

信息

量子信息

© L^eP_tC (萌狸)

笔记项目主页: <http://leptc.github.io/lenote>



精

(同〈量子〉)

Nielsen & Chuang. Quantum Computation and Quantum Information. Cambridge

└ 中译: 赵千川. 量子计算和量子信息 (一: 量子计算部分, 二: 量子信息部分). 清华大学出版社

参

Preskill@Caltech 讲义

基本实验

电子通过双缝有干涉条纹 (Merli 1976 电子双棱镜, 此前一直是思想实验) → **波粒二象性**
[发生干涉时, 粒子性 $|c_1|^2 + |c_2|^2$, 波动性 $|c_1 + c_2|^2 = |c_1|^2 + |c_2|^2 + 2|c_1||c_2|\cos\theta$, 即多了条纹]
Zeilinger Tonomura

累积实验 每次只发射一个粒子, 统计打在接收屏上的位置, 有条纹 (蔡林格 1982 中子, 殿村 1989 电子)
complementarity principle

互补原理 / 并协原理 (玻尔 1927) 微观物体的波动性与粒子性互补

which way

哪条路实验 监测每个粒子通过了哪条缝, 监测手段提取信息能力越强, 条纹衬比度越低 (皮查德 1995, 用共振光照原子) 退相干的直接原因, 不是光子散射带来动量干扰, 而是提取信息后带来随机相移

Scully micromaser
(斯卡利 1991, 激发态原子通过微波激射腔, 可从哪个腔中有光子判断哪条路) 退相干与 $\Delta x \Delta p$ 无关
退相干源于原子态和腔态的纠缠, 若又擦除纠缠信息 (对腔态偏迹), 则相干恢复

quantum eraser

量子擦除实验 (乔瑞宇 1992) 正交偏振的光无条纹, 再做同向检偏可恢复条纹 (但记录粒子数减半)

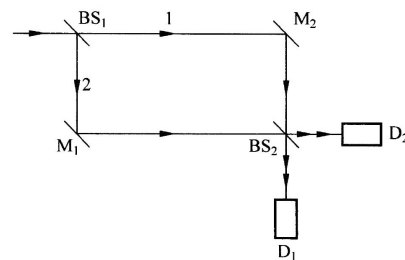
delayed choice Wheeler Hellmuth

延迟选择实验 (惠勒 1978) (赫尔穆特 1987 实验)

无 BS_2 时, $D_1 D_2$ 各 50%, 有 BS_2 时, 光程差可调, 一个 0% 另一个 100%

延迟选择: 在光脉冲通过 BS_1 后再决定是否放入 BS_2

结论: 和非延迟的实验结果相同



SG 实验

Stern-Gerlach experiment

施特恩 - 格拉赫实验 (1922 银原子 ($4d^{10}5s^1$ 核 $\frac{1}{2}^-$), 1927 氢原子) 加热射出一束中性原子, 沿 y 方向通过 z 方向有梯度的磁场, 原子束分裂成分立的两束 → 电子除轨道角动量外还有内部转动自由度 (电子自旋)

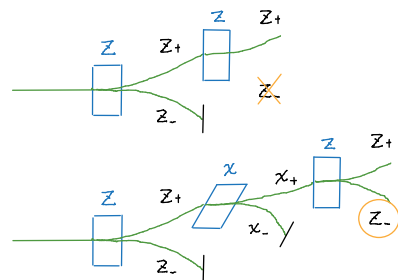
(如果用自由电子束, 自旋和轨道磁矩带来的分裂相当)

sequential Stern-Gerlach experiment

级联施特恩 - 格拉赫实验 取 S_z^+ 束后测 S_x 得 S_x^\pm (按经典应都得零), 取 S_z^+ 后测 S_x 并取 S_x^+ 后又测 S_z 得 $S_z^\pm \rightarrow \hat{S}_x, \hat{S}_z$ 不能同时测准

可用经典的偏振光类比: S_z^\pm 是 $0^\circ, 90^\circ$ 线偏, S_x^\pm 是 $45^\circ, 135^\circ$ 线偏, S_y^\pm 是 L, R 圆偏

注 如果测量的可观测量仅参照一个基底, 量子实验的确允许经典解释



贝尔态

Bell state / EPR pair

贝尔态 / EPR 对 2 量子比特, 关联 $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, 反关联 $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ → 此 4 态称为 **贝尔基**

Einstein-Podolsky-Rosen paradox space-like separated

EPR 佯谬 (爱因斯坦 1935) 即使是类空分隔的纠缠对, 测量其中一个也会立刻导致另一个坍缩

① 量子力学认为未被观察的粒子尚不具有物理性质的测量值 → 导致存在超距作用

hidden variable

② 本来是有确定值的, 量子力学理论不完备, 引入某个隐藏物理量 **隐变量** 可使测量值能准确预测

Alice 和 Bob 分别持 EPR 对中的一个, 分别沿 \vec{a}, \vec{b} 方向测自旋, 得结果 ± 1 (实验的话存在丢失还有 0)

两人结果相乘, 重复多次实验求平均, 定义 **自旋关联** $\langle \vec{a}, \vec{b} \rangle \equiv \langle \psi | \hat{\sigma}_a \hat{\sigma}_b | \psi \rangle$ 量子力学 $= -\cos(\vec{a} \wedge \vec{b})$ (高量)

