第一章 量子信息论的基础

§1.1. 经典信息论简介

①. 信息的概念和度量

△什么是信息：信息就是获得消息和消除掉的不确定性（不仅与消息有关，且与接收者有关）

信息量：就是消除掉的不确定性的度量。

x_i事件 → $P(x_i)$为事件发生的概率　　下雨. 地震　$P_i > P_j$　　$P=1$　$I=0$

自信息量（事件x_i的信息量）$I(x_i) = -\log P(x_i)$.

·如不特别声明，常取2为底数，给出的信息量单位为比特.

事件集：$X=\{x_1, x_2, \cdots x_m\}$　　$P=\{p_1, p_2, \cdots p_m\}$

（香农熵）信息熵：事件集中各自信息量的统计平均为事件集的信息熵。它反映整体的统计平均不确定性. $H(X)=\sum_{i=1}^{n} p_i I(x_i) = -\sum_{i=1}^{m} p_i \log_2 p_i$

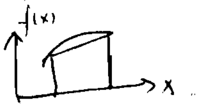
$H(X)$是X中的一个事件平均给出的信息量

香农熵的性质　①. 正定性　$H(X)>0$

② 可加性　$\{X\}$, $\{Y\}$为独立事件集　$\{XY\}$ 则 $H(XY)=H(X)+H(Y)$

② 强可加性　$H(A,B)=H(A)+H(B/A)$

③ 上凸性　$aH(X_1)+(1-a)H(X_2) \leq H(aX_1+(1-a)X_2)$



② 信源和信道

信源是一个物理系统，其状态随空间坐标或时间变化.

物理属性 $\left\{\begin{array}{l}\text{空间信源}\\ \text{时间信源}\end{array}\right.$　　概率属性 $\left\{\begin{array}{l}\text{无记忆信源}\\ \text{Markov信源（受有限时间内的影响）}\end{array}\right.$

信号的数学属性 $\left\{\begin{array}{l}\text{离散}\\ \text{连续}\end{array}\right.$

以下以离散无记忆信源为基础来介绍信息学的基本概念.

$X=\{x_1, x_2, \cdots x_m\}$　　$P=\{p_1, p_2, \cdots p_m\}$　　$\sum_{i=1}^{n} p_i = 1$

信道：（离散信道）

信源 $\xrightarrow{\text{输入}}$ ( ) $\longrightarrow$ 输出 信宿

信源 $X=\{x_1, x_2, \cdots x_m\}$　输出事件集 $Y=\{y_1, y_2, \dots, y_n\}$

环境噪声的存在使得信道中存在随机干扰，输入输出的关系不确定，用条件概率来描述该事实：

信道传递概率矩阵：$p(Y|X)=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & & & \\ p_{n1} & p_{n2} & \cdots & p_{nm} \end{bmatrix}$　　$p(x_i Y_j)=p(x_i)p(Y_j|x_i)$

△ 互信息量：事件集 $\{A_i B_j\}$ 的概率为 p_{ij}，A_i、B_j 的互信息量定义为：接收到消息 B_j 后消除掉的关于 A_i 的不确定性：

$$I(A_i, B_j) = \underset{\substack{\uparrow \\ \text{自信息}}}{I(A_i)} - \underset{\substack{\uparrow \\ \text{条件自信息量}}}{I(A_i/B_j)} = -\log_2 p(A_i) + \log_2 p(A_i/B_j)$$

← 举概率特性的说明

$$-\log_2 p(A_i)+\log_2 p(A_i/B_j) = \log_2\frac{p(A_i/B_j)}{p(A_i)} = \log_2\frac{p(A_i B_j)}{p(A_i)p(B_j)}$$

$\therefore\ I(A_i, B_j) = I(B_j, A_i)$

△ 事件集 $\{A_i B_j\}$ 的总熵

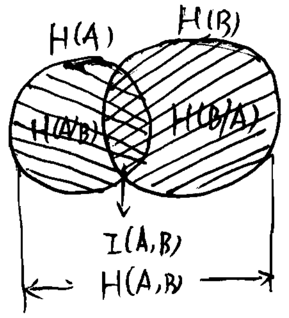
$$\begin{aligned} H(A,B) &= -\sum_{ij} p_{ij}\log_2 p_{ij} \\ &= -\sum_{ij} p_i\, p(B_j/A_i)\log_2 p_i\, p(B_j/A_i) \\ &= -\sum_{ij} p_i\, p(B_j/A_i)\log_2 p_i - \sum_{ij} p_i\, p(B_j/A_i)\log_2 p(B_j/A_i) \\ &= -\sum_i p_i\log_2 p_i - \sum_{ij} p_{ij}\log_2 p(B_j/A_i) \\ &= H(A) + \underset{\substack{\uparrow \\ \text{条件熵}}}{H(B/A)} \end{aligned}$$

条件熵，也称为信道疑义度。　（强可加性）

△ 事件集的互信息量：$I(A,B)$

$$\begin{aligned} I(A,B) &= \sum_{ij} p_{ij}\, I(A_i B_j) \\ &= \sum_{ij} p_{ij}\left(-\log_2 p_i + \log_2 p(A_i/B_j)\right) \\ &= H(A) - H(A/B) \\ &= H(B) - H(B/A) \\ &= H(A)+H(B)-H(A,B) \end{aligned}$$

互信息量 $I(A,B)$ 表示事件集的关联程度.



