Quantum Computing

From quantum mechanics to algorithms

Goal

- Quantum mechanics and Schrodinger’s cat
- Qubits, operators, and measurements
- The bomb tester
- Quantum operators
- A quantum algorithm

Microscale

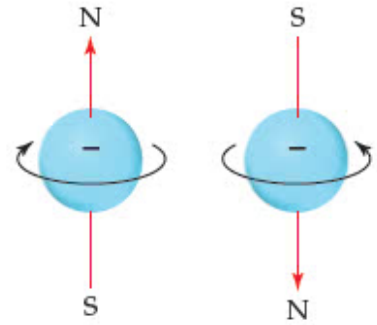
Our classical sense is dictated by physics in macroscale which includes the idea of equilibrium and second law of thermodynamics.

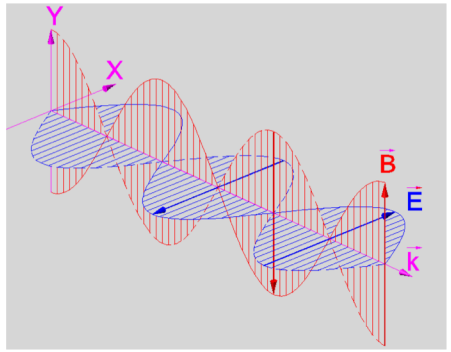
However, a quantum system is a microscale system. Equilibrium and laws of thermodynamics **do not** apply.

Wikipedia: “Quantum mechanics is a fundamental theory in physics that provides a description of the physical properties of nature at the **scale of atoms** and subatomic particles”.

Quantum properties

- Electron spin
- Photon polarization
- The principle of superposition
- Measurement
- Tensor (product state and entangle state)





