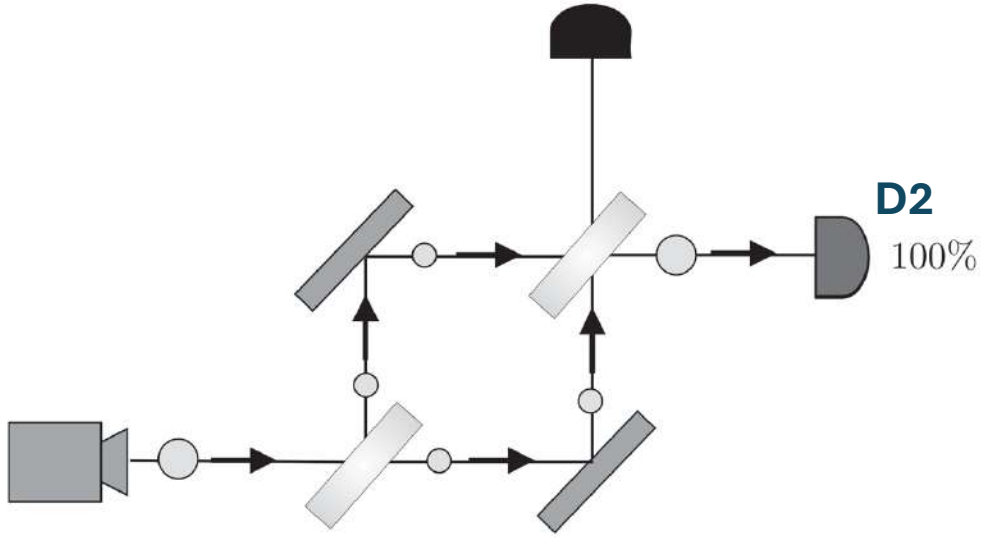
Double beam splitter setting (Mach-Zehnder Interferometer)



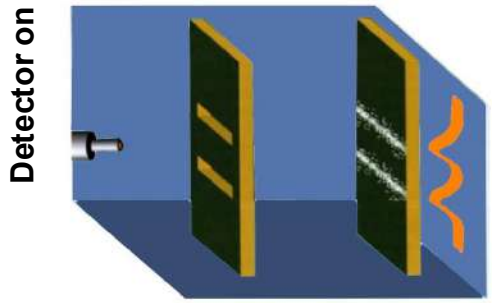
Photon taking Path 0

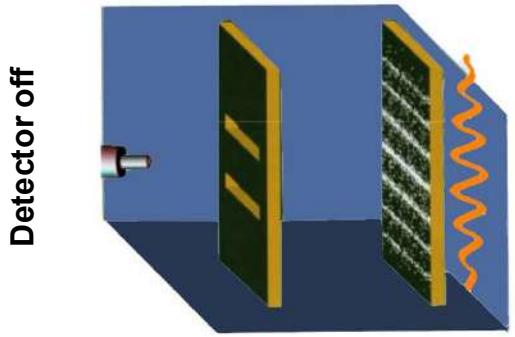


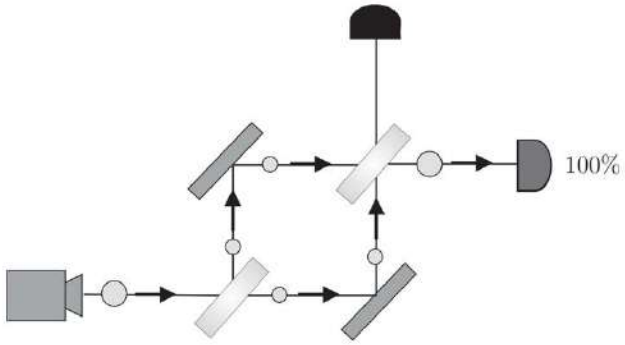
Photon taking Path 1



Summary :Quantum Interference / particle behavior

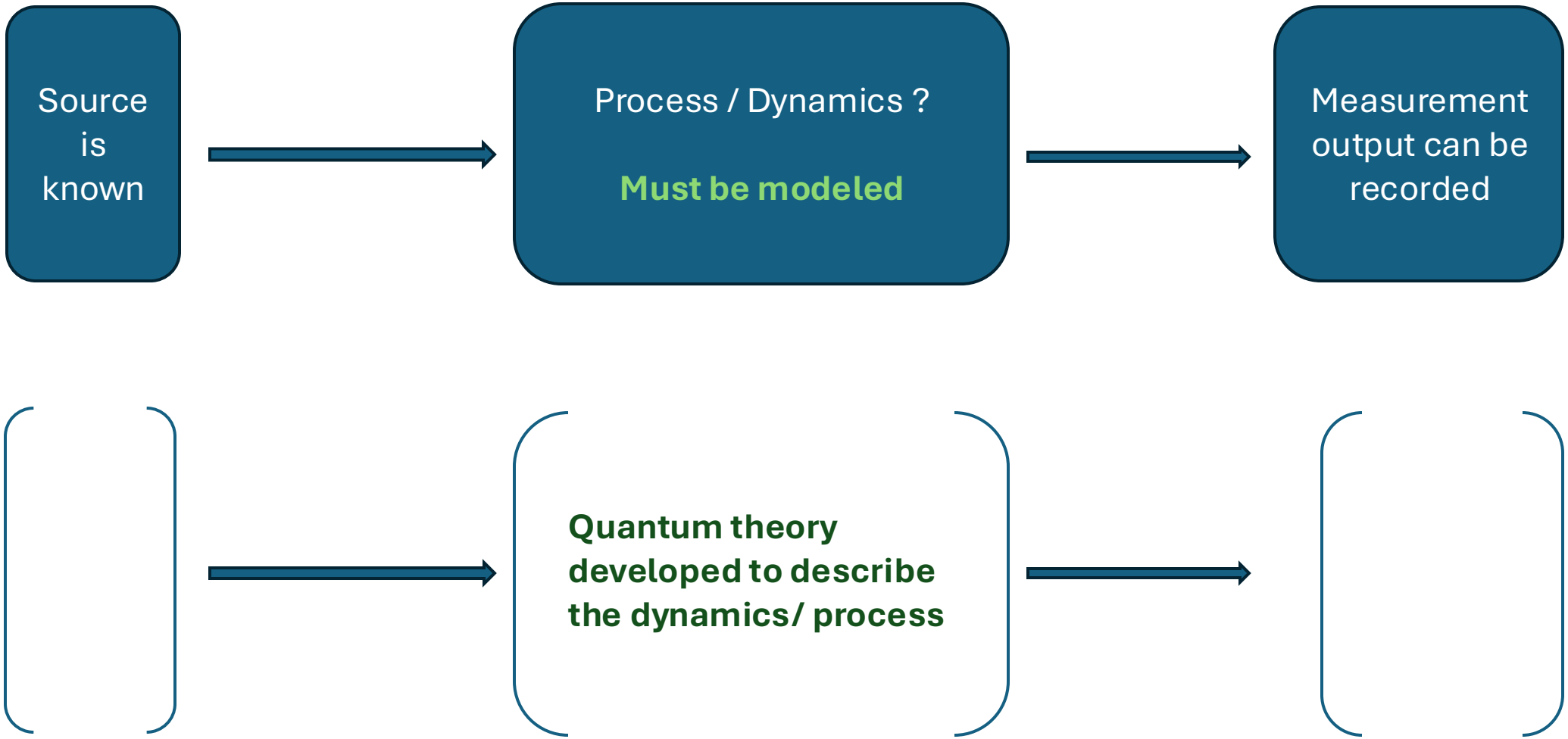






- Knowing which slit or path a photon travel through is a form of measurement
- One way to determine which path is by maintaining different polarization state in each path or slit
- Measuring collapses its wavefunction
- When particle behavior is observed, interference fails to form
- If no information exists to link photo to specific path, the wave behavior resumes, and interference pattern is observed

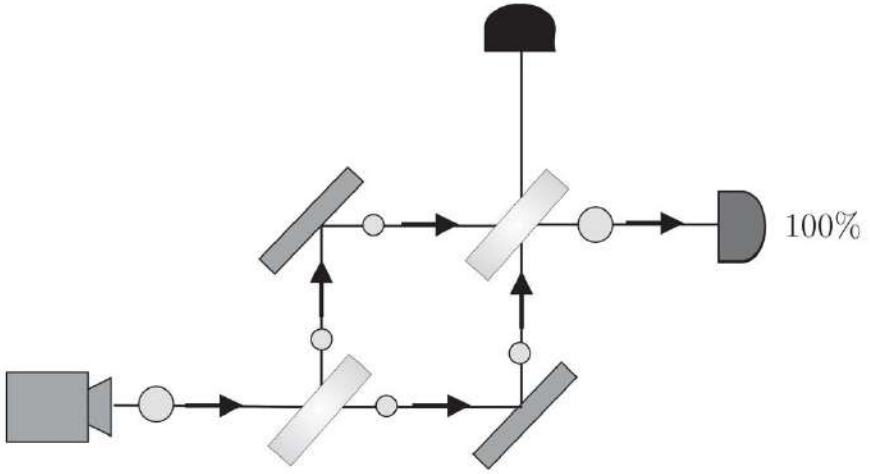
How to understand the dynamics ?



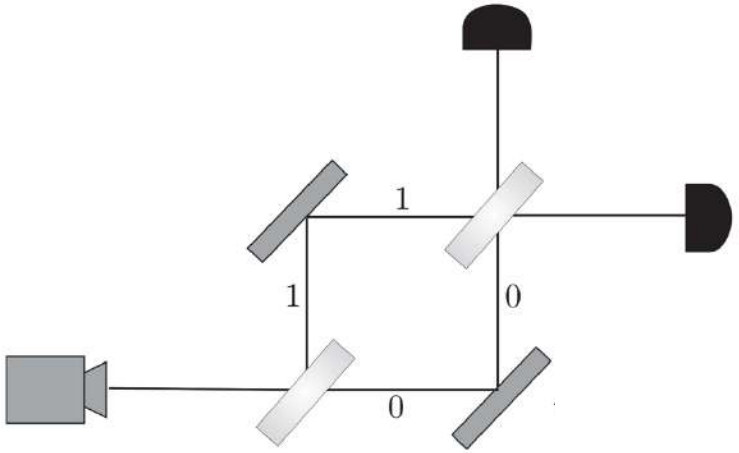
Needs complex space vector representation to model / develop a quantum theory

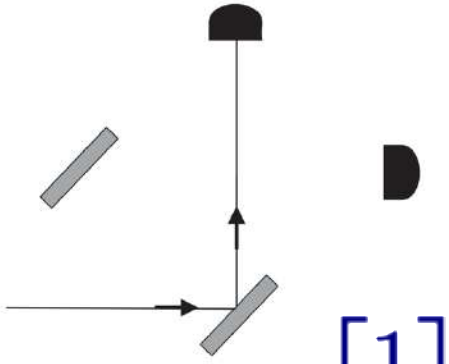
Let us model the dynamics of the photon in interferometer setup

Source is known → Process / Dynamics ? **Must be modeled** → Measurement output can be recorded

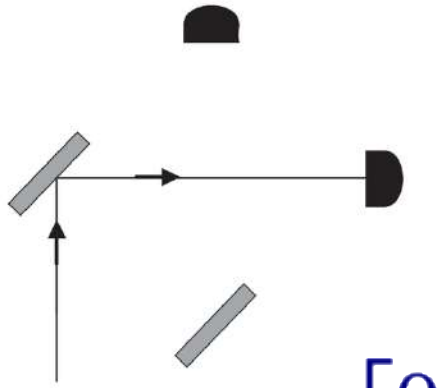


Vector representation and complex numbers

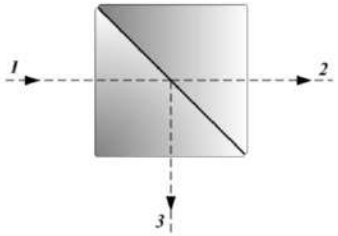




Photon in Path 0 $= \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

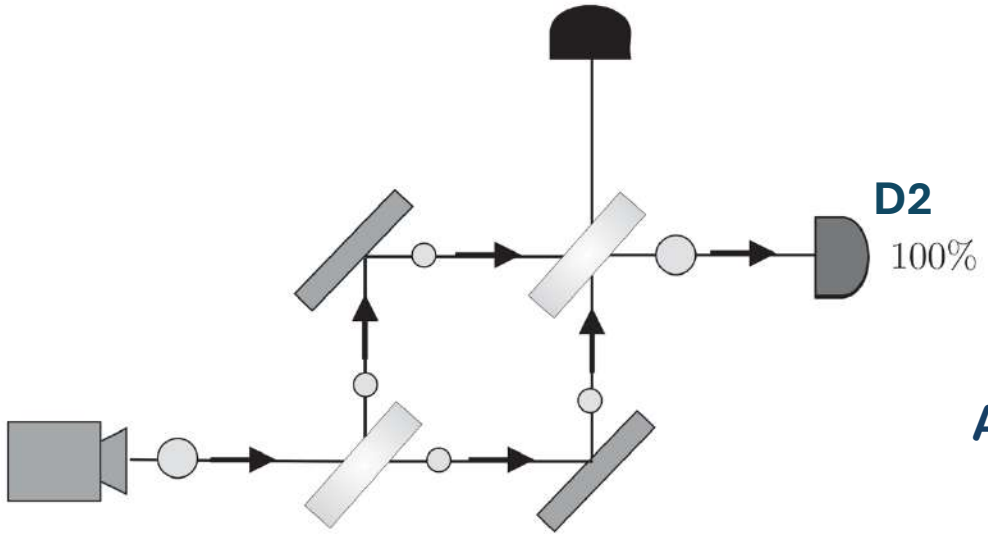


Photon in Path 1 $= \begin{bmatrix} 0 \\ 1 \end{bmatrix}$



$$BS = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

Vector representation and complex numbers



After first BS :

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

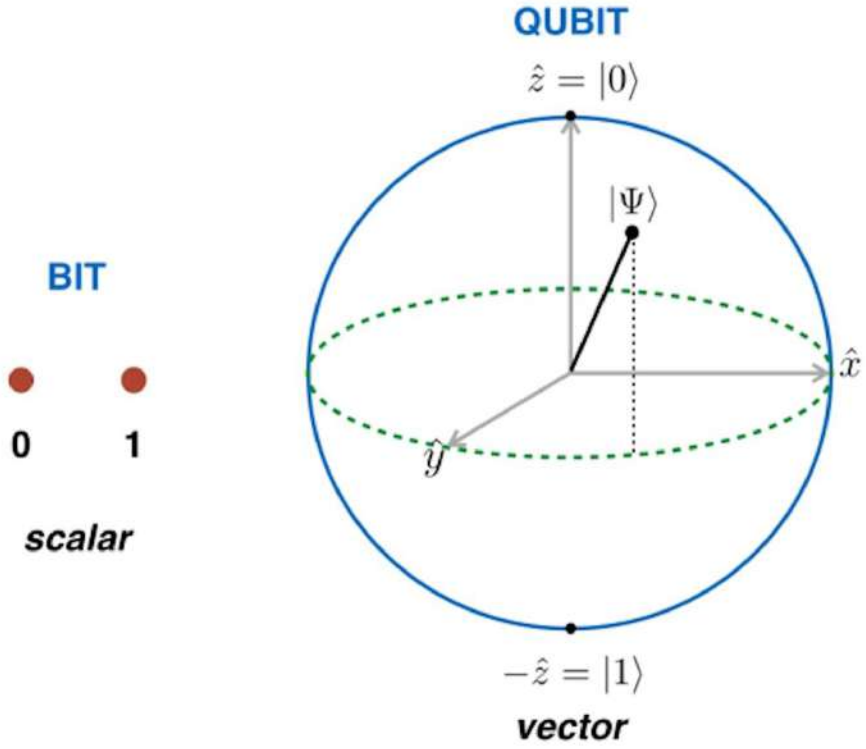
After second BS :

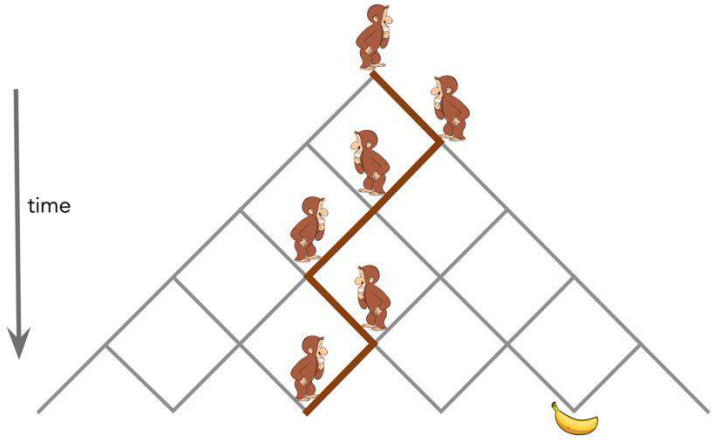
$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix}$$

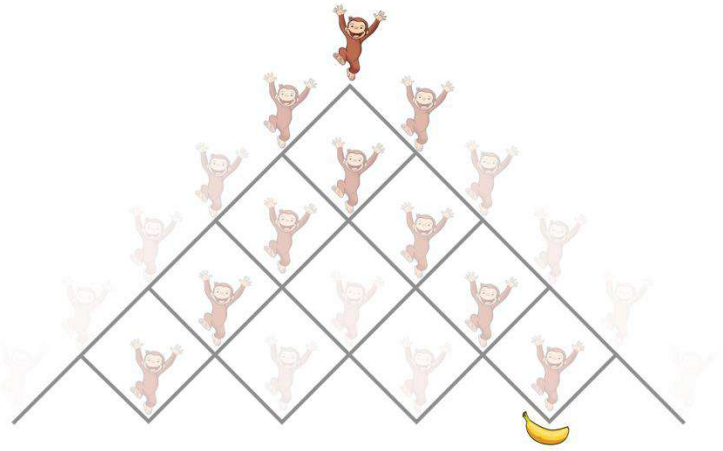
This simple math shows how interference is Making photon get detected only at D2

Quantum Superposition and Interference

Quantum state represented by atom, photon or electron spin can simultaneously be at more than one state at any given time.







Classical bit at any given time can only be in 0 or 1 but qubit can simultaneously be in both 0 and 1.

Qubit Representation – 2D Hilbert Space

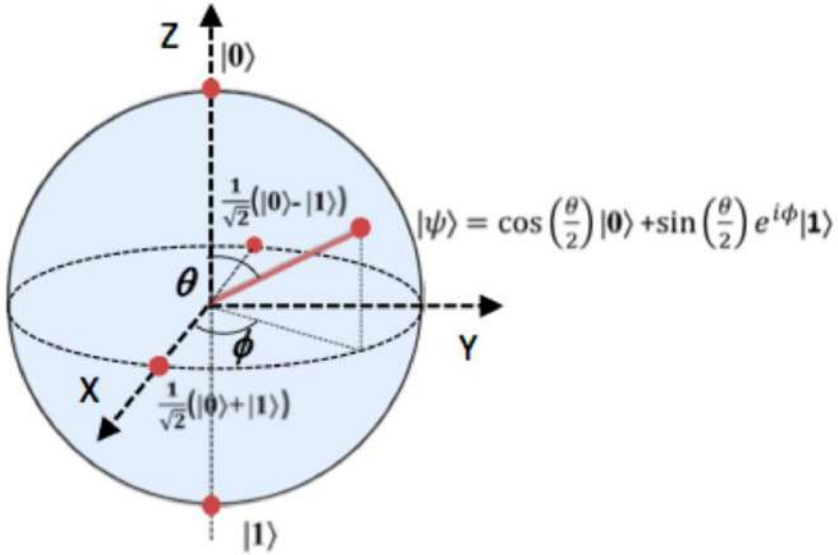
- classical bit :{0 , 1}
- Qubit - Ideal two-state quantum system : $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$

  logical /computational states

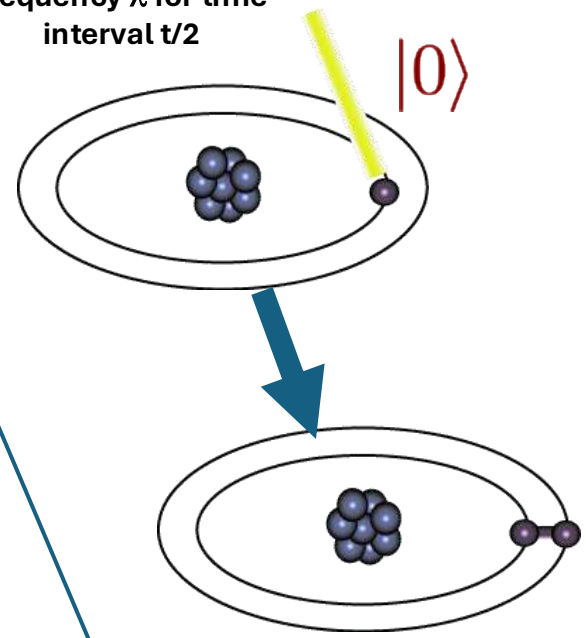
  - photons (V and H polarization, transmission mode - path encoding)
  - electrons or other spin-$\frac{1}{2}$ systems (spin up and down)
  - systems defined by two energy levels of atoms or ions

Allows superposition : $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$\alpha, \beta \in \mathbb{C}$; $|\alpha|^2 + |\beta|^2 = 1$; $|\Psi\rangle = e^{i\eta}|\Psi\rangle$



Light pulse of frequency λ for time interval t/2



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

Dirac Notations – composite system

Two qubit representation – Tensor product state – four-dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

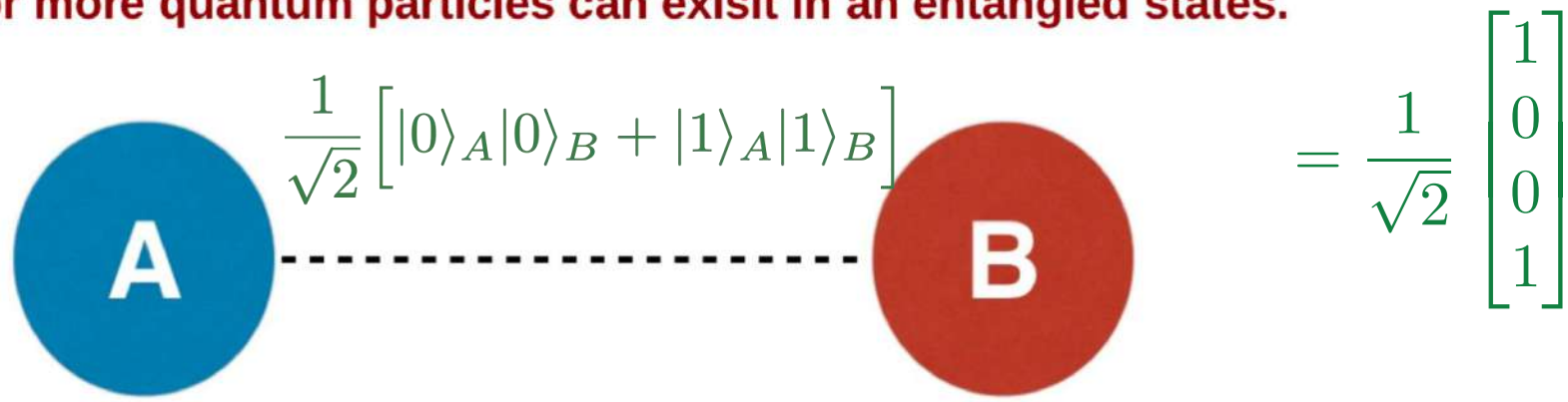
$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

$$|1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle$$

Two-qubit state - Quantum Entanglement

Two or more quantum particles can exisit in an entangled states.



For example : Two carefully preapred photons, A and B can be physically saperated from one another and any change of state performed on photon A will instantly result with a change of state on photon B **(instantaneous information transfer).**

In Summary:

Superposition allows us to simultaneously explore all possible options /solutions.

Interference allows us to engineer constructive interference towards desired result and distructive interference at undesired options.

Entanglement allows us to achieve instantaneous and secured information exchange.

Dirac Notations – composite system

Three qubit representation – Tensor product state, 8-dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$

- Consider a 3 qubit register. An equally weighted superposition of all possible states would be denoted by :

$$|\Psi\rangle = \frac{1}{\sqrt{8}}\left[|000\rangle + |001\rangle + |010\rangle + |100\rangle + ... + |111\rangle\right]$$

General quantum states

- *n*-dimensional quantum system consists of *n* basis states :

$$|\Psi_n\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle + ... + \alpha_n|n\rangle$$

$$|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + ... + |\alpha_n|^2 = 1$$

- 2^n dimensional system can be constructed as a tensor product of ***n*** qubit system

n-qubit registrar in composite system

- In general, an n qubit register can represent the numbers 0 through 2^n-1 simultaneously.

Sound too good to be true?…It is!

- If we attempt to retrieve the values represented within a superposition, the **superposition randomly collapses** to represent just one of the original values.

Quantum Operations

Unitary transformations :

- Linear transformations that preserve vector norm.
- In 2 dimensions, linear transformations that preserve unit circle (rotations and reflections).

Examples :

- Bit flip $|0\rangle \Rightarrow |1\rangle$, $|1\rangle \Rightarrow |0\rangle$
- Hadamard transformation $|0\rangle \Rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \Rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$U_{\text{bit-flip}}|0\rangle = \sigma_x|0\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$$

$$U_{\text{bit-flip}}|1\rangle = \sigma_x|1\rangle = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$$

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

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

What will two times the above two operations return ?

Universal set of gates for QC

Identity : $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Pauli x : $\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

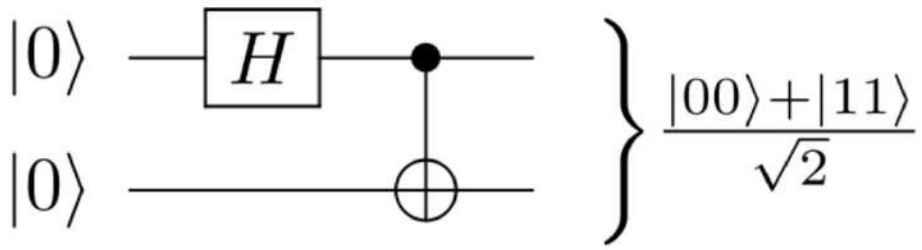
Pauli y : $\sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Pauli z : $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

$\pi/8$ Phase : $T_{\pi/8} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

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

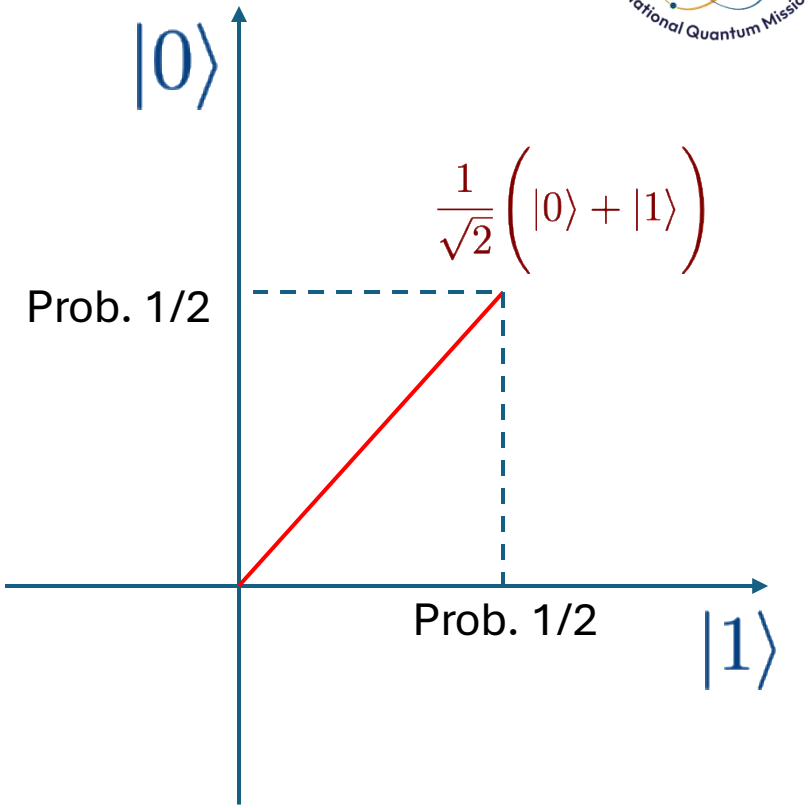


$$CNOT|00\rangle = |00\rangle$$
$$CNOT|01\rangle = |01\rangle$$
$$CNOT|10\rangle = |11\rangle$$
$$CNOT|11\rangle = |10\rangle$$

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

Measurements

- Measuring $\alpha|0\rangle + \beta|1\rangle$ in basis $|0\rangle, |1\rangle$ gives:
  - 0 with probability $|\alpha|^2$,
  - 1 with probability $|\beta|^2$.



- Measurement changes the state: it becomes $|0\rangle$ or $|1\rangle$.

- Repeating the measurement gives the same outcome.

General measurements

Even for any two orthogonal one-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$$

It is equivalent to mapping them to $|0\rangle, |1\rangle$ and measuring.

Partial Measurements

Let us take a simple two qubit state and make measurement only on the first qubit :

$$|\Psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

First qubit collapses to $|0\rangle$

First qubit collapses to $|1\rangle$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

This will be 50% probability

$$|\Psi_2\rangle = |10\rangle$$

This will be 50% probability

Classical vs. Quantum

Classical Bits:

- Can be measured completely
- States don’t chance by measurements
- Can be copied
- Can be erased

Quantum Bits:

- Can be measured partially
- States alter by measurements
- Cannot be copied (no cloning)
- Cannot be erased

No cloning of any arbitrary quantum state

Directly related to impossibility of measuring an arbitrary quantum state perfectly

- Let us imagine that we could copy quantum states :

$$|0\rangle \Rightarrow |0\rangle|0\rangle$$
$$|1\rangle \Rightarrow |1\rangle|1\rangle$$

- Then, by linearity condition we will get

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

- This is not the same as two copies of $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$

Linear Algebra (short review)

Z^* - complex conjugate

if $Z = a + b \cdot i$ then $Z^* = a - b \cdot i$

$|\psi\rangle$ - vector, "ket" i.e.

$$\begin{bmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{bmatrix}$$

$|\psi\rangle$ - vector, "bra" i.e.

$$[c_1^*, c_2^*, \dots, c_n^*]$$

$\langle\varphi|\psi\rangle$ - inner product between vectors $|\varphi\rangle$ and $|\psi\rangle$.

Note for QC this is on $\mathbb{C}^n$ space not $\mathbb{R}^n$!

Note $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$

Example: $|\varphi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix}, |\psi\rangle = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$

$$\langle\varphi|\psi\rangle = [2, -6i] \begin{bmatrix} 3 \\ 4 \end{bmatrix} = 6 - 24i$$

$|\varphi\rangle \otimes |\psi\rangle$ - tensor product of $|\varphi\rangle$ and $|\psi\rangle$.

Also written as $|\varphi\rangle|\psi\rangle$

$$\text{Example: } |\varphi\rangle|\psi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix} \otimes \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \times 3 \\ 2 \times 4 \\ 6i \times 3 \\ 6i \times 4 \end{bmatrix} = \begin{bmatrix} 6 \\ 8 \\ 18i \\ 24i \end{bmatrix}$$

Linear Algebra (short review)

A^* - complex conjugate of matrix A.

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^* = \begin{bmatrix} 1 & -6i \\ -3i & 2-4i \end{bmatrix}$$

A^T - transpose of matrix A.

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^T = \begin{bmatrix} 1 & 3i \\ 6i & 2+4i \end{bmatrix}$$

$A^\dagger$ - Hermitian conjugate (adjoint) of matrix A.

Note $A^\dagger = \left(A^T\right)^*$

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^\dagger = \begin{bmatrix} 1 & -3i \\ -6i & 2-4i \end{bmatrix}$$

Linear Algebra (short review)

A^* - complex conjugate of matrix A.

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^* = \begin{bmatrix} 1 & -6i \\ -3i & 2-4i \end{bmatrix}$$

A^T - transpose of matrix A.

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^T = \begin{bmatrix} 1 & 3i \\ 6i & 2+4i \end{bmatrix}$$

$A^\dagger$ - Hermitian conjugate (adjoint) of matrix A.

Note $A^\dagger = \left(A^T\right)^*$

$$\text{if } A = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \text{ then } A^\dagger = \begin{bmatrix} 1 & -3i \\ -6i & 2-4i \end{bmatrix}$$

$\| |\psi\rangle \|$ - norm of vector $|\psi\rangle$

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

Important for normalization of $|\psi\rangle$ i.e. $|\psi\rangle / \| |\psi\rangle \|$

$\langle\varphi|A|\psi\rangle$ - inner product of $|\varphi\rangle$ and $A|\psi\rangle$.

or inner product of $A^\dagger|\varphi\rangle$ and $|\psi\rangle$

Postulates of Quantum Mechanics

An important distinction needs to be made between quantum mechanics, quantum physics and quantum computing. Quantum mechanics is a mathematical language, much like calculus. Just as classical physics uses calculus to explain nature, quantum physics uses quantum mechanics to explain nature. Just as classical computers can be thought of in boolean algebra terms, quantum computers are reasoned about with quantum mechanics. There are four postulates to quantum mechanics, which will form the basis of quantum computers:

- **Postulate 1:** Definition of a quantum bit, or *qubit*.
- **Postulate 2:** How qubit(s) transform (evolve).
- **Postulate 3:** The effect of measurement.
- **Postulate 4:** How qubits combine together into systems of qubits.

Postulate 1 : A Quantum Bit

Postulate 1 (Nielsen and Chuang, page 80):

> "Associated to any *isolated* physical system is a complex vector space with inner product (i.e. a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a *unit vector* in the system's state space."

Postulate 1 : A Quantum Bit

Postulate 1 (Nielsen and Chuang, page 80):

> "Associated to any *isolated* physical system is a complex vector space with inner product (i.e. a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a *unit vector* in the system's state space."

Consider a single qubit - a two-dimensional state space. Let $|\phi_0\rangle$ and $|\phi_1\rangle$ be orthonormal basis for the space. Then a qubit $|\psi\rangle = a|\phi_0\rangle + b|\phi_1\rangle$. In quantum computing we usually label the basis with some boolean name but note carefully that this is *only* a name. For example, $|\phi_0\rangle = |0\rangle$ and $|\phi_1\rangle = |1\rangle$. Making this more concrete one might imagine that "$|0\rangle$" is being represented by an up-spin while "$|1\rangle$" by a down-spin. The key is there is an abstraction between the technology (spin state or other quantum phenomena) and the logical meaning. This same detachment occurs classically where we traditionally call a high positive voltage "1" and a low ground potential "0".

Note that $|\psi\rangle = a|0\rangle + b|1\rangle$ must be a unit vector. In other words, $\langle\psi|\psi\rangle = 1$ or $|a|^2 + |b|^2 = 1$. For quantum computing $\{a, b\} \in \mathbb{C}$

Qubit

Classical Bit : $\{0, 1\}$

Qubit : $|0\rangle$ and $|1\rangle$ possible (allowed) basis states

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

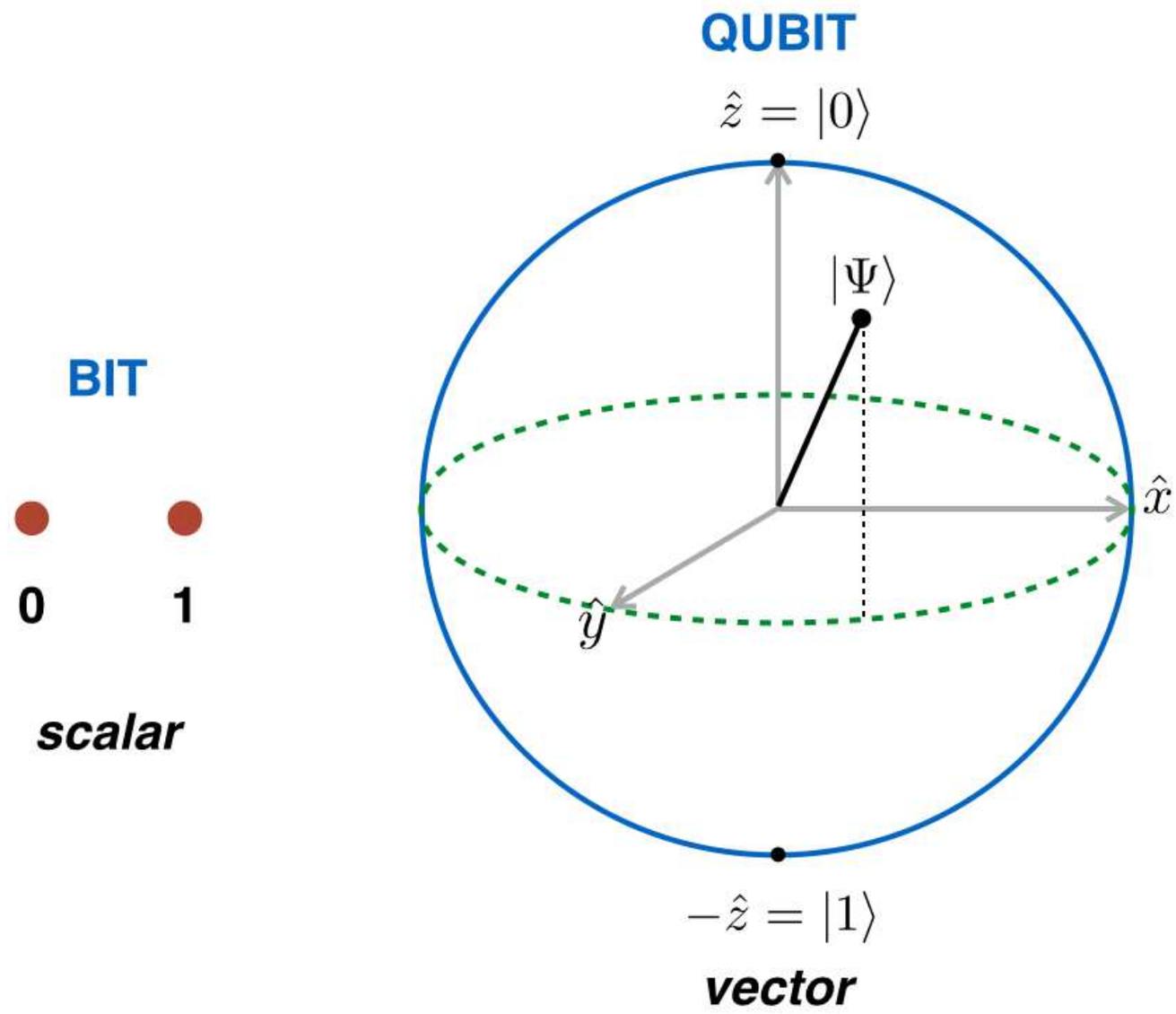
Any quantum system with exactly two degree of freedom
(state of an hydrogen atom, spin of an electron)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1$$

Superposition state

In Dirac notation : $$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Bloch Sphere representation of Qubit



Postulate 2 : Evolution of Quantum Systems

$$\text{NOT}: \quad \begin{pmatrix}1\\0\end{pmatrix} \mapsto \begin{pmatrix}0\\1\end{pmatrix}, \qquad \begin{pmatrix}0\\1\end{pmatrix} \mapsto \begin{pmatrix}1\\0\end{pmatrix}.$$

From this information, we can construct the matrix for the NOT gate (in the computational basis):

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

The gate acts on the state of a qubit by matrix multiplication from the left:

$$\text{NOT}|0\rangle \equiv \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \equiv |1\rangle.$$

The NOT gate is often identified with the symbol X, and is one of the four *Pauli gates*:

$$\sigma_0 \equiv I \equiv \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.$$

Postulate 2 : Evolution of Quantum Systems

Postulate 2 (Nielsen and Chuang, page 81):

"The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state of $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on times t_1 and t_2."

Example:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$|\psi'\rangle = U|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle$$

Example:

$$\text{Let } |\psi\rangle = 1|0\rangle + 0|1\rangle = |0\rangle$$
$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$
$$|\psi'\rangle = U|\psi\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Postulate 2 : Evolution of Quantum Systems

Important: U must be unitary, that is $U^\dagger U = I$

Example:

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ then } U^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$U^\dagger U = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$$

Postulate 3 : Measurement

Postulate 3 (Nielsen and Chuang, page 84):

"Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

and the state of the system after measurement is:

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the *completeness equation*:

$$\sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = I$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle \text{ "}$$

Postulate 3 : Measurement

Some important measurement operators are $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$

$$M_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} [1,0] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$M_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} [0,1] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Observe that $M_0^\dagger M_0 + M_1^\dagger M_1 = I$ and are thus complete.

Example:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle$$

Note that $M_0^\dagger M_0 = M_0$, hence

$$p(0) = \langle\psi|M_0|\psi\rangle = [a^*, b^*] \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} =$$

$$= [a^*, b^*] \begin{bmatrix} a \\ 0 \end{bmatrix} = |a|^2$$

Hence the probability of measuring $|0\rangle$ is related to its probability amplitude a by way of $|a|^2$.

Postulate 4 : Multi-qubit Systems

Postulate 4 (Nielsen and Chuang, page 94):

> "The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. [sic] e.g. suppose systems 1 through n and system i is in state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$."

Example:

Suppose $|\psi_1\rangle = a|0\rangle + b|1\rangle$ and $|\psi_2\rangle = c|0\rangle + d|1\rangle$, then:

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle = a \cdot c|0\rangle|0\rangle + a \cdot d|0\rangle|1\rangle + b \cdot c|1\rangle|0\rangle + b \cdot d|1\rangle|1\rangle =$$
$$ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

Entanglement

Entanglement is a uniquely quantum phenomenon. Entanglement is a property of a multi-qubit state space (multi-qubit system) and can be thought of as a resource. To explain entanglement we'll examine the creation and destruction of an EPR pair of qubits named after Einstein, Podolsky, and Rosen.

Suppose you begin with a qubit $|\psi_1\rangle$ in a zero $|0\rangle$ state.

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

Then let $|\psi_1'\rangle = H|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Now take another qubit $|\psi_2\rangle$ also in the zero $|0\rangle$ state. The joint state-space probability vector is the tensor product of these two:

$$|\psi_1'\rangle \otimes |\psi_2\rangle = |\psi_1'\psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle$$

Now define a new unitary transform:

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

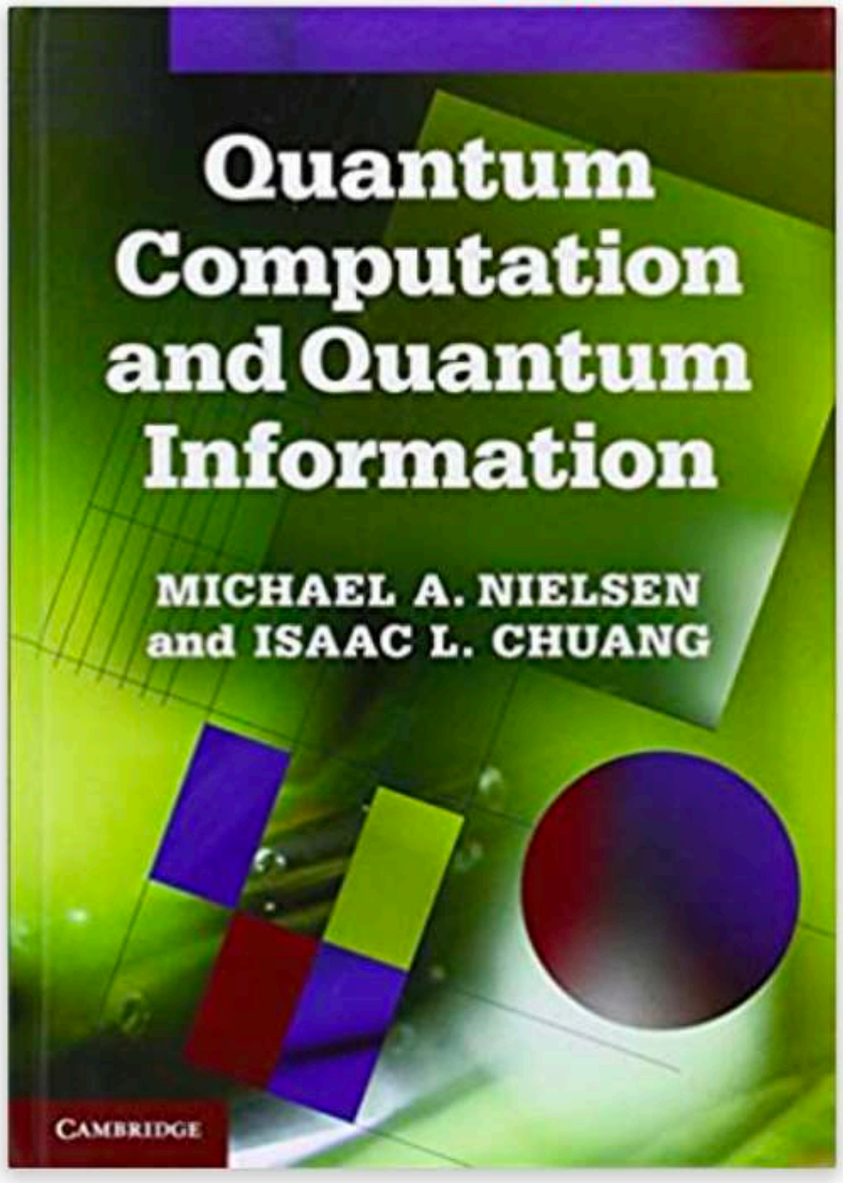
Entanglement

$$|(\psi_1'\psi_2)''\rangle = CNot|\psi_1'\psi_2\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

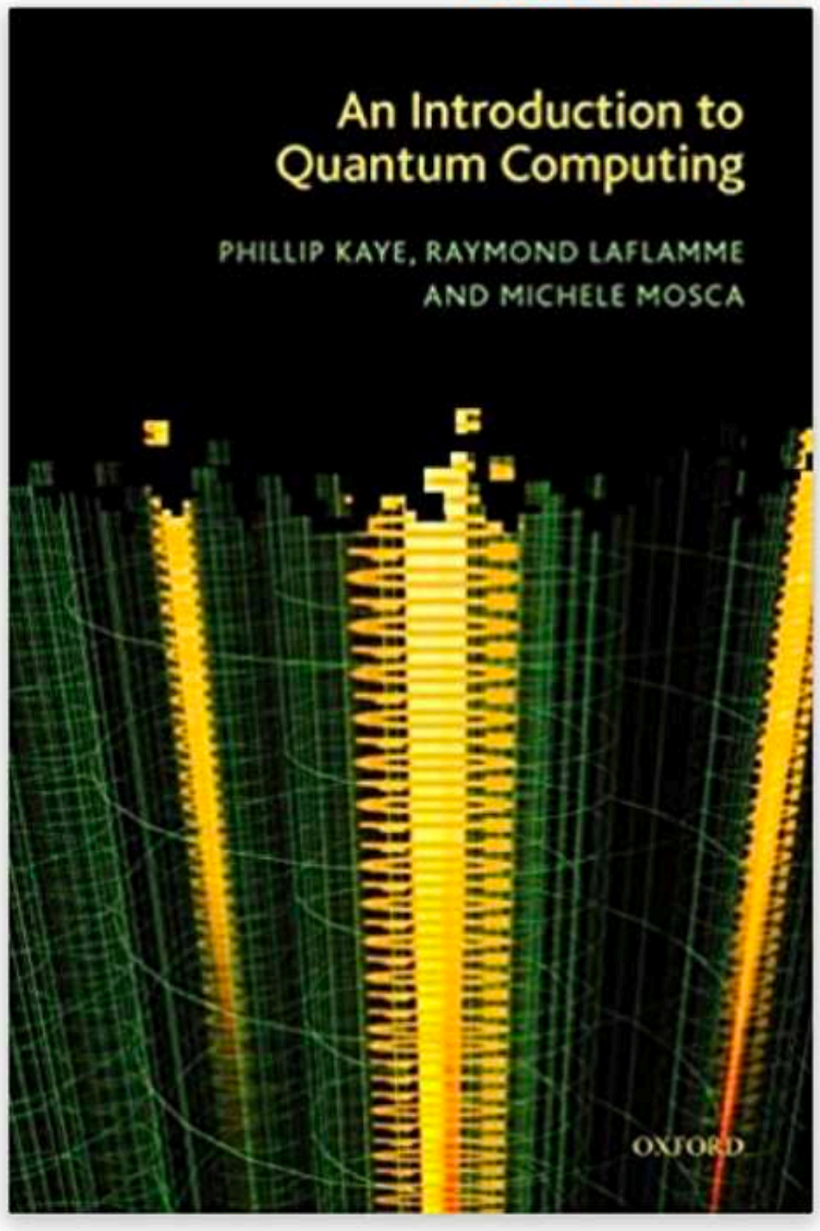
The key to entanglement is the property that the state space cannot be decomposed into component spaces. That is, for our example, there does not exists any $|\varphi_1\rangle$ and $|\varphi_2\rangle$ such that $|\varphi_1\rangle \otimes |\varphi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Quantum computing

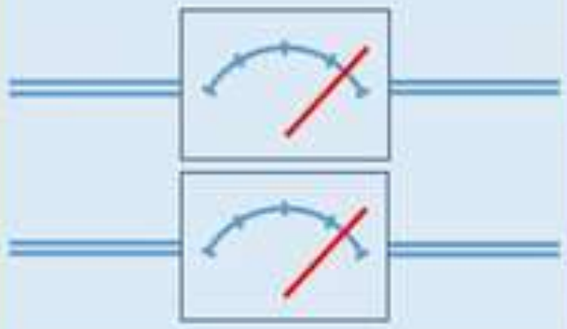
Look inside ↓



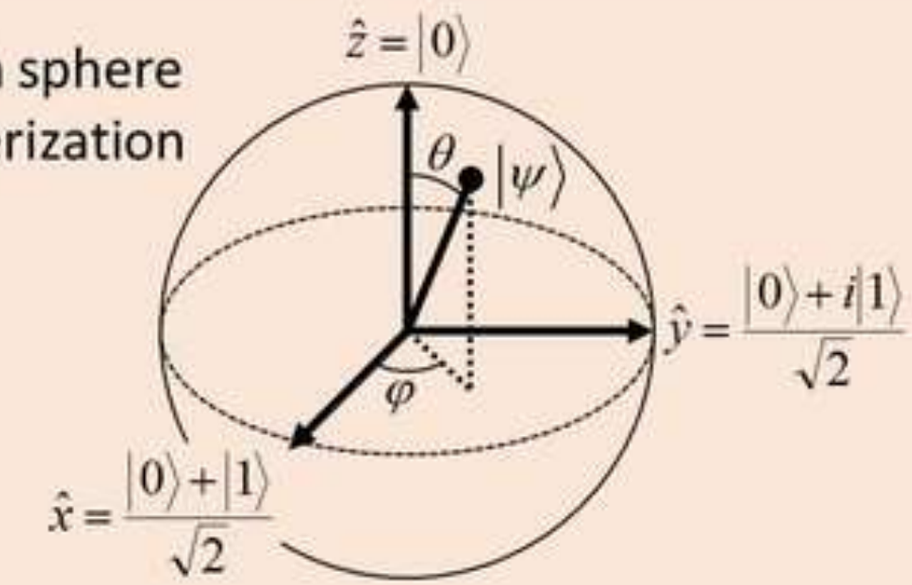
Look inside ↓



Classical vs Quantum computer

	input	measurement	result
bits	$b \in \{0,1\}$ 0 1		0 w/probability 1 1 w/probability 1
qubits	$\lvert\psi\rangle = \alpha\lvert 0\rangle + \beta\lvert 1\rangle$ $\lvert\alpha\rvert^2 + \lvert\beta\rvert^2 = 1$ $\alpha, \beta \in C$		$\lvert 0\rangle$ w/probability $\lvert\alpha\rvert^2$ $\lvert 1\rangle$ w/probability $\lvert\beta\rvert^2$

e.g. Bloch sphere parameterization



$$\alpha = \cos(\theta/2)$$

$$\beta = e^{i\varphi}\sin(\theta/2)$$

Quantum computer

Quantum Computer : A device that uses a quantum mechanical representation of information to perform calculations. Information in quantum computers is stored in qbits and the states can be represented by l_2 normalized vectors in complex vector space,

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle$$

$a_x \in C$ satisfies $\sum_{x\in\{0,1\}^n} |a_x|^2 = 1$ and basis of state $|x\rangle$ is computation basis.

A vector is l_1 normalized if its integral over all space = 1 and l_2 if its integral of function times complex conjugate =1.

For a finite set S, the normalized uniform superposition of its elements can be written as

$$|S\rangle = \frac{1}{\|S\|}\sum_{s\ \in S} |s\rangle.$$

If quantum computer stores state $|\psi\rangle$ in one register and $|\phi\rangle$ in another register the state can be written as

$$|\psi\rangle \otimes |\phi\rangle \equiv |\psi\rangle|\phi\rangle \equiv |\psi, \phi\rangle$$

How do you make Programmable Quantum Computers ?

The qubits are prepared in a particular state

They undergo a sequence of quantum logic gates

A quantum measurement extracts the algorithm's output

Single and two qubit operations

$$\text{Identity}: \quad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Pauli } x: \quad \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

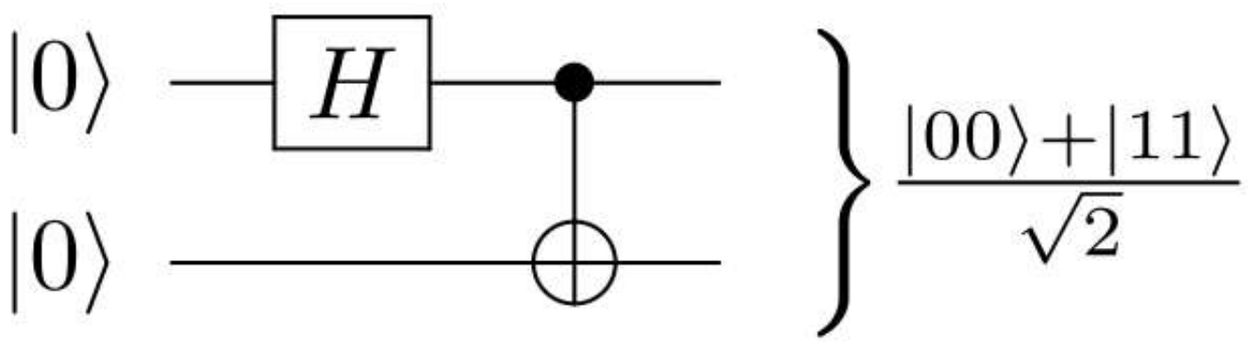
$$\text{Pauli } y: \quad \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\text{Pauli } z: \quad \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

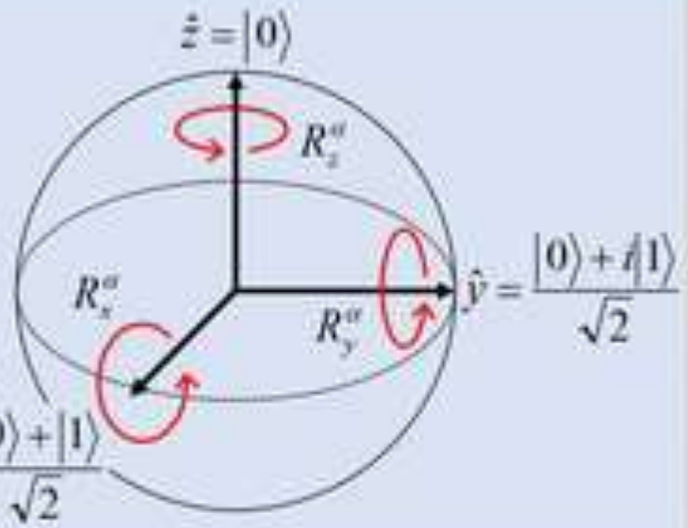
$$\pi/8 \text{ Phase}: \quad T_{\pi/8} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

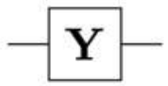
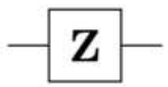
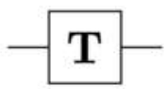
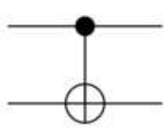
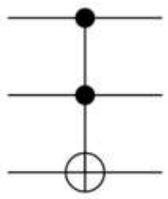


Qubit rotations

	input state	circuit symbol	output state	operator depictions and representations
Qubit rotations	$\|q_1\rangle$	R_z^α	$\|q_2\rangle = R_z^\alpha \|q_1\rangle$	$R_z^\alpha \equiv e^{-i\alpha Z/2} = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{+i\alpha/2} \end{pmatrix}$
	$\|q_1\rangle$	R_y^α	$\|q_2\rangle = R_y^\alpha \|q_1\rangle$	$R_y^\alpha \equiv e^{-i\alpha Y/2} = \begin{pmatrix} \cos(\alpha/2) & -\sin(\alpha/2) \\ \sin(\alpha/2) & \cos(\alpha/2) \end{pmatrix}$
	$\|q_1\rangle$	R_x^α	$\|q_2\rangle = R_x^\alpha \|q_1\rangle$	$R_x^\alpha \equiv e^{-i\alpha X/2} = \begin{pmatrix} \cos(\alpha/2) & -i\sin(\alpha/2) \\ -i\sin(\alpha/2) & \cos(\alpha/2) \end{pmatrix}$
CNOT	$\|q_c\rangle$ $\|q_t\rangle$		$\|q_c\rangle$ $\|q_c \oplus q_t\rangle$	$\|q_c\rangle \otimes \|q_c \oplus q_t\rangle = U_{CNOT} \|q_c\rangle \otimes \|q_t\rangle$ $U_{CNOT} = \begin{matrix} \langle 0_c 0_t \| \\ \langle 0_c 1_t \| \\ \langle 1_c 0_t \| \\ \langle 1_c 1_t \| \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$



Quantum logic gates

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
π/8 (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Measurements and partial measurements

Suppose 3 qubits are in the superposition

$$|\Psi\rangle = \frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|101\rangle - \frac{1}{2}|111\rangle$$

and the third qubit is measured. What are the probabilities of the two possible measurement outcomes and what are the resulting superpositions of the three qubits for each case ?

Measurements and partial measurements

Suppose 3 qubits are in the superposition

$$|\Psi\rangle = \frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|101\rangle - \frac{1}{2}|111\rangle$$

To determine the answer, we write

$$|\psi\rangle = \left(\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle\right)|0\rangle + \left(\frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle\right)|1\rangle\,.$$

The probability that the measurement outcome is 0 is

$$\left\|\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle\right\|^2 = \frac{1}{2}$$

and in this case the resulting superposition is

$$\sqrt{2}\left(\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|100\rangle\,.$$

The probability that the measurement outcome is 1 is

$$\left\|\frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle\right\|^2 = \frac{1}{2}$$

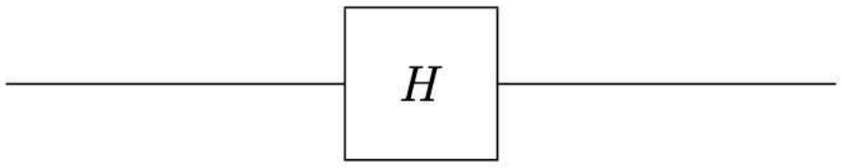
and in this case the resulting superposition is

$$\sqrt{2}\left(\frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle\right)|1\rangle = \frac{1}{\sqrt{2}}|101\rangle - \frac{1}{\sqrt{2}}|111\rangle\,.$$

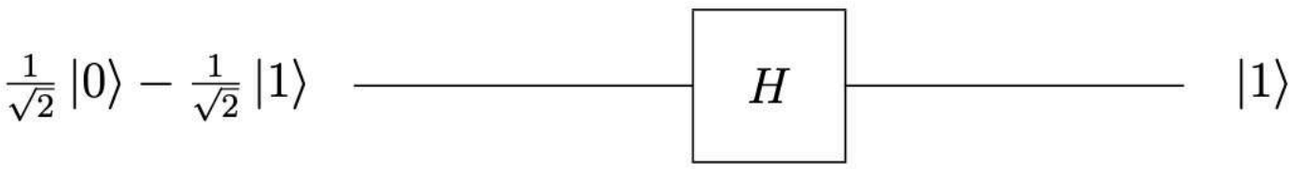
Quantum circuits

- Time goes from left to right
- Horizontal lines represent quits
- Operations and measurements are represented by different symbols

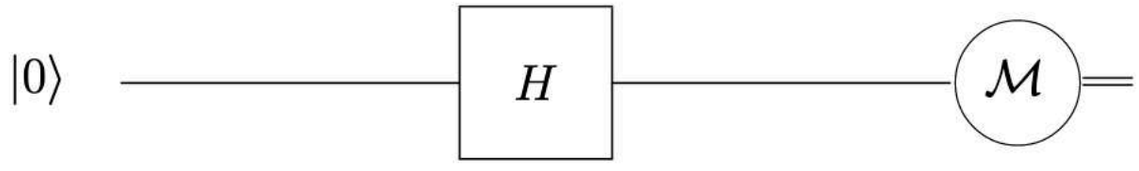
Example 1. The following diagram represents a Hadamard transform applied to a single qubit:



If the input is $|\psi\rangle$, the output is $H|\psi\rangle$. Sometimes when we want to explain what happens for a particular input, we label the inputs and outputs with superpositions, such as:



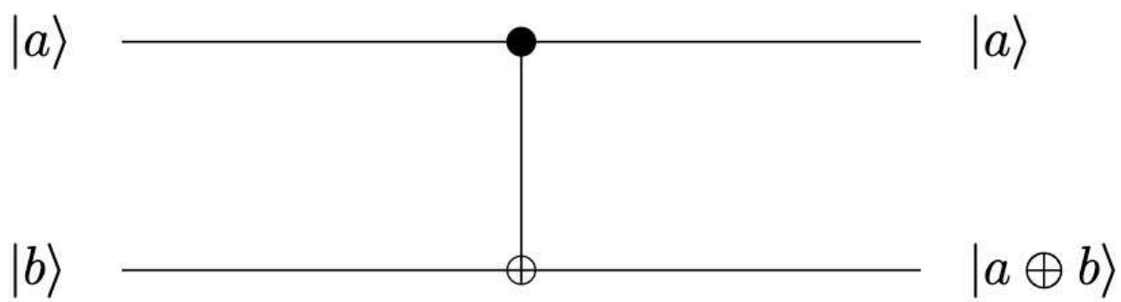
Example 2. Measurements are indicated by circles (or ovals) with the letter $\mathcal{M}$ inside. For example:



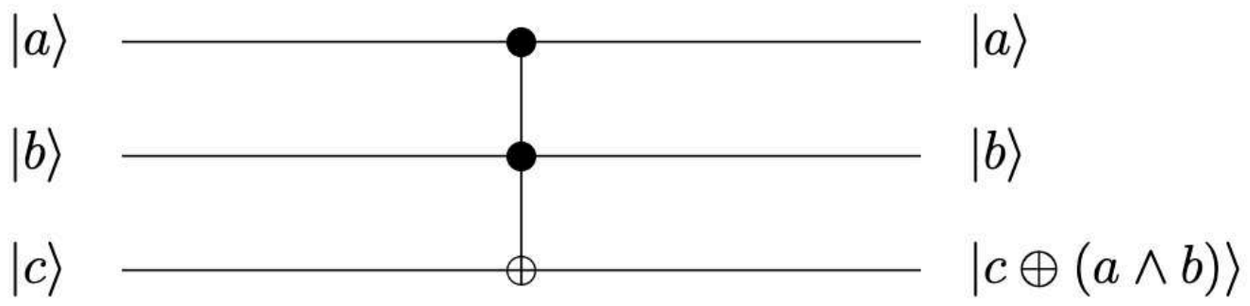
The result of the measurement is a classical value, and sometimes (as in the above diagram) we draw double lines to indicate classical bits. In this case the outcome is a uniformly distributed bit.

Quantum circuits

Example 3. Multiple-qubit gates are generally represented by rectangles, or have their own special representation. For instance, this is a *controlled-not* operation:



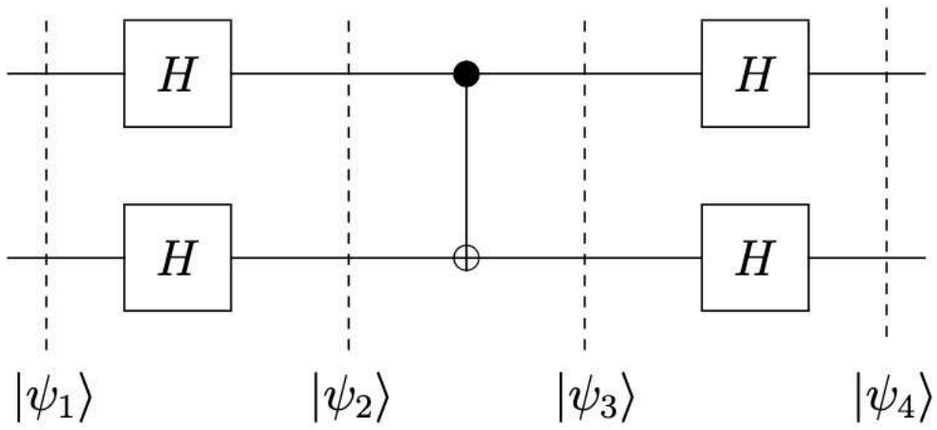
Here the action is indicated for classical inputs (meaning $a, b \in \{0, 1\}$). Along similar lines, here is a *controlled-controlled-not* operation, better known as a *Toffoli gate*:



Here the action is described for each choice of $a, b, c \in \{0, 1\}$.

Quantum circuits

Example 4



Suppose first that $|\psi_1\rangle = |00\rangle$. Then

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\,,$$

$$|\psi_3\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle + \frac{1}{2}|10\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_4\rangle = |00\rangle\,.$$

Next suppose that $|\psi_1\rangle = |01\rangle$. Then

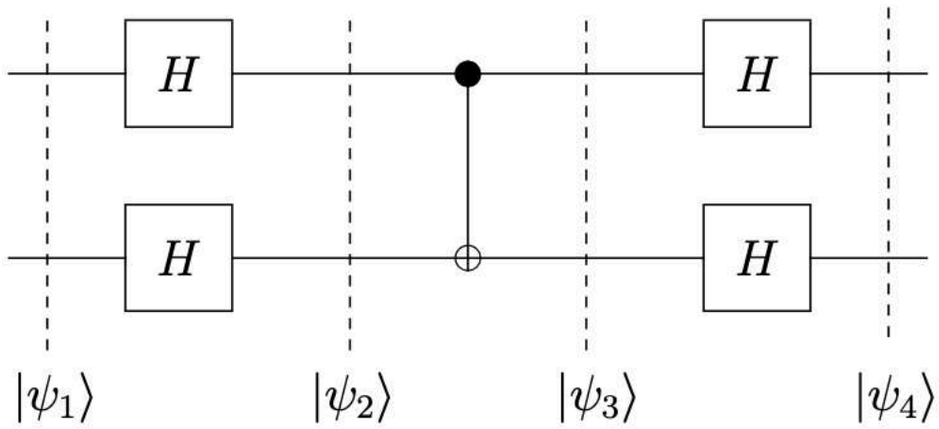
$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle\,,$$

$$|\psi_3\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle - \frac{1}{2}|10\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_4\rangle = |11\rangle\,.$$

Quantum circuits

Example 4



Next suppose that $|\psi_1\rangle = |10\rangle$. Then

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle,$$

$$|\psi_3\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle - \frac{1}{2}|10\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_4\rangle = |10\rangle.$$

Finally, suppose that $|\psi_1\rangle = |11\rangle$. Then

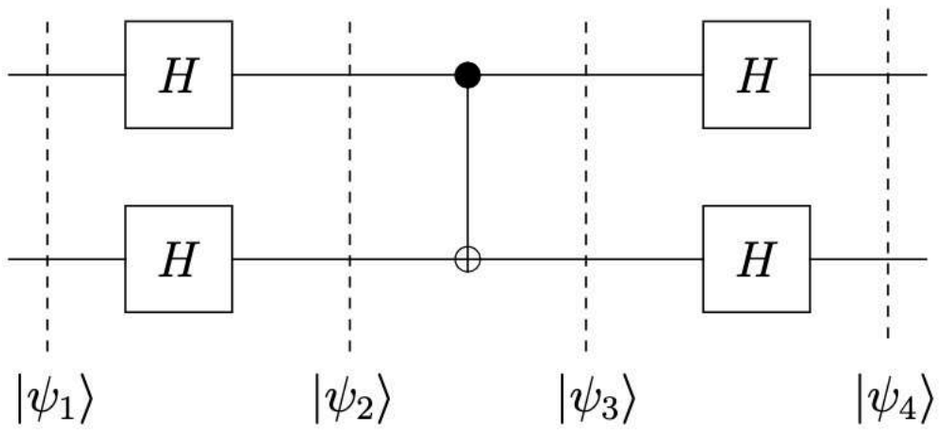
$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle,$$

$$|\psi_3\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle + \frac{1}{2}|10\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

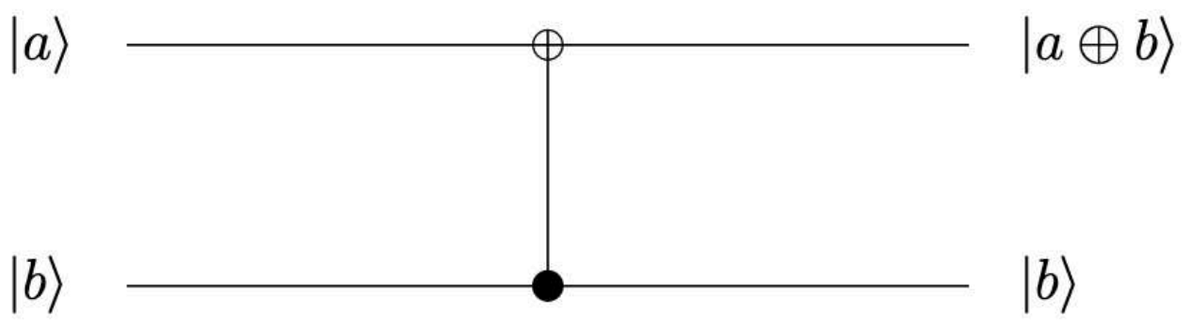
$$|\psi_4\rangle = |01\rangle.$$

Quantum circuits

Example 4



It turns out that the circuit is equivalent to this gate:



Superdense coding

Superdense coding

Alice and Bob are in different parts of the world. Alice has two bits : ***a*** and ***b.*** She would like to communicate these two bits to **Bob** by sending him just a single qubit. Alice cannot encode two classical bit into a single qubit in any way that would give Bob more than just one bit of information about the pair ***(a, b).***

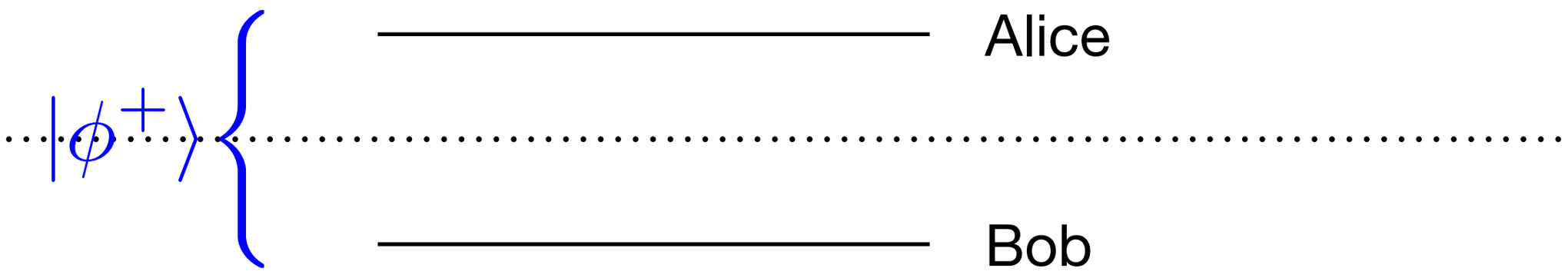
This can be accomplished with additional resources, if Alice and Bob share an entangled bit (e-bit).