← 阐明信道疑义度

R（信道的信息传输率）$= I(A,B) = H(A) - H(A/B)$

△ 对于固定的信道（$P(B|A)$ 一定），总存在一种信源，使信道的信息传输率最大，这个最大值定义为信道容量. $C = \max_{\{P_i\}} I(A,B)$ （比特/符号）

C：刻画了信道传输信息的能力.

$C_t = C \times$ 单位时间传送的符号 $=$ bit/单位时间

△ 信源与信道的匹配问题

$R = C$ 匹配　　$R < C$ 不匹配

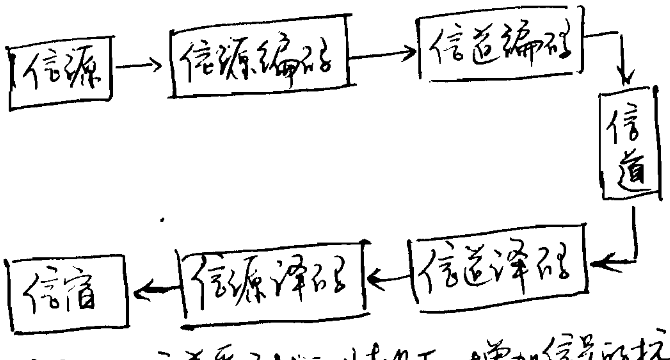
信道剩余度 $= C - R$.

△ 信源编码

为什么？ 用信道能传输的符号来代表信源发出的信息，使信源适合于信道的传输。

进一步考虑：在不失真或允许一定失真的条件下，用尽可能少的信号来传送信源信息，提高信息传输率.

对于一个实际的通讯过程.



（顺带说明信道编码的作用：主要是在信道受干扰的情况下，增加信号的抗干扰能力，同时又保持尽可能大的信息传输率）

信息论的成功之处：信源编码和信道编码看似是相互矛盾的，但它证明了，至少存在某种最佳的编码能解决上述矛盾，做到既有效又可靠地传送信息。

信源输出的符号集 $S=\{s_1, s_2, \cdots, s_q\}$

编码符号集 $X=\{x_1, x_2, \cdots, x_m\}$ x_i 称为码元

码字（由码元组成的码元符号序列）

$W_i=(x_{i1}\, x_{i2} \cdots x_{il})$ $x_{ik}\in X$

i_l：码字长 所有的码字集合为 $C=\{w_1, w_2, \cdots w_q\}$

编码：使信源符号或信源符号序列与 C 中的码字建立起一一对应的关系

定义码字的平均长度 $l=\sum_{i=1}^{q} p(s_i) i_l$ （定长码、变长码）

由于信源一旦给定 $H(S)$ 就确定了，$H(S)$ 为平均每个信源符号携带的比特。编码后，每个信源符号平均用 l 个码元表示，l 越小，每个码元荷载的信息量也越大，以码元作为新信源的熵也就越大

新信源（经信源编码后的）信息传输率 $R=\dfrac{H(S)}{l}\ \dfrac{(\text{比特/信源符号})}{(\text{码元符号/信源符号})}=H(X)\ \dfrac{\text{比特}}{\text{码元符号}}$

信源编码：就是根据输出符号序列的统计特性，寻找一定的方法，把信源输出的序列变换为最短的码字序列，使每个码元的平均信息量最大。

例子：

$$\begin{array}{ccccc} S: & s_1 & s_2 & s_3 & s_4 \\ P: & \frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \frac{1}{8} \end{array}$$

一种编码 00 01 10 11 $l=2$

另一种编码 0 10 110 111 $l=\frac{7}{4}$

③ 香农定理

1948年 Shannon 第一定理（无失真的信源编码定理）

$\{A_i\}_n$ $\{p(A_i)\}_n$ 能否用 m 个元素来表示呢？ $m<n$

要保证信息无失真 $\{A_i\}\rightarrow\{B_j\}\rightarrow\{A_i'\}$，要求 $\{A_i'\}$ 与 $\{A_i\}$ 的差别趋于 0

例 $\{a, b\}$ $\{P_a=0.99\ \ P_b=0.01\}$

考虑其 2 次扩展信源：$\{aa, ab, ba, bb\}$ $\{0.9801, 0.0099, 0.0099, 0.0001\}$

用 $\log_2 3$ 个比特来表示 抛除

随着信号位数（信号序列的长度）的增加，我们地除掉一些信号，引起一个错误概率P_n，但随着n的增加，P_n指数地趋于0.