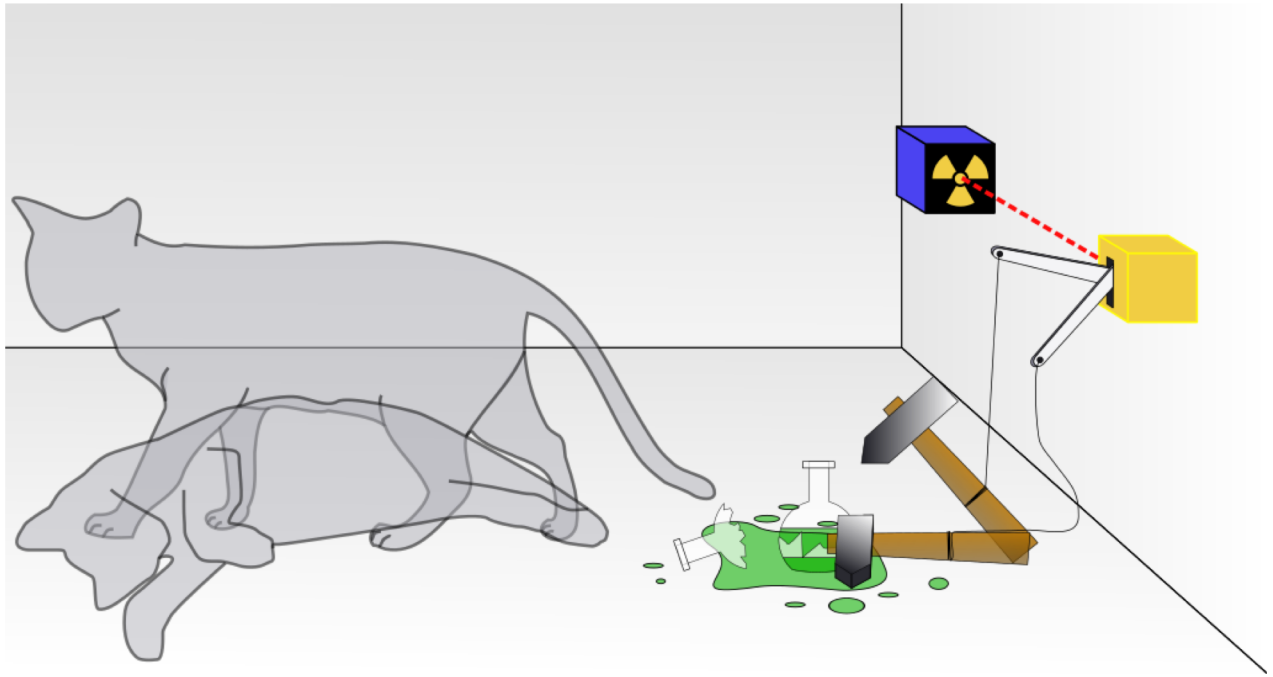
Superposition of two spin states

$$\left|\nearrow\right\rangle = a\left|\uparrow\right\rangle + b\left|\downarrow\right\rangle$$

$$|a|^2 + |b|^2 = 1$$

Schrodinger's cat

A butterfly effect that sets a macroscopic object into a superposition like a microscopic system.



Qubits

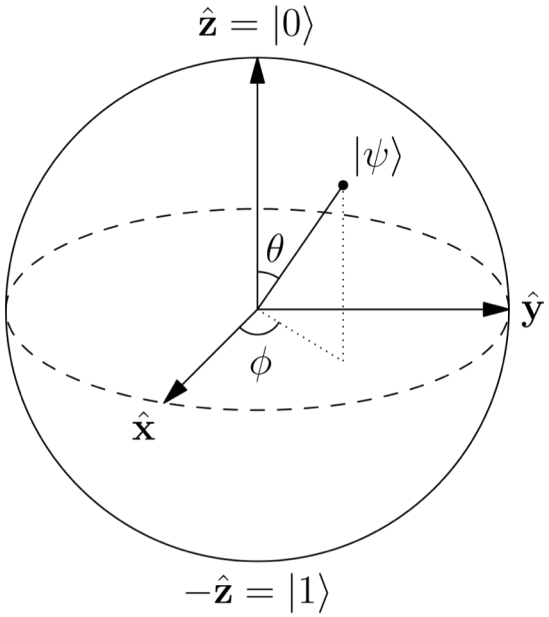
$$|\psi\rangle = \alpha_z |z+\rangle + \beta_z |z-\rangle$$

$$= \alpha_y |y+\rangle + \beta_y |y-\rangle$$

$$= \alpha_x |x+\rangle + \beta_x |x-\rangle$$

$$= \alpha |0\rangle + \beta |1\rangle \quad , \quad \text{normally} \quad |0\rangle \equiv |z+\rangle, \quad |1\rangle \equiv |z-\rangle$$

$$= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$



e.g. let $|\psi\rangle = |y+\rangle$

Then $|\psi\rangle = |y+\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle$

Operator

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$M|\psi\rangle = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

↑ operator

, M must be unitary $\left(M^\dagger M = M M^\dagger = I \right)$

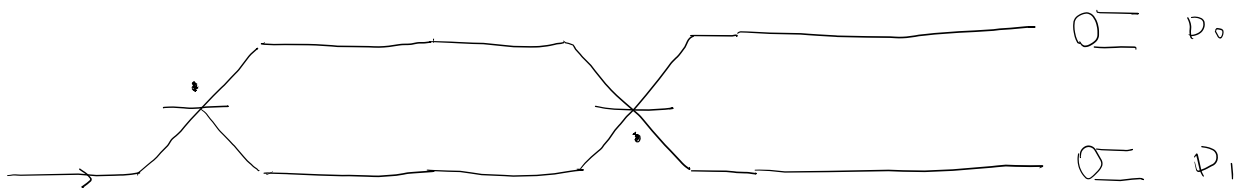
aka. $M^\dagger = M^{-1}$

Dagger $\dagger$ is transpose t plus complex conjugate $*$

$$M^\dagger = (M^t)^* = \begin{pmatrix} a & c \\ b & d \end{pmatrix}^* = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$$

Beam splitter

$$B_u = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \qquad B_\ell = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