Clauser Horne Shimony Holt

local hidden variable theory

CHSH 不等式 Alice 沿 a_1, a_2 方向测, Bob 沿 b_1, b_2 测, 可证明任何 **局域隐变量理论** 会得

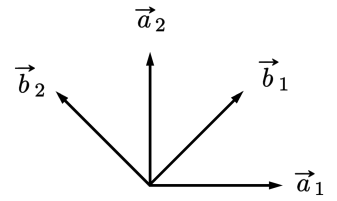
$$|\langle \vec{a}_1, \vec{b}_1 \rangle + \langle \vec{a}_2, \vec{b}_1 \rangle + \langle \vec{a}_2, \vec{b}_2 \rangle - \langle \vec{a}_1, \vec{b}_2 \rangle| \leq 2$$

既然实验结果预先确定, 则可以被列举, 设系统处于测得 $(\alpha_1, \alpha_2, \beta_1, \beta_2)$ 态的概率为 p , 计算:

$$a_1 b_1 + a_2 b_1 + a_2 b_2 - a_1 b_2 = (a_1 + a_2) b_1 + (a_2 - a_1) b_2 = \pm 1 \quad (\text{因为要么 } a_1 = a_2 \text{ 或 } a_1 = -a_2, \text{ 必有一项为零})$$

另可以证明 $\langle \alpha_1 \beta_1 + \alpha_2 \beta_1 + \alpha_2 \beta_2 - \alpha_1 \beta_2 \rangle = \langle \alpha_1 \beta_1 \rangle + \langle \alpha_2 \beta_1 \rangle + \langle \alpha_2 \beta_2 \rangle - \langle \alpha_1 \beta_2 \rangle$, 故测量结果平均值

$$\langle \alpha_1 \beta_1 + \alpha_2 \beta_1 + \alpha_2 \beta_2 - \alpha_1 \beta_2 \rangle \equiv \sum_{\alpha_1 \alpha_2 \beta_1 \beta_2} p(\alpha_1, \alpha_2, \beta_1, \beta_2) (\alpha_1 \beta_1 + \alpha_2 \beta_1 + \alpha_2 \beta_2 - \alpha_1 \beta_2) \\ \leq \sum_{\alpha_1 \alpha_2 \beta_1 \beta_2} p(\alpha_1, \alpha_2, \beta_1, \beta_2) \times 2 = 2$$



对于量子力学, 沿如图方向可得 $|\langle \vec{a}_1, \vec{b}_1 \rangle + \langle \vec{a}_2, \vec{b}_1 \rangle + \langle \vec{a}_2, \vec{b}_2 \rangle - \langle \vec{a}_1, \vec{b}_2 \rangle| =$

$\cos \frac{\pi}{4} + \cos \frac{\pi}{4} + \cos \frac{\pi}{4} - \cos \frac{3\pi}{4} = 2\sqrt{2}$ **注** CHSH 不等式的代数上限是 4 (Popescu 1994)
non-signalling box stronger-than-quantum Popescu-Rohrlich box information causality

(对于非信令盒子模型, 数学上还存在比量子还强的关联 (如 PR 盒), 但都违背 **信息因果律**)

(CHSH 1969 等) 实验验证贝尔不等式被破坏, 可能要放弃定域性或实在性

locality reality
定域性 物体只能被其紧接的周围所直接影响 **实在性** 物理性质独立于观测行为而存在

GHZ 态

Greenberger-Horne-Zeilinger state

GHZ 态 (1990) 3 量子比特纠缠态, z 基换到 x 基下:

$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = (|x_+x_+x_+\rangle + |x_+x_-x_-\rangle + |x_-x_+x_-\rangle + |x_-x_-x_+\rangle)$ ($\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ 则是所有位取反)
 特点: 任意 2 位已知后, 可确定第 3 位的态 \rightarrow **量子秘密共享**

$[\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = \frac{1}{2\sqrt{2}}[(|y_+\rangle + |y_-\rangle)^{\otimes 2}(|x_+\rangle + |x_-\rangle) - \frac{1}{i}(|y_+\rangle - |y_-\rangle)^{\otimes 2}(|x_+\rangle - |x_-\rangle)] = |y_+y_+x_+\rangle + \dots]$

Alice, Bob, Charlie 各自沿 x 或 y 测自旋, 现实发现, 当两人测 Y 一人测 X 时, 结果之积总为 $+1$
 结果预先确定, 照旧列举, 在“任意 $2Y1X$ 得 $+1$ ”的限制下只有 8 种可能的状态组合:

$\begin{bmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix}$ 都 $=1$, $\begin{bmatrix} 1 & -1 & -1 \\ 1 & -1 & -1 \end{bmatrix}$ 等 3 种, $\begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & 1 \end{bmatrix}$ 等 3 种, $\begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \end{bmatrix}$

因此当三人都测 x 时结果为 $+1$, 然而量子力学预测结果为 -1 (用的是 $|\text{GHZ}_-\rangle$ 态)

GHZ 定理 三粒子纠缠态, 存在一组对易可观测量, 直接确定地(而非统计地)给出与经典不相容的结果
 (潘建伟 1999 实验实现) 用光的两偏振态 $|H\rangle, |V\rangle$

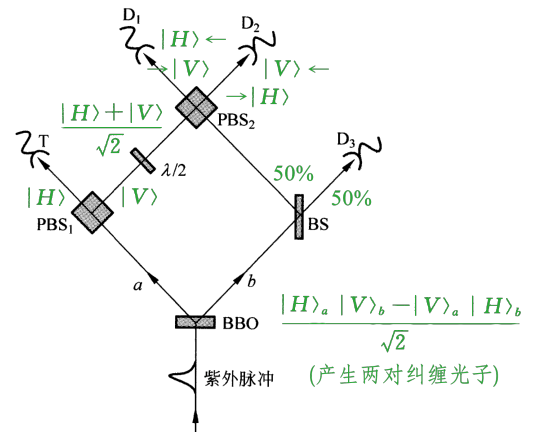
用一束紫外脉冲产生两对(4 个)纠缠光子, 一个作触发, 脉冲 (200 fs) 远小于相干时间 (500 fs) 以保证纠缠