注意：我们不只对信源的单个符号进行一一对应的编码，我们只对信源A所产生的符号序列进行编码（即$A^N = A_1A_2\cdots A_N$，对符号$a_i = a_{i1}a_{i2}\cdots a_{iN}$进行编码），从而使平均码长下降。

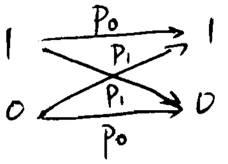
Shannon第一定理：（选取其中的一种表述）

离散无记忆信源的N次扩展信源S^N，其熵为$H(S^N)$，并有码符号集$X:\{a_1,a_2,\cdots a_r\}$，对信源S^N进行编码，总可以找到一种编码方法，使S中的每个信源符号所需要的平均码长$\bar{n}$满足：$$\lim_{N\to\infty}\bar{n} = \frac{H(S)}{\log_2 r}$$

Shannon第二定理（信道编码定理）

信道编码的目的：加上冗余信息，增强信息的稳定性.

例子：二元对称信道



$P_0 = P(1|1) = P(0|0)$

$P_1 = P(1|0) = P(0|1)$

为了克服失真：$1 \longrightarrow 111 \quad 0 \longrightarrow 000$

	P_0^3	$3P_0^2P_1$	$3P_0P_1^2$	P_1^3
111	111	110, 101, 011	100, 010, 001	000

解码原则：少数服从多数. $\left.\begin{matrix}111\\110,101,011\end{matrix}\right\} \longrightarrow 1$.

则错误率 $1-P_0^3-3P_0^2P_1 = 3P_0P_1^2+P_1^3 \propto P_1^2$ 失真度被减小.

编码原则：希望传输速率大，失真度尽可能小.

Shannon第二定理（选取一种描述）：只要信道的信息传输率R不超过信道容量C，则总可以找到一种编码，一方面使最小平均错误译码概率P_{emin}任意小，一方面又可以使信道的信息传输速率R无限地接近信道容量C，使通信既有效，又可靠。

（该定理为存在性定理，它没有回答如何去怎样找到的问题）

§1.2 量子力学的基本公设

1. 量子态（Hilbert空间的射线）

Hilbert空间的定义：a). 它是复数域上的一个~~[illegible]~~矢量空间，矢量用Dirac符号 $|\psi\rangle$ 表示.

（矢量空间：一组元素 $\{u, v, w\}$ 的集合 $\mathcal{L}$ 为矢量空间，若 $\mathcal{L}$ 在加法运算下是封闭的；数域F中的任一个数与 $\mathcal{L}$ 中的任一元素可以被乘法结合成 $\mathcal{L}$ 中的一元。

$$u, v \in \mathcal{L}. \quad a, b \in F$$

$$a(u+v) = au + av \in \mathcal{L}$$

$$(a+b)u = au + bu \in \mathcal{L}$$

$$a(bu) = (ab)u \in \mathcal{L}$$

b). 对该空间的任意两个矢量 $|\psi\rangle, |\phi\rangle$，定义值域为C的内积，内积满足：

i) 正定性：$\langle\psi|\psi\rangle \geq 0$ "=" iff $|\psi\rangle = 0$

ii) 线性性：$\langle\phi|(a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\phi|\psi_1\rangle + b\langle\phi|\psi_2\rangle$

iii) 反称性：$\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

$\langle\psi|$ 为矢量 $|\psi\rangle$ 的共轭矢量.

c) 存在范数（模） $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$

$\| |\psi\rangle \| \| |\phi\rangle \| \geq |\langle\psi|\phi\rangle|$ Schwarz不等式.

$\|v\| + \|u\| \geq \|v + u\|$

▲ $\|u+v\|^2 + \|u-v\|^2 = 2\|u\|^2 + 2\|v\|^2$

d) 完备性（针对无限维空间）

Cauchy序列，称 $c_1, c_2, \cdots c_n$ 为Cauchy序列，若对任意小的正数 ε，都可以找到一个正整数 N，使得对任意两个整数 $n > N$, $m > N$，都有 $|c_n - c_m| < \varepsilon$ 成立。根据Cauchy收敛准则，Cauchy序列一定有极限存在，即对任意小的正数 ε，总有一个正整数 N，当 $n > N$ 时，有 $|c_n - c| < \varepsilon$ 成立，c 称为Cauchy序列的极限

内积空间完备性的要求：任意一个以内积空间 $\mathcal{L}$ 中矢量为元素的Cauchy序列，其极限也在 $\mathcal{L}$ 中，则称 $\mathcal{L}$ 是完备的.

