量子信息概论

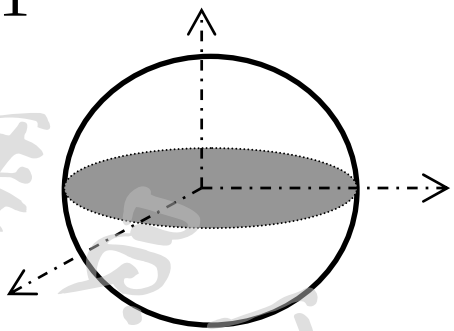
郭光灿

❶ 量子比特

- 比特（bit）是经典计算和经典信息的基本概念，经典信息的基本单元。
- 比特：0或1，$|0\rangle$ 或 $|1\rangle$，
- 量子比特：$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle, |\alpha|^2+|\beta|^2=1$

  称$|0\rangle$和$|1\rangle$为计算基态。
- 等效表示：$|\psi\rangle=\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$

  式中θ,φ为实数，θ和φ定义单位三维球面上的一个点。Bloch球。



- 量子比特的物理载体：任意二态的量子体系，如光子、原子、电子、原子核等。
- 一个量子比特表示多少信息?

  若对$|\psi\rangle$进行一次测量，只能给出0或1，量子比特的测量后的态为$|0\rangle$或$|1\rangle$。因此，从一次测量，人们只能获得关于量子比特态的一个比特的信息。

  - 如若不进行测量，一个量子比特代表多少信息?

——这是个微妙的问题。如果不进行测量，人们如何度量信息呢？尽管如此，这里仍有重要概念性问题存在。因为当Nature 演化量子比特的封闭量子系统，不做任何“测量”，她显然会保持住用于描述该态的全部连续变量（如α和β）的踪迹。在某种意义上讲，Nature 在一个量子比特的态中，隐藏有大量的“hidden information”（隐信息），更有趣的是，这种额外“信息”的数量随着量子比特的数目指数增加。如何理解这类隐信息正是我们要致力研究的问题，也是量子力学之所以成为信息处理强有力工具的核心。

❷ 多量子比特

- 两个量子比特

两个经典比特，有4种可能状态：00, 01, 10, 11。

两个量子比特有4个计算基态：$|00\rangle, |01\rangle, |10\rangle, |11\rangle$。

- 两个量子比特可表示为

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

归一化条件

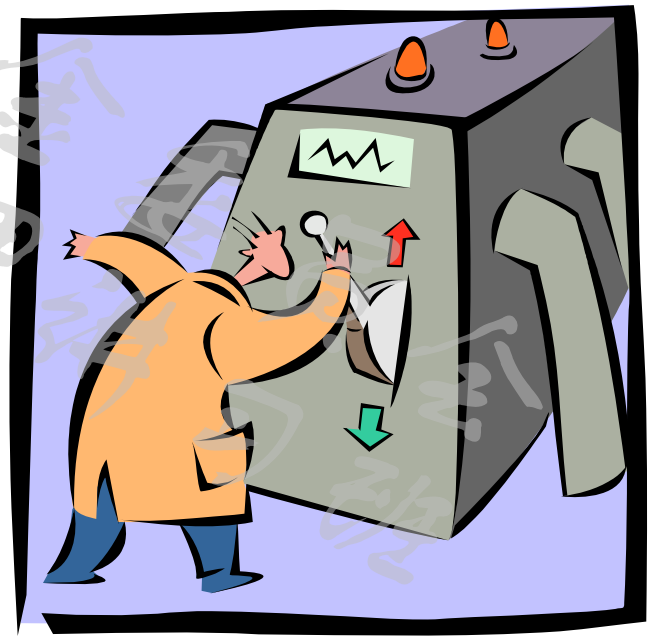
$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1, \quad x = 00, 01, 10, 11$$

$\{0,1\}^2$代表长为2的字符串集合，每个字符取0或1。

若测量子集（第一个量子比特），测得0的几率为 $|\alpha_{00}|^2+|\alpha_{01}|^2$,测量后的量子态为（归一化）

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

- 两量子比特的重要量子态是Bell态或EPR对，如 $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$，两量子比特之间存在量子关联。

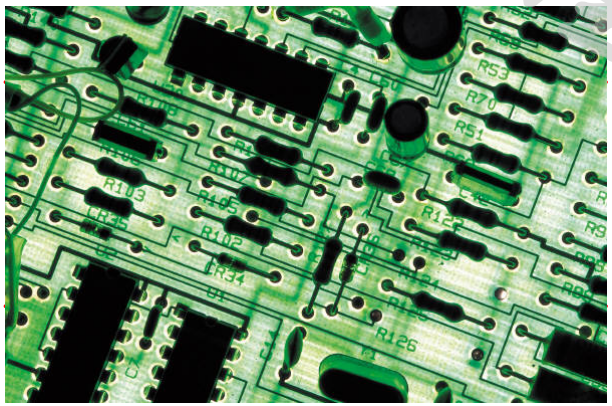


n个量子比特系统

计算基态 $|x_1, x_2, \cdots, x_n\rangle$, $|\psi'\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x'\rangle$,

有2^n个振幅系数，例如，n=500，2^n比宇宙中的原子数目还多。

若能制备n个量子比特存储器，则它具有巨大的存储数据能力。



❸ 量子计算

量子计算机由包含有导线和基本量子门的量子线路（quantum circuit）构成，导线用于传递量子信息，量子门用于操作量子信息。

（1）单个量子比特门

量子门对量子态作用是线性的，如量子非门

$$\alpha|0\rangle+\beta|1\rangle \xrightarrow{\text{NOT}} \alpha|1\rangle+\beta|0\rangle$$

为什么门作用不会是非线性？

这归结于量子力学的线性特性。非线性量子力学会导致超光速通信、违背热力学第二定律等。

量子非门的矩阵表示

(以$|0\rangle, |1\rangle$为基)

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

例

$$X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

即

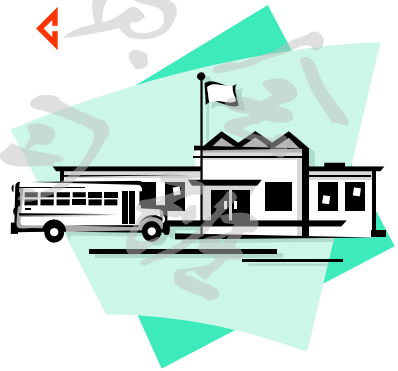
$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{X} \beta|0\rangle + \beta\alpha|1\rangle$$

作用于单个量子比特的量子门都可用2×2矩阵描述。

用做量子门的矩阵有何限制？

- 描述单个量子门的矩阵U是么正的，即$U^{+}U=I$。
- 这个么正性限制是对量子门的唯一限制。

任意么正矩阵均可标志有效量子门！



Z 门

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

其作用：$|0\rangle$ 不变，将 $|1\rangle$ 变为 $-|1\rangle$。

Hardmard 门

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

其作用：

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

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

$$H^2 = I$$

某些重要单量子比特门

$$\alpha|0\rangle + \beta|1\rangle \text{ —[X]— } \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \text{ —[Z]— } \alpha|0\rangle - \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \text{ —[H]— } \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

存在无数多个 2×2 么正矩阵，因而有无数多个单量子比特门。

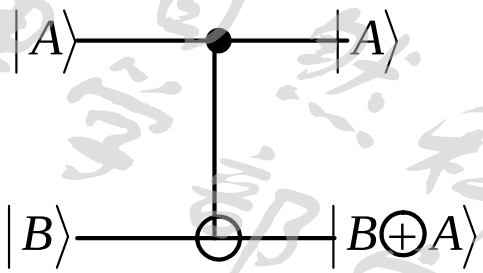
业已证明，任意么正矩阵可做如下分解

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{r}{2} & -\sin\frac{r}{2} \\ \sin\frac{r}{2} & \cos\frac{r}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}$$

式中为实数，注意：第二个矩阵为普通旋转矩阵，第一、三矩阵为绕围Z轴的旋转。这个分解式给出任意单量子比特量子逻辑门的精确表述。

（2）多量子比特门

典型多量子比特门是受控非门(Controlled -NOT or CNOT)



$$U_{CN}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix},\quad U_{CN}^{+}U_{CN}=I$$

其中$|A\rangle$为控制量子比特(control qubit), $|B\rangle$为目标量子比特(target qubit)。

作用：当控制比特为$|0\rangle$时，目标比特不改变；当控制比特为$|1\rangle$时，目标比特倒置，即$|0\rangle\rightarrow|1\rangle$, $|1\rangle\rightarrow|0\rangle$。

业已证明：任意多量子比特门均可以由**CNOT**和单量子比特门构成。

（3）基于非计算基的测量

量子比特 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$

采用基矢$|0\rangle,|1\rangle$进行测量，结果为$|0\rangle$和$|1\rangle$的几率分别为$|\alpha|^2$和$|\beta|^2$。

计算基并非是唯一的测量基，例如，可以选择另组正交基：

$$|+\rangle\equiv\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ |-\rangle\equiv\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

可将任意态写成：

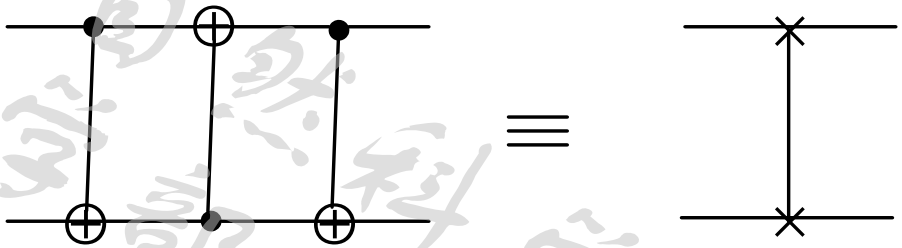
$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\frac{\alpha+\beta}{\sqrt{2}}|+\rangle+\frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

测量之后，将坍缩到$|+\rangle$或$|-\rangle$,几率为$\frac{1}{2}|\alpha+\beta|^2,\frac{1}{2}|\alpha-\beta|^2$。