$T, D_{1\sim 3}$ 同时触发时, T 必然记录 $|H\rangle$, 其伴侣必为 $|V\rangle$ 沿 b , 另一对光子 a 束为 $|V\rangle$, 在 PBS_1 全反射后变叠加态, b 束为 $|H\rangle$, 有两种可能:

① 伴侣到 D_3 , a 束 50% 的 $|H\rangle$ 进 D_2 , b 束进 D_1 , 得 $|HHV\rangle$

② 伴侣到 D_2 , a 束 50% 的 $|V\rangle$ 进 D_1 , b 束进 D_3 , 得 $|VVH\rangle$

最终产生 $\frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle)$ [加号另证]



量子信息

quantum computation QCP

① **量子计算** 通用量子计算, 量子模拟计算

communication cryptography

QKD

QSS

QSDC

QAA

② **量子通信** ① 量子密码学: 量子密钥分发, 量子秘密共享, 量子安全直接通讯, 量子振幅放大
 teleportation dense coding steering

② 量子通讯: 超空间传态, 密集编码, 量子导向, 量子成像

metrology

③ **量子计量** 量子钟

量子比特

qubit

任何双态量子体系都可称为一个 **量子比特**, 状态记为 $|\psi\rangle = a|0\rangle + b|1\rangle \xrightarrow[\text{取 } a \text{ 为实}]{\text{归一}} \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$

(注: 量子信息的习惯是 $|0\rangle$ 代表 $|z_+\rangle$, $|1\rangle$ 代表 $|z_-\rangle$, 这样矩阵就左边从 $|00\dots\rangle$ 编码开始)

等效内存 n 量子比特的状态含 2^n 个复振幅 (不进行测量, 则隐含大量信息, 且随比特数指数上升)

qutrit

(注: 用三级量子系统的任何差别理论上来看都可忽略)

Bloch sphere

$|\psi\rangle$ 可看作二维复向量空间中单位向量 \rightarrow **布洛赫球** 面

任意混合态量子比特的密度矩阵可写为 $\hat{\rho} = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma})$, $|\vec{r}| \leq 1$

极化矢量 $\vec{r} = |r|(\sin\theta \cos\phi, \sin\theta \sin\phi, \cos\theta) = \langle\psi|\hat{\sigma}|\psi\rangle =$

$$\begin{bmatrix} a^* & b^* \end{bmatrix} \begin{pmatrix} \hat{\sigma}_x \\ \hat{\sigma}_y \\ \hat{\sigma}_z \end{pmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{pmatrix} a^*b + b^*a, i(b^*a - a^*b), a^*a - b^*b \end{pmatrix}$$

$\text{tr}(\hat{\rho}^2) = \frac{1}{2}(1 + |\vec{r}|^2)$, 当 $a^2 + b^2 = 1$ 时 $|\vec{r}| = 1$ 表示 **纯态**

$|\vec{r}| = 0$ 时 $\hat{\rho} = \frac{I}{2}$ 表示 **完全混合态** (不仅指 $|0\rangle, |1\rangle$ 出现概率相等, 而且所有相对相角 ϕ 都有可能出现)

$$\hat{\rho}^{\text{纯态}} = \begin{bmatrix} a^*a & b^*a \\ a^*b & b^*b \end{bmatrix} \xrightarrow{\text{一般}} \frac{1}{2} \begin{bmatrix} 1+r_z & r_x - ir_y \\ r_x + ir_y & 1-r_z \end{bmatrix} \quad \text{例 } |z_+\rangle: \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, |z_-\rangle: \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, |x_+\rangle: \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, |x_-\rangle: \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

affine map

定理 任意保迹量子运算的图像是布洛赫球到自身的仿射映射, 么正变换对应布洛赫球面的旋转

测量

量子测量由一组测量算符 $\{\hat{X}_x\}$ 描述, 这些算符作用在态矢上以概率 $p_x = \langle\psi|\hat{X}_x^\dagger \hat{X}_x|\psi\rangle$ 得实验结果 x , 测量后体系的状态变成 $\frac{1}{\sqrt{p_x}} \hat{X}_x|\psi\rangle$ (要求测量算符完备 $\sum \hat{X}_x^\dagger \hat{X}_x = I$, 从而概率和 $\sum p_x = 1$)

推论 先测 X_i 再测 X_j 等价于单次测量 $X_k \equiv X_j X_i$

Positive Operator-Valued Measure

POVM 测量 可知 $\hat{E}_x \equiv X_x^\dagger \hat{X}_x$ 是半正定算符, 满足完备性(不要求正交)的 $\{\hat{E}_x\}$ 称为一个 POVM

(不考虑测量后处于什么状态, 不必具有可重复性, 适用于如光子被测量后被吸收了的情况)

projective measurement

$[\hat{E}_x \text{ 构成正交投影算符}] \rightarrow$ **投影测量** 厄米算符 \hat{X} 有谱分解 $\hat{X} = \sum x \hat{P}_x$, 投影算符 $\hat{P}_x = |x\rangle\langle x|$,

collapse

则测得 x 的概率为 $p_x = \langle\psi|\hat{P}_x|\psi\rangle$, 测量后状态坍缩到本征态 $\frac{1}{\sqrt{p_x}} \hat{P}_x|\psi\rangle$

repeatability

投影测量有 **可重复性** 坍缩后重复测量, 每次都得 x , 不改变状态

定理 非正交的量子态不能可靠区分 (以概率 1 得不同结果) (否则就可以利用纠缠对超光速通讯了)