Superdense coding

Alice and Bob are in different parts of the world. Alice has two bits : ***a*** and ***b.*** She would like to communicate these two bits to **Bob** by sending him just a single qubit. Alice cannot encode two classical bit into a single qubit in any way that would give Bob more than just one bit of information about the pair ***(a, b).***

This can be accomplished with additional resources, if Alice and Bob share an entangled bit (e-bit).

$$|\Psi_{AB}\rangle = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Superdense coding protocol

1. If $a = 1$, Alice applies the unitary transformation

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

   to the qubit A. (If $a = 0$ she does not.)

2. If $b = 1$, Alice applies the unitary transformation

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

   to the qubit A. (If $b = 0$ she does not.)

3. Alice sends the qubit A to Bob. (This is the only qubit that is sent during the protocol.)

4. Bob applies a controlled-NOT operation to the pair (A, B), where A is the control and B is the target. The corresponding unitary matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

5. Bob applies a Hadamard transform to A.

6. Bob measures both qubits A and B. The output will be (a, b) with certainty.

Superdense coding protocol

ab	state after step 1	state after step 2	state after step 4	state after step 5
00	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\left(\frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle\right)\|0\rangle$	$\|00\rangle$
01	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|10\rangle + \frac{1}{\sqrt{2}}\|01\rangle$	$\left(\frac{1}{\sqrt{2}}\|1\rangle + \frac{1}{\sqrt{2}}\|0\rangle\right)\|1\rangle$	$\|01\rangle$
10	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\left(\frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle\right)\|0\rangle$	$\|10\rangle$
11	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|10\rangle - \frac{1}{\sqrt{2}}\|01\rangle$	$\left(\frac{1}{\sqrt{2}}\|1\rangle - \frac{1}{\sqrt{2}}\|0\rangle\right)\|1\rangle$	$-\|11\rangle$

When Bob measures at the end of the protocol, it is clear that he sees ab as required.

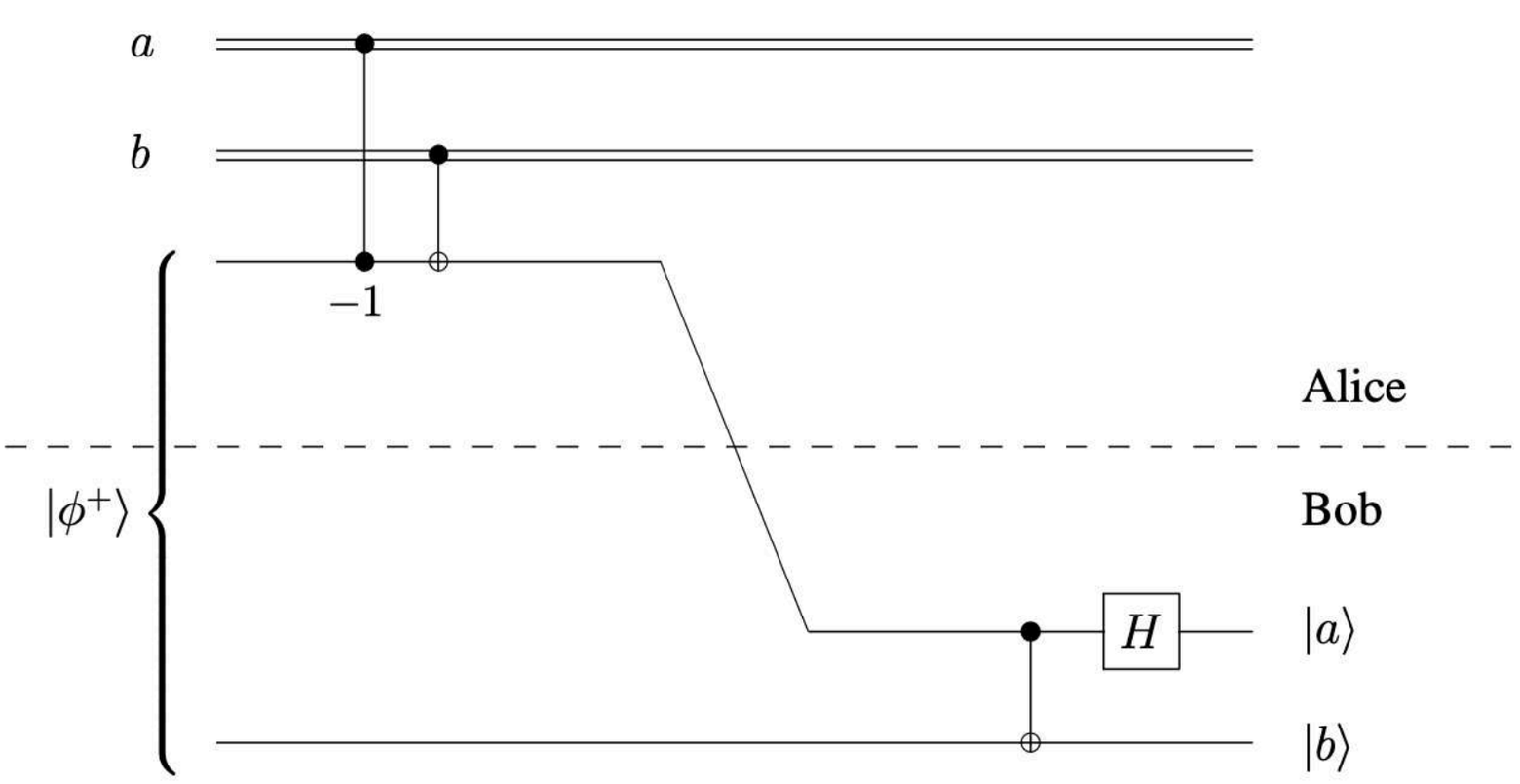
Superdense coding protocol

ab	state after step 1	state after step 2	state after step 4	state after step 5
00	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\left(\frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle\right)\|0\rangle$	$\|00\rangle$
01	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|10\rangle + \frac{1}{\sqrt{2}}\|01\rangle$	$\left(\frac{1}{\sqrt{2}}\|1\rangle + \frac{1}{\sqrt{2}}\|0\rangle\right)\|1\rangle$	$\|01\rangle$
10	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\left(\frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle\right)\|0\rangle$	$\|10\rangle$
11	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|10\rangle - \frac{1}{\sqrt{2}}\|01\rangle$	$\left(\frac{1}{\sqrt{2}}\|1\rangle - \frac{1}{\sqrt{2}}\|0\rangle\right)\|1\rangle$	$-\|11\rangle$

When Bob measures at the end of the protocol, it is clear that he sees ab as required.

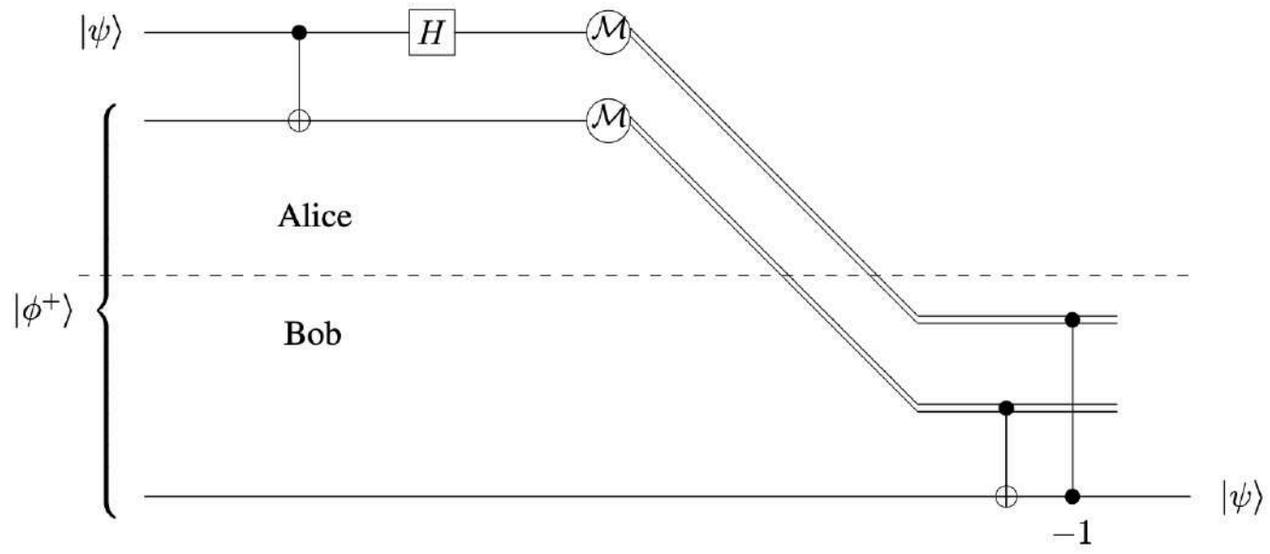
First gate represent a Controlled-σ_z =

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



Quantum Teleportation

Quantum Teleportation



Let us assume that $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. The starting state is

$$(\alpha\,|0\rangle + \beta\,|1\rangle)\left(\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle\right) = \frac{1}{\sqrt{2}}\,(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle)\,.$$

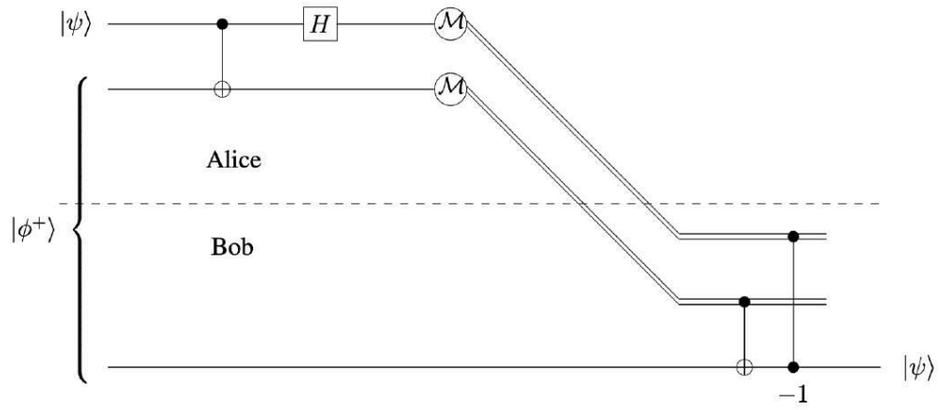
First the CNOT gate is applied, which transforms the state to

$$\frac{1}{\sqrt{2}}\,(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle)\,.$$

Next, the Hadamard transform is applied, which transforms the state to

$$\begin{aligned}&\frac{1}{2}\,(\alpha\,|000\rangle + \alpha\,|100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|010\rangle - \beta\,|110\rangle + \beta\,|001\rangle - \beta\,|101\rangle)\\ &= \frac{1}{2}\,|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + \frac{1}{2}\,|01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + \frac{1}{2}\,|10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + \frac{1}{2}\,|11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle).\end{aligned}$$

Quantum Teleportation



Case 1: Alice measures 00. This happens with probability

$$\left\| \frac{1}{2}(\alpha\,|0\rangle + \beta\,|1\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle).$$

Alice transmits the classical bits 00 to Bob. Because both bits are zero, he does not perform either of the two possible operations, and so his qubit remains in the state $\alpha\,|0\rangle + \beta\,|1\rangle$ at the end of the protocol.

Case 2: Alice measures 01. This happens with probability

$$\left\| \frac{1}{2}(\alpha\,|1\rangle + \beta\,|0\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle).$$

Alice transmits the classical bits 01 to Bob. Because the first transmitted bit is 0 and the second is 1, Bob performs a NOT operation on his qubit. Thus, the state of his qubit becomes $\alpha\,|0\rangle + \beta\,|1\rangle$.

Quantum Teleportation

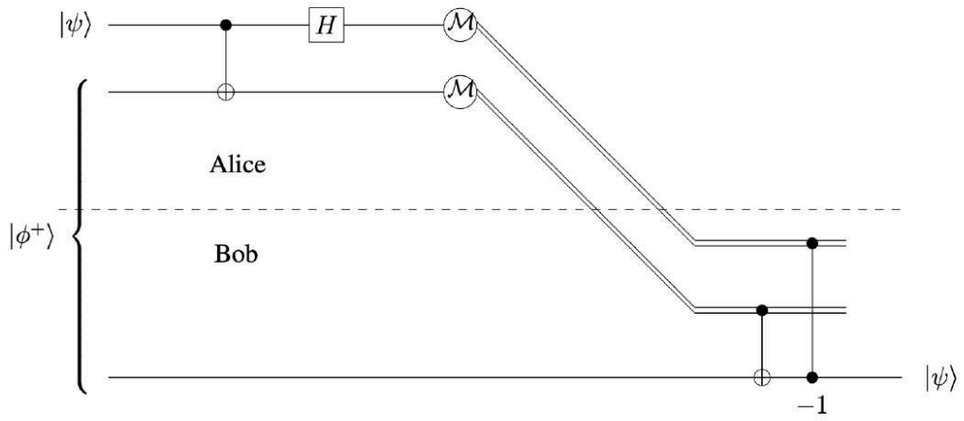
Case 3: Alice measures 10. This happens with probability

$$\left\| \frac{1}{2}(\alpha \left|0\right\rangle - \beta \left|1\right\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$\left|10\right\rangle (\alpha \left|0\right\rangle - \beta \left|1\right\rangle).$$

Alice transmits the classical bits 10 to Bob. Because the first transmitted bit is 1 and the second is 0, Bob performs a σ_z operation on his qubit. Thus, the state of his qubit becomes $\alpha \left|0\right\rangle + \beta \left|1\right\rangle$.



Case 4: Alice measures 11. This happens with probability

$$\left\| \frac{1}{2}(\alpha \left|1\right\rangle - \beta \left|0\right\rangle) \right\|^2 = \frac{1}{4}.$$

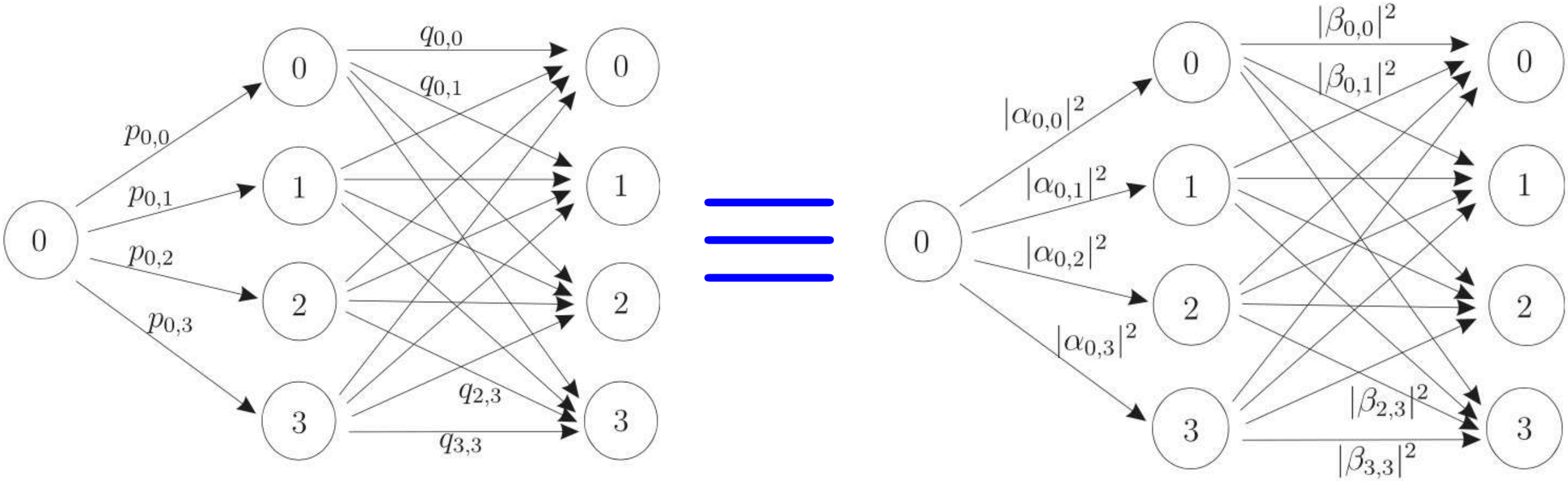
Conditioned on this outcome, the state of the three qubits becomes

$$\left|11\right\rangle (\alpha \left|1\right\rangle - \beta \left|0\right\rangle).$$

Alice transmits the classical bits 11 to Bob. Because both transmitted bits are 1, Bob first performs a NOT operation on his qubit, transforming it to $\alpha \left|0\right\rangle - \beta \left|1\right\rangle$, and then performs a σ_z gate to it, transforming it to the state $\alpha \left|0\right\rangle + \beta \left|1\right\rangle$.

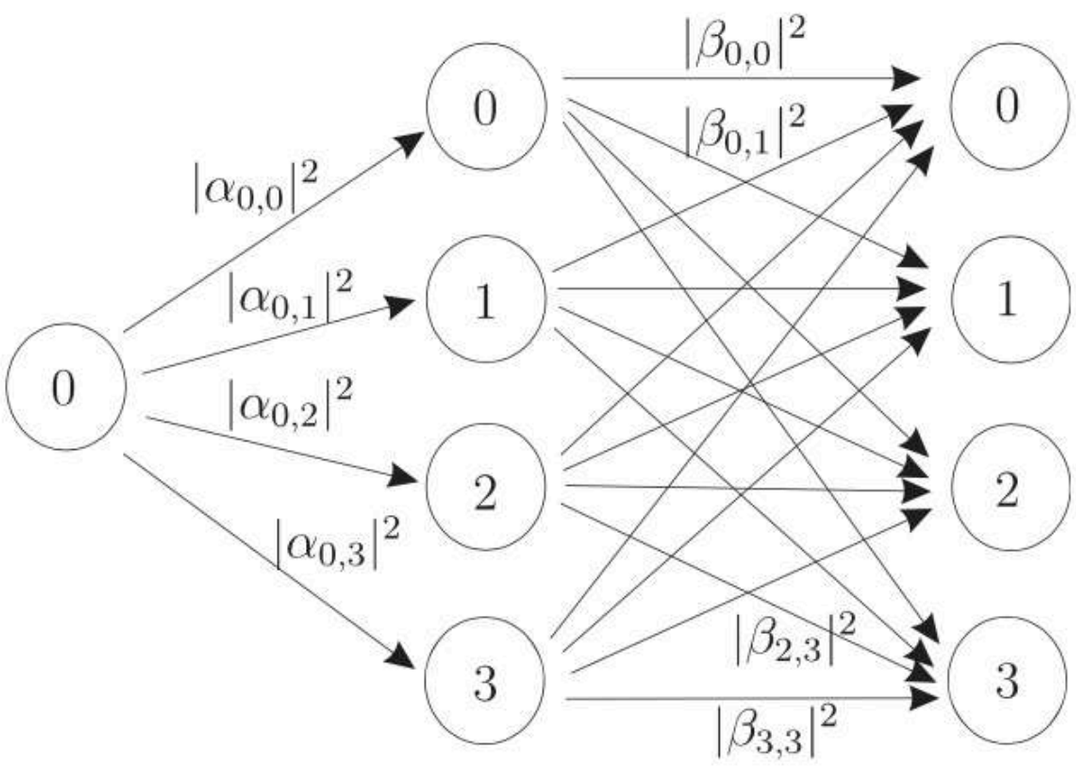
Quantum Algorithms

Probabilistic versus quantum algorithms

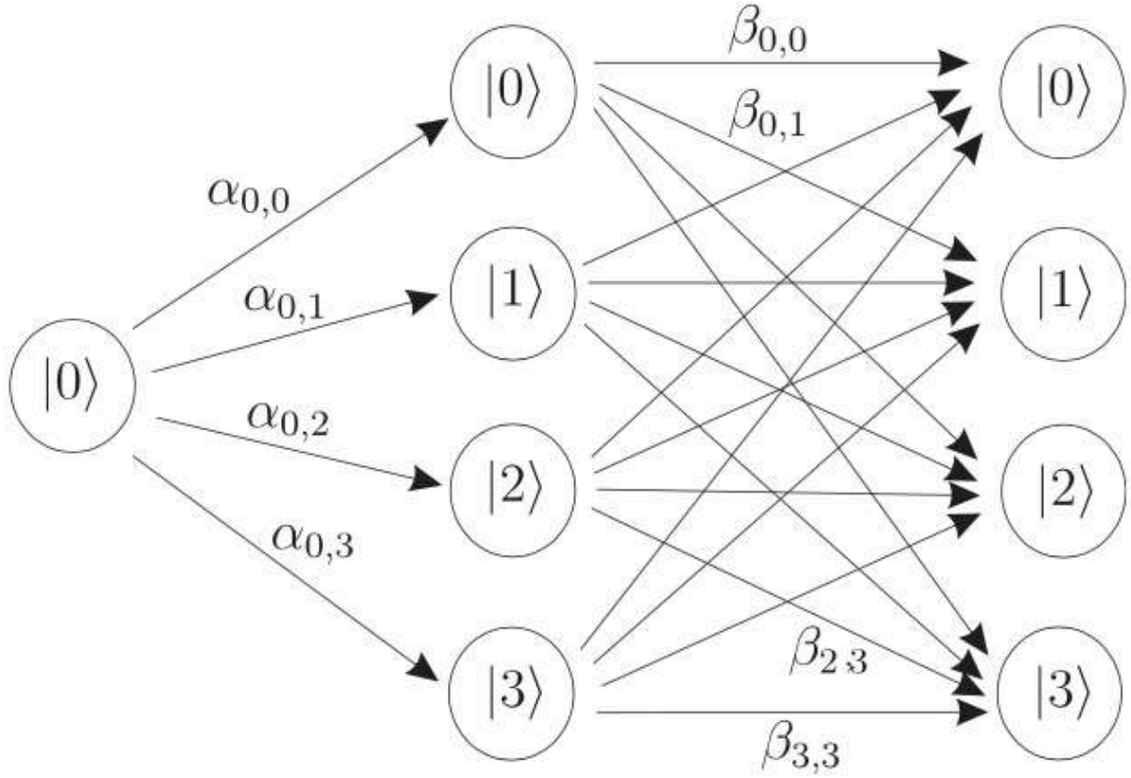


Quantum Algorithms

Probabilistic versus quantum algorithms

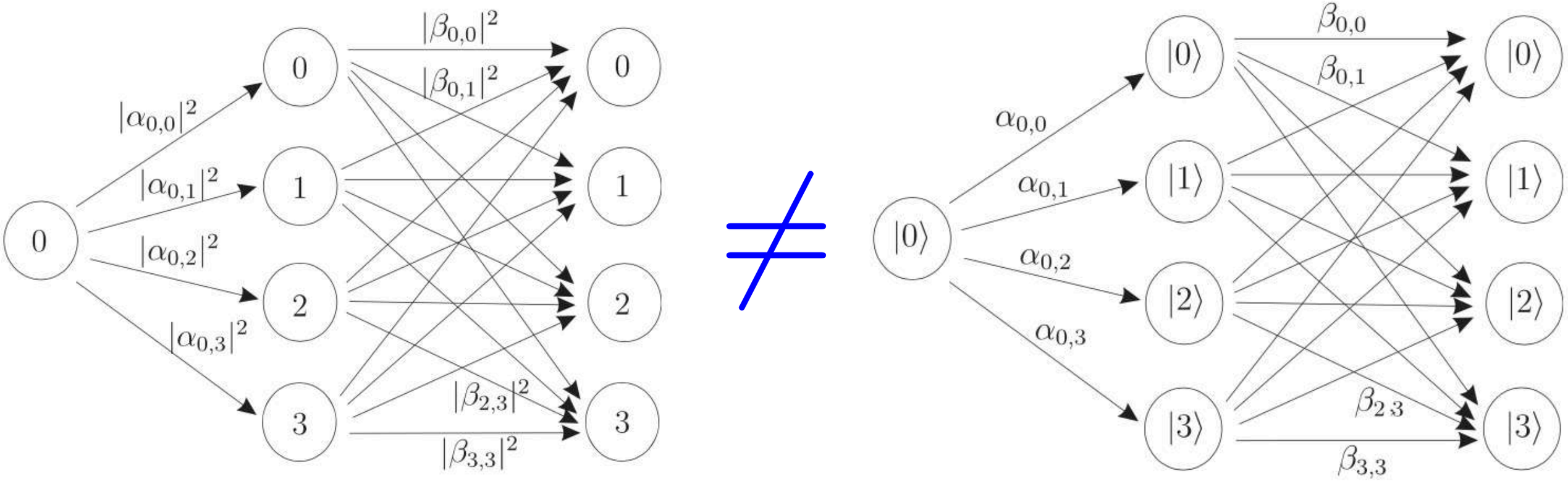


≠



Quantum Algorithms

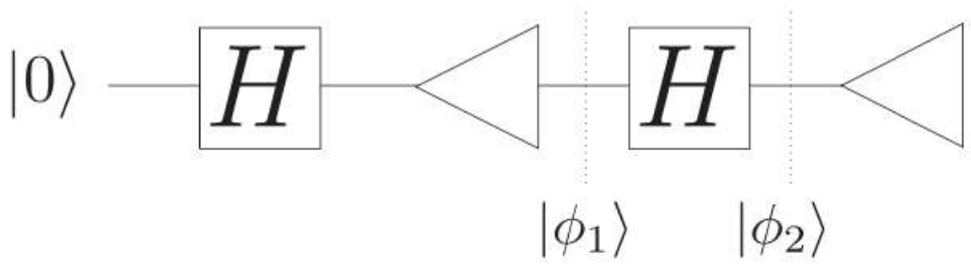
Probabilistic versus quantum algorithms

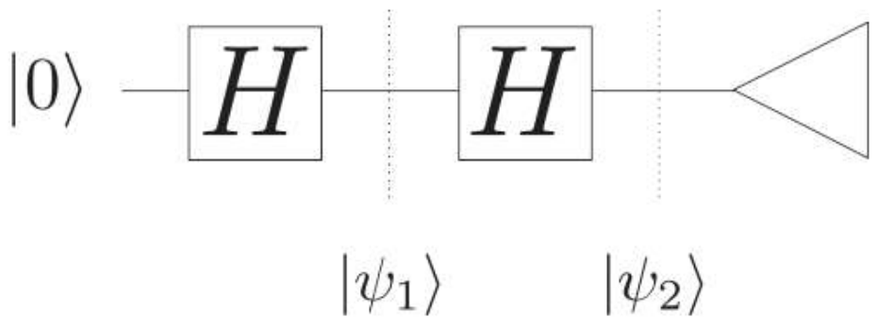


No interference versus interference

Quantum Algorithms

No interference versus interference





$$|\phi_1\rangle = \begin{cases} |0\rangle \text{ with probability } \frac{1}{2} \\ |1\rangle \text{ with probability } \frac{1}{2}. \end{cases}$$

$$|\phi_2\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ with probability } \frac{1}{2} \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ with probability } \frac{1}{2}. \end{cases}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

$$\begin{aligned} |\psi_2\rangle &= H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}H|0\rangle + \frac{1}{\sqrt{2}}H|1\rangle \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle \\ &= |0\rangle. \end{aligned}$$

Phase Kick-Back to control register

Phase Kick-Back to control register

$$\text{CNOT} \;:\; |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Phase Kick-Back to control register

$$\text{CNOT} \;:\; |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\text{CNOT} \;:\; |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |1\rangle \left((-1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = -|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Phase Kick-Back to control register

$$\text{CNOT} \ : \ |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\text{CNOT} \ : \ |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |1\rangle \left((-1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = -|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\text{CNOT} \ : \ \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Phase Kick-Back to control register

$$\text{CNOT} \ : \ |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\text{CNOT} \ : \ |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow |1\rangle \left((-1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = -|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\text{CNOT} \ : \ \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\text{CNOT} \ : \ |b\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow (-1)^b |b\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Phase Kick-Back to control register

$$\text{CNOT} \;:\; (\alpha_0|0\rangle + \alpha_1|1\rangle)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow (\alpha_0|0\rangle - \alpha_1|1\rangle)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Z-operation on control qubit (phase kick-back to control register).

Phase Kick-Back to control register

More general 2 qubit operation U_f implementing an arbitrary function $f : \{0,1\} \longrightarrow \{0,1\}$ by mapping

$$U_f \ : \ |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle$$

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

Depending on the two cases : $f(x) = 0$ and $f(x) = 1$ we have

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

When control qubit is in superposition

$$U_f \ : \ (\alpha_0|0\rangle + \alpha_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow ((-1)^{f(0)}\alpha_0|0\rangle + (-1)^{f(1)}\alpha_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

You can notice that the state of the second registrar $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of U_f and the eigenvalue $(-1)^{f(x)}$ is kicked back in front of the control registrar. This technique of inputting an eigenstate to the target qubit of an operator and associating the eigenvalue with the state of the control register will be very useful in eigenvalue estimation.

Quantum Phase Estimation

Hadamard operation is self-inverse operation (It does the opposite as well) and it can be used to encode information into the phases.

$$H|x\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^x|1\rangle\right] = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle.$$

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

The value of x is encoded into the relative phases between the basis states $|0\rangle$ and $|1\rangle$.

Hadamard operation on an $n-$qubit basis state is given by

$$H^{\otimes n}|X\rangle = \frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle.$$

Information about the value of X is encoded into the phases $(-1)^{X\cdot Y}$.

$$H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle\right) = H^{\otimes n}(H^{\otimes n}|X\rangle) = (H^{\otimes n}H^{\otimes n})|X\rangle = \mathbb{1}|X\rangle.$$

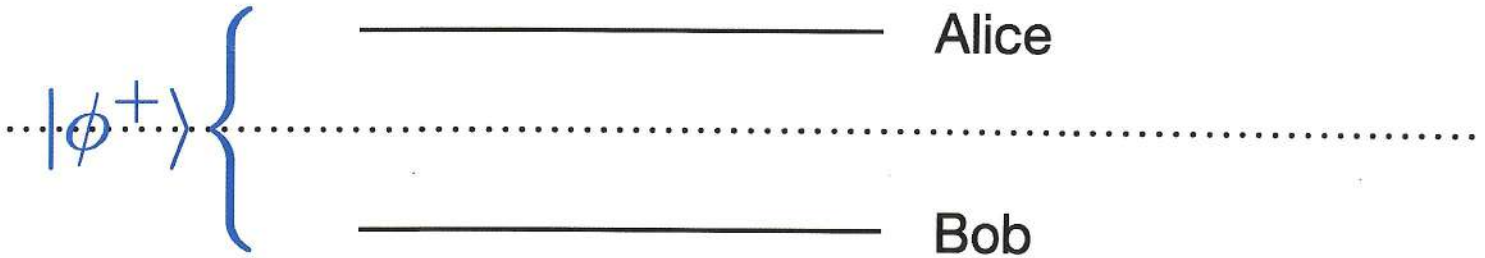
Note that $(-1)^{X\cdot Y}$ are phases of specific form. General form is a complex number $e^{2\pi i\omega}$ for any real number $\omega \in (0,1)$ (phase "-1" corresponds to $\omega = \frac{1}{2}$). The $n-$qubit Hadamard operation is not able to fully access information that is encoded in more general ways.

Superdense coding

Alice and Bob are in different parts of the world. Alice has two bits : ***a*** and ***b.*** She would like to communicate these two bits to **Bob** by sending him just a single qubit. Alice cannot encode two classical bit into a single qubit in any way that would give Bob more than just one bit of information about the pair ***(a, b).***

This can be accomplished with additional resources, if Alice and Bob share an entangled bit (e-bit).

$$|\Psi_{AB}\rangle = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Superdense coding protocol

1. If $a = 1$, Alice applies the unitary transformation

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

   to the qubit A. (If $a = 0$ she does not.)

2. If $b = 1$, Alice applies the unitary transformation

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

   to the qubit A. (If $b = 0$ she does not.)

3. Alice sends the qubit A to Bob. (This is the only qubit that is sent during the protocol.)

4. Bob applies a controlled-NOT operation to the pair (A, B), where A is the control and B is the target. The corresponding unitary matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

5. Bob applies a Hadamard transform to A.

6. Bob measures both qubits A and B. The output will be (a, b) with certainty.

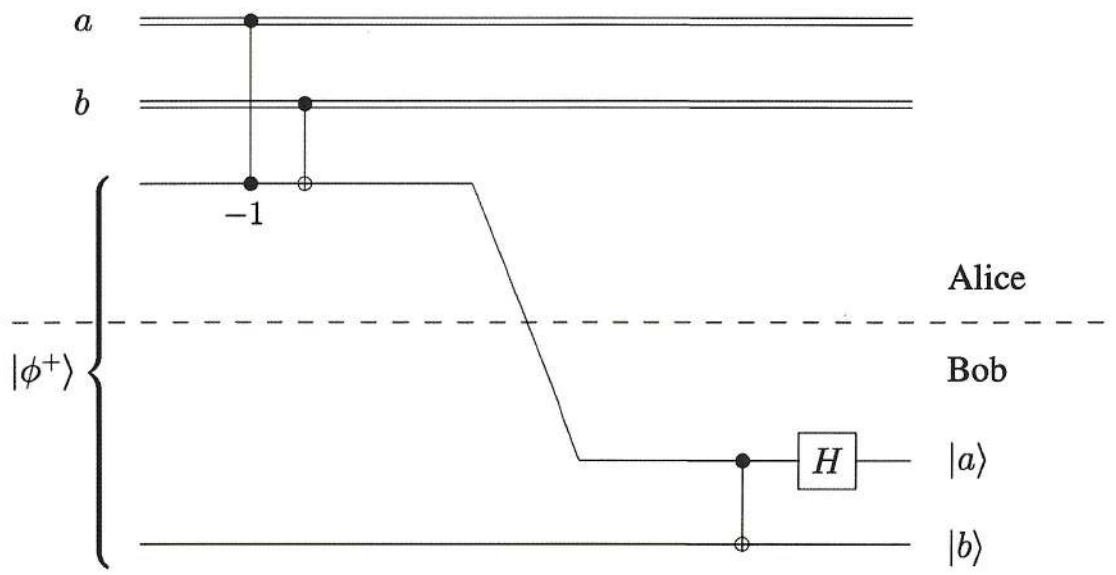
Superdense coding protocol

ab	state after step 1	state after step 2	state after step 4	state after step 5
00	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\left(\frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle\right)\|0\rangle$	$\|00\rangle$
01	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|10\rangle + \frac{1}{\sqrt{2}}\|01\rangle$	$\left(\frac{1}{\sqrt{2}}\|1\rangle + \frac{1}{\sqrt{2}}\|0\rangle\right)\|1\rangle$	$\|01\rangle$
10	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\left(\frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle\right)\|0\rangle$	$\|10\rangle$
11	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\frac{1}{\sqrt{2}}\|10\rangle - \frac{1}{\sqrt{2}}\|01\rangle$	$\left(\frac{1}{\sqrt{2}}\|1\rangle - \frac{1}{\sqrt{2}}\|0\rangle\right)\|1\rangle$	$-\|11\rangle$

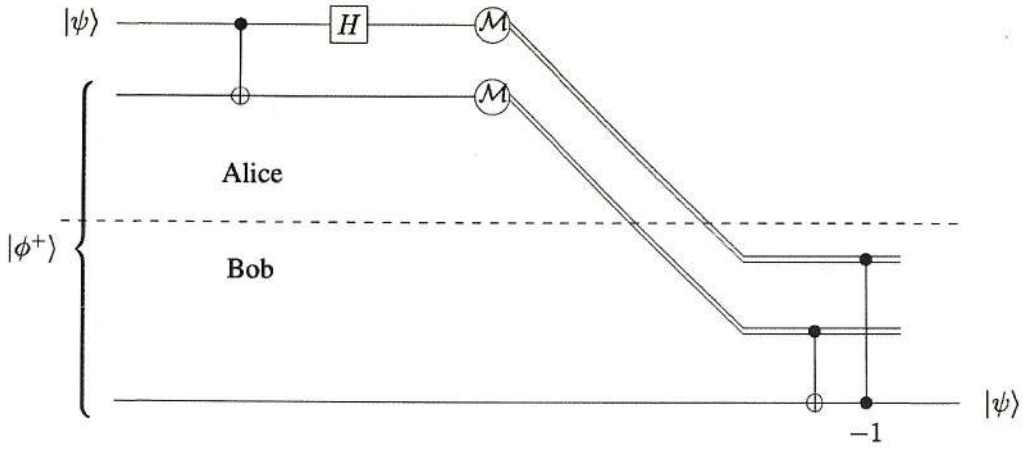
When Bob measures at the end of the protocol, it is clear that he sees ab as required.

First gate represent a Controlled-σ_z =

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



Quantum Teleportation



Let us assume that $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The starting state is

$$(\alpha|0\rangle + \beta|1\rangle)\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$

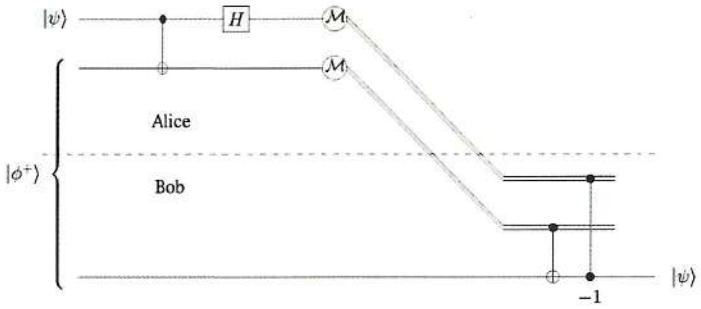
First the CNOT gate is applied, which transforms the state to

$$\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle).$$

Next, the Hadamard transform is applied, which transforms the state to

$$\frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle)$$
$$= \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle).$$

Quantum Teleportation



Case 1: Alice measures 00. This happens with probability

$$\left\| \frac{1}{2}(\alpha |0\rangle + \beta |1\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|00\rangle (\alpha |0\rangle + \beta |1\rangle).$$

Alice transmits the classical bits 00 to Bob. Because both bits are zero, he does not perform either of the two possible operations, and so his qubit remains in the state $\alpha |0\rangle + \beta |1\rangle$ at the end of the protocol.

Case 2: Alice measures 01. This happens with probability

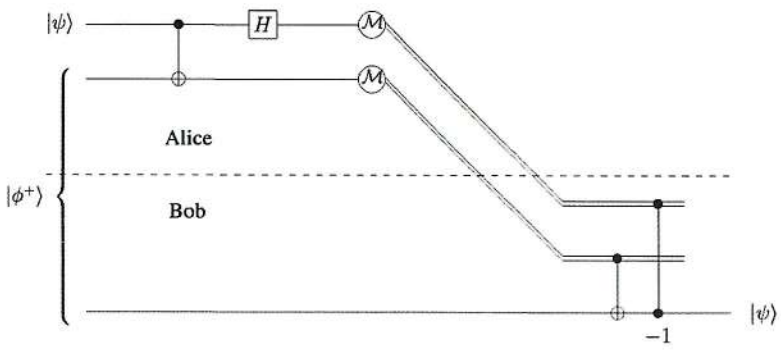
$$\left\| \frac{1}{2}(\alpha |1\rangle + \beta |0\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|01\rangle (\alpha |1\rangle + \beta |0\rangle).$$

Alice transmits the classical bits 01 to Bob. Because the first transmitted bit is 0 and the second is 1, Bob performs a NOT operation on his qubit. Thus, the state of his qubit becomes $\alpha |0\rangle + \beta |1\rangle$.

Quantum Teleportation



Case 3: Alice measures 10. This happens with probability

$$\left\| \frac{1}{2}(\alpha |0\rangle - \beta |1\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

$$|10\rangle (\alpha |0\rangle - \beta |1\rangle).$$

Alice transmits the classical bits 10 to Bob. Because the first transmitted bit is 1 and the second is 0, Bob performs a σ_z operation on his qubit. Thus, the state of his qubit becomes $\alpha |0\rangle + \beta |1\rangle$.

Case 4: Alice measures 11. This happens with probability

$$\left\| \frac{1}{2}(\alpha |1\rangle - \beta |0\rangle) \right\|^2 = \frac{1}{4}.$$

Conditioned on this outcome, the state of the three qubits becomes

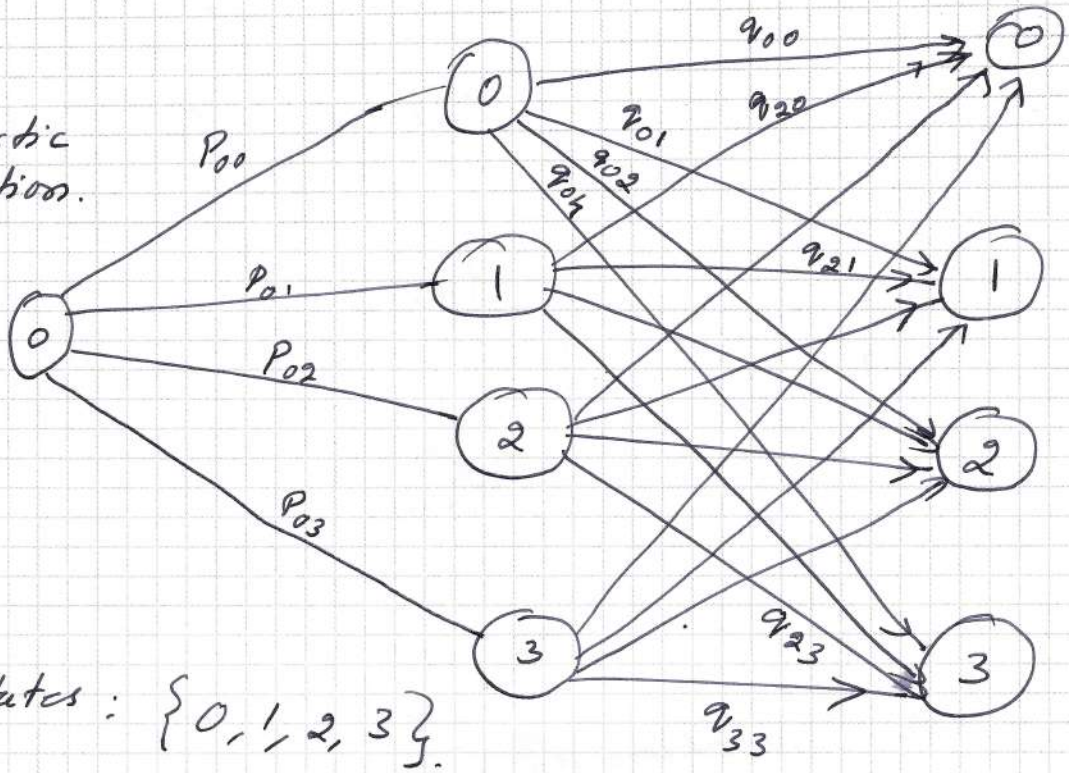
$$|11\rangle (\alpha |1\rangle - \beta |0\rangle).$$

Alice transmits the classical bits 11 to Bob. Because both transmitted bits are 1, Bob first performs a NOT operation on his qubit, transforming it to $\alpha |0\rangle - \beta |1\rangle$, and then performs a σ_z gate to it, transforming it to the state $\alpha |0\rangle + \beta |1\rangle$.

Quantum Algorithms

→ Probabilistic versus quantum algorithms

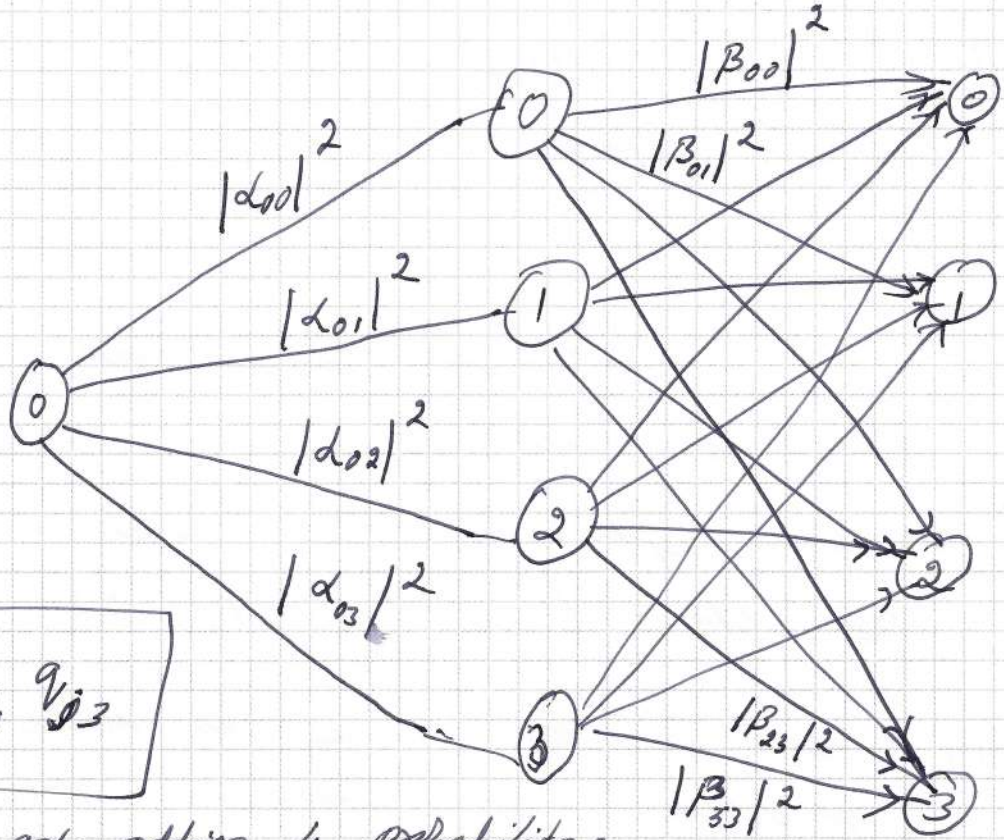
Probabilistic computation.



Four states : $\{0, 1, 2, 3\}$.

P_{0j}

Probabilistic computation in quantum setting



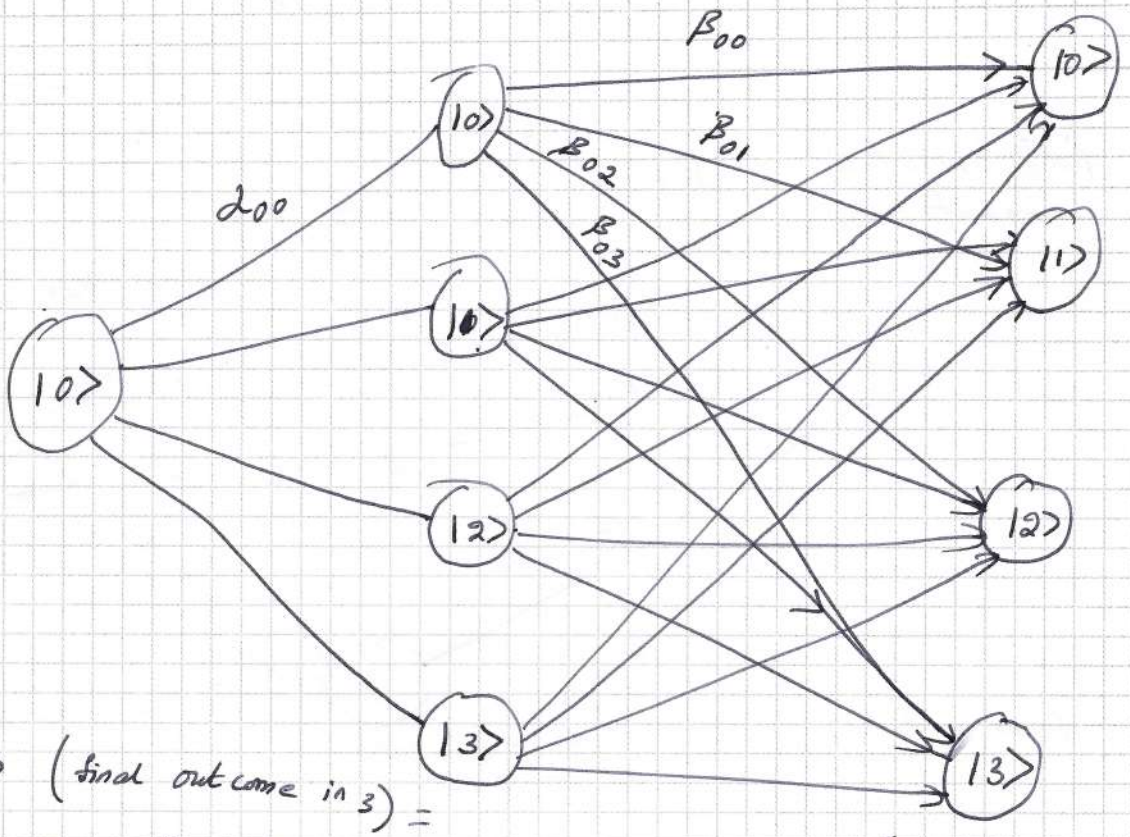
$P_{0j} = |\alpha_{0j}|^2$

$q_{jk} = |\beta_{jk}|^2$

$$\text{Prob}(\text{at } 3) = \sum_j P_{0j}\, q_{j3}$$

you get adding 4 probabilities

Fully Quantum computation



Prob (final outcome in 3) =

in classical probabilistic computation.

$$\sum_j |\alpha_{0j}|^2 |\beta_{j3}|^2.$$

$$= \sum_j |\alpha_{0j}\beta_{j3}|^2$$

Prob (final outcome in 3)

in Quantum setting

$$= \left| \sum_j \alpha_{0j}\beta_{j3} \right|^2$$

Interference shows up.

This happens only when we don't make measurement till the completion of all the steps in the algorithm.

* In some algorithms you can make partial measurement or complete measurement after few steps (after some interference has happened)

1. Phase kick-back to control register.

CNOT : $\text{CNOT}\left[|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right] = |0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

$$\text{CNOT}\left[|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right] = |1\rangle\left(\frac{|1\rangle-|0\rangle}{\sqrt{2}}\right)$$

$$= (-1)\left[|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right]$$

↓ phase

when $b \in \{0,1\}$

$$\longrightarrow \text{CNOT}\left[|b\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right] = (-1)^b |b\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

When control bit is in superposition

$$\longrightarrow \text{CNOT}\left[\alpha_0|0\rangle + \alpha_1|1\rangle\right)\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

$$= \left(\alpha_0|0\rangle - \alpha_1|1\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

Equivatant to applying 'Z' gate on control qubit.

(Q) What will happen if we replace CNOT by more general 2-qubit unitary (U_2) operation & implementing $e_i : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$ by mapping $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$

$$U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle \qquad (4)$$

$$U_f\left[|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] = \frac{U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle}{\sqrt{2}}$$

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

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

If $f(x) = 0$ action of '$\oplus f(x)$' has no effect.

$\Rightarrow b \oplus 0 = b$

If $f(x) = 1$ action of '$\oplus f(x)$' flips the state.

$\Rightarrow b \oplus 1 = a$

$f(x) = 0$: $\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$f(x) = 1$: $\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \frac{|1\rangle - |0\rangle}{\sqrt{2}}$

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

Depending on value of $f(x)$ two possibilities differ by a factor of (-1).

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

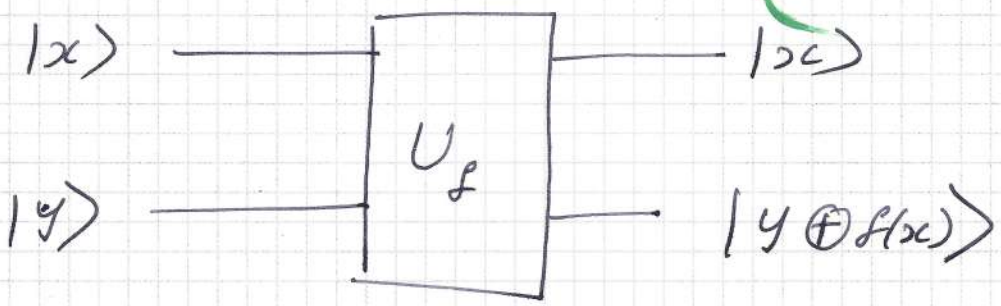
$$\Rightarrow \quad |x\rangle (-1)^{f(x)} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

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

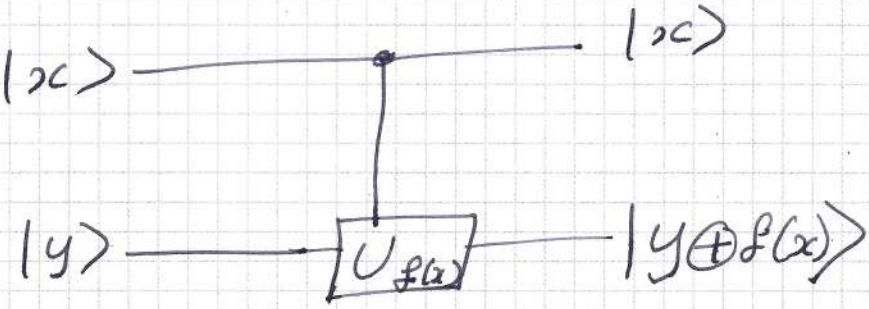
$$U_f \left(\alpha_0 |0\rangle + \alpha_1 |1\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = \left((-1)^{f(0)} \alpha_0 |0\rangle + (-1)^{f(1)} \alpha_1 |1\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

In circuit representation.

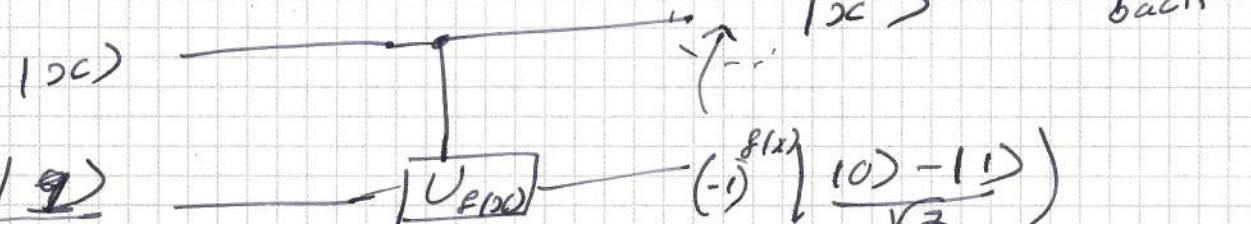
$\Rightarrow$



$\equiv$



If second registaar is $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ phase kicked back



Deutsch's Algorithm (1996)

Suppose we are given a Boolean function

$f: \{0,1\} \to \{0,1\}$ and we are told that it is constant or balanced.

we have to find out whether the function is constant or balanced.

What is constant function?

$$f(0) = f(1) = 0 \quad \text{or} \quad f(0) = f(1) = 1.$$

What is balanced function?

$$\left.\begin{aligned} f(0) = 0 \neq f(1) = 1 \\ f(0) = 1 \neq f(1) = 0 \end{aligned}\right\} f(0) \neq f(1)$$

To know whether given function is constant or balanced we have to know the value of function at each single input, 0 and 1.

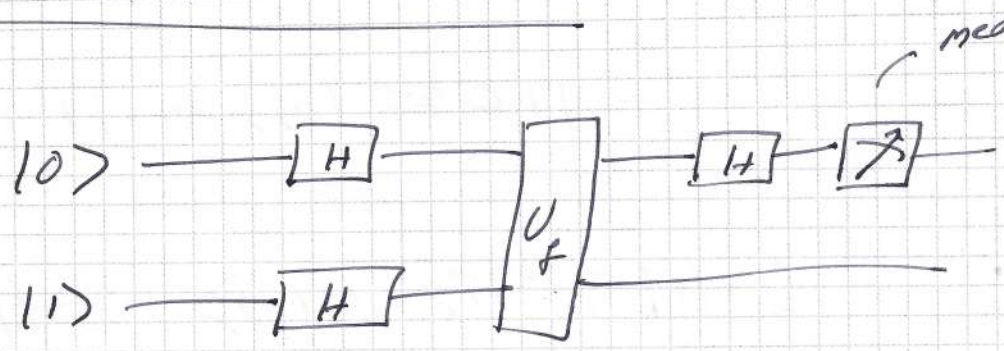
Classically the function has to be called twice.

The more call the algorithm makes to a function, the more complex and slow it becomes.

we call it query complexity

Deutsch proposed quantum algorith that reduces query complexity.

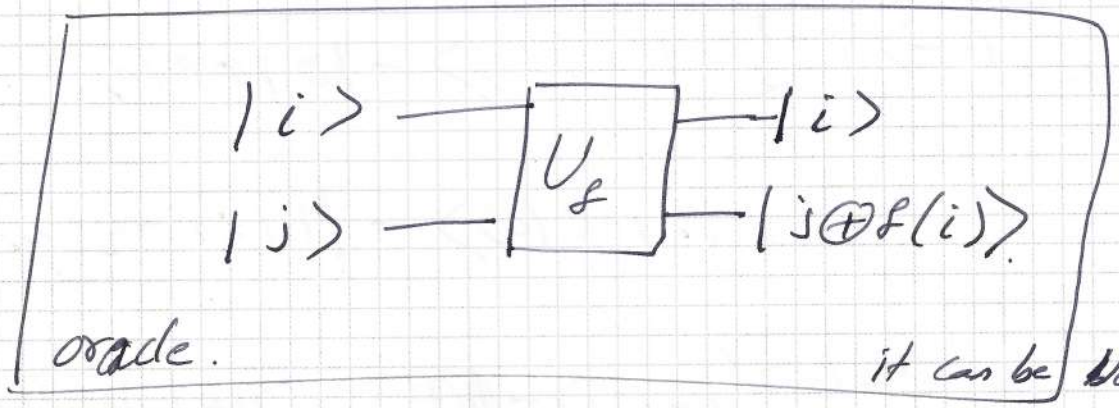
In quantum circuit form:



The gate U_f, called an oracle (XOR oracle)

$$\Rightarrow |i\rangle|j\rangle \xrightarrow{U_f} |i\rangle|j \oplus f(i)\rangle.$$

Since second qubit is controlled by 'i' first qubit input it is controlled gate.



Analysis

$$|01\rangle \xrightarrow{H\otimes H} |+-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$\xrightarrow{U_f} \frac{1}{2} U_f (|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$= \frac{1}{2}(|0\, 0\oplus f(0)\rangle - |0\, 1\oplus f(0)\rangle + |1\, 0\oplus f(1)\rangle - |1\, 1\oplus f(1)\rangle)$$

Let us assume function 'f' is constant, we can substitute $f(1)$ by $f(0)$ $= f_c$.

$$U_{f_c}|+-\rangle = \frac{1}{2}\left(|0\,0\oplus f_c(0)\rangle - |0\,1\oplus f_c(0)\rangle + |1\,0\oplus f_c(0)\rangle - |1\,1\oplus f_c(0)\rangle\right)$$

$$= \frac{1}{2}\left((|0\rangle+|1\rangle)|f_c(0)\rangle - \frac{1}{2}(|0\rangle+|1\rangle)|1\oplus f_c(0)\rangle\right)$$

$$\boxed{U_{f_c}|+-\rangle = |+\rangle\frac{1}{\sqrt{2}}\left(|f_c(0)\rangle - |1\oplus f_c(0)\rangle\right)}$$

Consider case where 'f' is balanced

$$f_b(1) = 1 - f_b(0)$$

$$U_{f_b}|+-\rangle = \frac{1}{2}\left(|0\,f_b(0)\rangle - |0\,1\oplus f_b(0)\rangle + |1\,1-f_b(0)\rangle - |1\,1\oplus 1-f_b(0)\rangle\right)$$

$$= \frac{1}{2}|0\rangle\left(|f_b(0)\rangle - |1\oplus f_b(0)\rangle\right) + \frac{1}{2}|1\rangle\left(|1-f_b(0)\rangle - |1\oplus 1-f_b(0)\rangle\right)$$

When $f_b(0) = 1$

$$U_{f_{b,1}}|+-\rangle = \frac{1}{2}|0\rangle\left(|1\rangle - |1\oplus 1\rangle\right) + \frac{1}{2}|1\rangle\left(|0\rangle - |1\oplus 1-1\rangle\right)$$

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

When $f_b(0) = 0$

$$U_{f_{b,0}} |+-\rangle = \frac{1}{2}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle(|1\rangle - |1 \oplus 1\rangle)$$

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

In summary

When 'f' is constant

$$U_{f_c} |+-\rangle = \pm |+-\rangle$$

When 'f' is balanced.

$$U_{f_b} |+-\rangle = \pm |--\rangle$$

If we apply Hadamard gate on first qubit.

~~$U_{f_c} |+-\rangle$~~

$$\left[U_{f_c} |+-\rangle\right] \xrightarrow{H \otimes \mathbb{1}} \pm |0-\rangle$$

$$U_{f_{bi}} |+-\rangle \xrightarrow{H \otimes \mathbb{1}} \pm |1-\rangle$$

If first qubit is '0' 'f' is constant

'1' 'f' is balanced.

Deutsch algorithm is more general.

suppose

$$|U\rangle = \sum_i u_i |i\rangle \qquad |b\rangle = \sum_j b_j |j\rangle.$$

$$|U\rangle|b\rangle = \sum_{ij} u_i b_j |i\,j\rangle \xrightarrow{U_f} \sum_{ij} u_i b_j |i\rangle|j \oplus f(i)\rangle$$

$$= \underline{u_0 b_0 |0\rangle|0 \oplus f(0)\rangle} + \underline{u_0 b_1 |0\rangle|1 \oplus f(0)\rangle}$$

$$+ \underline{u_1 b_0 |1\rangle|0 \oplus f(1)\rangle} + \underline{u_1 b_1 |1\rangle|1 \oplus f(1)\rangle}. \quad (A)$$

If function is constant. $f_c(0) = f_c(1)$.

$$U_{f_c}(|U\rangle|b\rangle) = (u_0 b_0 |0\rangle + u_1 b_0 |1\rangle)|f_c(0)\rangle$$

$$+ (u_0 b_1 |0\rangle + u_1 b_1 |1\rangle)|1 \oplus f_c(0)\rangle. \quad (1)$$

when f is balanced, $f_b(0) \neq f_b(1)$.

we group (1) and (4) in A, (2) and (3) terms in A.

$$U_{f_b}(|U\rangle|b\rangle) = (u_0 b_0 |0\rangle + u_1 b_1 |1\rangle)|f_b(0)\rangle \quad (2)$$

$$+ (u_0 b_1 |0\rangle + u_1 b_0 |1\rangle)|1 \oplus f_b(0)\rangle$$

Note that the above equation's (1) and (2) are telling that the bottom incoming qubit cannot be in a state with $b_0 = b_1$. If they are equal we cannot identify

For algorithm to work condition should be

$$b_0 \neq b_1.$$

For simplicity we can choose $b_0 = 1/\sqrt{2} = -b_1$

$$U_{f_c}(|u\rangle|-\rangle) = \frac{1}{\sqrt{2}}(u_0|0\rangle + u_1|1\rangle)|f_c(0)\rangle$$

$$-\frac{1}{\sqrt{2}}(u_0|0\rangle + u_1|1\rangle)|1 \oplus f_c(0)\rangle$$

$$= \frac{1}{\sqrt{2}}(u_0|0\rangle + u_1|1\rangle)(|f_c(0)\rangle - |1 \oplus f_c(0)\rangle)$$

and

$$U_{f_b}(|u\rangle|-\rangle) = \frac{1}{\sqrt{2}}(u_0|0\rangle - u_1|1\rangle)|f_b(0)\rangle$$

$$-\frac{1}{\sqrt{2}}(u_0|0\rangle - u_1|1\rangle)|1 \oplus f_b(0)\rangle$$

$$= \frac{1}{\sqrt{2}}(u_0|0\rangle - u_1|1\rangle)(|f_b(0)\rangle - |1 \oplus f_b(0)\rangle)$$

Since we want single measurement on first qubit, we need to choose u_0 and u_1 such that

$$\frac{(u_0|0\rangle + u_1|1\rangle)}{\sqrt{2}} \text{ and } \frac{(u_0|0\rangle - |u_1|1\rangle)}{\sqrt{2}}$$

are perpendicular

This will be enough to know whether 'f' is constant or balanced.

Deutsch-Jozsa algorithm (DJ)

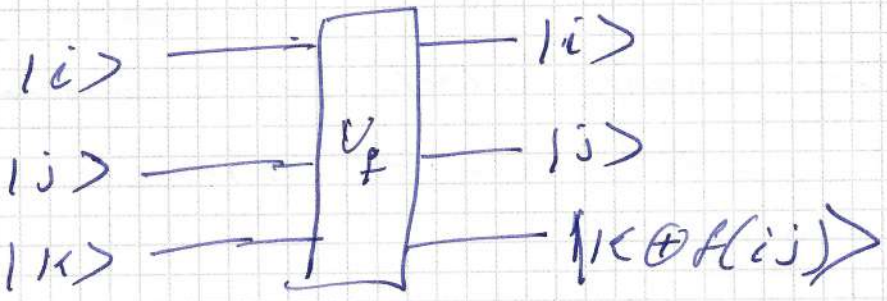
suppose you are given a Boolean function

$f: \{0,1\}^n \longrightarrow \{0,1\}$ and you are told that it is a constant or balanced.

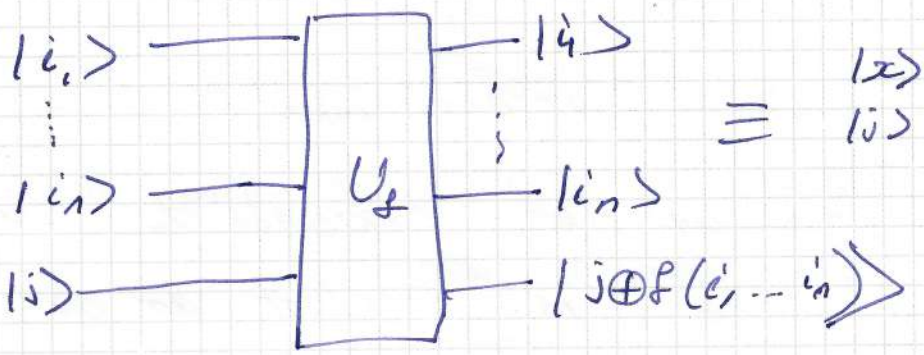
Finding whether the function is constant or balanced by calling function 'f' a fewer number of times than the classical optimal solution is what DJ algorithm will do.

'n' = 1 is a case we already discussed Deutsch algorithm

What will operations for 'n' = 2



for $n = n$



Bernstein - Vazirani Algorithm (BV)

Deutsch and Deutsch-Jozsa are twice as fast as classical computer in solving (identifying) balanced or constant functions.

→ BV algorithm will give us a linear speed up in number of queries relative to the best classical algorithm.

Definition of problem:

Let 'f' be a function from bit strings of length 'n' to a single bit,

$$f : \{0,1\}^n \longrightarrow \{0,1\},$$

such that for all input strings

$x \in \{0,1\}^n$, there exists a secret string $s \in \{0,1\}^n$ such that

$$f(x) = x \cdot s$$

('.' denotes inner product modulo 2)

The problem is to find 's' by querying 'f' as few times as possible.

Ex

$x_0 = 000$ $\quad s = 101$

$x_0 \cdot s = (0)(1) + (0)(0) + (0)(1) \pmod 2$

$= 0$

$x_1 = 001$ $\quad s = 101$

$x_1 \cdot s = (0)(1) + (0)(0) + (1)(1) \pmod 2$

$= 1$

$x_2 \cdot s = (1,0,0) \cdot (1,0,1) = 1$

Problem: Consider function f on 2 bits

x	$f(x)$
00	0
01	0
10	1
11	1

$f(x) = s \cdot x$.

can we determine secret string 's'

use: cryptography, Error correction.

How do we solve this classically?

We can solve in 'n' classical queries.

→ we send an input string 'x' into blackbox and learn value of $f(x)$.