更一般，给出任意基态$|a\rangle$和$|b\rangle$,可以将任意态表示为$\alpha|a\rangle+\beta|b\rangle$,只要$|a\rangle$,$|b\rangle$为正交，就可以进行相对于$|a\rangle$和$|b\rangle$的测量，以$|\alpha|^2$几率给出$\alpha$，以$|\beta|^2$几率给出$\beta$,$|\alpha|^2+|\beta|^2=1$。

❹ 量子线路

以包含有三个量子门的量子线路为例



线路中的每条线不一定对应物理上的导线，它可能是时间流向，或许是从某处传送到另处的物理粒子，如光子。

该线路功能：

$$|a,b\rangle \rightarrow |a,a\oplus b\rangle$$

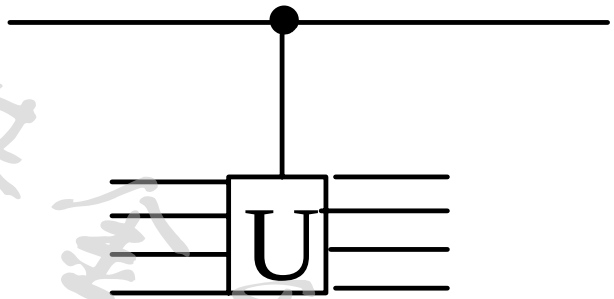
$$\rightarrow |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle$$

$$\rightarrow |b,(a\oplus b)\oplus b\rangle = |b,a\rangle$$

实际效果是交换了两个量子比特。

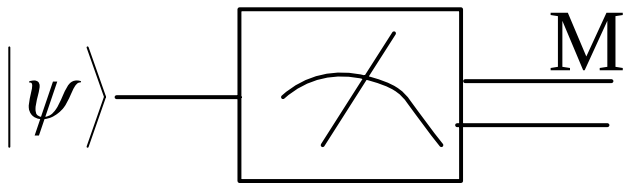
可控—U门

假定U是作用在某n个量子比特上的任意么正矩阵，U可以看作是作用在这些量子比特上的量子门，定义可控—U门，它有单个控制量子比特，n个目标量子比特。如果控制量子比特为0，则目标量子比特不发生任何变化，若控制量子比特为1，则门U作用在目标量子比特上。



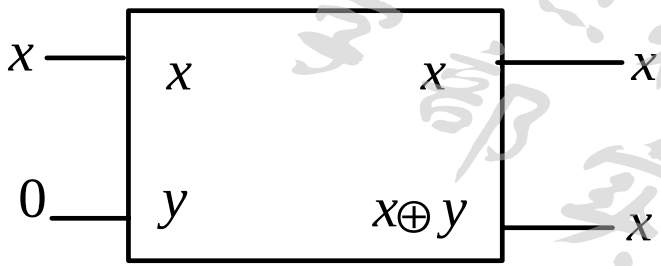
显然，CNOT门是其特例，（非门）

另类重要操作是测量。用指针表示，这种操作将单个量子比特态$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$变换成概率经典比特M，以$|\alpha|^2$概率得0，以$|\beta|^2$概率得1，用双线表示。

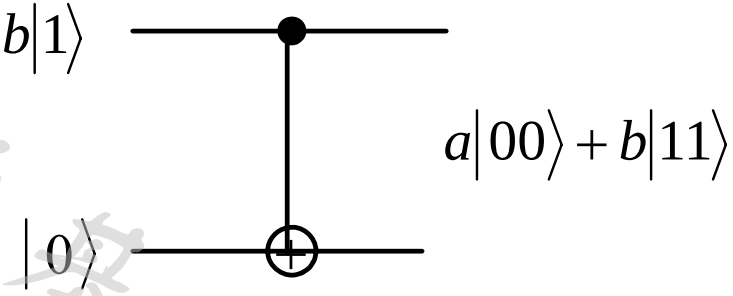


量子比特复制线路?

经典比特可用CNOT门精确地复制，量子比特可否精确复制?



经典复制线路



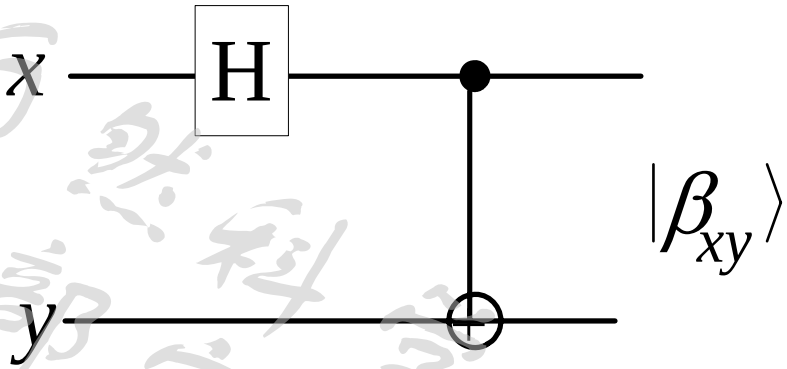
量子复制线路

量子CNOT门作用于$|\psi\rangle$得到$a|00\rangle+b|11\rangle$

这显然不是$|\psi\rangle|\psi\rangle=a^2|00\rangle+ab|01\rangle+ab|10\rangle+b^2|11\rangle$

量子不可克隆定理：不存在任何物理过程可以精确复制任何未知的量子态。

Bell 态（EPR对）

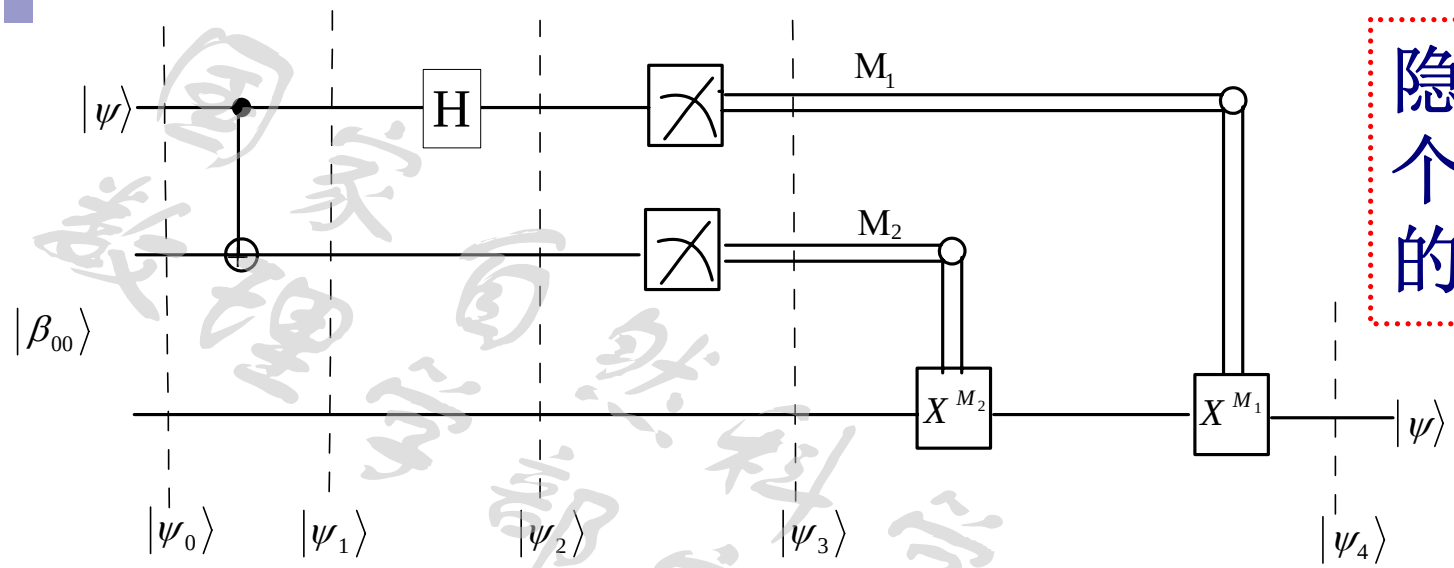


In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

量子隐形传态(Quantum Teleportation)

将未知量子态（量子比特）传送到远处而不传送量子态的物理载体。

- Alice和Bob各自拥有EPR对的一个纠缠粒子。
- Alice对处于未知量子态$|\psi\rangle$粒子和她的纠缠粒子进行量子测量，获得4个可能经典结果00,01,10,11中的一个。
- Alice将测量的结果传送给Bob
- Bob依据Alice的信息对他手中的EPR粒子做相应操作，便可恢复出原始的量子态。



隐形传送一个量子比特的量子线路

▲待送未知量子比特：$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$

构成量子通道的EPR态：$|\beta_{00}\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$

▲输入 $|\psi_0\rangle=|\psi\rangle\otimes|\beta_{00}\rangle=\frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|00\rangle+|11\rangle)]$

▲Alice对前两个粒子做CNOT门操作得到

$$|\psi_1\rangle=\frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|10\rangle+|01\rangle)]$$

▲Alice 将第一个粒子通过Hadamard门，得到

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle)+\beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)]$$

$$= \frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)]$$

▲Alice 对前两个粒子进行正交测量，得到00, 01, 10, 11中的任一个，Bob的粒子将坍缩到相应的测量后(post-measurement)态：

$$00 \mapsto |\psi_3(00)\rangle \equiv [|\alpha(0)\rangle+\beta|1\rangle]$$

$$01 \mapsto |\psi_3(01)\rangle \equiv [|\alpha(1)\rangle+\beta|0\rangle]$$

$$10 \mapsto |\psi_3(10)\rangle \equiv [|\alpha(0)\rangle-\beta|1\rangle]$$

$$11 \mapsto |\psi_3(11)\rangle \equiv [|\alpha(1)\rangle-\beta|0\rangle]$$

- Bob依照Alice传送来的测量结果，将其粒子通过适当量子门便可恢复出原始原子态$|\psi\rangle$:

若测量结果为00，Bob无需做任何操作

若测量结果为01，Bob施加X门

若测量结果为10，Bob施加Z门

若测量结果为11，Bob施加Z X

(先施加X门，再作用Z门)

故Bob需要施加的变换为 $Z^{M_1}X^{M_2}$

量子隐形传态有许多有趣的特性，例如

(1) 隐形传送是否允许超光速地传送量子态？

不可能，因为只有Alice通过经典信道将测量结果传送给Bob，才有可能实现这种隐形传态。没有这个经典通信，teleportation无法传送任何信息。

(2) 隐形传态似乎产生了一份待传送量子态的复制，违背了量子不可克隆定理。事实上，原始粒子的态在Alice测量时被破坏，它最终处于或，因此这里量子隐形传态强调了量子力学的不同信源的相互交换能力，它证明，一对共享EPR对连同两个经典通信比特起码等同于一个通信量子比特的信源。

❺ 量子算法

是否能找到这样问题，量子计算可以完成得比经典计算机更好?