$|\psi_0\rangle = |1\rangle$ $\quad |\psi_1\rangle = B_u|\psi_0\rangle$ $\quad |\psi_2\rangle = B_\ell|\psi_1\rangle$

$$|\psi_0\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi_1\rangle = B_u|\psi_0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|\psi_2\rangle = B_\ell|\psi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+1 \\ 1-1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

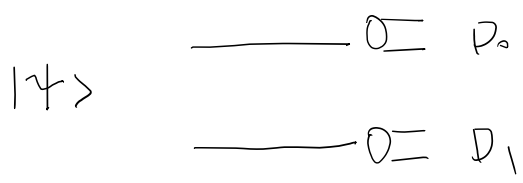
Measurements

$$|x\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\langle x| = (|x\rangle)^\dagger$$

$$= (|x\rangle^t)^*$$

$$= \begin{pmatrix} a^* & b^* \end{pmatrix}$$



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

$$P(|\psi\rangle = |0\rangle) = |\langle 0|\psi\rangle|^2$$

$$= |\langle 0|\alpha|0\rangle + \langle 0|\beta|1\rangle|^2$$

$$= |\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle|^2$$

$$= |\alpha|^2 = \alpha^*\alpha$$

$$P(|\psi\rangle = |1\rangle) = |\langle 1|\psi\rangle|^2$$

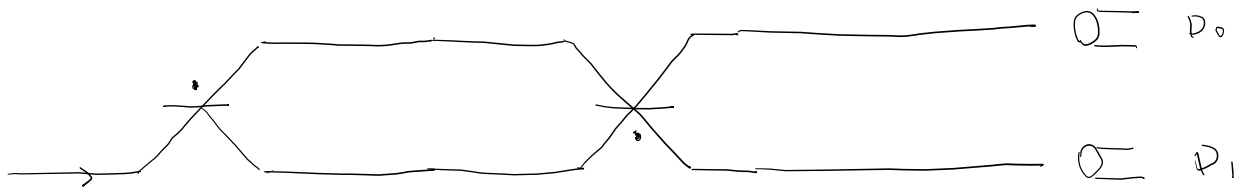
$$= |\beta|^2 = \beta^*\beta$$

$$= \left| \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right|^2$$

$$= |\alpha|^2$$

orthonormal basis

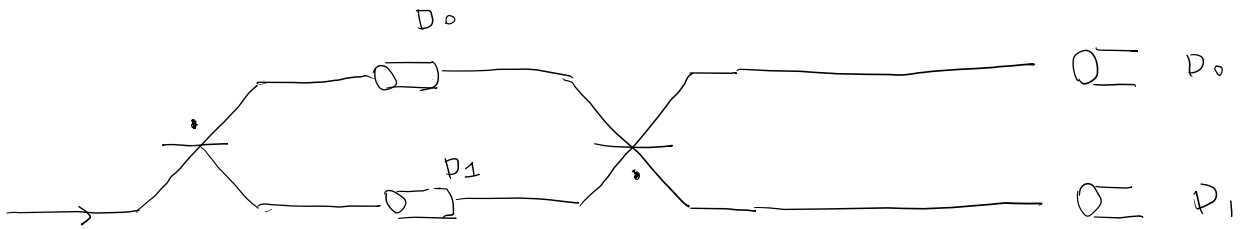
Measurement matters



$|\psi_0\rangle = |1\rangle$ $\quad |\psi_1\rangle = B_u|\psi_0\rangle$ $\quad |\psi_2\rangle = B_\ell|\psi_1\rangle$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

$$|\psi_2\rangle = \begin{pmatrix}1\\0\end{pmatrix} \rightarrow P(|\psi_2\rangle = |0\rangle) = 100\%$$



$|\psi_0\rangle = |1\rangle$ $\quad |\psi_1\rangle = B_u|\psi_0\rangle$ $\quad |\psi_2\rangle = B_\ell|\psi_1\rangle$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

$$P(|\psi_1\rangle = |0\rangle) = |\langle 0|\psi_1\rangle|^2 = \left|\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\right|^2 = \frac{1}{2}$$

$$P(|\psi_1\rangle = |1\rangle) = |\langle 1|\psi_1\rangle|^2 = \frac{1}{2}$$

↳ Measurement

50% $\quad |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ → 25% = $P(|\psi_2\rangle = |0\rangle)$, 25% = $P(|\psi_2\rangle = |1\rangle)$