满足 (a) — (d) 称为Hilbert空间.

射线，它是一个等价类，其等价类中的矢量仅差一个复数因子，我们一般取归一化态为代表。

关于完备性的说明：完备性的要求并不能马上给出物理意义，但它是基本的，因为关于Hilbert空间的很多理论的证明要求趋于某个limit，而这个limit必须也属于Hilbert空间。如果完备性不足，我们就不能有Hilbert空间，于是，一些为Hilbert空间证明的一些理论也就失效了。

2. 力学量：

原则上可以被观测的量.

数学上：Hilbert空间中的自共轭算符 $A^+=A$.

算符 $\hat{A}$，它的作用是对态产生一个映射：$\hat{A}|\psi\rangle=|\phi\rangle$

如对任意的 $|\psi\rangle$ 和 $|\phi\rangle$，$\langle\psi|A|\phi\rangle=\langle\phi|B|\psi\rangle$

则 A、B 互为转置算子. 记为：$B=\tilde{A}$

A^+ 就是对其转置算子求复共轭：$A^+=\tilde{A}^*$

如. A. B 为力学量 $\Longrightarrow$ $A+B$，$i[A,B]$ 也是力学量.

但，一般 AB 不一定是力学量.

如. 一力学量 A 作用于 $|\psi\rangle$，有 $A|\psi\rangle=a|\psi\rangle$. 则 $|\psi\rangle$ 为 A 的本征态.

任一力学量的本征态构成Hilbert空间中一组正交完备的基矢 $(|1\rangle,|2\rangle,\ldots|n\rangle)$

定义投影算符. $P_i=|i\rangle\langle i|$

则算符 $\hat{A}$ 有谱分解. $A=\sum_i a_i P_i$ $\qquad P_iP_j=\delta_{ij}P_i \qquad P_i^+=P_i$

3. 态的演化 （量子演化之一）

孤立量子系统态矢量随时间的演化遵从Schrödinger方程.

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle=\hat{H}|\psi\rangle \qquad \hat{H} \text{ 为系统的哈密顿量}$$

这是一个保内积的映射，

设 $|\psi_1(t)\rangle$，$|\psi_2(t)\rangle$ 是 SE 的两个解，可以证明 $\frac{\partial}{\partial t}\langle\psi_1(t)|\psi_2(t)\rangle=0$.

这是一个幺正演化，$|\psi(t)\rangle=U(t)|\psi(0)\rangle$

$$U(t)U^+(t)=I \qquad U(t)=e^{-iHt/\hbar} \qquad (H\text{不含时})$$

4 测量（非幺正过程）（量子演化之二）

Von-Neumann假定，测 $\hat{A}=\sum_n a_n|n\rangle\langle n|$ $\quad |\psi\rangle=\sum_n \alpha_n|n\rangle$

① 测量结果为本征值 a_n 之一，相应的概率为 $P_n=|\alpha_n|^2$

② 如测量结果为 a_n 的话，测量后的量子态为 $|n\rangle$

③ 如果未选择测量结果，我们将其表达为混态系综的形式 $\rho=\sum_n|\alpha_n|^2|n\rangle\langle n|$.

两点说明：i) 系统与测量仪器相互作用，从而改变了原来态制备过程中的限定条件，测量后的态不再是原来的态。测量可以说是一种新的态制备过程。

（为什么会产生随机的，不可逆的坍缩？但如上是用演化的观点来讲的）。只是，这里的演化不一定再是封闭的了。$|\psi\rangle\langle\psi|:\begin{pmatrix}\times&\times\\ \times&\times\end{pmatrix}\to\begin{pmatrix}\times&0\\ 0&\times\end{pmatrix}$. 但世界为什么只选择一种结果呢？（平行宇宙？）

ii) 在 QI 与 QC 中，量子测量与量子迭加性构成一对矛盾。我们要不断地对同一态所构成的系综进行测量，才能获得量子迭加的信息。于是，这启发人们在量子计算中，要尽可能增大所需要的结果出现的概率，减小不需要的结果出现的概率。

§1.3. 混合态系统和 Schmidt 分解

1. 混合态.