（1）有效量子算法

Shor(1994)：量子计算机原则上可以有效地进行大数因子分解。

因子分解是典型的难解问题(intractable),其特性：

—— 一旦找到解，很容易验证。（n=pq）

—— 但解很难找到。（给定n，求q,p）

“One way”问题，寻找因子所需时间是 log(n)的超多项式函数：

$$T \approx \exp[c(\ln n)^{1/3}(\ln\ln n)^{2/3}],\ c = (\frac{64}{9})^{1/3} = 1.9$$

例：130位数～1个月; 400位数～1010年(宇宙年龄)

不可能在输入长度(logn)的多项式时间内求解。

大数因子分解是现代公开密钥RSA体系安全性的基石。

Shor算法：$T \sim O[(\ln n)^3]$,可在多项式时间内求解。

（2）量子复杂性　　(Benioff, Feynman, 1982)

考虑N个量子比特的系统，其量子态是2^N维空间中的一个矢量。设希氏空间的基矢量选为　　$|0110\cdots10\rangle$（计算机数字态），一般矢量可表示为

$$\sum_{x=0}^{2^N-1} a_x |x\rangle, \quad \sum_x |a_x|^2 = 1$$

若对该矢量进行测量，可得到输出为 $|x\rangle$ 的几率为 $|a_x|^2$

量子计算基本过程

- 将N个量子比特制备在某标准初态中，如$|x=0\rangle$
- 用么正变换U作用在N量子比特上（U是标准量子门的乘积）
- 测量所有量子比特使之投影到 $\{|0\rangle|1\rangle\}$ 的基上，测量后输出便是计算的输出，因此最后输出是经典信息。

注意：QC所实行的算法是一种概率算法。它给出可能输出值的概率分布。(重复同一运算，每次给出不同的经典信息)。

经典计算机也可以存储矢量，旋转矢量，投影矢量到正交轴上。

∴ 量子计算机并不能做经典计算机做不到的事，原则上，经典计算机可以任意高精度模拟量子计算机的过程，只要有足够的资源。但是，这种模拟需要多长时间？

例：N=100，表示典型的量子态要有$2^N=2^{100}\sim10^{30}$个复数！

任何现有经典计算机都做不到。

而且还要对10^{30}维空间中的矢量旋转，更是无能为力！

∴ 对经典计算机而言，“量子力学”是个“难解问题”！（动力学不同）

Feynman最先注意到这个问题，并指出：

量子计算机可以实现经典计算机事实上无法做到的事情。

量子计算机可以模拟量子体系本身！

更重要的：N量子比特系统存在非局域关系，任何局域概率算法都无法得到量子力学的结论。

（3）量子并行性 (*Quantum Parallelism*)

Deutsch（1985）强调：量子并行性是量子计算机发挥其计算潜力的根源。

Deutsch问题：黑盒子 $x \to f(x),\ x = 0,1;\ f(x) = 0,1$

想知道：$f(x)$ 是constant(即 $f(0) = f(1)$)或balanced(即 $f(0) \neq f(1)$)

经典计算需要两次。假定用量子黑盒来计算 $f(x)$:

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$$ (类似受控非操作)

功能：若作用在第一个量子比特上的*f*是1，则第二个量子比特倒转(flip)，否则不变。

运行两次，便可判定*f*(*x*)是constant还是balanced。能否运行一次量子黑盒子就给出答案？Deustch问题。

设第二个量子比特制备在$\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$,则

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

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

函数体现在f依赖于x的相位上。

假设第1个量子比特制备在: $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，则

$$U_f:\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\to\frac{1}{\sqrt{2}}[(-)^{f(0)}|0\rangle+(-)^{f(1)}|1\rangle]\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

测量：将第1个量子比特投影到下列基矢上: (正交测量)

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

若$f(0)\neq f(1)$ balanced；则总得到$|-\rangle$

$f(0)=f(1)$ constant；则总得到$|+\rangle$。(一次操作)

Deutsch问题的肯定显示出量子计算与经典计算的区别：

量子计算机不限于只计算 $f(0)$ 或 $f(1)$，它可同时对$|0\rangle$和$|1\rangle$叠加施加作用，提取出有关的global（整体）特性，这个信息同时依赖于 $f(0)$和 $f(1)$，这就是量子并行性。

更一般场合：

研究作用于N量子比特上的函数 f，其整体特性。

f 的变量有2^N个，经典计算需2^N次，列出表格后加以研究。

输入存储器　输出存储器

量子计算：$U_f : |x\rangle|0\rangle \to |x\rangle|f(x)\rangle$

将输入存储器制备为

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

仅对 f 计算一次，则生成

$\frac{1}{2^{N/2}}\sum_{x=0}^{2^N-1}|x\rangle|f(x)\rangle$ 关联态，纠缠态

有关函数 $f(x)$ 的整体特性就编码在这个态上，如果能找到合适的方法便可从中获取其中的某些性质。

量子计算显示出大规模量子并行性(*massive quantum parallelism*)，量子计算机运行一次，其效果相当于

- 一台经典计算机运行2^N次，或者
- 2^N台经典计算机并行运行一次。

注意：

- 量子信息的本质特征是它可以编码在物理系统不同部分之间的非局域关联上，如上述 $\sum|x\rangle|f(x)\rangle$ “输入存储器”和“输出存储器”之间关系（纠缠态entangled state）

- 这种非局域的信息不容易解码。

例如，若测量输入存储器，得到期$|x_0\rangle$，x_0是2^N个数中任一个，测量结果将纠缠态投影到

$$|x_0\rangle|f(x_0)\rangle$$

虽然得到$f(x_0)$但其代价是破坏了原先纠缠态，使非局域信息丧失掉，这种提取信息的方法并不显示出量子计算的优越性。

∴ 关键：找合适的方法能有效地运用这种非局域关联——量子算法！ **Shor的贡献**

（4）复杂性之分类

经典复杂性理论研究：

哪类问题属“难”算的，

哪类问题属“易”算的。

“难”与“易”借助于所需的时间或内储数目来区别。

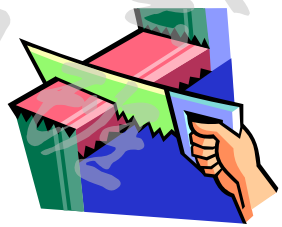
“难”与“易”的定义应当具有普适性，不依赖于所用机器。

目前，集中于“多项式时间”和“指数式时间”的区分。对于任意算法A（作用在于长度可变的输入上），定义相应的复杂性函数$T_A(N)$

N — 输入比特的长度，

$T_A(N)$是用算法A运行N比特输入所需的最长时间。

- 若$T_A(N) \le Poly(N)$ ($Poly(N)$表示N的多项式)，则说A是多项式时间。
  —(“易解”)P问题
- 若问题不是多项式时间，则说它是指数式时间。这种区分机器无关。(“难解”)



此定义的普适性来自计算机科学的关键性结论：

一台通用经典计算机在最坏场合下，也可以用多项式时间来模拟另一台计算机。

Shor证明：

- 量子计算机的非多项式时间模拟是可能的。
- 复杂性理论所得成果，作为数学真理是正确的，它表征经典计算机（图灵机）的能力。
- 但作为物理学真理则不正确。

- 若复杂性的量子分类确实不同于经典的分类，则必然会动摇计算机科学的基础，并将冲击未来的高技术！量子信息论（通讯，计算）

（5）量子计算

(i) 量子算法

应用量子相干性有效地加速运算。体现于幺正变换U的设计上。

目前有：

Shor平行算法：

将大数因子分解的问题变成P问题。

Grover搜寻算法：

将$\frac{N}{2}$变成$\sqrt{N}$(实验验证)。

(ii) 量子网络(硬件)

N量子比特的量子体系(宏观多体量子体系), N要大, 便于实现量子操作(即U的物理实现)

目前：
- 腔QED
- 离子阱（Q.CN门）
- 核磁共振 N=3,5,7
- 硅基原子核自旋

(iii) 量子编码)

量子相干性的脆弱性

寻找克服消相干(decoherence)的方法

- 量子纠错码(Quantum error-correcting code)
- 量子防错码(Quantum error-preventing code)
- 量子避错码(Quantum error-avoiding code)

（6）Shor量子算法

量子计算是如何有效地加速运算的？

1. 寻找周期性函数的周期

设周期函数 $f(x)$, x=1,2,3

有两串量子比特（两个存储器）

X系列：含有变量x,

Y系列：取函数值 $f(x)$

例：$f(x)=\cos(\pi x)+1$, 周期$T=2$

若取$x=5$, 则 $f(5)=0$

两个存储器X和Y处于下列态：

$$X:\left|00\cdots\cdots101\right\rangle, Y:\left|00\cdots\cdots000\right\rangle$$

可将X，Y的态写成：$\left|x, f(x)\right\rangle$

上式为$\left|x, f(x)\right\rangle=\left|000\cdots101,\ 000\cdots000\right\rangle$

$\left|x, f(x)\right\rangle=\left|5,0\right\rangle$

二进制

十进制

更复杂的态 $\left|k, f(n)\right\rangle$

其叠加态为(XY量子态):

$$\sum_{k,n} C_{k,n}\left|k, f(n)\right\rangle$$

Shor算法

- 初始将X置于所有数字态(计算基矢)的均等叠加态。例，X有三个量子比特，有$2^3=8$个数字态，其均等叠加态为

$$X:\frac{1}{\sqrt{8}}(|000\rangle+|100\rangle+|010\rangle+|001\rangle+|011\rangle+|101\rangle+|110\rangle+|111\rangle)$$