$f(x) = x \cdot s = s$ $\quad$ [s is bit wise]

similarly

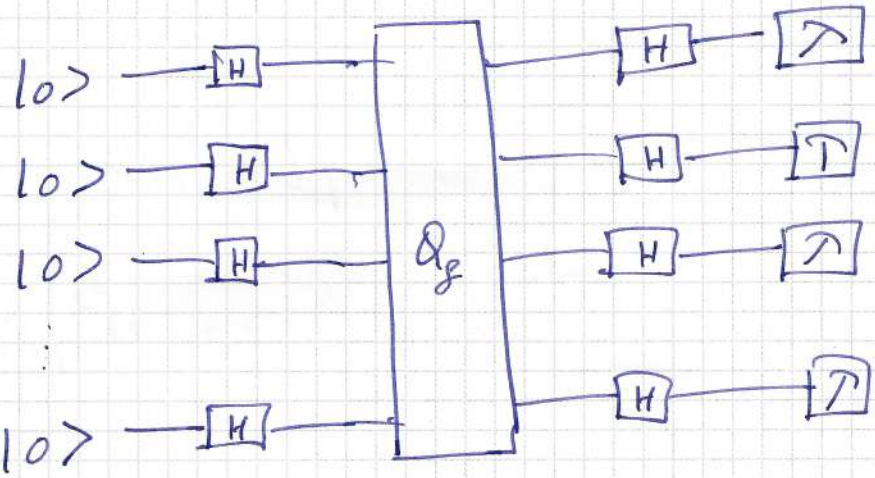
$$x_j \cdot s = s_j$$

$x_1 = 1000\ldots0$

x_j is a bit string with a 1 in the jth component and 2nd's elsewhere.

→ you need 'n' queries to determine 's' explicitly.

Quantum algorithm for this problem



Algorithm uses 'n' qubits and output each bit of secret string 's' once measurement are made.

Thereby problem is solved in one query

→ A linear speedup

$$|0\rangle^{\otimes n} \longmapsto |+\rangle^{\otimes n} = \sum_{x \in \{0,1\}^n} |x\rangle$$

At this point we make a query to our function f

$$\sum_{x\in\{0,1\}^n} |x\rangle - \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle$$

Pandhiri?

using BV function condition $f(x) = x \cdot s$

$$\sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle = \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x} |x\rangle$$

$$= \left(|0\rangle + (-1)^{s_1}|1\rangle\right) \otimes \left|(-1)^{s_2}|1\rangle\right.$$

$$= \left(|0\rangle + (-1)^{s_1}|1\rangle\right) \otimes \left(|0\rangle + (-1)^{s_2}|1\rangle\right) \otimes \cdots \left(|0\rangle + (-1)^{s_n}|1\rangle\right)$$

$$= \bigotimes_{j=1}^{n} \left(|0\rangle + (-1)^{s_j}|1\rangle\right)$$

by performing Hadamard gate on all qubits we get:

$$\longrightarrow H^{\otimes n}\left(|0\rangle - (-1)^{s_i}|1\rangle\right) = \bigotimes_{j=1}^{n} H\left(|0\rangle + (-1)^{s_j}|1\rangle\right)$$

$$= \bigotimes_{j=1}^{n} |s_j\rangle$$

By measuring all qubits we get value s_i

Simon's Algorithm

Consider a binary function $f: \{0,1\}^n \longrightarrow \{0,1\}^n$ which is evaluated by an oracle and promised to satisfy $f(x) = f(x \oplus s)$ for all $x \in \{0,1\}^n$ where an unknown bit string $s \in \{0,1\}^n$, with $s \neq 0^n$ & $f(x) \neq f(y)$ for $y \neq x \oplus s$.

($\oplus$ denotes bitwise addition modulo 2.

For example, if $x \oplus s = y$ then

$$y_j = (x_j + s_j) \bmod 2$$

for all $j \in \{0, 1, \ldots n-1\}$ the problem is to find s.

Example:

x	000	001	010	011	100	101	110	111
$f(x)$	101	010	000	110	000	110	101	010

Since $f(x) = f(x \oplus s)$ and $f(000) = f(110)$ we can find that $s = 110$

How?

$x_1 \oplus x_2$

$000 \oplus 110 = 110$

$x_1 \oplus (x_2 + s)$

$000 + 110 = 110$ → s

Classical Analysis (query)

Birthday paradox

Suppose we are in a room of 64 people
What is the probability of finding two people sharing same Birth date.

will it be 50% ?

→ If we have 'n' people we can form

$$\binom{n}{2} = \frac{n(n-1)}{2} \quad \text{pairs}$$

A paired B $\equiv$ B paired A

with increase in 'n' no. of pairs grows quadratically.

$$\frac{n(n-1)}{2} = O(n^2)$$

For birthday paradox, we know that once the no. of pairs is on the order of 365 we have good probability of finding a collision pair.

11th

For simon's problem:

After 't' queries we have t^2 pairs.

we can find matching pairs one

$$t^2 = O(2^n)$$

$$t = O(2^{n/2})$$

n-bits

2^n → combination (arrangements)

Best classical query complexity algorithm cannot be better than $O(2^{n/2})$.

→ Let analyse the probability of finding collision of output with increase in queries.

After one query of on the input 'x', the probability of getting a collision after one more input y is

$$P(x=y) = \frac{1}{2^n - 1}$$

However we have 2^n outcomes we have queried once so it is $2^n - 1$

Therefore, after 't' queries it will be

$$P(\text{collision after 't' queries}) \leq \frac{t(t-1)}{2^n - 1}$$

For this to be good say "$P = 1/2$"

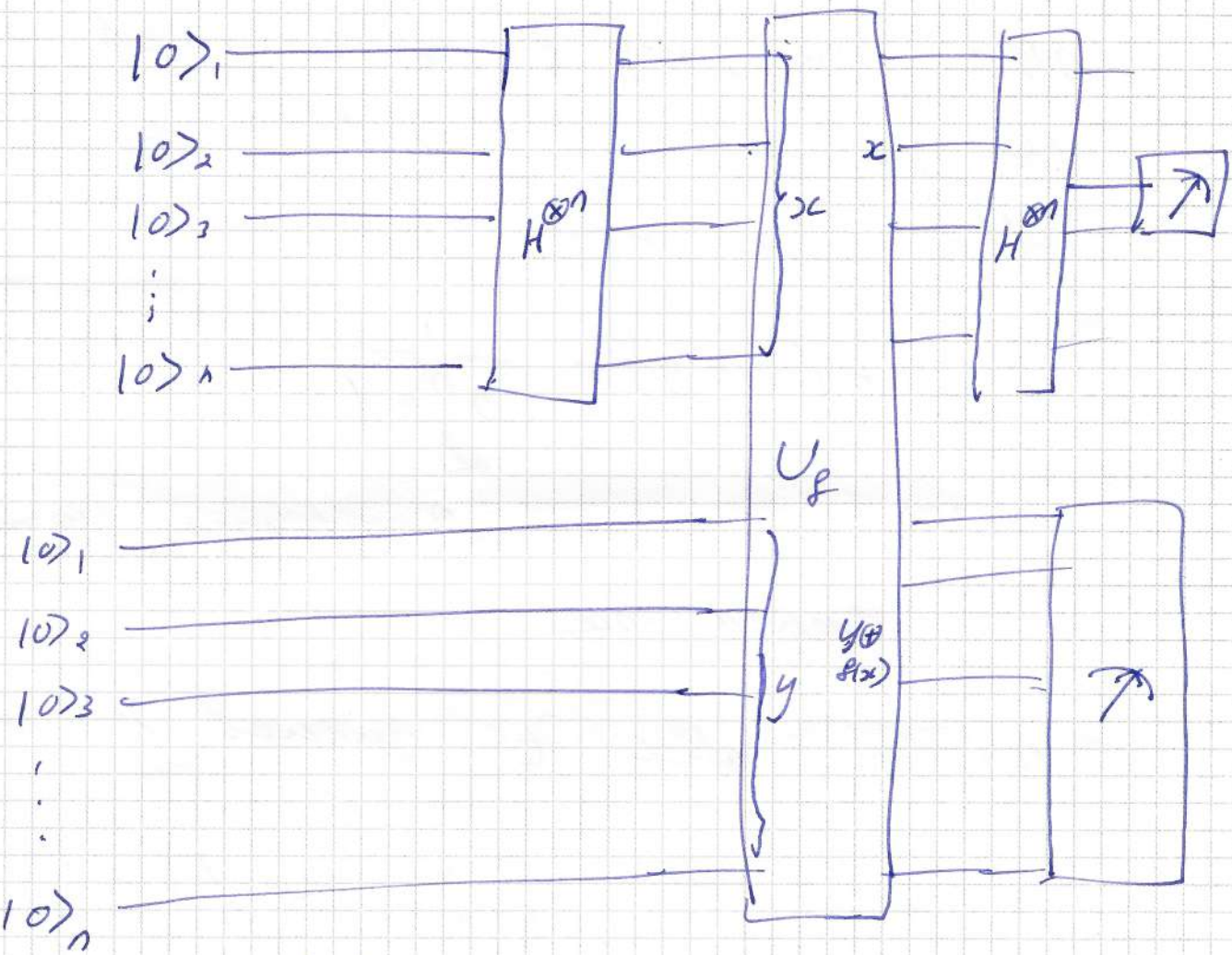
$$t = O(2^{n/2}).$$

can quantum algorithm do this better or far better?

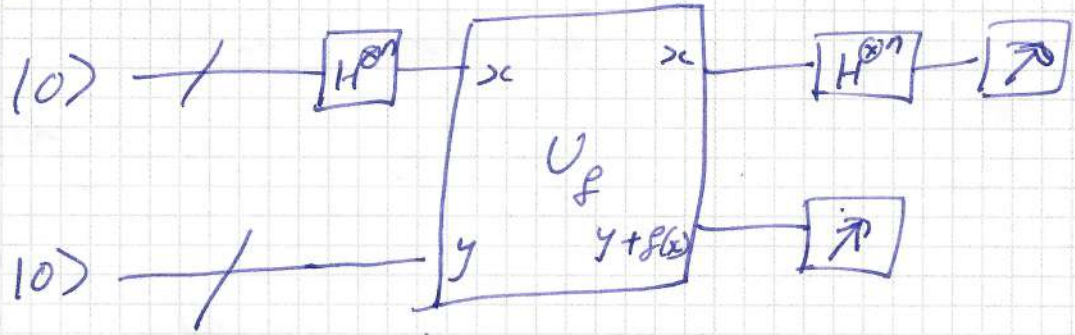
Quantum algorithm for Simon's problem

Simon's algorithm.

→ It will give is exponential speed up compared to classical.



Simplified representation:



U_f is a black box

$$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$$

Analysis

After the first Hadamard,

$$|0\rangle|0\rangle \xrightarrow{H^{\otimes n}\otimes \mathbb{1}} H^{\otimes n}|0\rangle|0\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=1}^{2^n-1} |x\rangle|0\rangle.$$

{ Remember $|0\rangle = |0\cdots0_n\rangle$ }

{ 2^n-1 }

After applying U_f (oracle) we will get

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

When we make measurement second register if the output is $f(\omega) = f(\omega \oplus s)$, the corresponding first register state will be

$$\frac{1}{\sqrt{2}}(|\omega\rangle + |\omega \oplus s\rangle).$$

Now performing Hadamard gate again on the first register we will get

$$\frac{1}{\sqrt{2}}(|\omega\rangle + |\omega\oplus s\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}}(H^{\otimes n}|\omega\rangle + H^{\otimes n}|\omega\oplus s\rangle$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(H^{\otimes n}|\omega\rangle + H^{\otimes n}|\omega\oplus s\rangle\right)$$

we should note that

$$H^{\otimes n}|\omega\rangle = H|\omega_{n-1}\rangle \otimes \cdots\cdots \otimes H|\omega_0\rangle$$

$$= \bigotimes_{j=1}^{n} H|\omega_{n-j}\rangle$$

$$= \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{w_{n-j}} |1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{j=1}^{n} \sum_{x_{n-j}=0}^{1} (-1)^{x_{n-j} w_{n-j}} |x_{n-j}\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot w} |x\rangle.$$

where $x \cdot w = x_{n-1} w_{n-1} + x_{n-2} w_{n-2} + \cdots + x_0 w_0$.

Subsitituing ~~th~~ this to First register we will get

$$\frac{1}{\sqrt{2}} \left(H^{\otimes n}|w\rangle + H^{\otimes n}|w \oplus s\rangle\right) = \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot w} |x\rangle + \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot (w \oplus s)} |x\rangle \right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} \left[(-1)^{x \cdot w} + (-1)^{x \cdot (w \oplus s)} \right] |x\rangle$$

If the measurement of the first register gives output z we will have

$$(-1)^{z \cdot w} = (-1)^{z \cdot (w \oplus s)}$$

$$\Leftrightarrow (z \cdot w) \bmod 2 = (z \cdot (w \oplus s)) \bmod 2$$

$$\Leftrightarrow (z \cdot w) \bmod 2 = (z \cdot w \oplus z \cdot s) \bmod 2$$

$$\Leftrightarrow 0 = (z \cdot s) \bmod 2.$$

Thus by calling oracle one time we will find $z \in \{0,1\}^n$ such that $z \cdot s = 0 \bmod 2$.

Now suppose we call oracle more often such that each call returns new 'z'. That is z_j will be the output of first register during 'j'th measurement.

[Given that $z_1 \neq 0^n$, but $z_1 \cdot s = 0 \bmod 2$, we can rule out half of all possibilities for $s \in \{0, \ldots, 2^n - 1\}$.]

That is

We can rule out half of the possibities of 's' value, by eliminating when $z_j \cdot s = 0 \bmod 2$.

In $(n-1)$ iteration we can obtain exact value of 's'.

Lets check the example for $n=3$ [see notes 1st page]

Suppose we measure $z_1 = 001 \neq 0^n$

We will get $(z_1 \cdot 000) \bmod 2 = 0$; $(z_1 \cdot 100) \bmod 2 = 0$

$(z_1 \cdot 001) \bmod 2 = 1$; $(z_1 \cdot 101) \bmod 2 = 1$

$(z_1 \cdot 010) \bmod 2 = 0$; $(z_1 \cdot 110) \bmod 2 = 0$

$(z_1 \cdot 011) \bmod 2 = 1$; $(z_1 \cdot 111) \bmod 2 = 1$

Now the 4 marked in red are ~~the~~ not the ~~only~~ suspects for s.

In Next iteration, if we measure $z_2 = 110 \neq 0$

$(z_2 \cdot 000) \bmod 2 = 0$ $\quad$ $(z_2 \cdot 100) \bmod 2 = 1$

$(z_2 \cdot 010) \bmod 2 = 1$ $\quad$ $(z_2 \cdot 110) \bmod 2 = 0$.

Note during each iteration we removed which are not suspected value of 's' and reduce the options by half.

From above possibility of

$$s \in \{000, 110\}$$

We know 's' cannot be 000

So value of $\boxed{s = 110}$

In summary we need to call oracle {Quantum} only $(n-1)$ times to get value of 's'

Compared to $O(2^{n/2})$ classically.

Quantum Fourier Transform

Quantum Fourier Transform (QFT) is a unitary *Discrete Fourier Transform* (DFT) upon the quantum state. DFT of a discrete function $f_1, ..., f_N$ is given by

$$\tilde{f}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} f_j,$$

where $f_0, f_1, f_2, ..., f_{N-1}$ and $\tilde{f}_1, \tilde{f}_2, ..., \tilde{f}_{N-1}$ are the input and output functions, respectively.

The inverse transform is

$$f_j \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j k/N} \tilde{f}_k.$$

In QFT we do a DFT on the amplitudes of a quantum state :

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

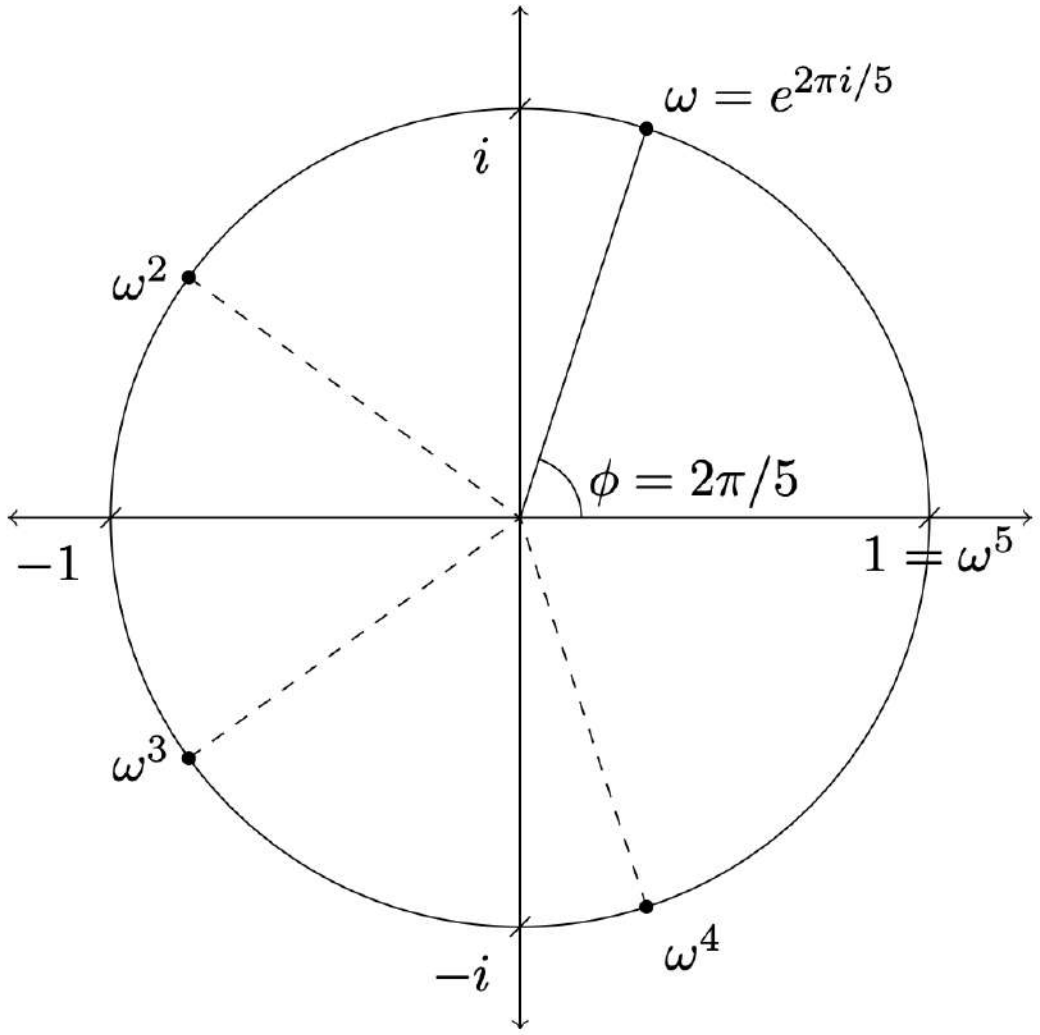
$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

amplitudes y_k are DFT of amplitudes x_j.

Quantum Fourier Transform

$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Another way of writing this is to say that the jkth entry of QFT_M is ω^{jk}.



$$QFT_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

As you can see, QFT_2 is simply equal to $H^{\otimes 2}$.
How about QFT_4? The primitive 4th root of unity is i, so that

$$QFT_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Quantum Fourier Transform

$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Another way of writing this is to say that the jkth entry of QFT_M is ω^{jk}.

$$QFT_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

As you can see, QFT_2 is simply equal to $H^{\otimes 2}$.
How about QFT_4? The primitive 4th root of unity is i, so that

$$QFT_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$$|f\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$|g\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \text{ and } |h\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

QFT_4 to $|f\rangle$.

$$\left|\hat{f}\right\rangle = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

QFT_4 on $|g\rangle$:

$$|\hat{g}\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

QFT_4 on $|h\rangle$:

$$\left|\hat{h}\right\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}$$

Quantum Fourier Transform

Let $|\Theta\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$ and $|\Phi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix}$. Then

If we need only probability, we don't see any difference

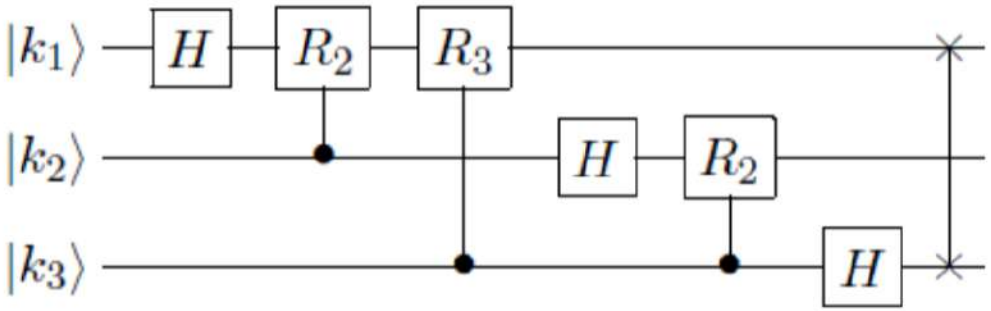
$$\left|\hat{\Theta}\right\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ \alpha_0 + i\alpha_1 - \alpha_2 - i\alpha_3 \\ \alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 \\ \alpha_0 - i\alpha_1 - \alpha_2 + i\alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

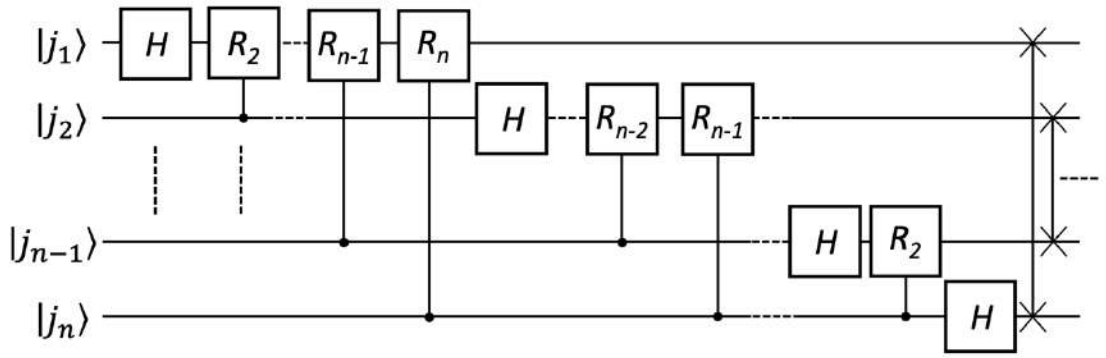
$$\left|\hat{\Phi}\right\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ -i\alpha_0 + \alpha_1 + i\alpha_2 - \alpha_3 \\ -\alpha_0 + \alpha_1 - \alpha_2 + \alpha_3 \\ i\alpha_0 + \alpha_1 - i\alpha_2 - \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ -i\beta_1 \\ -\beta_2 \\ i\beta_3 \end{pmatrix}$$

The important point here is that the only difference between $\left|\hat{\Theta}\right\rangle$ and $\left|\hat{\Phi}\right\rangle$ is a relative phase shift.

How many operations do we have to do for M X M matrix?

Quantum Fourier Transform





Where $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$ is a single qubit unitary *rotation* gate.

As an example, for $n = 3$ we have the 3-qubit product state

$$F_8|k_1k_2k_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.k_3}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.k_2k_3}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.k_1k_2k_3}|1\rangle).$$

$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

What is a quantum operational form QFT ?

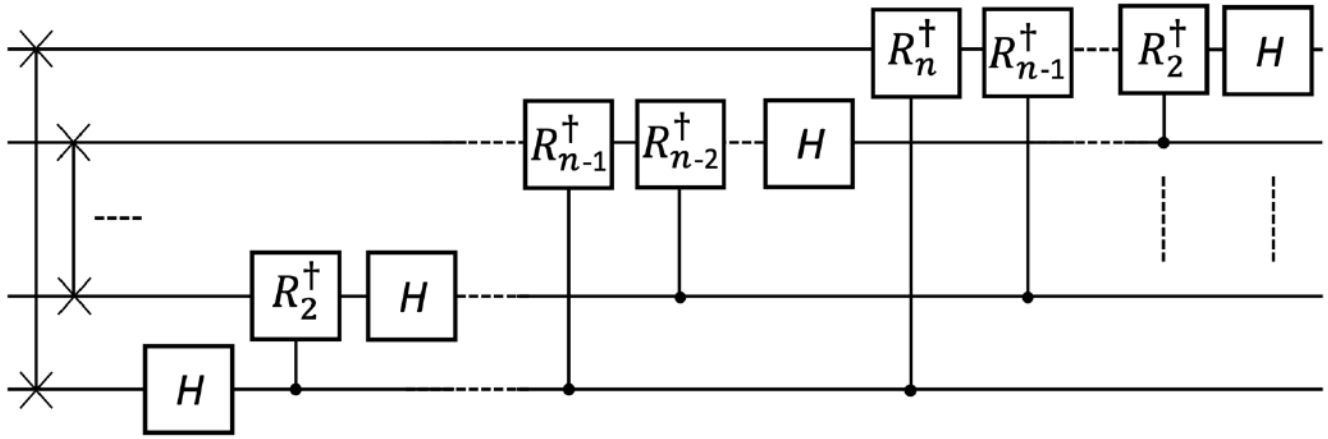
Inverse Quantum Fourier Transform

To invert the QFT, we must run the circuit in reverse, with the inverse of each gate in place to achieve the transform:

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle \rightarrow |j\rangle$$

We have already seen that the Hadamard gate is self-inverse, and the same is clearly true for the SWAP gate; the inverse of the rotations gate R_k is given by:

$$R_k^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{-2\pi i/2^k} \end{bmatrix}$$



Quantum Phase Estimation

Hadamard operation is self-inverse operation (It does the opposite as well) and it can be used to encode information into the phases.

$$H|x\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^x|1\rangle\right] = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle.$$

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

The value of x is encoded into the relative phases between the basis states $|0\rangle$ and $|1\rangle$. Hadamard operation on an $n-$qubit basis state is given by

$$H^{\otimes n}|X\rangle = \frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle.$$

Information about the value of X is encoded into the phases $(-1)^{X\cdot Y}$.

$$H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle\right) = H^{\otimes n}(H^{\otimes n}|X\rangle) = (H^{\otimes n}H^{\otimes n})|X\rangle = \mathbb{1}|X\rangle.$$

Note that $(-1)^{X\cdot Y}$ are phases of specific form. General form is a complex number $e^{2\pi i\omega}$ for any real number $\omega \in (0,1)$ (phase "-1" corresponds to $\omega = \frac{1}{2}$). The $n-$qubit Hadamard operation is not able to fully access information that is encoded in more general ways.

Useful notations and identity

Notation for binary fraction :

$$\omega = 0\ .\ x_1x_2x_3\cdots\cdots = \frac{x_1}{2} + \frac{x_2}{2^2} + \frac{x_3}{2^3} + \cdots\cdots$$

similarly, $\quad 2^k\omega = x_1x_2x_3\cdots x_k\ .\ x_{k+1}x_{k+2}\cdots$ and $e^{2\pi ik} = 1$ for any k,

$$\begin{aligned} e^{2\pi i(2^k\omega)} &= \exp[2\pi i(x_1x_2x_3\cdots x_k\ .\ x_{k+1}x_{k+2}\cdots)] \\ &= \exp[2\pi i(x_1x_2x_3\cdots x_k)]\exp[2\pi i(x_{k+1}x_{k+2}\cdots)] = \exp[2\pi i(0.x_{k+1}x_{k+2}\cdots\cdots)] \end{aligned}$$

$$0\ .\ x_lx_{l+1}x_{l+2}\cdots\cdots x_n = \frac{x_l}{2} + \frac{x_{l+1}^2}{2^2} + \frac{x_{l+2}^3}{2^3} + \cdots\cdots + \frac{x_n}{2^{n-l+1}}$$

Product representation :

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^{n-1}} e^{2\pi i\omega y}|y\rangle = \frac{|0\rangle + e^{2\pi i(2^{n-1}\omega)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(2^{n-2}\omega)}|1\rangle}{\sqrt{2}} \otimes \cdots\cdots \otimes \frac{|0\rangle + e^{2\pi i(\omega)}|1\rangle}{\sqrt{2}}$$

$$= \frac{|0\rangle + e^{2\pi i(0\ .\ x_nx_{n+1}\cdots\cdots)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0\ .\ x_{n-1}x_nx_{n+1}\cdots\cdots)}|1\rangle}{\sqrt{2}} \otimes \cdots\cdots \otimes \frac{|0\rangle + e^{2\pi i(0\ .\ x_1x_2x_3\cdots\cdots)}|1\rangle}{\sqrt{2}}$$

Quantum Phase Estimation

Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$

Problem : Obtain a good estimate of the phase parameter w

If the input is one-qubit $(n = 1)$, $\omega = 0 \,.\, x_1$ then we get

$$\frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i (0 \,.\, x_1) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i \left(\frac{x_1}{2}\right) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\pi i (x_1 y)} |y\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{y=1}^{1} (-1)^{x_1 y} |y\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{x_1} |y\rangle\right)$$

You can recall that Hadamard operation on the preceding expression will return you the value of x_1 and hence the value of ω for one-qubit.

Quantum Phase Estimation

Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$

Problem : Obtain a good estimate of the phase parameter w

When we have a two qubit state ($n = 2$), $\omega = 0 \,.\, x_1 x_2$ then using product representation we get

$$\frac{1}{\sqrt{2^2}} \sum_{y=0}^{3} e^{2\pi i(\omega)y} |y\rangle = \frac{1}{\sqrt{2^2}} \sum_{y=0}^{3} e^{2\pi i(0\,.\,x_1x_2)y} |y\rangle = \frac{|0\rangle + e^{2\pi i(0\,.\,x_2)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0\,.\,x_1x_2)}|1\rangle}{\sqrt{2}}$$

Hadamard operation on the first qubit will return the value for x_2. If $x_2 = 0$ the value of x_1 can be obtained but not if $x_2 = 1$.

To obtain x_1 when $x_2 = 1$ we need to define a phase rotation operation,

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0.01)} \end{pmatrix} \quad \text{in base 2}$$

$$R_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i(0.01)} \end{pmatrix}$$

If $x_2 = 1$, R_2^{-1} followed by an Hadamard operation (H) will return the value of x_1.

Quantum Phase Estimation

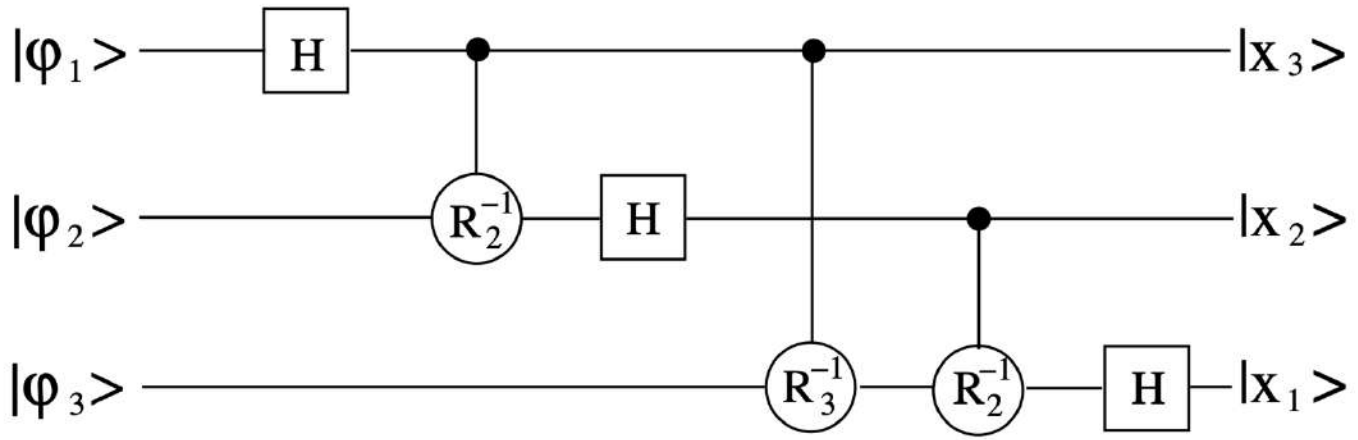
Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$

Problem : Obtain a good estimate of the phase parameter w

for a three-qubit, H on first qubit will return x_3, if $x_3 = 0$ you can find x_2, if $x_2 = 0$ find x_1 directly. If $x_3 = 1$, R_2^{-1} followed by an H will return x_2 and if $x_2 = 1$, R_3^{-1} followed by R_2^{-1} and H will return x_1. See the circuit diagram below where,

$$|\varphi_1\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_3)}|1\rangle}{\sqrt{2}} \quad ; \quad |\varphi_2\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_2 x_3)}|1\rangle}{\sqrt{2}} \quad ; \quad |\varphi_3\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_1 x_2 x_3)}|1\rangle}{\sqrt{2}}.$$



Grover's Search Algorithm (Unstructured database)

Problem : Find i such that $x_i = 1$

Queries : ask i, get x_i

Classically : $N - 1$ queries required (worst case) [N elements in search space]

Quantum : $O(\sqrt{N})$ queries [grover, 1996]

Steps Grover's algorithm

1. Begin with the computer in state $|0\rangle^{\otimes n}$. Use Hadamard transformation to put the computer in equal superposition state,

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

2. Repeat $O(\sqrt{N})$ times the following two steps (Grover iteration)

   - Apply the Oracle $O\ |x\rangle \longrightarrow (-1)^{f(x)}|x\rangle$
   - Apply the operator $U_s = 2|S\rangle\langle S| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$

3. Measure the resulting state

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{for } x = \omega, \text{ that is, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{for } x \neq \omega, \text{ that is, } f(x) = 0. \end{cases}$$

Grover's Search Algorithm (quadratic speedup)

(Unstructured database)

Intuition for a quadratic speedup (heuristic argument)

Let's take a database of N items and assign a number to each item :

$$[\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_N]$$

These are all real numbers in the classical case for which we will assign a probability for each item i-1, 1, 2,3, ... N

$$p_i = \frac{\alpha_i}{\sum_{i=1}^{N} \alpha_i} \qquad (\text{classical})$$

Probability of finding i^{th} item

$$\alpha_m = O(N) \qquad (\text{classical})).$$

Good chance of finding item index m when $p_m = O(N)$

In the quantum case, probabilities are defined using amplitudes in the wavefunction, which are in general complex numbers.

$$p_i = \frac{|\alpha_i|^2}{\sum_{i=1}^{N} |\alpha_i|^2} \qquad (\text{quantum}) \qquad p_m \text{ now goes by } |\alpha_m|^2 \qquad \text{Implies} \qquad \alpha_m = O\left(\sqrt{N}\right) \qquad (\text{quantum})$$

Grover's Search Algorithm (Unstructured database)

Problem : Find i such that $x_i = 1$

Queries : ask i, get x_i

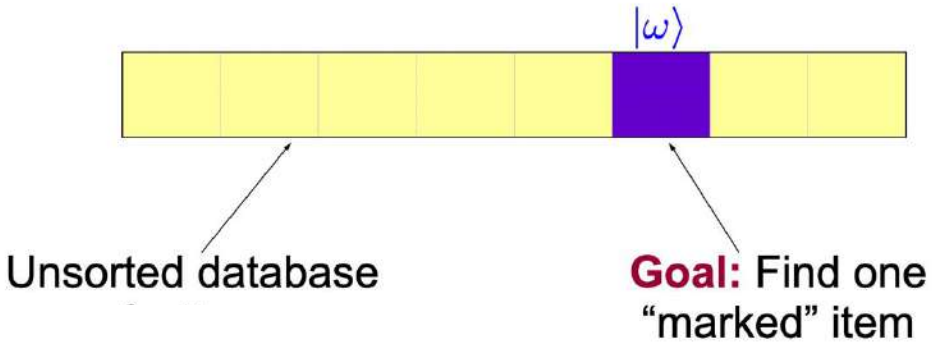
.....	0	0	1	0	0	0	0	.....

Classically : $N - 1$ queries required (worst case) [N elements in search space]

Quantum : $O(\sqrt{N})$ queries [grover, 1996]

Define the problem using quantum states

N = 2^n elements can be represented using n qubits

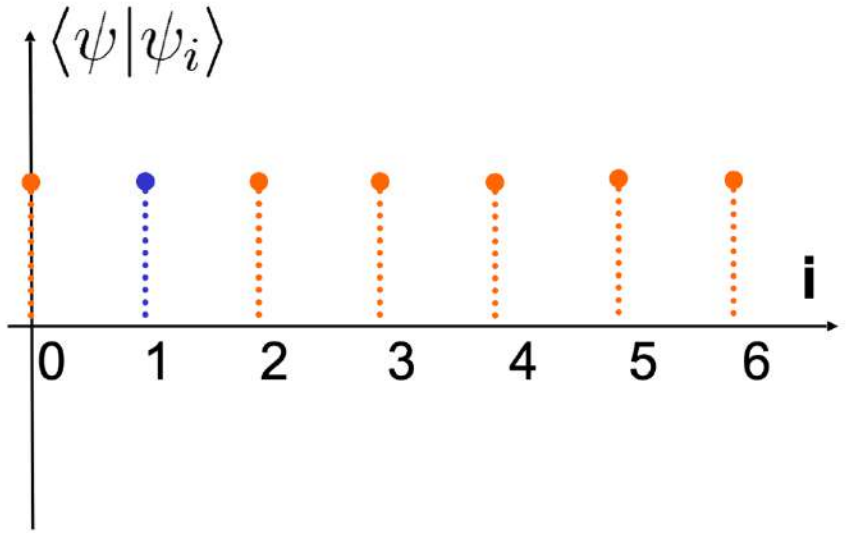


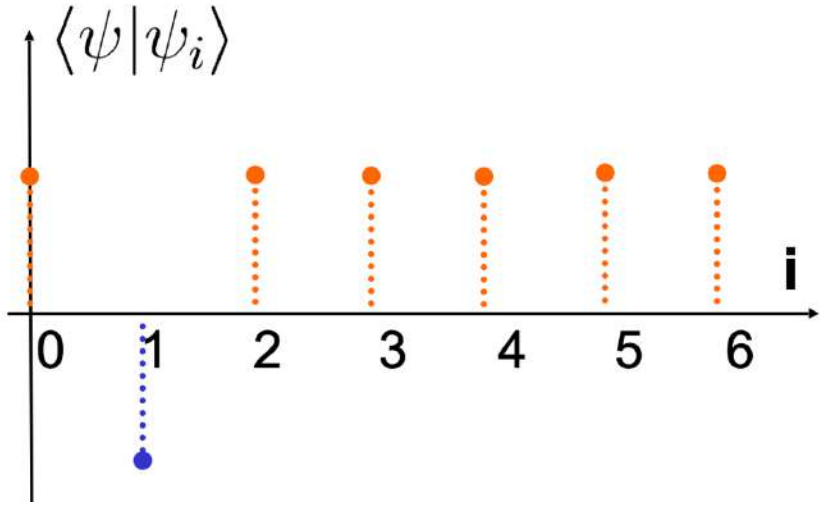
Grover's Search Algorithm

(Unstructured database)

Phase rotation operator

$$R = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$



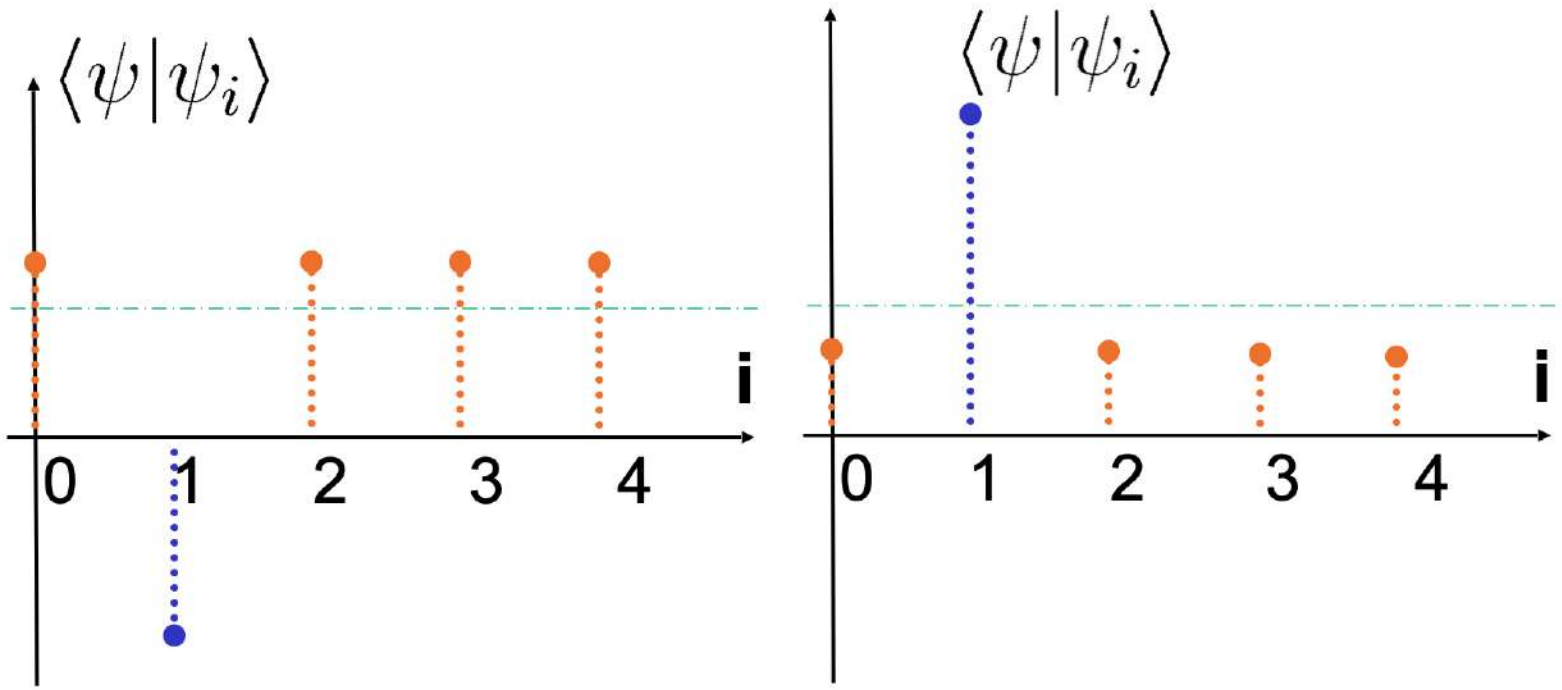


Grover's Search Algorithm

(Unstructured database)

Diffusion operator

$$D = \begin{bmatrix} -1+\frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & -1+\frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & -1+\frac{2}{N} \end{bmatrix}$$



Grover's Search Algorithm (Unstructured database)

Problem : Find i such that $x_i = 1$

Queries : ask i, get x_i

.....	0	0	1	0	0	0	0	.....

Classically : $N - 1$ queries required (worst case) [N elements in search space]

Quantum : $O(\sqrt{N})$ queries [grover, 1996]

Steps Grover's algorithm

1. Begin with the computer in state $|0\rangle^{\otimes n}$. Use Hadamard transformation to put the computer in equal superposition state,

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

2. Repeat $O(\sqrt{N})$ times the following two steps (Grover iteration)
   - Apply the Oracle O $|x\rangle \longrightarrow (-1)^{f(x)}|x\rangle$
   - Apply the operator $U_s = 2|S\rangle\langle S| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$
3. Measure the resulting state

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{for } x = \omega, \text{ that is, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{for } x \neq \omega, \text{ that is, } f(x) = 0. \end{cases}$$

Grover's Search Algorithm (Circuit from book Nelsen and Chuang)

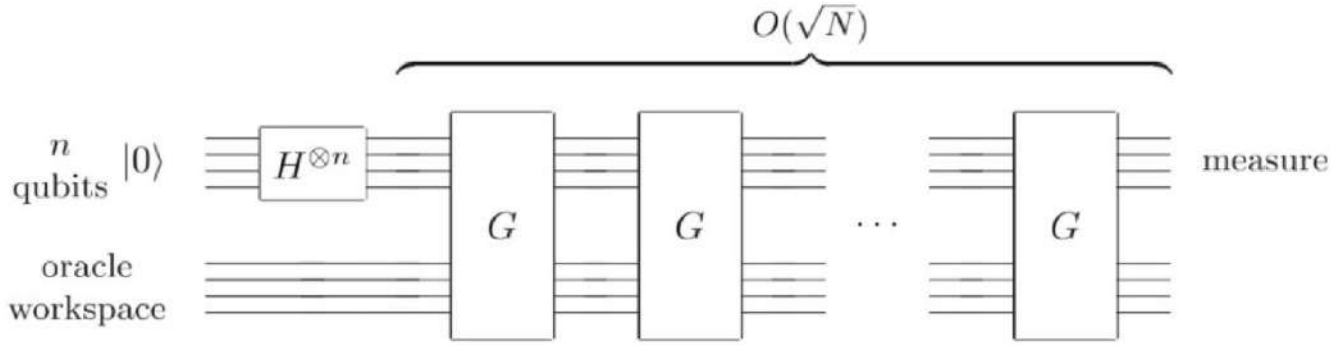


Figure 6.1. Schematic circuit for the quantum search algorithm. The oracle may employ work qubits for its implementation, but the analysis of the quantum search algorithm involves only the n qubit register.

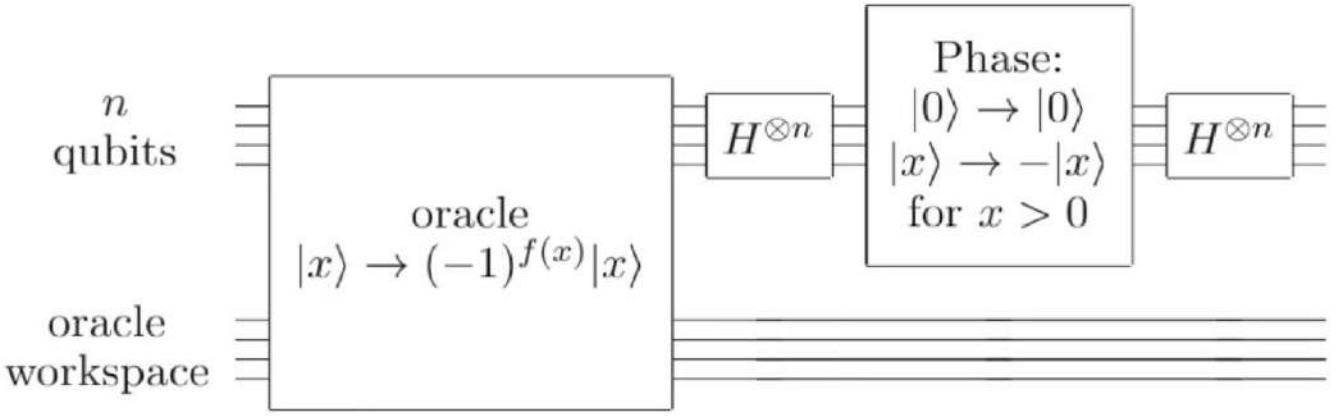
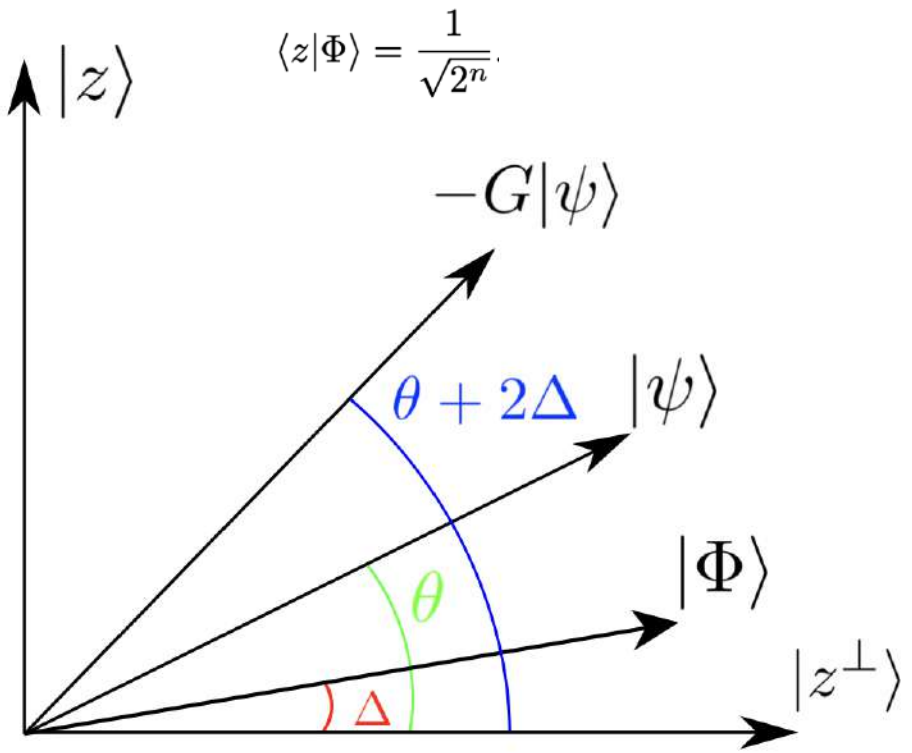


Figure 6.2. Circuit for the Grover iteration, G.

Grover's Search Algorithm (Geometrical picture)

$$|\Phi\rangle = \frac{1}{\sqrt{2^n}}\left[|\text{wrong}\rangle + |\text{wrong}\rangle + \cdots + |\text{wrong}\rangle + |z\rangle + |\text{wrong}\rangle + \cdots + |\text{wrong}\rangle\right]$$



1. Reflect about the correct solution $|z\rangle$.
2. Reflect about the equal superposition state (initial guess) $|\Phi\rangle$.

The first reflection can be written

$$R_z := 2|z\rangle\langle z| - I$$

and the second reflection can be written

$$R_\Phi := 2|\Phi\rangle\langle\Phi| - I$$

where I is the identity operator.

these two reflections rotate any state vector $|\psi\rangle$ closer to the correct state $|z\rangle$.

Grover iteration $G := R_\Phi R_z$ on the initial state $|\Phi\rangle$

$$R_z|\Phi\rangle = \frac{2}{\sqrt{2^n}}|z\rangle - |\Phi\rangle$$

$$R_\Phi R_z|\Phi\rangle = R_\Phi\left(\frac{2}{\sqrt{2^n}}|z\rangle - |\Phi\rangle\right) = \left(\frac{4}{2^n} - 1\right)|\Phi\rangle - \frac{2}{\sqrt{2^n}}|z\rangle.$$

The amplitude of z is increased

Quantum Simulation Algorithm

Simulation of Hamiltonian

- We want to simulate the evolution

$$|\psi_t\rangle = e^{-iHt}|\psi_0\rangle$$

- The Hamiltonian is a sum of terms:

$$H = \sum_{\ell=1}^{M} H_\ell$$

  - We can perform

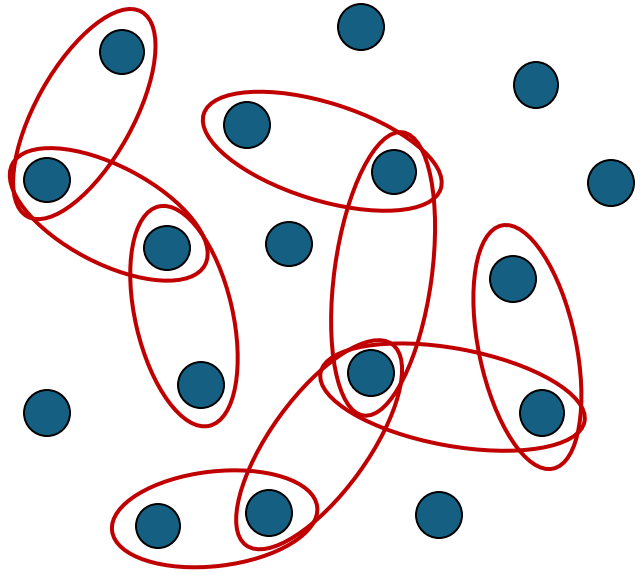
$$e^{-iH_\ell t}$$

  - For short times we can use

$$e^{-iH_1\delta t}e^{-iH_2\delta t}\ldots e^{-iH_{M-1}\delta t}e^{-iH_M\delta t} \approx e^{-iH\delta t}$$

  - For long times

$$\left[e^{-iH_1 t/r}e^{-iH_2 t/r}\ldots e^{-iH_M t/r}\right]^r \approx e^{-iHt}$$



Simulation of Hamiltonian

- For short times we can use

$$e^{-iH_1\delta t}e^{-iH_2\delta t}\ldots e^{-iH_{M-1}\delta t}e^{-iH_M\delta t}\approx e^{-iH\delta t}$$

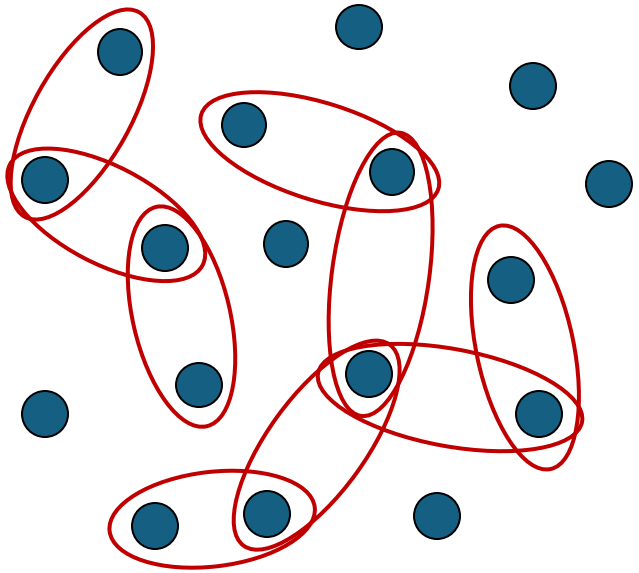
- This approximation is because

$$\begin{aligned}
&e^{-iH_1\delta t}e^{-iH_2\delta t}\ldots e^{-iH_{M-1}\delta t}e^{-iH_M\delta t}\\
&=\left(\mathbb{I}-iH_1\delta t+O(\delta t^2)\right)\left(\mathbb{I}-iH_2\delta t+O(\delta t^2)\right)\ldots\\
&\qquad\ldots\left(\mathbb{I}-iH_M\delta t+O(\delta t^2)\right)\\
&=\mathbb{I}-iH_1\delta t-iH_2\delta t\ldots-iH_M\delta t+O(\delta t^2)\\
&=\mathbb{I}-iH\delta t+O(\delta t^2)\\
&=e^{-iH\delta t}+O(\delta t^2)
\end{aligned}$$

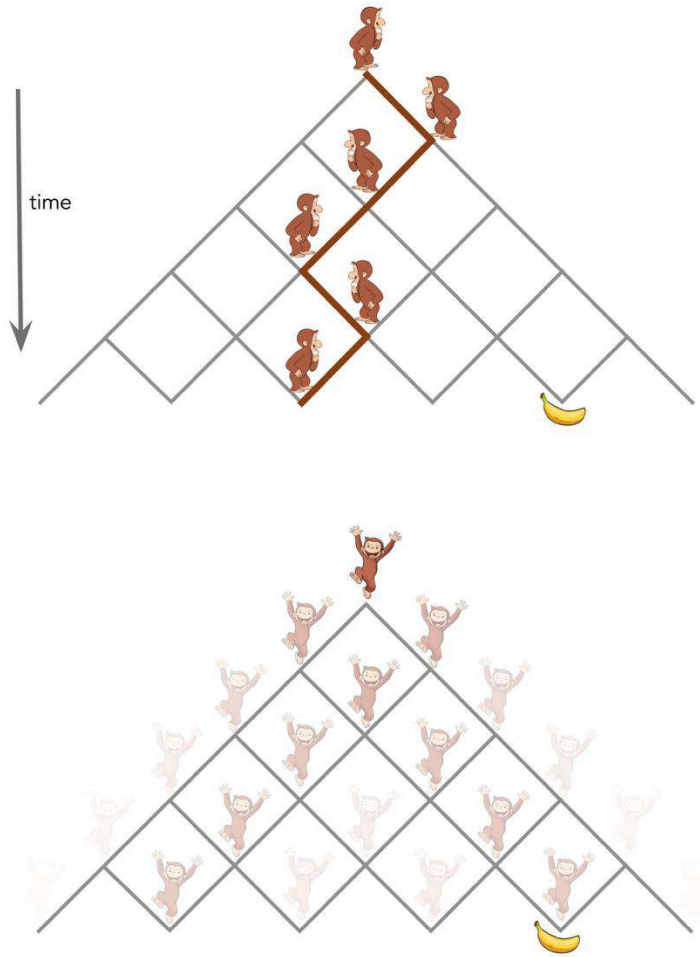
- If we divide long time t into r intervals, then

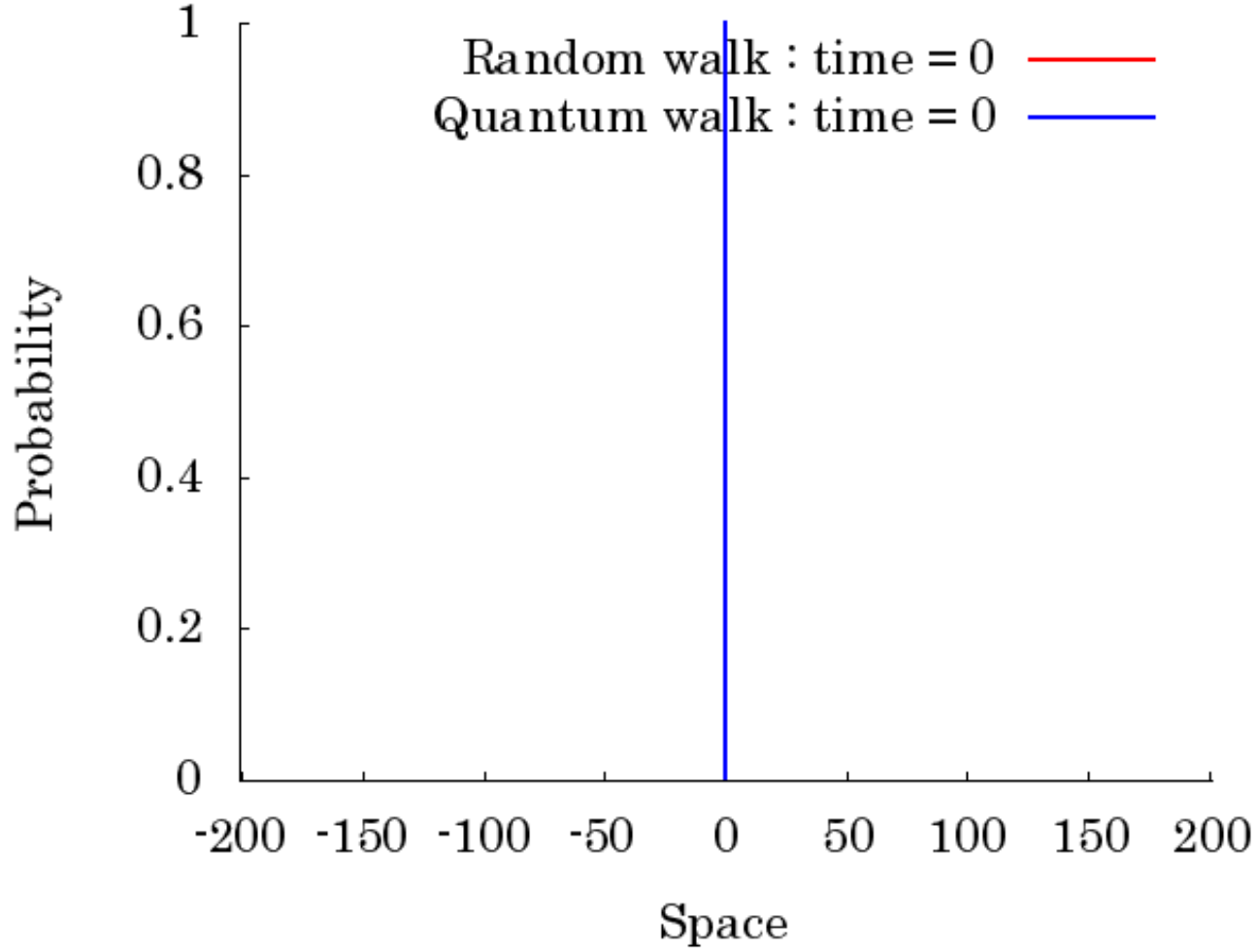
$$\begin{aligned}
e^{-iHt}=\left(e^{-iHt/r}\right)^r&=\left[e^{-iH_1t/r}e^{-iH_2t/r}\ldots e^{-iH_Mt/r}+O\left((t/r)^2\right)\right]^r\\
&=\left[e^{-iH_1t/r}e^{-iH_2t/r}\ldots e^{-iH_Mt/r}\right]^r+O(t^2/r)
\end{aligned}$$

- Typically, we want to simulate a system with some maximum allowable error ε.
- Then we need $r\propto t^2/\varepsilon$.

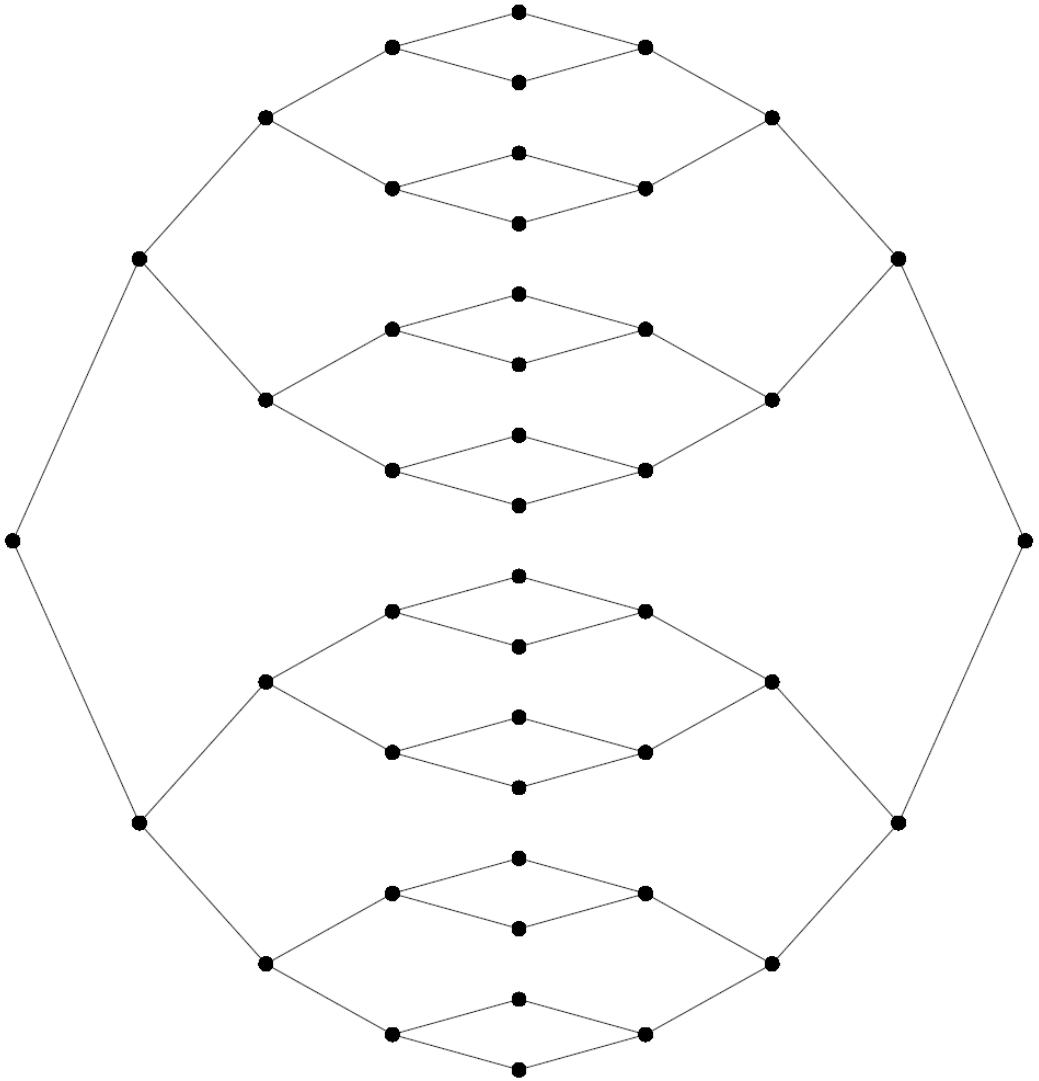


Quantum Simulation Algorithm
Quantum walk





Continuous walk on a graph (Classical)



The walk position is any node on the graph.

Describe the generator matrix K by

$$K_{aa'} = \begin{cases} \gamma, & a \neq a', aa' \in G \\ 0, & a \neq a', aa' \notin G \\ -d(a)\gamma, & a = a' \end{cases}$$

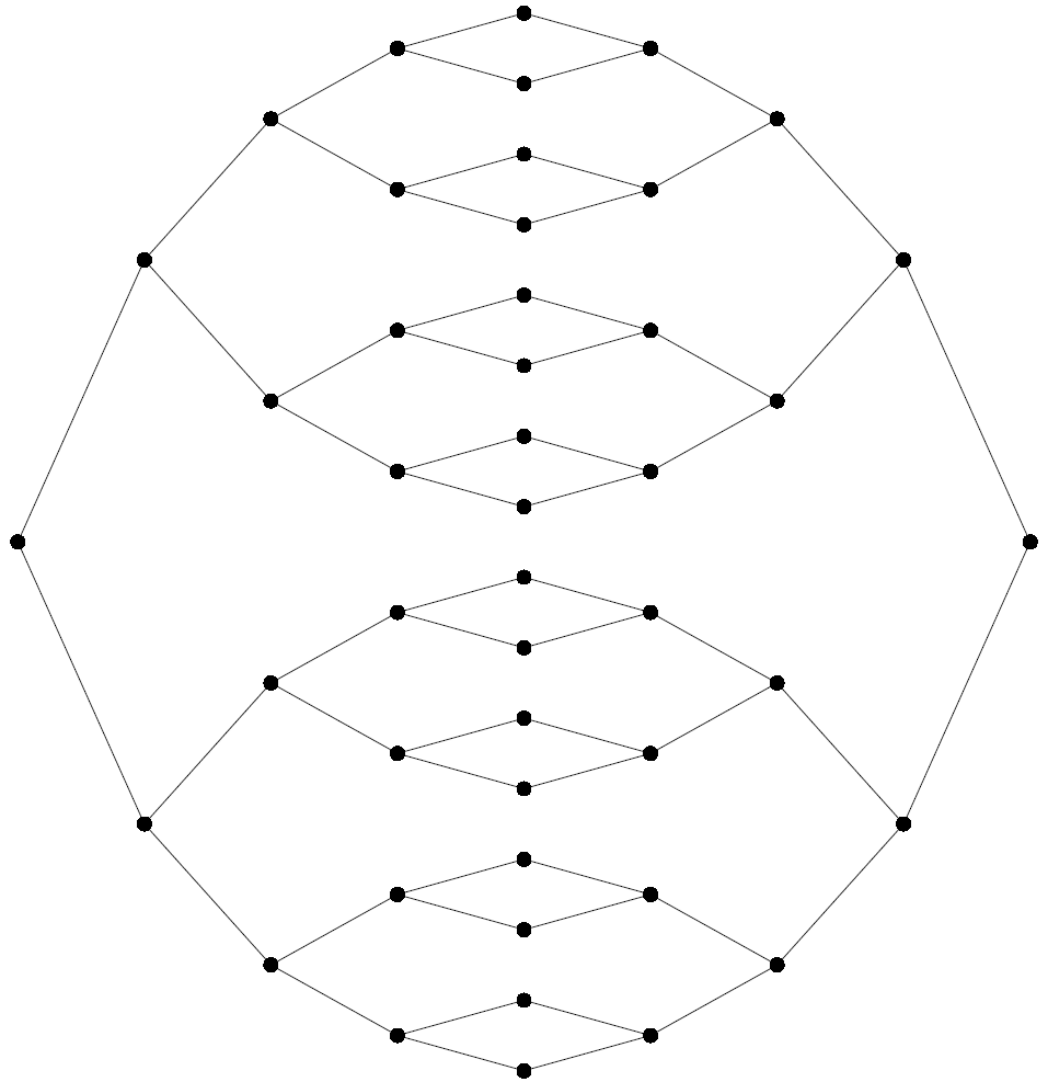
The quantity $d(a)$ is the number of edges incident on vertex a.

An edge between a and a' is denoted aa'.

The probability distribution for a continuous walk has the differential equation

$$\frac{dp_a(t)}{dt} = \sum_{a'} K_{aa'} p_{a'}(t)$$

Quantum walk on a graph



$$\frac{dp_a(t)}{dt} = \sum_{a'} K_{aa'} p_{a'}(t)$$

- Quantum mechanically we have

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

$$i\frac{d}{dt}\langle a|\psi(t)\rangle = \sum_{a'}\langle a|H|a'\rangle\langle a'|\psi(t)\rangle$$

- The natural quantum analogue is

$$\langle a|H|a'\rangle = K_{aa'}$$

- We take

$$\langle a|H|a'\rangle = \begin{cases}\gamma, & a \neq a', aa' \in G \\ 0, & \text{otherwise.}\end{cases}$$

- Probability is conserved because H is Hermitian.