[设存在测量 $E_i, i=1, 2$ 使 $\langle\psi_i|E_i|\psi_i\rangle=1$, 由测量算符完备, 有 $\sum_i \langle\psi_1|E_i|\psi_1\rangle=1$, 从而 $\langle\psi_1|E_2|\psi_1\rangle=1-1=0$ 然而 $|\psi_1\rangle, |\psi_2\rangle$ 并非正交, 与 $\langle\psi_2|E_2|\psi_2\rangle=1$ 矛盾]

例 要区分 $|\psi_1\rangle=|0\rangle, |\psi_2\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, 靠投影测量有概率误判, 用 POVM 测量可不误判 (代价是有概率不能区分):

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|, E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} \frac{1}{2} (|0\rangle - |1\rangle)(\langle 0| - \langle 1|), E_3 = I - E_1 - E_2$$

测得 1 必为 ψ_2 , 测得 2 必为 ψ_1 , 测得 3 无法区分

quantum money

量子钞 银行在发行的钞票上印上经典序列号和非正交量子比特序列, 只有银行保存这两者匹配的列表, (可信赖的) 商家想验证真伪时, 把经典序列号告诉银行, 银行指示商家按哪种基来测量量子比特

量子门

quantum gate

量子门 么正性是唯一的要求 (故总可逆)

单比特

Pauli gate

泡利门 $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (量子非门, 交换幅度), $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Hadamard gate

哈达玛门 $H = \frac{X+Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, 即 $|0\rangle \rightarrow |x_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \rightarrow |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $H^2 = I$ (先绕 y 转 90° , 再绕 x 转 180°)

相位门 $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ (Z 门的根号) $\left[\frac{\pi}{8} \text{ 门} \right] T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \propto \hat{R}_z(\frac{\pi}{4})$ (S 门的根号)

$$[e^{i\hat{\sigma}_n\theta} = I \cos \theta + i\hat{\sigma}_n \sin \theta] \quad \hat{R}_z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}, \quad \hat{R}_x(\theta) = \begin{bmatrix} \cos \theta/2 & -i \sin \theta/2 \\ -i \sin \theta/2 & \cos \theta/2 \end{bmatrix}, \quad \hat{R}_y(\theta) = \begin{bmatrix} \cos \theta/2 & -\sin \theta/2 \\ \sin \theta/2 & \cos \theta/2 \end{bmatrix}$$

定理 任意单量子比特门 (2×2 么正矩阵) 可分解为 $U = e^{i\alpha} \hat{R}_n(\theta) = e^{i\alpha} \hat{R}_z(\beta) \hat{R}_y(\gamma) \hat{R}_z(\delta) \rightarrow e^{i\alpha} A X B X C$

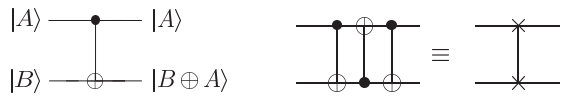
常用 线路恒等式 $XYX = -Y$, $X\hat{R}_y(\theta)X = \hat{R}_y(-\theta)$, $HXH = Z$, $HYH = -Y$, $HZH = X$, $HTH = \hat{R}_x(\frac{\pi}{4})$

多比特

Controlled NOT

受控非门 |控制 c , 目标 t $\rightarrow |c, t \oplus c\rangle$ (控制比特为 0 则目标比特不变, 为 1 则翻转)

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad U_{SW} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad H^{\otimes 2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$



swap

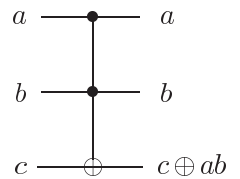
对换 3 个 CNOT, 中间的反放 $[|a, b\rangle \rightarrow |a, a \oplus b\rangle \rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \rightarrow |b, a\rangle]$

n 量子比特上的 H 变换: $H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{a,b} (-1)^{ab} |a\rangle \langle b|$

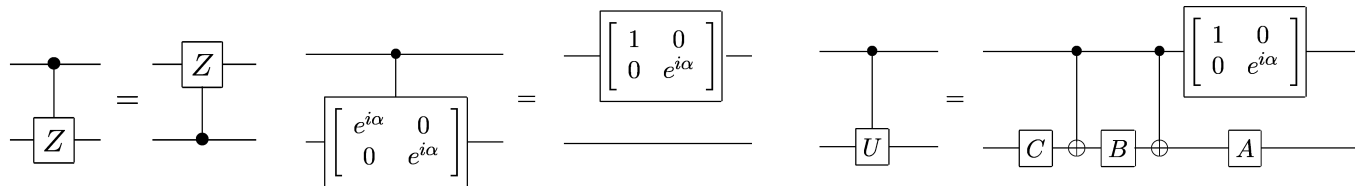
Toffoli / CCNOT

控控非门 $C^2(X)$, 可逆, 逆是自身, 可实现与 $c=0$, 非 $a=b=1$, 与非 $c=1$

\rightarrow 故量子机可以做经典计算 (量子机原则上不需要经典部分, 但有的话会更方便)