或

$$\frac{1}{\sqrt{8}}(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle) \quad \leftarrow \text{十进制}$$

(量子并行性→存储能力)　同时存储2^N个(经典)数

Y：取所有量子比特于基态$|0\rangle$，$\psi_0=\frac{1}{\sqrt{8}}\sum_x|x\rangle\otimes|0\rangle$

- 将X、Y置于态的均等叠加

$$\Psi=\frac{1}{\sqrt{8}}\sum_x|x,f(x)\rangle,\quad U_f:\Psi_0\to\Psi$$

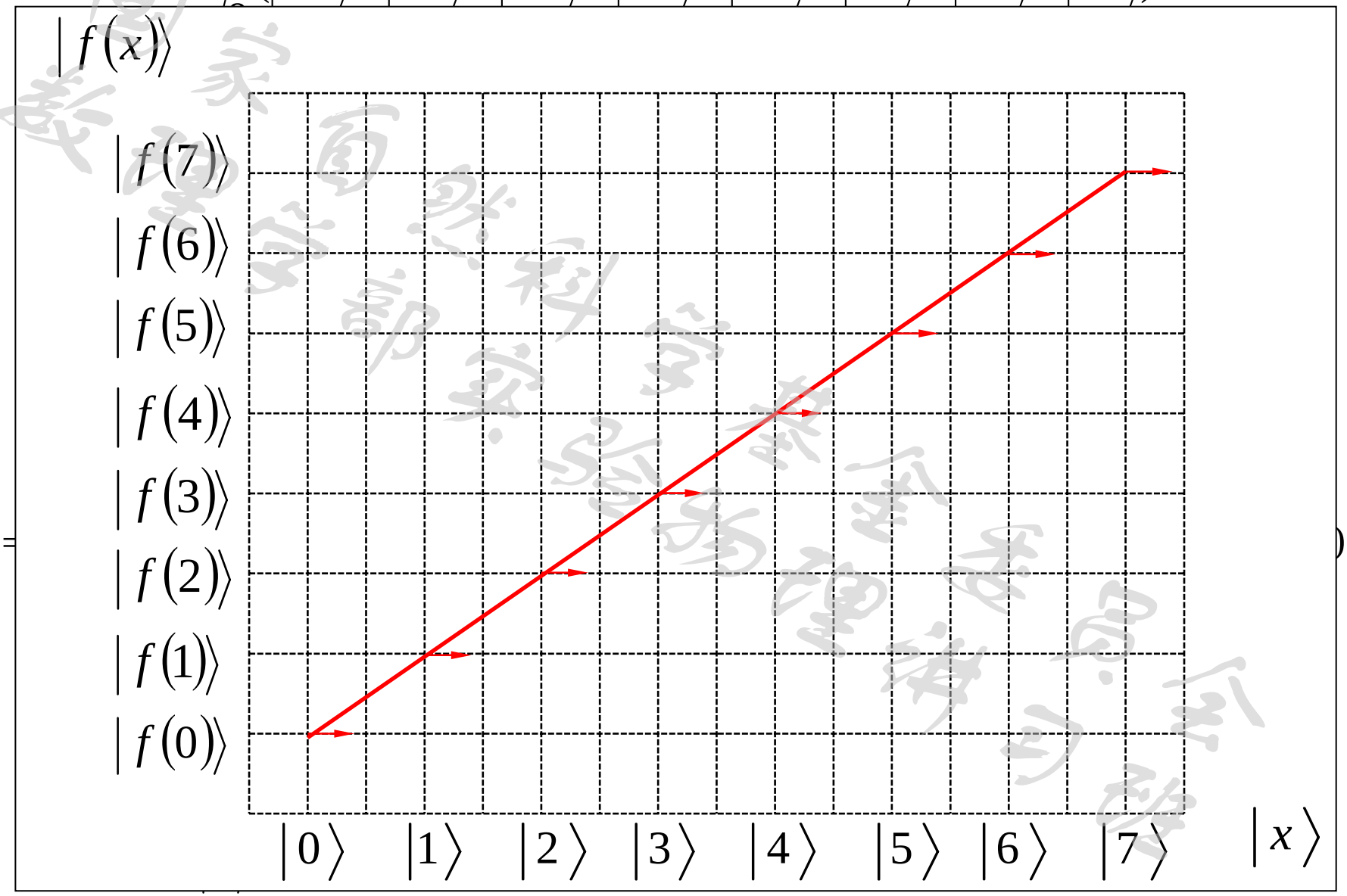
$$\Psi=\frac{1}{\sqrt{8}}|0,f(0)\rangle+|1,f(1)\rangle+|2,f(2)\rangle+|3,f(3)\rangle+|4,f(4)\rangle+|5,f(5)\rangle+|6,f(6)\rangle+|7,f(7)\rangle$$

对存储器X做离散富利叶变换(Discrete Fourier Transform, DFT) (局域操作)

$$|x\rangle=\frac{1}{\sqrt{8}}\sum_{k=0}^{7}e^{2\pi ikx/8}|k\rangle$$

即每个$|x\rangle$变成叠加态。

$$x:\frac{1}{\sqrt{8}}(|000\rangle+|100\rangle+|010\rangle+|001\rangle+|011\rangle+|101\rangle+|110\rangle+|111\rangle)$$



$\Psi =$ $\rangle$

$$\Psi' = \frac{1}{8}\sum_{x}\sum_{k=0}^{7} e^{2\pi i kx/8}\left|k, f(x)\right\rangle$$

$$= \frac{1}{8}\left|0\right\rangle\{\left|f(0)\right\rangle + \left|f(1)\right\rangle + \cdots\cdots \left|f(7)\right\rangle\}$$

$$+ \frac{1}{8}\left|1\right\rangle\{\left|f(0)\right\rangle + e^{2\pi i/8}\left|f(1)\right\rangle + \cdots\cdots e^{2\pi i 7/8}\left|f(7)\right\rangle\}$$

$$+ \cdots\cdots$$

$$+ \frac{1}{8}\left|7\right\rangle\{\left|f(0)\right\rangle + e^{14\pi i/8}\left|f(1)\right\rangle + \cdots\cdots e^{14\pi i 7/8}\left|f(7)\right\rangle\}$$