Quantum walk on a graph

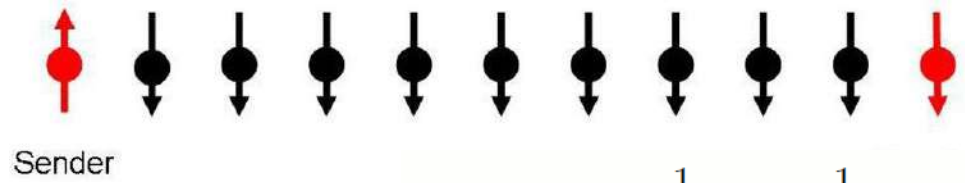
- The goal is to traverse the graph from entrance to exit.
- Classically the random walk will take exponential time.
- For the quantum walk, define a superposition state

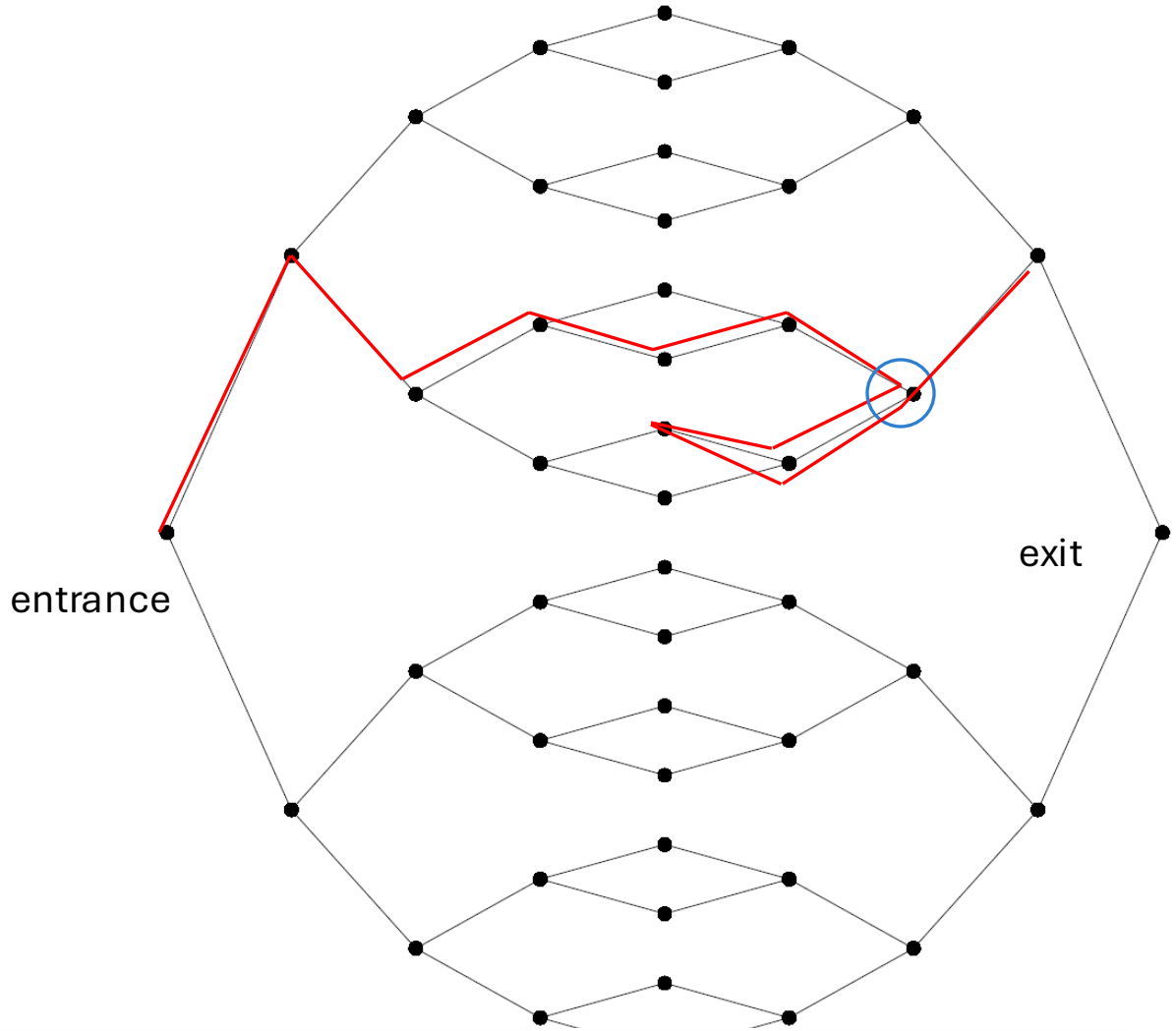
$$|\text{col } j\rangle = \frac{1}{\sqrt{N_j}} \sum_{a \in \text{column } j} |a\rangle$$

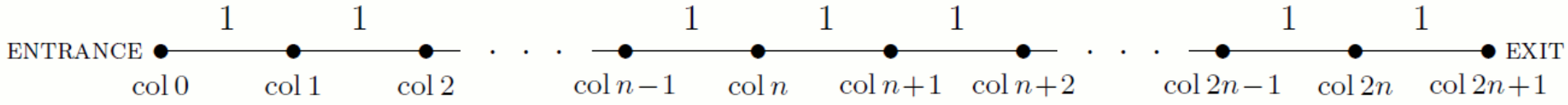
$$N_j = \begin{cases} 2^j & 0 \le j \le n \\ 2^{2n+1-j} & n+1 \le j \le 2n+1 \end{cases}$$

- On these states the matrix elements of the Hamiltonian are

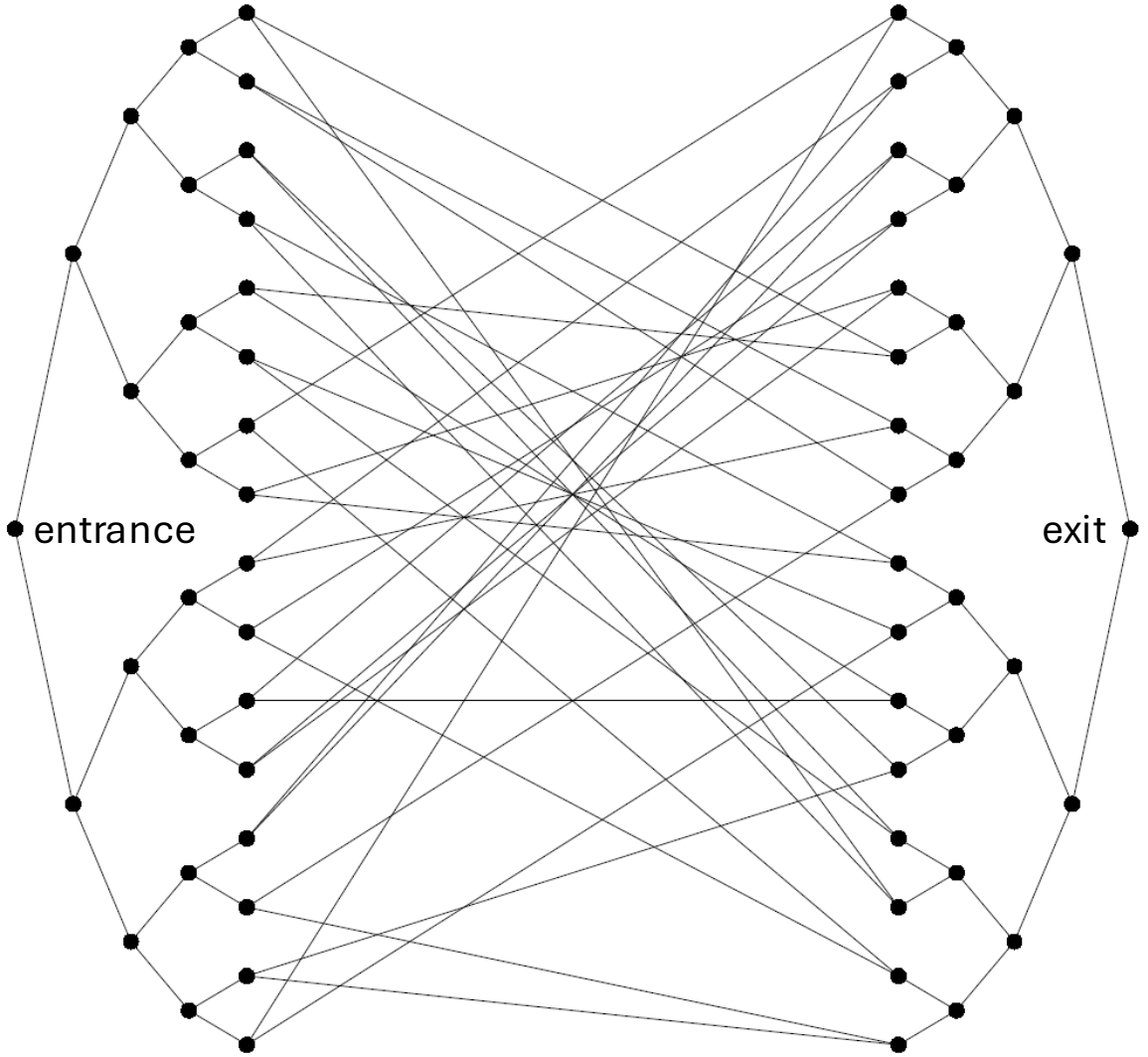
- $\langle \text{col } j | H | \text{col } (j \pm 1) \rangle = \sqrt{2}\gamma$







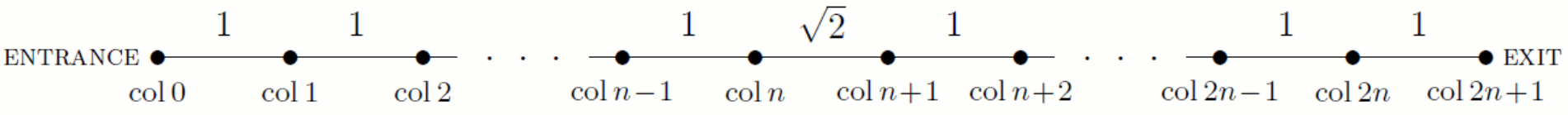
Quantum walk on a graph



- Add random connections between the two trees.
- All vertices (except entrance and exit) have degree 3.
- Again using column states, the matrix elements of the Hamiltonian are

$$\langle \text{col } j|H|\text{col } (j \pm 1)\rangle = \begin{cases} \sqrt{2}\gamma & j \neq n \\ 2\gamma & j = n \end{cases}$$

- This is a line with a defect.
- There are reflections off the defect, but the quantum walk still reaches the exit efficiently.



Continuous-time Quantum walk on a graph

- CTQW has its position space defined by a graph $\Gamma(V, E)$
- Adjacency matrix A_{ij} is defined on Γ :

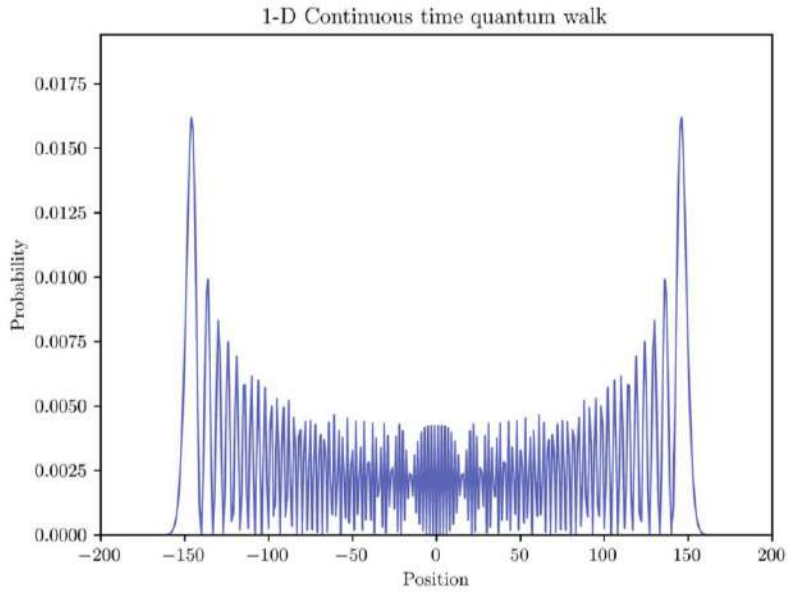
$$A_{ij} := \begin{cases} 1 & \text{edge } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

The vertices are labeled by the computational basis states $\{|1\rangle, |2\rangle, ..., |N\rangle\}$

- Hamiltonian H_Γ :

$$H_\Gamma = \gamma L = \gamma(D - A),$$

$$\implies H_{\Gamma_{ij}} = \begin{cases} -\gamma & i \neq j, \ (i,j) \in E \\ 0 & i \neq j, \ (i,j) \notin E \\ d_{ii}\gamma & i = j, \end{cases}$$



CTQW will simulate the Schrodinger equation (Hamiltonian of that form)

Quantum walks

- Quantum analog of classical random walks

Quantum walks

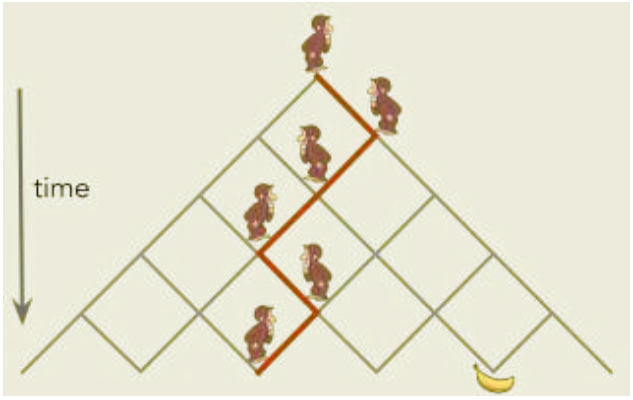
- Quantum analog of classical random walks
- Controllable quantum evolution in discrete space

Quantum walks

- Quantum analog of classical random walks
- Controllable quantum evolution in discrete space
- Operational (algorithmic) approach to control quantum dynamics
  - a tool for quantum algorithms and quantum simulations

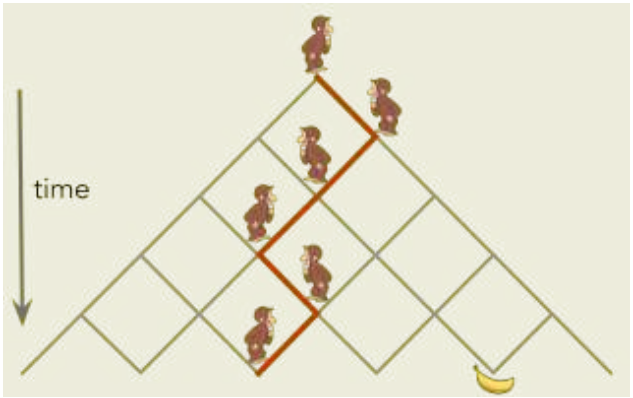
Classical random walk and stochastic problems

Classical random walk and stochastic problems



Classical random walk

Classical random walk and stochastic problems



Classical random walk

REVIEWS OF
MODERN PHYSICS

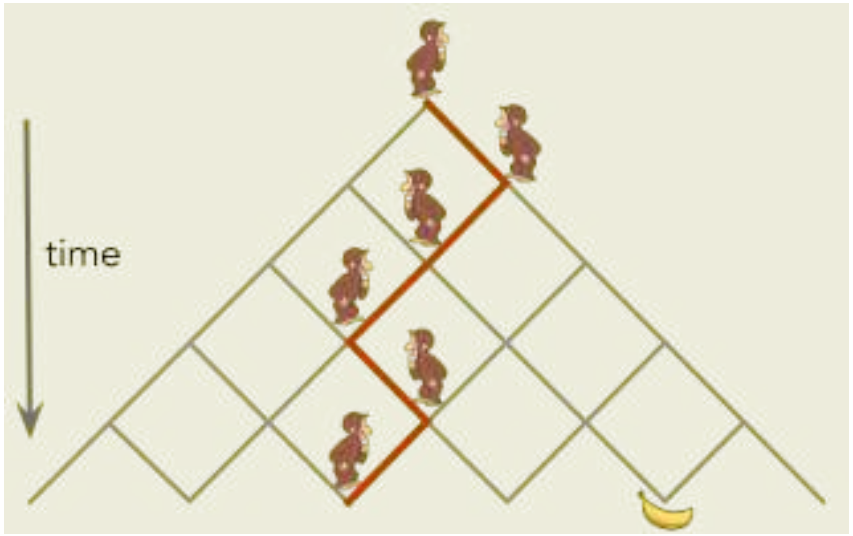
VOLUME 15, NUMBER 1 JANUARY, 1943

Stochastic Problems in Physics and Astronomy

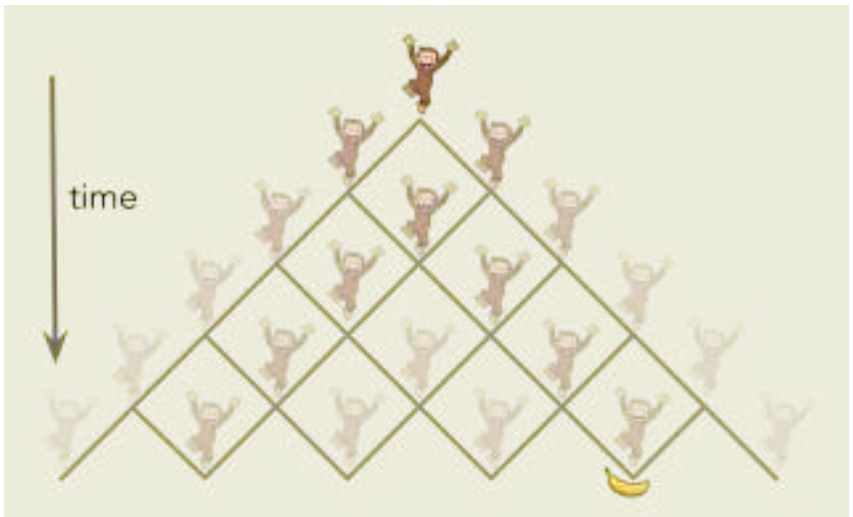
S. CHANDRASEKHAR
Yerkes Observatory, The University of Chicago, Williams Bay, Wisconsin

CONTENTS

Quantum walk



Classical random walk



Quantum walk

Continuous-time quantum walk

Continuous-time quantum walk

- CTQW has its position space defined by a graph $\Gamma(V, E)$
- Adjacency matrix A_{ij} is defined on Γ :

$$A_{ij} := \begin{cases} 1 & \text{edge } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

The vertices are labeled by the computational basis states $\{|1\rangle, |2\rangle, ..., |N\rangle\}$

- Hamiltonian H_Γ :

$$H_\Gamma = \gamma L = \gamma(D - A),$$

$$\implies H_{\Gamma_{ij}} = \begin{cases} -\gamma & i \neq j, \ \ (i,j) \in E \\ 0 & i \neq j, \ \ (i,j) \notin E \\ d_{ii}\gamma & i = j, \end{cases}$$

Continuous-time quantum walk

- CTQW has its position space defined by a graph $\Gamma(V, E)$
- Adjacency matrix A_{ij} is defined on Γ :

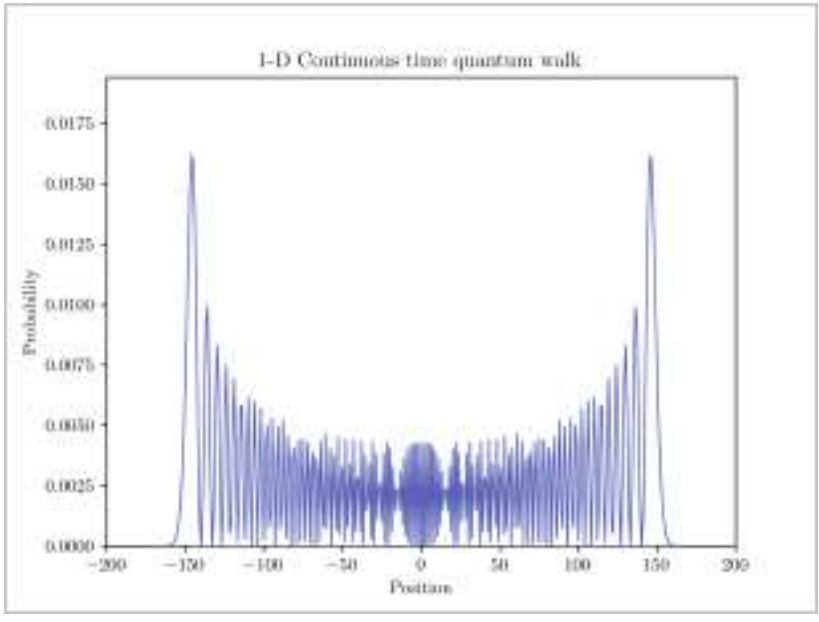
$$A_{ij} := \begin{cases} 1 & \text{edge } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

The vertices are labeled by the computational basis states $\{|1\rangle, |2\rangle, ..., |N\rangle\}$

- Hamiltonian H_Γ :

$$H_\Gamma = \gamma L = \gamma(D - A),$$

$$\implies H_{\Gamma_{ij}} = \begin{cases} -\gamma & i \neq j, \ (i,j) \in E \\ 0 & i \neq j, \ (i,j) \notin E \\ d_{ii}\gamma & i = j, \end{cases}$$



Continuous-time quantum walk

for every pair $j,k \in V$. The other important matrix associated with the graph G is the generator matrix $\mathbf{H}$ given by

$$\mathbf{H}_{j,k} = \begin{cases} d_j\gamma & j = k, \\ -\gamma & (j,k) \in E, \\ 0 & \text{otherwise}, \end{cases} \tag{2}$$

where d_j is the degree of the vertex j and γ is the probability of transition between neighboring nodes per unit time.

If $p_j(t)$ denotes the probability of being at vertex j at time t, then the transition on graph G is defined as the solution of the differential equation

$$\frac{d}{dt}p_j(t) = -\sum_{k\in V}\mathbf{H}_{j,k}p_k(t). \tag{3}$$

The solution of the differential equation is given by

$$p(t) = e^{-\mathbf{H}t}p(0). \tag{4}$$

By replacing the probabilities p_j by quantum amplitudes $a_j(t) = \langle j|\psi(t)\rangle$, where $|j\rangle$ is spanned by the orthogonal basis of the position Hilbert space $\mathcal{H}_p$, and introducing a factor of i, we obtain

$$i\frac{d}{dt}a_j(t) = \sum_{k\in V}\mathbf{H}_{j,k}a_k(t). \tag{5}$$

We can see that Eq. (5) is the Schrödinger equation

$$i\frac{d}{dt}|\psi\rangle = \mathbf{H}|\psi\rangle. \tag{6}$$

Since the generator matrix is an Hermitian operator, the normalization is preserved during the dynamics. The solution of the differential equation can be written in the form

$$|\psi(t)\rangle = e^{-i\mathbf{H}t}|\psi(0)\rangle. \tag{7}$$

Therefore the continuous-time quantum walk is of the form of the Schrödinger equation, a nonrelativistic quantum evolution.

Discrete-time quantum walk

- Walk is defined on the Hilbert space $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$

  $\mathcal{H}_c$ (particle) is spanned by $|\uparrow\rangle$ and $|\downarrow\rangle$
  $\mathcal{H}_p$ (position) is spanned by $|j\rangle, j \in \mathbb{Z}$

Discrete-time quantum walk

- Walk is defined on the Hilbert space $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$

  $\mathcal{H}_c$ (particle) is spanned by $|\uparrow\rangle$ and $|\downarrow\rangle$
  $\mathcal{H}_p$ (position) is spanned by $|j\rangle, j \in \mathbb{Z}$

- Initial state : $|\Psi_{in}\rangle = [\cos(\delta)|\uparrow\rangle + e^{i\eta}\sin(\delta)|\downarrow\rangle] \otimes |j = 0\rangle$

Discrete-time quantum walk

- Walk is defined on the Hilbert space $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$

  $\mathcal{H}_c$ (particle) is spanned by $|\uparrow\rangle$ and $|\downarrow\rangle$
  $\mathcal{H}_p$ (position) is spanned by $|j\rangle, j \in \mathbb{Z}$

- Initial state : $|\Psi_{in}\rangle = [\cos(\delta)|\uparrow\rangle + e^{i\eta}\sin(\delta)|\downarrow\rangle] \otimes |j = 0\rangle$
- Evolution :
  - Coin operation : $C(\theta) = \begin{bmatrix} \cos(\theta) & -i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{bmatrix}$

Discrete-time quantum walk

- Walk is defined on the Hilbert space $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$

  $\mathcal{H}_c$ (particle) is spanned by $|\uparrow\rangle$ and $|\downarrow\rangle$
  $\mathcal{H}_p$ (position) is spanned by $|j\rangle, j \in \mathbb{Z}$

- Initial state : $|\Psi_{in}\rangle = [\cos(\delta)|\uparrow\rangle + e^{i\eta}\sin(\delta)|\downarrow\rangle] \otimes |j = 0\rangle$

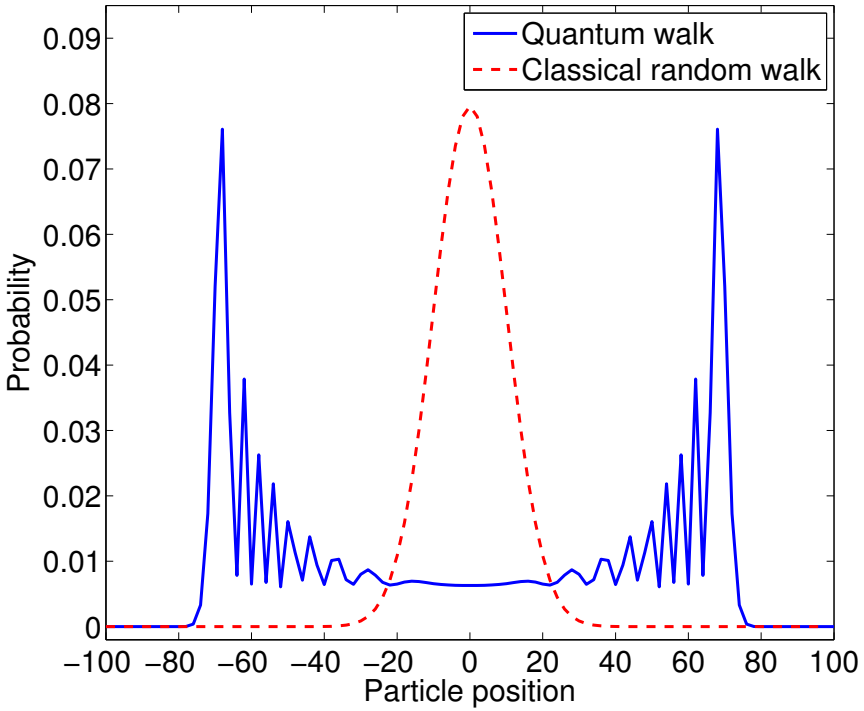
- Evolution :
  - Coin operation : $C(\theta) = \begin{bmatrix} \cos(\theta) & -i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{bmatrix}$
  - Conditional unitary shift operation S:

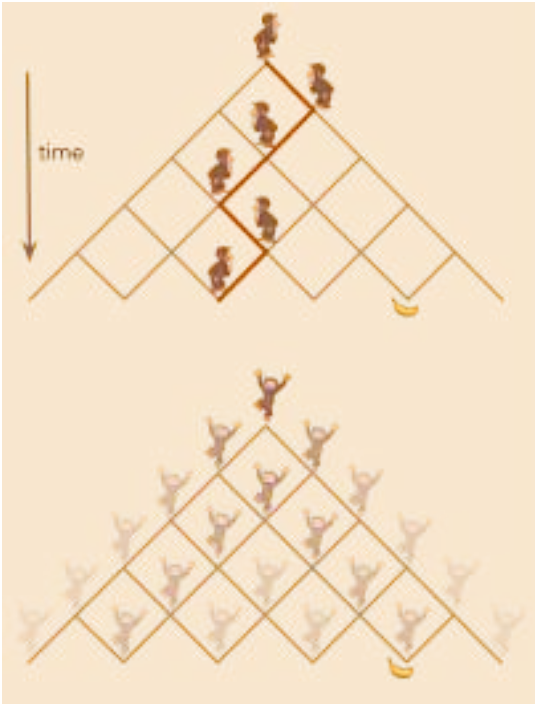
$$S = \sum_{j\in\mathbb{Z}} \Big[|\uparrow\rangle\langle\uparrow| \otimes |j-1\rangle\langle j| + |\downarrow\rangle\langle\downarrow| \otimes |j+1\rangle\langle j| \Big]$$

state $|\uparrow\rangle$ moves to the left and state $|\downarrow\rangle$ moves to the right

Quantum walk

- Each step of QW : $W = S(C(\theta) \otimes \mathbb{1})$





100 step of CRW and QW $[S(C(\pi/4) \otimes \mathbb{1})]^{100}$on a particle with initial state $\frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\downarrow\rangle)$

- G. V. Riazanov (1958), R. Feynman (1986)
- K.R. Parthasarathy, Journal of applied probability 25, 151-166 (1988)
- Y. Aharonov, L. Davidovich and N. Zugury, Phys. Rev. A, 48, 1687 (1993)

From discrete-time quantum walk to relativistic equations :Klein-Gordon, Dirac

(free quantum field dynamics)

Symmetric evolution of DQW and hyperbolic PDE

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\Big[|\uparrow\rangle \pm i|\downarrow\rangle\Big] \otimes |x = 0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

Symmetric evolution of DQW and hyperbolic PDE

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\Big[|\uparrow\rangle \pm i|\downarrow\rangle\Big] \otimes |x=0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\Big[|\uparrow\rangle \pm |\downarrow\rangle\Big] \otimes |x=0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & -i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{bmatrix}$$

Symmetric evolution of DQW and hyperbolic PDE

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\Big[|\uparrow\rangle \pm i|\downarrow\rangle\Big] \otimes |x=0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\Big[|\uparrow\rangle \pm |\downarrow\rangle\Big] \otimes |x=0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & -i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{bmatrix}$$

In the form of left moving and right moving component

$$\psi^0_{x,t+1} = \cos(\theta)\psi^0_{x+1,t} - i\sin(\theta)\psi^1_{x-1,t}$$
$$\psi^1_{x,t+1} = \cos(\theta)\psi^1_{x-1,t} - i\sin(\theta)\psi^0_{x+1,t}$$

Symmetric evolution of DQW and hyperbolic PDE

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\left[|\uparrow\rangle \pm i|\downarrow\rangle\right] \otimes |x=0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\left[|\uparrow\rangle \pm |\downarrow\rangle\right] \otimes |x=0\rangle \qquad B(\theta) = \begin{bmatrix} \cos(\theta) & -i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{bmatrix}$$

In the form of left moving and right moving component

$$\psi^0_{x,t+1} = \cos(\theta)\psi^0_{x+1,t} - i\sin(\theta)\psi^1_{x-1,t}$$
$$\psi^1_{x,t+1} = \cos(\theta)\psi^1_{x-1,t} - i\sin(\theta)\psi^0_{x+1,t}$$

Differential equation form in continuum limit :Klein-Gordon equation

$$\left[\frac{\partial^2}{\partial t^2} - \cos(\theta)\frac{\partial^2}{\partial x^2} + 2[1-\cos(\theta)]\right]\psi^{0(1)}_{x,t} = 0$$

CMC, SB and RS, PRA, **81** 062340 (2010)

Dirac equation from Discrete-time QW

Dirac equation

$$\left(i\hbar\frac{\partial}{\partial t} - \hat{\mathbf{H}}_{\mathbf{D}}\right)\Psi = \left(i\hbar\frac{\partial}{\partial t} + i\hbar c\hat{\alpha}\cdot\frac{\partial}{\partial x} - \hat{\beta}mc^2\right)\Psi = 0$$

From DTQW when $\theta = 0$, the expression in continuum limit takes the form

$$\left[i\hbar\frac{\partial}{\partial t} - i\hbar\sigma_3\frac{\partial}{\partial x}\right]\Psi(x,t) = 0$$

David Mayer (1996) and Fredrick Strauch (2006)
For $\theta \neq 0$
Giuseppe Molfetta - Fabrice Debbasch (2013) and CMC (2013)

Dirac equation from Discrete-time QW

Dirac equation

$$\left(i\hbar\frac{\partial}{\partial t} - \hat{\mathbf{H}}_{\mathbf{D}}\right)\Psi = \left(i\hbar\frac{\partial}{\partial t} + i\hbar c\hat{\alpha}\cdot\frac{\partial}{\partial x} - \hat{\beta}mc^2\right)\Psi = 0$$

From DTQW when $\theta = 0$, the expression in continuum limit takes the form

$$\left[i\hbar\frac{\partial}{\partial t} - i\hbar\sigma_3\frac{\partial}{\partial x}\right]\Psi(x,t) = 0$$

David Mayer (1996) and Fredrick Strauch (2006)
For $\theta \neq 0$
Giuseppe Molfetta - Fabrice Debbasch (2013) and CMC (2013)

Quantum simulation of Dirac equation

- Dirac equation

$$\left(i\hbar\frac{\partial}{\partial t} - \hat{\mathsf{H}}_{\mathsf{D}}\right)\Psi = \left(i\hbar\frac{\partial}{\partial t} + i\hbar c\hat{\alpha}\cdot\frac{\partial}{\partial x} - \hat{\beta}mc^2\right)\Psi = 0$$

Quantum simulation of Dirac equation

- Dirac equation

$$\left(i\hbar\frac{\partial}{\partial t} - \hat{\mathrm{H}}_{\mathrm{D}}\right)\Psi = \left(i\hbar\frac{\partial}{\partial t} + i\hbar c\hat{\alpha}\cdot\frac{\partial}{\partial x} - \hat{\beta}mc^2\right)\Psi = 0$$

- Dirac cellular automaton (DCA) from discretization of Dirac equation :

$$U_{DCA} = \begin{pmatrix} \alpha T_- & -i\beta \\ -i\beta & \alpha T_+ \end{pmatrix} = \alpha\{T_- \otimes |\uparrow\rangle\langle\uparrow| + T_+ \otimes |\downarrow\rangle\langle\downarrow|\} - i\beta(I \otimes \sigma_x)$$

α corresponds to the hopping strength, β corresponds to the mass term.

$$T_- = |x-1\rangle\langle x| \;\; ; \;\; | \;\; T_+ = |x+1\rangle\langle x|$$

$$\Psi(x) \to \Psi(x-1) \;\; ; \;\; \Psi(x) \to \Psi(x+1)$$

Quantum simulation of Dirac equation

- Dirac equation

$$\left(i\hbar\frac{\partial}{\partial t} - \hat{\mathrm{H}}_{\mathrm{D}}\right)\Psi = \left(i\hbar\frac{\partial}{\partial t} + i\hbar c\hat{\alpha}\cdot\frac{\partial}{\partial x} - \hat{\beta}mc^2\right)\Psi = 0$$

- Dirac cellular automaton (DCA) from discretization of Dirac equation :

$$U_{DCA} = \begin{pmatrix} \alpha T_- & -i\beta \\ -i\beta & \alpha T_+ \end{pmatrix} = \alpha\{T_- \otimes |\uparrow\rangle\langle\uparrow| + T_+ \otimes |\downarrow\rangle\langle\downarrow|\} - i\beta(I \otimes \sigma_x)$$

α corresponds to the hopping strength, β corresponds to the mass term.

$$T_- = |x-1\rangle\langle x| \;\; ; \;\; | \;\; T_+ = |x+1\rangle\langle x|$$
$$\Psi(x) \to \Psi(x-1) \;\; ; \;\; \Psi(x) \to \Psi(x+1)$$

- Associated Hamiltonian in momentum basis, produces DH,

$$H(k) = \frac{a}{c\tau}\begin{pmatrix} -kc & mc^2 \\ mc^2 & kc \end{pmatrix}$$

with the identification $\beta = \frac{mac}{\hbar}$, k is a eigenvalue of momentum operator.

$DTQW$

The general form of the evolution operator

$$U_{QW} = \begin{pmatrix} \cos(\theta)\ T_- & -i\sin(\theta)\ T_- \\ -i\sin(\theta)\ T_+ & \cos(\theta)\ T_+ \end{pmatrix}$$

$$U_{QW} = \cos(\theta)\{\, T_- \otimes |\uparrow\rangle\langle\uparrow| + T_+ \otimes |\downarrow\rangle\langle\downarrow|\,\} + \sin(\theta)\{\, T_- \otimes |\uparrow\rangle\langle\downarrow|) + T_+ \otimes |\downarrow\rangle\langle\uparrow|\,\}$$

$DTQW$

The general form of the evolution operator

$$U_{QW} = \begin{pmatrix} \cos(\theta)\ T_- & -i\sin(\theta)\ T_- \\ -i\sin(\theta)\ T_+ & \cos(\theta)\ T_+ \end{pmatrix}$$

$$U_{QW} = \cos(\theta)\{\, T_- \otimes |\uparrow\rangle\langle\uparrow| + T_+ \otimes |\downarrow\rangle\langle\downarrow|\,\} + \sin(\theta)\{\, T_- \otimes |\uparrow\rangle\langle\downarrow|) + T_+ \otimes |\downarrow\rangle\langle\uparrow|\,\}$$

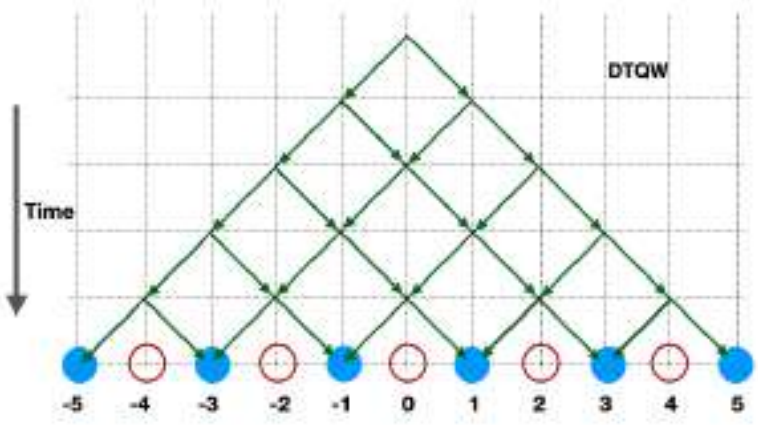
$$U_{DCA} = \begin{pmatrix} \alpha T_- & -i\beta \\ -i\beta & \alpha T_+ \end{pmatrix} = \alpha\{\, T_- \otimes |\uparrow\rangle\langle\uparrow| + T_+ \otimes |\downarrow\rangle\langle\downarrow|\} - i\beta(I \otimes \sigma_x)$$

By taking the value of $\theta \to 0$ the off-diagonal terms can be ignored and a massless DH can be recovered.

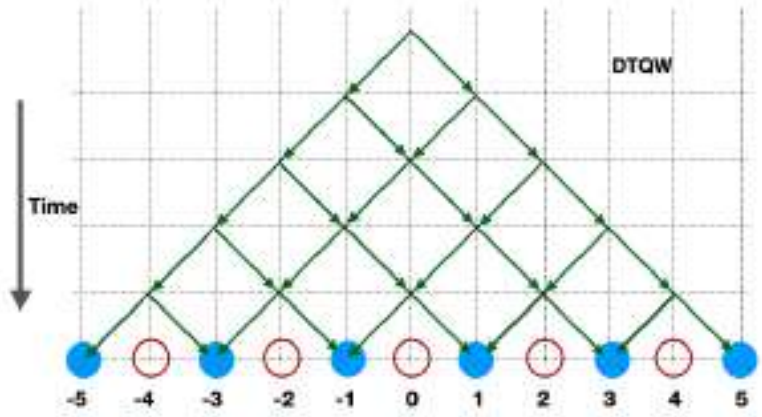
David Mayer (1996) ; Fredrick Strauch (2006) ; CSB (2010)

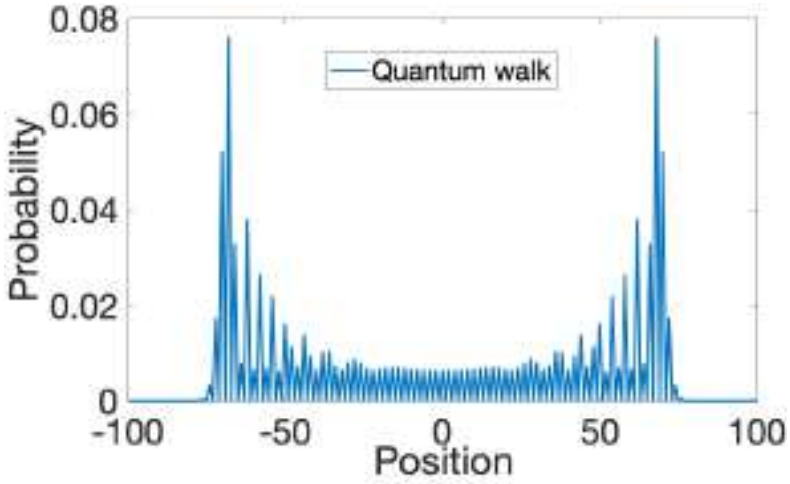
DTQW and DCA

DTQW and DCA

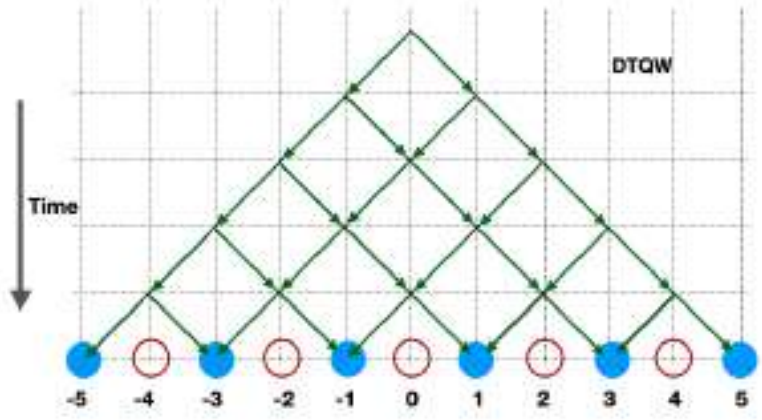


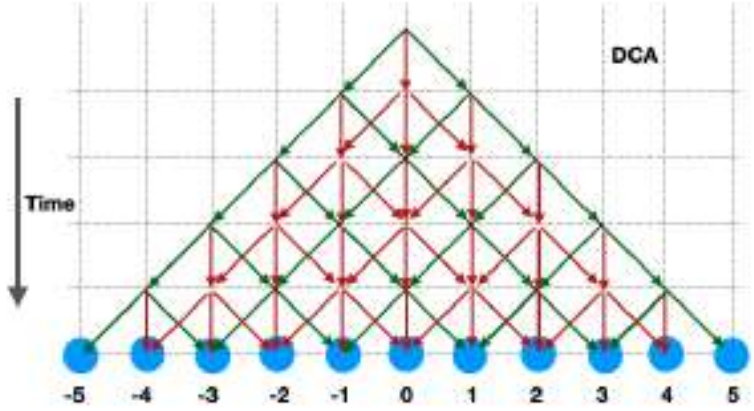
DTQW and DCA

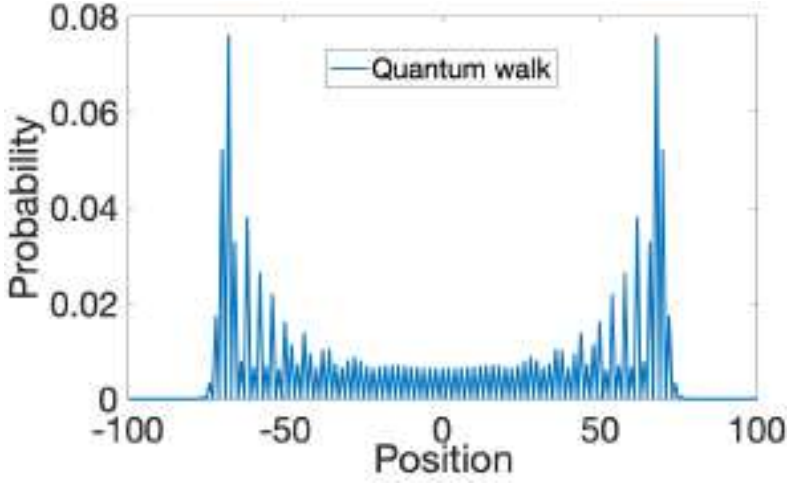

DTQW
Time
-5
-4
-3
-2
-1
0
1
2
3
4
5


Quantum walk
Probability
0.08
0.06
0.04
0.02
0
-100
-50
0
50
100
Position

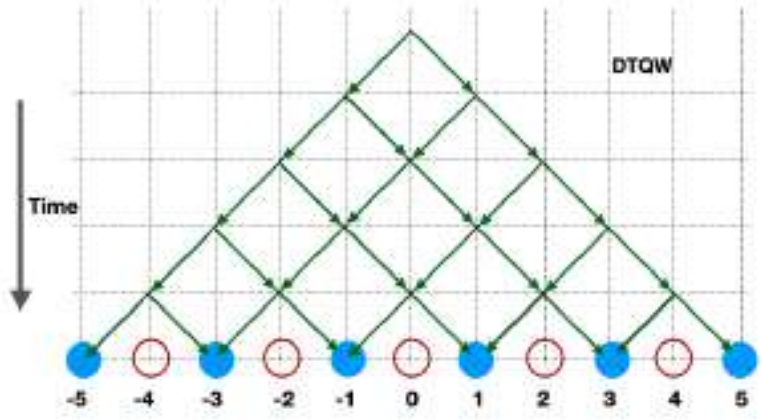
DTQW and DCA

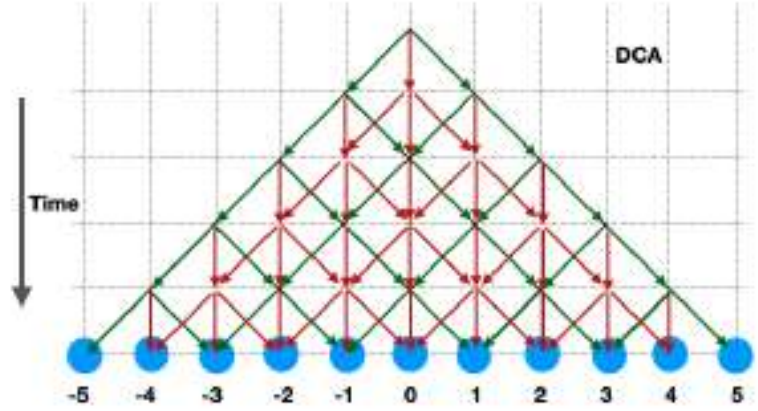

DTQW
Time
-5
-4
-3
-2
-1
0
1
2
3
4
5

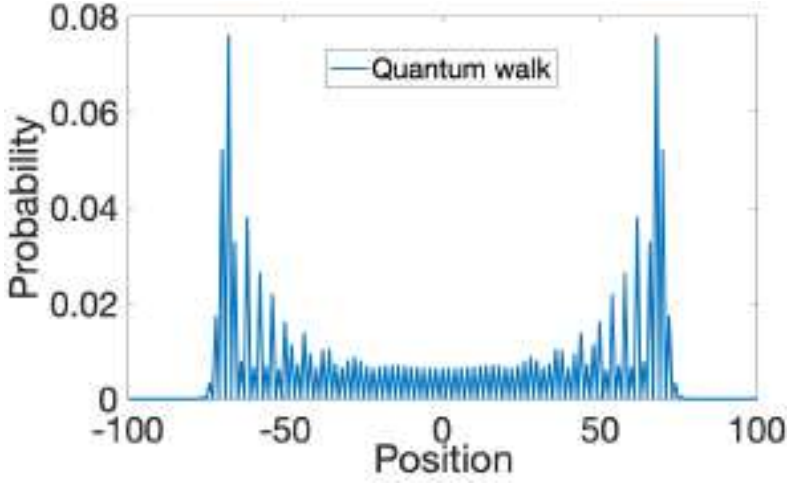

DCA
Time
-5
-4
-3
-2
-1
0
1
2
3
4
5

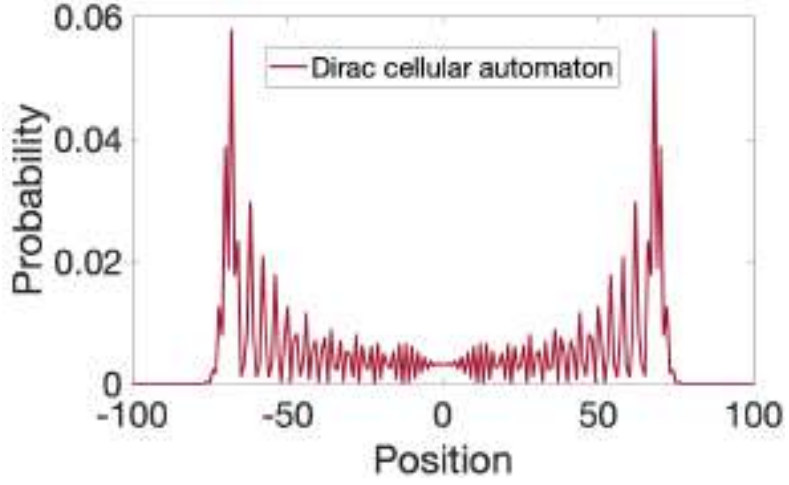

Quantum walk
Probability
0.08
0.06
0.04
0.02
0
-100
-50
0
50
100
Position

DTQW and DCA


DTQW
Time
-5
-4
-3
-2
-1
0
1
2
3
4
5

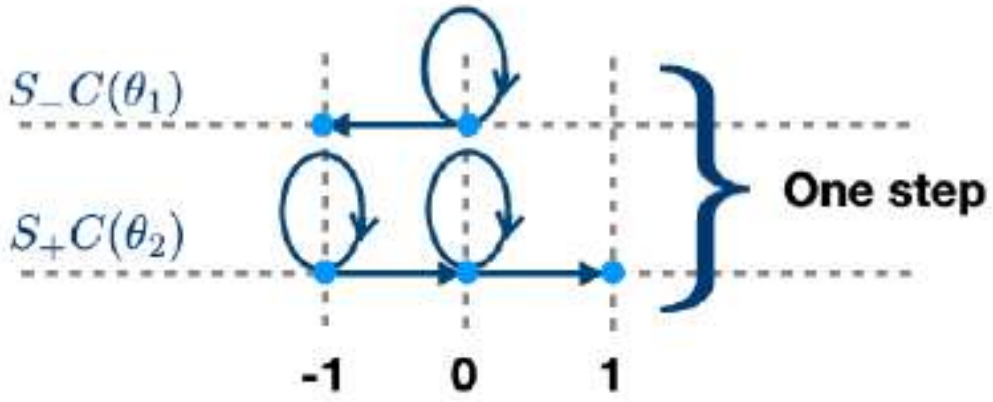

DCA
Time
-5
-4
-3
-2
-1
0
1
2
3
4
5


Quantum walk
Probability
0.08
0.06
0.04
0.02
0
-100
-50
0
50
100
Position

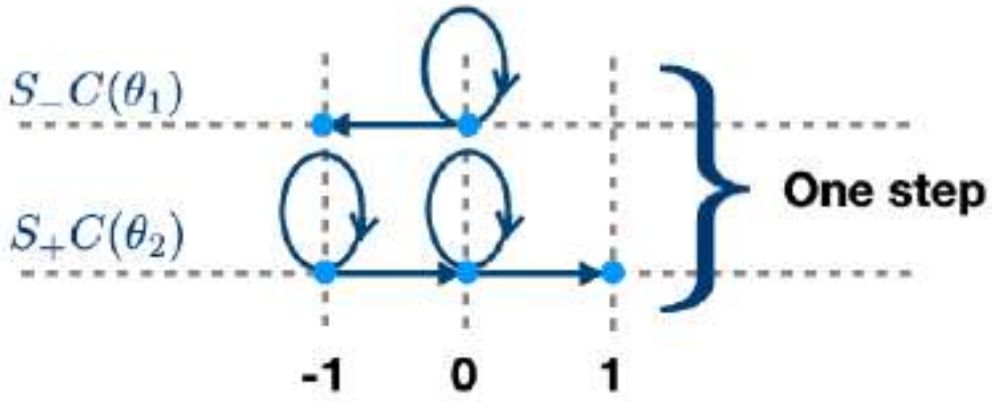

Dirac cellular automaton
Probability
0.06
0.04
0.02
0
-100
-50
0
50
100
Position

DE with mass term : Split-step

DE with mass term : Split-step



DE with mass term : Split-step



$$C(\theta_1) = \begin{pmatrix} \cos(\theta_1) & -i\sin(\theta_1) \\ -i\sin(\theta_1) & cos(\theta_1) \end{pmatrix} \quad ; \quad C(\theta_2) = \begin{pmatrix} \cos(\theta_2) & -i\sin(\theta_2) \\ -i\sin(\theta_2) & \cos(\theta_2) \end{pmatrix}$$

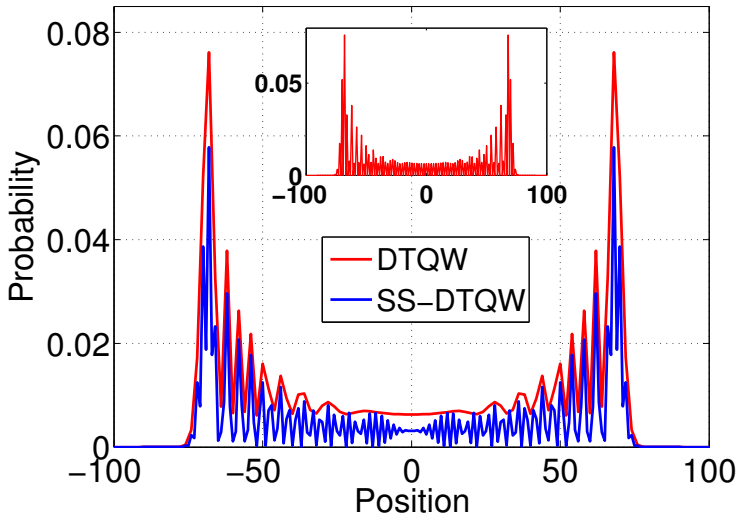
and a two half-shift operators,

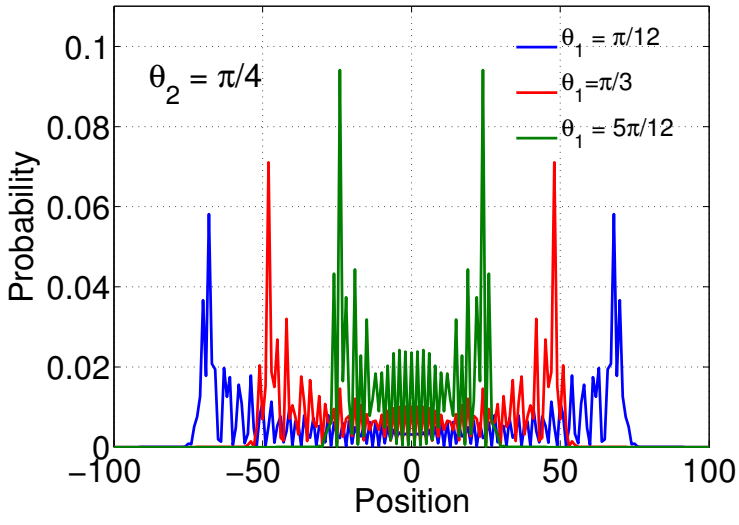
$$S_- = \begin{pmatrix} T_- & 0 \\ 0 & I \end{pmatrix}, \qquad S_+ = \begin{pmatrix} I & 0 \\ 0 & T_+ \end{pmatrix} \qquad S = \begin{pmatrix} T_- & 0 \\ 0 & T_+ \end{pmatrix}$$

$$T_- = |j-1\rangle\langle j| \quad ; \quad T_+ = |j+1\rangle\langle j|$$

$$U_{SQW} = S_+\Big(C(\theta_2)\otimes I\Big)S_-\Big(C(\theta_1)\otimes I\Big) \equiv S\Big(C(\theta_2)\otimes I\Big)S\Big(C(\theta_1)\otimes I\Big)$$

DCA and SS-QW





SSQW :

$S_+ C(\theta_2) S_- C(\theta_1)$ when $(\theta_1 = 0, \theta_2 = \pi/4) =$ DCA

$$U_{SSQW} = \begin{pmatrix} \cos(\theta_2)\, T_- & -i \sin(\theta_2) I \\ -i \sin(\theta_2) I & \cos(\theta_2)\, T_+ \end{pmatrix}$$

which is in the same form as U_{DCA} where $\beta = \sin(\theta_2) \equiv \frac{mca}{\hbar}$ and $\alpha = \cos(\theta_2)$.

CMC (2013) ; CMC & Mallick (2015) ; SS et. al. (2021)

DTQW/ DCA on circuit-based quantum processor

DTQW/ DCA on circuit-based quantum processor

Single and two qubit gates

Identity : $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Pauli x : $\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

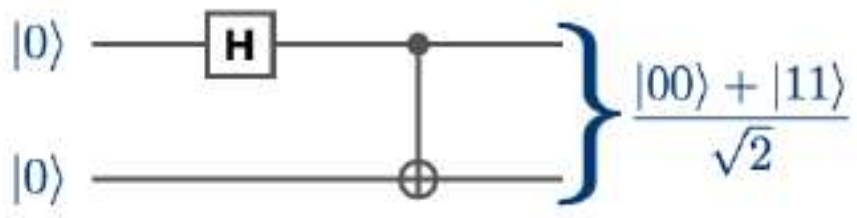
Pauli y : $\sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Pauli z : $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

$\pi/8$ Phase : $T_{\pi/8} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

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



DTQW/ DCA on circuit-based quantum processor

Single and two qubit gates

Identity : $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Pauli x : $\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

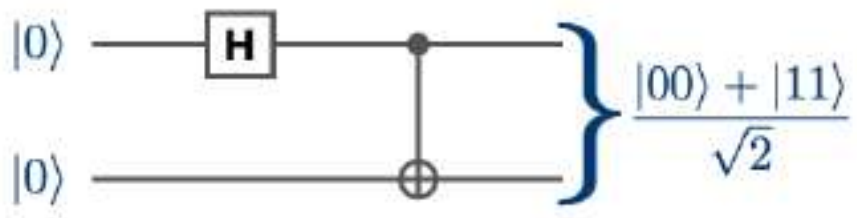
Pauli y : $\sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Pauli z : $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

$\pi/8$ Phase : $T_{\pi/8} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

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



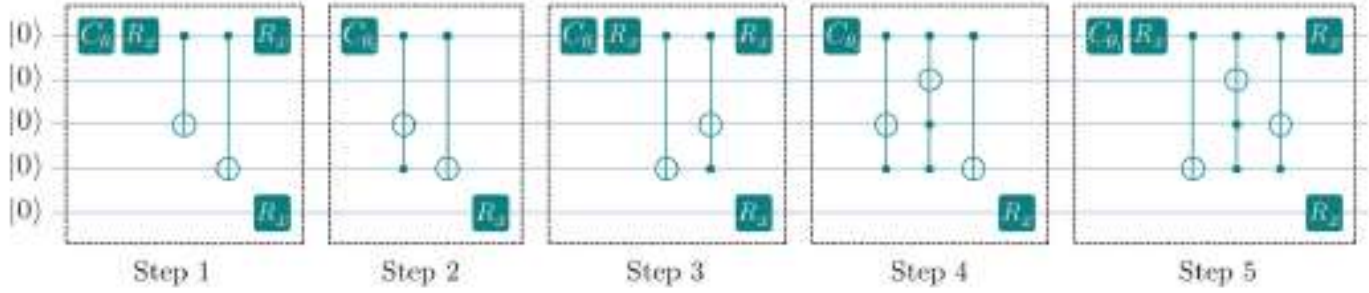
Mapping of position to qubit gates

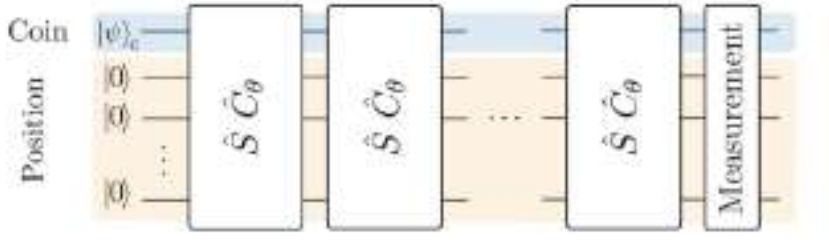
Position	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7
Qubit basis	|1001⟩	|1010⟩	|1011⟩	|0100⟩	|0101⟩	|0110⟩	|0111⟩	|0000⟩	|0001⟩	|0010⟩	|0011⟩	|1100⟩	|1101⟩	|1110⟩	|1111⟩

ARTICLE

https://doi.org/10.1038/s41467-020-17519-4 OPEN

Quantum walks and Dirac cellular automata on a programmable trapped-ion quantum computer



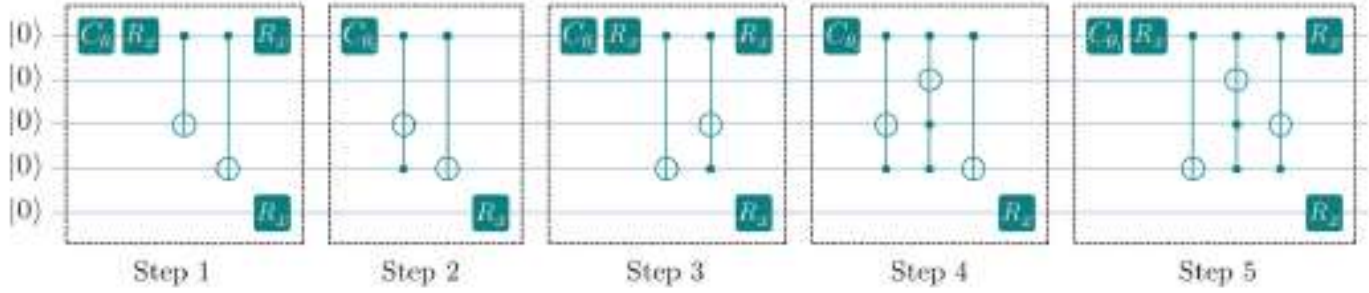


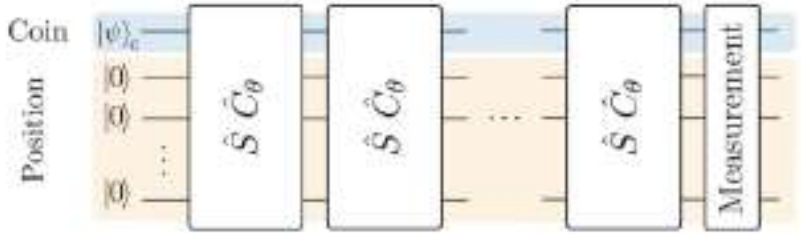
	DQW				DCA	
	$\|0\rangle/\|1\rangle$		$\|0\rangle + i\|1\rangle$		$\|0\rangle + i\|1\rangle$	
step	R	XX	R	XX	R	XX
1	5	2	6	2	5	2
2	10	4	10	4	12	4
3	12	4	12	4	11	4
4	25	11	25	11	27	11
5	26	11	26	11	26	11
Total:	78	32	79	32	81	32

ARTICLE

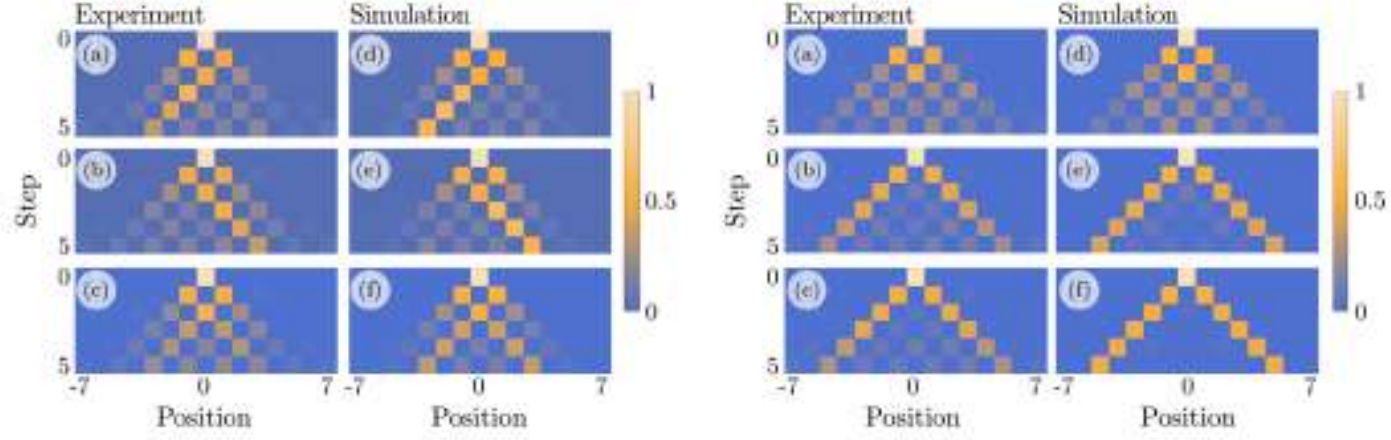
https://doi.org/10.1038/s41467-020-17519-4 OPEN

Quantum walks and Dirac cellular automata on a programmable trapped-ion quantum computer





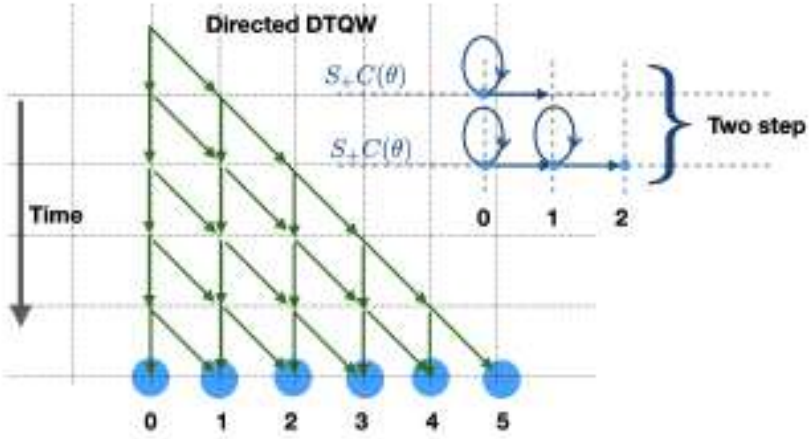
	DQW				DCA	
	$\|0\rangle/\|1\rangle$		$\|0\rangle + i\|1\rangle$		$\|0\rangle + i\|1\rangle$	
step	R	XX	R	XX	R	XX
1	5	2	6	2	5	2
2	10	4	10	4	12	4
3	12	4	12	4	11	4
4	25	11	25	11	27	11
5	26	11	26	11	26	11
Total:	78	32	79	32	81	32



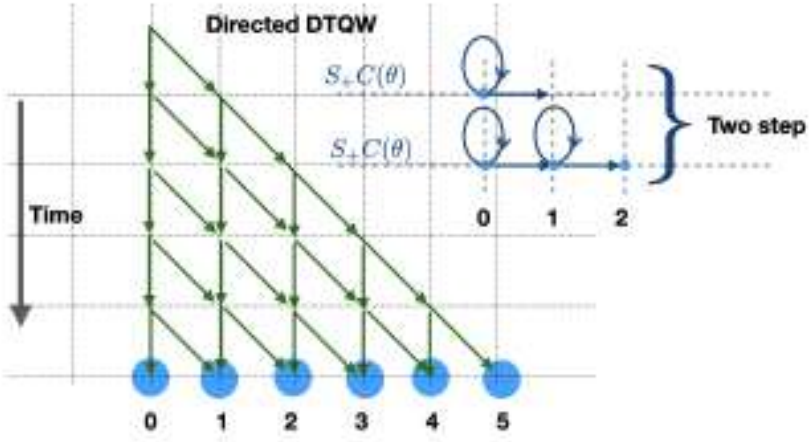
Nature Communication 11, 3720 (2020) ; Phys. Rev. A 104, 062401 (2021)

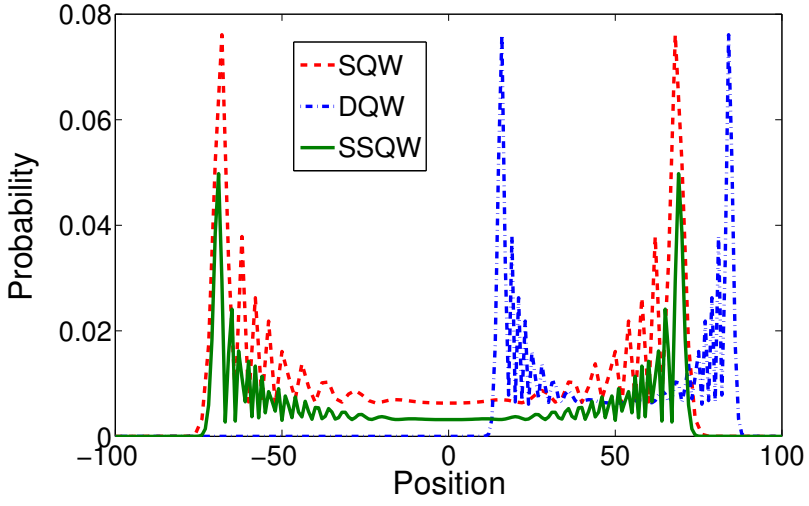
Directed quantum walks and equivalence

Directed quantum walks and equivalence

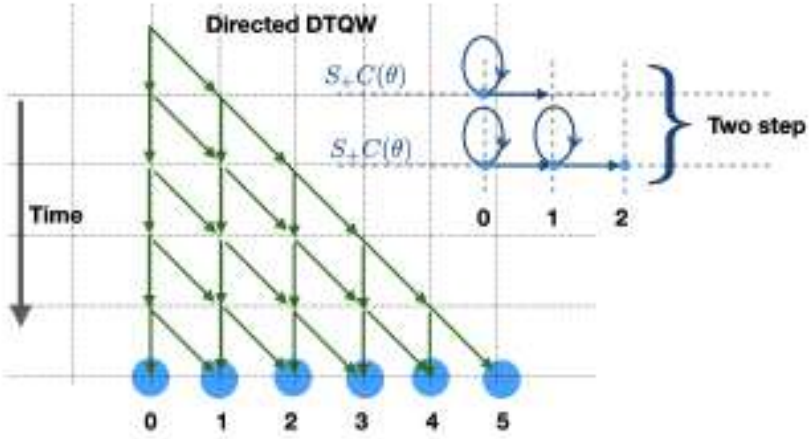


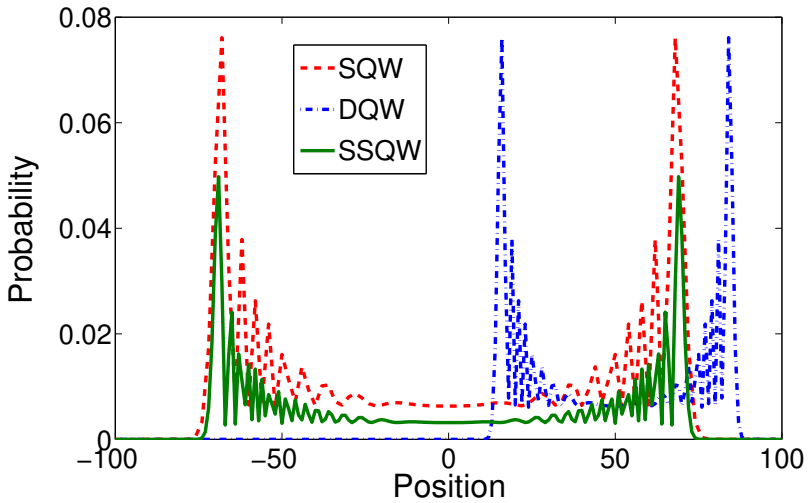
Directed quantum walks and equivalence

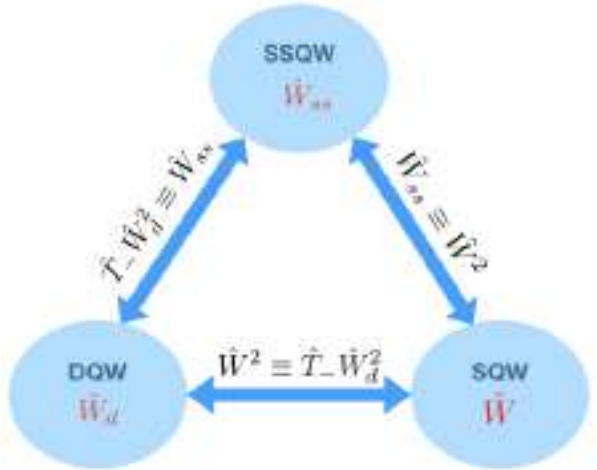




Directed quantum walks and equivalence







$$i\hbar\frac{\partial}{\partial t}\left|\psi(t)\right\rangle = \hat{H}\left|\psi(t)\right\rangle$$

$$\frac{\partial|\Psi(t)\rangle}{\partial t} = -\frac{i}{\hbar}\hat{H}|\Psi(t)\rangle$$

$$\int_0^\tau \frac{\partial|\Psi(t)\rangle}{|\Psi(t)\rangle} = \int_0^\tau -\frac{i}{\hbar}\hat{H}\partial t$$

$$\ln\left|\Psi(\tau)\right\rangle - \ln\left|\Psi(0)\right\rangle = -\frac{i}{\hbar}\hat{H}\tau$$

$$\Psi(\tau)\rangle = e^{-i\hat{H}\tau/\hbar}|\Psi(0)\rangle,$$

Simulation of Hamiltonians

- Two scenarios:

1. The Hamiltonian is given as a sum of interaction terms:

$$H = \sum_j H_j$$

2. The Hamiltonian is sparse, in that it has no more than d nonzero elements in any row or column.

Standard methods

Decompose the Hamiltonian as

$$H = \sum_{k=1}^{M} H_k$$

The individual Hamiltonians H_k can be limited-dimension interaction Hamiltonians (Lloyd, 1996).

