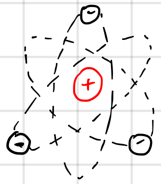
Quantum Computing

波粒二象性 (wave-particle duality)

光的干涉 ⇒ 光由 { tiny particles / wave } 组成，爱因斯坦后称这种 tiny articles 为 photons (光子)

借此 新的 atom (原子) 的结构被提出.



⊕ : nucleus (核)，带正电

⊖ : electrons (电子)，带负电

quantum: a minimum quantity of energy (复数形式是 quanta)

$E_2 - E_1 = \Delta E = hf$

⇓

电子由一个 orbit (轨道) 跃迁至另一个时产生的能量，是不可分割的

(电子可以发射或吸收一个量子的能量，从一个能级跃迁至另一个能级)

Heisenberg's uncertainty principle (不确定性定理):

The more precisely the position of some particle is determined, the less precisely its momentum can be known, and vice versa

Δx 越小

位置越能够准确确定

动量越不能准确知道.

ΔP 越大

The position and velocity (速度) of a particle can't both be measured exactly.

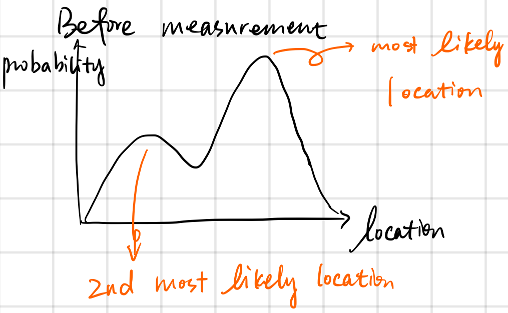
$$\Delta x \, \Delta p \geq \frac{h}{4\pi} = \frac{\hbar}{2}$$

位置不确定性 动量不确定性

Copenhagen Interpretation 哥本哈根诠释

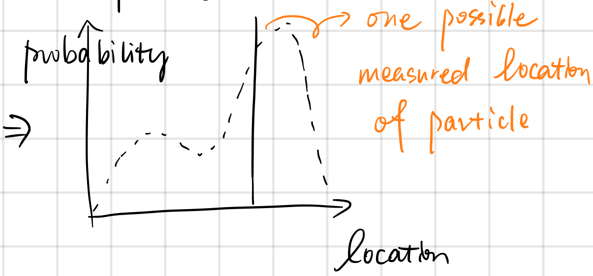
A quantum article doesn't exist in one state or another, instead, it's in all of its possible states simultaneously. It's only when we observe this state that a quantum particle is forced to choose one probability, and that's the state we observe.