50% $\quad |\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ → 25% = $P(|\psi_2\rangle = |0\rangle)$, 25% = $P(|\psi_2\rangle = |1\rangle)$

$P(|\psi_2\rangle = |0\rangle) = 50\%$

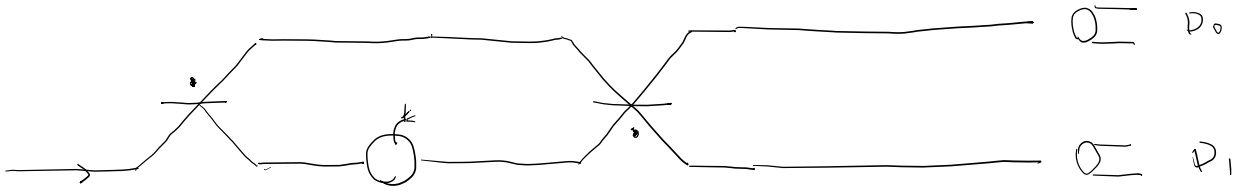
$P(|\psi_2\rangle = |1\rangle) = 50\%$

Elitzur–Vaidman bomb tester

The problem (from Wikipedia):
“Consider a collection of light-sensitive bombs, of which some are duds. When their triggers detect any light, even a single photon, the light is absorbed, and the bomb explodes. The triggers on the dud bombs have no sensor, so the photon cannot be absorbed. Thus, the dud bomb will not detect the photon and will not detonate. Is it possible to determine which bombs are functional and which are duds without detonating all of the live ones”?

Classically, the only way to check if the bomb works is to send a photon through the detector. If the bomb explodes, then the bomb was working. Otherwise, the bomb is dud. There is no way to tell if a bomb works without triggering it.

Elitzur–Vaidman bomb tester



If the bomb is working, then it does a measurement on $|\psi_1\rangle$ which change the state of $|\psi_1\rangle$.
If the bomb is dud, $|\psi_1\rangle$ remains the state of superposition.

Bomb is dud

outcome	P
photon reaches D_0	1
photon reaches D_1	0
bomb explodes	0

Bomb is working

outcome	P
photon reaches D_0	1/4
photon reaches D_1	1/4
bomb explodes	1/2

This experiment demonstrates the potential of quantum system. If we can exploit such properties, we can outperform classical systems.

Half time questions

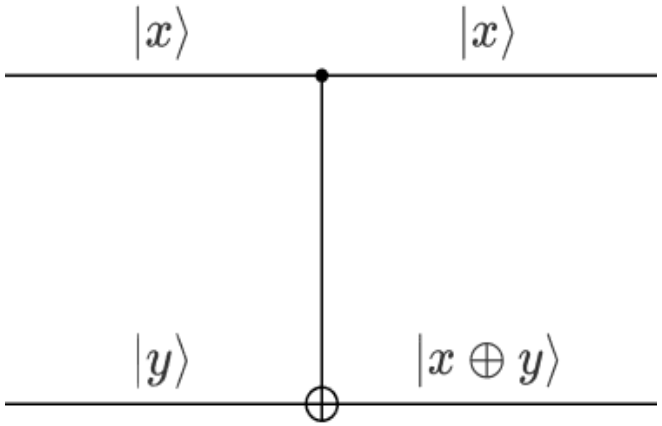
Tensor product of two-level states

For one bit, $0 = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $1 = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$.

For two bits, $|0\rangle\otimes|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |00\rangle$.

$$00 = |00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, 01 = |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, 10 = |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, 11 = |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Controlled-Not gate



$\|x_{in}\rangle$	$\|y\rangle$	$\|x_{out}\rangle$	$\|x \oplus y\rangle$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

In a classical sense, if x is 0, does noting on y.
However, if x is 1, turns y into not(y).

