量子信息与量子计算笔记

Leoeon

2016.01.11

Contents

1 量子信息 **5**

1.1 量子系综 5

1.1.1 5

1.1.2 5

1.1.3 Schmidt分解 6

1.1.4 6

1.1.5 性质 6

1.1.5.1 单比特双态系统 7

1.2 测量 7

1.2.1 投影测量 7

1.2.2 POVM测量 7

1.2.2.1 直和空间 7

1.2.2.2 直积空间 7

1.2.2.3 Neumark定理 8

1.3 8

1.3.1 von Neumann 熵 8

1.3.1.1 von Neumann熵 8

1.3.1.2 联合熵 8

1.3.1.3 条件熵 8

1.3.1.4 互信息 8

1.3.1.5 相对熵 9

1.3.2 9

1.3.2.1 制备熵 9

1.3.2.2 测量熵 9

1.3.2.3 Holevo界 9

1.3.3 两个量子态之间的距离 9

1.3.3.1 迹距离 9
1.3.3.2 保真度 9
1.3.4 纠缠度量 10
1.3.4.1 生成纠缠度 10
1.3.4.2 蒸馏纠缠度 10
1.3.4.3 Concurrence 10
1.3.4.4 PPT判据 10
1.4 量子通信 10
1.4.1 量子态克隆 10
1.4.1.1 量子态不可克隆定理1 10
1.4.1.2 量子态不可克隆定理2 11
1.4.1.3 概率克隆定理 11
1.4.2 Bell基 11
1.4.3 量子密钥分配（QKD） 12
1.4.3.1 EPR 12
1.4.3.2 BB84 12
1.4.3.3 B92 12
1.4.4 量子隐形传态 12

2 量子计算 13

2.1 量子比特门 13
2.1.1 单比特 13
2.1.1.1 X门 13
2.1.1.2 Z门 13
2.1.1.3 Hadamard门 13
2.1.1.4 相位门 13
2.1.1.5 $\frac{\pi}{8}$门 14
2.1.2 双比特 14
2.1.2.1 Cnot门 14
2.1.2.2 Swap门 14
2.1.2.3 复制量子比特 14
2.1.2.4 Cz门 14
2.1.3 三比特 14
2.1.3.1 Toffoli门 14
2.1.3.2 复制量子比特 14
2.1.3.3 经典与非门 15

2.1.3.4 Deutsch门 . . . 15
2.1.4 理论 . . . 15
2.2 量子算法 . . . 15
2.2.1 Deutsch算法 . . . 15
2.2.1.1 Deutsch . . . 15
2.2.1.2 Deutsch-Jozsa . . . 15
2.2.2 量子傅里叶变换 . . . 16
2.2.2.1 QFT . . . 16
2.2.2.2 相位估计 . . . 16
2.2.2.3 求阶 . . . 17
2.2.2.4 Shor算法 . . . 17
2.2.2.5 求周期 . . . 17
2.2.3 量子搜索 . . . 17
2.2.3.1 Grover算法 . . . 17
2.3 图态 . . . 18
2.3.0.2 图态 . . . 18
2.3.0.3 . . . 18
2.4 绝热模型 . . . 19
2.4.0.4 3-SAT问题 . . . 19
2.4.0.5 Exact Cover 问题 . . . 19
2.5 量子编码 . . . 19
2.5.1 Shor码 . . . 19
2.5.2 CSS码 . . . 19
2.5.2.1 目标 . . . 19
2.5.2.2 纠错 . . . 20

Chapter 1

量子信息

1.1 量子系综

1.1.1

混态$\{|\psi_k\rangle = \sum_i c_{ik}|\phi_i\rangle$，每个$|\psi_k\rangle$概率$q_k\}$。（$\langle\phi_i|\phi_j\rangle = \delta_{ij}$）

密度矩阵$\rho \overset{def}{=} \sum_k |\psi_k\rangle q_k \langle\psi_k| = \sum_{ij} |\phi_i\rangle p_{ij} \langle\phi_j|$，$p_{ij} = \sum_k c_{ik} q_k c^*_{jk}$

力学量平均值$< \hat{A} >= \sum_k q_k \langle\psi_k|\hat{A}|\psi_k\rangle = \sum_{ij} p_{ij} \langle\phi_j|\hat{A}|\phi_i\rangle = tr(\rho\hat{A})$

约化密度矩阵$\rho_A = tr_B(\rho_{AB})$

纯态时：可分离态可写为$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$，否则为纠缠态。可分离态可写为$\rho_{AB} = \sum_k p_k \rho_{Ak} \otimes \rho_{Bk}$，否则为纠缠态。

可分离态复合系统的子系统未必是可分离态。

1.1.2

量子Liouvill方程：

$$i\hbar\frac{d}{dt}\rho(t) = [H, \rho(t)]$$

若H不显含时间，则可积分得：

$$\begin{cases} U(t) = e^{\frac{1}{i\hbar}Ht} \\ \rho(t) = U(t)\rho(0)U^{-1}(t) \end{cases}$$

设环境初态为$|0\rangle_E$，总初态$\rho_{AE}(0)=\rho_A(0)\otimes|0\rangle_E{}_E\langle 0|$。经时间演化为

$$\begin{aligned}\rho_A(t) &= \$(\rho_A(0))\\ &= tr_E(\rho_{AE}(t))\\ &= tr_E(U_{AE}(t)\rho_A(0)\otimes|0\rangle_E{}_E\langle 0|U^+_{AE}(t))\\ &= \textstyle\sum_\mu {}_E\langle\mu|U_{AE}(t)\rho_A(0)\otimes|0\rangle_E{}_E\langle 0|U^+_{AE}(t)|\mu\rangle_E\\ &= \textstyle\sum_\mu M_\mu(t)\rho_A(0)M^+_\mu(t)\end{aligned}$$