一般的 **受控 U 门** 实心点表示 1 时起作用, 空心圈表示 0 时起作用



用 Toffoli 门可构造出经典的可逆电路 (完成计算之后把逻辑门逆序再操作一遍) 计算过程不消耗能量

通用门 最早确认的一组是受控非门 (CNOT) 加两个非平行的单量子比特门 (如 H 门加 $\frac{\pi}{8}$ 门), 可以任意精度近似任意酉运算, 后 (Yaoyun Shi 2002) 证明只用 Toffoli 门加上单比特的 H 门就可实现任意量子线路 (量子计算不过就是经典计算多个 H 门)

量子线路

initialization operation

rotation superposition

entanglement detection

① 初始化 ② 操作 (经典: 单:NOT, 双:NAND, 量子: 单:旋转 \rightarrow 叠加, 双:CNOT \rightarrow 纠缠) ③ 探测 acyclic

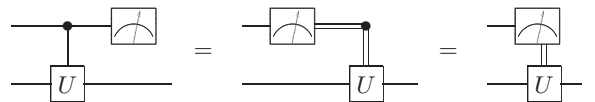
无环 量子线路不允许回路 (即无反馈) 线路不允许汇合, 禁止扇入扇出 (因为不可逆)

measurement

测量 把单量子比特状态变成 (依概率的) 经典比特状态, 经典线路用双线表示

principle of deferred measurement

推迟测量原理 总可以把测量从量子线路的中间步骤移到线路末端 (如果中间需用到测量结果, 可用量子运算代替)



principle of implicit measurement

隐含测量原理 量子线路中任何未终结的量子连线 (未被测量量子比特) 总可视作被测量

$[$ 第一量子比特的约化密度矩阵不受第二量子比特上测量的影响 $]$

结论 要使测量可逆, 它必须不揭示被测量子态的任何信息

no-cloning theorem

不可克隆定理 不可能制作未知量子态的拷贝 $[$ 量子理论是线性的 $]$ (可以有以概率成功克隆的方法)

$[$ 若 $\exists U$ 能 $|00\rangle \xrightarrow{U} |00\rangle, |10\rangle \xrightarrow{U} |11\rangle$, 则对于叠加态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 有 $|\psi 0\rangle \xrightarrow{U} (\alpha|00\rangle + \beta|11\rangle) \neq |\psi\rangle \otimes |\psi\rangle$ $]$

(U_{CN} 可以拷贝经典态)

tomography

量子态层析 通过反复制备相同量子态, 以不同方式测量, 建立量子态的完整描述

quantum repeater

量子中继器 不能直接放大或测量, 把距离切成很多段, 接连做量子传态

entanglement distillation

跑一段距离后纯度会降低 → **纠缠纯化**

贝尔态应用

4 种贝尔态可由 H 门后 CNOT 制备, 顺序反过来即为 **贝尔基测量**

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix}$$

superdense coding

超密编码 (Bennett 1992) Alice 和 Bob 分别持 EPR 对中的一个, Alice 想把 2 比特信息传给 Bob, 她只需: 若 $|00\rangle$ 不动, 若 $|01\rangle$ 做 X 门, 若 $|10\rangle$ 做 Z 门, 若 $|11\rangle$ 做 $ZX=iY$

然后她把手中的量子比特传给 Bob, Bob 做贝尔基测量即可

quantum teleportation

量子传态 (Bennett 1993, 潘建伟 1997) 无需量子通信信道就可转移量子态 (需经典通讯, 故未超光速)

[以 EPR 对 $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ 为例, Alice 持有左边那个, Bob 持右边那个, Alice 想把 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ 传给 Bob, 她把 $|\psi\rangle$ 和粒子放一起做贝尔基测量(上方 2 根线), 然后通过经典通讯告诉 Bob 结果(双线), Bob 根据结果做相应操作可恢复 $|\psi\rangle$: 若 $|00\rangle$ 不动, 若 $|01\rangle$ 做 X 门, 若 $|10\rangle$ 做 Z 门, 若 $|11\rangle$ 做 ZX]

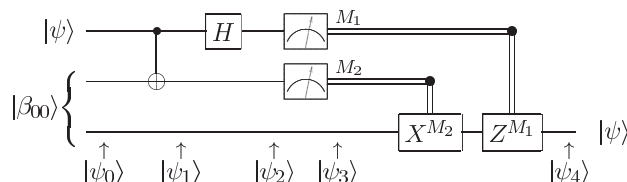
$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$$

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

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

→ 测量导致坍缩, 按前 2 位重新分组 →

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



结论 纠缠对是一种静态资源, 消耗一个 EPR 对加 2 经典比特通讯可实现 1 量子比特的传送

注 当 Alice 测量后, 未传经典消息前, Bob 端是 4 种量子态经典叠加, 可算得其 $\hat{\rho} = \frac{I}{2}$, 故不含任何信息

Quantum Secret Sharing

量子秘密共享 (Hillery 1999) ① Alice, Bob, Charlie 各持 GHZ 纠缠态的一个粒子 ② 三方随机选择在 x 或 y 方向做测量, 三方公布测量基 (B,C 先告诉 A, A 再公布所有) ③ Bob, Charlie 必须把它们的信息联合起来才能还原 Alice 的信息, 粒子利用效率为 $\frac{1}{2}$ (例如 A,B 测了 x, C 有 $\frac{1}{2}$ 概率也测了 x, 则 C 知 A B 同或反, B C 一起才能推出 A)