Before measurement

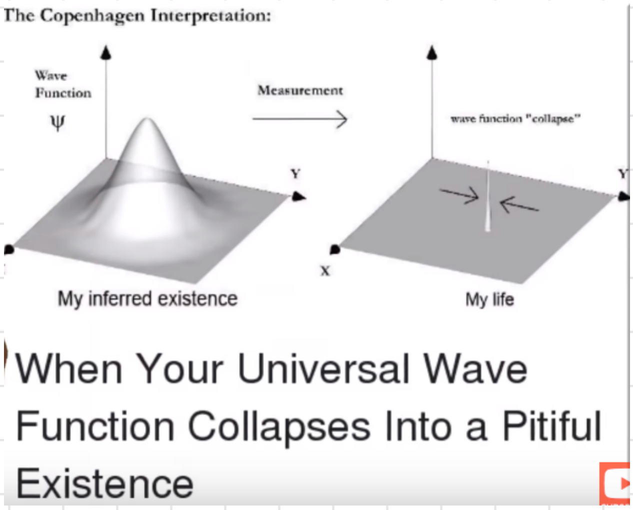


⇒

After measurement



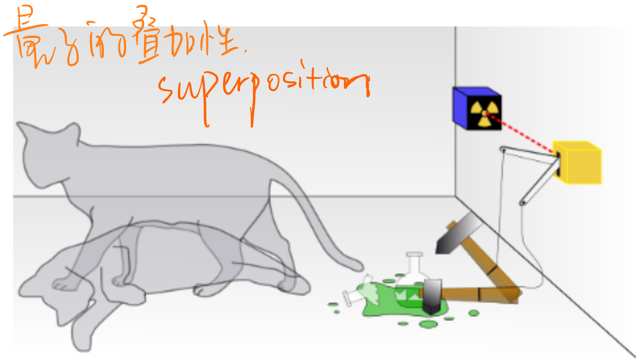
波函数：用来计算粒子在某位置或处于某种运动状态的机率。测量的动作造成了波函数塌缩，原本的量子态机率地塌缩成一个测量允许的量子态。



哥本哈根诠释可以被 Schrodinger's cat theoritically proven.（薛定谔的猫）

theoratical experiment

量子的叠加性 superposition



把一只猫、一个装有氰化氢气体的玻璃烧瓶和放射性物质放进封闭的盒子里。当盒子内的监控器侦测到衰变粒子时，就会打破烧瓶，杀死这只猫。根据量子力学的哥本哈根诠释，在实验进行一段时间后，猫会处于又活又死的叠加态。可是，假若实验者观察盒子内部，他会观察到一只活猫或一只死猫，而不是同时处于活状态与死状态的猫。这事实引起一个谜题：到底量子叠加是在甚么时候终止，并且塌缩成两种可能状态中的一种状态?

在打开箱子之前，猫有0.5的可能性活，
有0.5的可能性死

Quantum entanglement：量子缠结

A phenomena by which the quantum states of two or more objects can be described in reference to each other. You can't describe the state of one without referencing the other, and that same property applies even when these particles are seperated by any amount of space.

爱因斯坦称之为 spooky action-at-a-distance.

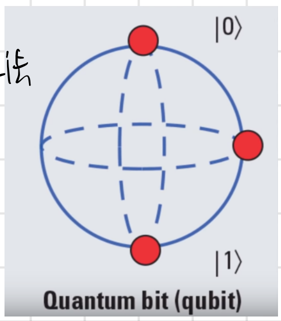
此词语的由来是来自物理学中的远距作用，是指一个物体在和另一物体中间没有粒子交换的情形下，影响另一物体的现象，量子力学的量子缠结就是远距作用的一个例子，爱因斯坦将此称为“鬼魅似的远距作用”（spooky action-at-a-distance）。

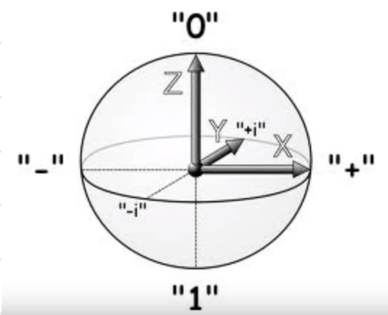
Simulating Physics with Computers. 很重要的论文!!

① 传统 computer: 0-1 binary data

② Quantum computer:

可以 { speed up 已有算法
创造新算法





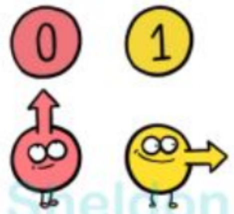
Qubit can occupy 2 states simultaneously.

如果两个状态是一个体系允许出现的状态，它们的任意线性叠加也是这个体系允许出现的状态.

While a quantum computer is running, its qubits can be infinitely many superpositions between 0 and 1. When a qubit is in superposition, it has some probability of being in state 0 and some probability of being in state 1.

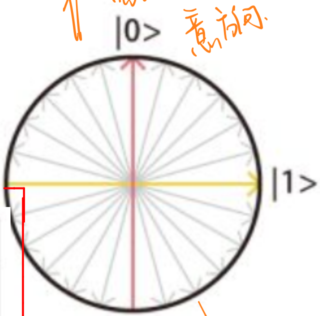
superposition 是脆弱的，如果我们观察它，就会collapse 成为0或1.