在上一节中，我们对量子系统的描述强调的是孤立系统。如果我们仅仅将考虑的对象限于一个大系统中的子系统，则：

① 态不一定是射线；

② 测量不一定是正交投影；

③ 演化不一定是幺正的。

对复合系统的子系

重新考虑系统状态的描述：

A系统正交基 $\{|0\rangle_A,|1\rangle_A\}$ $\quad$ B系统正交基 $\{|0\rangle_B,|1\rangle_B\}$

$|\psi\rangle_{AB}=a|0\rangle_A|0\rangle_B+b|1\rangle_A|1\rangle_B$

假定测量A子系，向 $\{|0\rangle_A,|1\rangle_A\}$ 基上投影，以 $|a|^2$ 的几率获得 $|0\rangle_A$，测量将把态制备到 $|0\rangle_A|0\rangle_B$ 上；以 $|b|^2$ 的几率获得 $|1\rangle_A$，测量将把态制到 $|1\rangle_A|1\rangle_B$ 上。

设力学量 M_A（A系统中），测其平均值，$M_A\otimes I_B$

$$\langle M_A\rangle = {}_{AB}\langle\psi|\, M_A\otimes I_B\,|\psi\rangle_{AB}$$

$$= \left(a^*\,{}_A\langle 0|\,{}_B\langle 0| + b^*\,{}_A\langle 1|\,{}_B\langle 1|\right) M_A\otimes I_B \left(a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B\right)$$

$$= |a|^2\langle 0|M_A|0\rangle + |b|^2\langle 1|M_A|1\rangle$$

$$= \mathrm{Tr}\,(M_A\rho_A) \qquad \mathrm{Tr}_B(|\psi\rangle_{AB}\langle\psi|) = \rho_A = |a|^2|0\rangle_A\langle 0| + |b|^2|1\rangle_A\langle 1|$$ （A系统的约化密度矩阵）

$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ $\{p_i, |\psi_i\rangle\}$ 不同的 $|\psi_i\rangle$ 之间没有相干性

它有两种含义：

① 混合态所描述的系统

② 混和态描述纯态的约化态

实现混合态系统的方式有无穷种，而对于纯态则即使生成方式不同，但所有着同样密度矩阵的系统一旦生成，在统计上它们无法区分的。

2. 密度算符的特征

① 自共轭性 $\rho = \rho^\dagger$

② 半正定性 对于任意 $|\psi_A\rangle\in H_A$ $\langle\psi_A|\rho|\psi_A\rangle \geq 0$

③ 归一性 $\mathrm{tr}\,\rho = 1$

④ 对于纯态 $\rho = |\psi\rangle\langle\psi|$ $\rho^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho$

密度矩阵的演化（与外界无相互作用）
（封闭系统）

$$H_{AB} = H_A\otimes I_B + I_A\otimes H_B$$

$U_{AB}(t) = U_A(t)\otimes U_B(t)$ $|\psi(0)\rangle = \sum_{i,\mu} a_{i\mu}|i(0)\rangle_A|\mu(0)\rangle_B$ $\{|i(0)\rangle\}$, $\{|\mu(0)\rangle\}$ 正交

$|\psi(t)\rangle_{AB} = \sum_{i,\mu} a_{i\mu}|i(t)\rangle_A|\mu(t)\rangle_B$ $|i(t)\rangle_A = U_A(t)|i(0)\rangle_A$ $|\mu(t)\rangle_B = U_B(t)|\mu(0)\rangle_B$

$$\rho_A(t) = \mathrm{Tr}_B\,\rho_{AB}(t)$$
$$= \sum_{ij\mu} a_{i\mu}a_{j\mu}^*\,|i(t)\rangle_A\langle j(t)| = U_A(t)\rho_A(0)U_A^\dagger(t)$$

$$i\hbar\frac{\partial}{\partial t}\rho(t) = i\hbar\frac{\partial}{\partial t}\sum_{ij\mu}a_{i\mu}a_{j\mu}^*|i(t)\rangle\langle j(t)|$$
$$= H\rho - \rho H = [H,\rho]$$

区别 Heisenberg 方程．$i\hbar\frac{\partial}{\partial t}\hat{A} = [\hat{A}, H]$

3. Schmidt分解定理.

适用对象：二子系统的纯态.

定理内容：二粒子系统A、B，其Hilbert空间记为$H=H_A\otimes H_B$，该空间的任一纯态$|\psi\rangle_{AB}$，能够表示为如下的标准形式：

$|\psi\rangle_{AB}=\sum_i p_i|i\rangle_A|i'\rangle_B$. 其中$\{|i\rangle_A\}$为$H_A$中的一组正交归一态，$\{|i'\rangle_B\}$为$H_B$中的一组正交归一态.