DFT使XY处于纠缠态，测量X的态便可找到的周期。

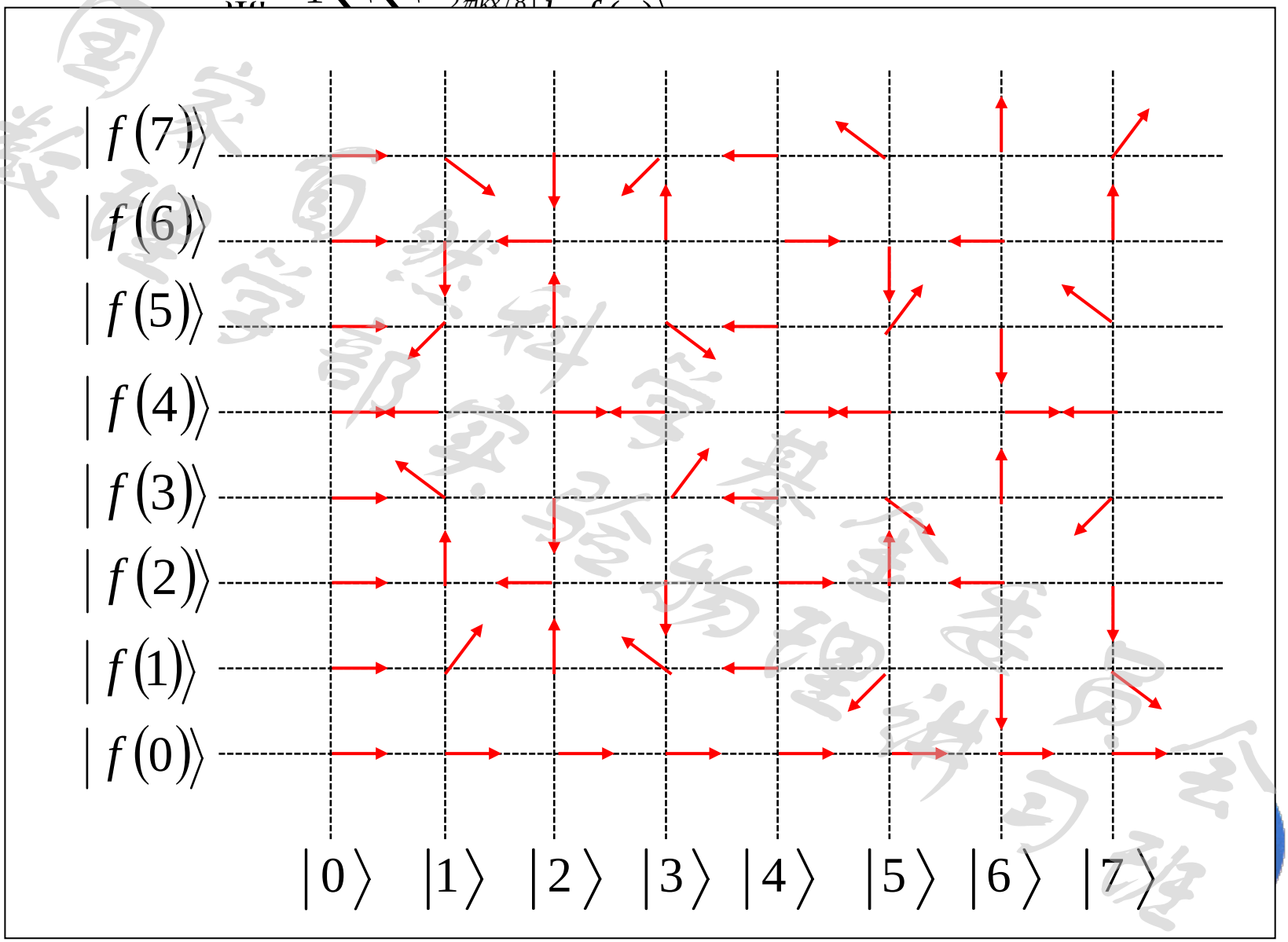
例：假定 $f(x)$的周期$T=2$，即

$$f(0) = f(2) = f(4) = f(6)$$

$$f(1) = f(3) = f(5) = f(7)$$

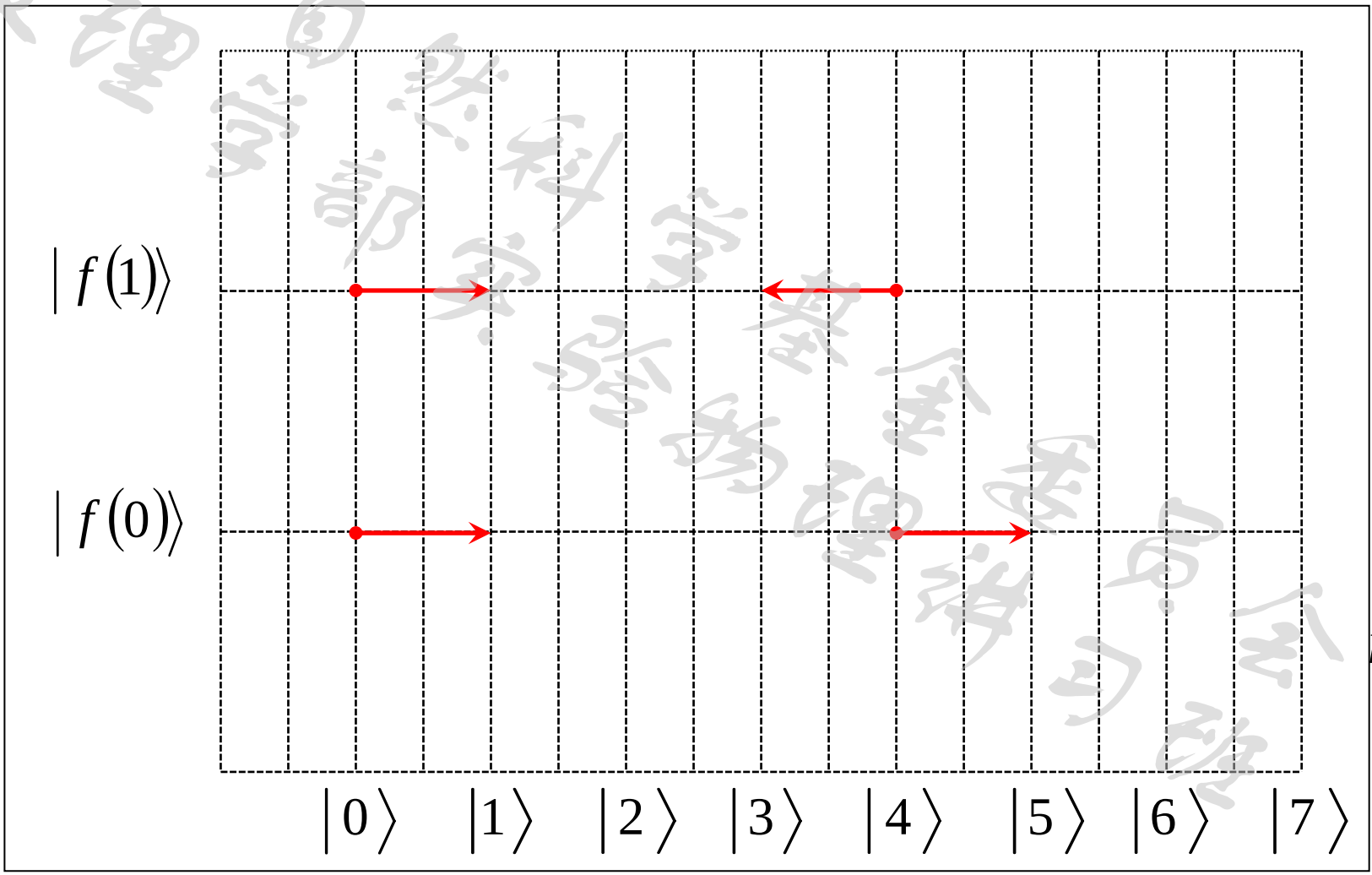
此时

$$\frac{1}{8}\sum_{x=0}^{7} 2\pi i k x/8 \,|\, f(x)\rangle$$



$$\Psi' = \frac{1}{2}|0\rangle\{|f(0)\rangle + |f(1)\rangle\}$$

$$+\frac{1}{8}|1\rangle\{|f(0)\rangle(1 + e^{(\frac{1.2}{8})2\pi i} + e^{(\frac{1.4}{8})2\pi i} + e^{(\frac{1.6}{8})2\pi i})$$



$$\Psi' = \frac{1}{2}|0\rangle\{|f(0)\rangle + |f(1)\rangle\}$$
$$+\frac{1}{8}|1\rangle\{|f(0)\rangle(1+e^{(\frac{1.2}{8})2\pi i}+e^{(\frac{1.4}{8})2\pi i}+e^{(\frac{1.6}{8})2\pi i})$$
$$+|f(1)\rangle(e^{(\frac{1.1}{8})2\pi i}+e^{(\frac{1.3}{8})2\pi i}+e^{(\frac{1.5}{8})2\pi i}+e^{(\frac{1.7}{8})2\pi i})\}$$
$$+\frac{1}{8}|2\rangle\{|f(0)\rangle(\cdots)+|f(1)\rangle(\cdots)\}$$
$$+\cdots\cdots$$

纠缠态中各项的相位大多相干相消，结果可写成:

$$\Psi' = \frac{1}{2}\{|0, f(0)\rangle + |0, f(1)\rangle + |4, f(0)\rangle + e^{i\pi}|4, f(1)\rangle\}$$

测量X，可能值为0或4，各自几率为$\frac{1}{2}$。

Shor算法

X态测量可给出下列k值中的一个$k = 0,\ D/T,\ 2D/T, \cdots\cdots \frac{T-1}{T}D$

式中D是X可能数字态的数目，$D=2^N$，N——量子比特数目。在N=3时，D=8，上例中，测量X，给出k=0或4

$$T=\frac{D}{k}=2$$

一般场合，k值有许多，如何确定周期？

例：$T=8, N=7, D=2^7=128$

k值有：

$$k=0,16,2\times16=32,$$
$$3\times16=48,\cdots\cdots7\times16=112$$

假定实测 k 值为k =80，于是$\frac{D}{K}=\frac{128}{80}$，找最大公因子得$\frac{D}{k}=\frac{8}{5}$，这个分数的分子等于周期T。

若实测到其它 k 值，则有$\frac{D}{k}=8,4,\frac{8}{3},2,\frac{4}{3},\frac{8}{7}$，可将$\frac{D}{k}$ 降低到最小项，其分子的最大值为T。

Shor算法

X态的测量会以相同几率给出下列 k 值：

$$k=m\frac{D}{T},m=0,1,2,\cdots T-1$$

如果 T 和 m 不存在不等于1的公因子，则分数

$$\frac{D}{k}=\frac{T}{m}$$

在最低项中有最大的分子，该分子就是周期。

业已证明：提供有效计算的几率可高达接近于1。

小结：

关键在于设计出纠缠态 Ψ'

自动地排选出所需要的X态，给出 $m\frac{D}{T}$

量子算法是确定性的，但输出概率性的。

量子计算机的优点在于能平行地处理X的所有可能值，并使“不需要”的相干相消，“需要的”相干相长。

2. DFT

量子力学如何描述DFT?

假定存储器X有L个量子比特（即x取$0-2^{L}-1$任意数）

以十进制表示：

$$|x\rangle=|x_{L-1}x_{L-2}\cdots x_1x_0\rangle=|x_{L-1}\rangle\otimes|x_{L-2}\rangle\cdots\otimes|x_1\rangle\otimes|x_0\rangle$$

式中 $x=\sum_{i=0}^{L-1}x_i2^i$，x_i=0或1。

● 单个量子比特操作算符 A_j

——仅作用于第 j 个量子比特上，能以适当方式使第j个量子态处于$|0_j\rangle$ 和$|1_j\rangle$ 的任意叠加态。

● 算符显示式

$$A_j = 2^{-\frac{1}{2}}\left(|0_j\rangle\langle 0_j| + |0_j\rangle\langle 1_j| + |1_j\rangle\langle 0_j| - |1_j\rangle\langle 1_j|\right) \qquad j = 0,1,\cdots,L-1$$

式中$|i_j\rangle\langle k_j|$对$|n_j\rangle$的作用法则为 $|l_j\rangle\langle k_j|\cdot|n_j\rangle = \delta_{kn}|l_j\rangle$

矩阵形式 $$|0_j\rangle\langle 1_j| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}_j$$

● 两个量子比特的操作算符B_{jk}

$$B_{jk} = |0_{jk}\rangle\langle 0_{jk}| + |1_{jk}\rangle\langle 1_{jk}| + |2_{jk}\rangle\langle 2_{jk}| + e^{i\theta_{jk}}|3_{jk}\rangle\langle 3_{jk}| \qquad \theta_{jk} = \pi/2^{k-j}$$

式中

$$|0_{jk}\rangle = |0_j 0_k\rangle, \quad |1_{jk}\rangle = |0_j 1_k\rangle$$

$$|2_{jk}\rangle = |1_j 0_k\rangle, \quad |3_{jk}\rangle = |1_j 1_k\rangle$$

操作规则：

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

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

$$B_{jk}\left|0_{jk}\right\rangle=\left|0_{jk}\right\rangle,\quad B_{jk}\left|1_{jk}\right\rangle=\left|1_{jk}\right\rangle$$

$$B_{jk}\left|2_{jk}\right\rangle=\left|2_{jk}\right\rangle,\quad B_{jk}\left|3_{jk}\right\rangle=e^{i\pi/2^{k-j}}\left|3_{jk}\right\rangle$$