Approximate evolution for short time as

$$e^{-iHT} = \prod_{k=1}^{M} e^{-iH_k T}$$

For longer times, we divide the time up into many short times

$$e^{-iHT} = \left(\prod_{k=1}^{M} e^{-iH_k T/r} \right)^r$$

Standard methods

- More generally, we would like to be able to simulate *sparse* Hamiltonians.

$$H = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & \sqrt{2}i & \cdots & 0 \\ 0 & 3 & 0 & 0 & 0 & 1/2 & \cdots & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & \cdots & -\sqrt{3}+i \\ 0 & 0 & 0 & 1 & e^{i\pi/7} & 0 & \cdots & 0 \\ 0 & 0 & 0 & e^{-i\pi/7} & 2 & 0 & \cdots & 0 \\ -\sqrt{2}i & 1/2 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -\sqrt{3}-i & 0 & 0 & 0 & \cdots & 1/10 \end{pmatrix}$$

- Positions and values of non-zero elements are given by oracle.

- This enables application to many other problems.

Standard methods

- The individual H_k can be 1-sparse Hamiltonians obtained by a decomposition technique (2003).
- Efficiency can be increased by improved decomposition techniques (2007; 2010).
- Higher-order decomposition formulae can also be used to obtain greater efficiency (2007).

Quantities involved in simulation

We want to simulation quantum evolution under a Hamiltonian

$$\frac{d}{dt}|\psi\rangle = -iH(t)|\psi\rangle$$

- ε – allowable error in the simulation
- T – time of evolution under the Hamiltonian
- d – sparseness, i.e. maximum number of nonzero elements
- $\|H\|$ – norm of the Hamiltonian to be simulated
- $\|H'\|$ – norm of the time-derivative of the Hamiltonian
- N – dimension of the system

Standard methods - Limitations

- The scaling is always polynomial in the allowable error, ε.
- The scaling for time-dependent Hamiltonians depends heavily on the derivatives of the Hamiltonian.

- The scaling in T is always superlinear, whereas lower bound is linear in T.
- The scaling is at best d^3 in the sparseness.

Known results

- It is possible to decompose a sparse Hamiltonian into $O(d^2)$ 1-sparse Hamiltonians with complexity $O(\log^* n)$.
- This can be improved to $O(d)$ Hamiltonians, at the cost of complexity linear in d.

- Arbitrary order Lie-Trotter-Suzuki formulae can be used to obtain scaling as $O((\|H\|T)^{1+1/2k})$ for arbitrarily large integer k. The scaling in terms of the allowable error is $O\left(\frac{1}{\varepsilon^{\frac{1}{2k}}}\right)$.
- Using quantum walks without a decomposition enables complexity strictly linear in $\|H\|T$, but as scaling in the error of $O(1/\sqrt{\varepsilon})$

.

- Similar scaling can be obtained for *time-dependent* Hamiltonians, but the complexity now depends on the higher-order derivatives.
- An algorithm with randomised times enables complexity independent of the derivatives of the Hamiltonian, at the expense of worse scaling in ε.

1. Decompose Hamiltonian to 1-sparse

- Sparse Hamiltonian has no more than d nonzero elements in any row or column, e.g. $d = 2$

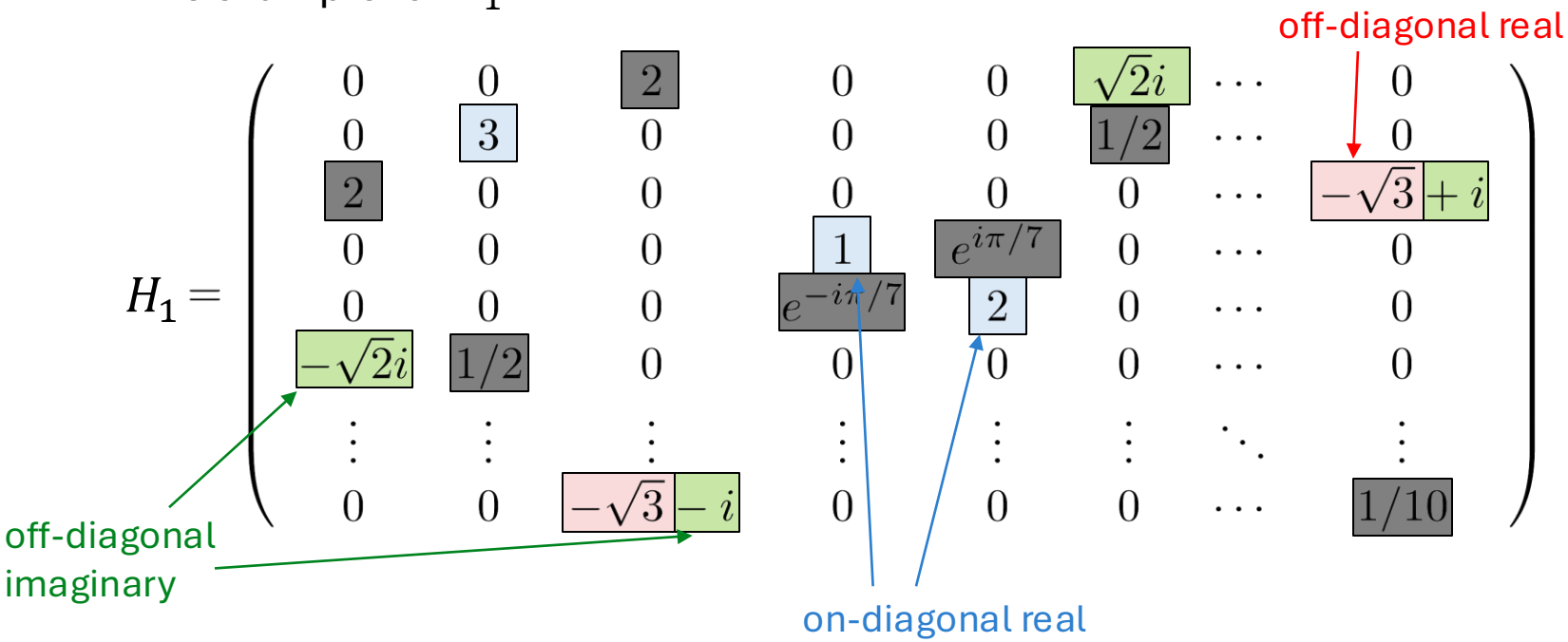
$$H = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & \sqrt{2}i & \cdots & 0 \\ 0 & 3 & 0 & 0 & 0 & 1/2 & \cdots & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & \cdots & -\sqrt{3}+i \\ 0 & 0 & 0 & 1 & e^{i\pi/7} & 0 & \cdots & 0 \\ 0 & 0 & 0 & e^{-i\pi/7} & 2 & 0 & \cdots & 0 \\ -\sqrt{2}i & 1/2 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -\sqrt{3}-i & 0 & 0 & 0 & \cdots & 1/10 \end{pmatrix}$$

- A 1-sparse Hamiltonian has no more than one nonzero element.
- We could decompose Hamiltonian into H_1 and H_2 shown in blue and yellow.

D. W. Berry, G. Ahokas, R. Cleve, and B. C. Sanders, Comm. Math. Phys. **270**, 359 (2007).

2. Decompose 1-sparse to self-inverse

- We further divide the 1-sparse Hamiltonian into X, Y and Z components, in this example for H_1.



- The X and Y components are proportional to Pauli X and Y matrices in each 2×2 subspace.
- The Z component is a phase shift in a 1×1 subspace.

2. Decompose 1-sparse to self-inverse

- Consider just the X component. We further decompose it into components of magnitude $2\varepsilon_H$.

$$H_{1,X} = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & \sqrt{2}i & \cdots & 0 \\ 0 & 3 & 0 & 0 & 0 & 1/2 & \cdots & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & \cdots & -\sqrt{3}+i \\ 0 & 0 & 0 & 1 & e^{i\pi/7} & 0 & \cdots & 0 \\ 0 & 0 & 0 & e^{-i\pi/7} & 2 & 0 & \cdots & 0 \\ -\sqrt{2}i & 1/2 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -\sqrt{3}-i & 0 & 0 & 0 & \cdots & 1/10 \end{pmatrix}$$

Take $\varepsilon_H = 1/4$. Then we can approximate

$$-\sqrt{3} \approx -\frac{1}{2} - \frac{1}{2} - \frac{1}{2} + 0$$

take component 2

2. Decompose 1-sparse to self-inverse

- Consider just the X component. We further decompose it into components of magnitude $2\varepsilon_H$.

$$H_{1,X,2} = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & \sqrt{2}i & \cdots & 0 \\ 0 & 3 & 0 & 0 & 0 & 1/2 & \cdots & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & \cdots & -1/2 + i \\ 0 & 0 & 0 & 1 & e^{i\pi/7} & 0 & \cdots & 0 \\ 0 & 0 & 0 & e^{-i\pi/7} & 2 & 0 & \cdots & 0 \\ -\sqrt{2}i & 1/2 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -1/2 - i & 0 & 0 & 0 & \cdots & 1/10 \end{pmatrix}$$

- Take $\varepsilon_H = 1/4$. Then we can approximate

$$-\sqrt{3} \approx -\frac{1}{2} - \frac{1}{2} - \frac{1}{2} + 0$$

take component 2

2. Decompose 1-sparse to self-inverse

- To obtain self-inverse matrices, we want $+1$ or -1 to appear in each column once.

$$H_{1,X,2} = \begin{pmatrix} 0 & 0 & 2 & 0 & 0 & \sqrt{2}i & \cdots & 0 \\ 0 & 3 & 0 & 0 & 0 & 1/2 & \cdots & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & \cdots & -1/2 + i \\ 0 & 0 & 0 & 1 & e^{i\pi/7} & 0 & \cdots & 0 \\ 0 & 0 & 0 & e^{-i\pi/7} & 2 & 0 & \cdots & 0 \\ -\sqrt{2}i & 1/2 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -1/2 - i & 0 & 0 & 0 & \cdots & 1/10 \end{pmatrix}$$

- We further expand

$$\frac{1}{2} = \frac{1}{4} + \frac{1}{4} \qquad -\frac{1}{2} = -\frac{1}{4} - \frac{1}{4} \qquad 0 = \frac{1}{4} - \frac{1}{4}$$

2. Decompose 1-sparse to self-inverse

To obtain self-inverse matrices, we want $+1$ or -1 to appear in each column once.

$$H_{1,X,2,+} = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & \sqrt{2}i & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 1/2 & \cdots & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & \cdots & -1+i \\ 0 & 0 & 0 & 1 & e^{i\pi/7} & 0 & \cdots & 0 \\ 0 & 0 & 0 & e^{-i\pi/7} & 1 & 0 & \cdots & 0 \\ -\sqrt{2}i & 1/2 & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & -1-i & 0 & 0 & 0 & \cdots & 1/10 \end{pmatrix} \varepsilon_H$$

- We further expand

take first component

$$\frac{1}{2} = \frac{1}{4} + \frac{1}{4} \qquad -\frac{1}{2} = -\frac{1}{4} - \frac{1}{4} \qquad 0 = \frac{1}{4} - \frac{1}{4}$$

- To make it 1-sparse we fill in on the diagonal as needed.

3. Trotter expansion

- The Hamiltonian evolution is

$$\exp(-i(H_1 + H_2)T)$$

- More generally time-dependent evolution

time ordering → $\mathscr{T}$ $\exp\left[-i\int_0^T (H_1(t) + H_2(t))dt\right]$

- This can be thought of as the limit of a large number, r, of small intervals.

$$\lim_{r\to\infty} \prod_{j=1}^{r} e^{-iH_1(t_j)\delta t} e^{-iH_2(t_j)\delta t} \qquad t_j = j\delta t, \quad \delta t = T/r$$

- We can approximate the time evolution using finite r. The error scales as

$$O\left(\frac{(\Lambda T)^2}{r}\right) \qquad \Lambda = \max(\|H\|, \|H'\|)$$

- To bound error by ε, can use

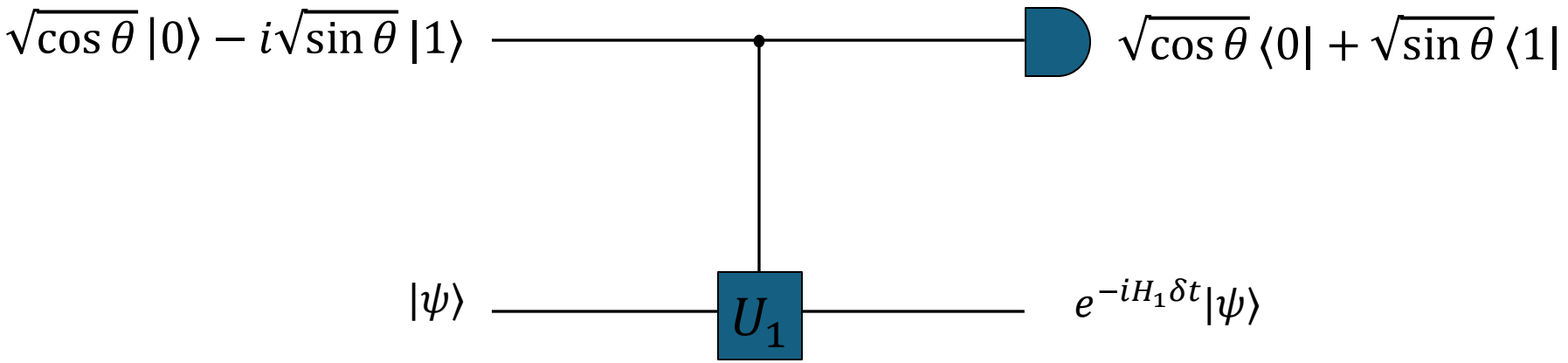
$$r \propto \frac{(\Lambda T)^2}{\varepsilon}$$

4. Using CGMSY'09 technique

- $H_1 = \varepsilon_H U_1$, where U_1 is self-inverse, so

$$e^{-iH_1\delta t} = \mathbb{I}\cos\theta - iU_1\sin\theta \qquad \theta = \varepsilon_H \delta t$$

- Implement the operation probabilistically with a control qubit.



R. Cleve, D. Gottesman, M. Mosca, R. Somma, and D. Yonge-Mallo, In Proc. 41st ACM Symposium on Theory of Computing, pp. 409-416 (2009).

4. Using CGMSY'09 technique

- $H_1 = \varepsilon_H U_1$, where U_1 is self-inverse, so

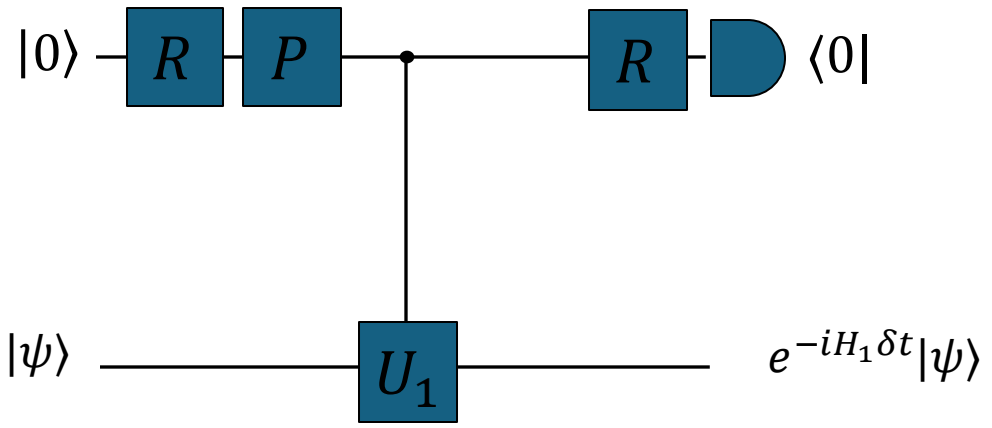
$$e^{-iH_1\delta t} = \mathbb{I}\cos\theta - iU_1\sin\theta \qquad \theta = \varepsilon_H \delta t$$

- Implement the operation probabilistically with a control qubit.

$$R = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$$

$$\beta = \sqrt{\sin\theta}$$

$$P = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$



Density Operator

Suppose we have an apparatus which prepares quantum systems in certain states. For instance, this could be an oven producing spin 1/2 particles, or a quantum optics setup producing photons. But suppose that this apparatus is imperfect, so it does not always produces the same state. That is, suppose that it produces a state $|\psi_1\rangle$ with a certian probability q_1 or a state $|\psi_2\rangle$ with a certain probability q_2 and so on.

All that we assume is that they behave like classical probabilities (classical uncertainty)

$$q_i \in [0,1], \qquad \text{and} \quad \sum_i q_i = 1$$

Now let A be an observable. If the state is $|\psi_1\rangle$, then the expectation value of A will be $\langle\psi_1|A|\psi_1\rangle$. But if it is $|\psi_2\rangle$ then it will be $\langle\psi_2|A|\psi_2\rangle$. To compute the actual expectation value of A we must therefore perform an average of quantum averages:

$$\langle A\rangle = \sum_i q_i \langle\psi_i|A|\psi_i\rangle$$

What is important to realize is that this type of average *cannot* be writen as $\langle\phi|A|\phi\rangle$ for some ket $|\phi\rangle$. If we want to attribute a "state" to our system, then we must generalize the idea of ket.

$$\langle\psi_i|A|\psi_i\rangle = \mathrm{tr}\left[A|\psi_i\rangle\langle\psi_i|\right] \Longrightarrow \langle A\rangle = \sum_i q_i \,\mathrm{tr}\left[A|\psi_i\rangle\langle\psi_i|\right] = \mathrm{tr}\left\{A\sum_i q_i|\psi_i\rangle\langle\psi_i|\right\}$$

Density Operator

$$\langle\psi_i|A|\psi_i\rangle = \mathrm{tr}\left[A|\psi_i\rangle\langle\psi_i|\right] \qquad \Longrightarrow \quad \langle A\rangle = \sum_i q_i \,\mathrm{tr}\left[A|\psi_i\rangle\langle\psi_i|\right] = \mathrm{tr}\left\{A\sum_i q_i|\psi_i\rangle\langle\psi_i|\right\}$$

This motivates us to define the **density matrix** as

$$\boxed{\rho = \sum_i q_i|\psi_i\rangle\langle\psi_i|}$$

With this idea, we may now recast all of quantum mechanics in terms of density matrices, instead of kets.

Therefore, most general representation of a quantum system is written in terms of an operator ρ called the **density operator, or density matrix**. It is designed in a way that naturally encompasses both quantum and classical probabilities.

When $\rho = |\psi\rangle\langle\psi|$ we say we have a pure state. And in this case, it is not necessary to use ρ at all. One may simply continue to use ket notation.

A state which is not pure is usually called a mixed state. In this case kets won't help us and we must use ρ

Example

To start, suppose a machine tries to produce qubits in the state $|0\rangle$. But it is not very good so it only produces $|0\rangle$ with probability q. And, with probability $1-q$ it produces a state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$, where θ may be some small angle. The density matrix for this system will then be

$$\rho = q|0\rangle\langle 0| + (1-q)|\psi\rangle\langle\psi| = \begin{pmatrix} q + (1-q)\cos^2\frac{\theta}{2} & (1-q)\sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ (1-q)\sin\frac{\theta}{2}\cos\frac{\theta}{2} & (1-q)\sin^2\frac{\theta}{2} \end{pmatrix}$$

For instance, machine can produce $|0\rangle, |\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle,$ and so on.

The mixed state will have all these states with some probability.

Example

Let us consider a $50:50$ mixture of states $|0\rangle$ and $|1\rangle$

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

Let us consider a $50:50$ mixture of states $|\pm\rangle$

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

We see that both are identical. Hence, we have *no way to tell* if we began with a 50-50 mixture of $|0\rangle$ and $|1\rangle$ or of $|+\rangle$ and $|-\rangle$. By mixing stuff, we have lost information.

Interpretation of matrix element in density matrix

For an arbitrary state $c_\uparrow|\uparrow\rangle + c_\downarrow|\downarrow\rangle$,

$$\rho = \begin{pmatrix} c_\uparrow^* & c_\downarrow^* \end{pmatrix} \begin{pmatrix} c_\uparrow \\ c_\downarrow \end{pmatrix} = \begin{pmatrix} |c_\uparrow|^2 & c_\downarrow^* c_\uparrow \\ c_\uparrow^* c_\downarrow & |c_\downarrow|^2 \end{pmatrix}$$

Diagonal elements = probabilities

Off-diagonal elements = "coherences"
(provide info. about relative phase)

Example

Let us consider a $50:50$ mixture of states $|0\rangle$ and $|1\rangle$

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

$$\text{For a state } |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix},$$

$$\rho = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}.$$

We can see the off-diagonal element appearing for the superposition state (coherence / relative phase).

What happens when we don't look at part of the system ?

When you calculate expectation values, you trace over the system.
If your operators depend only on a subsystem, then it makes no difference whether you trace over *other* systems before or after:

$$
\begin{aligned}
\mathrm{Tr}\rho A &= \sum_i \langle i|\rho A|i\rangle \\
&\Rightarrow \sum_i \sum_j \langle i|_{sys}\langle j|_{env}\rho A|i\rangle_{sys}|j\rangle_{env} \\
&= \sum_i \langle i|_{sys}\left\{\sum_j \langle j|_{env}\rho|j\rangle_{env}\right\}A|i\rangle_{sys} \\
&\equiv \sum_i \langle i|_{sys}\left\{\mathrm{Tr}_{env}\rho\right\}A|i\rangle_{sys} \\
&= \mathrm{Tr}_{sys}\rho_{sys}A\ , \\
\mathrm{with}\rho_{sys} &\equiv \mathrm{Tr}_{env}\rho\ .
\end{aligned}
$$

Decoherence arise from loss of information

Taking this trace over the environment retains only terms diagonal in the environment variables – i.e., no cross-terms (coherences) remain if they refer to different states of the environment.

(If there is any way – even in principle – to tell which of two paths was followed, then no interference may occur.)

Suppose that the environment has a record of the spin of our system, such that the total state of the universe is $|\uparrow\rangle_s|\uparrow\rangle_e + |\downarrow\rangle_s|\downarrow\rangle_e$.

ρ_s when env is ↑

$$\rho = \begin{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1/2 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix} \end{pmatrix}$$

ρ_s when env is ↓

Decoherence arise from loss of information

$$\rho = \begin{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1/2 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1/2 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix} \end{pmatrix}$$

coherence lost

$$\mathrm{Tr}_{env}\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

There is still coherence between ↓↓ and ↑↑, but if the environment is not part of your interferometer, you may as well consider it to have "collapsed" to ↑ or ↓ .

This means there is no effective coherence if you look only at the system.

Density operators - summary

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|.$$

(**Characterization of density operators**). *An operator ρ is the density operator associated to some ensemble $\{p_j, |\psi_j\rangle\}_j$ if and only if it satisfies the following conditions:*

i) ρ *has trace equal to one, i.e.,* $\mathrm{Tr}\,(\rho) = 1$

ii) ρ *is positive (and, thus, Hermitian), i.e.,* $\rho \geq 0$.

Please prove this as an exercise

(**Pure density operators**). *The density operator describes a pure state (i.e., a single state vector) if and only if* $\mathrm{Tr}\,(\rho^2) = 1$.

Density operators - summary

(**Pure density operators**). *The density operator describes a pure state (i.e., a single state vector) if and only if* $\mathrm{Tr}\left(\rho^2\right) = 1$.

Proof.

$$\begin{aligned}
\mathrm{Tr}\left(\rho^2\right) &= \mathrm{Tr}\left(\sum_{j,k} p_j p_k \left|\psi_j\right\rangle \left\langle\psi_j|\psi_k\right\rangle \left\langle\psi_k\right|\right) \\
&= \sum_{j,k} p_j p_k \mathrm{Tr}\left(\left|\psi_j\right\rangle \left\langle\psi_j|\psi_k\right\rangle \left\langle\psi_k\right|\right) \\
&= \sum_{j,k} p_j p_k \underbrace{\left|\left\langle\psi_j|\psi_k\right\rangle\right|^2}_{\leq 1} \\
&\leq \sum_{j,k} p_j p_k \\
&= 1.
\end{aligned}$$

Density operators - summary

1) We denote the space of density operators on $\mathcal{H}$ by $\mathcal{D}(\mathcal{H})$.

2) We call $\mathrm{Tr}\,(\rho^2)$ the purity of ρ. It satisfies $1/\dim(\mathcal{H}) \leq \mathrm{Tr}\,(\rho^2) \leq 1$.

3) If ρ is not pure, i.e., $\mathrm{Tr}\,(\rho^2) \neq 1$, then we say that ρ is mixed.

4) If $\mathrm{Tr}\,(\rho^2) = 1/\dim(\mathcal{H})$, we say that ρ is maximally mixed.

Note that different ensembles can give rise to the same density operator. For example, with $|a\rangle = \sqrt{3/4}\,|0\rangle + \sqrt{1/4}\,|1\rangle$ and $|b\rangle = \sqrt{3/4}\,|0\rangle - \sqrt{1/4}\,|1\rangle$, the ensemble $\{(1/2, |a\rangle), (1/2, |b\rangle)\}$ gives rise to the same density operator as $\{(3/4, |0\rangle), (1/4, |1\rangle)\}$, since

$$\begin{aligned}
\rho &= \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| \\
&= \frac{1}{2}\left(\frac{3}{4}|0\rangle\langle 0| + \frac{\sqrt{3}}{4}|0\rangle\langle 1| + \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|\right) \\
&+ \frac{1}{2}\left(\frac{3}{4}|0\rangle\langle 0| - \frac{\sqrt{3}}{4}|0\rangle\langle 1| - \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|\right) \\
&= \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.
\end{aligned}$$

Evolutions in density operators

The evolution of the closed system is described by a unitary transformation.

When states are evolved, action of unitary operator will be :

$$|\psi\rangle \rightarrow |\psi'\rangle = U|\psi\rangle$$

When density operators are evolved, action of unitary operator will be :

$$\rho \rightarrow \rho' = U\rho U^{\dagger}$$

The evolution of the open systems is described using Kraus operators. We will not discuss that here.

The von Neumann equation : Time evolution o any ket in density operator $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle.$

$$\rho(t) = \sum_i q_i e^{-iHt}|\psi_i(0)\rangle\langle\psi_i(0)|e^{iHt} = e^{-iHt}\rho(0)e^{iHt}.$$

von Neumann's equation:

Differentiating with respect to t we then get

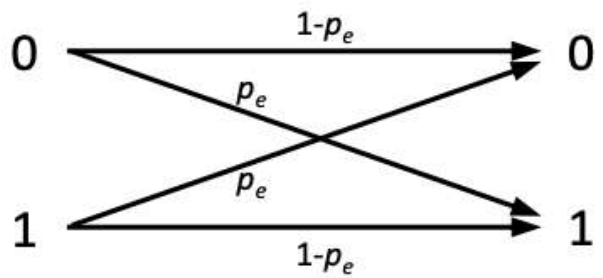
$$\frac{\mathrm{d}\rho}{\mathrm{d}t} = (-iH)e^{-iHt}\rho(0)e^{iHt} + e^{-iHt}\rho(0)e^{iHt}(iH) = -iH\rho(t) + i\rho(t)H$$

$$\frac{\mathrm{d}\rho}{\mathrm{d}t} = -i[H,\rho], \qquad \rho(t) = e^{-iHt}\rho(0)e^{iHt}$$

Quantum Errors' and Quantum Error corrections

Classical Errors' : Binary symmetric channel

One of the simplest models for single-bit (classical) errors is the *binary symmetric channel*, in which each possible state of the bit, 0 and 1 "flips" to the other with some probability p_e:



Note that, without loss of generality we can assume $p_e \leq 0.5$, because if $p_e > 0.5$ then it is more likely than not that a bit-flip has occurred, so we can interpret a received 0 as a 1 and vice-versa. In the case where $p_e = 0.5$ we cannot recover any information from the channel.

Errors in quantum computers

- Classically, bits can flip. (Or be erased.)
  - i.e., 0 -> 1 and 1 -> 0 with some probability p.
- Qubits have a larger state space, therefore more things can go wrong.
  - Any operation which can be considered a gate can also be considered an error.
  - Example: Pauli errors

$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$	$Y\|0\rangle = i\|1\rangle = iXZ\|0\rangle$ $Y\|1\rangle = -i\|0\rangle = iXZ\|1\rangle$
Bit flip	Phase flip	Bit & phase flip

Depolarizing channel

$$X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad Y=\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix},\quad Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

$$\mathcal{E}(\rho)=(1-p)\rho+\frac{p}{3}\left(X\rho X+Y\rho Y+Z\rho Z\right)$$

$$X^2=Y^2=Z^2=I\Rightarrow\sum M_a^{\dagger}M_a=(1-p)I+3(p/3)I=I$$

Classical 'Errors' : the three bit repetition code

If we wish to send a single bit over a binary symmetric channel, then we can encode the bit, by simply repeating it three times. That is, if we wish to transmit a 0, we send three bits (sequentially) in the state 0, and likewise for 1. This can be denoted as:

$$0 \to 000$$
$$1 \to 111$$

Once the three bits have been received, they are decoded by a "majority vote". So in order for an error to occur, it is necessary that either two of the three bits have been flipped (which can occur in three different ways), or all three have been, that is:

$$p'_e = 3p_e^2(1-p_e) + p_e^3$$

Which is less than p_e if $p_e < 0.5$. Typically, p_e is small, and we can describe this as suppressing the error to $\mathcal{O}(p_e^2)$.

Can I do the same for qubits ?

It appears that we cannot directly transfer the classical error correction techniques to the problem of quantum error correction for the following three reasons:

1. The no-cloning principle forbids the copying of quantum states
2. Measurement destroys quantum information
3. Quantum states are continuous : $\alpha|0\rangle + \beta|1\rangle$
   Therefore, quantum errors are also continuous :

$$\alpha|0\rangle + \beta|1\rangle \rightarrow (\alpha + \epsilon_0)|0\rangle + (\beta + \epsilon_1)|1\rangle$$

Thus, classical techniques cannot be directly applied to qubit errors.

Nevertheless, with some ingenuity, techniques to correct quantum errors have been developed.

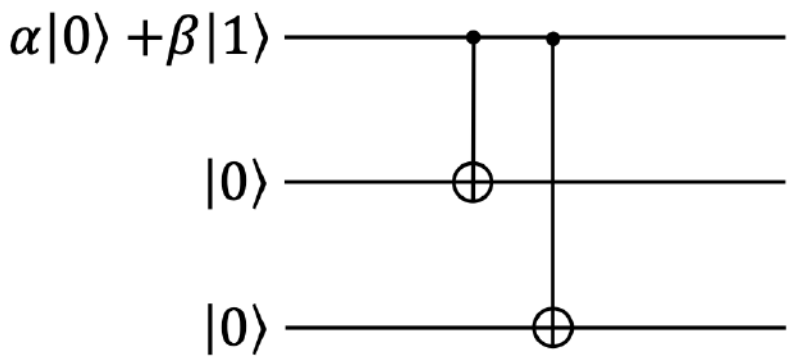
Three qubit bit-flip correction code

The three-bit repetition code guarantees to return the correct bit value, so long as at most one of the bits in the code is flipped. We now use this as inspiration for the **three-qubit bit-flip code, in which entanglement** rather than cloning plays the role of the repetition. That is, we encode the computational basis states:

$$|0\rangle \rightarrow |000\rangle$$

$$|1\rangle \rightarrow |111\rangle$$

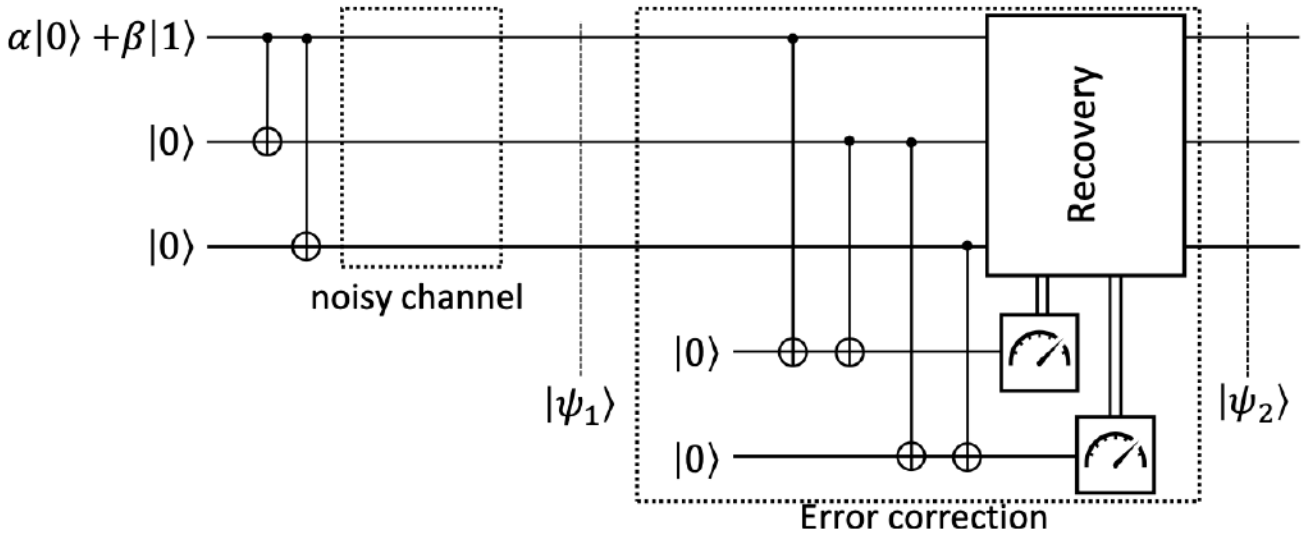
Which is achieved using the following circuit:



The above circuit will result in : $(\alpha|0\rangle + \beta|1\rangle)|0\rangle^{\otimes 2} \rightarrow \alpha|000\rangle + \beta|111\rangle$

The three-qubit bit-flip code: error detection and recovery

To detect and recover bit-flip errors, we supplement the circuit with two ancillas that we use for error detection:



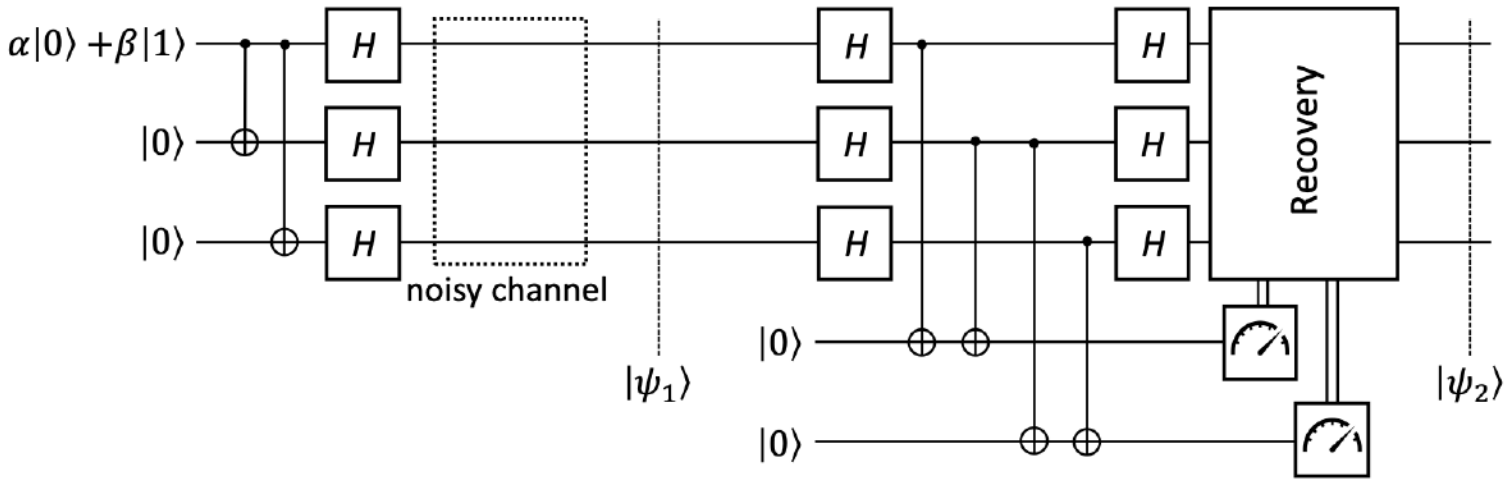
With this circuit, we can detect and recover a single-qubit bit-flip errors

Bit-flip	$\|\psi_1\rangle$	M_1	M_2	Recovery	$\|\psi_2\rangle$
-	$\alpha\|000\rangle + \beta\|111\rangle$	0	0	$I \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
1	$\alpha\|100\rangle + \beta\|011\rangle$	1	0	$X \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
2	$\alpha\|010\rangle + \beta\|101\rangle$	1	1	$I \otimes X \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
3	$\alpha\|001\rangle + \beta\|110\rangle$	0	1	$I \otimes I \otimes X$	$\alpha\|000\rangle + \beta\|111\rangle$

In the circuit we have made we have made comparative parity-check measurements that tell us only about the error and not about the quantum state itself, and so these measurements have not destroyed the quantum state.

The three-qubit phase -flip code: error detection and recovery

To detect and recover phase-flip errors, we again supplement the circuit with two ancillas that we use for error detection:



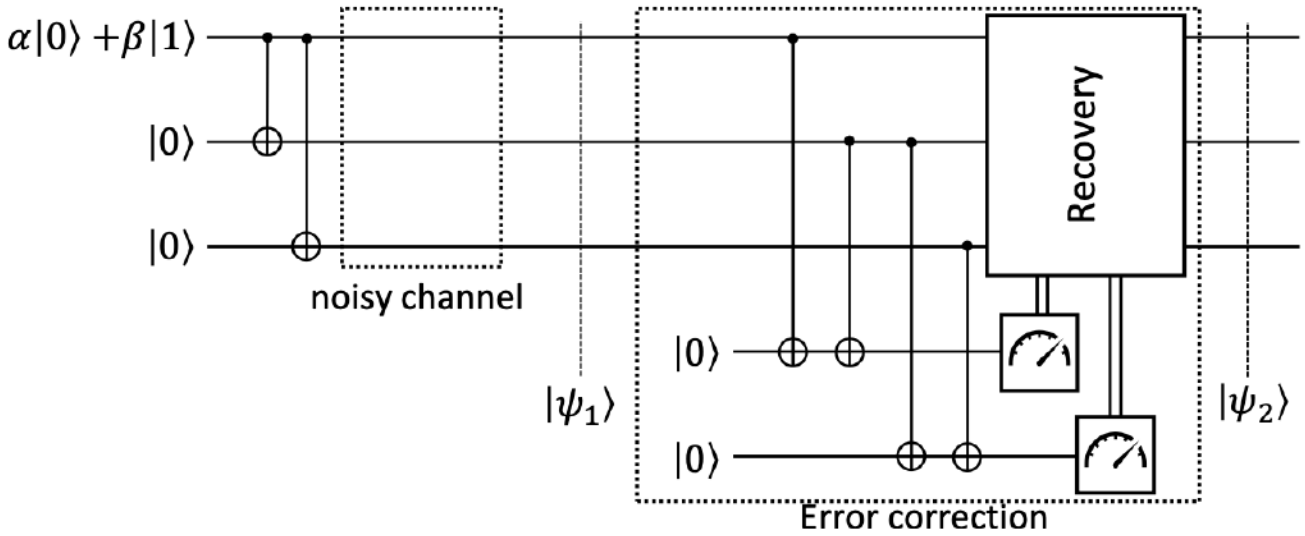
With this circuit, we can detect and recover a single-qubit bit-flip errors

Phase-flip sends : $|\pm\rangle \rightarrow |\mp\rangle$

Phase-flip	$\|\psi_1\rangle$	M_1	M_2	Recovery	$\|\psi_2\rangle$
-	$\alpha\|+++\rangle+\beta\|---\rangle$	0	0	$I\otimes I\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
1	$\alpha\|-++\rangle+\beta\|+--\rangle$	1	0	$Z\otimes I\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
2	$\alpha\|+-+\rangle+\beta\|-+-\rangle$	1	1	$I\otimes Z\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
3	$\alpha\|++-\rangle+\beta\|--+\rangle$	0	1	$I\otimes I\otimes Z$	$\alpha\|+++\rangle+\beta\|---\rangle$

The three-qubit bit-flip code: error detection and recovery (Recap)

To detect and recover bit-flip errors, we supplement the circuit with two ancillas that we use for error detection:



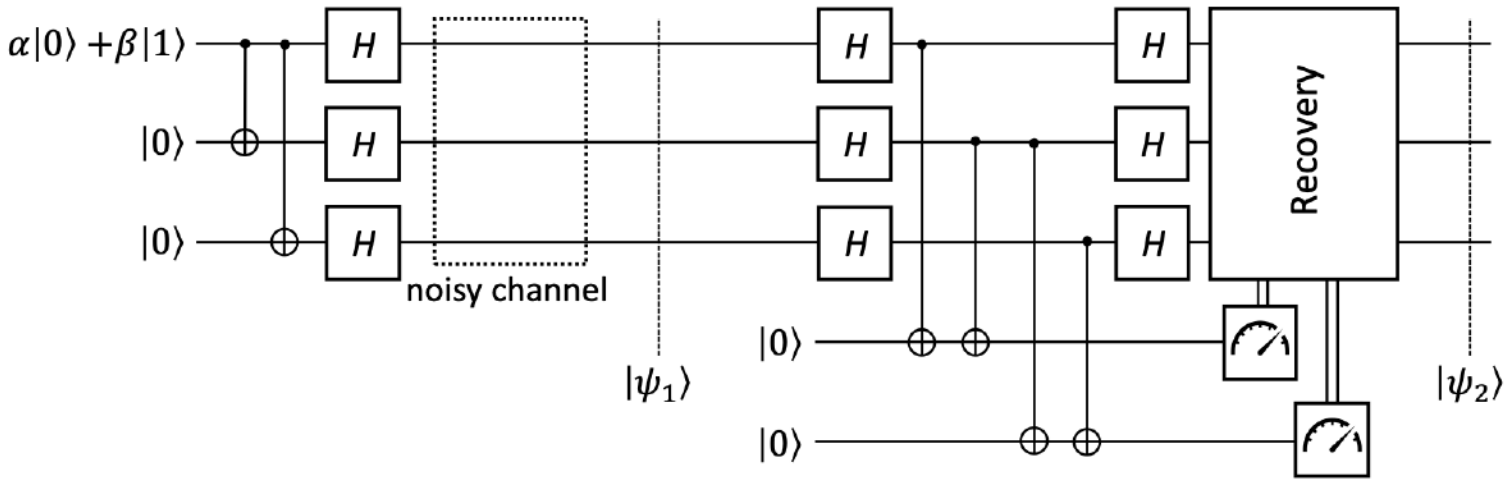
With this circuit, we can detect and recover a single-qubit bit-flip errors

Bit-flip	$\|\psi_1\rangle$	M_1	M_2	Recovery	$\|\psi_2\rangle$
-	$\alpha\|000\rangle + \beta\|111\rangle$	0	0	$I \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
1	$\alpha\|100\rangle + \beta\|011\rangle$	1	0	$X \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
2	$\alpha\|010\rangle + \beta\|101\rangle$	1	1	$I \otimes X \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
3	$\alpha\|001\rangle + \beta\|110\rangle$	0	1	$I \otimes I \otimes X$	$\alpha\|000\rangle + \beta\|111\rangle$

In the circuit we have made we have made comparative parity-check measurements that tell us only about the error and not about the quantum state itself, and so these measurements have not destroyed the quantum state.

The three-qubit phase -flip code: error detection and recovery ((Recap)

To detect and recover phase-flip errors, we again supplement the circuit with two ancillas that we use for error detection:



With this circuit, we can detect and recover a single-qubit bit-flip errors

Phase-flip sends : $|\pm\rangle \rightarrow |\mp\rangle$

Phase-flip	$\|\psi_1\rangle$	M_1	M_2	Recovery	$\|\psi_2\rangle$
-	$\alpha\|+++\rangle+\beta\|---\rangle$	0	0	$I\otimes I\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
1	$\alpha\|-++\rangle+\beta\|+--\rangle$	1	0	$Z\otimes I\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
2	$\alpha\|+-+\rangle+\beta\|-+-\rangle$	1	1	$I\otimes Z\otimes I$	$\alpha\|+++\rangle+\beta\|---\rangle$
3	$\alpha\|++-\rangle+\beta\|--+\rangle$	0	1	$I\otimes I\otimes Z$	$\alpha\|+++\rangle+\beta\|---\rangle$

The Shor code - 9-qubit code

The Shor code is a 9-qubit code which is constructed by **concatenating** the **three-qubit bit-flip and three-qubit phase-flip codes:**

- Concatenation is an important, often used concept in error correction.
- The idea is simply to combine the two codes.
  - **Step 1:** Apply bit flip code to physical qubit.
  - **Step 2:** Apply phase flip code to the logical qubit.

This encodes the computational basis states as follows:

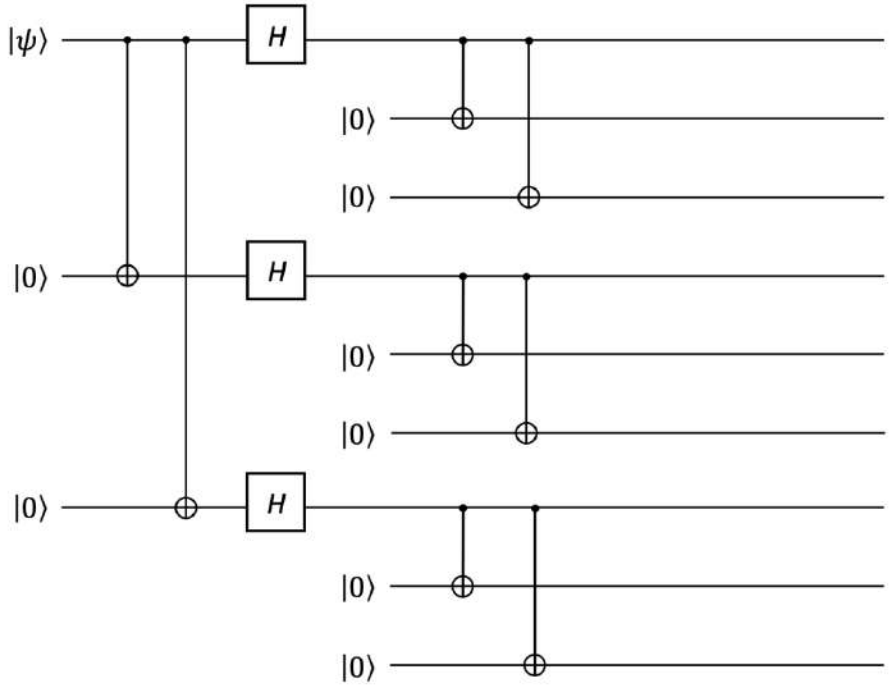
$$|0\rangle \rightarrow |0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \rightarrow |1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

How do we generate a 9-qubit state

$$|0\rangle \rightarrow |0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

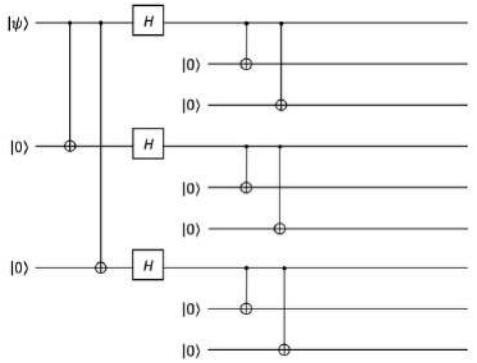
$$|1\rangle \rightarrow |1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$



$$\frac{1}{2\sqrt{2}}\Big(\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$+ \beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

Correcting bit-flip with Shor code



The Shor code can detect and correct a bit-flip on any single qubit. For example, suppose we have an arbitrary quantum state $\alpha|0\rangle+ \beta|1\rangle$. which we encode with the Shor code as:

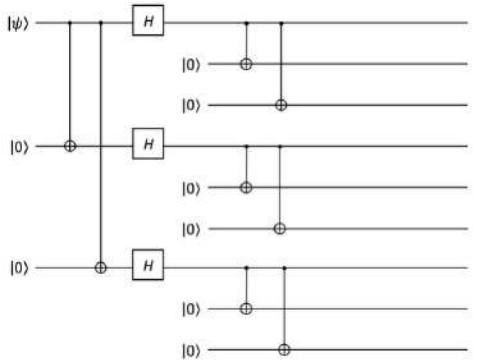
$$\frac{1}{2\sqrt{2}}\Big(\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) + \beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

If a bit-flip occurs on the first qubit, the state becomes:

$$\frac{1}{2\sqrt{2}}\Big(\alpha(|100\rangle + |011\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) + \beta(|100\rangle - |011\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

Which can be detected (and thus recovered from) by parity-check measurements between the first three qubits as in the three-qubit bit-flip code. By symmetry we can see that the same principle applies to all of the nine qubits.

Correcting bit-flip with Shor code



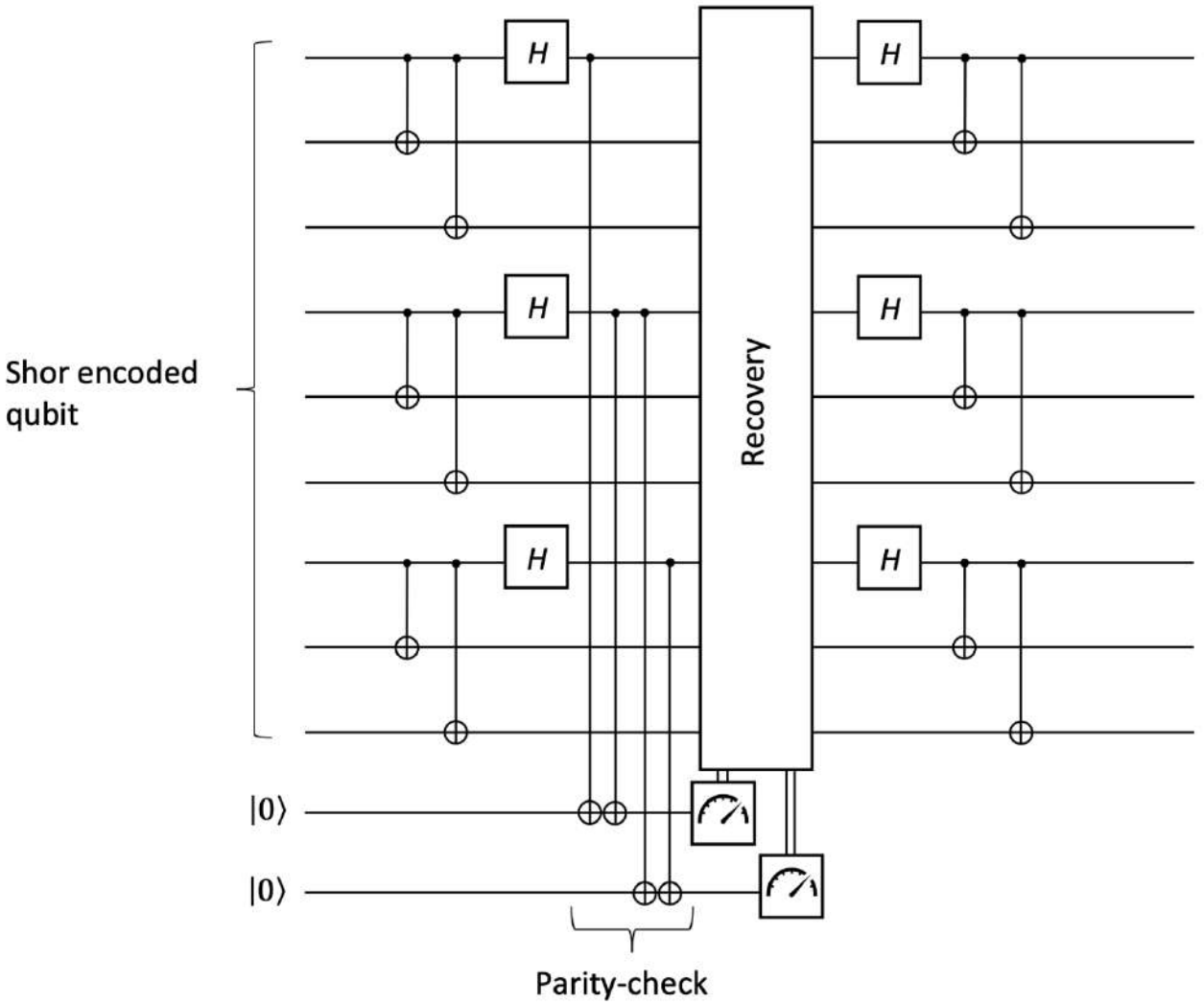
The Shor code can also detect and correct a phase-flip on any single qubit. If a phase-flip occurs on the first qubit, the state becomes:

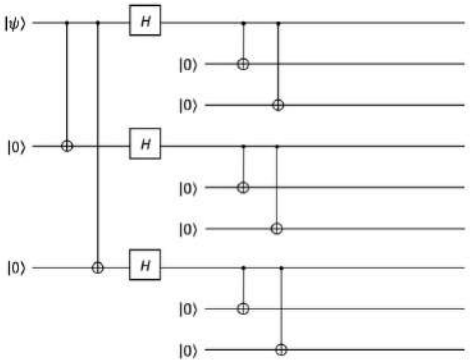
$$\frac{1}{2\sqrt{2}}\Big(\alpha(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) + \beta(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

The key idea here is to detect which of the three blocks of three qubits has experienced a change of sign. This is achieved using the circuit shown on the following slide.

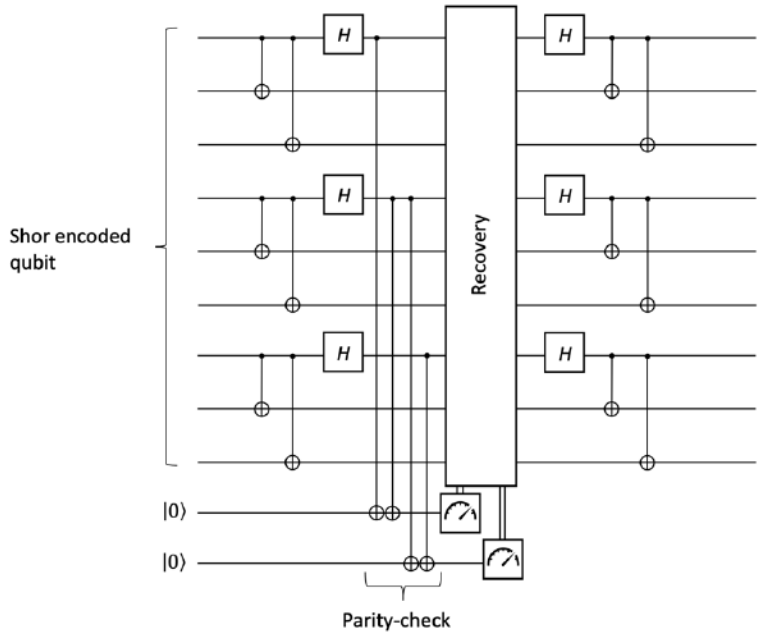
We can also correct combinations of bit- and phase-flips in this way.

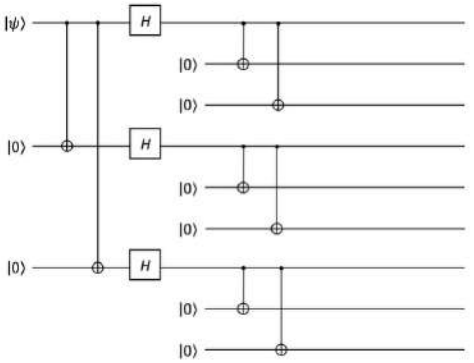
Circuit for correcting phase-flip with Shor code





Circuit for correcting phase-flip with Shor code





The bit-flip error will be identified by two parties of each triplet of the qubit

$$
\begin{aligned}
&Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I, \\
&Z \otimes I \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I, \\
&I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I, \\
&I \otimes I \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes I \otimes I, \\
&I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I, \\
&I \otimes I \otimes I \otimes I \otimes I \otimes I \otimes Z \otimes I \otimes Z.
\end{aligned}
$$

Phase-flip error will be identified by

$$
\begin{aligned}
&X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I, \\
&I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X.
\end{aligned}
$$

The depolarising channel

When studying the (classical) three-bit repetition code, we saw that in practise it is more useful to think of it as a code that suppresses the error in the binary symmetric channel from p_e to $\mathcal{O}(p_e^2)$.

In the quantum case, we can see something similar: Consider the depolarising channel, in which a physical qubit is left unchanged with probability $1 - p_e$; experiences a bit-flip with probability $\frac{p_e}{3}$; experiences a phase-flip with probability $\frac{p_e}{3}$; or experiences both a bit- and phase-flip with probability $\frac{p_e}{3}$.

An analogous argument to that made for the binary symmetric channel can be made to show that the Shor code suppresses the error from p_e to $\mathcal{O}(p_e^2)$ in the depolarising channel.

Correcting any single bit-flip with the Shor code

Suppose the first qubit encounters an error which sends $|0\rangle \to a|0\rangle + b|1\rangle$ and $|1\rangle \to c|0\rangle + d|1\rangle$. We thus have the state:

$$\frac{1}{2\sqrt{2}}\Big(\alpha(a|000\rangle + b|100\rangle + c|011\rangle + d|111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$+ \beta(a|000\rangle + b|100\rangle - c|011\rangle - d|111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

Letting $k+m=a$, $k-m=d$, $l+n=b$ and $l-n=c$, we get

$$\frac{1}{2\sqrt{2}}\Big(k\Big(\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$+ \beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

$$+l\Big(\alpha(|100\rangle + |011\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$+ \beta(|100\rangle - |011\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

$$+m\Big(\alpha(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$+ \beta(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)$$

$$+n\Big(\alpha(|100\rangle - |011\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$+ \beta(|100\rangle + |011\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\Big)\Big)$$

Correcting any single bit-flip with the Shor code ....

We first perform parity-check measurements to detect a bit-flip. The parity check for a bit-flip in the first block of three qubits requires two ancillas (the first comparing the first and second qubits, the second comparing the second and third qubits), whose state (after the parity-check CNOTs) we can append to the Shor code state:

$$\frac{1}{2\sqrt{2}}\Big(k\Big(\alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$
$$+\beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)|00\rangle$$
$$+l\Big(\alpha(|100\rangle+|011\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$
$$+\beta(|100\rangle-|011\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)|10\rangle$$
$$+m\Big(\alpha(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$
$$+\beta(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)|00\rangle$$
$$+n\Big(\alpha(|100\rangle-|011\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$
$$+\beta(|100\rangle+|011\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)|10\rangle\Big)$$

Correcting any single bit-flip with the Shor code ....

If the parity-check measurement outcome is 00, the state collapses to (un-normalised):

$$k\Big(\alpha(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle) + \beta(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)$$

$$+m\Big(\alpha(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle) + \beta(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)$$

In which case there is no bit-flip

If the measurement outcome is 10:

$$l\Big(\alpha(|100\rangle+|011\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle) + \beta(|100\rangle-|011\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)$$

$$+n\Big(\alpha(|100\rangle-|011\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle) + \beta(|100\rangle+|011\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)\Big)\Big)$$

In which case a bit-flip has occurred we can then correct

Correcting any error by correcting only bit- and phase-flips

Following the bit-flip parity-check measurement (and correction if necessary) we perform a parity-check measurement to check for a phase flip. Using the same argument as for the bit-flip detection,

if we measure 0 the state collapses to:

$$\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) + \beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Or if we measure a 1 we get:

$$\alpha(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) + \beta(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

i.e., a phase-flip has occurred which we can then correct. Therefore we have recovered the original state.

Therefore performing bit- and phase-flip parity-check measurements collapses a general state into the case where either the bit / phase flip has occurred or not as per the measurement outcome. This remarkable property allows us to correct a continuum of errors by performing only bit- and phase-flip checks.

Hamming code

Repetition codes are useful for demonstrating the principle of error correction, but are rather too inefficient to use in practise. One particularly elegant code is **the (7,4) Hamming code**, a linear code that encodes a 4-bit data-word, **d**, as a 7-bit code-word **c**.

From Wiki

In coding theory, **Hamming (7,4)** is a linear error-correcting code that encodes four bits of data into seven bits by adding three parity bits. It is a member of a larger family of Hamming codes, but the term *Hamming code* often refers to this specific code that Richard W. Hamming introduced in 1950. At the time, Hamming worked at Bell Telephone Laboratories and was frustrated with the error-prone punched card reader, which is why he started working on error-correcting codes.

Code word **c= Gd mod 2, where G is the generator matrix:**

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

Any errors are detected by applying the parity-check matrix, H, to a given code-word

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

Hamming code - example

Four data bit : (1011)

$$\mathbf{p} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Transmitted code word **c**

$$\mathbf{c = Gp} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \\ 2 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

0110011. will be transmitted in place of 1011

Parity check

$$\mathbf{z = Hc} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

z is syndrome vector, it indicated whether an error has occurred or not. If **z** is null vector, no error

$$\mathbf{c1 = c + e} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Hamming code

0110011. will be transmitted in place of 1011

z is syndrome vector, it indicated whether an error has occurred or not. If **z** is null vector, no error

$$\textbf{c1 = c + e} = \begin{pmatrix}0\\1\\1\\0\\0\\1\\1\end{pmatrix} + \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\1\\0\\1\\1\\1\end{pmatrix}$$

$$\textbf{Hc1} = \begin{pmatrix}1&0&1&0&1&0&1\\0&1&1&0&0&1&1\\0&0&0&1&1&1&1\end{pmatrix}\begin{pmatrix}0\\1\\1\\0\\1\\1\\1\end{pmatrix} = \begin{pmatrix}3\\4\\3\end{pmatrix} = \begin{pmatrix}1\\0\\1\end{pmatrix}$$

$$\textbf{Corrected c1} = \begin{pmatrix}0\\1\\1\\0\\\overline{1}\\1\\1\end{pmatrix} = \begin{pmatrix}0\\1\\1\\0\\0\\1\\1\end{pmatrix}$$

Quantum error correction codes from Hamming code - Steane code

Classical linear codes are efficient, in the sense that code-words are generated by multiplying the data-word by a matrix, which can be compactly described. There is a technique for using classical linear codes to find quantum error correction codes. These codes are known as CSS (Calderbank-Shor-Steane) codes

Among them one particular CSS code, the Steane code, which is constructed from the (7,4) Hamming code and encodes the logical states 0 and 1 as follows:

$$|0_L\rangle = \frac{1}{\sqrt{8}}\big(\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\,\big)$$
$$|1_L\rangle = \frac{1}{\sqrt{8}}\big(\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle$$
$$|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\,\big)$$

Quantum error correction codes from Hamming code - Steane code

Classical linear codes are efficient, in the sense that code-words are generated by multiplying the data-word by a matrix, which can be compactly described. There is a technique for using classical linear codes to find quantum error correction codes. These codes are known as CSS (Calderbank-Shor-Steane) codes

Among them one particular CSS code, the Steane code, which is constructed from the (7,4) Hamming code and encodes the logical states 0 and 1 as follows:

$$|0_L\rangle = \frac{1}{\sqrt{8}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$
$$|1_L\rangle = \frac{1}{\sqrt{8}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle$$
$$|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

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

Any errors are detected by applying the parity-check matrix, H, to a given code-word

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

Quantum error correction codes from Hamming code - Steane code

Classical linear codes are efficient, in the sense that code-words are generated by multiplying the data-word by a matrix, which can be compactly described. There is a technique for using classical linear codes to find quantum error correction codes. These codes are known as CSS (Calderbank-Shor-Steane) codes

Among them one particular CSS code, the Steane code, which is constructed from the (7,4) Hamming code and encodes the logical states 0 and 1 as follows:

$$|0_L\rangle = \frac{1}{\sqrt{8}}\big(\,|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\,\big)$$
$$|1_L\rangle = \frac{1}{\sqrt{8}}\big(\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle$$
$$|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\,\big)$$

Like the Shor code, the Steane code guarantees to correct any bit- and / or phase-flip that occurs on a single qubit. Thus we can see that it also suppresses the error of the depolarising channel from p_e to $O(p^2_e)$.

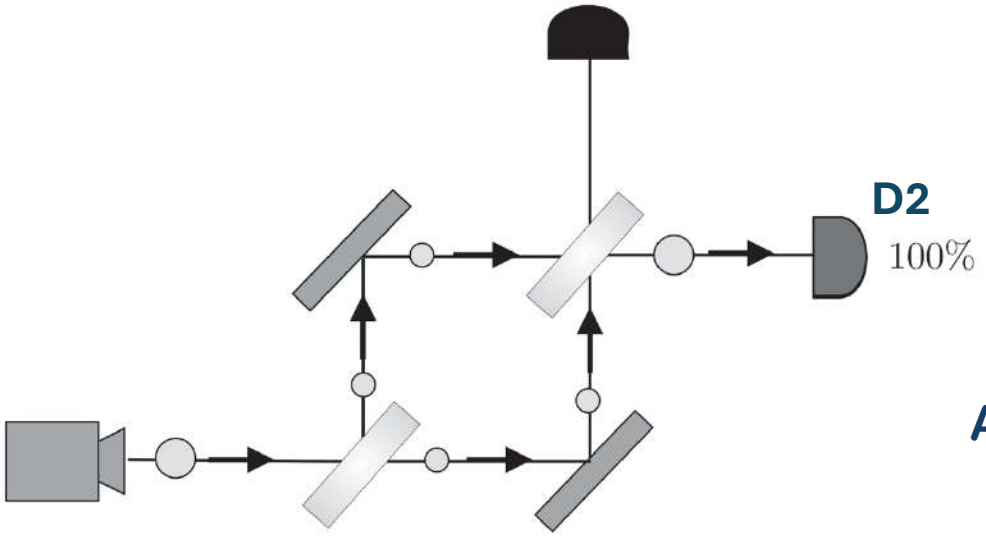
Summary - QEC

We have seen that there are three obstacles to applying the techniques and principles of classical error correction directly to quantum error correction, each of which can be worked around:

- The no-cloning principle means that we cannot simply copy quantum states in repetition codes – instead, we can use entangling to “copy” the information.
- Measurements destroy quantum information: so instead we design the error correcting codes so that the measurements only tell us whether an error has occurred, and nothing about the quantum state itself.
- Quantum errors are continuous, but we have seen that the process of error correction effectively digitises the errors.

Additionally, we have seen that, in practice, classical error correction codes are typically more sophisticated and efficient than simple repetition codes, and that these can be used to design quantum error correction codes, of which the Steane code is an important example.