量子计算

目前只有 3 类已知优于经典算法的量子算法:

hidden subgroup discrete logarithm factoring

① **量子傅氏变换** 隐含子群问题, 离散对数, 求阶 → 求因子 (肖氏算法 1994) → 攻破 RSA (指数加速)

unsorted database search

quadratic

② **量子搜索** 无序数据库搜索 (葛氏算法 1996) (仅为根号加速, 但应用比肖氏广泛)

simulation

③ **量子模拟** (费曼 1982) 所需资源随问题规模线性增加 (量子搜索可视为一种量子模拟问题的解)

counting

量子计数 结合了 ① ② 两者

量子并行

equal superposition

n 个 H 门同时作用的效果是 **均衡叠加** $|0^n\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$ 设存在 U_f 作用是 $|x, y\rangle \xrightarrow{U_f} |y \oplus f(x)\rangle$,

对前 n 比特做 H 变换, 然后连接第 n+1 比特做 U_f , 可同时计算出所有函数值

$$|0^n\rangle |0\rangle \xrightarrow{H^{\otimes n}, U_f} \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle \quad (\text{此并行性不能直接利用, 因为一次测量只能坍出一个 } x)$$

量子傅变

离散傅氏变换是 $N=2^n$ 个复数集合 $\{x_j\}$ 到 $\{y_k\}$ 的变换 $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j$

设有幺正变换 $|j\rangle \xrightarrow{U} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$, 则 $\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{U} \sum_{k=0}^{N-1} y_k |k\rangle$

把 j 写成二进制 $j=j_n \cdot j_{n-1} \dots j_1$, 有量子傅氏变换的直积形式: (格里菲斯 1996)

$$|j\rangle \rightarrow 2^{-n/2} (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)$$

经典的 FFT 花 $N \lg(N) = n 2^n$ 步, 量子傅氏变换用 $(\lg N)^2 = n^2$ 步, 指数加速, 但计算结果不能直接利用

phase estimation

相位估计 设幺正算符 U 有一本征值为 $e^{2\pi i \varphi}$ 的本征矢 $|u\rangle$, 假定可以制备 $|u\rangle$, 要估计 φ

Shor's algorithm

肖氏算法 解决的是求素因子问题: 给出合数 N , 求其非平凡的素因子 $p \neq 1, N$, 算法包括两部分:

① 传统部分 (以下记 (a, b) 为最大公约数)

① 任选数字 $a < N$, 用经典算法 (如辗转相除法) 算 (a, N) , 若 $\neq 1$ 则已找到素因子 a

② 否则 a 与 N 互素, 问题化为求函数 $f(x) = a^x \bmod N$ 的周期 r (即 $f(x+r) = f(x)$)

③ 若 r 是奇数, 换个 a 重来, 若 $a^{r/2} \equiv -1 \bmod N$ 也要重来, 否则, $(a^{r/2} \pm 1, N)$ 就是 N 的素因子

例 分解 $N=14$, 取 $a=3$, 可验证 $3^0 \bmod 14 = 1, \dots, 3^6 \bmod 14 = 1$, 故周期 $r=6$, 是偶数,

$$3^3 + 1 = 28, 3^3 - 1 = 26, (28, 14) = 7, (26, 14) = 2, \text{故得 } N = 7 \times 2$$

② 量子部分

传统部分把问题化为了求周期 $f(x+r) = f(x), 0 < r < 2^L$, 可用量子傅立叶变换实现加速:

① 需用到 1 个寄存器, 初态为 $|0\rangle$, 和 $O(L)$ 个量子比特的存储器, 初始化为 $|0\rangle$

② 对第一个寄存器应用 H 门等, 产生叠加态 $\frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |0\rangle$

③ 需用到一个执行运算 $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ 的 **黑箱** U , (\oplus 表示模 2 加法)

应用 U 得到态 $\frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |f(x)\rangle \approx \frac{1}{\sqrt{r 2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i l x / r} |x\rangle |F(l)\rangle$, 其中 $|F(l)\rangle$ 是 $|f(x)\rangle$ 的傅立叶变换

$$|F(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=1}^{r-1} e^{-2\pi i l x / r} |f(x)\rangle \quad \text{④ 对第一个寄存器进行逆傅里叶变换 } \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{l/r}\rangle |F(l)\rangle$$

⑤ 测量第一个寄存器得到相位 l/r 的一个估计 $\widetilde{l/r}$ (l 是随机选取的) ⑥ 用连分式算法得到 r

例 还以 $N=14$ 为例, $N^2=196$, 需 $L=8, 2^L=256$

由于 $f(x)$ 以 6 为周期, 傅变后很多项近似相消, 留下 $[m \frac{2^8}{6}]$, $m=0, 1, \dots, 5$ 这些项概率幅明显不为零 $\frac{2^8}{6} \approx 42.67$, 故实验会得 43, 86, ... 等结果中的一个, 用连分式可还原出所渐进的分数 $\frac{256}{43} \approx 5.95 \approx 6$