运用(A_j, B_{jk})操作可实现离散富利叶变换

例：对L量子比特$|x\rangle$，操作顺序为：

A_{L-1}

$A_{L-2}B_{L-2\ L-1}$

$A_{L-3}B_{L-3\ L-2}$，$B_{L-3,\ L-1}$

最终可得到DFT：$\left|x\right\rangle\Rightarrow 2^{-\frac{1}{2}}\sum_{k=0}^{2^L-1}e^{2\pi ikx/2^L}\left|k\right\rangle$ (x, k均为十进制)。

实现DFT所需要的步骤：

L次A_j操作和$[0+(L-1)]L/2$次B_{jk}操作

操作步骤的数目等于L平方的函数，此算法为有效算法。

3. 整数的量子分数

$$N=30$$

- 随机选择一个数Y，$(1<Y<N)$，Y与N的最大公因子为1
- 考虑周期性函数

$$f(x)=y^x \quad (\text{模 } N),\ x=0,1,2,\ldots\ldots$$

余数

例：$N=30$，选择$Y=11$

$f(0)=1$ (模30) $=1$

$f(1)=11$ (模30) $=11$

$f(2)=11^2$ (模30) $=1$

$f(3)=11^3$ (模30) $=11$

$f(4)=11^4$ (模30) $=1$

……

显然$f(x)$的周期$T=2$ (设这个周期已由DFT求出)

$f(x)$是周期函数

- 为求N的因子，计算 $Z = y^{T/2}$

例：$N = 30, T = 2$, 则$Z=11^1=1$

$(Z+1, N) = (12,30)$ 的最大公因子为6，$(Z-1, N) = (10,30)$ 最大公因子为10，数6，10均为30的因子

可见，若量子算法能有效地求出$f(x)$的周期，便可寻找N的两个因子。

这种方法有时会失效，如T为奇数场合，但已证明失败几率很小。

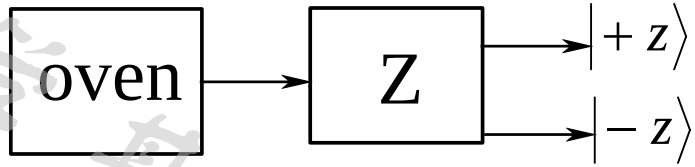
寻找N与Y的最大公因子，可使用Euclid算法。

❻ 量子信息处理的实验

有什么证据说明，Nature确实按照量子信息理论运行？大尺度晶的量子计算机在实验上实现可靠吗？是否存在某种物理原理本质上禁止量子线路的最终扩展？

（1）Stern-Gerlach实验

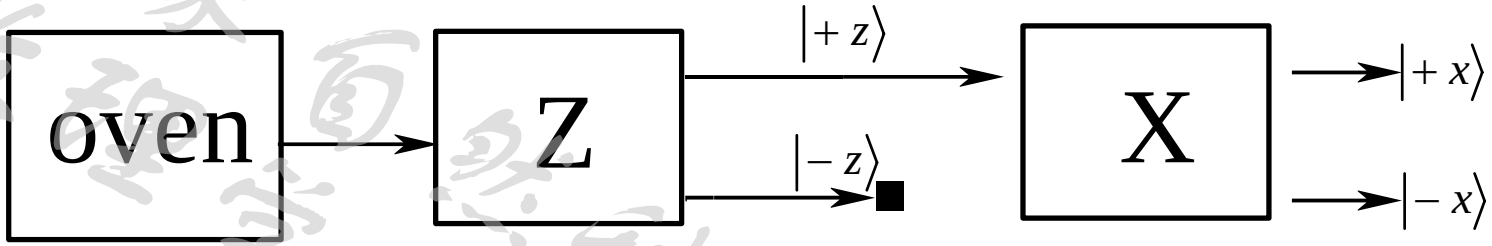
我们如何知道具有量子比特特性的系统在自然界确实存在？已有大量事实证实它的存在。早期显示量子比特结构的决定性实验是Stern于1921年提出并为Gerlach在1922年实现的S-G实验。



S-G 实验原理图

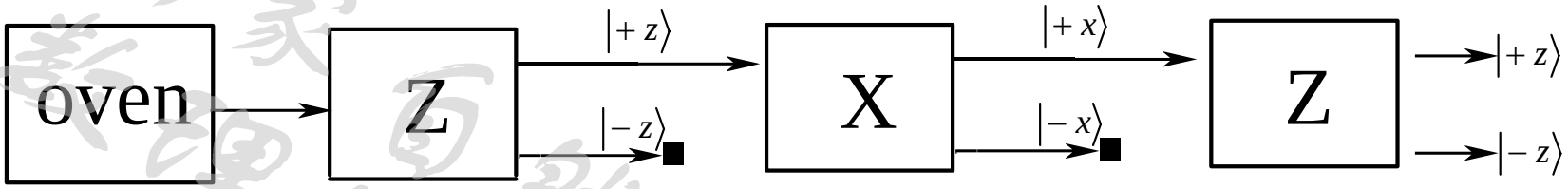
氢原子来由热炉产生，经过磁场，发生偏转，向上$|+z\rangle$或者向下$|-z\rangle$。（电子自旋本征值）。

考察级能联S-G实验



第一个S-G输出中$|+z\rangle$输入到第二个S-G（偏转方向在X），挡掉$|-z\rangle$。按照经典理论，沿$+\hat{z}$方向的经典磁矩不会有 $\hat{x}$方向的磁矩，因此第二个S-G输出应当在中心方向上有个峰，但实验观察到是等强度的两个峰：$|+x\rangle,|-x\rangle$。也许这些原子具有特殊性质，沿各个轴向都有确定磁矩，通过第二个S-G后它的态由$|+z\rangle|+x\rangle$ 或 $|+z\rangle|-x\rangle$ 来描述，这样就能与实际观察结果相一致。

再考察另个实验来验证这个经典假设是否正确。



- 若原子只有$|+z\rangle$方向磁矩，第三个S-G只能$|+z\rangle$输出，但实验[illegible]输[illegible]预[illegible]的$|+x\rangle$和$|-x\rangle$构成，而$|+x\rangle$由等分量的$|+z\rangle$和$|-z\rangle$构成。沿着$\hat{y}$ 轴的实验也是类似的。

- 量子比特模型提供对实验观察的简单解释,设$|0\rangle$和$|1\rangle$是量子比特的态。 $|+z\rangle \leftarrow |0\rangle$ $|-z\rangle \leftarrow |1\rangle$ [illegible] $|0\rangle+|1\rangle)$ [illegible] $|0\rangle-|1\rangle)$ [illegible]算基矢测量自旋，$\hat{x}-S-G$ 装置以 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ 为计算基矢测量自旋。量子比特模型正确地预言这种类型的级联S-G实验。

这个例子演示了量子比特是如何以可信方式描绘自然界的系统，还有其它实验结果，使人们确实电子自旋采用量子比特模型是最合适的。

（2）实际的量子信息处理器

研制量子信息处理装置是个巨大的挑战

最基本问题：是否有某种原理禁止我们研制这样或那样的量子信息处理器？两种可能的障碍是：噪声对实用量子处理器设置了基本障碍，或者量子力学可能并不正确。

噪声无疑是研制实用量子信息处理器的严重障碍，但它是否是从根本上无法克服的障碍，使得大尺度量子信息处理器无法研制成功呢？

量子纠错编码的理论指出，尽管量子噪声是必需关注的实际问题，但它并不构成原理上的基本问题。特别是量子计算的阈值定理(threshold theorem)指出，只要量子计算机的噪声水平被降到低于某个恒定“阈值”之下，使用量子纠错码可以使计算进行下去，对于计算复杂度不大情况，甚至可永远计算下去。阈值定理对自然界、量子计算机的噪声大小和实现量子计算的体系结构做了某些假定，只要这些假定可以满足，噪声对量子信息处理的影响就可以忽略不计。

另种可能性：

量子力学要是不正确的话，量子信息处理也就难以实现。若人们在Nature的某个层次上发现存在量子力学无法解释的现象，这将会对整个科学和技术领域带来巨大冲击，正如当时量子力学发现的冲击那样。当然，这种冲击对量子信息处理器的功能是增强、削弱还是没有影响，迄今人们无从知道。目前，所有证据都显示量子力学是世界完美和正确的描述。

既然构造量子信息处理装置已不存在原则性的障碍，那么我们为什么还要花大多时间和金钱来研究相关问题？事实上，我们已知若干实际应用：量子密码学，大数因子分解，获取对Nature和信息处理的基础知识等。但仍有许多问题不清，如“量子计算机是否具有比经典计算机更强的功能？”

量子态层析照相(tomography)

和量子过程的层析照相两个基本过程，它们的实现对量子计算和量子信息有十分重大意义。

量子态层析照相是种确定系统的量子态的方法，为此必须克服量子态的隐藏特性（hidden nature）。需要重复制备许多相同量子态，并以不同方法进行测量，以建立量子态的完备描述。

量子过程层析照相是种完备表征量子系统动力学的办法，它可用来表征量子门或量子通道的性能，可用于确定系统中不同噪声过程的类型和大小，在其他与量子效应有关的科技领域中也有重要应用。

量子信息可能应用

近期：

- 实用量子密码
- 量子隐形传态
- 量子通信网络

中期：

- 量子处理器
- 模拟量子系统

长期：

- 大数因子分解
- 求分立对数
- 量子搜寻

❼ 量子信息论

量子信息论的基本目的

▲鉴别量子力学中稳定资源的基本类型，
如，量子比特，Bell态等。

▲鉴别量子力学中动力学过程的基本类型
如，存储器(memory)，量子信息传输，量子态的复制，保护量子信息处理免除噪声影响的过程等。

▲鉴别实现基本动力学过程所付出的资源代价(resource tradeoffs)
如，采用噪声通信通道在两用户之间可靠传送量子信息所需要的最少信源。

量子信息论若干问题

经典信息论的基本结果是香农无噪声通道编码定理和香农噪声通道编码定理。

什么是信源(information source)?