Recap – Superposition and interference



After first BS :

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

After second BS :

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix}$$

This simple math shows how interference is
Making photon get detected only at D2

Entanglement and Non-locality

Quantum non-locality

Entangled states are those that cannot be written as a tensor product of separate states
The most famous example is the EPR pair :

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Alice will have the first qubit
Bob will have the second qubit
(no constraint on where they should be located)

If Alice makes measurement, Bob's state also collapses and vice versa – Instantaneous information exchange

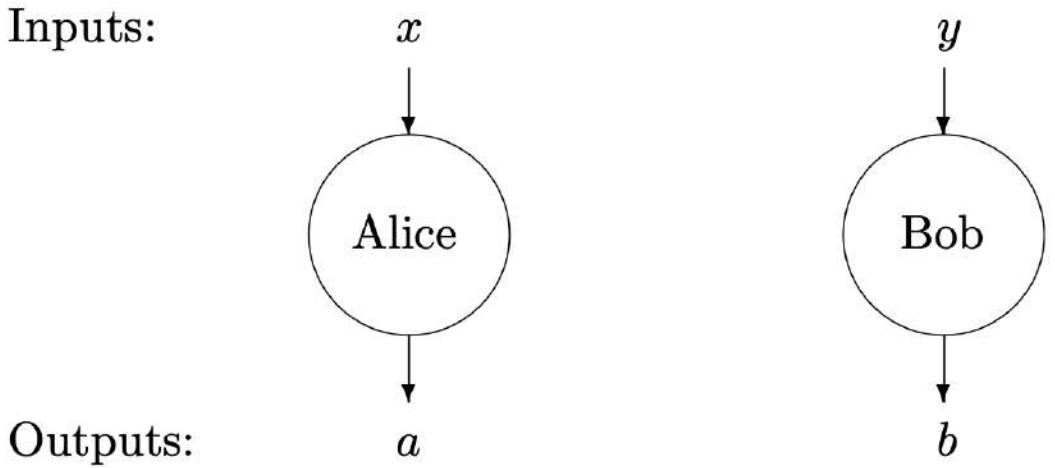
Does not violate locality – No information is transferred from Alice to Bob
It's realist because the measurement has a definite outcome

But still, no local realist theory explains this phenomena

John Bell devised an entanglement-based experiment to explain this

Entanglement and Non-locality

Two party setting to explain this



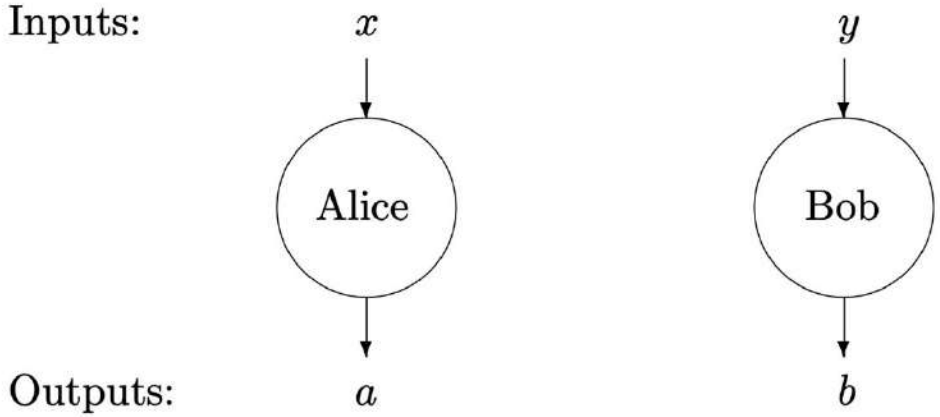
Alice receives input *x* and Bob receives input y, and they produce outputs a and b, respectively, that have to be correlated in a certain way (which depends on the game). They are not allowed to communicate.

This setting captures all local realist models.

In the quantum model Alice and Bob are allowed to share entangled states, such as EPR-pairs. The goal is to show that entanglement-based strategies can do things that local realist strategies cannot.

CHSH: Clauser-Horne-Shimony-Holt

CHSH game



$$a \oplus b = x \wedge y,$$

('$\wedge$' is logical AND; '$\oplus$' is parity, i.e. addition mod 2)

$$\begin{aligned} a_0 \oplus b_0 &= 0, \\ a_0 \oplus b_1 &= 0, \\ a_1 \oplus b_0 &= 0, \\ a_1 \oplus b_1 &= 1. \end{aligned}$$

It's impossible to satisfy all four equations simultaneously summing them modulo 2 yields 0 = 1

a_0, a_1 be the outputs Bob give on inputs $x = 0$ and $x = 1$

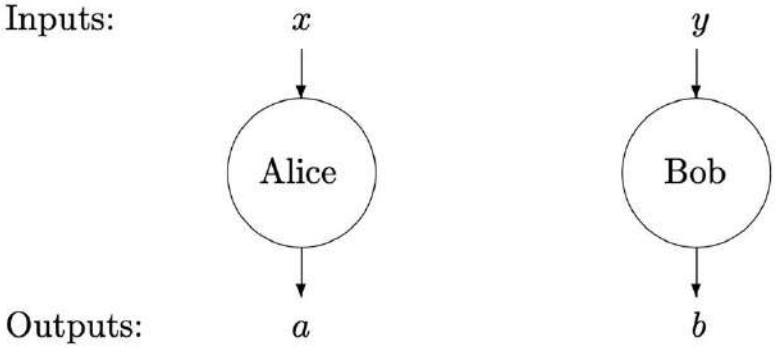
b_0, b_1 be the outputs Bob give on inputs $y = 0$ and $y = 1$

Probabilistically, you can have a success of ¾ times.

CHSH: Clauser-Horne-Shimony-Holt

Quantum strategy for CHSH game

$$a \oplus b = x \wedge y,$$



$$\begin{aligned} a_0 \oplus b_0 &= 0, \\ a_0 \oplus b_1 &= 0, \\ a_1 \oplus b_0 &= 0, \\ a_1 \oplus b_1 &= 1. \end{aligned}$$

Alice and Bob are supplied with a shared 2-qubit system initialized to the entangled state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Recall the unitary operation that rotates the qubit by angle θ

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

If x= 0 then Alice applies R(−π/16) to her qubit; and if x= 1 she applies R(3π/16). Then Alice measures her qubit in the computational basis and outputs the resulting bit a. Bob's procedure is the same, depending on his input bit y. It is straightforward to calculate that if Alice rotates by θ_A and Bob rotates by θ_B, the state becomes

$$\frac{1}{\sqrt{2}}(\cos(\theta_A+\theta_B)(|00\rangle - |11\rangle) + \sin(\theta_A+\theta_B)(|01\rangle + |10\rangle))$$

After the measurements, the probability that

$$a \oplus b = 0 \text{ is } \cos(\theta_A + \theta_B)^2$$

if $x \wedge y = 0$

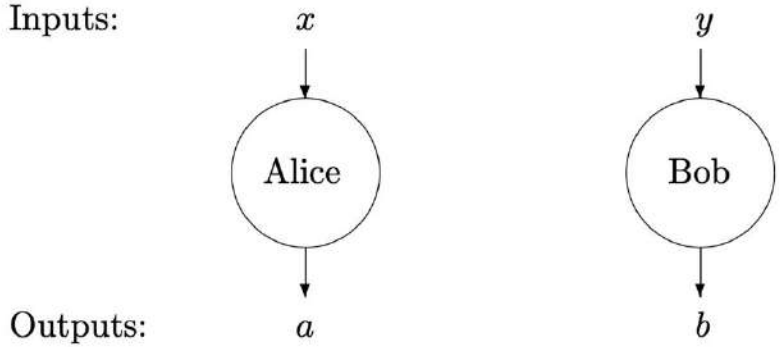
then $\theta_A + \theta_B = \pm\pi/8$, while if $x \wedge y = 1$ then $\theta_A + \theta_B = 3\pi/8$.

Hence the condition $a \oplus b = x \wedge y,$ is satisfied

with probability $\cos(\pi/8)^2$ for all four input possibilities

P = 0.85 is higher than what can be achieved classically

CHSH in equality



a_0, a_1 be the outputs Bob give on inputs $x = 0$ and $x = 1$

b_0, b_1 be the outputs Bob give on inputs $y = 0$ and $y = 1$

Suppose that the observables a_0, a_1, b_0, b_1 take values in 0 *or* 1

We will define

$$\boldsymbol{a} = (-1)^{a_0} , \qquad \boldsymbol{a}' = (-1)^{a_1} ,$$
$$\boldsymbol{b} = (-1)^{b_0} , \qquad \boldsymbol{b}' = (-1)^{b_1} .$$

If $\boldsymbol{a}, \boldsymbol{a}' = \pm 1$, it follows that either $\boldsymbol{a}+\boldsymbol{a}' = 0$, in which case $\boldsymbol{a}-\boldsymbol{a}' = \pm 2$, or else $\boldsymbol{a} - \boldsymbol{a}' = 0$, in which case $\boldsymbol{a} + \boldsymbol{a}' = \pm 2$; therefore

$$\boldsymbol{C} \equiv (\boldsymbol{a} + \boldsymbol{a}')\boldsymbol{b} + (\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{b}' = \pm 2 .$$

$$|\langle \boldsymbol{C} \rangle| \leq \langle |\boldsymbol{C}| \rangle = 2,$$

so that

$$|\langle \boldsymbol{ab} \rangle + \langle \boldsymbol{a'b} \rangle + \langle \boldsymbol{ab'} \rangle - \langle \boldsymbol{a'b'} \rangle| \leq 2.$$

$$\begin{aligned} a_0 \oplus b_0 &= 0, \\ a_0 \oplus b_1 &= 0, \\ a_1 \oplus b_0 &= 0, \\ a_1 \oplus b_1 &= 1. \end{aligned}$$

Suppose that Charlie generates the input bits at random. Then there is a very simple strategy that enables Alice and Bob to win the game three times out of four: they always choose the output a= b= 0 so that they lose only if the input is x= y= 1.

if we denote by p_{xy} the probability that above equation satisfied when the input bits are (x,y), then

$$\begin{aligned} \langle \boldsymbol{ab} \rangle &= 2p_{00} - 1 , \\ \langle \boldsymbol{ab'} \rangle &= 2p_{01} - 1 , \\ \langle \boldsymbol{a'b} \rangle &= 2p_{10} - 1 , \\ \langle \boldsymbol{a'b'} \rangle &= 1 - 2p_{11} ; \end{aligned}$$

the value of **ab** is +1 when Alice and Bob win and −1 when they lose.

$$2\left(p_{00} + p_{01} + p_{10} + p_{11}\right) - 4 \leq 2$$

$$\langle p \rangle \equiv \frac{1}{4}\left(p_{00} + p_{01} + p_{10} + p_{11}\right) \leq \frac{3}{4}$$

CHSH in equality .....

$$\frac{1}{\sqrt{2}}\left(\cos(\theta_A+\theta_B)(|00\rangle-|11\rangle)+\sin(\theta_A+\theta_B)(|01\rangle+|10\rangle)\right)$$

After the measurements, the probability that

$$a \oplus b = 0 \text{ is } \cos(\theta_A+\theta_B)^2$$

if $x \wedge y = 0$

then $\theta_A+\theta_B = \pm\pi/8$, while if $x \wedge y = 1$ then $\theta_A+\theta_B = 3\pi/8$.

Hence the condition $a \oplus b = x \wedge y$, is satisfied

with probability $\cos(\pi/8)^2$ for all four input possibilities

P = 0.85 is higher than what can be achieved classically

If

$$\langle p\rangle \equiv \frac{1}{4}\left(p_{00}+p_{01}+p_{10}+p_{11}\right) \quad = 0.853$$

We will get

$$2\left(p_{00}+p_{01}+p_{10}+p_{11}\right)-4 \leq 2\sqrt{2}$$

$$\langle ab\rangle + \langle ab'\rangle + \langle a'b\rangle - \langle a'b'\rangle \leq 2\sqrt{2}$$

Upper bound – Cirel'son bound for a quantum state

For classical, we only get 2

How do we test if the given state is entangled or not

Lets take two photons entangled in polarization degree of freedom

Valid for bipartite system.

$$S = \left| E(a,b) - E(a,b') + E(a',b) + E(a',b') \right|$$

If $S > 2$ state is Entangled

$S_{max} = 2\sqrt{2}$ $\quad S < 2$ – classical

what are $E(\alpha, \beta)$?

$$E(\alpha,\beta) = \frac{N(\alpha,\beta) + N(\alpha_\perp, \beta_\perp) - N(\alpha_\perp, \beta) - N(\alpha, \beta_\perp)}{N(\alpha,\beta) + N(\alpha_\perp, \beta_\perp) + N(\alpha_\perp, \beta) + N(\alpha, \beta_\perp)}$$

$\alpha, \beta \rightarrow$ two polarizers placed infront of detectors.
'$\perp$' means angle perpendicular to other angle.

$N(\alpha, \beta) \rightarrow$ coincidence rate when two polarization is set at angle 'α' and 'β'

lets consider changing the basis by rotating the state.

$$\text{rotation matrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$\begin{cases} |V\rangle = \cos\theta\,|V'\rangle - \sin\theta\,|H'\rangle \\ |H\rangle = \sin\theta\,|V'\rangle + \cos\theta\,|H'\rangle \end{cases}$$

Now we will replace $|V\rangle$ and $|H\rangle$ in.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|V\rangle|V\rangle + |H\rangle|H\rangle\right)$$ with new basis states.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big((\cos\theta|V'\rangle - \sin\theta|H'\rangle)(\cos\theta|V'\rangle - \sin\theta|H'\rangle) + (\sin\theta|V'\rangle + \cos\theta|H'\rangle)(\sin\theta|V'\rangle + \cos\theta|H'\rangle)\Big)$$

$$\Rightarrow \frac{1}{\sqrt{2}}\Big[(\cos^2\theta + \sin^2\theta)|V'\rangle|V'\rangle + (\cos^2\theta + \sin^2\theta)|H'\rangle|H'\rangle\Big]$$

$$= \frac{1}{\sqrt{2}}\left(|V'\rangle|V'\rangle + |H'\rangle|H'\rangle\right)$$

This allows us to use any two angles which are perpendicular to each other to represent the entanglement in state.

Using this fact:

$$E(\alpha,\beta) = P_{VV}(\alpha,\beta) + P_{HH}(\alpha,\beta) - P_{VH}(\alpha,\beta) - P_{HV}(\alpha,\beta)$$

↓ probabilities of receiving in respective polarizations

$$P_{VV} = \frac{N(\alpha,\beta)}{N(\alpha,\beta) + N(\alpha_\perp,\beta_\perp) + N(\alpha_\perp,\beta) + N(\alpha,\beta_\perp)}$$

$$P_{HH} = \frac{N(\alpha_\perp,\beta_\perp)}{N(\alpha,\beta) + N(\alpha_\perp,\beta_\perp) + N(\alpha_\perp,\beta) + N(\alpha,\beta_\perp)}$$

$$P_{HV} = \frac{N(\alpha_\perp,\beta)}{N(\alpha,\beta) + N(\alpha_\perp,\beta_\perp) + N(\alpha_\perp,\beta) + N(\alpha,\beta_\perp)}$$

$$P_{VH} = \frac{N(\alpha,\beta_\perp)}{N(\alpha,\beta) + N(\alpha_\perp,\beta_\perp) + N(\alpha_\perp,\beta) + N(\alpha,\beta_\perp)}$$

$$P_{VV} = \left| \langle V|\langle V| \, \Pi(a,b) \left(\frac{1}{\sqrt{2}} (|V\rangle|V\rangle + |H\rangle|H\rangle) \right) \right|^2$$

$$P_{HH} = \left| \langle H|\langle H| \, \Pi(a,b) \left(\frac{1}{\sqrt{2}} (|V\rangle|V\rangle + |H\rangle|H\rangle) \right) \right|^2$$

$$P_{HV} = \left| \langle H|\langle V| \quad \text{--''--} \right|^2$$

$$P_{VH} = \left| \langle V|\langle H| \quad \text{--''--} \right|^2 \qquad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\Pi(a,b) = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix} \otimes \begin{pmatrix} \cos b & -\sin b \\ \sin b & \cos b \end{pmatrix}$$

(7) →

$$\Pi(a,b) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos a \cos b + \sin a \sin b \\ \cos a \sin b - \sin a \cos b \\ \sin a \cos b - \cos a \sin b \\ \sin a \sin b + \cos a \cos b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos(a-b) \\ -\sin(a-b) \\ \sin(a-b) \\ \cos(a-b) \end{pmatrix}$$

$$P_{VV} = |\langle V|\langle V|\Pi(a,b)|\psi_0\rangle|^2 = \left\{ (1\,0\,0\,0) \frac{1}{\sqrt{2}} \begin{pmatrix} \cos(a-b) \\ -\sin(a-b) \\ \sin(a-b) \\ \cos(a-b) \end{pmatrix} \right\}^2$$

$$= \frac{1}{2} \cos^2(a-b)$$

III 4

$$P_{HH} = \frac{1}{2}\cos^2(a-b)$$

$$P_{HV} = \frac{1}{2}\sin^2(a-b)$$

$$P_{VH} = \frac{1}{2}\sin^2(a-b)$$

$$E(a,b) = \frac{1}{2}\cos^2(a-b) + \frac{1}{2}\cos^2(a-b) - \frac{1}{2}\sin^2(a-b) - \frac{1}{2}\sin^2(a-b)$$

$$= \cos^2(a-b) - \sin^2(a-b)$$

$$E(a,b) = \cos 2(a-b)$$

$$S = |\cos 2(a-b) - \cos 2(a-b') + \cos 2(a'-b) + \cos 2(a'-b')|$$

$= 2.82$ ($a = 135$ $a' = 0$ $b = 157.5$ $b' = 22.5$

S = 2.83 for
a = 135, a' =0,
b = 157.5, b'=22.5

Other ways to measure entanglement

Given a classical probability distribution $\{p_i\}$, the Shannon entropy is

$$S = -\sum_i p_i \log p_i$$

Similarly, the von Neumann Entropy for a quantum state ρ is

$$S(\rho) = -\operatorname{tr} \rho \log \rho$$

- $S(\rho) \geq 0$ and $S(\rho) = 0$ if and only if $S(\rho)$ is a pure state.
- In a N dimensional Hilbert Space, the entropy takes its maximum value $S = \log N$

Entanglement Entropy for a bipartite system will be :

$$E(\rho_{AB}) = S(\rho_A) = S(\operatorname{tr}_B \rho) = S(\operatorname{tr}_A \rho) = S(\rho_B)$$

Concurrence
Negativity

Are other measures

DiVincenzo Criteria - Desired condition

1. A scalable physical system of well-characterized qubits;

2. the ability to initialize the state of the qubits to a simple fiducial state;

3. long (relative) decoherence times, much longer than the gate-operation time;

4. a universal set of quantum gates; and

5. a qubit-specific measurement capability.

Two additional criteria, which are necessary conditions for quantum computer networkability are

6. the ability to interconvert stationary and flying qubits and

7. the ability to faithfully transmit flying qubits between specified locations.

DiVincenzo Criteria - Table of QC approaches

QC Approach	The DiVincenzo Criteria							
	Quantum Computation						QC Networkability	
	#1	#2	#3	#4	#5		#6	#7
NMR								
Trapped Ion								
Neutral Atom								
Cavity QED								
Optical								
Solid State								
Superconducting								
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.							

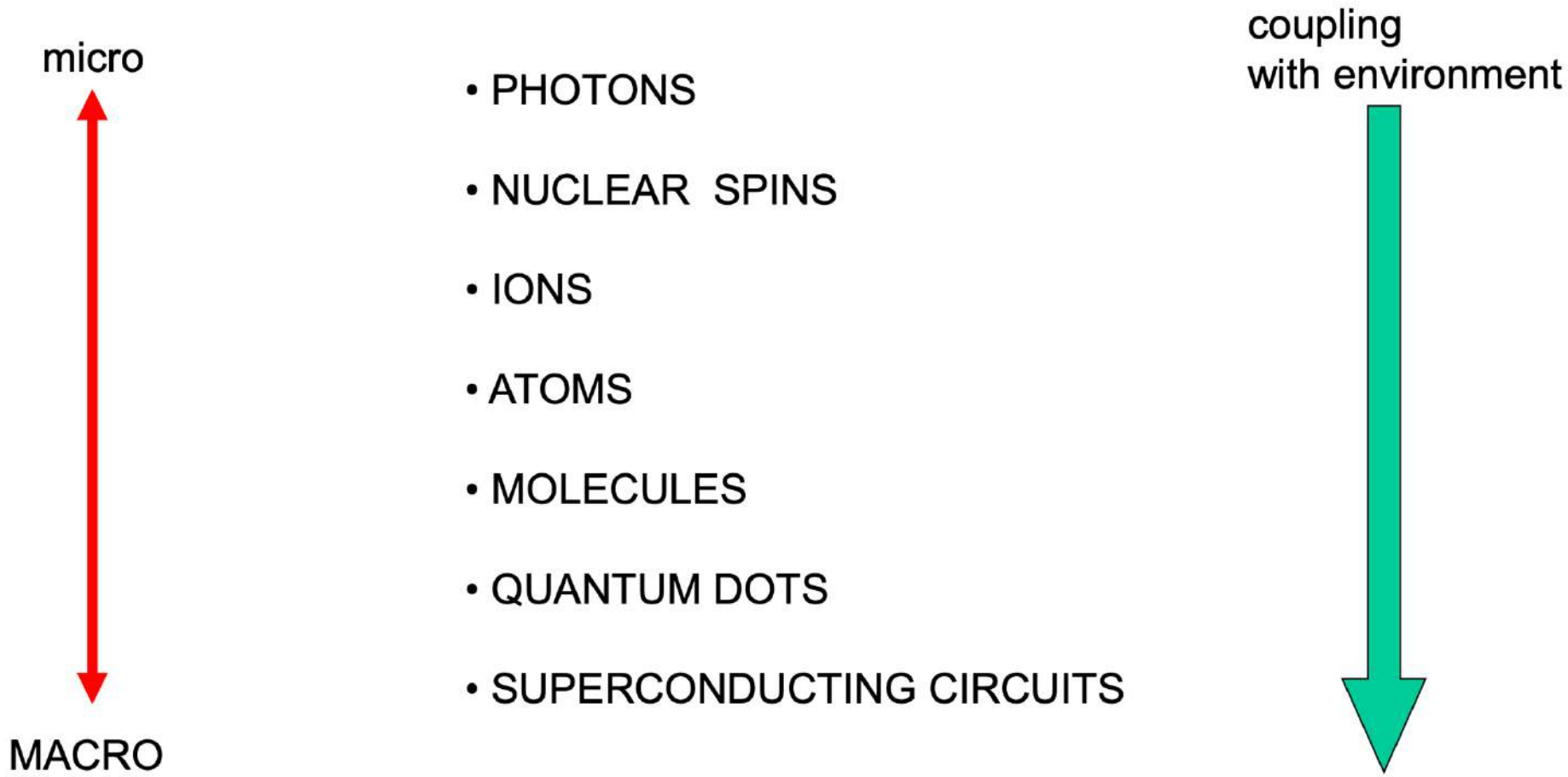
This is a table from 2004

What has changed now to green is marked in red circle

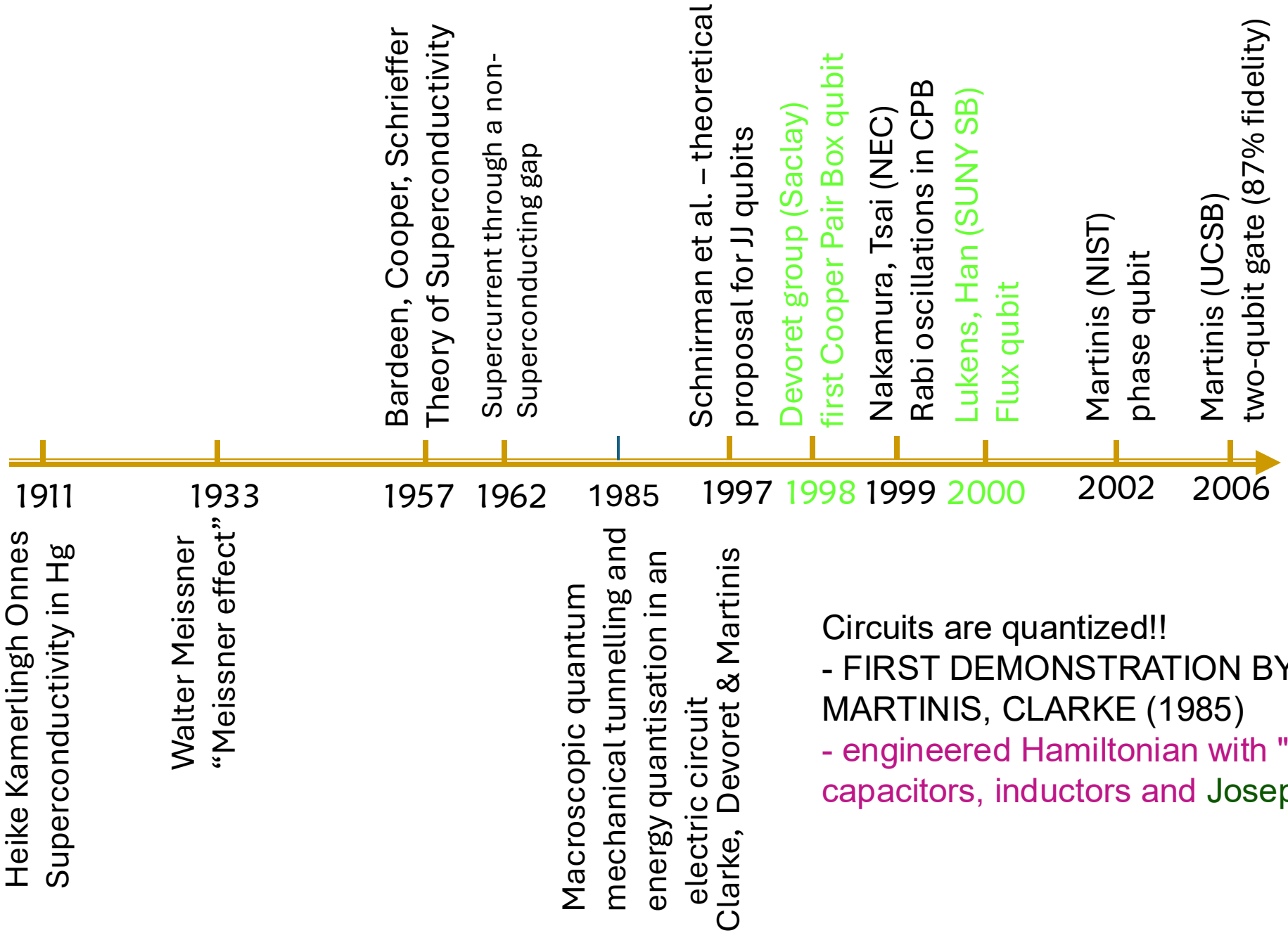
Legend:
= a potentially viable approach has achieved sufficient proof of principle
= a potentially viable approach has been proposed, but there has not been sufficient proof of principle
= no viable approach is known

#1. A scalable physical system with well-characterized qubits.
#2. The ability to initialize the state of the qubits to a simple fiducial state.
#3. Long (relative) decoherence times, much longer than the gate-operation time.
#4. A universal set of quantum gates.
#5. A qubit-specific measurement capability.
#6. The ability to interconvert stationary and flying qubits.
#7. The ability to faithfully transmit flying qubits between specified locations.

Quantum computing platform: from varying size to coupling with environment



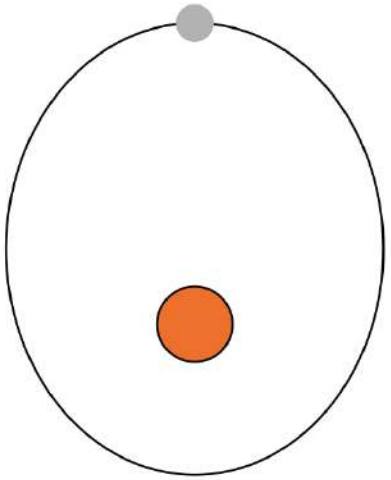
Superconducting qubits – a timeline



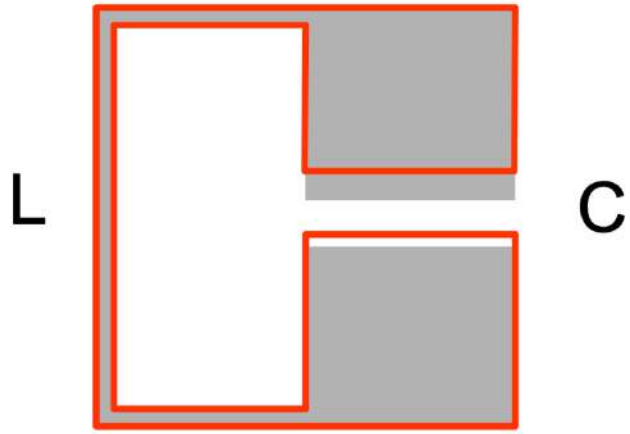
Circuits are quantized!!
- FIRST DEMONSTRATION BY DEVORET, MARTINIS, CLARKE (1985)
- engineered Hamiltonian with "LEGO" blocks: capacitors, inductors and Josephson junctions

Superconducting circuit (building an artificial atoms)

Rydberg atom



Superconducting
LC oscillator



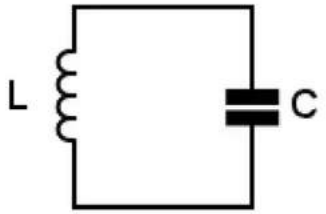
velocity of electron → voltage (charge) across capacitor
force on electron → current (flux) through inductor

Superconducting circuit (building an artificial atoms)

Quantum LC oscillator

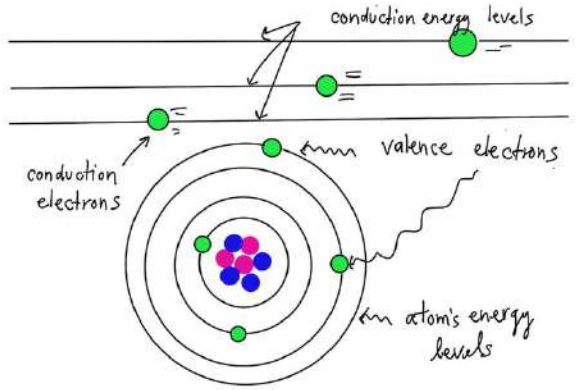
$$\hat{H} = \frac{\hat{\Phi}^2}{2L} + \frac{\hat{Q}^2}{2C}$$

$$\hat{H} = \frac{1}{2}\hbar\omega\left\{\hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger\right\}$$



$$\hat{a}^\dagger = -i\frac{1}{\sqrt{2C\hbar\omega}}\hat{Q} + \frac{1}{\sqrt{2L\hbar\omega}}\hat{\Phi}$$

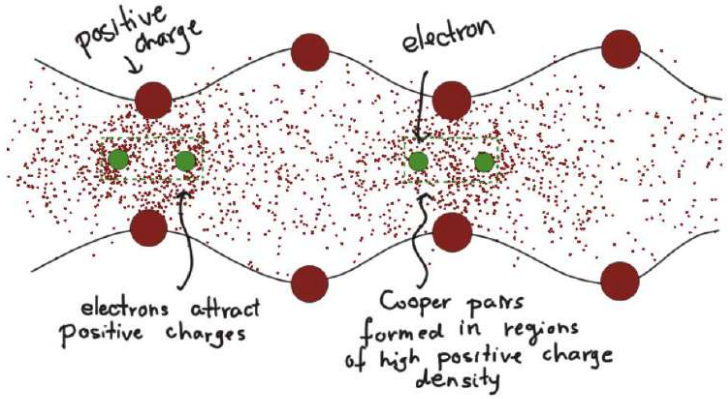
$$\hat{a} = i\frac{1}{\sqrt{2C\hbar\omega}}\hat{Q} + \frac{1}{\sqrt{2L\hbar\omega}}\hat{\Phi}$$

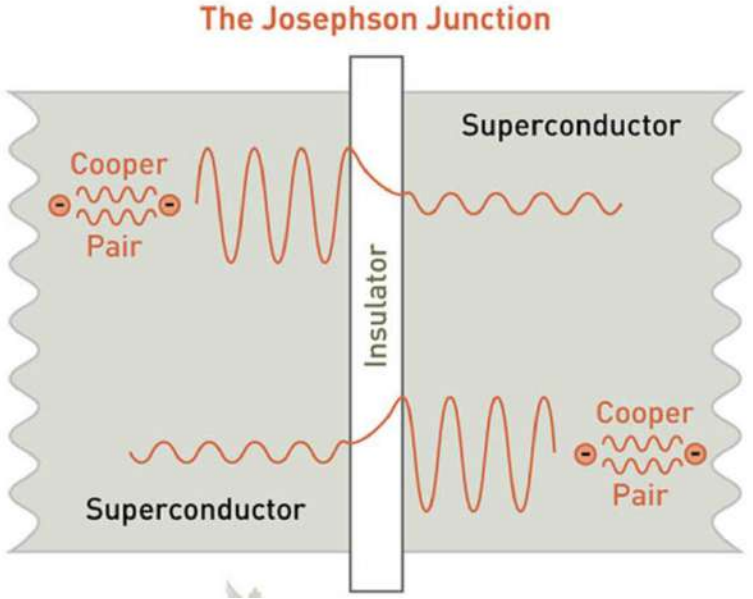


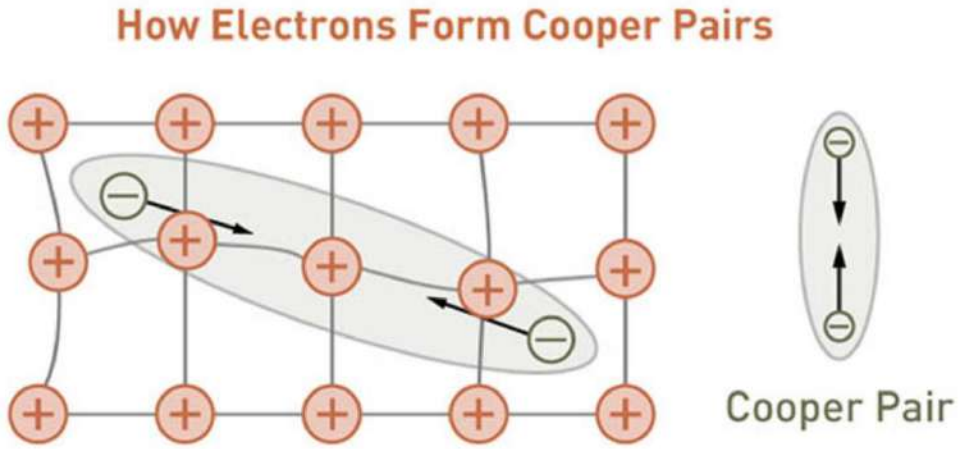
Valence and conduction energy levels

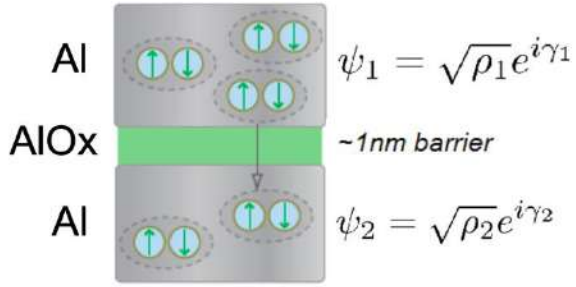
The first quantum circuit we will introduce is the LC oscillator, as it is the simplest example of a quantum integrated circuit. Studying the simplest case will help us understand the circuits of the superconducting qubits and their Hamiltonians. LC circuits consist of an inductor L connected to a capacitor C. All of the wires connecting the elements must be superconducting for the circuit to be quantum, this way the energy levels in the superconducting gap will be discrete. The LC circuit obeys the equations of motion of the linear harmonic oscillator. The flux in the inductor Φ is analogous to the position coordinate and the charge Q on the capacitor is analogous to the conjugate momentum. The $\hat{\Phi}$ and $\hat{Q}$ variables are conjugate quantum operators, which do not commute $[\hat{\Phi}, \hat{Q}] = i\hbar$ The inductance L of the system can be thought as the 'mass' and the inverse of de capacitance 1/C as the 'spring constant'. Knowing the LC oscillator is analogous to the harmonic oscillator we can write the Hamiltonian in terms of the raising and lowering operators $\omega = 1/\sqrt{LC}$ being the resonance frequency of the circuit

Superconducting circuit (building an artificial atoms) – Cooper pairs and Josephson Junction









$\psi_1 = \sqrt{\rho_1} e^{i\gamma_1}$

$\psi_2 = \sqrt{\rho_2} e^{i\gamma_2}$

$\rho_{1(2)}$ density of electrons on either side of the SC

$\gamma_{1(2)}$ phase of the SC

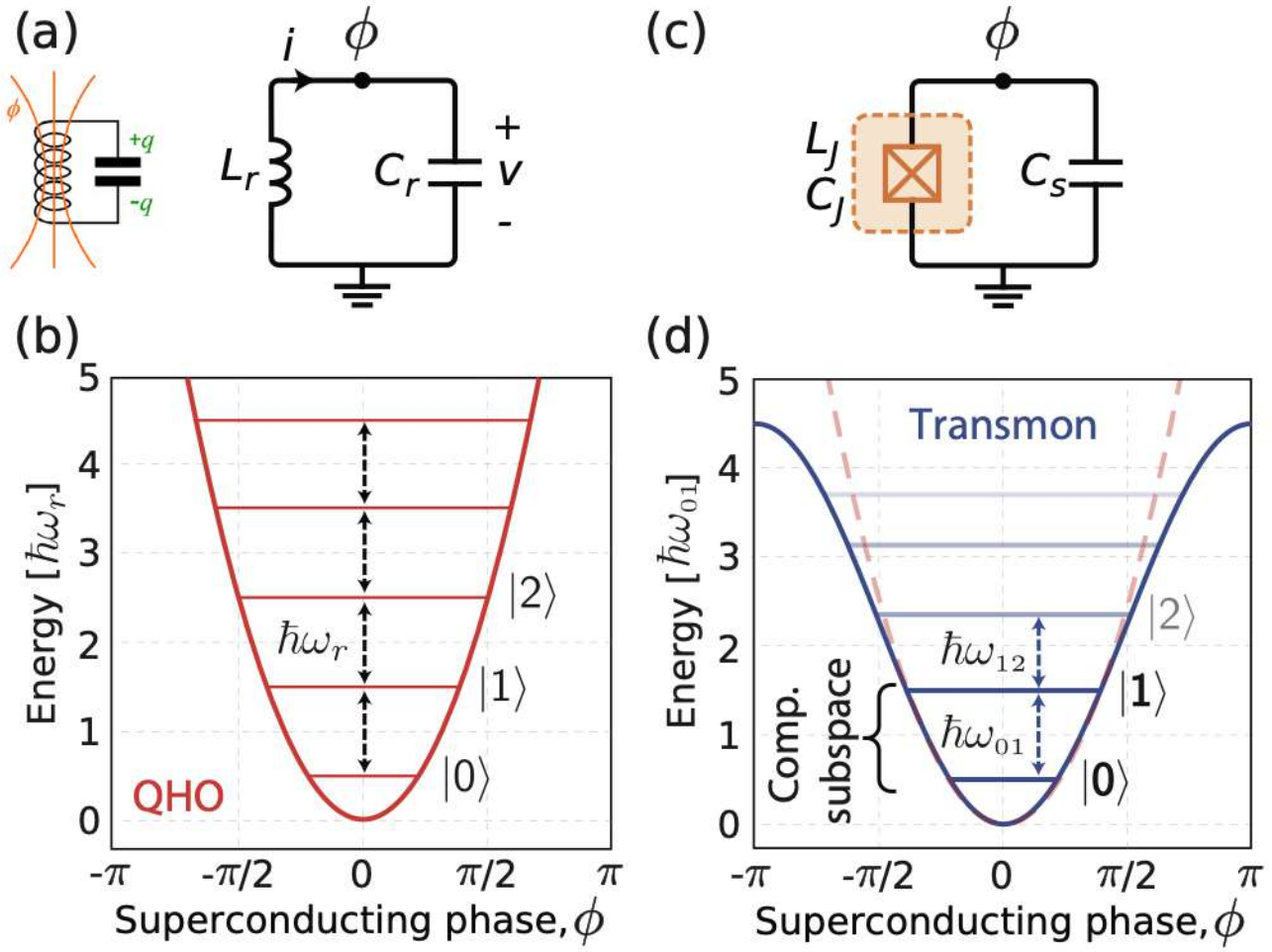
Equations of motion from a toy model

$$i\hbar \frac{\partial}{\partial t} \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} = \begin{pmatrix} 2eV & K \\ K & 0 \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix}$$

K – tunneling energy

2eV – energy across the junction

Superconducting circuit (building an artificial atoms)



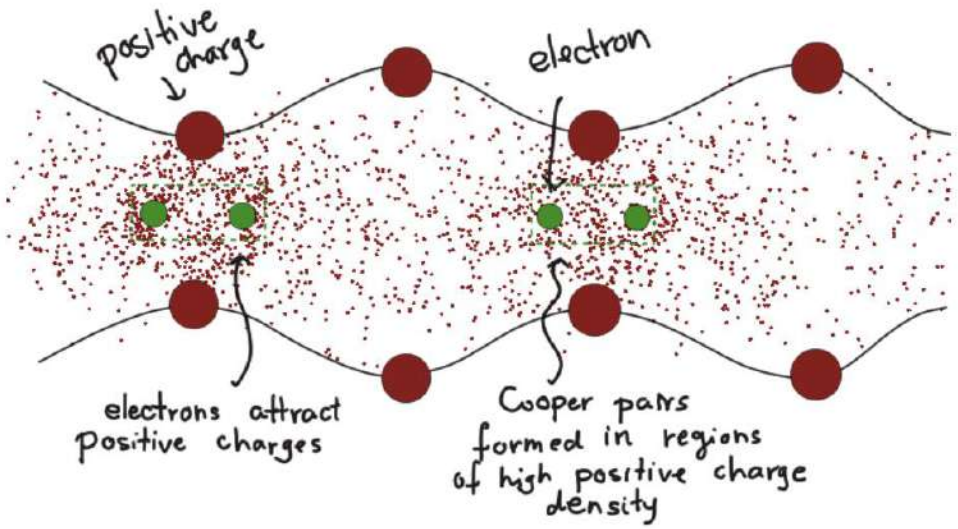
(a) Circuit for a parallel LC-oscillator (quantum harmonic oscillator, QHO), with inductance L in parallel With capacitance, C. The superconducting phase on the island is denoted φ, referencing ground as zero.

(b) Energy potential for the QHO, where energy levels are equidistantly spaced ωr apart.

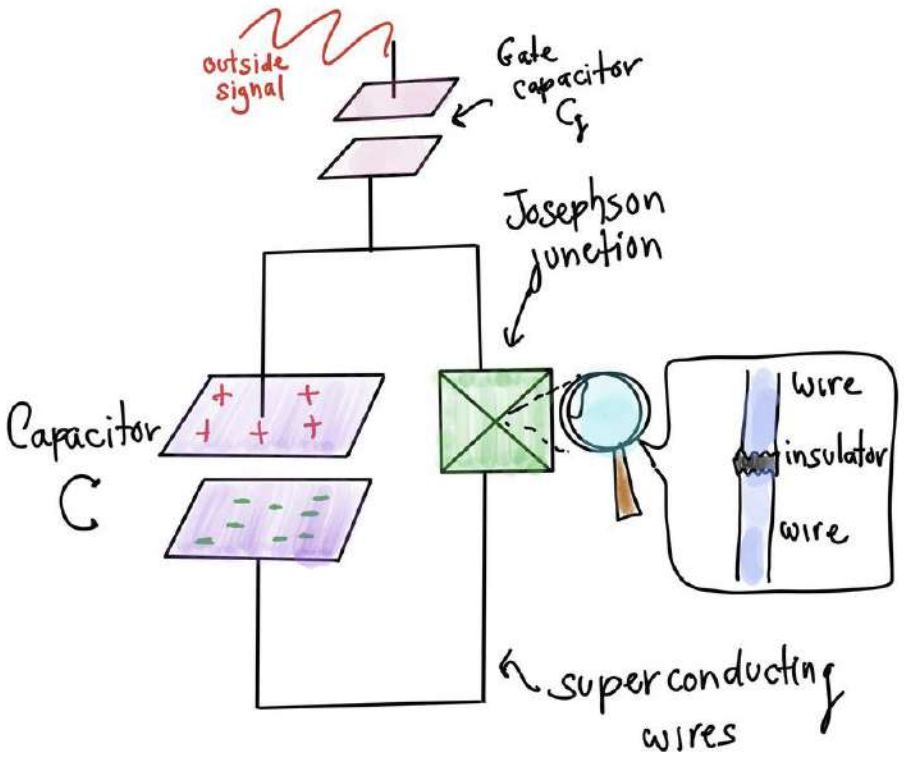
(c) Josephson qubit circuit, where the nonlinear inductance LJ (represented with the Josephson -subcircuit in the dashed orange box) is shunted by a capacitance, Cs.

(d) The Josephson inductance reshapes the quadratic energy potential (dashed red) into sinusoidal (solid blue), which yields non-equidistant energy levels. This allows us to isolate the two lowest energy levels |0⟩and |1⟩, forming a Computational subspace with an energy separation ω01, which is different than ω12.

Superconducting circuit

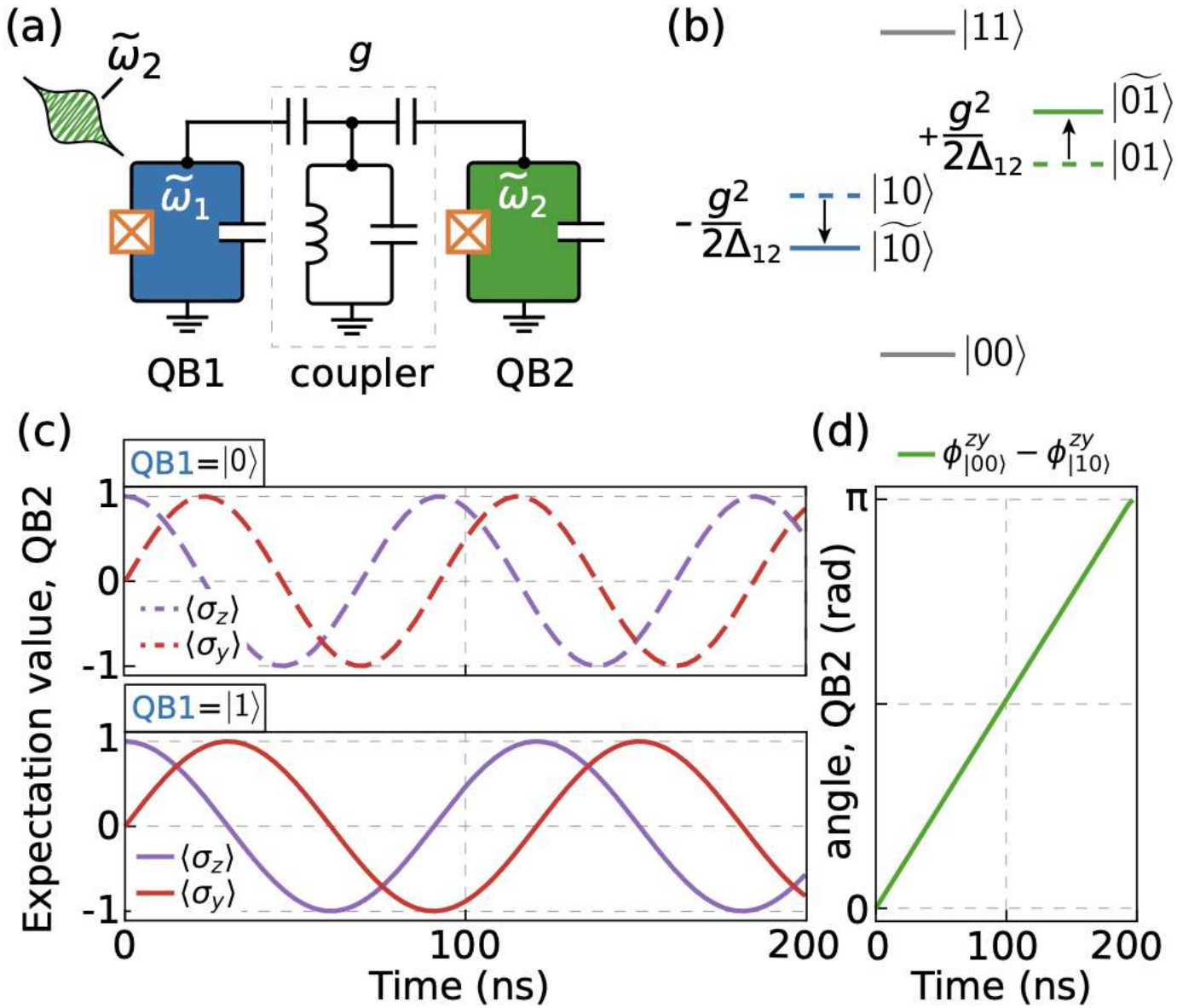


Cooper pairs are formed by alternating regions of high and low density of positive charge (phonons) represented by the density of red dots.

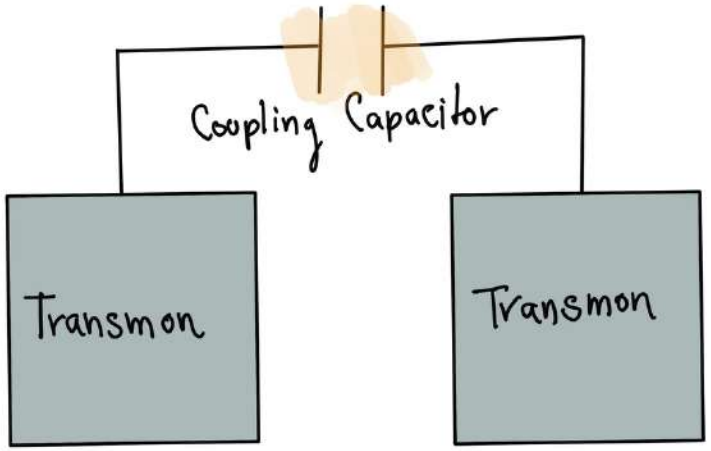


Circuit with a Josephson junction and a gate capacitor

Example of two qubit operaiton

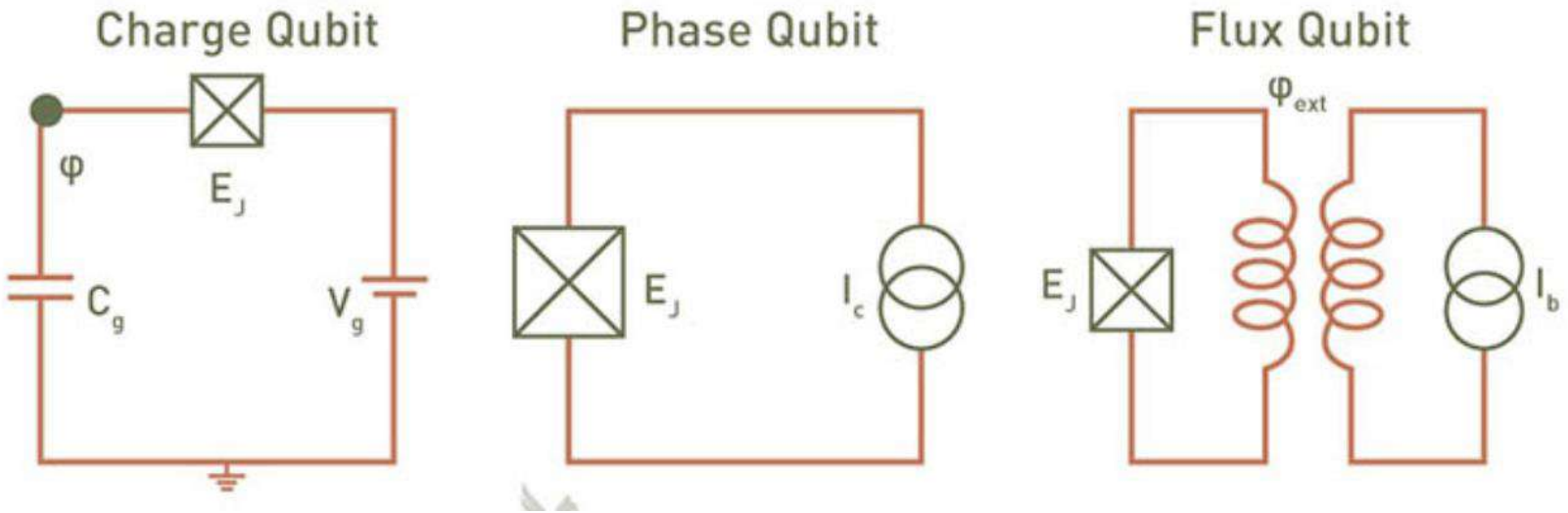


Schematic circuit diagram of two fixed frequency transmons coupled through a resonator yielding an overall coupling coefficient g. Qubit 1 driven at the frequency of qubit 2 leads to the CR gate.

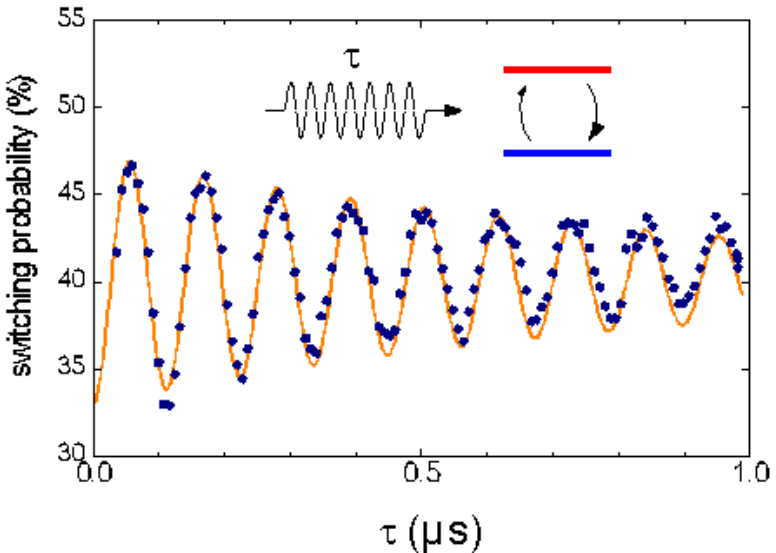


Two transmons connected through a coupling capacitor

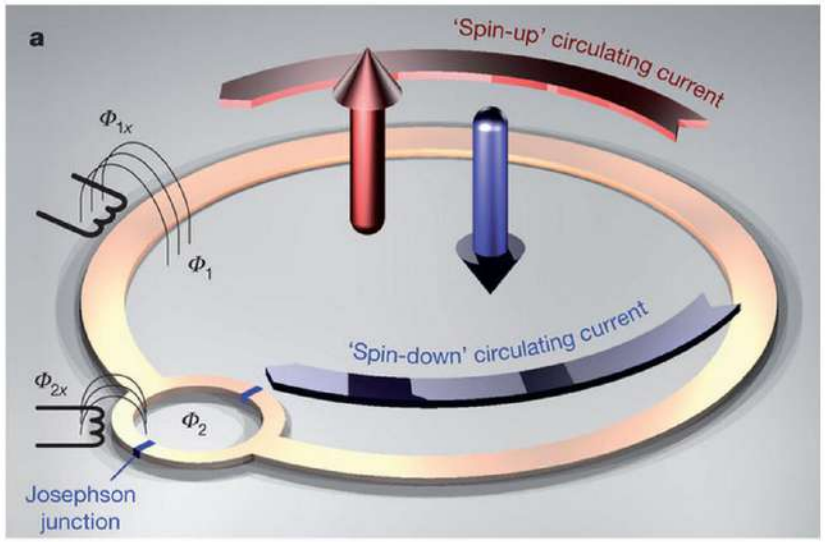
Superconducting circuit (building an artificial atoms)

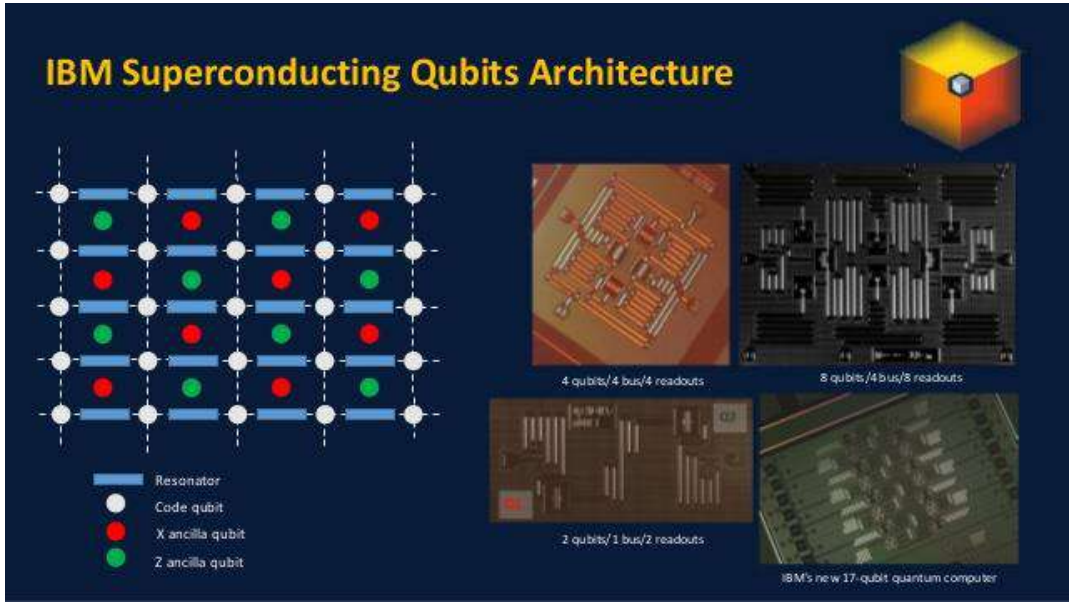


decoherence



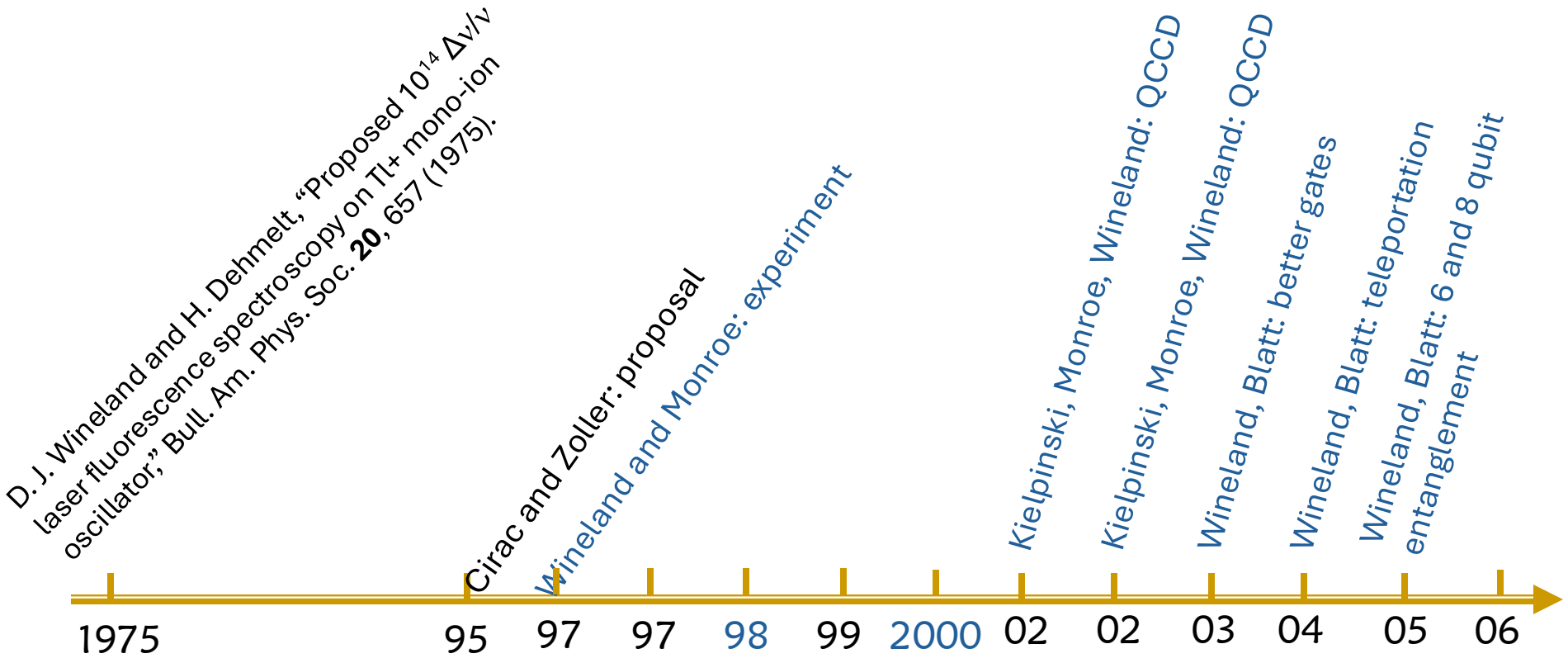
Superconducting circuit (building an artificial atoms)





Trapped ion qubits – timeline

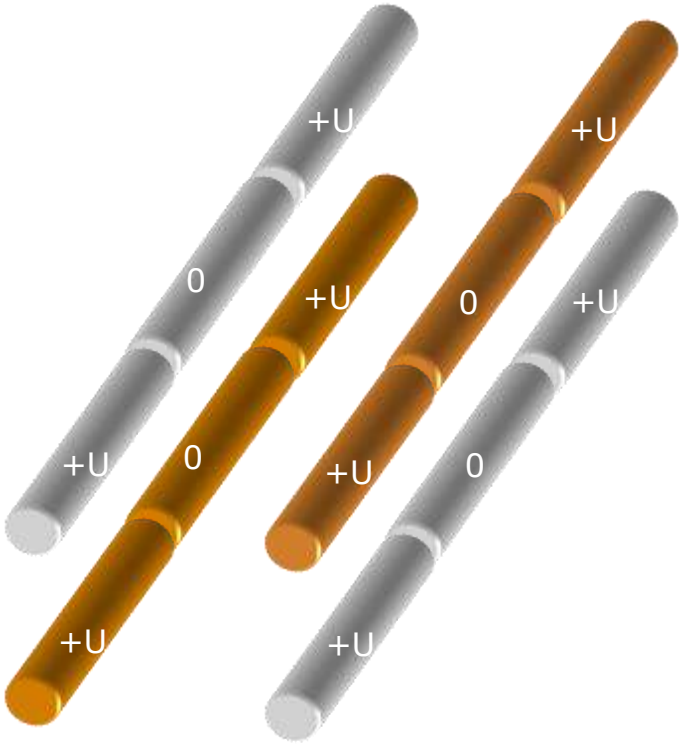
QCCD- quantum charged couple devices

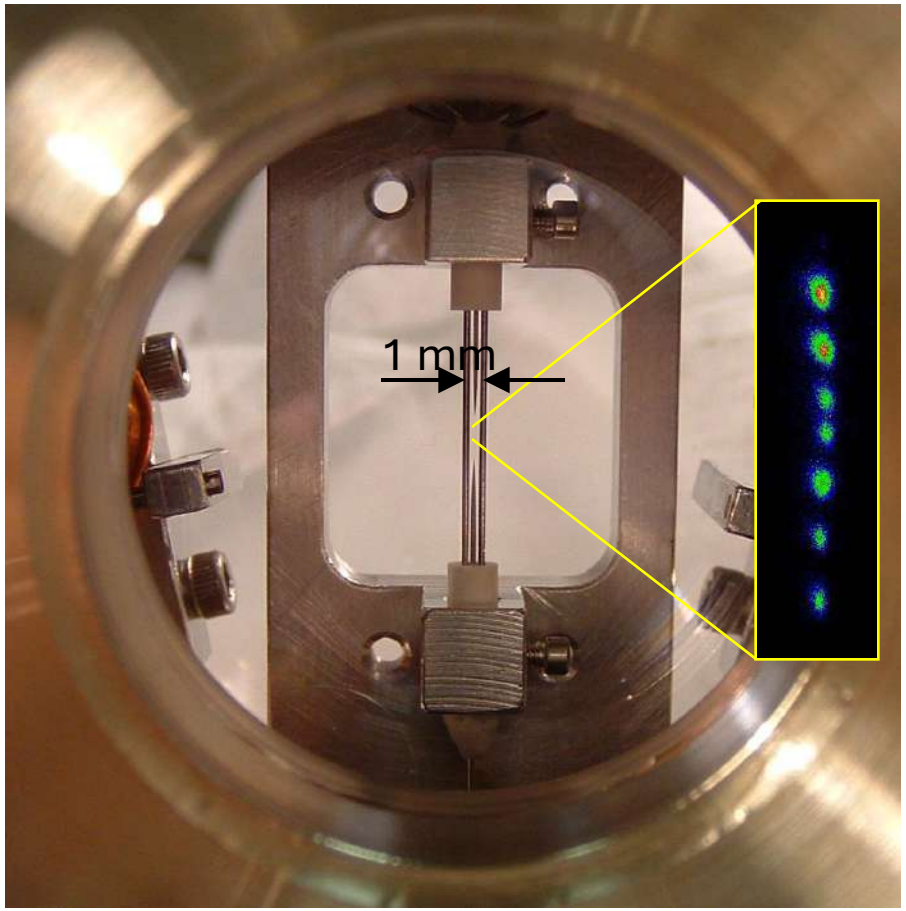


1989 (Paul and Dehmelt) – Development of ion trap technique

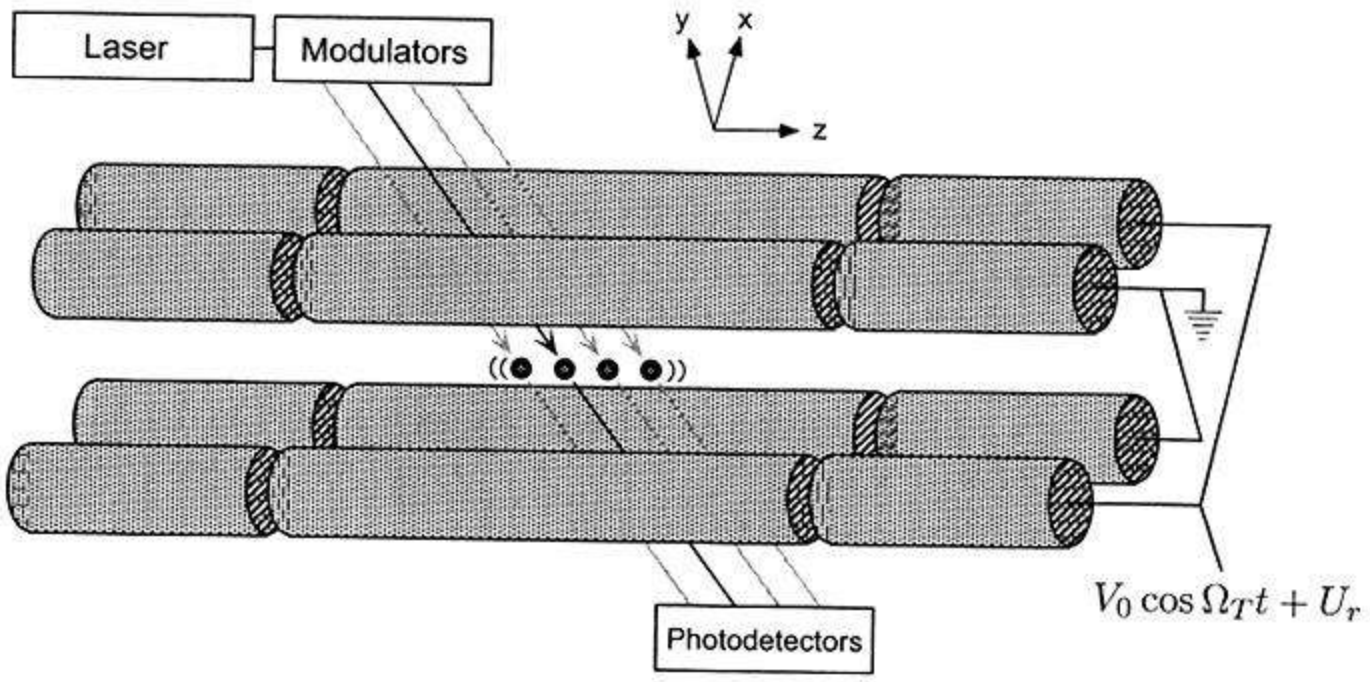
2012 (Wineland) – Development of ion trap technique and using it for quantum computing

Trapped ion qubits





Ion trap systems for qubits



Complex qubit organization: each row is a separate image of 53 trapped ion qubits, with each qubit fluorescing (state 1) or dark (state 0) upon measurement.