Let $|x\rangle \otimes |y\rangle = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix}$

Controlled-Not gate: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ v_4 \\ v_3 \end{pmatrix}$

$$CN|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle$$

$$CN|01\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

$$CN|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

$$CN|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

Hadamard gate

Hadamard gate turns a discrete state of n qubits into a superposition that has equal probability across all bases.
It is a generalized even beam splitter.

$$H^{\otimes 1} = \frac{1}{\sqrt{2}} \begin{pmatrix} (-1)^{0\wedge 0} & (-1)^{0\wedge 1} \\ (-1)^{1\wedge 0} & (-1)^{1\wedge 1} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

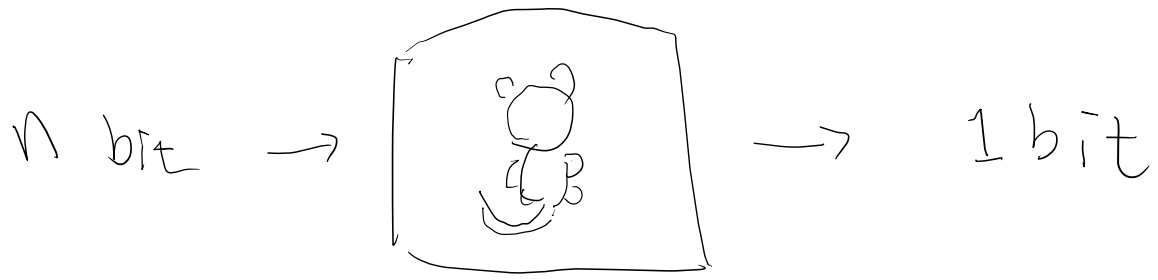
$$H^{\otimes 2} = \frac{1}{\sqrt{4}} \begin{pmatrix} (-1)^{0\wedge 0\oplus 0\wedge 0} & (-1)^{0\wedge 0\oplus 0\wedge 1} & (-1)^{0\wedge 1\oplus 0\wedge 0} & (-1)^{0\wedge 1\oplus 0\wedge 1} \\ (-1)^{0\wedge 0\oplus 1\wedge 0} & (-1)^{0\wedge 0\oplus 1\wedge 1} & (-1)^{0\wedge 1\oplus 1\wedge 0} & (-1)^{0\wedge 1\oplus 1\wedge 1} \\ (-1)^{1\wedge 0\oplus 0\wedge 0} & (-1)^{1\wedge 0\oplus 0\wedge 1} & (-1)^{1\wedge 1\oplus 0\wedge 0} & (-1)^{1\wedge 1\oplus 0\wedge 1} \\ (-1)^{1\wedge 0\oplus 1\wedge 0} & (-1)^{1\wedge 0\oplus 1\wedge 1} & (-1)^{1\wedge 1\oplus 1\wedge 0} & (-1)^{1\wedge 1\oplus 1\wedge 1} \end{pmatrix}$$

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

Balanced function problem

Let’s consider a problem. There is a function operates by an intelligent monkey. The input of the function is a N bits string. The intelligent monkey performs a secret algorithm and give a 1-bit output. We want to know if the function is balanced or constant.

(Assume the function is either balanced or constant.)



balanced: $f(0) = 0, f(1) = 1$

balanced: $f(0) = 1, f(1) = 0$

constant: $f(0) = 1, f(1) = 1,$

constant: $f(0) = 0, f(1) = 0,$

1 bit input example

Classical solution

We need to test just more than half of the domain and compare the output to see if they are all the same.

If all output are the same, then the function is constant.