经典信源用概率集合$p_i, j=1,2,\cdots,d$来描述，每用一次信源会导致以p_j概率随机地发出“字符”j，信源的各次使用相互独立。

香农无噪声通道编码定理指出，用概率p_j描述的经典信源可以被压缩，平均地讲，每次使用信源可用$H(p_j)$比特信息来表示，$H(p_j)=-\sum_j p_j \log(p_j)$是信源概率分布的函数，称为香农熵。

若用少于这个比特值的信息来发送，则最终恢复出被发送信息的误差会变大。信息论的研究目的：鉴别两类稳定资源：比特和信源；鉴别两阶段动力学过程：压缩信源，消除压缩并复原信源；最后，找到确定采用最优数据压缩所消耗资源的定量判据。

- 香农噪声通道编码定理给出经由噪声通道可靠传送的信息量。假定我们要通过噪声通道将某些信源产生的信息传送到另个地方(可以是空间上另一点，也可是时间上另一点(存储问题))，基本思想是：采用纠错编码来编制信息，使得通道引入的任何噪声在通道终端都可以得到纠正。纠错编码是将足够冗余量引到经过通道传送的信息中，某些信息被破坏后仍然可恢复出原始信息，例如，假定传送单个比特，需要两个比特编码才能可靠地传送信息，那么这样的通道就具有半个比特的经典容量(capacity)。
- 这个定理可以达到信息论的三个目的：两类稳定资源：信源和经由通道传送的比特；三类动力学过程：主要过程是通道噪声，在纠错编码过程中编码和解码的过程；若要可靠地实现信息传送，采用最优纠错方案需要引进多少冗余度。

经由量子通道传送的量子信息

什么是量子信源？

量子信源用概率 p_j 和相应的量子态 $|\psi_j\rangle$ 的集合来描述，每使用一次信源，将以概率 p_j 产生量子态 $|\psi_j\rangle$，信源的每次使用彼此独立。

有无可能压缩来自这样的量子力学信息源的输出？

考察如下量子比特信源：

以概率p输出态$|0\rangle$, 以概率$(1-p)$输出$|1\rangle$。这本质上等同于发射单个比特的经典信源，因此采用类似技术来压缩信源并令人奇怪。存储被压缩信源只需要 $H(p,1-p)$ 量子比特，$H(\ )$是香农熵函数。

若信源为：以概率p产生态 $|0\rangle$，以概率$(1-p)$产生态 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，情况将如何？

经典的数据压缩技术不再适用，因为我们无法识别态 $|0\rangle$ 和态 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$，是否能采用某种技术来实现压缩操作？

业已证明，在这种场合，某种类型的压缩仍然可能。有趣的是这种压缩可能不再是无误差的。由信源产生的量子态在压缩—解压缩过程可能会被发生畸变，尽管如此，我们要求这种畸变应当很小，而且在大块被压缩信源输出的极限下可以略去不计。为度量这种畸变，引入保真度（fidelity）来度量由压缩过程造成的平均畸变。量子数据压缩的思想是被压缩的数据应当能被以很好保真度得以恢复；在大块长度极限下，保真度趋于1即无误差。

Schumacher无噪声通道编码定理给出在可能以近似于1的保真度复原信息的这种限制下，实现量子数据压缩所需要的资源。在信源以概率p_j产生正交量子态$|\psi_j\rangle$的情况下，这个定理告诉我们，信源可以被压缩但不会超过经典极限$H(p_j)$。在信源产生非正交态的场合，Schumacher定理告诉我们，量子信源可以被压缩多少，但答案不是香农熵$H(p_j)$，而是新的熵量，即冯·诺依曼熵。

一般地讲，当且仅当$|\psi_j\rangle$ 为正交时冯·诺依曼熵与香农熵一致，否则

Alice用不同基$(|0\rangle,|1\rangle)$和$(|+\rangle,|-\rangle)$测量其EPR粒子，导致Bob的EPR粒子坍缩到态$|0\rangle$或$|1\rangle$，或者$|+\rangle$或$|-\rangle$。若Bob有能力识别$|0\rangle,|1\rangle,|+\rangle,|-\rangle$，则他可以瞬时地（超空速）得到有关Alice 的信息。

(*quantum distinguishably*)

经典信息原则上是可识别的，但量子力学不可能识别任意量子态。

非正交量子态的这种不可识别性是量子计算和量子信息的核心，它也是量子态含有无法被提取的隐信息的本质所在，这在量子计算和量子密码中起着关键性作用。

假定我们可以识别任意量子态，将意味着有能力利用纠缠来实现超光速的通信。设想Alice和Bob共享EPR对：

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$$

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

式中

$$\begin{cases}|0\rangle=\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)\\ |1\rangle=\frac{1}{\sqrt{2}}(|+\rangle-|-\rangle)\end{cases}$$

不可伪造的银行货币

想象银行在其制作的货币上打印一串(经典)数和一系列量子比特(处于态 $|0\rangle$ 和 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ 当中一个态)，除银行外，没人知道嵌入在货币上的这两个量子态顺序，银行保存一份经典数与所嵌入的量子态相对应的清单。这种货币是不可能被精确地伪造的，因为想要伪造的人不可能以百分百概率确定打印在货币上的量子比特的态，而不会破坏它。当商家收到银行货币时，他可以检验货币是否是伪造的，他打电话给银行，告诉货币的号码，并询问货币上应嵌印的量子态系列，然后按照银行的指导，采用 $|0\rangle$，$|1\rangle$ 或 $(|0\rangle+|1\rangle)/\sqrt{2}$，$(|0\rangle-|1\rangle)/\sqrt{2}$ 为基矢来测量子比特，以检验该货币的真实性，伪造者被发现的概率随被检验的量子比特数目以指数增长到1。这种想法是量子密码方案的基础，它演示了非正交量子态的不可识别性的用处。

❽ 量子测量

量子力学假定封闭量子系统演变是么正演化。量子测量是外部装置与被测量子系统发生相互作用，因而该量子系统不再是封闭的，也不一定会是么正演化。为描述测量对量子系统的影响，量子力学引入如下假设：

量子测量由测量算符集合$\{M_m\}$来描述，这些算符作用在被测系统的态空间上，标志m指在测量中可能发生的测量输出，若测量之前量子系统的态是$|\psi\rangle$，那么产生结果为m的概率为

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

而且，测量之后，系统的态为

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

测量算符满足完备性关系

$$\sum_m M_m^+M_m=I$$

完备性方程表示概率和为1的这样事实：

$$1=\sum_m p(m)=\sum_m\langle\psi|M_m^+M_m|\psi\rangle$$

这个方程对所有态$|\psi\rangle$都是满足，这就等效于完备性方程。

重要例子：在计算基矢上测量一个量子比特

定义两个测量算符：

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

显然测量算符是厄米的：

$$M_0^2 = M_0, \quad M_1^2 = M_1$$

满足完备性关系：

$$I = M_1^+ M_1 + M_0^+ M_0 = M_1 + M_0$$

假定被测量子比特为

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

测量得到输出为0的概率为

$$p(0) = \langle\psi|M_0^+ M_0^1|\psi\rangle = |\alpha|^2$$

类似地

$$p(1) = |\beta|^2$$

测量之后的量子态：

$$\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle, \quad \frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|}|1\rangle$$

测量装置本身也是量子力学系统，因此待测系统和被量系统构成一个封闭的量子系统，按照量子力学的基本假设，它应用么正演化来描述，那么从这个假设出发能否推导上述关于量子测量的假设呢？迄今物理学家仍未有统一看法，因此，不妨仍采用“量子测量的基本假设”。

量子态的识别　(量子测量假设的重要应用)

假定Alice从与Bob两人都知道的某固定态集中选出一个态 $|\psi_i\rangle(1\le i\le n)$。她将 $|\psi_i\rangle$ 传送给Bob，Bob的任务是识别由Alice发送来的态。若态 $|\psi_i\rangle$ 是正交的，Bob采用下列办法进行量子测量，就可以识别这些量子态：定义 $M_i\equiv|\psi_i\rangle\langle\psi_i|$ 测量算符，另一个附加测量算符M_0定义为正定算符的平方根，

$$M_0=I-\sum_{i\neq 0}|\psi_i\rangle\langle\psi_i|$$

这些算符满足完备性关系。若制备了态 $|\psi_i\rangle$，则

$$p(i)=\langle\psi_i|M_i|\psi_i\rangle=1,$$

因此有可能可靠地识别正交态 $|\psi_i\rangle$。

若态 $|\psi_i\rangle$不正交，可以证明，没有任何一种量子测量方案有能力识别这些态。

想法是：Bob进行以测量算符M_j描述的测量，输出为j，Bob根据测量的输出，企图用某种规则$i=f(j)$来猜测i是什么。为什么Bob无法识别非正交态$|\psi_1\rangle$和$|\psi_2\rangle$的关键点是，$|\psi_2\rangle$可以分解成平行于$|\psi_1\rangle$和与$|\psi_1\rangle$正交的两部分，假设j是使$f(j)=1$的测量输出，亦即当Bob观察到j他便猜测态是$|\psi_1\rangle$，但是$|\psi_2\rangle$有平行$|\psi_1\rangle$的部分，因此当制备态$|\psi_2\rangle$时，仍然有非零的概率得到输出j，因而Bob有可能会做出错误的识别。

非正交态不可识别的证明

假定识别非正交态$|\psi_1\rangle$和$|\psi_2\rangle$的实验是可能的，若制备的态是$|\psi_1\rangle(|\psi_2\rangle)$，那么测量$j$使得的$f(j)=1(f(j)=2)$概率必定等于1，

定义$E_i \equiv \sum_{j:f(j)=i} M_j^+ M_j$，这个观察结果可以写成：

$$\langle\psi_1|E_1|\psi_1\rangle=1,\ \langle\psi_2|E_2|\psi_2\rangle=1$$

$$\because \sum_i E_i = I\ ,$$

$$\therefore \sum_i \langle \psi_i | E_i | \psi_i \rangle = 1$$

$$\because \langle \psi_1 | E_1 | \psi_1 \rangle = 1$$

必需有

$$\langle \psi_1 | E_2 | \psi_1 \rangle = 0\ ,$$

$$\therefore \sqrt{E_2} | \psi_1 \rangle = 0$$

假定将$|\psi_2\rangle$分解成

$$|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\varphi\rangle\ ,$$

式中$|\varphi\rangle$正交于$|\psi_1\rangle$，$|\alpha|^2 + |\beta|^2 = 1$。

由于$|\psi_1\rangle$和$|\psi_2\rangle$非正交，故$|\beta| < 1$，

那么，$\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$

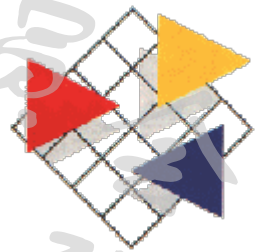
这会导致矛盾结果：

$$\langle \psi_2 | E_2 | \psi_2 \rangle = |\beta|^2 \langle \varphi | E_2 | \varphi \rangle \le |\beta|^2 < 1$$