Qubit representation: Hyperfine (nuclear spin) state of an atom and phonons of trapped atoms

Unitary evolution:

Laser pulses manipulate atomic state

Qubits interact via shared phonon state

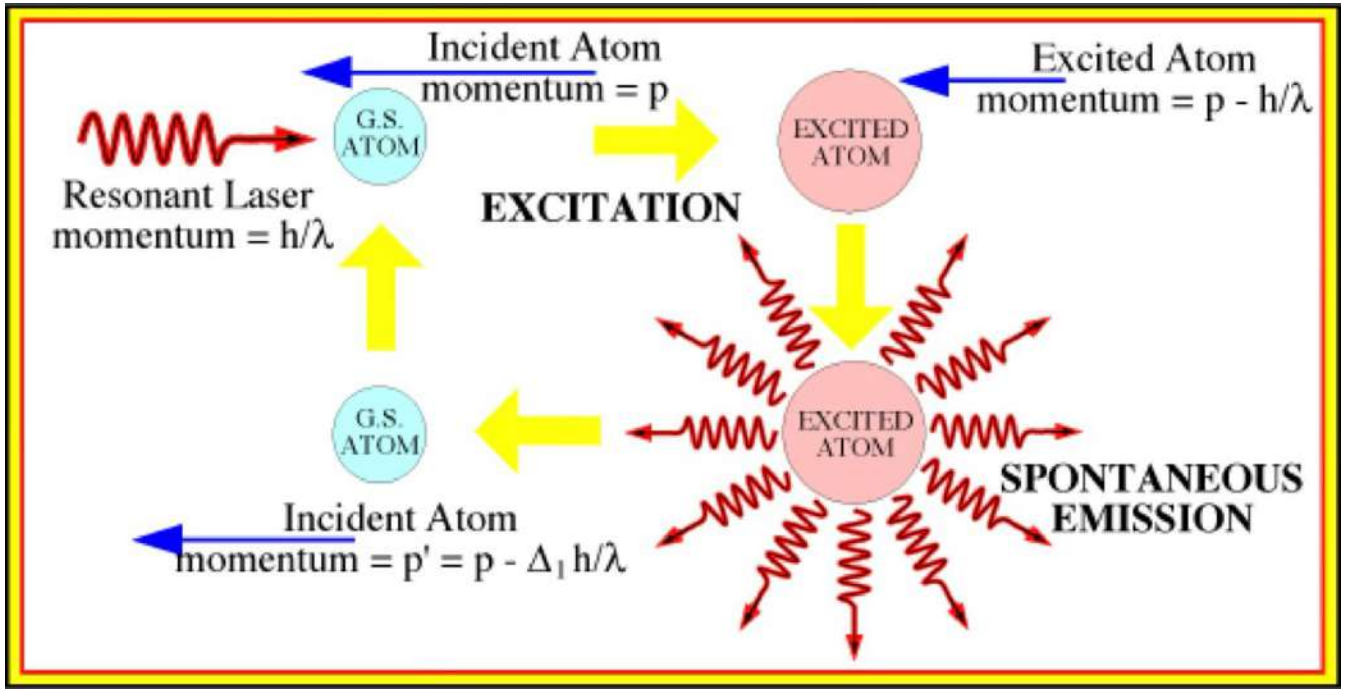
Initial state preparation: Cool the atoms to ground state using optical pumping

Readout: Measure population of hyperfine states

Drawbacks: Phonon lifetimes are short, and ions are difficult to prepare in their ground states.

Cold atoms for qubits

Cooling cycle



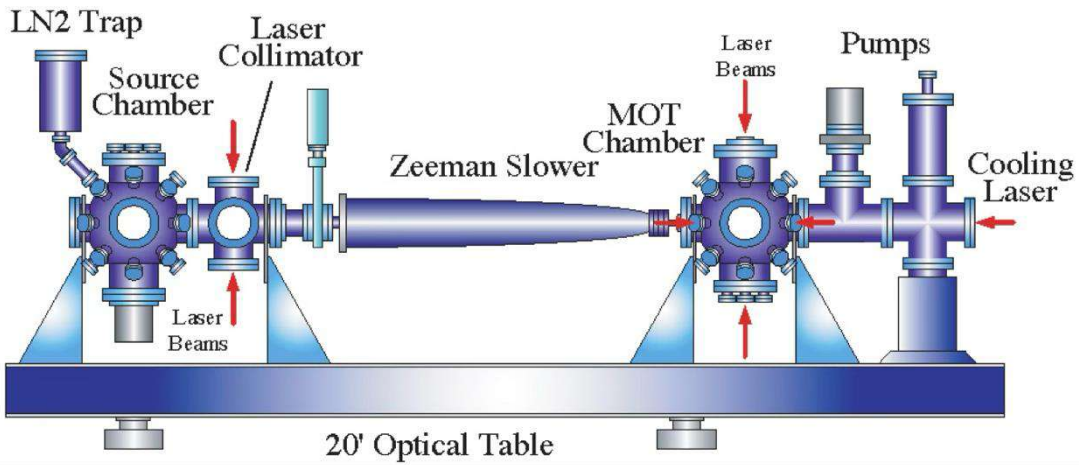
Atoms respond only to a very specific color (frequency) of light

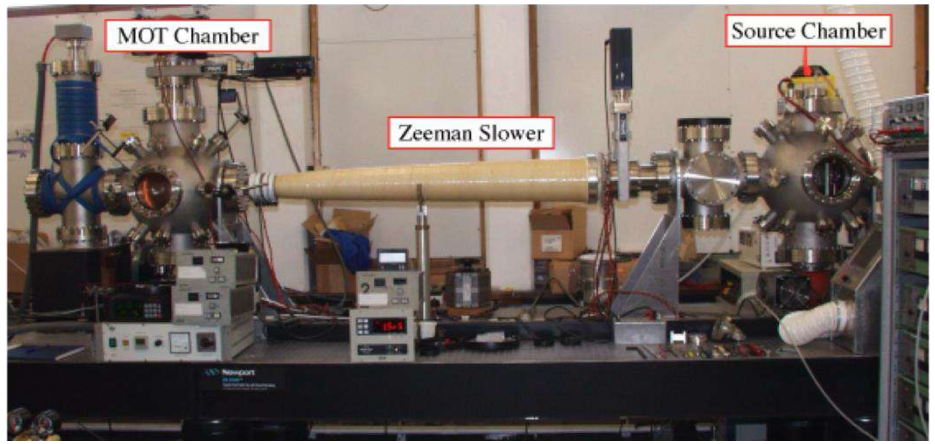
Only a tuned laser can do that

For each specimen of atoms we need to find lasers with frequency that can be absorbed by atom and excite to higher energy level

Can I take sample of atoms from this room and cool them using lasers?

Zeeman slower





What happens when we have atoms going at different speeds?

If the laser was set to slow fast ones, wouldn't it just blast the slow ones in the other direction, and leave them faster and hotter?

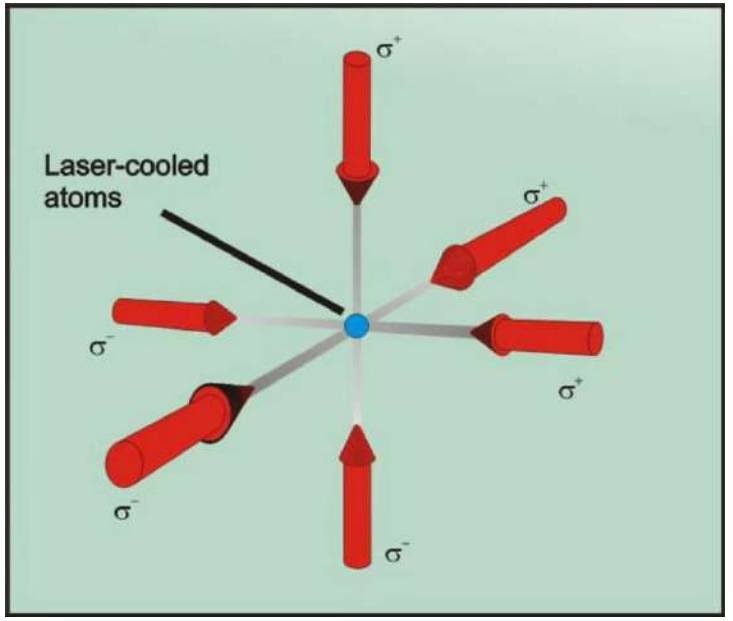
Cold atoms (Doppler effect)

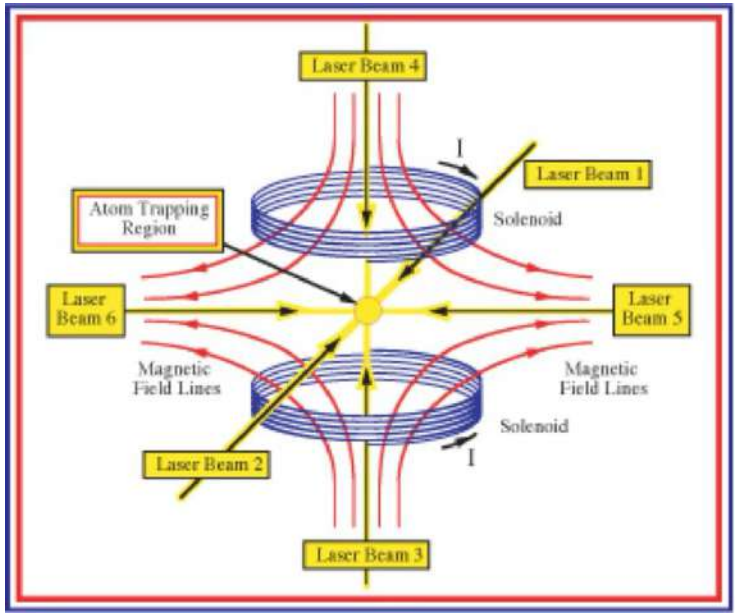
Atom going towards laser light → Blue shift

Atoms going away from laser light → Red shift

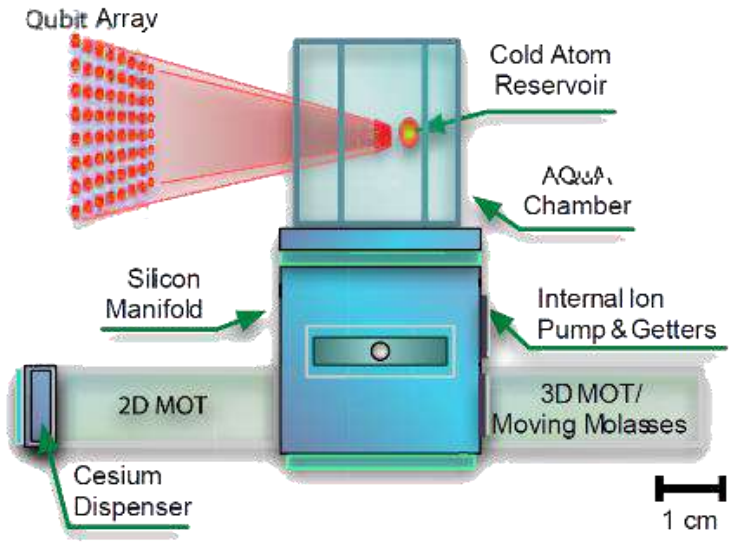
Amount of shift depends on the speed of an atom

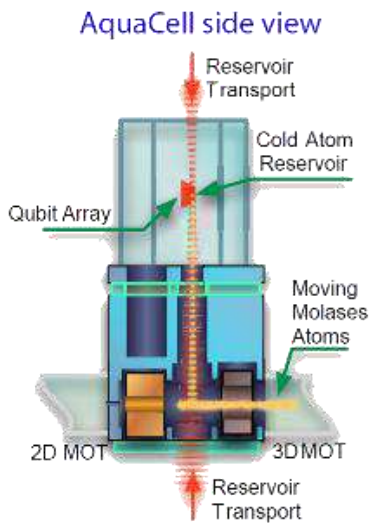
If the atom is moving slowly, or in wrong direction, the Doppler shift will be different and the laser light does not excite the electron, just goes by the atom

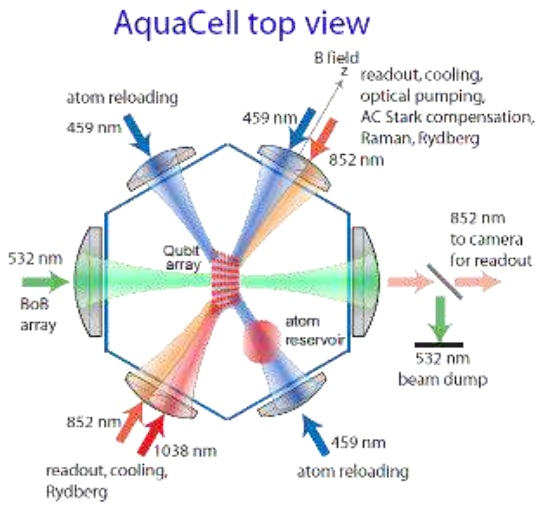




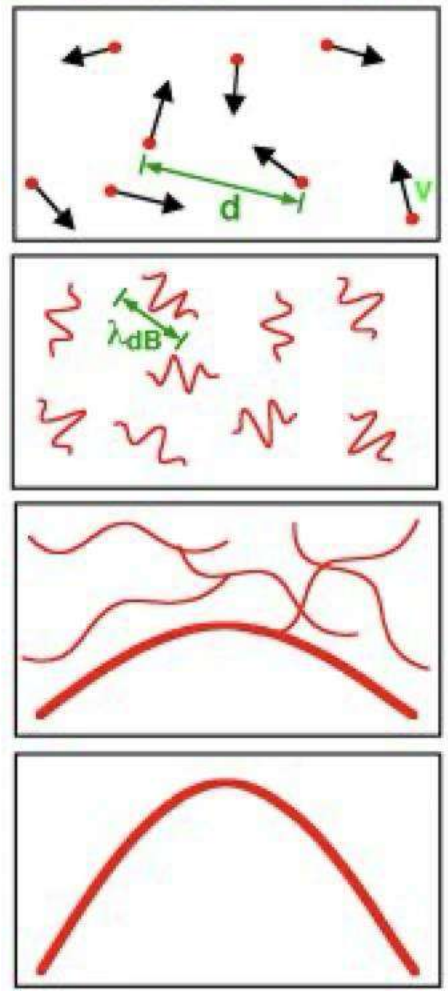
Example of qubit array







What is Bose-Einstein condensation (BEC)?



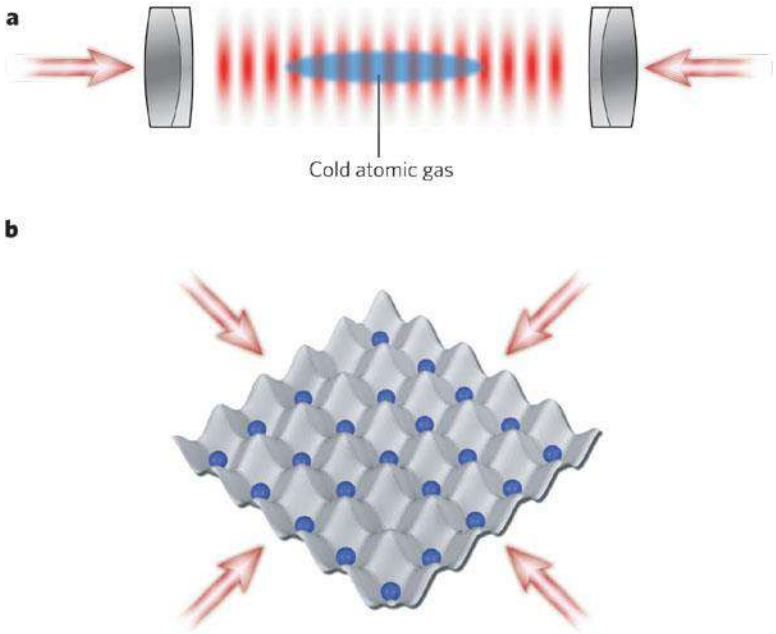
High Temperature T:
thermal velocity v
density d^{-3}
"Billiard balls"

Low Temperature T:
De Broglie wavelength
$\lambda_{dB}=h/mv \propto T^{-1/2}$
"Wave packets"

$T=T_{crit}$: Bose-Einstein Condensation
$\lambda_{dB} = d$
"Matter wave overlap"

T=0: Pure Bose condensate
"Giant matter wave"

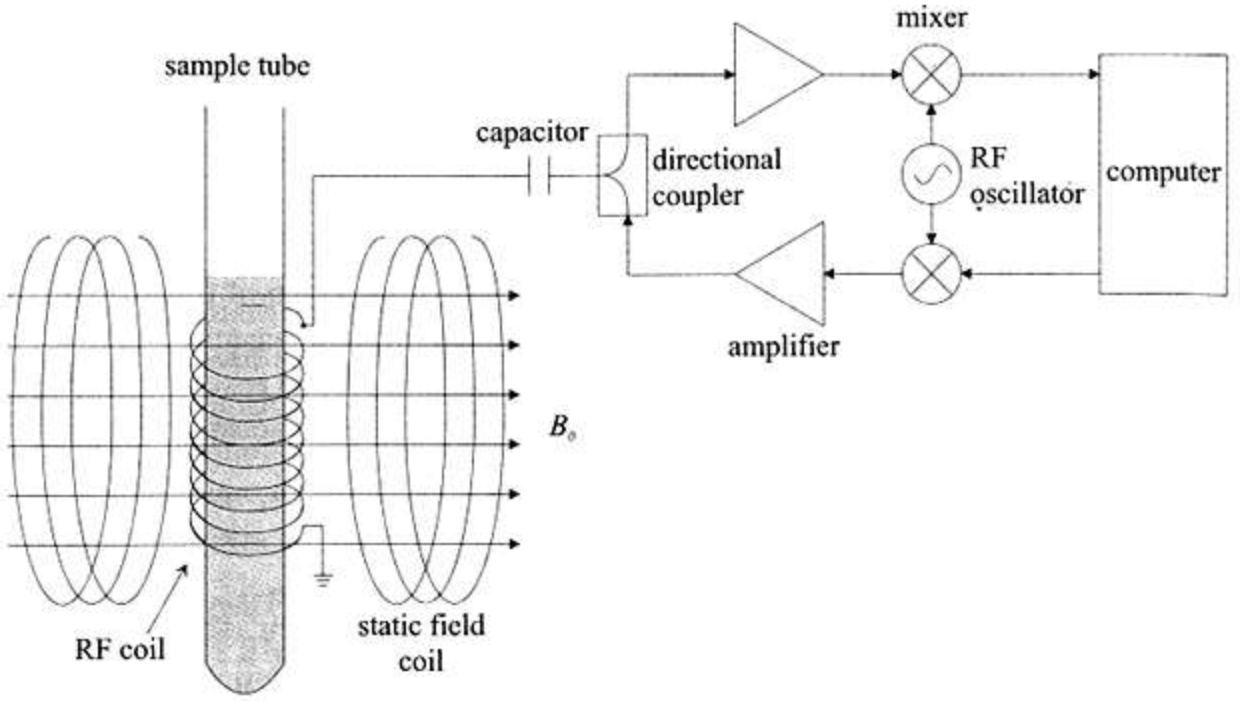
Cold atoms for qubits



a. An optical standing wave is generated by superimposing two laser beams. The antinodes (or nodes) of the standing wave act as a perfectly periodic array of microscopic laser traps for the atoms. The crystal of light in which the cold atoms can move and are stored is called an optical lattice.

b, If several standing waves are overlapped, higher-dimensional lattice structures can be formed, such as the two-dimensional optical lattice shown here.

NMR system for qubits



NMR apparatus

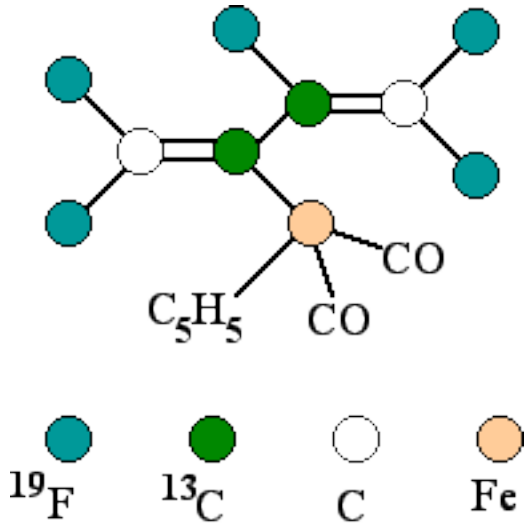
Qubit representation:

Spin of an atomic nucleus

Unitary evolution:

Transforms are constructed from magnetic field pulses applied to spins in a strong magnetic field. Couplings between spins are provided by chemical bonds between neighboring atoms.

NMR system for qubits



perfluorobutadienyl iron complex

A molecular computer

The computing is done by the ^{19}F and ^{13}C nuclear spins.

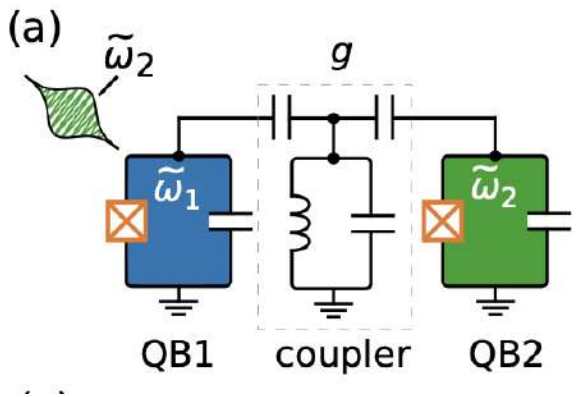
5 Flourine atoms nuclear spin and 2 Carbon - 13 atoms nuclear spins carry the qubits of a quantum computation.

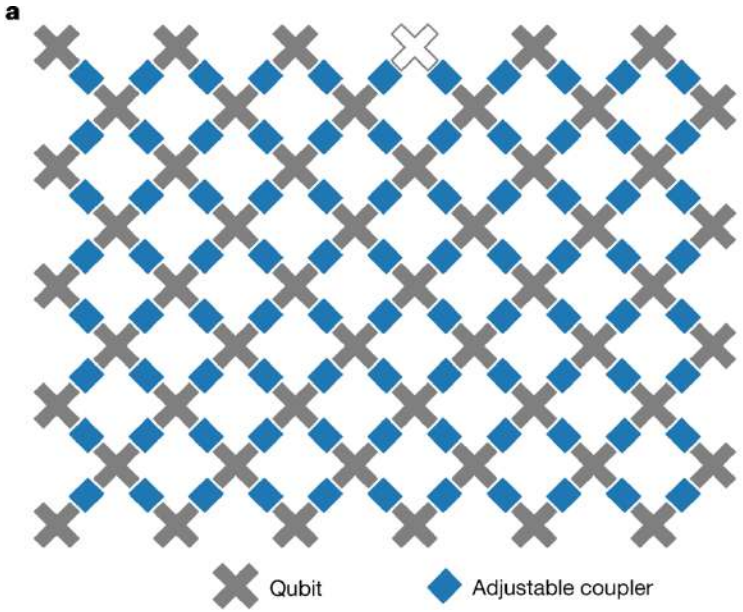
They can be programmed by radio pulses, they can interact, and they can be read out by NMR instruments.

Using Shor's quantum factoring algorithm 15 was factored using the above 7 qubits.

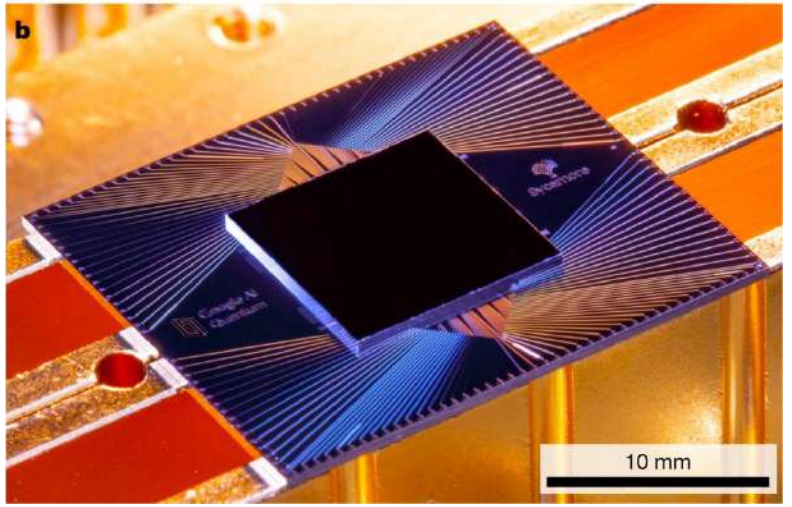
The answer : 3 X 5 was obtained in about 720ms.

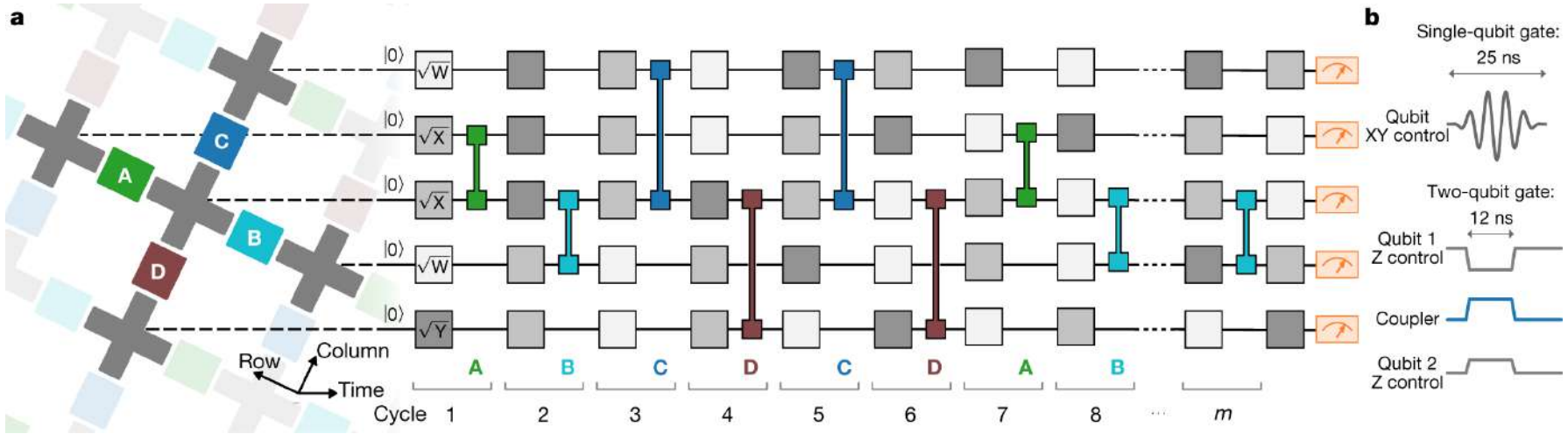
Quantum supremacy using programmable Superconducting qubits ?



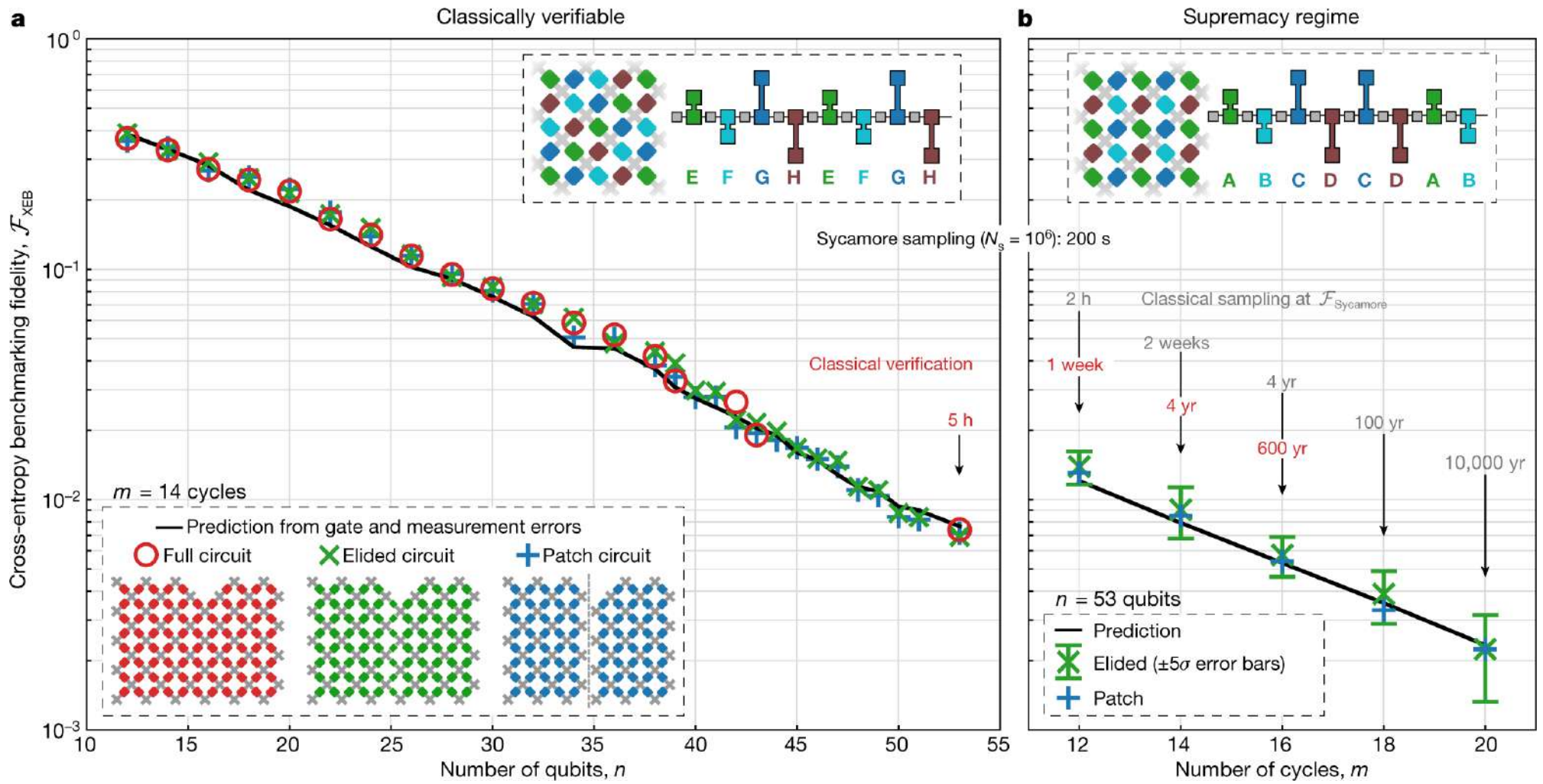


54 qubit Sycamore chip - google





Quantum supremacy using programmable Superconducting qubits ?



54 qubit Sycamore chip - google

This claim has been questioned by an alternative classical algorithm

DiVincenzo criteria for Quantum Computation

For realization of quantum computation, the system should have

Photonic quantum systems

- Well-defined state space of qubits

  Presence or absence of photon – single rail encoding, dual rail encoding

- Ability to initialize the state of the qubits

  You can initialize the multi-qubit states

- Long decoherence time

  Photons interact very weakly with The environment. Decoherence time is long.

- Ability to implement a universal set of quantum gates

  Combinations of beamsplitters, waveplates, and phase-shifters—an optical interferometer implements universal gates

- Qubit-specific measurement capability

  Projective measurement techniques of photonic quantum states are well developed

Quantum Computation with photons

Advantages

- The quantum operations can be done at room temperature
- More robust against the external environment
- Access to multiple degrees of freedom of photons
- Most of the hardware and fabrication techniques are common between classical and quantum optical devices

Challenge

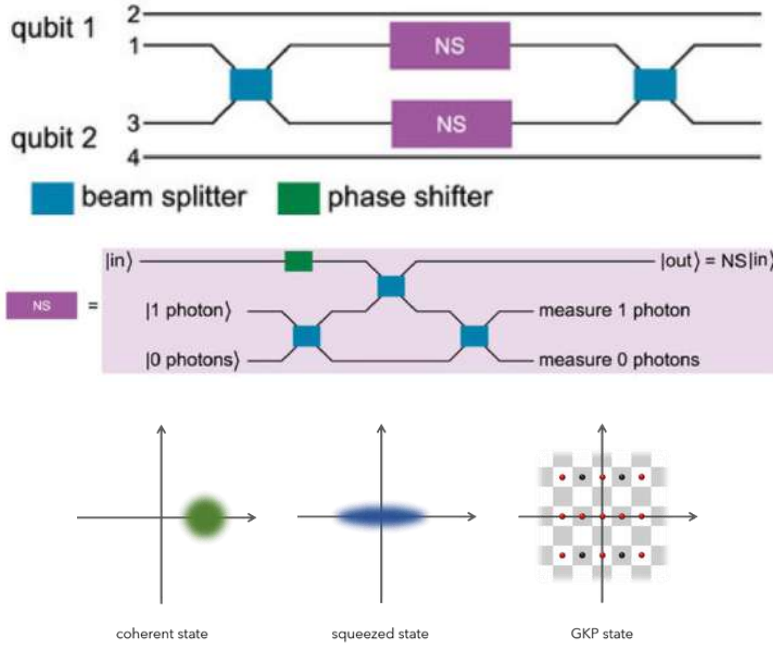
Designing controlled operations between multiple photons

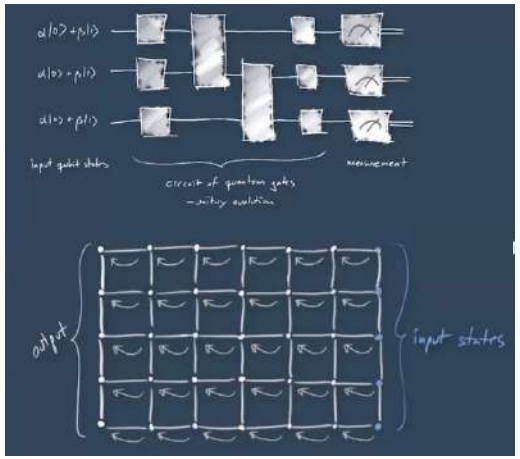
Controlling fast-moving photons

Models for photonic quantum computation

Universal quantum computation

- **Discrete variable (DV) using single photons**
  Dual rail encoding – polarization, paths, frequency, time bin, qudits
- **Continuous variable (CV) using Gaussian state of light**
  GKP states and Gaussian operation
- **Cluster states using squeezed modes**
  Measurement-based / one-way computation
- **Hybrid CV-DV cluster approach using higher-dimensional encoding**
  Fusion based





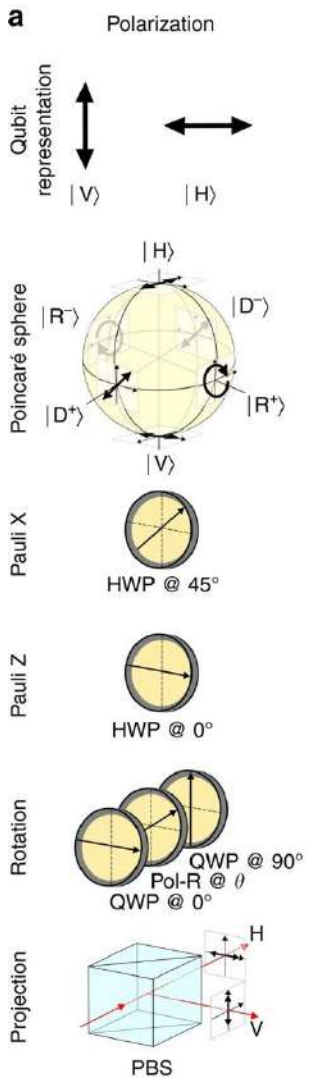
Special purpose quantum computation

- Boson sampling
- -------

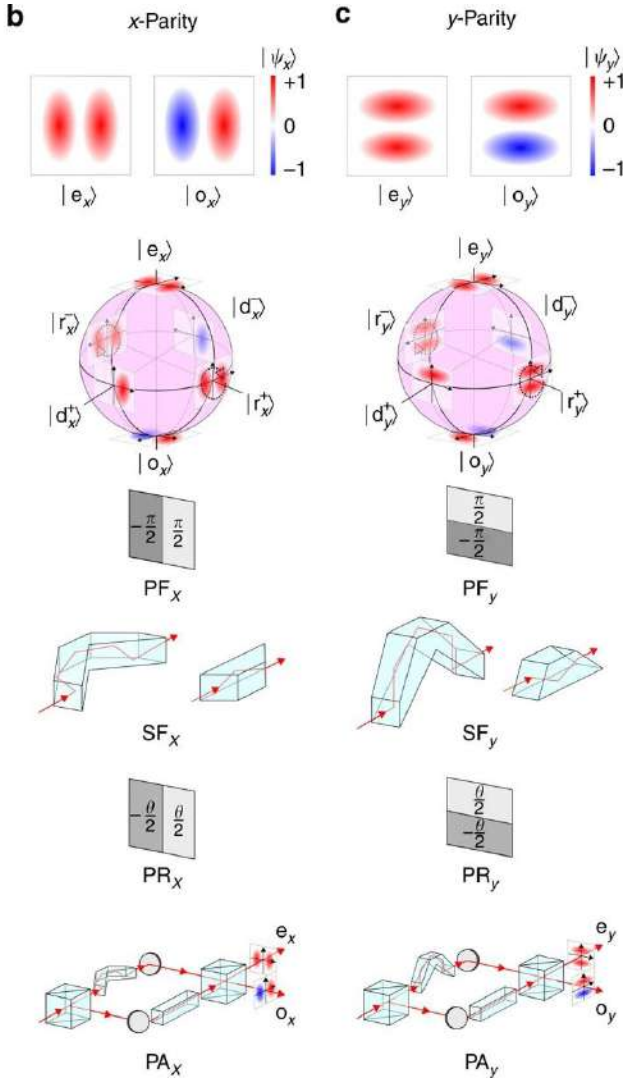
Different schemes for realizing operations under each model has been proposed and experimentally realized

Quantum operations on photonic qubits

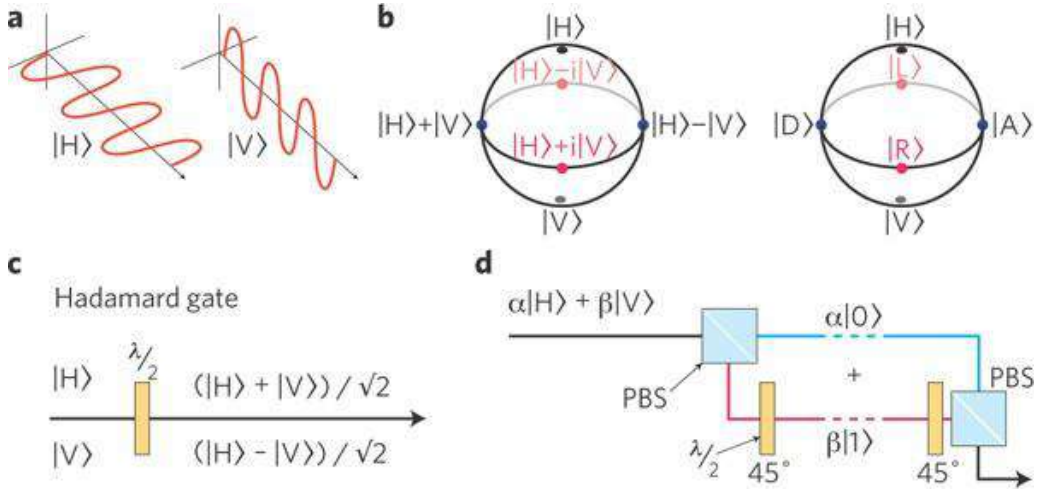
DV as qubit



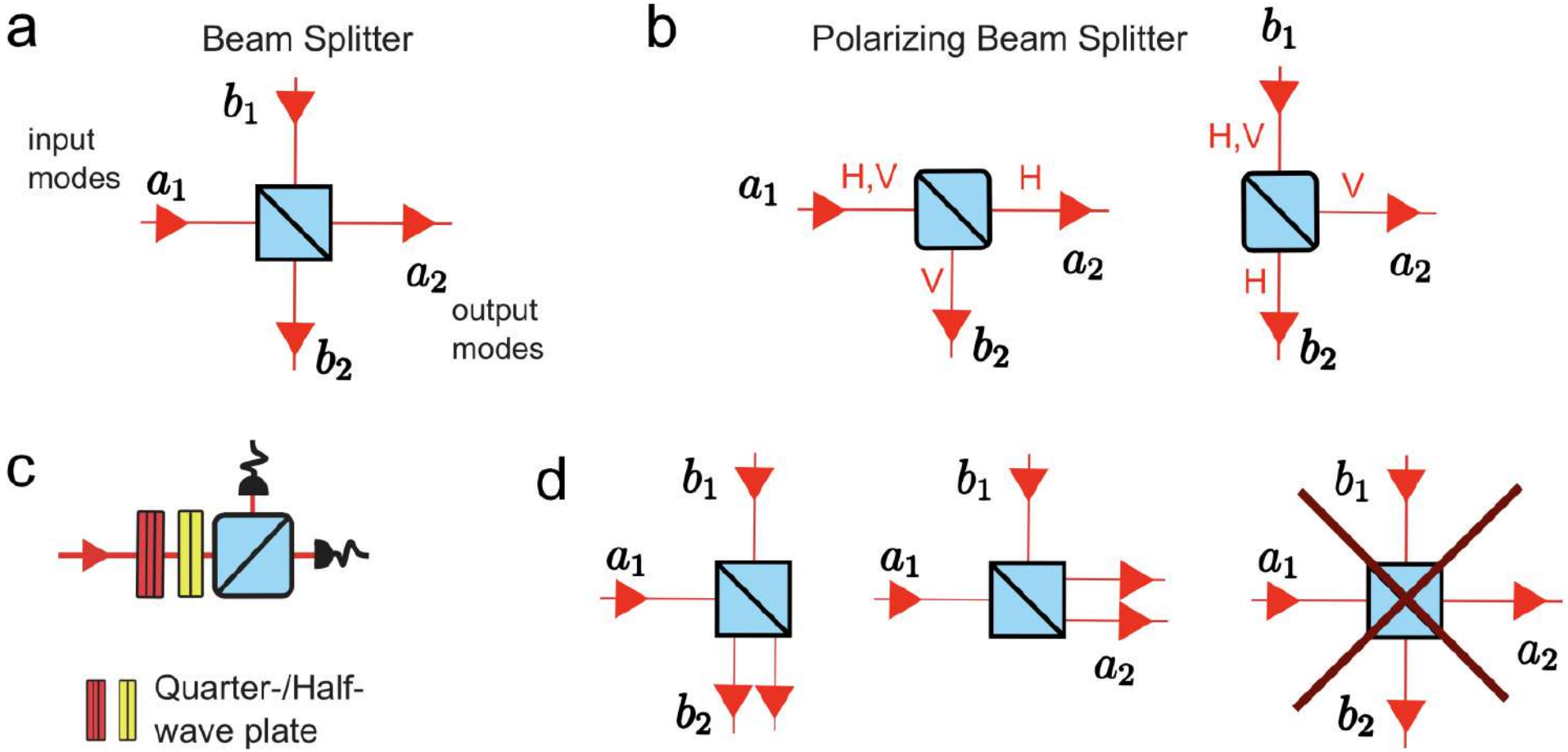
CV as qubit



Operations of polarization qubit

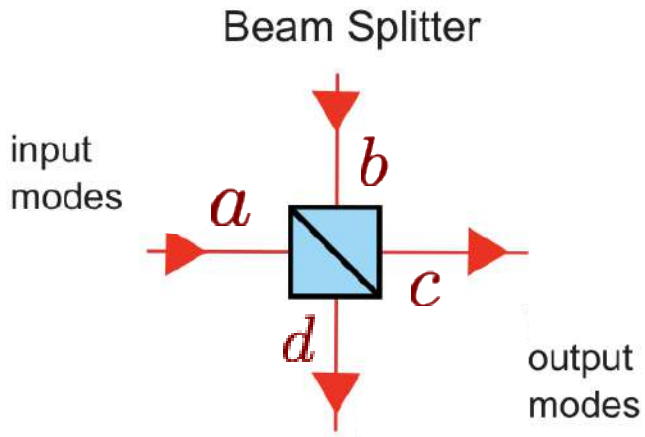


Quantum operations on photons limitation



Bosonic behavior limits photon-photon interaction

Two photon interaction



Annililation and creation operators $\hat{a}, \hat{a}^\dagger,$ and $\hat{b}, \hat{b}^\dagger$

Fock state representation : $|0\rangle_a$ Corresponds to mode a empty (vacuum)

$|1\rangle_a$ Corresponds to one photon in mode a

One input photon along mode a : $|1\rangle_a = \hat{a}^\dagger |0\rangle_a$

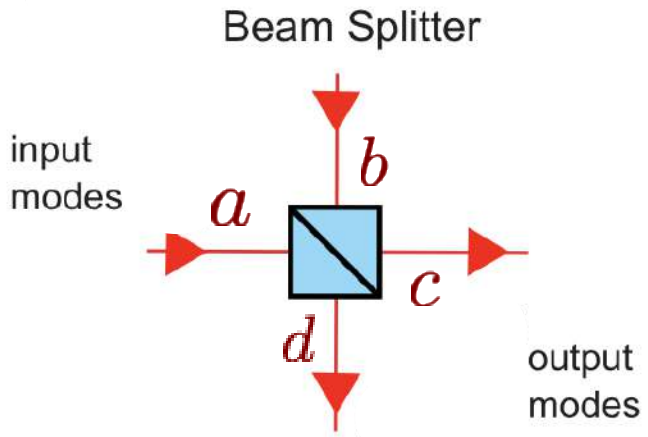
Two input photon, one along mode a and other along b :

$$|1,1\rangle_{ab} = \hat{a}^\dagger \hat{b}^\dagger |0,0\rangle_{ab}$$

When we have one input photon along mode a

$$\hat{a}^\dagger |0\rangle_a \rightarrow \frac{1}{\sqrt{2}} \left(\hat{c}^\dagger + \hat{d}^\dagger\right) |00\rangle_{cd}, \quad = \frac{1}{\sqrt{2}} (|1\rangle_c + |1\rangle_d) \equiv \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \text{ qubit representation}$$

Two photon interaction



Annililation and creation operators $\hat{a}, \hat{a}^\dagger,$ and $\hat{b}, \hat{b}^\dagger$

$$|1,1\rangle_{ab} = \hat{a}^\dagger \hat{b}^\dagger |0,0\rangle_{ab}$$

$$\hat{a}^\dagger |0\rangle_a \rightarrow \frac{1}{\sqrt{2}} \left(\hat{c}^\dagger + \hat{d}^\dagger\right) |00\rangle_{cd},$$

$$\hat{a}^\dagger \rightarrow \frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}} \quad \text{and} \quad \hat{b}^\dagger \rightarrow \frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}}$$

Two mode beam splitter matrix

$$\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix}.$$

When we have two photon inputs along two modes

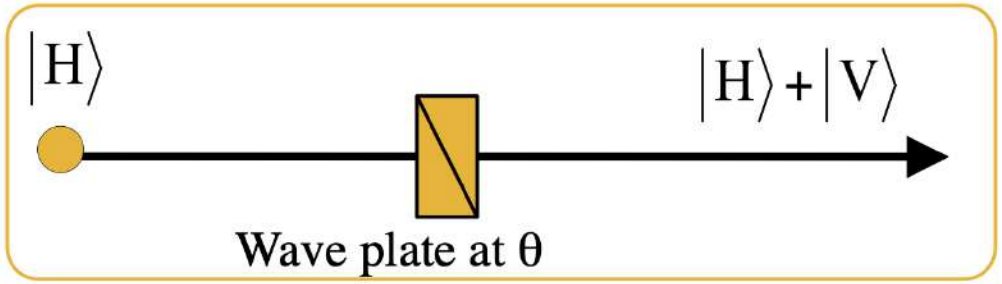
$$|1,1\rangle_{ab} = \hat{a}^\dagger \hat{b}^\dagger |0,0\rangle_{ab} \rightarrow \frac{1}{2} \left(\hat{c}^\dagger + \hat{d}^\dagger\right) \left(\hat{c}^\dagger - \hat{d}^\dagger\right) |0,0\rangle_{cd}$$

$$= \frac{1}{2} \left(\hat{c}^{\dagger 2} - \hat{d}^{\dagger 2}\right) |0,0\rangle_{cd} = \frac{|2,0\rangle_{cd} - |0,2\rangle_{cd}}{\sqrt{2}},$$

Root 2 is from normalization

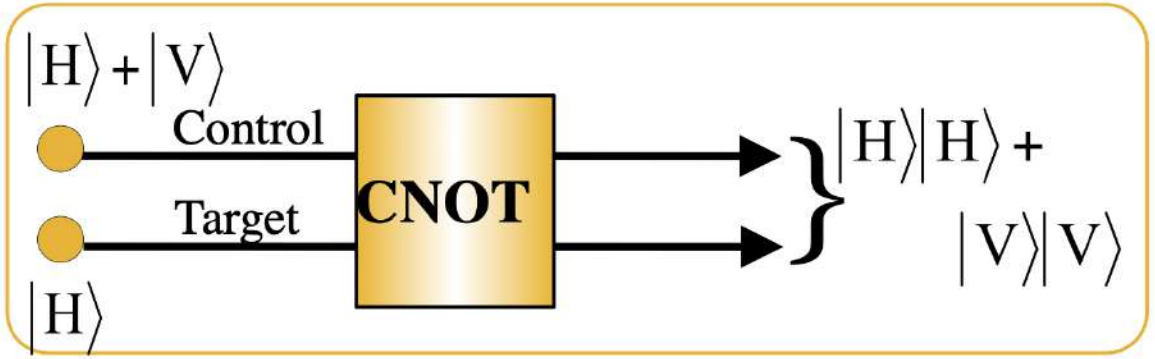
Quantum operations on photons

- Single photon operations



Easy

- Two photon operations

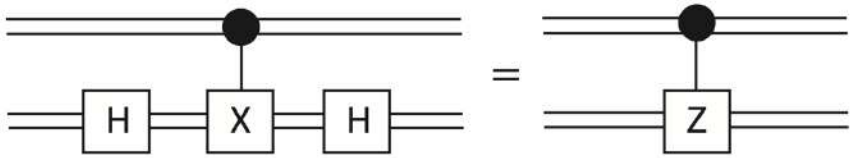


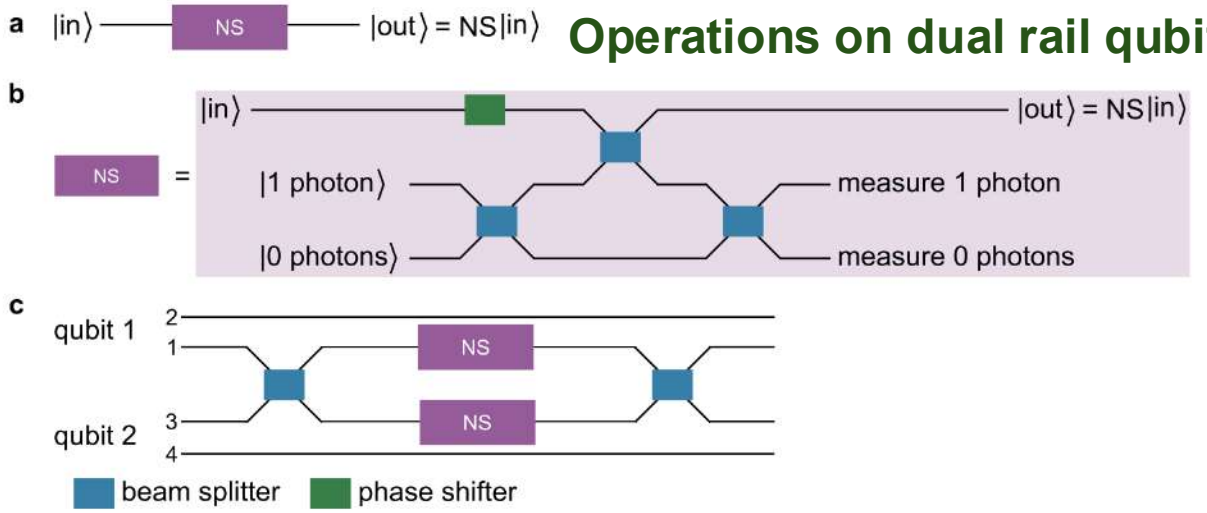
Hard !!!!

This is the problem with linear optics - it is linear and the CNOT is a nonlinear operation

CNOT operation on photon using (NS) non-linear sign shift operation

Why sign change operation and CNOT gate relation

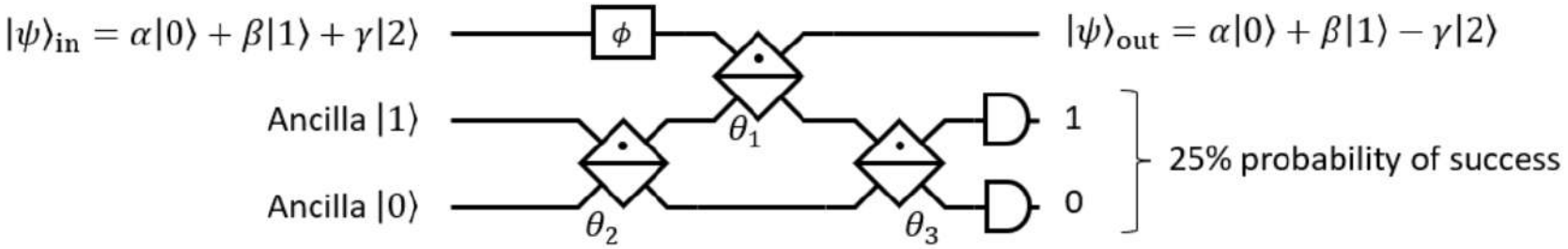




Operations on dual rail qubits

NS – Non-linear phase shifter

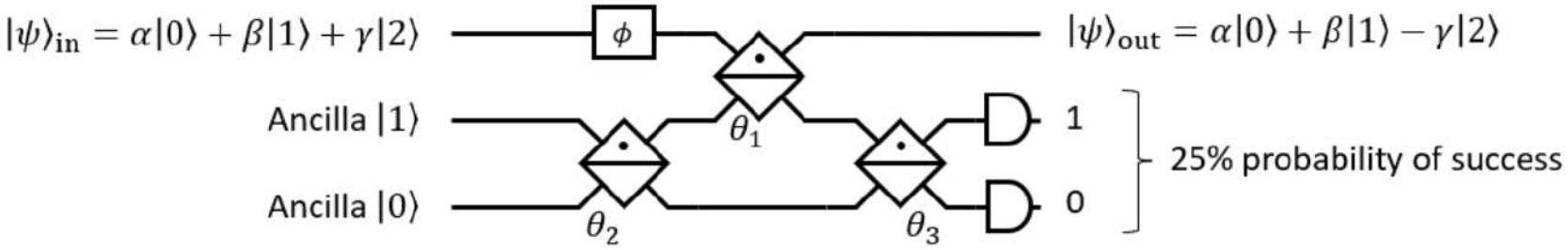
One single NS operation

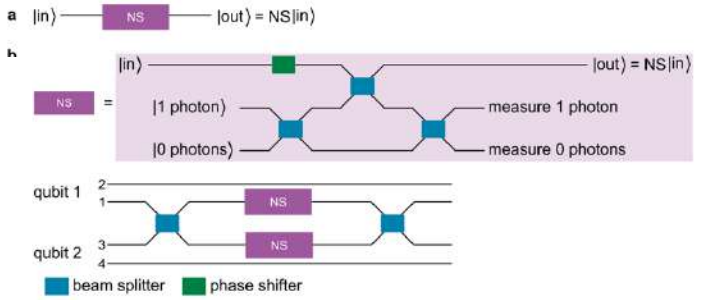


$\phi = 180°$ $\theta_1 = 65.5302°$ $\theta_2 = -\theta_3 = 22.5°$

Knill, Laflamme and Milburn (2001)
KLM model

CNOT operation on photon using (NS) non-linear sign shift operation





$$\phi = 180° \qquad \theta_1 = 65.5302° \qquad \theta_2 = -\theta_3 = 22.5°$$

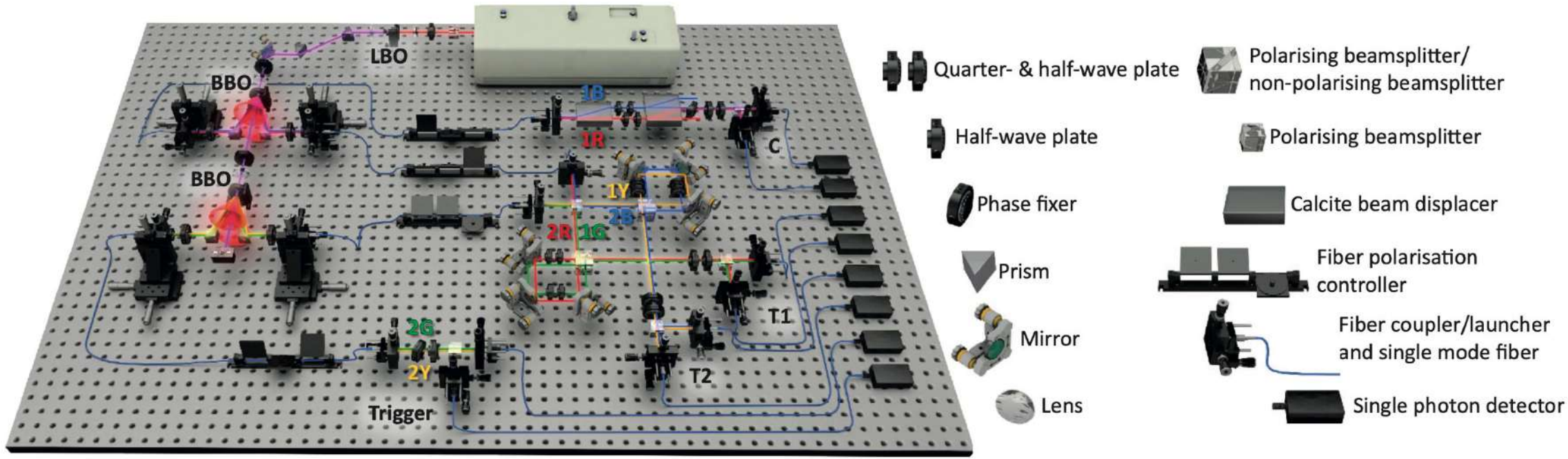
$$U = \begin{pmatrix} 1-\sqrt{2} & \frac{1}{\sqrt{\sqrt{2}}} & \sqrt{\frac{3}{\sqrt{2}}-2} \\ \frac{1}{\sqrt{\sqrt{2}}} & \frac{1}{2} & \frac{1}{2}-\frac{1}{\sqrt{2}} \\ \sqrt{\frac{3}{\sqrt{2}}-2} & \frac{1}{2}-\frac{1}{\sqrt{2}} & \sqrt{2}-\frac{1}{2} \end{pmatrix}$$

We can look at three cases individually :

$$|0\rangle_1|1\rangle_2|0\rangle_3 \rightarrow \left(\cos^2\theta_1 \cos\theta_2 + \sin^2\theta_1\right)|0\rangle_1|1\rangle_2|0\rangle_3$$
$$|1\rangle_1|1\rangle_2|0\rangle_3 \rightarrow -\left(\cos^2\theta_1 \cos 2\theta_2 + \sin^2\theta_1 \cos\theta_2\right)|1\rangle_1|1\rangle_2|0\rangle_3$$
$$|2\rangle_1|1\rangle_2|0\rangle_3 \rightarrow -\cos\theta_2\left(\tfrac{1}{2}\cos^2\theta_1\{3\cos 2\theta_2 - 1\} + \sin^2\theta_1 \cos\theta_2\right)|2\rangle_1|1\rangle_2|0\rangle$$

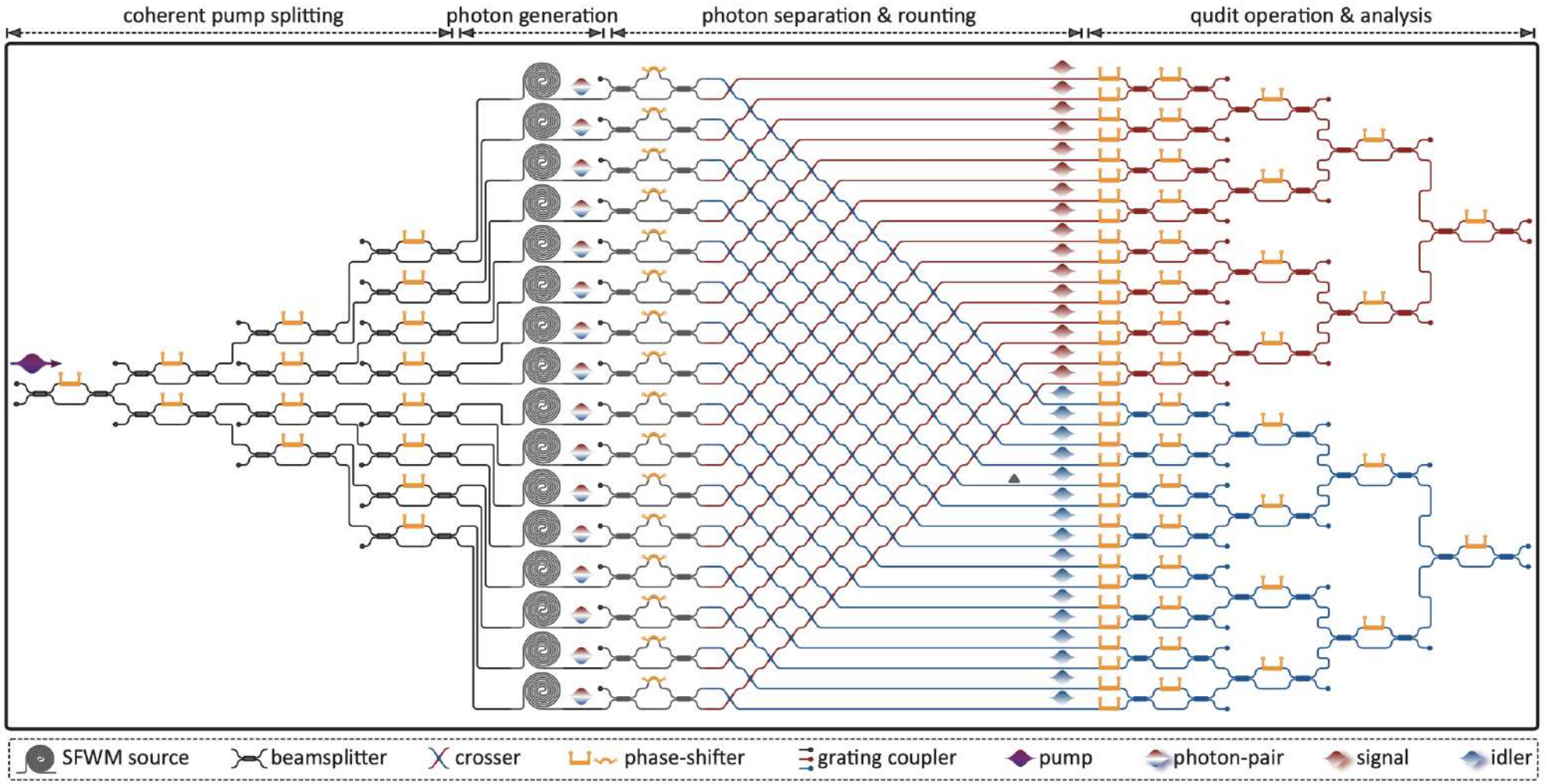
Choose $\cos^2\theta_1 = \frac{1}{4-2\sqrt{2}}$ $\cos^2\theta_2 = 3-2\sqrt{2}$

Thus, $(\alpha|0\rangle_1 + \beta|1\rangle_1 + \gamma|2\rangle_1)|1\rangle_2|0\rangle_3 \rightarrow (\alpha|0\rangle_1 + \beta|1\rangle_1 - \gamma|2\rangle_1)|1\rangle_2$



Using bulk optics

Single photon in four wave mixing – 16 qubit

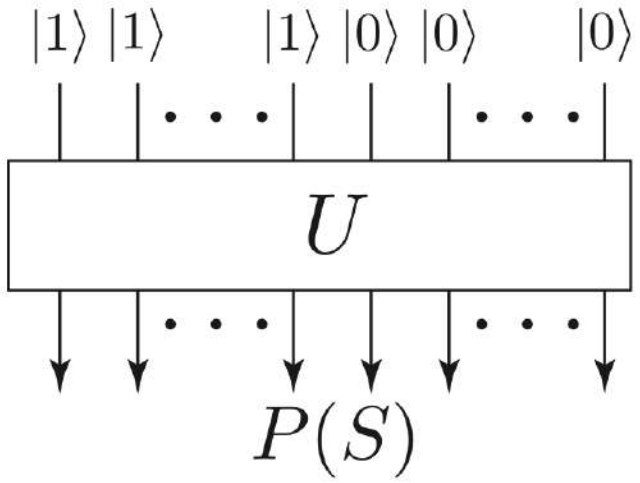


Special task photonic system – boson sampling

Optical circuit, maximum of 76 photons detected in one test and an average of 43 across several tests.