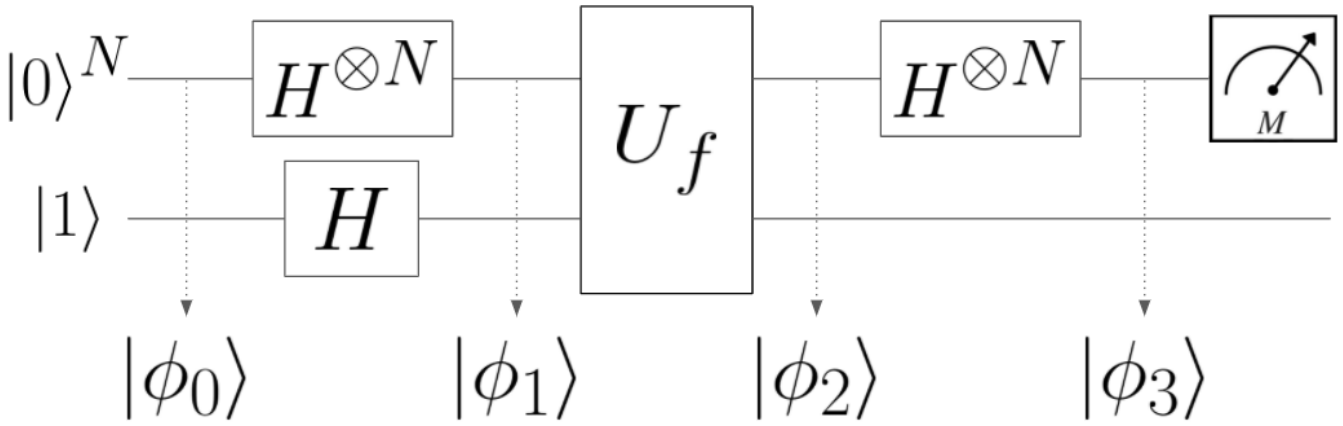
If at least one output is different than another, then the function is balanced.

For a conventional deterministic algorithm, $k = 2^{n-1} + 1$ is needed to decide weather a function is balanced. (n bits input)

$O(g) = 2^n$.

Deutsch-Jozsa Quantum Algorithm

Assume the intelligent monkey function is quantized such that it can handle qubits and superpositions.



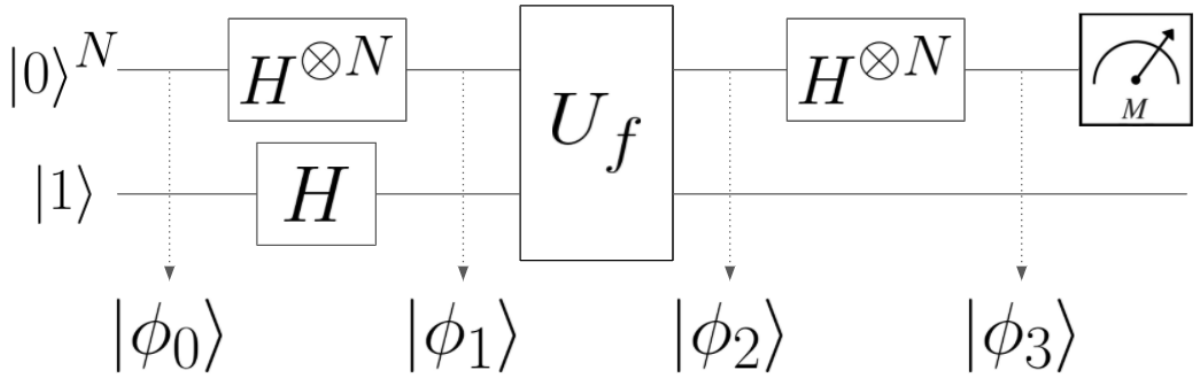
For simplicity, the calculation will be performed using n = 1.

Deutsch-Jozsa Quantum Algorithm

- $|\varphi_0\rangle = \Big|0,1\rangle = |0\rangle|1\rangle$

- $|\varphi_1\rangle = (H|0\rangle)(H|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

$$= \frac{1}{2}(+|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle) = \begin{matrix}00\\01\\10\\11\end{matrix}\begin{pmatrix}+1/2\\-1/2\\+1/2\\-1/2\end{pmatrix}$$