(与$\langle \psi_2 | E_2 | \psi_2 \rangle = 1$矛盾)

上式中最后不等式来自

$$\langle \psi_2 | E_2 | \psi_2 \rangle \le \sum_i \langle \varphi | E_i | \varphi \rangle = \langle \varphi | \varphi \rangle = 1$$



投影测量
(Projective measurements)

投影测量是一般测量假设的特殊情况，其应用广泛。

所谓“投影测量”指：它用可观测量M描述，M是作用在待测系统的态空间上的厄米算符，可观测量具有谱分解性质:

$$M = \sum_m m P_m$$

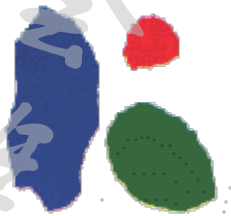
式中P_m是投影到本征值为m的M本征空间上的投影子，

测量的可能输出对应于可观察量的本征值。若测量$|\psi\rangle$，则得到结果为m的概率是

$$P(m) = \langle \psi | P_m | \psi \rangle$$

给出输出为后，量子系统在测量之后即刻变为

$$\frac{P_m|\psi\rangle}{\sqrt{P(m)}}$$



投影测量可以看成为测量假设的特殊情况。除了要求满足完备性关系 $\sum_m M_m^+ M_m = I$ 外还要M_m满足是正交投影的条件，即：

M_m是厄米的，且$M_m M_{m'} = \delta_{mm'} M_m$

有了这些附加限制，量子测量假设就简化上述定义的投影测量。

投影测量的特性：

测量的平均值

$$E(M) = \sum_m mP(m) = \sum_m m\langle\psi|P_m|\psi\rangle$$
$$= \langle\psi|(\sum_m mP_m)|\psi\rangle$$
$$= \langle\psi|M|\psi\rangle$$

测量M的标准偏差

$$\Delta(M) = \left\langle (M - < M >)^2 \right\rangle$$
$$= \left\langle M^2 \right\rangle - \left\langle M \right\rangle^2$$

例，假定$\vec{v}$是假定三维单位矢量，那么可定义如下可观察量 $\vec{v}\cdot\vec{\sigma} \equiv v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3$

测量这个观察量习惯上称为“沿$\vec{v}$轴测量自旋”。

POVM测量

量子测量假设包含有两个基本内容：

①给出描述测量统计特殊的规则。即各种可能测量输出的概率；

②给出描述系统测量后量子态的规则。

若对测量后的量子态兴趣不大，则可采用特别有用的数学工具，称POVM公式(Positive Operator-Valued Measure)。

假定对处于态$|\psi\rangle$的量子系统实施用测量算符M_m所描述的测量，那么输出m的几率为

$$p(m)=\langle\psi|M_m^{+}M_m|\psi\rangle$$

若定义$E_m\equiv M_m^{+}M_m$,那么由量子测量假设和线性代数可知，E_m是使得$\sum_m E_m=I$和$p(m)=\langle\psi|E_m|\psi\rangle$的正定算符。算符集合$E_m$足以确定不同测量输出的几率，算符$E_m$称为该测量POVM基元(element)。完备集合$\{E_m\}$叫做POVM。

例1. 考察用测量算符P_m描述的投影测量。其中P_m是满足$P_m P_{m'} = \delta_{mm'} P_m$的投影子，在这种场合，所有POVM基元与测量算符本身相同，因为

$$E_m = P_m^+ P_m = P_m$$

假定$\{E_m\}$是满足$\sum_m E_m = I$的某任意正定算符集合，可以证明存在用来定义由POVM $\{E_m\}$所描述的测量算符M_m集合。

定义$M_m \equiv \sqrt{E_m}$，则有

$$\sum_m M_m^+ M_m = \sum_m E_m = I$$

因此集合$\{M_m\}$描述具有POVM $\{E_m\}$的测量。

基于这个理由，可以方便地定义POVM为任意算符集合$\{E_m\}$，后者满足

(a) 每个算符E_m为正定;

(b)完备定性关系

$$\sum_m E_m = I$$

它表示几率和为1的事实。给定POVM $\{E_m\}$，输出m的几率为

$$p(m) = \langle \psi | E_m | \psi \rangle$$

例2. 假定Alice发出给Bob一个量子比特，后者制备在态 $|\psi_1\rangle=|0\rangle$ 和 $|\psi_2\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ 中的任一个。我们知道，Bob不可能完全确定他所接受到的粒子处于那一个态。但是他有可能实现这样的测量，其中某些次的测量可以识别量子态，而决不会发生识别上的错误。考察包含下列三个基元的POVM：

$$E_1=\frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|$$

$$E_2=\frac{\sqrt{2}}{1+\sqrt{2}}\frac{(|0\rangle-|1\rangle)(\langle 0|-\langle 1|)}{2}$$

$$E_3=I-E_1-E_2$$

可以直接验证，这些算符是满足 $\sum_m E_m=I$ 的正定算符，因而构成合理的POVM。

假定，发送给Bob的态$|\psi\rangle_1 = |0\rangle$，Bob实旋由POVM$\{E_1, E_2, E_3\}$描述的测量，他观测$E_1$到的几率为0，因为$\langle 0|E_1|0\rangle = 0$。因此，若Bob测量结果是$E_1$，则他完全可以断定他所接收到的量子态是$|\psi_2\rangle$。类似地，若Bob测量到$E_2$，则他所接收到的必是$|\psi_1\rangle$，当然有时候Bob会得到$E_3$的测量输出，这时他就无法识别他所接收到的量子态。关键点是Bob决不会作出错误的判断。这种可信性来自于这样的代价，即Bob有时对态的识别会一无所知。

这个例子演示了POVM公式的用处，它特别适用于只关心测量统计特性的场合。

复合系统的量子测量

假定有一量子系统，态空间为Q，我们想对系统Q实施由测量算符M_m所描述的测量。为此，引进辅助系统，态空间为M，它具有正交态$|m\rangle$，它与我们要测量的可能输出值一一对应。这个辅助系统可以看成只是个数学装置，也可以在物理上理解为引入的额外量子系统，其态空间具有所需要的性质。

令$|0\rangle$为M的任意固定态，定义算符U作用在QM的直积态$|\psi\rangle|0\rangle$上：

$$U|\psi\rangle|0\rangle \equiv \sum_m M_m|\psi\rangle|m\rangle$$

应用态$|m\rangle$的正交性和完备性关系$\sum_m M_m^+ M_m = I$，可以看到，U保持形式为$|\psi\rangle|0\rangle$的态之间的内积：

$$\begin{aligned}\langle\varphi|\langle 0|U^+U|\psi\rangle|0\rangle &= \sum_{m,m'}\langle\varphi|M_m^+M_m|\psi\rangle\langle m|m'\rangle \\ &= \sum_m \langle\varphi|M_m^+M_m|\psi\rangle \\ &= \langle\varphi|\psi\rangle\end{aligned}$$

可以证明，U可以扩展为作用在空间$Q \otimes M$上的么正算符，仍记为U。

假定对这两个系统实施投影测量，用投影子 $P_m = I_Q \otimes |m\rangle\langle m|$表示。输出$m$发生的几率为

$$\begin{aligned} p(m) &= \langle\psi|\langle 0|U^+ P_m U|\psi\rangle|0\rangle \\ &= \sum_{m',m''} \langle\psi|M_{m'}^+ \langle m'|(I_Q \otimes |m\rangle\langle m\rangle M_{m''}|\psi\rangle m'') \\ &= \langle\psi|M_m^+ M_m|\psi\rangle \end{aligned}$$

这正是“量子测量假设”给出的测量结果，在结果为m测量之后，QM系统的联合态由下式给出

$$\frac{P_m U|\psi\rangle|0\rangle}{\sqrt{\langle\psi|U^+ P_m U|\psi\rangle}} = \frac{M_m|\psi\rangle|m\rangle}{\sqrt{\langle\psi|M_m^+ M_m|\psi\rangle}}$$

由此可知，系统M在测量之后的态为$|m\rangle$，Q系统的态为

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

这正是量子测量假设给出的。因此么正动力学和投影测量，以及引入辅助系统的能力，可使得“量子测量假设”的任何形式测量均可得以实现。

量子态系综的测量公式

系统的密度算符 $\rho \equiv \sum_i P_i |\psi_i\rangle\langle\psi_i|$

封闭系统的演化由么正算符 U 表示，则有 $\rho \xrightarrow{U} U\rho U^+$

设测量算符为 M_m，则输出为 m 的几率为 $p(m) = tr(M_m^+ M_m \rho)$

测试之后的态为

$$\rho_m = \frac{M_m \rho M_m^+}{tr(M_m^+ M_m \rho)}$$

设量子系统以概率 p_i 制备在态 ρ_i 上，该系统的密度矩阵为

$$\rho = \sum_i p_i \rho_i$$

式中 $\rho_i = \sum_j p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$

假设对 ρ 测量(算符为 M_m)，但测量结果丢失掉，即不知准确的 m 值。于是测量之后系统以几率 p_m 处于态 ρ_m 上，系统状态为

$$\begin{aligned}\rho &= \sum_m p(m)\rho_m \\ &= \sum_m tr(M_m^+ M_m \rho) \frac{M_m \rho M_m^+}{tr(M_m^+ M_m \rho)} \\ &= \sum_m M_m \rho M_m^+\end{aligned}$$


Thank you
very much!
灿郭
印光