其中，$M_\mu(t)\overset{def}{=}{}_E\langle\mu|U_{AE}(t)|0\rangle_E$

性质：

- $\sum_\mu M^+_\mu M_\mu=\mathbb{I}_A$
- 线性性：$\$(\rho_1+\rho_2)=\$(\rho_1)+\$(\rho_2)$
- 保厄米性：若$\rho^+=\rho$，则$\$(\rho)^+=\$(\rho)$
- 保迹性：若$tr(\rho)=1$，则$tr(\$(\rho))=1$
- 保正定性：$\$(\rho)\geq 0$

1.1.3 Schmidt分解

任一两体纯态

$$\begin{aligned}|\psi\rangle_{AB} &= \sum_{i\mu}\alpha_{i\mu}|i\rangle_A|\mu\rangle_B\\ &= \sum_i\sqrt{p_i}|i\rangle_A|i'\rangle_B\end{aligned}$$

$|i\rangle_A$取ρ_A的正交基，即$\rho_A=\sum_i|i\rangle_A p_{iA}\langle i|$，
则$|i'\rangle_B=\frac{1}{\sqrt{p_i}}\sum_\mu\alpha_{i\mu}|\mu\rangle_B$亦正交归一，$\rho_B=\sum_i|i'\rangle_B p_{iB}\langle i'|$

1.1.4

任意混态$\rho=\sum_k|\psi_k\rangle q_k\langle\psi_k|$ 都可以写成更高维空间的纯态$|\Psi\rangle=\sum_k\sqrt{q_k}|\psi_k\rangle|\alpha_k\rangle$

1.1.5 性质

$\rho=\rho^+$
$tr(\rho)=1$，$tr(\rho^2)\leq 1$（纯态取等号）
ρ本征值非负，故对$\forall|\phi\rangle,\langle\phi|\rho|\phi\rangle\geq 0$
N维Hilbert空间中全体ρ构成N^2-1维凸集，纯态为凸集端点（不能表示为其他元素线性组合）
$f(\rho)=\sum_{n=0}^\infty c_n\rho^n=\sum_{n=0}^\infty c_n(\sum_i p_i|i\rangle\langle i|)^n=\sum_{n=0}^\infty c_n\sum_i p_i^n|i\rangle\langle i|=\sum_i f(p_i)|i\rangle\langle i|$

1.1.5.1 单比特双态系统

$\rho \overset{可写为}{=} \frac{1}{2}(1+\vec{p}\vec{\sigma})$，$\vec{p}$画出Bloch球，$\vec{p}^2 \leq 1$(纯态取等号)。
$|\psi\rangle \overset{可写为}{=} \cos\frac{\theta}{2}e^{-i\frac{\phi}{2}}|\uparrow\rangle + \sin\frac{\theta}{2}e^{i\frac{\phi}{2}}|\downarrow\rangle$）
SU(2)幺正操作：$U(\theta,\vec{n}) = exp(-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma})$（绕$\vec{n}$轴旋转$\theta$角）

1.2 测量

一组测量算子$\{M_m\}$测量$|\psi\rangle$，
结果为m的可能性为$\langle\psi|M_m^+M_m|\psi\rangle$，
测量后系统状态为$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^+M_m|\psi\rangle}}$
测量算子满足完备性方程：$\sum_m M_m^+M_m = 1$

1.2.1 投影测量

M_m厄米且相互正交。
可写为谱分解$M = \sum_m mM_m$，
结果为m的可能性为$\langle\psi|M_m|\psi\rangle$，
测量后系统状态为$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m|\psi\rangle}}$
测量平均值$< M >= \sum_m m\langle\psi|M_m|\psi\rangle = \langle\psi|M|\psi\rangle$

1.2.2 POVM测量

1.2.2.1 直和空间

$H = H_A \oplus H_A^{\perp}$
H的正交归一基$\{|u_m\rangle\}$，在H_A空间投影$\{|\tilde{\psi}_m\rangle\}$未必正交归一，归一化为$\{|\psi_m\rangle = \frac{1}{\sqrt{\lambda_m}}|\tilde{\psi}_m\rangle\}$未必正交
H中的正交投影算符$\hat{E}_m = |u_m\rangle\langle u_m|$，在$H_A$中的投影$\hat{F}_m = |\tilde{\psi}_m\rangle\langle\tilde{\psi}_m| = \lambda_m|\psi_m\rangle\langle\psi_m|$
$Prob(m) = \langle u_m|\rho_A|u_m\rangle = \langle\tilde{\psi}_m|\rho_A|\tilde{\psi}_m\rangle = \lambda_m\langle\psi_m|\rho_A|\psi_m\rangle = tr(\hat{F}_m\rho_A)$
测量后$\rho_A \to \rho'_A = \sum_m \lambda_m\langle\psi_m|\rho_A|\psi_m\rangle|\psi_m\rangle\langle\psi_m| = \sum_m\sqrt{\hat{F}_m}\rho_A\sqrt{\hat{F}_m}$
性质：（$\hat{F}_m \geq 0$）（$\sum_m \hat{F}_m = \mathbb{I}$）（$\hat{F}_m^+ = \hat{F}_m$）（$dim(H_A) \leq N(\hat{F}_m) \leq N(\hat{E}_m) = dim(H_A \oplus H_A^+)$）