Science **370**, 1460–1463 (2020)

Boson sampling

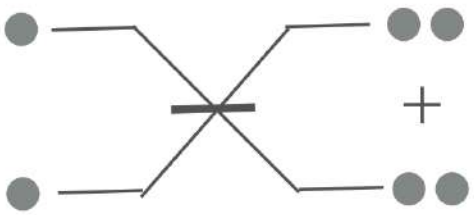


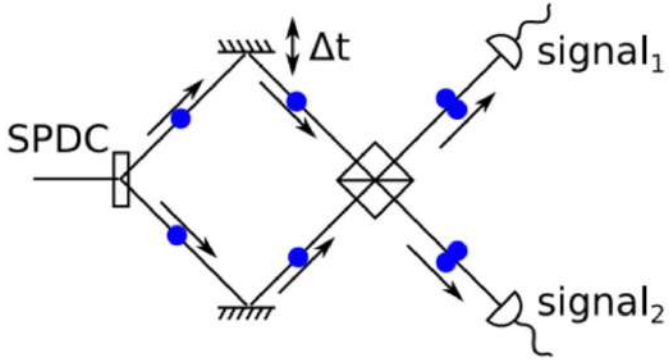
- Multi-photon input state
- Pure linear optics network
- Passive - no feedforward, no memory
- No qubits, no qubit gates like CNOTs etc.
- Number-resolving measurement

Not universal quantum computing but still can perform what is classically hard

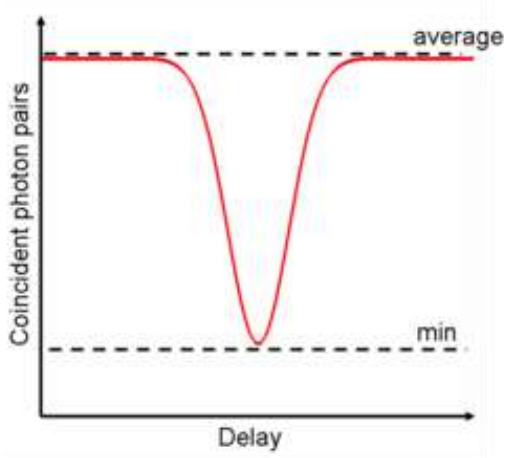
With two-photon input state we evolve to $\frac{|2,0\rangle - |0,2\rangle}{\sqrt{2}}$

The $|1,1\rangle$ term 'dips' because $\mathrm{Per}\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = 0$





HOM dip



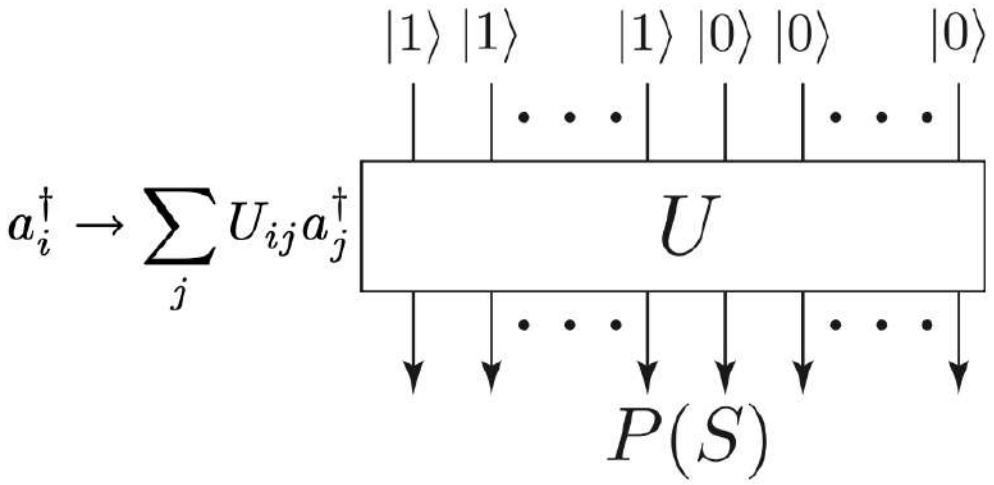
Boson sampling details and calculating permanents

- Matrix permanent problem. Calculating, or even approximating Perm[*A*] is **#P**-complete (by Valiant).

$$\mathrm{Per}\,(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)},$$

A is the amplitude matrix

$$|\psi_{\mathrm{in}}\rangle = |1_1, \ldots, 1_n, 0_{n+1}, \ldots, 0_N\rangle$$



$$|\psi_{\mathrm{out}}\rangle = \sum_S \gamma_S |n_1^{(S)}, n_2^{(S)} \ldots, n_N^{(S)}\rangle$$

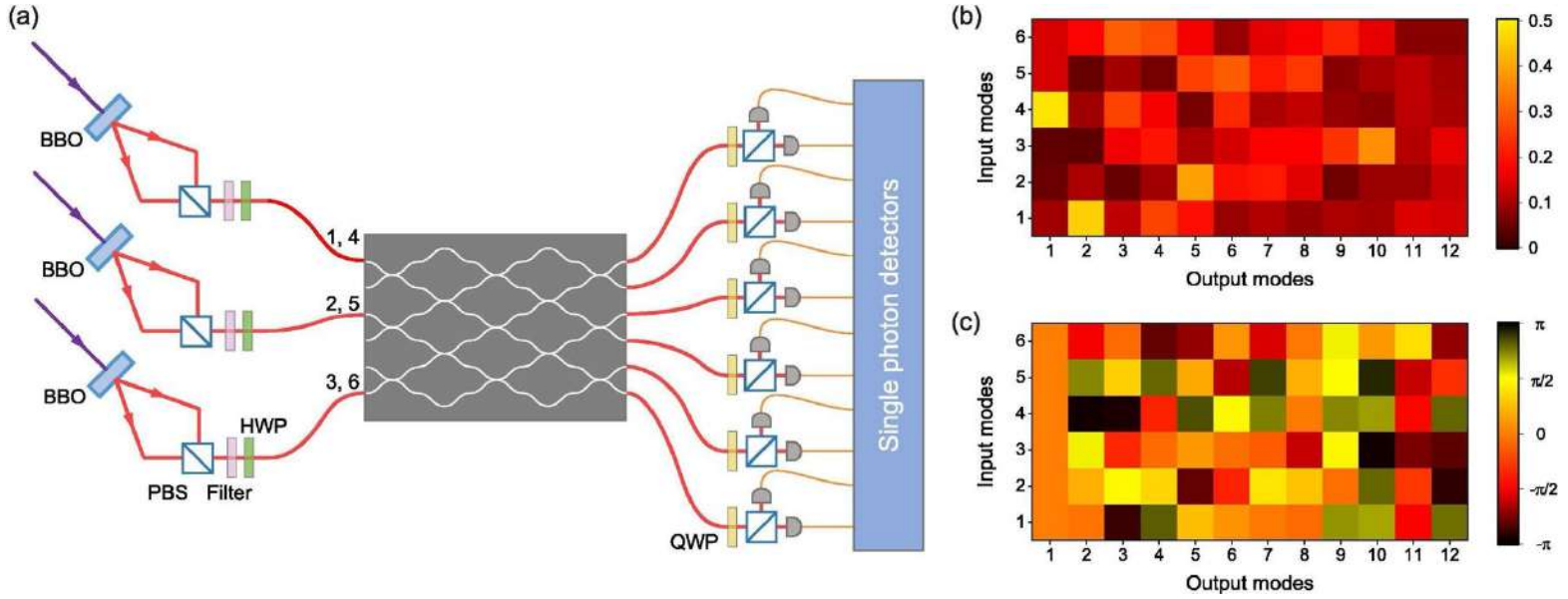
- When we do a measurement

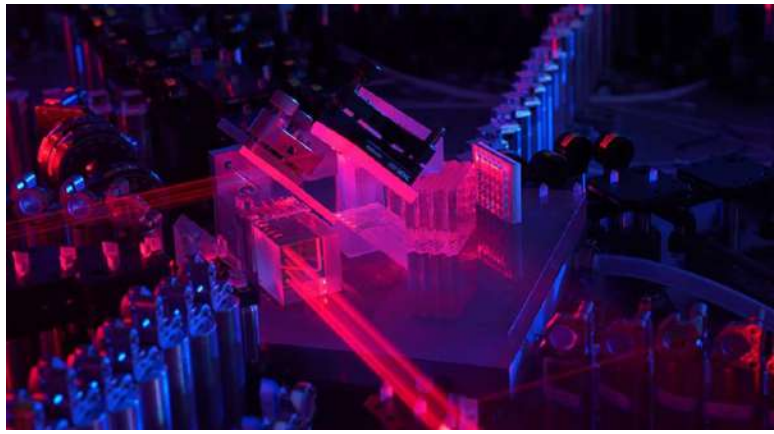
$$\Pr[S] = |\alpha_S|^2 = |\langle\psi|S\rangle|^2$$

- Result: $\Pr_{\mathcal{D}_A}[S] = \dfrac{|\mathrm{Per}\,(A_S)|^2}{s_1! \cdots s_m!}.$

Special task photonic system – boson sampling

76 photons and 144 modes – *Jiuzhang (specific task photonic QC)*

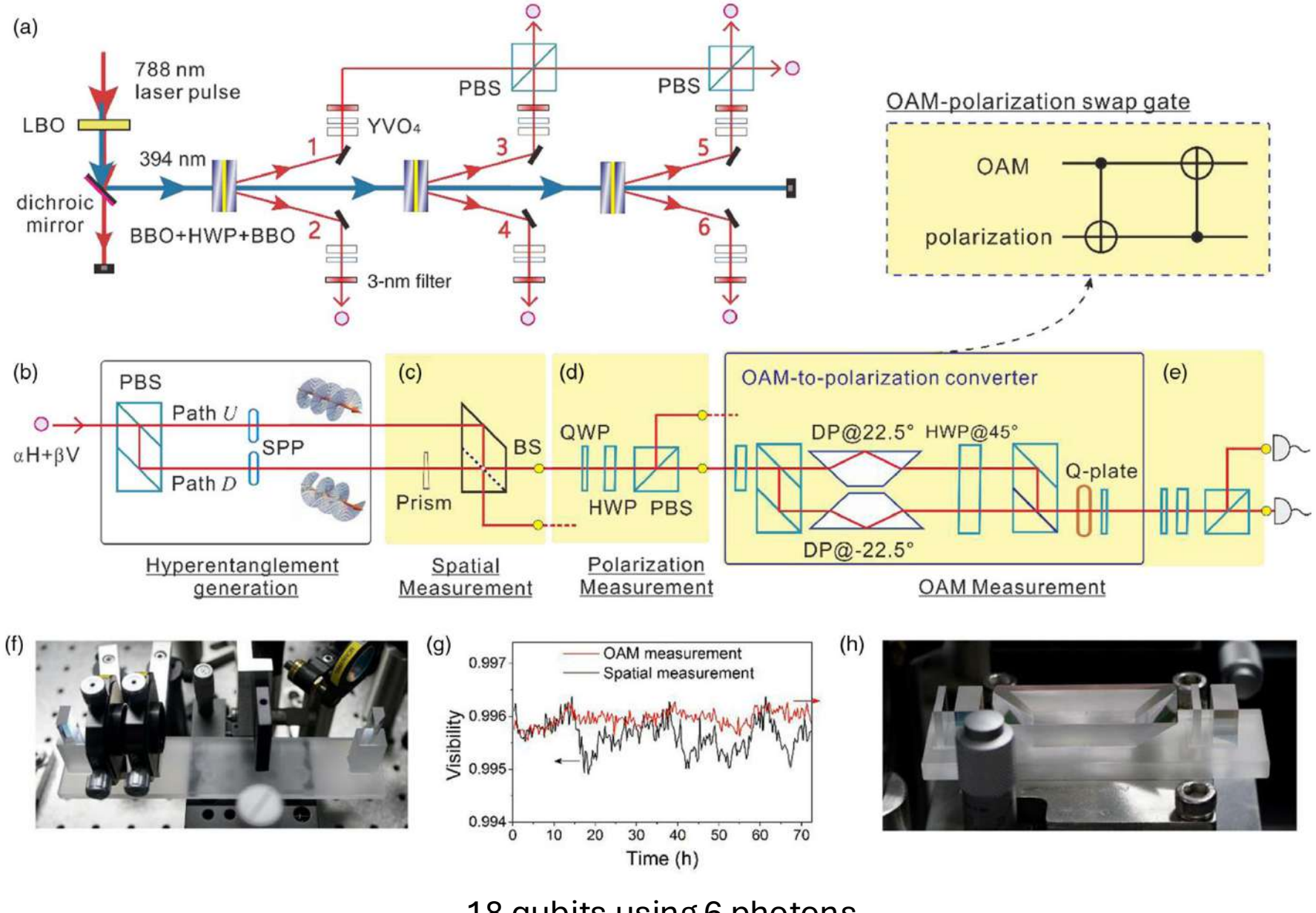




The dimension of the entangled state grows exponentially with both the number of photons and the modes, which quickly renders the storage of the quantum probability amplitudes impossible. The state-of-the-art classical simulation algorithm calculates one probability amplitude (Permanent of the submatrix) at a time. The Permanent is classically hard, and because at least one Permanent is evaluated for each sample, the sample size loophole can be avoided. In addition, boson samplers use photons that can be operated at room temperature and are robust to decoherence.

2020 - 2021

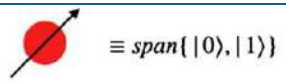
QC using different degrees of freedom of photons



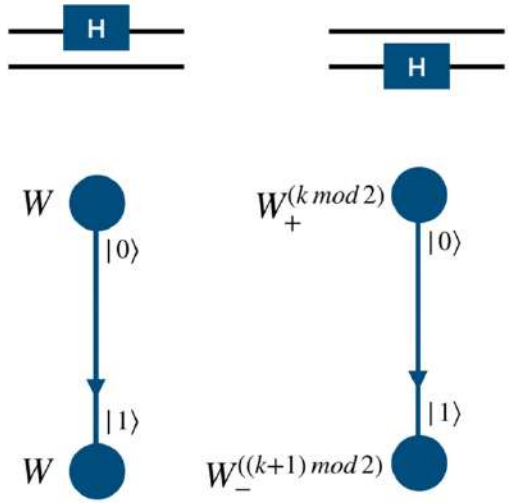
18 qubits using 6 photons

Gate operations using different degree of freedom of photons

Particle and position space as qubits

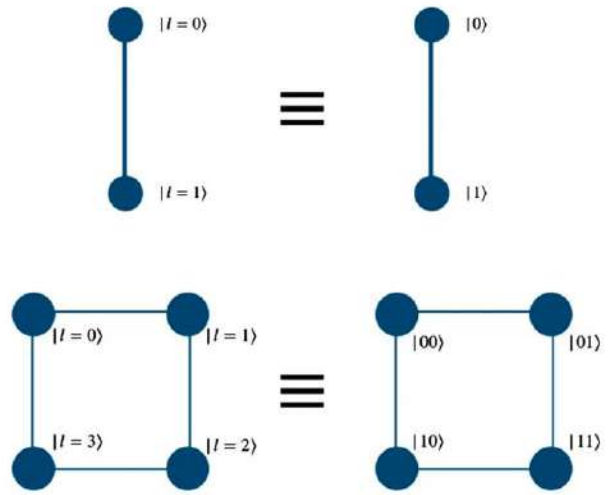


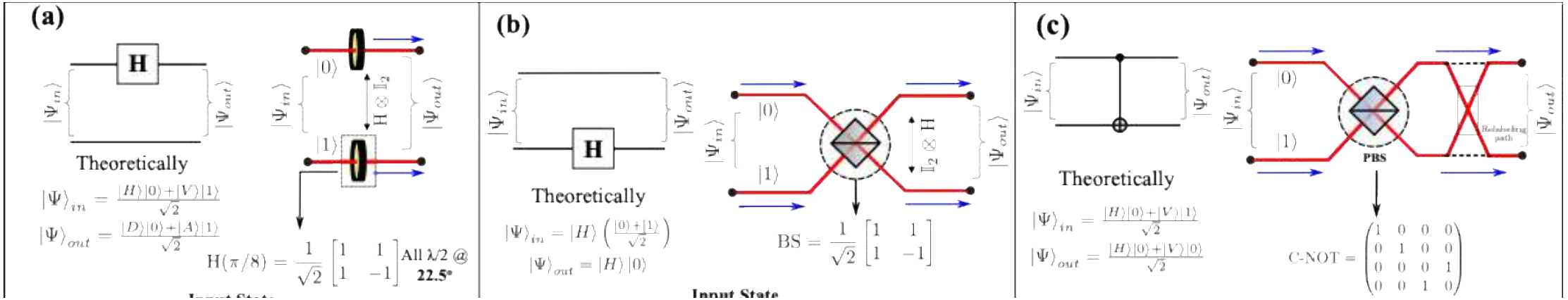
Hadamard operation



Mapping of position state to multi-qubit state

Position ⟩	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7
| Qubit basis⟩	|1001⟩	|1010⟩	|1011⟩	|0100⟩	|0101⟩	|0110⟩	|0111⟩	|0000⟩	|0001⟩	|0010⟩	|0011⟩	|1100⟩	|1101⟩	|1110⟩	|1111⟩





Limitations of NIQS / near-term quantum computers

- **Available coherence time resulting in short circuit depth**
- **Limited connectivity between qubits results in more gates to perform controlled operations**
- **The quality and number of qubits are still very small in number for error corrections**

To perform simulations of large quantum systems on near-term quantum hardware:

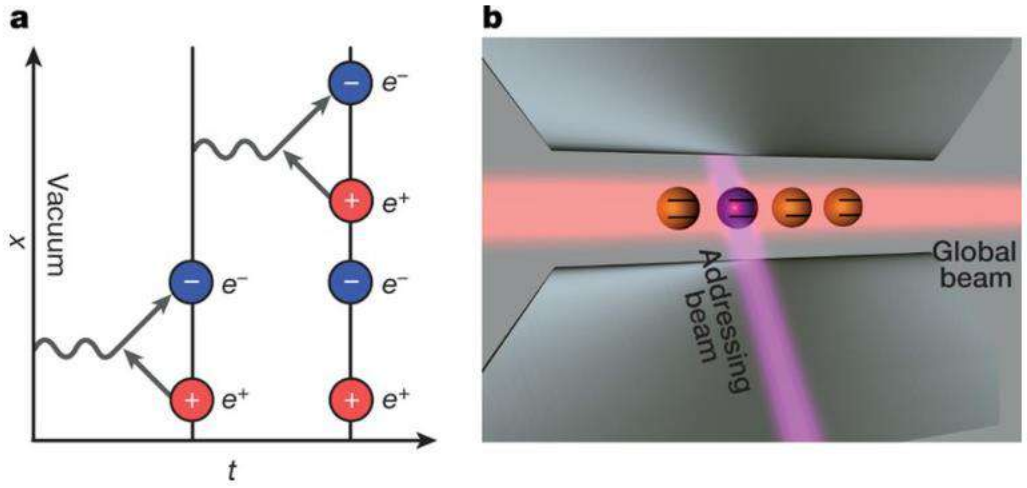
We need quantum algorithms with a short circuit depth that finish within the available coherence time.

A way to stay within the limits of coherence is to design and optimize gates for specific algorithm of interest optimized to the hardware of choice.

Or use the combination of classical and quantum systems to implement an algorithm

Some simple and interesting problems being simulated

- **Real-time dynamics of lattice gauge theories using a four-qubit system** (quantum Monte Carlo methods describe equilibrium phenomena, no systematic techniques exist to tackle the dynamical long-time behaviour)



Coherent real-time dynamics of particle - antiparticle creation by realizing the Schwinger model on four $^{40}Ca^{+}$ ion qubit quantum computer.

Real-time quantum simulations of non-Abelian lattice gauge theories ?

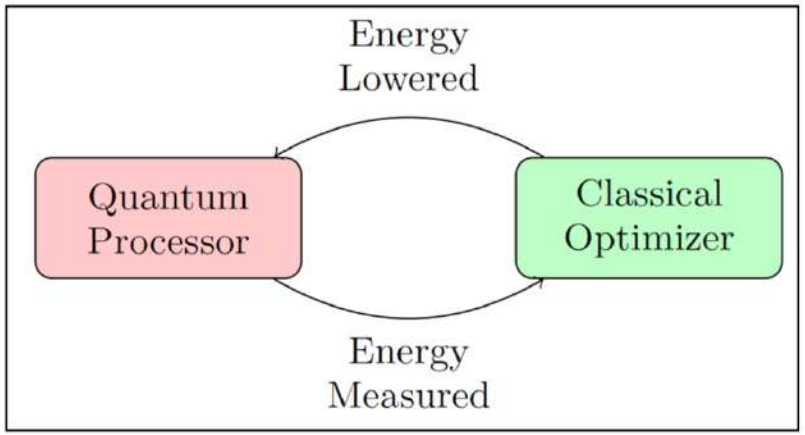
2016

Quantum optimization

We don't expect a quantum computer to solve worst case instances of NP-hard problems, but it might find better approximate solutions, or find them faster.

Hybrid quantum/classical algorithms.

Combine quantum evaluation of an expectation value with a classical feedback loop for seeking a quantum state with a lower value.

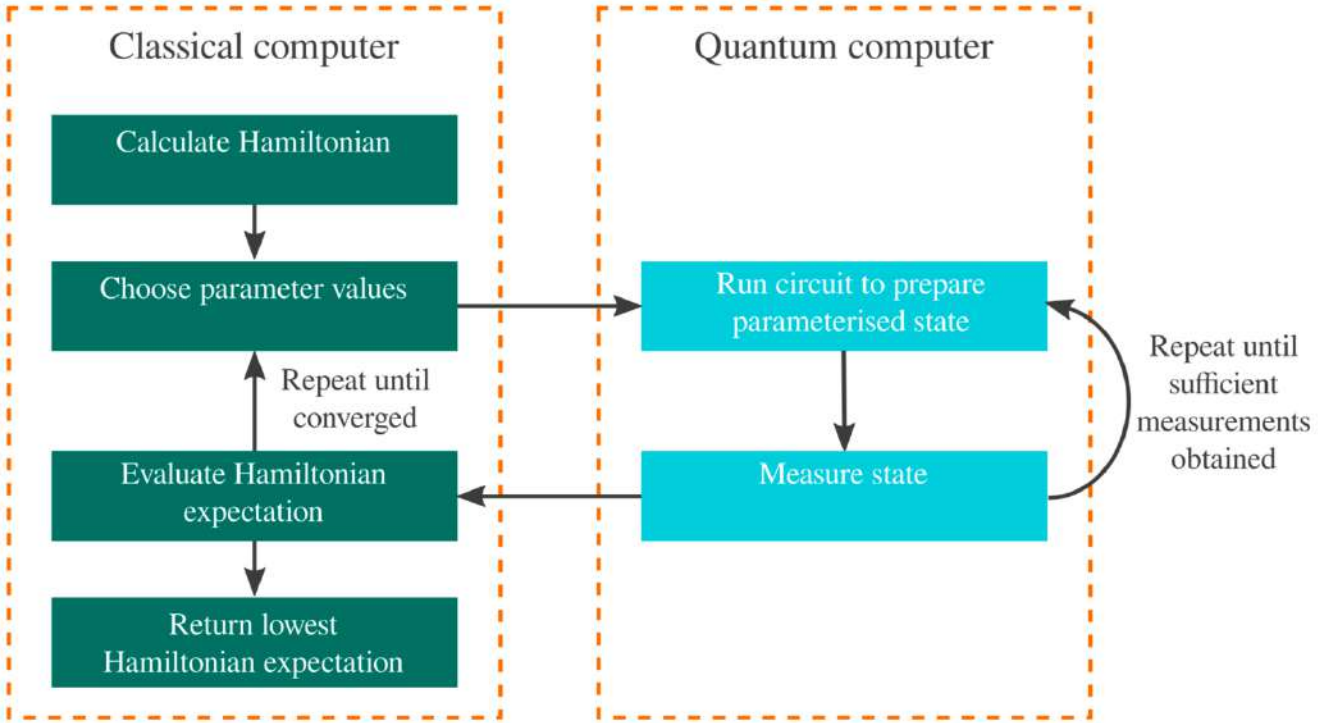


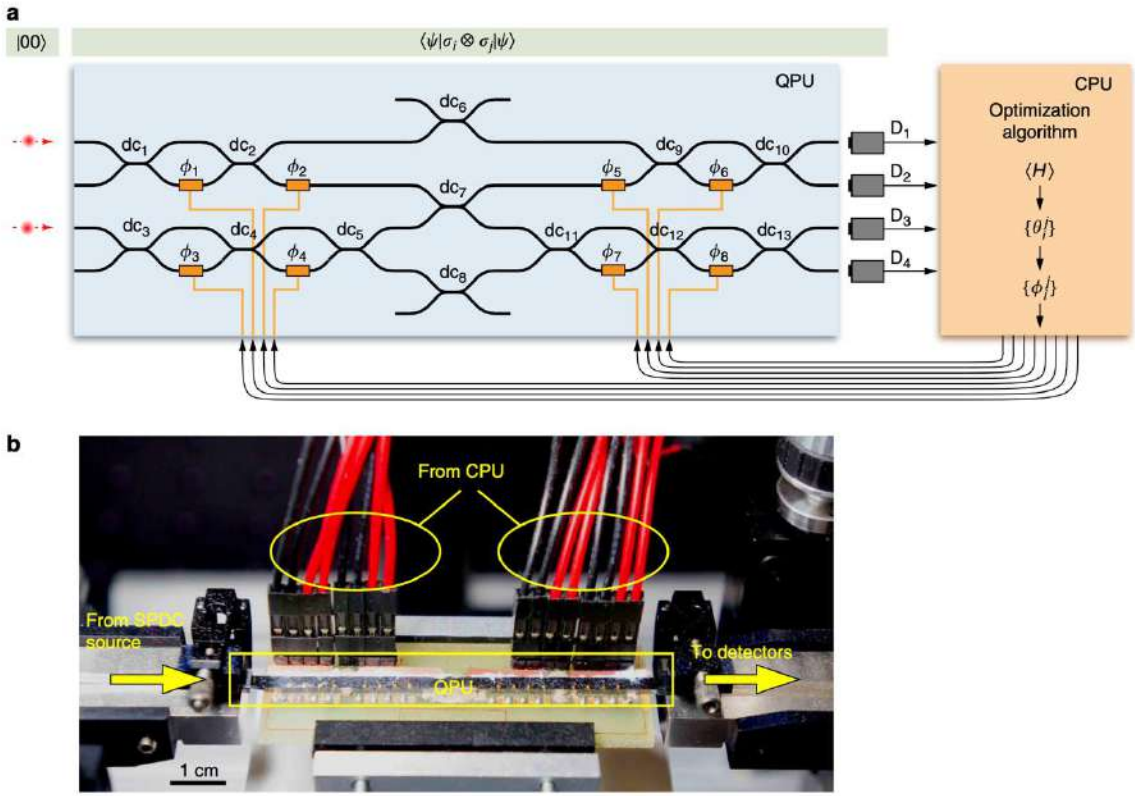
Quantum approximate optimization algorithm (QAOA).
Seek low-energy states of a classical spin glass.

Variational quantum eigensolvers (VQE).
Seek low energy states of a quantum many-body system with a local Hamiltonian H. (Much easier than algorithms which require simulation of time evolution governed by H.)

Classical optimization algorithms (for both classical and quantum problems) are sophisticated and well-honed after decades of hard work. Will NISQ be able to do better?

Variational Eigenvalue Solver (Classical – Quantum)

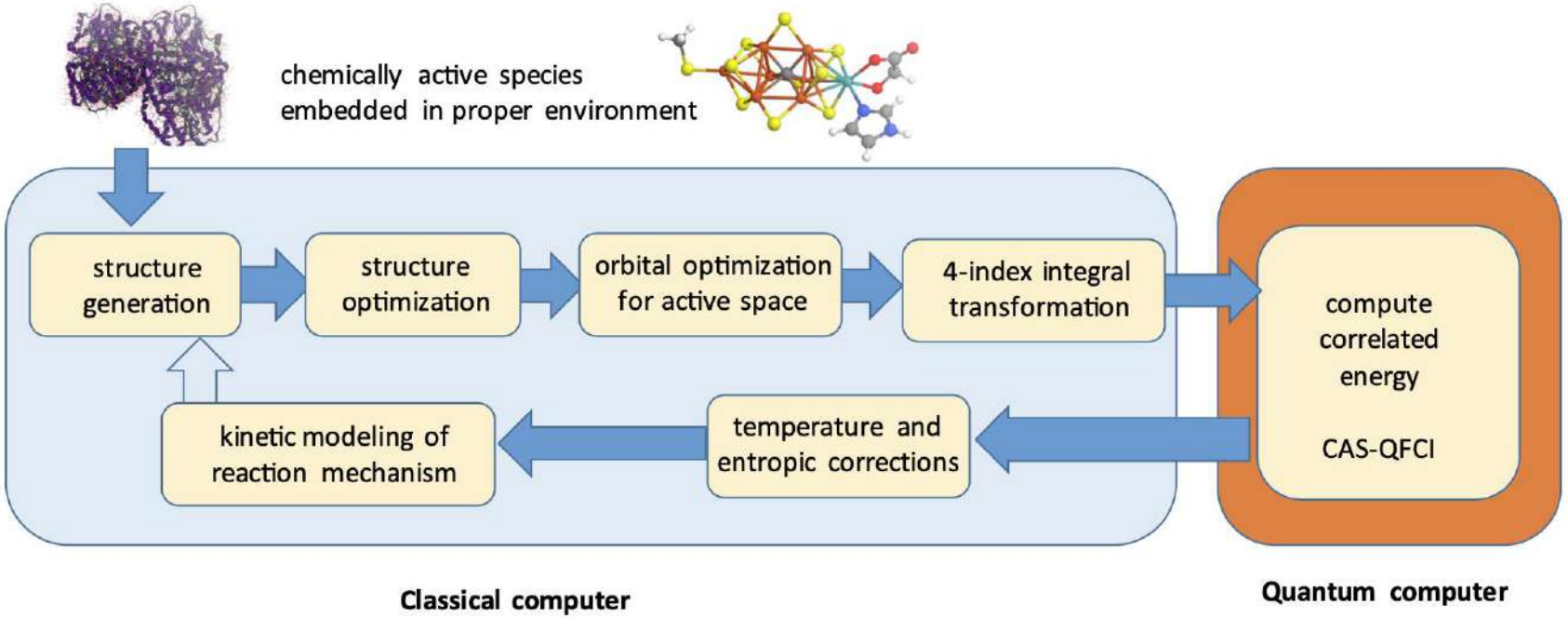


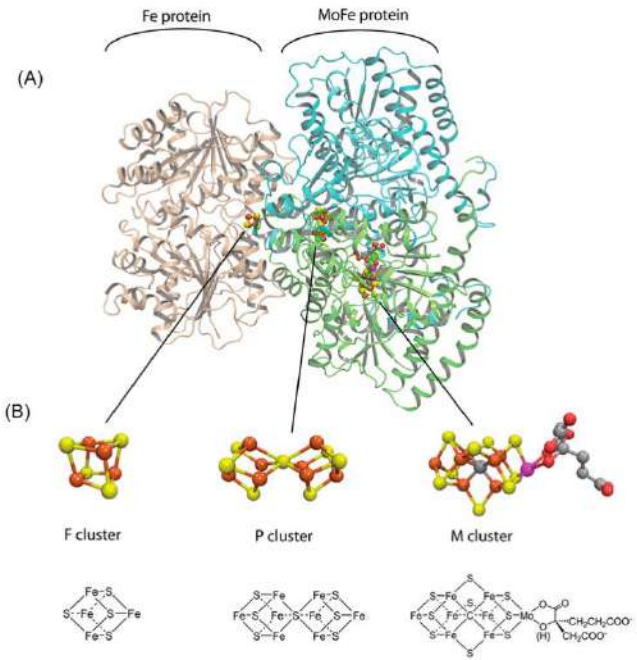


- **Calculating the ground-state molecular energy for He-H⁺**

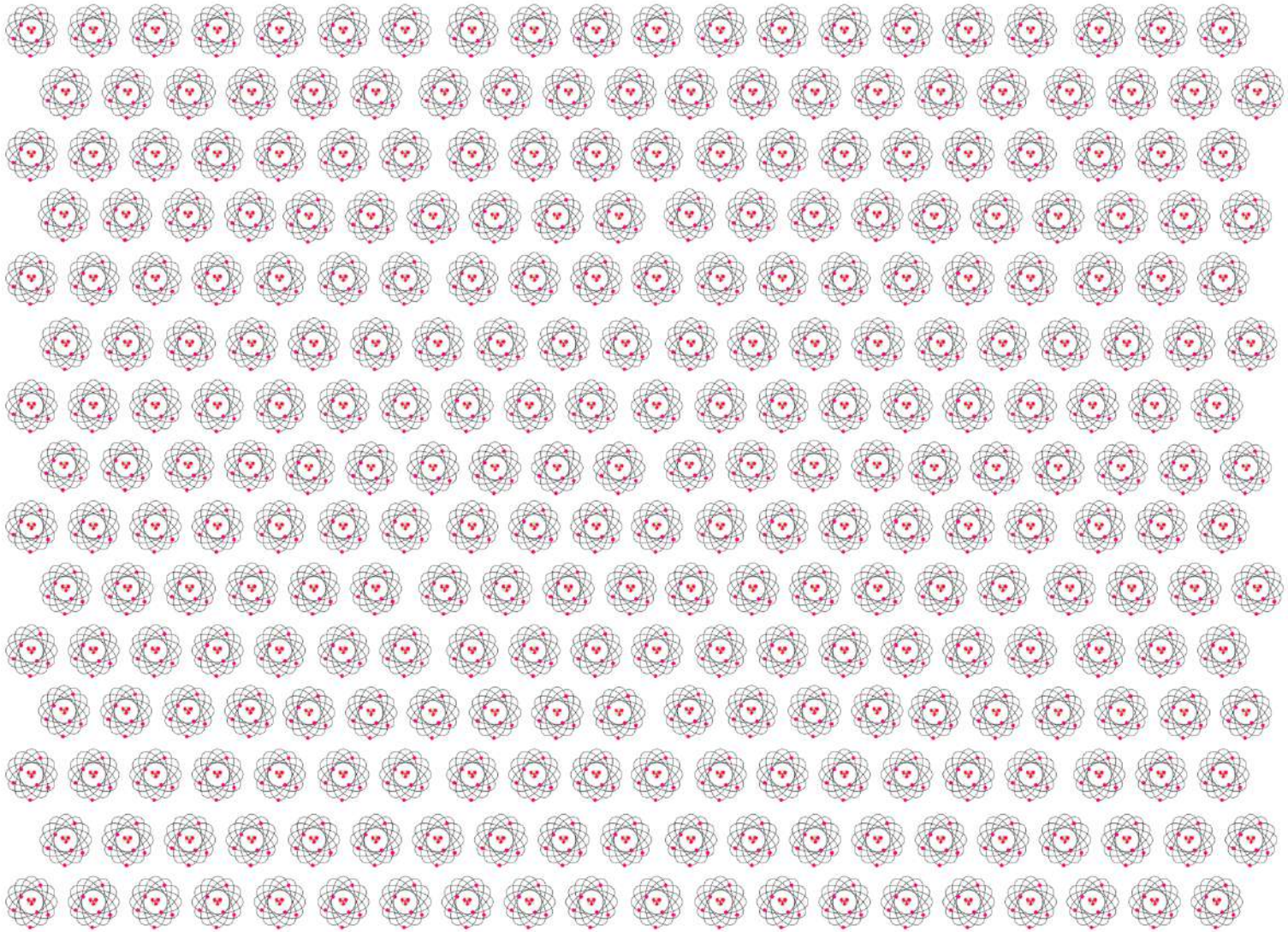
Variational Eigenvalue Solver (Classical – Quantum)

- **Biological nitrogen fixation by the enzyme nitrogenase**





From Prof. Preskill's slide



A complete description of a typical quantum state of just 300 qubits requires more bits than the number of atoms in the visible universe.

Quantum Fourier Transform

Quantum Fourier Transform (QFT) is a unitary *Discrete Fourier Transform* (DFT) upon the quantum state. DFT of a discrete function $f_1, ..., f_N$ is given by

$$\tilde{f}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} f_j,$$

where $f_0, f_1, f_2, ..., f_{N-1}$ and $\tilde{f}_1, \tilde{f}_2, ..., \tilde{f}_{N-1}$ are the input and output functions, respectively.

The inverse transform is

$$f_j \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j k/N} \tilde{f}_k.$$

In QFT we do a DFT on the amplitudes of a quantum state :

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

amplitudes y_k are DFT of amplitudes x_j.

Quantum Fourier Transform

$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Another way of writing this is to say that the jkth entry of QFT_M is ω^{jk}.

$$QFT_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \omega \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

As you can see, QFT_2 is simply equal to $H^{\otimes 2}$.
How about QFT_4? The primitive 4th root of unity is i, so that

$$QFT_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$$|f\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$|g\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \text{ and } |h\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

QFT_4 to $|f\rangle$.

$$\left|\hat{f}\right\rangle = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

QFT_4 on $|g\rangle$:

$$|\hat{g}\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

QFT_4 on $|h\rangle$:

$$\left|\hat{h}\right\rangle = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}$$

Quantum Fourier Transform

Let $|\Theta\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$ and $|\Phi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix}$. Then

If we need only probability, we don't see any difference

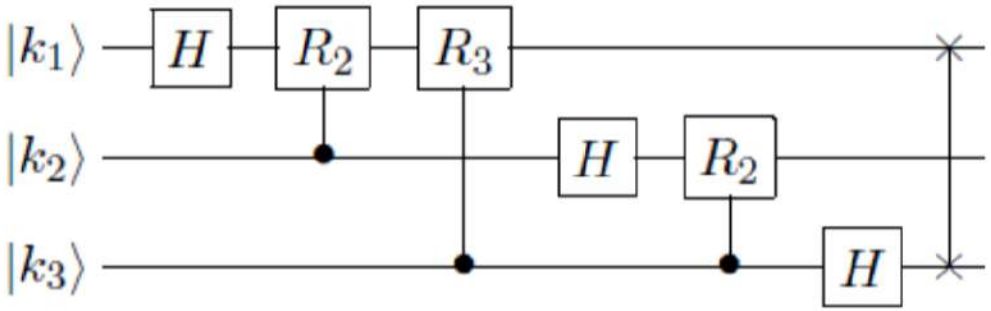
$$\left|\hat{\Theta}\right\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ \alpha_0 + i\alpha_1 - \alpha_2 - i\alpha_3 \\ \alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 \\ \alpha_0 - i\alpha_1 - \alpha_2 + i\alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

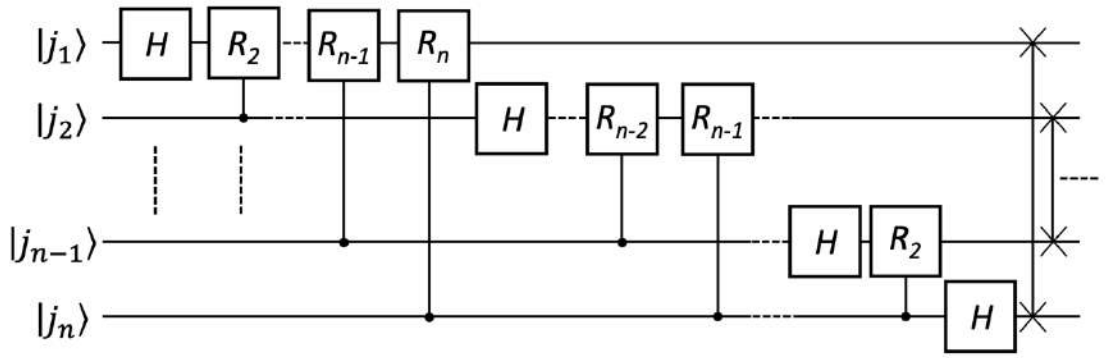
$$\left|\hat{\Phi}\right\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \\ -i\alpha_0 + \alpha_1 + i\alpha_2 - \alpha_3 \\ -\alpha_0 + \alpha_1 - \alpha_2 + \alpha_3 \\ i\alpha_0 + \alpha_1 - i\alpha_2 - \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ -i\beta_1 \\ -\beta_2 \\ i\beta_3 \end{pmatrix}$$

The important point here is that the only difference between $\left|\hat{\Theta}\right\rangle$ and $\left|\hat{\Phi}\right\rangle$ is a relative phase shift.

How many operations do we have to do for M X M matrix?

Quantum Fourier Transform





Where $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$ is a single qubit unitary *rotation* gate.

As an example, for $n = 3$ we have the 3-qubit product state

$$F_8|k_1k_2k_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.k_3}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.k_2k_3}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.k_1k_2k_3}|1\rangle).$$

$$QFT_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

What is a quantum operational form QFT ?

Quantum Phase Estimation

Hadamard operation is self-inverse operation (It does the opposite as well) and it can be used to encode information into the phases.

$$H|x\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^x|1\rangle\right] = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle.$$

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

The value of x is encoded into the relative phases between the basis states $|0\rangle$ and $|1\rangle$. Hadamard operation on an $n-$qubit basis state is given by

$$H^{\otimes n}|X\rangle = \frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle.$$

Information about the value of X is encoded into the phases $(-1)^{X\cdot Y}$.

$$H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle\right) = H^{\otimes n}(H^{\otimes n}|X\rangle) = (H^{\otimes n}H^{\otimes n})|X\rangle = \mathbb{1}|X\rangle.$$

Note that $(-1)^{X\cdot Y}$ are phases of specific form. General form is a complex number $e^{2\pi i\omega}$ for any real number $\omega \in (0,1)$ (phase "-1" corresponds to $\omega = \frac{1}{2}$). The $n-$qubit Hadamard operation is not able to fully access information that is encoded in more general ways.

Quantum Phase Estimation

Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$

Problem : Obtain a good estimate of the phase parameter w

If the input is one-qubit $(n = 1)$, $\omega = 0 \,.\, x_1$ then we get

$$\frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i (0 \,.\, x_1) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i \left(\frac{x_1}{2}\right) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\pi i (x_1 y)} |y\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{y=1}^{1} (-1)^{x_1 y} |y\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{x_1} |y\rangle\right)$$

You can recall that Hadamard operation on the preceding expression will return you the value of x_1 and hence the value of ω for one-qubit.

Quantum Phase Estimation

Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$

Problem : Obtain a good estimate of the phase parameter w

When we have a two qubit state ($n = 2$), $\omega = 0 \,.\, x_1 x_2$ then using product representation we get

$$\frac{1}{\sqrt{2^2}} \sum_{y=0}^{3} e^{2\pi i(\omega)y} |y\rangle = \frac{1}{\sqrt{2^2}} \sum_{y=0}^{3} e^{2\pi i(0\,.\,x_1x_2)y} |y\rangle = \frac{|0\rangle + e^{2\pi i(0\,.\,x_2)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0\,.\,x_1x_2)}|1\rangle}{\sqrt{2}}$$

Hadamard operation on the first qubit will return the value for x_2. If $x_2 = 0$ the value of x_1 can be obtained but not if $x_2 = 1$.

To obtain x_1 when $x_2 = 1$ we need to define a phase rotation operation,

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0.01)} \end{pmatrix} \quad \text{in base 2}$$

$$R_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i(0.01)} \end{pmatrix}$$

If $x_2 = 1$, R_2^{-1} followed by an Hadamard operation (H) will return the value of x_1.

Quantum Phase Estimation

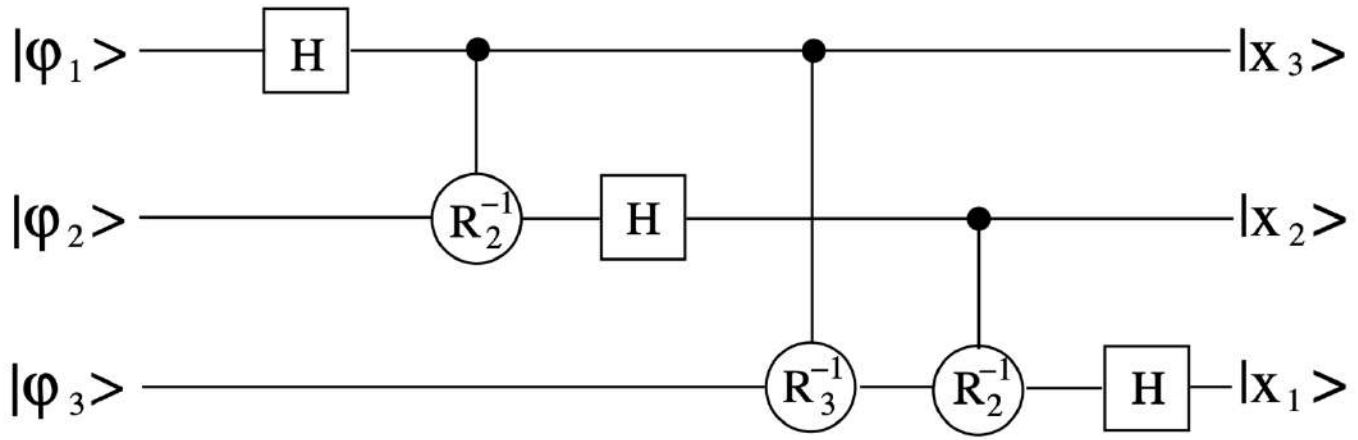
Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$

Problem : Obtain a good estimate of the phase parameter w

for a three-qubit, H on first qubit will return x_3, if $x_3 = 0$ you can find x_2, if $x_2 = 0$ find x_1 directly. If $x_3 = 1$, R_2^{-1} followed by an H will return x_2 and if $x_2 = 1$, R_3^{-1} followed by R_2^{-1} and H will return x_1. See the circuit diagram below where,

$$|\varphi_1\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_3)}|1\rangle}{\sqrt{2}} \quad ; \quad |\varphi_2\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_2 x_3)}|1\rangle}{\sqrt{2}} \quad ; \quad |\varphi_3\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_1 x_2 x_3)}|1\rangle}{\sqrt{2}}.$$



The phase estimation procedure can solve a variety of interesting problems.

Order-finding problem

and

factoring problem

These two are equivalent to each other

Useful inputs from number theory :

- Order of an element x in a group is the least integer r, such that $x^r = 1_G$
- *Order-finding :* Given x and n, $x < n$ and gcd $(x, n) = 1$, the order of x in $\mathbb{Z}_n$ is the least positive integer r such that $x^r = 1 \pmod{n}$

Shor's factoring algorithm

Factoring : given $n = PQ$, find factor P and Q

Best algorithm - $2^{O(L^{1/3})}$; L- number of digits

The fastest classical computers can factor the number with approximately 100 digits

Shor's Factoring Algorithm - $O(L^2)$ [Shor, 1994]

Ref : Ekert and Jozsa, Rev. Mod. Phys. 68, 733 (1996) along with Nielsen and Chuang

When do we need Quantum algorithms?

1. If n is prime number : factors are 1 and n
2. If n is even number : one of the factor is 2
3. If $n = p^c$ (power of prime number) : one of the factor is p

Shor's factoring algorithm

4. If n is none of the above : choose a random number $x < n$

   (a) If gcd $(x, n) = d > 1$: one of the factor is d.

   (b) If gcd $(x, n) = 1$: That is, when x and n are co-prime, solution is non-trivial. Use quantum computer to find the order r of x mod n

Look for order finding algorithm

5. If r is even and $x^{r/2} \neq \pm 1 (\text{mod } n)$: Find gcd $(x^{\frac{r}{2}} - 1, n) > 1$ and gcd $(x^{\frac{r}{2}} + 1, n) > 1$, one of them is non-trivial factor of n

6. If r is odd return to step 4 and choose and other number x.

Useful inputs from number theory :

- Order of an element x in a group is the least integer r, such that $x^r = 1_G$
- *Order-finding :* Given x and n, $x < n$ and gcd $(x, n) = 1$, the order of x in $\mathbb{Z}_n$ is the least positive integer r such that $x^r = 1 \pmod{n}$
- If n is a non-prime number and $y \neq \pm 1 \pmod{n}$ is a solution of $y^2 = 1 \pmod{n}$, one of the gcd $(y-1, n)$ and gcd $(y+1, n)$ is a non-trivial factor of n.
- If gcd $(x, n) = 1$, x has an even order r $[x^r = 1 \pmod{n}]$. Therefore, $\equiv x^{r/2} \pmod{n} \neq \pm 1 \pmod{n}$ is the solution of x^r and one of the gcd $(x^{r/2} - 1, n)$ and gcd $(x^{r/2} + 1, n)$ is a non-trivial factor of n.

Order-finding algorithm

Create a quantum register and partition it into two sets, register 1 (source) and register 2 (target). Pick a integer $q = 2^k$ such that $n^2 \leq q < 2n^2$. Register one must have enough qubits (k) to store a number $(q-1)$. Register 2 (target) must have at least $N = log_2 n$ qubits, so that it can store $(n-1)$ or more basis states. Note that the total number of qubits required is then given by the sum of $k \leq 1 + 2\log_2 n$ and $N \leq \log_2 n$.

1. Both the registrar are initialized in the state $|0\rangle \otimes |0\rangle$.

2. Load register 1 with an equally weighted superposition of all integers from 0 to $(q-1)$. The total state of the quantum memory register at this point is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle$$

3. Apply a gate U_x (transformation) that implements $a \longrightarrow f(a) = x^a \bmod n$ to the content of source registrar 1 and store the result in register 2. Note f is distinct on $[0, r-1]$ and $f(a)$ will have r as its smallest period (see Nielsen and Chuang page-228). The state of the quantum memory register at this point is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod n\rangle$$

Here $q > n^2$ values of the function $f(a)$ are computed in parallel. Since $r < n$, the period r must manifest itself in the resulting sequence of function values now stored in the second register. So there can only be r different function values.

4. Measure the second register. When we measure, we must get some value which has to be one of the r distinct values of $f(a)$. Suppose it is $f(a_0)$. Then all superposed states of the register 1 inconsistent with this measured value must disappear. For simplicity, we shall restrict ourselves first to the case where $q = mr$, i.e., there are m different values of a which have the same value of $f(a)$. Then exactly q/r states of register 1 will contribute to the measured state of register 2, and after this measurement the combined state of the two registers must be given by

$$\frac{1}{\sqrt{q/r}} \sum_{z=0}^{q/r-1} |zr + a_0\rangle |f(a_0)\rangle$$

We now have a periodic superposition of state in register 1, with period r. From now on second registrar is irrelevant and can be dropped from the discussion.

5. First registrar has a periodic superposition whose period is the value we want to compute. This can't be done by simply measuring first registrar directly. Instead, we apply QFT modulo q to the state :

$$\text{QFT} \ :|\phi_{a_0}\rangle = \frac{1}{\sqrt{q/r}} \sum_{z=0}^{q/r-1} |zr + a_0\rangle \quad \longrightarrow \frac{1}{\sqrt{r}} \sum_{t=0}^{r-1} \omega^{ta_0} |t\frac{q}{r}\rangle$$

where ω is a primitive rth root of unity, $\omega = e^{\frac{2\pi i}{r}}$

6. Now we measure register 1. The measurement gives us a value $C = t\frac{q}{r}$ where t is a random number between 0 and $r-1$. Now we have q, C, and hence also the ratio $C/q = t/r$. If gcd $(t, r) = 1$, we can reduce the ratio C/q to an irreducible fraction, e.g., $1/r$. Since t is chosen at random in the measurement, then the probability that gcd $(t, r) = 1$ is greater than $1/\log r$ for larger values of r (see Appendix A.3 in Ekert and Jozsa, RMP 68, 733 (1996)). So one can repeat it and it is easy to see that with big probability gcd $(k, \frac{q}{r}) = 1$. Then by repeating the calculation $O(\log r) < O(\log n)$ times, one can amplify the success probability to as close to one as desired. So we have an efcient determination of the order r.

Once we know the order, we can find the factors

Quantum Computation and Algorithms

Chandrashekar, QT 207 November 2025 , IISc

Quantum Computer : A device that uses a quantum mechanical representation of information to perform calculations. Information in quantum computers is stored in qbits and the states can be represented by l_2 normalized vectors in complex vector space,

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle$$

$a_x \in C$ satisfies $\sum_{x\in\{0,1\}^n} |a_x|^2 = 1$ and basis of state $|x\rangle$ is computation basis.
A vector is l_1 normalized if its integral over all space = 1 and l_2 if its integral of function times complex conjugate =1.

For a finite set S, the normalized uniform superposition of its elements can be written as

$$|S\rangle = \frac{1}{\|S\|}\sum_{s\ \in S} |s\rangle.$$

If quantum computer stores state $|\psi\rangle$ in one register and $|\phi\rangle$ in another register the state can be written as

$$|\psi\rangle \otimes |\phi\rangle \equiv |\psi\rangle|\phi\rangle \equiv |\psi, \phi\rangle$$

Single and two qubit operations

Identity : $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Pauli x : $\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Pauli y : $\sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Pauli z : $\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Hadamard : $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\pi/8$ Phase : $T_{\pi/8} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

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

I. PHASE KICK-BACK TO CONTROL REGISTER

Phase Kick-Back using CNOT operation

$$\text{CNOT} \ : \ |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\text{CNOT} \ : \ |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow |1\rangle \left((-1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) = -|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\text{CNOT} \ : \ \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\text{CNOT} \ : \ |b\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow (-1)^b|b\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\text{CNOT} \ : \ (\alpha_0|0\rangle + \alpha_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow (\alpha_0|0\rangle - \alpha_0|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$\Longrightarrow$ Z-operation on control qubit (phase kick-back to control register).

More general 2 qubit operation U_f implementing an arbitrary function $f : \{0,1\} \longrightarrow \{0,1\}$ by mapping

$$U_f \ : \ |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle$$

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

Depending on the two cases : $f(x) = 0$ and $f(x) = 1$ we have

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

When control qubit is in superposition

$$U_f \ : \ (\alpha_0|0\rangle + \alpha_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \longrightarrow ((-1)^{f(0)}\alpha_0|0\rangle + (-1)^{f(1)}\alpha_1|1\rangle) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

You can notice that the state of the second registrar $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenvector of U_f and the eigenvalue $(-1)^{f(x)}$ is kicked back in front of the control registrar. This technique of inputting an eigenstate to the target qubit of an operator and associating the eigenvalue with the state of the control register will be very useful in eigenvalue estimation.

Note : For Deutsch, Deutsch-Jozsa and Simon's algorithms refer :

(1) *Quantum Computation and Quantum Information*, Nielsen and Chuang

(2) *An Introduction to Quantum Computing*, Kaye, Laflamme and Mosca

II. QUANTUM PHASE ESTIMATION

Hadamard operation is self-inverse operation (It does the opposite as well) and it can be used to encode information into the phases.

$$H|x\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^x|1\rangle\right] = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle.$$

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

The value of x is encoded into the relative phases between the basis states $|0\rangle$ and $|1\rangle$. Hadamard operation on an $n-$qubit basis state is given by

$$H^{\otimes n}|X\rangle = \frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle.$$

Information about the value of X is encoded into the phases $(-1)^{X\cdot Y}$.

$$H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{Y\in\{0,1\}^n}(-1)^{X\cdot Y}|Y\rangle\right) = H^{\otimes n}(H^{\otimes n}|X\rangle) = (H^{\otimes n}H^{\otimes n})|X\rangle = \mathbb{1}|X\rangle.$$

Note that $(-1)^{X\cdot Y}$ are phases of specific form. General form is a complex number $e^{2\pi i\omega}$ for any real number $\omega \in (0,1)$ (phase "-1" corresponds to $\omega = \frac{1}{2}$). The $n-$qubit Hadamard operation is not able to fully access information that is encoded in more general ways.

Useful notations and identity

Notation for binary fraction :

$$\omega = 0\ .\ x_1x_2x_3\cdots\cdots = \frac{x_1}{2} + \frac{x_2}{2^2} + \frac{x_3}{2^3} + \cdots\cdots$$

similarly, $\quad 2^k\omega = x_1x_2x_3\cdots x_k\ .\ x_{k+1}x_{k+2}\cdots$ and $e^{2\pi ik} = 1$ for any k,

$$\begin{aligned} e^{2\pi i(2^k\omega)} &= \exp[2\pi i(x_1x_2x_3\cdots x_k\ .\ x_{k+1}x_{k+2}\cdots)] \\ &= \exp[2\pi i(x_1x_2x_3\cdots x_k)]\exp[2\pi i(x_{k+1}x_{k+2}\cdots)] = \exp[2\pi i(0.x_{k+1}x_{k+2}\cdots\cdots)] \end{aligned}$$

$$0\ .\ x_lx_{l+1}x_{l+2}\cdots\cdots x_n = \frac{x_l}{2} + \frac{x_{l+1}^2}{2^2} + \frac{x_{l+2}^3}{2^3} + \cdots\cdots + \frac{x_n}{2^{n-l+1}}$$

Product representation :

$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^{n-1}} e^{2\pi i\omega y}|y\rangle = \frac{|0\rangle + e^{2\pi i(2^{n-1}\omega)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(2^{n-2}\omega)}|1\rangle}{\sqrt{2}} \otimes \cdots\cdots \otimes \frac{|0\rangle + e^{2\pi i(\omega)}|1\rangle}{\sqrt{2}}$$

$$= \frac{|0\rangle + e^{2\pi i(0\ .\ x_nx_{n+1}\cdots\cdots)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0\ .\ x_{n-1}x_nx_{n+1}\cdots\cdots)}|1\rangle}{\sqrt{2}} \otimes \cdots\cdots \otimes \frac{|0\rangle + e^{2\pi i(0\ .\ x_1x_2x_3\cdots\cdots)}|1\rangle}{\sqrt{2}}$$

Algorithm :

Input : The state $\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{2\pi i\omega y}|y\rangle$

Problem : Obtain a good estimate of the phase parameter w

If the input is one-qubit ($n = 1$), $\omega = 0\ .\ x_1$ then we get

$$\frac{1}{\sqrt{2}}\sum_{y=0}^{1} e^{2\pi i(0\ .\ x_1)y}|y\rangle = \frac{1}{\sqrt{2}}\sum_{y=0}^{1} e^{2\pi i\left(\frac{x_1}{2}\right)y}|y\rangle = \frac{1}{\sqrt{2}}\sum_{y=0}^{1} e^{\pi i(x_1 y)}|y\rangle$$

$$= \frac{1}{\sqrt{2}}\sum_{y=1}^{1}(-1)^{x_1 y}|y\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}|y\rangle\right)$$

You can recall that Hadamard operation on the preceding expression will return you the value of x_1 and hence the value of ω for one-qubit.

When we have a two qubit state ($n = 2$), $\omega = 0\ .\ x_1x_2$ then using product representation we get

$$\frac{1}{\sqrt{2^2}}\sum_{y=0}^{3} e^{2\pi i(\omega)y}|y\rangle = \frac{1}{\sqrt{2^2}}\sum_{y=0}^{3} e^{2\pi i(0\ .\ x_1x_2)y}|y\rangle \ = \ \frac{|0\rangle + e^{2\pi i(0\ .\ x_2)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0\ .\ x_1x_2)}|1\rangle}{\sqrt{2}}$$

Hadamard operation on the first qubit will return the value for x_2. If $x_2 = 0$ the value of x_1 can be obtained but not if $x_2 = 1$. To obtain x_1 when $x_2 = 1$ we need to define a phase rotation operation,

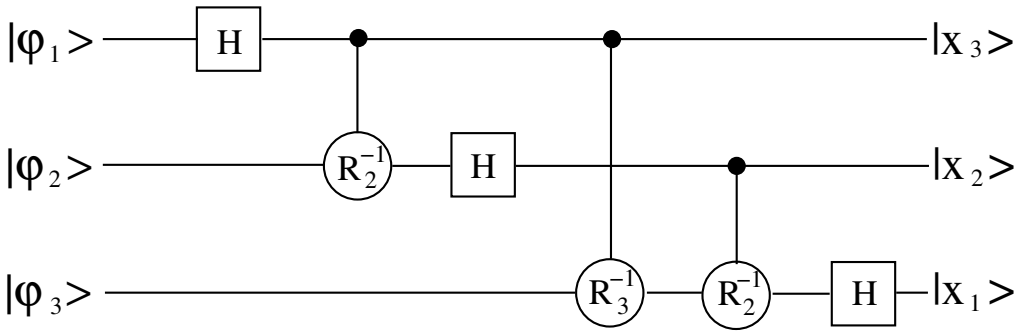
$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0.01)} \end{pmatrix} \qquad \text{in base } 2$$

and

$$R_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i(0.01)} \end{pmatrix}$$

If $x_2 = 1$, R_2^{-1} followed by an Hadamard operation (H) will return the value of x_1. Similarly for a three-qubit, H on first qubit will return x_3, if $x_3 = 0$ you can find x_2, if $x_2 = 0$ find x_1 directly. If $x_3 = 1$, R_2^{-1} followed by an H will return x_2 and if $x_2 = 1$, R_3^{-1} followed by R_2^{-1} and H will return x_1. See the circuit diagram below where,

$$|\varphi_1\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_3)}|1\rangle}{\sqrt{2}} \ \ ; \ \ |\varphi_2\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_2x_3)}|1\rangle}{\sqrt{2}} \ \ ; \ \ |\varphi_3\rangle = \frac{|0\rangle + e^{2\pi i(0\ .\ x_1x_2x_3)}|1\rangle}{\sqrt{2}}.$$



Exercise 1 : Expand the n qubit state

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$$

with $|0\rangle$ and $|1\rangle$ as computation basis in tensor product representation.

III. QUANTUM FOURIER TRANSFORM

Quantum Fourier Transform (QFT) is a unitary *Discrete Fourier Transform* (DFT) upon the quantum state. DFT of a discrete function $f_1, ..., f_N$ is given by

$$\tilde{f}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} f_j,$$

where $f_0, f_1, f_2, ..., f_{N-1}$ and $\tilde{f}_1, \tilde{f}_2, ..., \tilde{f}_{N-1}$ are the input and output functions, respectively.

The inverse transform is

$$f_j \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j k/N} \tilde{f}_k.$$

In QFT we do a DFT on the amplitudes of a quantum state :

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

amplitudes y_k are DFT of amplitudes x_j.

Exercise 2 : Find an operator $\hat{F}$ which transform a state into its DFT and show that its unitary.

IV. PERIODIC STATES

A superposition of state in the form

$$|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr + b\rangle,$$

is a periodic superposition of the state with **period** r, **offset** l, and m repetitions of the period.

Exercise 3 : Performing DFT on the above periodic state, $|\phi_{r,b}\rangle \longrightarrow |\tilde{\phi}\rangle$, obtain $|\tilde{\phi}\rangle$

V. SHOR'S FACTORING QUANTUM ALGORITHM

Factoring : given $n = PQ$, find factor P and Q

Best algorithm - $2^{O(L^{1/3})}$; L- number of digits

The fastest classical computers can factor the number with approximately 100 digits

Shor's Factoring Algorithm - $O(L^2)$ [Shor, 1994]

Ref : Ekert and Jozsa, Rev. Mod. Phys. 68, 733 (1996) along with Nielsen and Chuang

Summery of Shor's Algorithm

1. If n is prime number : factors are 1 and n
2. If n is even number : one of the factor is 2
3. If $n = p^c$ (power of prime number) : one of the factor is p
4. If n is none of the above : choose a random number $x < n$
   (a) If gcd $(x, n) = d > 1$: one of the factor is d.
   (b) If gcd $(x, n) = 1$: That is, when x and n are co-prime, solution is non-trivial. Use quantum computer to find the order r of x mod n (*Look below for* **order-finding algorithm**)
5. If r is even and $x^{r/2} \neq \pm 1 (\text{mod } n)$: Find gcd $(x^{\frac{r}{2}} - 1, n) > 1$ and gcd $(x^{\frac{r}{2}} + 1, n) > 1$, one of them is non-trivial factor of n

6. If r is odd return to step 4 and choose and other number x.

Useful inputs from number theory :

- Order of an element x in a group is the least integer r, such that $x^r = 1_G$
- *Order-finding :* Given x and n, $x < n$ and gcd $(x, n) = 1$, the order of x in $\mathbb{Z}_n$ is the least positive integer r such that $x^r = 1 \pmod{n}$
- If n is a non-prime number and $y \neq \pm 1 \pmod{n}$ is a solution of $y^2 = 1 \pmod{n}$, one of the gcd $(y-1, n)$ and gcd $(y+1, n)$ is a non-trivial factor of n.
- If gcd $(x, n) = 1$, x has an even order r $[x^r = 1 \pmod{n}]$. Therefore, $\equiv x^{r/2} \pmod{n} \neq \pm 1 \pmod{n}$ is the solution of x^r and one of the gcd $(x^{r/2} - 1, n)$ and gcd $(x^{r/2} + 1, n)$ is a non-trivial factor of n.

Order-finding algorithm

Create a quantum register and partition it into two sets, register 1 (source) and register 2 (target). Pick a integer $q = 2^k$ such that $n^2 \leq q < 2n^2$. Register one must have enough qubits (k) to store a number $(q-1)$. Register 2 (target) must have at least $N = log_2 n$ qubits, so that it can store $(n-1)$ or more basis states. Note that the total number of qubits required is then given by the sum of $k \leq 1 + 2\log_2 n$ and $N \leq \log_2 n$.

1. Both the registrar are initialized in the state $|0\rangle \otimes |0\rangle$.
2. Load register 1 with an equally weighted superposition of all integers from 0 to $(q-1)$. The total state of the quantum memory register at this point is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle$$

   Exercise 4 : Show that you can obtain the preceding expression by applying k qubit Hadamard operation and also by applying Fourier transform. What does this tell you about the relation between Hadamard and Fourier transform?

3. Apply a gate U_x (transformation) that implements $a \longrightarrow f(a) = x^a \bmod n$ to the content of source registrar 1 and store the result in register 2. Note f is distinct on

$[0, r-1]$ and $f(a)$ will have r as its smallest period (see Nielsen and Chuang page-228). The state of the quantum memory register at this point is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod n\rangle$$

Here $q > n^2$ values of the function $f(a)$ are computed in parallel. Since $r < n$, the period r must manifest itself in the resulting sequence of function values now stored in the second register. So there can only be r different function values.

4. Measure the second register. When we measure, we must get some value which has to be one of the r distinct values of $f(a)$. Suppose it is $f(a_0)$. Then all superposed states of the register 1 inconsistent with this measured value must disappear. For simplicity, we shall restrict ourselves first to the case where $q = mr$, i.e., there are m different values of a which have the same value of $f(a)$. Then exactly q/r states of register 1 will contribute to the measured state of register 2, and after this measurement the combined state of the two registers must be given by

$$\frac{1}{\sqrt{q/r}} \sum_{z=0}^{q/r-1} |zr + a_0\rangle |f(a_0)\rangle$$

We now have a periodic superposition of state in register 1, with period r. From now on second registrar is irrelevant and can be dropped from the discussion.

5. First registrar has a periodic superposition whose period is the value we want to compute. This can't be done by simply measuring first registrar directly. Instead, we apply QFT modulo q to the state :

$$\text{QFT} \ : |\phi_{a_0}\rangle = \frac{1}{\sqrt{q/r}} \sum_{z=0}^{q/r-1} |zr + a_0\rangle \quad \longrightarrow \frac{1}{\sqrt{r}} \sum_{t=0}^{r-1} \omega^{ta_0} |t\frac{q}{r}\rangle$$

where ω is a primitive rth root of unity, $\omega = e^{\frac{2\pi i}{r}}$

Exercise 5 : The sum got changed from q/r terms to r terms during QFT. This was a result of destructive interference in the QFT on the state. Show how it happened ?

6. Now we measure register 1. The measurement gives us a value $C = t\frac{q}{r}$ where t is a random number between 0 and $r - 1$. Now we have q, C, and hence also the ratio

$C/q = t/r$. If gcd $(t, r) = 1$, we can reduce the ratio C/q to an irreducible fraction, e.g., $1/r$. Since t is chosen at random in the measurement, then the probability that gcd $(t, r) = 1$ is greater than $1/\log r$ for larger values of r (see Appendix A.3 in Ekert and Jozsa, RMP 68, 733 (1996)). So one can repeat it and it is easy to see that with big probability gcd $(k, \frac{q}{r}) = 1$. Then by repeating the calculation $O(\log r) < O(\log n)$ times, one can amplify the success probability to as close to one as desired. So we have an efficient determination of the order r.

VI. GROVER'S SEARCH ALGORITHM

Problem : Find i such that $x_i = 1$

Queries : ask i, get x_i

Classically : $N - 1$ queries required (worst case) [N elements in search space]

Quantum : $O(\sqrt{N})$ queries [grover, 1996]

Steps Grover's algorithm

1. Begin with the computer in state $|0\rangle^{\otimes n}$. Use Hadamard transformation to put the computer in equal superposition state,

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

2. Repeat $O(\sqrt{N})$ times the following two steps (Grover iteration)

   - Apply the Oracle O $|x\rangle \longrightarrow (-1)^{f(x)}|x\rangle$
   - Apply the operator $U_s = 2|S\rangle\langle S| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$

3. Measure the resulting state

VII. CLASSICAL RANDOM WALKS TO QUANTUM WALKS

Classical random walks are widely studied in two forms, discrete-time classical random walk (DTCRW) and Continuous-time classical random walk (CTCRW). They have been successfully used as algorithms in classical computers, to understand and model dynamics in various systems from biology to social behavior for many decades now. Its quantum version, quantum walks has also also been explored in two forms, discrete-time quantum walk (DTQW) and continuous-time quantum walk (CTQW) for over decade now.

Classical random walk : Lets first recall the structure of the discrete-time classical random walk in one-dimension. The discrete-time classical random walk takes place on the position Hilbert space $\mathcal{H}_p$ with instruction from the coin operation. A coin flip defines the direction in which the particle moves and a subsequent position shift operation moves the particle in position space. For a walk on a line, a two sided coin with *head* (H) and *tail* (T) defines the movements to the *left* and *right*, respectively.

.....	-3	-2	-1	0	1	2	3	.....

1. **Initial state :** Particle at position $x = 0$
2. **Evolution :** (Coin, Position) = (H or T, $x \in \mathbb{Z}$)
   (a) (H, x) $\Longrightarrow (x-1)$
   (b) (T, x) $\Longrightarrow (x+1)$
3. **Probability :** P_x and $\sum_x P_x = 1$

Note: Each step evolution is independent of its previous step.

A. Discrete-time quantum walk (DTQW)

The DTQW also has a very similar structure to that of its classical counterpart. The coin flip is replaced by the quantum coin operation to evolve the particle (walker) into the superposition of the basis states. The quantum coin operation is followed by the unitary

conditional shift operation which defines the direction of propagation of the particle depending on the basis state of the particle. If the particle is in superposition of its basis sate the unitary shift operation evolves the particle in the superposition of the position space. The process is iterated without resorting to intermediate measurement to implement a large number of steps. During the walk on a line, interference between the left and the right propagating amplitude results in the quadratic growth of variance with the number of steps.

DTQW in one-dimension: The DTQW on a line is defined on a Hilbert space

$$\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p,$$

where $\mathcal{H}_c$ is the *coin* Hilbert space and $\mathcal{H}_p$ is the *position* Hilbert space. For a discrete-time quantum walk in one dimension, $\mathcal{H}_c$ is spanned by the basis state (internal state) of the particle $|0\rangle$ and $|1\rangle$ and $\mathcal{H}_p$ is spanned by the basis state of the position $|\psi_j\rangle$, where $j \in \mathbb{Z}$. One of the simple form of quantum coin operation is the Hadamard operation $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and the shift operation S can be written as

$$S = |0\rangle\langle 0| \otimes \sum_{j\in\mathbb{Z}} |\psi_{j-1}\rangle\langle\psi_j| + |1\rangle\langle 1| \otimes \sum_{j\in\mathbb{Z}} |\psi_{j+1}\rangle\langle\psi_j|.$$

The operator S delocalizes the wave packet in different basis states $|0\rangle$ and $|1\rangle$ over the position $(j-1)$ and $(j+1)$. To implement the DTQW on a particle at origin in state

$$|\Psi_{in}\rangle = |0\rangle \otimes |\psi_0\rangle \;\; ; \;\; |1\rangle \otimes |\psi_0\rangle \;\; ; \;\; \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \otimes |\psi_0\rangle \;\; ; \;\; \text{or any other superposition state,}$$

operation H is applied on the particle state followed by the operation S,

$$W = S(H \otimes \mathbb{1}).$$

For t step of the walk W is iterated t times, W^t without intermediate measurement. For generalized form of the DTQW evolution, Hadamard operation is replaced by $B \in U(2)$ as the quantum coin toss operation.

$$B_{\zeta,\alpha,\beta,\gamma} = e^{i\zeta} e^{i\alpha\sigma_x} e^{i\beta\sigma_y} e^{i\gamma\sigma_z},$$

where σ_x, σ_y and σ_z are the Pauli spin operators. Parameters of the coin operations $\zeta, \alpha, \beta, \gamma$ gives different superposition state of the particle. Therefore, each step of the walk is implemented by $S(B_{\zeta,\alpha,\beta,\gamma} \otimes \mathbb{1})$. A three parameter SU(2) operator is an other useful form of quantum coin operation.

B. Continuous-time quantum walk (CTQW)

To define the CTQW, it is easier to first define the CTCRW and quantize it by introducing quantum amplitudes in place of classical probabilities.

The CTCRW takes place entirely in the *position* space. To illustrate, let us define CTCRW on the position space $\mathcal{H}_p$ spanned by a vertex set V of a graph G with edges set E, $G = (V, E)$. A step of the random walk can be described by a adjacency matrix A which transform the probability distribution over V, i.e.,

$$A_{j,k} = \begin{cases} 1 & (j,k) \in E \\ 0 & (j,k) \notin E \end{cases}$$

for every pair $j, k \in V$. The other important matrix associated with the graph G is the generator matrix $\mathbf{H}$ given by

$$\mathbf{H}_{j,k} = \begin{cases} d_j\gamma & j = k \\ -\gamma & (j,k) \in E \\ 0 & \text{otherwise} \end{cases},$$

where d_j is the degree of the vertex j and γ is the probability of transition between neighboring nodes per unit time.

If $P_j(t)$ denotes the probability of being at vertex j at time t then the transition on graph G is defined as the solution of differential equation

$$\frac{d}{dt}P_j(t) = -\sum_{k\in V} \mathbf{H}_{j,k}P_k(t).$$

The solution of the differential equation is given by

$$P(t) = e^{-\mathbf{H}t}P(0).$$

By replacing the probabilities P_j by quantum amplitudes $a_j(t) = \langle j|\psi(t)\rangle$ where $|j\rangle$ is spanned by the orthogonal basis of the position Hilbert space $\mathcal{H}_p$ and introducing a factor of i we obtain

$$i\frac{d}{dt}a_j(t) = \sum_{k\in V} \mathbf{H}_{j,k}a_k(t).$$

We can see that the preceding expression is the Schrödinger equation

$$i\frac{d}{dt}|\psi\rangle = \mathbf{H}|\psi\rangle.$$

Since generator matrix is an Hermitian operator, the normalization is preserved during the dynamics. The solution of the differential equation can be written in the form

$$|\psi(t)\rangle = e^{-i\mathbf{H}t}|\psi(0)\rangle.$$

Therefore, the CTQW is of the form of Schrödinger equation, a non-relativistic quantum evolution.

To implement the CTQW on a line, the position Hilbert space $\mathcal{H}_p$ can be written as a state spanned by the basis states $|\psi_j\rangle$, where $j \in \mathbb{Z}$. The Hamiltonian $\mathbf{H}$ is defined such that,

$$\mathbf{H}|\psi_j\rangle = -\gamma|\psi_{j-1}\rangle + 2\gamma|\psi_j\rangle - \gamma|\psi_{j+1}\rangle$$

and is made to evolve with time t by applying the transformation

$$U(t) = \exp(-i\mathbf{H}t).$$

The Hamiltonian $\mathbf{H}$ of the process acts as the generator matrix which will transform the probability amplitude at the rate of γ to the neighboring sites, where γ is time-independent constant.