狄拉克符号："$|\rangle$" 表示量子力学中的状态。若一个体系能处于 $|0\rangle$ 和 $|1\rangle$，则它也能处于 $a|0\rangle+b|1\rangle$（任意线性叠加）.



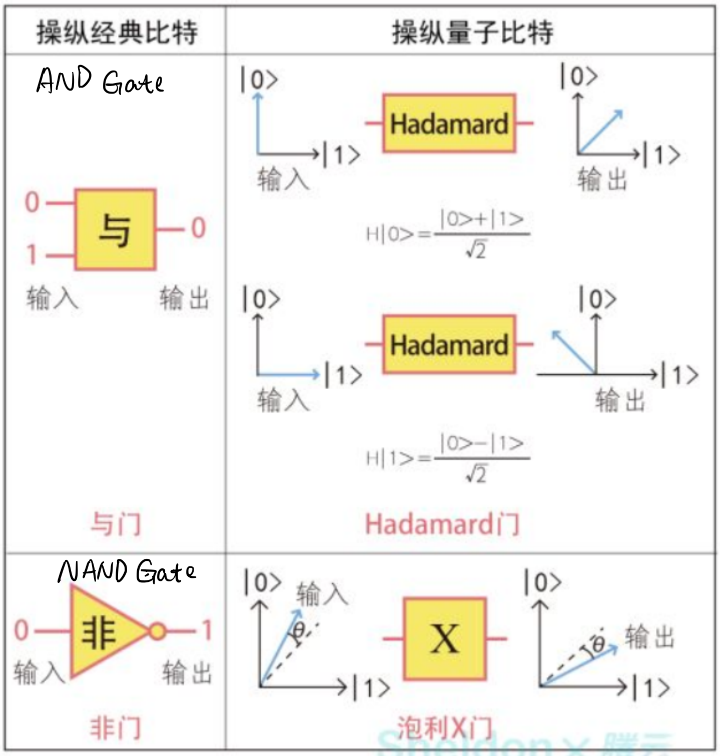
你把比特0和比特1分别想象成一个虚拟的空间中的两个相互垂直的坐标轴。对于经典比特来说，它要么处于比特0的轴上，要么处于比特1的轴上。

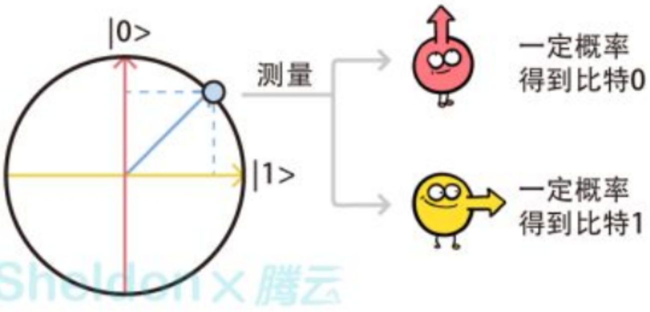
一个比特只能指向单位圆的上(0)或右(1)，但量子bit可以指向任意方向.



单位圆.

量子比特可以在两个轴之间的空间中任意"转动"。也就是说，它可以同时处于比特0和比特1的状态中，而且不同状态所占的"比例"可以任意变化。量子信息学中通常用Bloch球来表示量子比特的取值范围。为了便于理解，本文忽略了相位等技术细节，将球简化成了一个圆。





这样看来，一个量子比特似乎可以储存非常多的信息。但要想从量子比特中提取信息，你必须先做一次量子测量。量子力学告诉我们，当你测量量子比特时，只会随机得到两个结果：比特0和比特1。并且，得到这两个结果的概率跟量子比特在态空间中所指向的方向有关。

量子门 Quantum gate

例:

$|00\rangle$

⇓ Quantum Gate

$\sqrt{\frac{1}{2}}\cdot|01\rangle+\sqrt{\frac{1}{2}}\cdot|10\rangle$ ⇒ 根号的来源是因为在圆上，$(\frac{1}{\sqrt{2}})^2+(\frac{1}{\sqrt{2}})^2=1$

⇓ Quantum Gate

$\sqrt{\frac{1}{2}}\cdot|01\rangle+\sqrt{\frac{1}{6}}\cdot|10\rangle+\sqrt{\frac{1}{3}}|11\rangle$

⇓

observe: $|01\rangle$

1 qubit 可以用长度为2的向量表示：

vector

$|0\rangle \rightarrow \begin{bmatrix}1\\0\end{bmatrix}$: state 0

$|1\rangle \rightarrow \begin{bmatrix}0\\1\end{bmatrix}$: state 1

$\sqrt{\frac{1}{3}}|0\rangle+\sqrt{\frac{2}{3}}|1\rangle$: One of the superpositions

2 qubits 需要用长度为4的vector表示

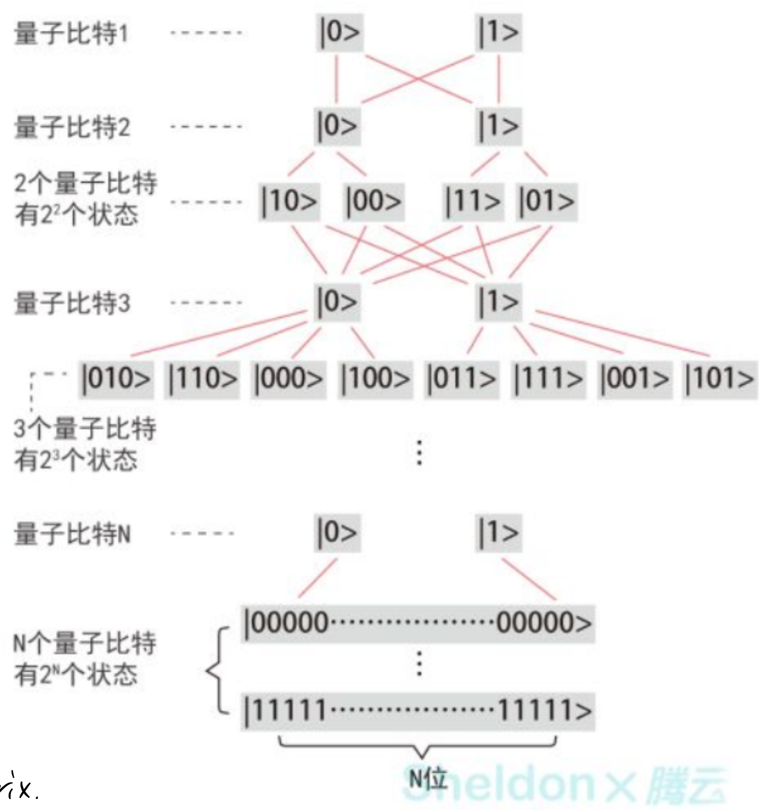
$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

上一页的例子可以解释为: $\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \xrightarrow{\text{量子门}} \begin{bmatrix}0\\\sqrt{\frac{1}{2}}\\\sqrt{\frac{1}{2}}\\0\end{bmatrix} \xrightarrow{\text{量子门}} \begin{bmatrix}0\\\sqrt{\frac{1}{3}}\\\sqrt{\frac{1}{3}}\\\sqrt{\frac{1}{3}}\end{bmatrix} \xrightarrow{\text{观察}} \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$

n个量子比特能存储 2^n 个比特信息

不知道你发现了没有，由于量子比特可以同时处于比特0和比特1的状态，量子门操纵它时，实际上同时操纵了其中的比特0和比特1的状态。

所以，操纵1个量子比特的量子计算机可以同时操纵2个状态。如果一个量子计算机可以同时操纵N个量子比特，那么它实际上可以同时操纵2^N个状态，其中每个状态都是一个N位的经典比特。这就是量子计算机传说中的并行计算能力。



共轭矩阵=逆矩阵

Unitary maxtrix [Conjugate transpose of the matrix is also its inverse (逆)]

每个量子门 Quantum gate 都对应一个不同的 Unitary matrix.