1.2.2.2 直积空间

$\rho_{AB} = \rho_A \otimes \rho_B$
H中的正交投影算符$\hat{E}_m$，在H_A中的投影$\hat{F}_m = tr_B[\hat{E}_m(\mathbb{I}_A \otimes \rho_B)]$
$Prob(m) = tr_{AB}(\hat{E}_m(\rho_A\otimes\rho_B)) = tr_A(\hat{F}_m\rho_A)$
测量后$\rho_{AB} \to \rho'_{AB} = \frac{\hat{E}_m(\rho_A\otimes\rho_B)\hat{E}_m}{tr_{AB}(\hat{E}_m(\rho_A\otimes\rho_B))}$，$\rho_A \to \rho'_A = \frac{tr_B(\hat{E}_m(\rho_A\otimes\rho_B)\hat{E}_m)}{tr_{AB}(\hat{E}_m(\rho_A\otimes\rho_B))} = \frac{\hat{F}_m\rho_A\hat{F}_m}{tr_B(\hat{F}_m\rho_A)} = \sqrt{\hat{F}_m}\rho_A\sqrt{\hat{F}_m}$

性质：（$\hat{F}_m \geq 0$）（$\sum_m \hat{F}_m = \mathbb{I}$）（$\hat{F}_m^+ = \hat{F}_m$）（$dim(H_A) \leq N(\hat{F}_m) \leq N(\hat{E}_m) = dim(H_A \otimes H_B)$）

1.2.2.3 Neumark定理

将H_A空间中的POVM测量提升为H空间的正交测量。
（待完善）

1.3

1.3.1 von Neumann 熵

1.3.1.1 von Neumann熵

$S(\rho) \stackrel{def}{=} -tr(\rho log\rho) = -\sum_a \lambda_a log\lambda_a = H(\lambda)$（$\lambda_a$为$\rho$矩阵特征值）
d维Hilbert空间中，$S(\rho) \leq logd$，当且仅当完全混合态$\rho = \frac{1}{d}$时取等号。
$S(U\rho U^+) = S(\rho)$，即幺正变换下S不变
用正交投影算子$\{M_i\}$进行测量，$S(\sum_i M_i\rho M_i) \geq S(\rho)$，当且仅当$\sum_i M_i\rho M_i = \rho$时取等号。
对纯态ρ_{AB}，$S(\rho_A) = S(\rho_B)$
$\sum_i p_i S(\rho_i) \leq S(\sum_i p_i\rho_i) \leq H(p) \leq H(p) + \sum_i p_i S(\rho_i)$

1.3.1.2 联合熵

$S(\rho_{AB}) \stackrel{def}{=} -tr(\rho_{AB} log\rho_{AB})$
$|S(\rho_A) - S(\rho_B)| \leq S(\rho_{AB})$
$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$，当且仅当$\rho_{AB} = \rho_A \otimes \rho_B$。（次可加性）
$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$（强次可加性）
$S(\rho_A) + S(\rho_B) \leq S(\rho_{AC}) + S(\rho_{BC})$（强次可加性）

1.3.1.3 条件熵

$S(\rho_A|\rho_B) \stackrel{def}{=} S(\rho_{AB}) - S(\rho_B)$
$S(\rho_A|\rho_{BC}) \leq S(\rho_A|\rho_B)$
$S(\rho_{AB}|\rho_{CD}) \leq S(\rho_A|\rho_c) + S(\rho_B|\rho_D)$

1.3.1.4 互信息

$S(\rho_A : \rho_B) \stackrel{def}{=} S(\rho_A) + S(\rho_B) - S(\rho_{AB})$
$S(\rho_A : \rho_B) \leq S(\rho_A : \rho_{BC})$

1.3.1.5 相对熵

$S(\rho||\sigma) \stackrel{def}{=} tr(\rho log\rho) - tr(\rho log\sigma)$

$S(\rho||\sigma) \geq 0$，当且仅当$\rho = \sigma$时取等号。（Klein不等式）

$S(\rho_A||\sigma_A) \leq S(\rho_{AB}||\sigma_{AB})$

1.3.2

1.3.2.1 制备熵

以$\{p_x\}$的概率制备$\{\rho_x\}$，$S(\sum_x p_x\rho_x) \leq H(X)$，当且仅当$\{\rho_x\}$彼此正交时取等号

意义：混合非正交态时，部分信息变为不能识别（经典信息丢失）。

1.3.2.2 测量熵

测量力学量$A = \sum_y a_y |y\rangle \langle y|$，$p_y = Prob(y) = \langle y|\rho|y\rangle$，则$S(\rho) \leq H(Y)$，当且仅当$[A, \rho] = 0$时取等号

1.3.2.3 Holevo界

以$\{p_x\}$的概率制备$\{\rho_x\}$，以POVM元$\{E_y\}$进行测量，则$H(X:Y) \leq S(\sum_x p_x\rho_x) - \sum_x p_x S(\rho_x) \leq H(X)$

1.3.3 两个量子态之间的距离

1.3.3.1 迹距离

$D(\rho, \rho') \stackrel{def}{=} \frac{1}{2}tr(|\rho - \rho'|)$ （其中，$|A| \stackrel{def}{=} \sqrt{A^+A}$）

当ρ和ρ'可对易时，取其共同本征态$\{|i\rangle\}$，则$D(\rho, \rho') = \frac{1}{2}tr(|\sum_i \lambda_i |i\rangle \langle i| - \sum_i \lambda'_i |i\rangle \langle i||) = D(\lambda, \lambda')$（本征值经典信息的迹距离）

迹距离在酉变化下不变$D(U\rho U^+, U\rho' U^+) = D(\rho, \rho')$

1.3.3.2 保真度

$F(\rho, \rho') = tr(\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}})$

当ρ和ρ'可对易时，取其共同本征态$\{|i\rangle\}$，则$F(\rho, \rho') = tr(\sqrt{\sum_i \lambda_i \lambda'_i |i\rangle \langle i|}) = F(\lambda, \lambda')$（本征值经典信息的保真度）