证明：

$\{|i\rangle_A\}$为H_A中的一组正交基，$\{|\mu_B\rangle\}$为H_B中的一组正交基

$|\psi\rangle_{AB}=\sum_{i,\mu}a_{i\mu}|i\rangle_A|\mu\rangle_B$

$=\sum_i|i\rangle_A|\tilde{i}_B\rangle \qquad |\tilde{i}\rangle_B=\sum_\mu a_{i\mu}|\mu\rangle_B$.

选定$\{|i\rangle_A\}$为ρ_A的本征态. 则$\rho_A=\sum_i p_i|i\rangle_A\langle i| \qquad \sum_i p_i=1$

$\rho_A=Tr_B\rho_{AB}=\sum_k {}_B\langle k|\psi_{AB}\rangle\langle\psi_{AB}||k\rangle_B$

$=\sum_k {}_B\langle k|\sum_{ij}|i\rangle_A|\tilde{i}\rangle_B {}_B\langle\tilde{j}|{}_A\langle j||k\rangle_B$

$=\sum_{ij}|i\rangle_A\langle j|\ \langle\tilde{j}|\sum_k|k\rangle\langle k|\tilde{i}\rangle$.

$=\sum_{ij}{}_B\langle\tilde{j}|\tilde{i}\rangle_B\ |i\rangle_A\langle j|=\sum_i p_i|i\rangle_A\langle i|$

$\therefore\ \langle\tilde{j}|\tilde{i}\rangle=p_i\delta_{ij}$. $\quad\therefore$ 令 $|i'\rangle_B=\frac{1}{\sqrt{p_i}}|\tilde{i}\rangle_B$ 则 $|\psi_{AB}\rangle=\sum_i\sqrt{p_i}|i\rangle_A|i'\rangle_B$.

$|i'\rangle_B$也是一组正交归一化态.

$\therefore$ 定理得证.

$\rho_A=\sum_i p_i|i\rangle_A\langle i| \qquad \rho_B=\sum_i p_i|i'\rangle_B\langle i'|$ 本征谱相同.

补充说明：①. H_A和H_B可以是不同维数的.

② 如ρ_A ρ_B中除了0本征值外，没有简并的本征值，则Schmidt分解由ρ_A和ρ_B唯一确定.

③ 存在简并本征值的情况，$|\psi\rangle_{AB}$的表示不唯一.

原因：$|\psi\rangle_{AB}=\frac{1}{\sqrt{N}}\sum_i|i\rangle_A|i'\rangle_B=\frac{1}{\sqrt{N}}\sum_{ij}\delta_{ij}|i\rangle_A|j'\rangle_B=\frac{1}{\sqrt{N}}\sum_{ijk}U_{ki}^*U_{kj}|i\rangle_A|j'\rangle_B$

$=\frac{1}{\sqrt{N}}\sum_{ijk}U_{ki}^*|i\rangle_A U_{kj}|j'\rangle_B=\frac{1}{\sqrt{N}}\sum_k|k\rangle_A|k'\rangle_B$.

△. 利用纠缠进行超光速通讯的不可能性：

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle + |\downarrow_z\rangle) \qquad |\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle - |\downarrow_z\rangle) \Longrightarrow |\uparrow_z\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle + |\downarrow_x\rangle) \quad |\downarrow_z\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle - |\downarrow_x\rangle)$$

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\uparrow_{z_A}\downarrow_{z_B}\rangle - |\downarrow_{z_A}\rangle|\uparrow_{z_B}\rangle) \qquad \rho_A = \rho_B = \frac{1}{2}(|\uparrow_z\rangle\langle\uparrow_z| + |\downarrow_z\rangle\langle\downarrow_z|) = \frac{1}{2}I$$

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{2}(|\uparrow\rangle+|\downarrow\rangle)(|\uparrow\rangle-|\downarrow\rangle) - \frac{1}{2}(|\uparrow\rangle-|\downarrow\rangle)(|\uparrow\rangle+|\downarrow\rangle)\right)$$

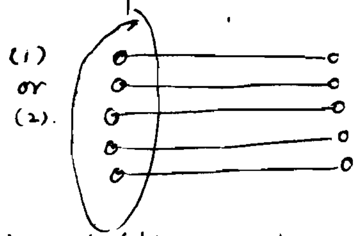
$$= \frac{1}{\sqrt{2}}(|\downarrow\rangle_x|\uparrow\rangle_x - |\uparrow\rangle_x|\downarrow\rangle_x)$$

按照原来的测量的描述 $M_A\otimes I_B$ 的测量会引起波包整体的坍缩

可是，我们使用 (1) σ_{xA} (2) σ_{zA}

$\downarrow$ $\searrow$

$\{|\uparrow_{xB}\rangle, |\downarrow_{xB}\rangle\}$ $\{|\uparrow_{zB}\rangle, |\downarrow_{zB}\rangle\}$