比如:

$$\underbrace{\begin{bmatrix}0 & 1 & 0 & 0\\ \sqrt{\frac{1}{2}} & 0 & -\sqrt{\frac{1}{2}} & 0\\ \sqrt{\frac{1}{2}} & 0 & \sqrt{\frac{1}{2}} & 0\\ 0 & 0 & 0 & 1\end{bmatrix}}_{\text{unitary matrix}} \underbrace{\begin{bmatrix}1\\0\\0\\0\end{bmatrix}}_{\text{input vector}} = \underbrace{\begin{bmatrix}0\\\sqrt{\frac{1}{2}}\\\sqrt{\frac{1}{2}}\\0\end{bmatrix}}_{\text{output vector}}$$

随机数据库搜索: Grover 算法

N个数据, 未排序. 找其中某个唯一的 x, 满足 $P(x)=$True.

传统算法时间复杂度: $O(N)$

相当于N个状态的叠加

Grover算法: N个数据存于 $\log_2 N$ 个 qubits 中. 同时算N个P( )的值.

⇒ 如果贸然读取, 会发现每个结果发生的概率都是$\frac{1}{N}$.
所以先不急读取, 而是通过量子操作增加为True的那个数据概率

时间复杂度: $O(\sqrt{N})$

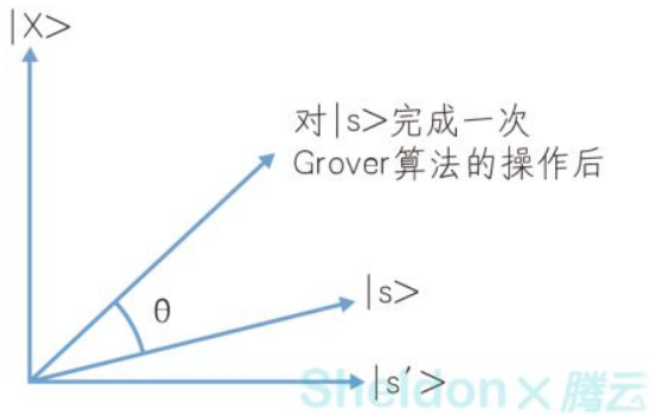
重复 $\frac{\pi\sqrt{N}}{4}$ 次后, 概率达到最大. $(1-2^{-N})$

此时再读数据, 就有很大概率读到想要的结果.

注：为什么Grover算法的操作必须且最多只能重复$\frac{\pi\sqrt{N}}{4}$次？

请你想象一个N维空间，每个维度代表$\log_2 N$个量子比特所存储的一个状态。由于这种空间在纸上画不出来，我们需要进行一些简化，假设右边这个二维空间代表那个N维空间。其中一个维度|X>表示你要搜索的数据对应的状态，另一个维度|s’>表示除|X>以外所有其他N-1个数据相叠加所对应的状态。

Grover算法的初始状态，就代表其中一个矢量|s>。



Grover算法采用的量子操作，就是像拨动表盘上的时针一样，不断将矢量|s>朝着|X>的方向拨过去，每次拨动的角度只能是θ，其中$\theta = 2\arcsin\frac{1}{\sqrt{N}}$。

注意我们说过，一个量子叠加态跟哪个方向的夹角越小，测量时得到哪个方向的结果的概率就越大。不难计算，将矢量|s>这样拨动$\frac{\pi}{2\theta} \simeq \frac{\pi\sqrt{N}}{4}$次之后，它与|X>的夹角最小，测量时得到你要找的正确结果的概率最大。

注意，在这个比喻中，我们没有考虑N个状态之间的相位，但这并不影响讨论的结果。

Shor算法(大数质因子)

用于 Integer factorization 分解质因数