保真度在酉变化下不变$F(U\rho U^+, U\rho' U^+) = F(\rho, \rho')$

对纯态$|\psi\rangle$，$F(|\psi\rangle \langle\psi|, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle}$

1.3.4 纠缠度量

1.3.4.1 生成纠缠度

对两体系统：通过LOCC过程，为制备ρ_{AB}所消耗的Bell基的平均最小数目E_F

1.3.4.2 蒸馏纠缠度

对两体系统：通过LOCC过程能从ρ_{AB}中提取的Bell基的平均最大数目E_D

1.3.4.3 Concurrence

对两体系统：
$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho(\sigma_y \otimes \sigma_y)$
$R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$，其本征值$\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$
$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}$。（$C(\rho) = 0$对应可分离态，$C(\rho) = 1$对应最大纠缠态）
$E_F(\rho) = h(\frac{1-\sqrt{1-C(\rho)^2}}{2})$，其中$h(x) = -xlogx - (1-x)log(1-x)$

1.3.4.4 PPT判据

对两体系统：
$E_D(\rho) = 0 \Leftarrow$ 对密度矩阵做任一单体的部分转置后仍是半正定矩阵（本征值非负）$\overset{\text{一单体双态，另一单体双态或三态}}{\rightleftharpoons}$ 可分离

1.4 量子通信

1.4.1 量子态克隆

1.4.1.1 量子态不可克隆定理1

对已知一组非正交态中任意一态，以决定论方式（即不含测量，即幺正演化），精确克隆是不可能的。
证明：
若

$$|\psi\rangle |S\rangle \xrightarrow{U} U |\psi\rangle |S\rangle = |\psi\rangle |\psi\rangle$$

则

$$\begin{array}{ccc} \langle\psi_1|\psi_2\rangle & = & \langle S| \langle\psi_1|\psi_2\rangle |S\rangle \\ & & \| \\ \langle\psi_1|\psi_2\rangle^2 & = & \langle S| \langle\psi_1|U^+U|\psi_2\rangle |S\rangle \end{array}$$

1.4.1.2 量子态不可克隆定理2

对任意未知态，不限定方式，精确克隆是不可能的。

证明：

若

$$|\psi_i\rangle |S\rangle |R_0\rangle \to |\psi_i\rangle |\psi_i\rangle |R_i\rangle$$

则

$$\begin{aligned} & (c_1 |\psi_1\rangle + c_2 |\psi_2\rangle) |S\rangle |R_0\rangle \\ \to \quad & (c_1 |\psi_1\rangle |\psi_1\rangle |R_1\rangle + c_2 |\psi_2\rangle |\psi_2\rangle |R_2\rangle) \\ \neq \quad & (c_1 |\psi_1\rangle + c_2 |\psi_2\rangle)(c_1 |\psi_1\rangle + c_2 |\psi_2\rangle) |R'\rangle \end{aligned}$$

1.4.1.3 概率克隆定理

对已知一组线性无关态中任意一态，用幺正操作U和测量M，可概率克隆

操作：

对

$$\begin{aligned} |\psi_i\rangle |S\rangle |R_0\rangle & \xrightarrow{U} U |\psi_i\rangle |S\rangle |R_0\rangle \\ & = \sqrt{\gamma_i} |\psi_i\rangle |\psi_i\rangle^m |R_0\rangle + \textstyle\sum_{j=1}^N |\Psi_j\rangle |R_j\rangle \end{aligned}$$

对R进行测量，克隆成功概率为γ_i。将$|\psi_i\rangle$克隆m份。

要求：

令$[X^{(i)}] = [\langle\psi_\mu|\psi_\nu\rangle^i]$，$[\sqrt{\Gamma}] = diag(\sqrt{\gamma_1}, \cdots, \sqrt{\gamma_n})$，则要求$X^{(1)} - \sqrt{\Gamma} X^{(m+1)} \sqrt{\Gamma}$半正定。

特殊地，实现概率的态识别 $\iff$ 无穷克隆即取$m = \infty \iff X^{(1)} - \Gamma$半正定

1.4.2 Bell基

本征值

	$\sigma_{1x}\sigma_{2x}$	$\sigma_{1y}\sigma_{2y}$	$\sigma_{1z}\sigma_{2z}$
$\|\phi^+\rangle$	$+$	$-$	$+$
$\|\phi^-\rangle$	$-$	$+$	$+$
$\|\psi^+\rangle$	$+$	$+$	$-$
$\|\psi^-\rangle$	$-$	$-$	$-$

态（$*\frac{1}{\sqrt{2}}$）

	x	y	z
$\|\phi^+\rangle$	$\|\uparrow_x\uparrow_x\rangle + \|\downarrow_x\downarrow_x\rangle$	$\|\uparrow_y\downarrow_y\rangle + \|\downarrow_y\uparrow_y\rangle$	$\|\uparrow_z\uparrow_z\rangle + \|\downarrow_z\downarrow_z\rangle$
$\|\phi^-\rangle$	$\|\downarrow_x\uparrow_x\rangle + \|\uparrow_x\downarrow_x\rangle$	$\|\uparrow_y\uparrow_y\rangle + \|\downarrow_y\downarrow_y\rangle$	$\|\uparrow_z\uparrow_z\rangle - \|\downarrow_z\downarrow_z\rangle$
$\|\psi^+\rangle$	$\|\uparrow_x\uparrow_x\rangle - \|\downarrow_x\downarrow_x\rangle$	$\|\uparrow_y\uparrow_y\rangle - \|\downarrow_y\downarrow_y\rangle$	$\|\uparrow_z\downarrow_z\rangle + \|\downarrow_z\uparrow_z\rangle$
$\|\psi^-\rangle$	$\|\downarrow_x\uparrow_x\rangle - \|\uparrow_x\downarrow_x\rangle$	$\|\uparrow_y\downarrow_y\rangle - \|\downarrow_y\uparrow_y\rangle$	$\|\uparrow_z\downarrow_z\rangle - \|\downarrow_z\uparrow_z\rangle$