量子搜索

Grover

葛氏算法 是一种无序数据库搜索算法, 通过一系列酉操作, 使要查找的态的振幅逐步放大到 1

设初态是 $|\beta\rangle$ (可推广到 M 个) 和其它各态 $|\alpha\rangle$ ($(N-M)$ 个) 的均衡叠加态 $|\psi\rangle = \frac{1}{\sqrt{N}} \sum |k\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i \notin \beta} |i\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \equiv \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \equiv \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |\beta\rangle$$

inversion about mean

均值反演运算 $\hat{O} = 2|\psi\rangle\langle\psi| - I$ [因为 $\hat{O}(\sum c_k |k\rangle) = \sum (2\langle c\rangle - c_k) |k\rangle$, 其中 $\langle c\rangle = \frac{1}{N} \sum c_k$]

oracle

设有一黑箱的作用是对要查找的态 $|\beta\rangle$ 的振幅取反 $2|\beta\rangle\langle\beta|-I$

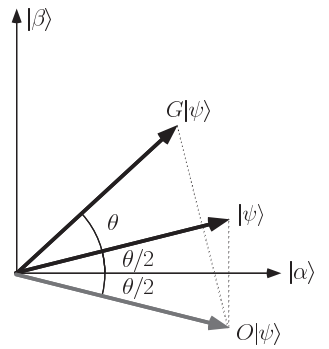
(物理上不知道 $|\beta\rangle$ 在哪, 但数据库中可对其操作) 记 $n=\lg N$

一次 Grover 迭代包括: ① $|\beta\rangle$ 态振幅取反 (相当于把 $|\psi\rangle$ 先对 $|\alpha\rangle$ 反射)

② 应用 H 变换 $H^{\otimes n}$ ③ $|0\rangle$ 态振幅取反 ④ 应用 H 变换 $H^{\otimes n}$

$H^{\otimes n}(2|0\rangle\langle 0|-I)H^{\otimes n}=2|\psi\rangle\langle\psi|-I$ (相当于再对 $|\psi\rangle$ 反射), 最终转过了 θ 角

$\lceil \sqrt{\frac{M}{N}} = \sin \frac{\theta}{2} \leq \frac{\theta}{2} \rceil$ 迭代 $\lceil \frac{\arccos \sqrt{M/N}}{\theta} \rceil \leq \lceil \frac{\pi/2}{\theta} \rceil \leq \lceil \frac{\pi}{4} \sqrt{\frac{N}{M}} \rceil$ 次可使 $|\psi\rangle$ 最接近 $|\beta\rangle$, 但最后不一定能和 $|\beta\rangle$ 完全重合 (经典要 $\frac{N}{2}$ 次)



phase matching

若修改第 ① ③ 步的取反为其它角度 φ, ϕ , 必须 $\varphi=\phi$ 才可能成功, 即 **相位匹配** 条件 (龙桂鲁 1999)
恰当地选择略小于 π 的角度可使最后结果刚好与 $|\beta\rangle$ 重合

量子通讯

Quantum Key Distribution

量子密钥分发 是一种用量子比特传输密钥的方案, 如果中间人想截获信息必然会引入干扰而被发现, 从而通讯双方可丢弃已被窃听的密钥重新传送

Bennett Brassard 1984

BB84 协议 ① 随机生成 $(4+\delta)n$ 比特数据用于密钥备选 ① Alice 随机使用 z 基 ($|0\rangle, |1\rangle$) 或 x 基 ($|+\rangle, |-\rangle$) 编码该比特串, 把量子比特发给 Bob (选基随机, \pm 按 ①) ② Bob 随机使用 z 基或 x 基测量收到的量子比特, 记录本征态 ③ 双方公布用过的测量基, 丢弃所有测量基不一样的 (至少要剩下 $2n$ 个, 否则重来) ④ 从 $2n$ 中挑出 n 个做窃听检测, 公布挑了哪几个 \rightarrow 如果双方测量结果全一致, 则存在窃听的概率为 $(\frac{3}{4})^n$, 剩下的 n 比特可作密钥

Bennett 1992

B92 协议 ① Alice 随机生成的比特数据 a , Bob 随机生成 b ① Alice 按 a 发送两种不正交的态 (如光子偏振 $90^\circ, 45^\circ$) 序列的量子比特 ② Bob 按 b 在这两个态的垂直方向上 ($0^\circ, -45^\circ$) 选基进行测量 ③ Bob 公布测量结果 c (而非测量基 b), 双方保留 $c=1$ 的测量结果 ④ 同理利用经典信道对比一部分结果来进行窃听检测 $\rightarrow a$ 作 Alice 的密钥 $= (1-b)$ 作 Bob 的密钥

(B92 的只使用 2 个状态, 但效率只有 $\frac{1}{4}$, 省探测器费时间)

Ekert 1991

E91 协议 ① 纠缠源发出 EPR 对分别被 Alice 和 Bob 接收 ① Alice 随机选用 $0^\circ, 45^\circ, 90^\circ$ 角度的基测量, Bob 随机选用 $45^\circ, 90^\circ, 135^\circ$ ② 双方公布测量基, 并公布用了不同测量基的测量结果 (相同基的保密) ③ 用 CHSH 不等式做窃听检测 (Alice 取方向 $0^\circ, 90^\circ$, Bob 取方向 $45^\circ, 135^\circ$) \rightarrow 窃听检测通过后, 相同基的测量结果可作密钥

QKD 的缺点在于只能发现窃听而不能避免窃听 \rightarrow

Quantum Secure Direct Communication

量子安全直接通信 (龙桂鲁 2003) 是可以安全地直接传输讯息的方案

① Alice 制备 $m+n$ 个 EPR 对, 都处于相同态, Alice 从每对中选一个粒子发给 Bob ② Bob 从他收到的 $m+n$ 个粒子序列中随机选出 n 个, 随机用 z 基或 x 基测量, 公布其选了哪些、测量基和结果 ③ Alice 测自己手中对应的 n 个粒子, 如果结果完全关联则剩下 m 个是安全的, (即使发现被窃听, 此时还没有传信息) ④ Alice 按密集编码的方法把要传递的信息 (加入适量用于安全检测的随机编码) 编在 m 个量子比特中发给 Bob ⑤ Bob 对手中 m 对粒子做贝尔基测量读出信息, 此时 Alice 再告诉 Bob 哪些是安全检测编码 (第一次安全检测已保证 Eve 无法获得信息, 第二次是为了判断是否信息被 Eve 破坏)