Deutsch-Jozsa Quantum Algorithm

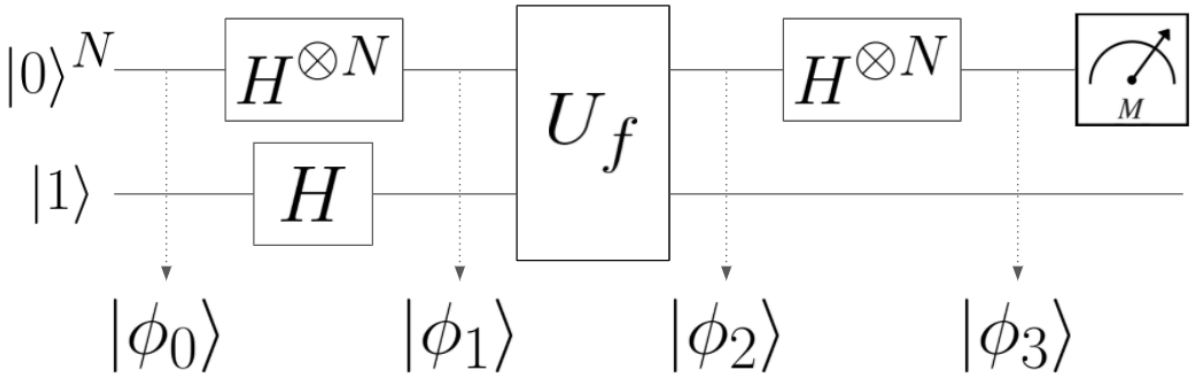
- $|\varphi_2\rangle = \left(\frac{(-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

  If $f(0)=0, f(1)=0$, then $|\varphi_2\rangle = \left(\frac{+|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

  If $f(0)=1, f(1)=1$, then $|\varphi_2\rangle = \left(\frac{-|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

  If $f(0)=0, f(1)=1$, then $|\varphi_2\rangle = \left(\frac{+|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

  If $f(0)=1, f(1)=0$, then $|\varphi_2\rangle = \left(\frac{-|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$



- So, $|\varphi_2\rangle = \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, if the function f is constant.

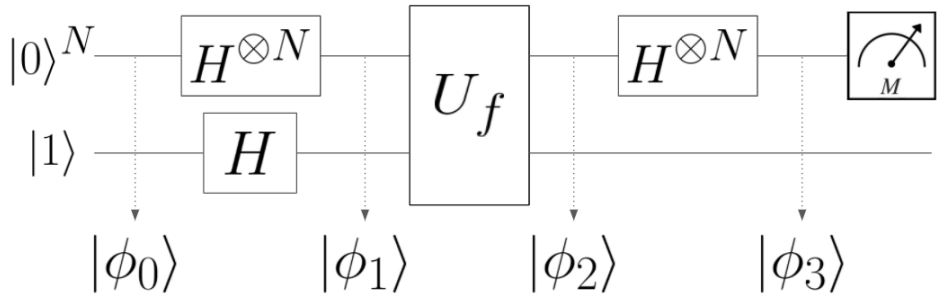
  $|\varphi_2\rangle = \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, if the function f is balanced.

Deutsch-Jozsa Quantum Algorithm

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

- Therefore, $|\varphi_3\rangle = \pm|0\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$, if the function f is constant.

  $|\varphi_3\rangle = \pm|1\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$, if the function f is balanced.



- As a result, by measuring the state of the top qubit, we can instantly find out if the function f is constant or balanced. With the technique of quantum computing, we don't need to repeat the experiment anymore. The time complexity is reduced to constant time $O(g) = c$.

Quantum algorithm learning list

- Deutsch’s Algorithm
- The Deutsch-Jozsa Algorithm
- Simon’s Periodicity Algorithm (Check out my report)
- Grover’s Search Algorithm
- Shor’s Factoring Algorithm
  - Destroy the current internet security protocol aka. Hash function

Famous quantum computer

- 2016 IBM Q: 5 qubit electron-based; open to operate
- 2019 Google's Sycamore: 53 qubit electron-based
- 2020 Jiuzhang 九章: 76 qubit photon-based
  - Gaussian Boson sampling task
- IBM promises 1000-qubit quantum computer by 2023