1.4.3 量子密钥分配（QKD）

1.4.3.1 EPR

1.二人拥有EPR对$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\uparrow\downarrow\rangle)$的量子比特串
2.二人分别随机用X、Z测量每个量子比特
3.二人分别公布各自测量的X、Z序列
4.二人只保留相同X、Z的量子比特，由这些量子比特的$|\uparrow\rangle$、$|\downarrow\rangle$作为01随机密钥

1.4.3.2 BB84

1.Alice随机制备$|\uparrow_x\rangle$、$|\downarrow_x\rangle$、$|\uparrow_z\rangle$、$|\downarrow_z\rangle$的量子比特串，发送给Bob
2.Bob随机用X或Z测量每个量子比特
3.Alice、Bob分别公布各自制备、测量的X、Z序列
4.二人只保留相同X、Z的量子比特，由这些量子比特的$|\uparrow\rangle$、$|\downarrow\rangle$作为01随机密钥

1.4.3.3 B92

1.Alice随机制备$|\uparrow_x\rangle$、$|\uparrow_z\rangle$的量子比特串，发送给Bob
2.Bob随机用X或Z测量每个量子比特
3.Bob公布测得的$|\uparrow\rangle$、$|\downarrow\rangle$序列
4.二人只保留$|\downarrow\rangle$的量子比特，由这些比特的X、Z作为01随机密钥

1.4.4 量子隐形传态

Alice有粒子12，Bob有粒子3。Alice要将粒子1的信息传至粒子3上。粒子23为预先分配好的Bell态。Alice用Bell基测量粒子12，公布测得结果，Bob根据结果对粒子3进行对应操作$\hat{U}_3^{-1}$，还原原粒子1信息

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}_1 |Bell_i\rangle_{23} = \frac{1}{2}(\sum_{j=1}^{4} |Bell_j\rangle_{12}\,\hat{U}_{ij3})\begin{pmatrix}\alpha\\ \beta\end{pmatrix}_3$$

$\hat{U}_3$	$\|\phi^+\rangle_{12}$	$\|\phi^-\rangle_{12}$	$\|\psi^+\rangle_{12}$	$\|\psi^-\rangle_{12}$
$\|\phi^+\rangle_{23}$	1	σ_z	σ_x	σ_y
$\|\phi^-\rangle_{23}$	σ_z	1	σ_y	σ_x
$\|\psi^+\rangle_{23}$	σ_x	σ_y	1	σ_z
$\|\psi^-\rangle_{23}$	σ_y	σ_x	σ_z	1

Chapter 2

量子计算

2.1 量子比特门

2.1.1 单比特

任意单比特门（2*2酉矩阵）$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) = e^{i\alpha} \begin{bmatrix} e^{-\frac{i\beta}{2}} & 0 \\ 0 & e^{\frac{i\beta}{2}} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & \sin\frac{\gamma}{2} \\ -\sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-\frac{i\delta}{2}} & 0 \\ 0 & e^{\frac{i\delta}{2}} \end{bmatrix}$

2.1.1.1 X门

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

2.1.1.2 Z门

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

2.1.1.3 Hadamard门

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

$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$（即用n个Hadamard门作用在$|0 \cdots 0\rangle$上可并行实现$2^n$种全状态叠加）

2.1.1.4 相位门

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

2.1.1.5 $\frac{\pi}{8}$门

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} = \begin{bmatrix} e^{-\frac{i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{bmatrix}$$

2.1.2 双比特

2.1.2.1 Cnot门

$$Cnot_{1\to2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$Cnot_{1\to2} \left|A\right\rangle \left|B\right\rangle = \left|A\right\rangle \left|A \oplus B\right\rangle$$

$H_1 H_2 Cnot_{1\to2} H_1 H_2 = Cnot_{2\to1}$ （即若以$\left|+\right\rangle \left|-\right\rangle$为基，则“控制”与“目标”比特颠倒）

2.1.2.2 Swap门

$$Swap = Cnot_{1\to2} Cnot_{2\to1} Cnot_{1\to2}$$

$$Swap \left|A\right\rangle \left|B\right\rangle = \left|B\right\rangle \left|A\right\rangle$$

2.1.2.3 复制量子比特

$$Cnot_{1\to2}(\alpha \left|0\right\rangle + \beta \left|1\right\rangle) \left|0\right\rangle = \alpha \left|0\right\rangle \left|0\right\rangle + \beta \left|1\right\rangle \left|1\right\rangle$$

2.1.2.4 Cz门

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

2.1.3 三比特

2.1.3.1 Toffoli门

$$Toffoli_{12\to3} \left|a\right\rangle \left|b\right\rangle \left|c\right\rangle = \left|a\right\rangle \left|b\right\rangle \left|c \oplus ab\right\rangle$$

2.1.3.2 复制量子比特

$$Toffoli_{12\to3} \left|1\right\rangle (\alpha \left|0\right\rangle + \beta \left|1\right\rangle) \left|0\right\rangle = \left|1\right\rangle (\alpha \left|0\right\rangle \left|0\right\rangle + \beta \left|1\right\rangle \left|1\right\rangle)$$