但是，作为接收方 $\frac{1}{2}(|\uparrow_x\rangle\langle\uparrow_x| + |\downarrow_x\rangle\langle\downarrow_x|) = \frac{1}{2}(|\uparrow_z\rangle\langle\uparrow_z| + |\downarrow_z\rangle\langle\downarrow_z|) = \frac{1}{2}I$

统计测量无法识别两个相同的密度矩阵 (未证明)

∴利用这种方式，无法进行超光速通信

△. 关于量子擦除

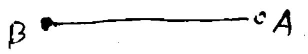
混合态：$\rho = \frac{1}{2}I = \frac{1}{2}(|\uparrow_z\rangle\langle\uparrow_z| + |\downarrow_z\rangle\langle\downarrow_z|)$

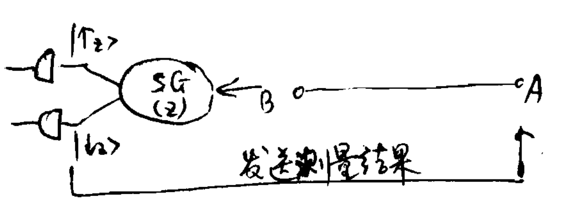
相干迭加态：$|\uparrow_x;\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle \pm |\downarrow_z\rangle)$

如测 σ_z 不可区分，测 σ_x 可以区分 (相干迭加的干涉效应)

相干迭加时相对相位有可观测的效应；而对非相干迭加，则没有相位的效应。

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle_A|\uparrow_z\rangle_B + |\downarrow_z\rangle_A|\downarrow_z\rangle_B)$$



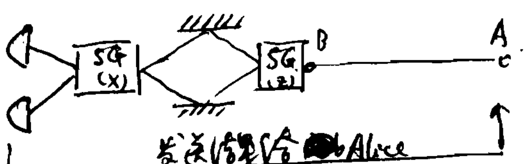


此时，A粒子无法传递相位 ($|\downarrow_z\rangle, |\uparrow_z\rangle$ 的干涉)

SG (x) < 随机输出

量子擦除（擦除路径信息）

擦除了上下的信息



以上的关于量子擦除的讨论，可以从系综选择的角度来理解。量子擦除实际上是从混合态 $\rho = \frac{I}{2}$ 中选择出一个以 $|\uparrow_x\rangle$ (或 $|\downarrow_x\rangle$ 为标志的子系综)

4. GHJW 定理（Gisin－Hughston－Josza－Wootters）

混和态的纯化的概念。

任何一个密度算符 ρ_A，总可以找到一个扩展空间的纯态 $|\psi\rangle_{AB}$，满足 $\rho_A = Tr_B(|\psi\rangle_{AB}\langle\psi|)$

$|\psi\rangle_{AB}$ 一定存在，但不唯一。

$\because \rho_A = \sum_i p_i |i\rangle_A\langle i|$ $\qquad |\psi_{AB}^{(1)}\rangle = \sum_i \sqrt{p_i}\,|i\rangle_A |i'\rangle_B$

$|\psi_{AB}^{(2)}\rangle = \sum_i \sqrt{p_i}\,|i\rangle_A |\tilde{i}\rangle_B \qquad |\tilde{i}_B\rangle = U_B|i'_B\rangle$

$|\psi_{AB}^{(2)}\rangle = \sum_i \sqrt{p_i}\,|i\rangle_A U_B|i'_B\rangle = (I_A\otimes U_B)|\psi_{AB}^{(1)}\rangle$

GHJW定理的内容：同一密度算符的任意两个纯化之间相差一个纯化空间（扩展空间）的幺正变换

§1.4. 量子比特及其操作

1. 量子比特

① 量子信息的单位

② 二能态的量子体系 $\quad a|0\rangle + b|1\rangle \quad a, b \in C$

例：偏振光子、1/2自旋粒子、二能级的原子、离子、光子数、声子数

2. 量子比特的数学描述

纯态 $\quad c_0|0\rangle + c_1|1\rangle$

混和态 $\rho \qquad 2\times2$ 的厄米矩阵 $\quad\Rightarrow$ 3个自由参数

泡利矩阵

$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \qquad \sigma_y = i|1\rangle\langle 0| - i|0\rangle\langle 1| \qquad \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$

$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$

$\sigma_k\sigma_l = i\epsilon_{klm}\sigma_m$

$\{\sigma_k, \sigma_l\}_+ = \sigma_k\sigma_l + \sigma_l\sigma_k = 2\delta_{kl} I$

$[\sigma_k, \sigma_l] = \sigma_k\sigma_l - \sigma_l\sigma_k = 2i\epsilon_{klm}\sigma_m$

$\{I \quad \sigma_x \quad \sigma_y \quad \sigma_z\}$ 为 ~~[illegible]~~ 独立的厄米算符，可以展开任意一个 2×2 的厄米阵

$$\rho = \frac{1}{2}(I + \vec{p}\cdot\vec{\sigma}) = \frac{1}{2}\begin{pmatrix} 1+p_3 & p_1 - ip_2 \\ p_1 + ip_2 & 1-p_3 \end{pmatrix} \qquad \text{（厄米的）}$$

$tr\rho = 1 \qquad$（求迹为1）

由于 ρ 为半正定. $\therefore \det\rho \geq 0$.