量子纠错

(历史上, 机械计算机困难的关键问题就在于出错 **信息学** 量子机同理, 纠错码相当于垒鸡蛋的架子)

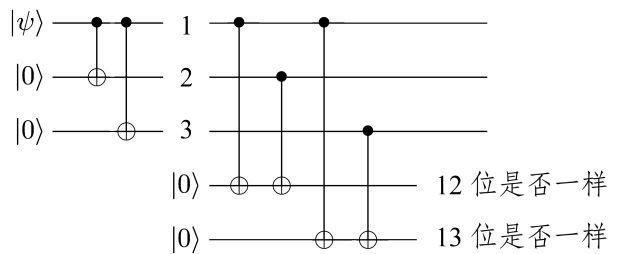
repetition code

问题 ① 不可克隆, 回答: 实现 **重复码** 并非直积态 (实际上是纠缠态)

例 $|0\rangle \rightarrow |000\rangle, |1\rangle \rightarrow |111\rangle$, 然后用 **多数判决** 解码

问题 ② 测量会破坏量子信息, 回答: **差错监测** 只指示出现了什么差错, 不揭示任何关于振幅 a, b 的信息

例 辅助位联合测量 可纠 1 个比特翻转错误

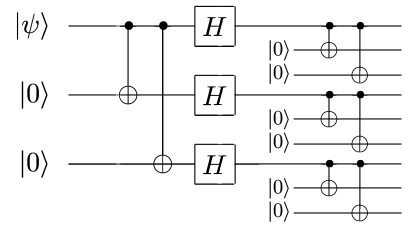


问题 ③ 差错是连续的, 无穷精度的, 回答:

Shor 码 (1995) 实现了 9 量子比特纠 1 量子比特任意错误

$|0\rangle \rightarrow |x_+\rangle^{\otimes 3} \rightarrow |\text{GHZ}_+\rangle^{\otimes 3}, |1\rangle \rightarrow |x_-\rangle^{\otimes 3} \rightarrow |\text{GHZ}_-\rangle^{\otimes 3}$

(第一步纠相位翻转, 第二步纠比特翻转)



quantum Hamming bound

量子哈明界 $2(1+3n) \leq 2^n \rightarrow n \geq 5$, 对抗单量子比特任意差错至少需 5 比特编码 (但 7 比特更常用)

消息 $\vec{\alpha} = \alpha_{1 \sim k}$, 记 $v(\alpha_{1 \sim k}) = \sum_i \alpha_i v_i$, **生成矩阵** $G = (v_{1 \sim k})^T$, 要求列线性无关 $\rightarrow v(\vec{\alpha}) = \vec{\alpha}G$

经典线性码 记用 n 比特来编码 k 个比特信息的为 $[n, k, t]$ 码, 最多能纠正 t 比特反转错误

x 为普通二进制序列的 k 行 1 列向量, G 为 n 行 k 列, 记 $G(x) = (Gx) \bmod 2$

parity check matrix

宇称校验矩阵 $Hv = 0$, 要求行线性无关 $\rightarrow HG^T = 0$, 记出错为 e , 有 $H(v+e) = He$

定理 H 的标准型为 $[A | I_{n-k}]$, 相应 G 的标准型为 $\begin{bmatrix} I_k \\ -A \end{bmatrix}$ (对于 \mathbb{Z}_2 域 $-A = A$)

效果: $\forall y \equiv (Gx) \bmod 2$, 使 $(Hy) \bmod 2 = 0$ (即无 error)

例 $[3, 1, 1]$ 码 $G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \rightarrow G(0) = (0, 0, 0), G(1) = (1, 1, 1), H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

Hamming

哈明码 是一类 $[2^r - 1, 2^r - r - 1]$ 经典线性码, 如 $[7, 4, 3]$ 码 $H_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, G_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

Calderbank-Shor-Steane

CSS 码 用两套哈明码分别纠正比特翻转和相位翻转错误, ($C_2 \subset C_1$, 商群 $|C_1/C_2| = 2^{k_1 - k_2}$)

CSS(C_1, C_2) 称为 $[[n, k_1 - k_2, t]]$ 量子纠错码, 如 Steane 码是 $[[7, 1, 3]]$, 纠正 1 量子比特的任何错误

$H_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} = G_1^T$

stabilizer code

稳定子码 用生成元组来描述更方便

7 比特 Steane 码有 6 个生成元 (各列为不同比特上的操作, 张量积)

(要求: 含偶数个 1, 且满足 $H \cdot v = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \bmod 2$)

[用生成元推: 从 $|0000000\rangle$ 开始, 测 g_4 , 则有可能得 $|0001111\rangle$]

$|0\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)$

(逻辑 $|1\rangle$ 态是对逻辑 $|0\rangle$ 态的每个比特取反)

threshold theorem

阈值定理 如果量子噪声可降到某阈值以下, 则量子纠错码可继续使它无限下降 (代价是仅增加一点计算复杂度)

g_1	I	I	I	X	X	X	X
g_2	I	X	X	I	I	X	X
g_3	X	I	X	I	X	I	X
g_4	I	I	I	Z	Z	Z	Z
g_5	I	Z	Z	I	I	Z	Z
g_6	Z	I	Z	I	Z	I	Z