2.1.3.3 经典与非门

$Toffoli_{12\to 3}\left|a\right\rangle\left|b\right\rangle\left|1\right\rangle = \left|a\right\rangle\left|b\right\rangle\left|\overline{ab}\right\rangle$
（其中$\left|a\right\rangle$与$\left|b\right\rangle$仅为经典$\left|0\right\rangle$或$\left|1\right\rangle$）

2.1.3.4 Deutsch门

$R_{12\to 3}(\theta)\left|a\right\rangle\left|b\right\rangle\left|c\right\rangle = \left|a\right\rangle\left|b\right\rangle R(\theta)\left|c\right\rangle$
当$\left|a\right\rangle\left|b\right\rangle \neq \left|1\right\rangle\left|1\right\rangle$时，$R(\theta) = \mathbb{I}$
当$\left|a\right\rangle\left|b\right\rangle = \left|1\right\rangle\left|1\right\rangle$时，$R(\theta) = -iR_x(\theta) = (-i)e^{i\frac{\theta}{2}\sigma_x}$

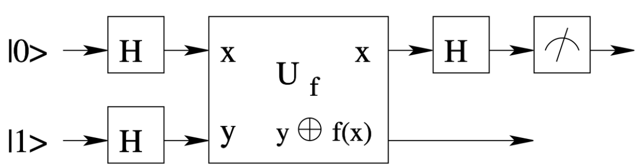
2.1.4 理论

任意多量子比特门都可用Cnot门和单量子比特门组合实现
任意酉算子可用Hadamard、相位、Cnot、$\frac{\pi}{8}$门组合实现
任意经典线路、可逆线路可用Toffoli门组合实现

2.2 量子算法

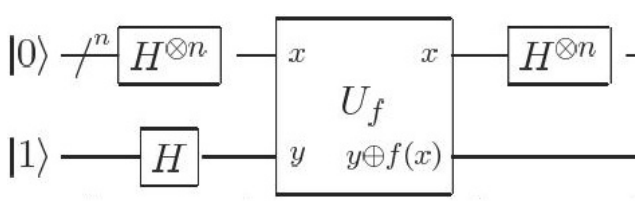
2.2.1 Deutsch算法

2.2.1.1 Deutsch



输入$\left|0\right\rangle\left|1\right\rangle$，输出$\left|f(0)\oplus f(1)\right\rangle\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}$
测量第一个比特，即可知U_f的$f(0)\oplus f(1)$

2.2.1.2 Deutsch-Jozsa



已知U_f的$f(x)$只有两种可能，一种对$\forall x$为常数，一种对$\forall x$得到0、1的数目相同

输入$\left|0\right\rangle^n\left|1\right\rangle$，输出$\sum_z\sum_x\frac{(-1)^{f(x)+x\cdot z}\left|z\right\rangle}{2^n}\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}} = \begin{cases}\left|0\right\rangle^n\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}} & \text{，f(x)为常数}\\ \sum_{z\neq\left|0\right\rangle^n}\sum_x\frac{(-1)^{f(x)+x\cdot z}\left|z\right\rangle}{2^n}\frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}} & \text{，f(x)为平衡}\end{cases}$

测量前n个比特，若全部为0则f(x)为常数，若存在1则f(x)为平衡

2.2.2 量子傅里叶变换

2.2.2.1 QFT

$$
\begin{aligned}
|x\rangle &= \sum_{y=0}^{2^n-1} \langle y|x\rangle\, |y\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{2^n}}\, |y\rangle
\end{aligned}
$$

记

$$
\begin{cases}
x = (x_{n-1}x_{n-2}\cdots x_0) = \sum_{i=0}^{n-1} 2^i x_i \\
y = (y_{n-1}y_{n-2}\cdots y_0) = \sum_{j=0}^{n-1} 2^j y_j
\end{cases}
$$

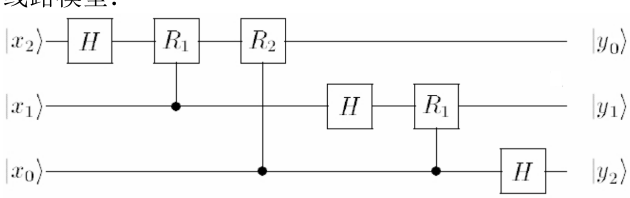
则

$$
\begin{aligned}
\frac{xy}{2^n} \mod 1 &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2^{i+j-n} x_i y_j \mod 1 \\
&= \sum_{j=0}^{n-1} y_j \sum_{i=0}^{n-j} 2^{i+j-n} x_i \\
&= y_{n-1} * (0.x_0) + y_{n-2} * (0.x_1 x_0) + \cdots y_0 * (0.x_{n-1}\cdots x_0)
\end{aligned}
$$

则

$$
\begin{aligned}
|x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_0\rangle &= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{xy}{2^n}} |y_{n-1}\rangle \otimes |y_{n-2}\rangle \otimes \cdots \otimes |y_0\rangle \\
&= \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 \\ e^{2\pi i * (0.x_0)} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ e^{2\pi i * (0.x_1 x_0)} \end{bmatrix} \otimes \cdots \begin{bmatrix} 1 \\ e^{2\pi i * (0.x_{n-1}\cdots x_0)} \end{bmatrix}
\end{aligned}
$$

线路模型：



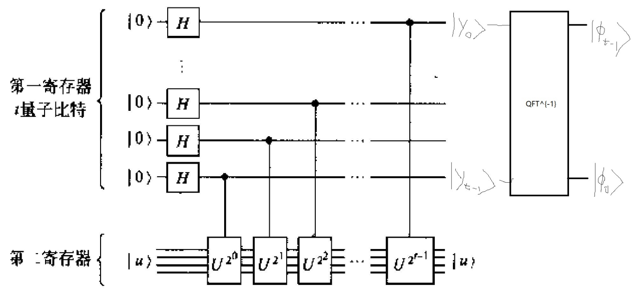
其中，$R_k \overset{def}{=} \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$

2.2.2.2 相位估计

算符U，特征值为$e^{2\pi i\phi}$，特征向量为u。

为以至少$1-\varepsilon$ 的概率精确到小数点后n比特估计ϕ，取$t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$

记ϕ舍入到小数点t位为$(0.\phi_{t-1}\cdots\phi_0)$



第一寄存器的第i个比特，在经过Hadamard门后，受控对第二寄存器的$|u\rangle$进行2^{t-1-i}次U测量，从而使自身变为$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 2^{t-1-i}\phi}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i*(0.\phi_i\cdots\phi_1)}|1\rangle)$

则第一寄存器所有输出为$\frac{1}{\sqrt{2^t}}\begin{bmatrix}1\\ e^{2\pi i*(0.\phi_0)}\end{bmatrix} \otimes \begin{bmatrix}1\\ e^{2\pi i*(0.\phi_1\phi_0)}\end{bmatrix} \otimes \cdots \begin{bmatrix}1\\ e^{2\pi i*(0.\phi_{t-1}\cdots\phi_0)}\end{bmatrix}$

对其进行逆傅里叶变换，即可还原ϕ

2.2.2.3 求阶

对互质的x与N，欲求最小正整数r使得$x^r \mod N = 1$

酉算子$U_{x,N}|y\rangle = |(xy) \mod N\rangle$，特征值为$e^{2\pi i\frac{s}{r}}$，特征向量为$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi i\frac{sk}{r}}|x^k \mod N\rangle$。由相位估计得$\frac{s}{r}$

实际操作中取$|u\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$，经过$U_{x,N}$得$\frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{2\pi i\frac{sj}{r}}|j\rangle|u_s\rangle$，（逆傅里叶变换得$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\widetilde{\frac{s}{r}}\rangle|u_s\rangle$，）测量塌缩到某个$|u_s\rangle$，得$\frac{1}{\sqrt{r2^t}}\sum_{j=0}^{2^t-1} e^{2\pi i\frac{sj}{r}}|j\rangle|u_s\rangle$，求相位$\frac{s}{r}$。

2.2.2.4 Shor算法

求合数N的不平凡因子

从1到N-1中任选x，求阶$x^r \mod N = 1$。若r是偶数，且$x^{\frac{r}{2}} \mod N \neq -1$，则$\gcd(x^{\frac{r}{2}}-1, N)$ 和$\gcd(x^{\frac{r}{2}}+1, N)$ 中至少一个为N的不平凡因子。否则算法失败。

2.2.2.5 求周期

运算$U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$，求f(x)周期。

对$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|0\rangle$ 应用U，得$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|f(j)\rangle = \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{2\pi i\frac{sj}{r}}|j\rangle|\tilde{f}(s)\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\widetilde{\frac{s}{r}}\rangle|\tilde{f}(s)\rangle$。测量，塌缩得某个$\frac{s}{r}$

2.2.3 量子搜索

2.2.3.1 Grover算法

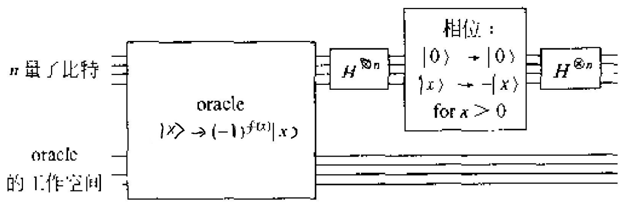
寻找某算法的解。

酉算子O能翻转解$O\left|\beta\right\rangle = -\left|\beta\right\rangle$（其中$\left|\beta\right\rangle = \frac{1}{\sqrt{M}}\sum_{x为解}\left|x\right\rangle$），保持非解$O\left|\alpha\right\rangle = \left|\alpha\right\rangle$（其中$\left|\alpha\right\rangle = \frac{1}{\sqrt{N-M}}\sum_{x非解}\left|x\right\rangle$）。

酉算子$P_{\left|\psi\right\rangle} = 2\left|\psi\right\rangle\left\langle\psi\right| - \mathbb{I} = H^{\otimes n}(-(-1)^{\delta_{0,x}})H^{\otimes n}$。

取算子$G = P_{\left|\psi\right\rangle}O$ 。

重复G算子$\sqrt{\frac{N}{M}}$遍，测量，可以大于$\frac{1}{2}$ 的概率塌缩到正确解。



2.3 图态

无向图，每个顶点为比特

2.3.0.2 图态

等价形式：

1.将所有顶点取为$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$。所有相连边进行Cz门操作$diag\{1,1,1,-1\}$。

2.每个比特a的stabilizer：$K_a \overset{def}{=} \sigma_a^x \prod_{b\in N_a} \sigma_b^z$（$N_a$意为a的邻居）。$H = -\sum_a K_a$的基态

2.3.0.3

Pauli群：$\{\pm i, \sigma_x, \sigma_y, \sigma_z\}$ 生成的群

Clifford群：Pauli群到Pauli群的算子组成的群

图的局域补操作：$|G\rangle \to |\tau_a(G)\rangle$：对比特a，任意两邻居$b_i, b_j \in N_a$ 之间的是否连线取反

$$\begin{cases} P^a_{z,\pm}|G\rangle = \dfrac{1}{\sqrt{2}}|z,\ \pm\rangle^a \otimes U^a_{z,\pm}|G-a\rangle \\ P^a_{y,\pm}|G\rangle = \dfrac{1}{\sqrt{2}}|y,\ \pm\rangle^a \otimes U^a_{y,\pm}|\tau_a(G)-a\rangle \\ P^a_{x,\pm}|G\rangle = \dfrac{1}{\sqrt{2}}|x,\ \pm\rangle^a \otimes U^a_{x,\pm}|\tau_{b_0}(\tau_a\tau_{b_0}(G)-a)\rangle \end{cases}$$

$$\begin{cases} U^a_{z,+} = 1 & U^a_{z,-} = \sigma_z^{N_a} \\ U^a_{y,+} = \sqrt{-i\sigma_z}^{N_a} & U^a_{y,-} = \sqrt{+i\sigma_z}^{N_a} \\ U^a_{x,+} = \sqrt{+i\sigma_y}^{b_0}\sigma_z^{N_a-(N_{b_0}b_0)} & U^a_{x,-} = \sqrt{-i\sigma_y}^{b_0}\sigma_z^{N_{b_0}-(N_a a)} \quad (b_0 \in N_a) \end{cases}$$

2.4 绝热模型

$H(t) = (1-\frac{t}{T})H_{初} + \frac{t}{T}H_{末}$

$H(t)\,|n;t\rangle = E_n(t)\,|n;t\rangle$

当基态与第一激发态的gap足够大，演化时间足够长时，系统可保持在基态上，由初态缓慢演化至末态

$g_{min} = \min_{0\le t\le T}(E_1(t) - E_0(t))$

$\varepsilon = \max_{0\le t\le T} |\,\langle n=1;t|\frac{dH}{dt}|n=0;t\rangle\,|$

$T \ge \frac{\varepsilon}{g_{min}^2}$

2.4.0.4 3-SAT问题

$$h_{初C}(z_{iC}, z_{jC}, z_{kC}) = \frac{1-\sigma_x^i}{2} + \frac{1-\sigma_x^j}{2} + \frac{1-\sigma_x^k}{2} \qquad H_{初} = \sum_C h_{初C}$$

$$h_{末C}(z_{iC}, z_{jC}, z_{kC}) = \begin{cases} 0 & , z_{iC}, z_{jC}, z_{kC}\text{符合第C条语句要求} \\ 1 & , z_{iC}, z_{jC}, z_{kC}\text{不符合第C条语句要求} \end{cases} \qquad H_{末} = \sum_C h_{末C}$$

2.4.0.5 Exact Cover 问题

初态为$|x_1\rangle \cdots |x_n\rangle$

$H_{末} = \sum_C h_{末C}$，$h_{末C}$为违反时的惩罚函数

2.5 量子编码

2.5.1 Shor码

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}^3}((|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}^3}((|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)) \end{aligned}$$

2.5.2 CSS码

2.5.2.1 目标

经典线性码$C_{1\{N*m_1\}}$、$C_{2\{N*m_2\}}$，$C_2 \subset C_1$，且C_1、$C_2^{\perp}$皆可纠t个差错。

则可定义$CSS(C_1, C_2)$为陪集$C_1/C_{2\{N*(m_1-m_2)\}}$，元素为$|x + C_1\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y\in C_2} |x+y\rangle\,(x \in C_1)$

2.5.2.2 纠错

$\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}|x+y\rangle$ 被污染为

$$\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{(x+y)e_2}|x+y+e_1\rangle$$

取辅助码$|0\rangle$，用C_1的校验矩阵H_1作用，得

$$\begin{aligned}&\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{(x+y)e_2}|x+y+e_1\rangle|H_1(x+y+e_1)\rangle\\=&\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{(x+y)e_2}|x+y+e_1\rangle|H_1e_1\rangle\end{aligned}$$

由$|H_1e_1\rangle$，非门翻转e_1对应比特，得

$$\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{(x+y)e_2}|x+y\rangle$$

用$H^{\otimes N}$作用，得

$$\begin{aligned}&\frac{1}{\sqrt{|C_2|2^N}}\sum_{z\in\{0,1\}^N}\sum_{y\in C_2}(-1)^{(x+y)(e_2+z)}|z\rangle\\=&\frac{1}{\sqrt{|C_2|2^N}}\sum_{z'\in\{0,1\}^N}\sum_{y\in C_2}(-1)^{(x+y)z'}|z'+e_2\rangle\\=&\sqrt{\frac{|C_2|}{2^N}}\sum_{z'\in C_2^\perp}(-1)^{xz'}|z'+e_2\rangle\end{aligned}$$

用$C_2^\perp$的校验矩阵$H_2^\perp$作用，得

$$\begin{aligned}&\sqrt{\frac{|C_2|}{2^N}}\sum_{z'\in C_2^\perp}(-1)^{xz'}|z'+e_2\rangle|H_2^\perp(z'+e_2)\rangle\\=&\sqrt{\frac{|C_2|}{2^N}}\sum_{z'\in C_2^\perp}(-1)^{xz'}|z'+e_2\rangle|H_2^\perp e_2\rangle\end{aligned}$$

由$|H_2^\perp e_2\rangle$，非门翻转e_2对应比特，得

$$\begin{aligned}&\sqrt{\frac{|C_2|}{2^N}}\sum_{z'\in C_2^\perp}(-1)^{xz'}|z'\rangle\\=&\frac{1}{\sqrt{|C_2|2^N}}\sum_{z'\in\{0,1\}^N}\sum_{y\in C_2}(-1)^{(x+y)z'}|z'\rangle\end{aligned}$$

用$H^{\otimes N}$作用，得

$$\frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{(x+y)}\left|x+y\right\rangle$$