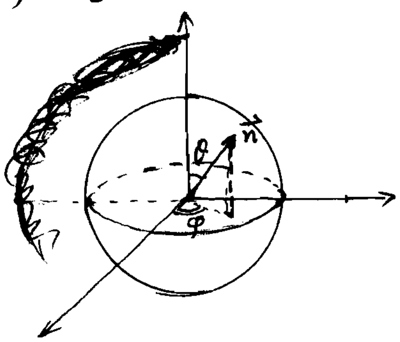
$$(1+p_3)(1-p_3)-p_1^2-p_2^2 = 1-(p_1^2+p_2^2+p_3^2) \geq 0 \Rightarrow |\vec{p}| \leq 1$$

$\vec{p}$ 称为Bloch矢量. 三维空间的球, 半径为1, 称为Bloch球.

$|\vec{p}|=1 \Rightarrow \det\rho = 0$. 由于 $\rho \geq 0$. $\therefore \lambda_1 = 1$ $\lambda_2 = 0 \rightarrow \rho = |\psi\rangle\langle\psi|$ 为纯态.

所有纯态(不区分整体相因子)的Bloch矢量与Bloch球面上的点一一对应.

$\rho = \frac{I}{2} \longrightarrow$ 对应球心.



对于纯态. $\vec{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$

$$\rho = \frac{1}{2}(I+\vec{n}\cdot\vec{\sigma})$$
$$= |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|$$
$$|\psi(\theta,\varphi)\rangle = \cos\frac{\theta}{2} e^{-i\varphi/2}|0\rangle + \sin\frac{\theta}{2} e^{i\varphi/2}|1\rangle.$$

Bloch矢量的用途:

求力学量平均. $\vec{n}\cdot\vec{\sigma}$ $\langle\vec{n}\cdot\vec{\sigma}\rangle = tr(\rho\,\vec{n}\cdot\vec{\sigma}) = tr\left[\left(\frac{1}{2}I+\frac{\vec{p}}{2}\cdot\vec{\sigma}\right)(\vec{n}\cdot\vec{\sigma})\right]$

由 $\mathrm{Tr}\,\sigma_i\sigma_j = 2\delta_{ij}$

$$= tr\frac{\vec{n}\cdot\vec{\sigma}}{2} + tr\frac{1}{2}(\vec{p}\cdot\vec{\sigma})(\vec{n}\cdot\vec{\sigma})$$
$$= \vec{p}\cdot\vec{n}.$$

进一步, 两qubit系统的密度矩阵的表示.

$$\rho = \frac{1}{4}\left(I\otimes I + \vec{r}\cdot\vec{\sigma}\otimes I + I\otimes\vec{s}\cdot\vec{\sigma} + \sum_{ij} t_{ij}\,\sigma_i\otimes\sigma_j\right)$$

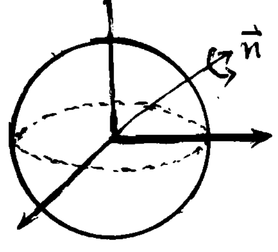
3 量子比特的操作:

(1) 单比特操作. $SU(2)$ 的幺正操作.

$$U(\theta,\vec{n}) = \exp\left(-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}\right).$$

$UU^+ = I$ (4个自由参数 $U(2)$)

$\det U = 1 \leftarrow SU(2)$ 去掉一个整体相位. (3个).



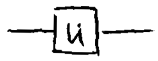
绕 $\vec{n}$ 轴(右手)旋转 θ 角.

$$U(\theta,\vec{n}) = \exp\left(-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}\right) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}.$$

为什么会有以上描述？ $\because H = aI + b\vec{n}\cdot\vec{\sigma}$ $U(t) = \exp(-i(aI+b\vec{n}\cdot\vec{\sigma})t)$

$= \exp(-iat)\,\underline{\exp(-ibt\,\vec{n}\cdot\vec{\sigma})}$

$\sigma_x = \begin{pmatrix}0&1\\1&0\end{pmatrix} \Longrightarrow \begin{cases}|0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle\end{cases}$ 比特反转.

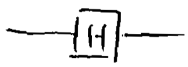


(U门的图示)

$\sigma_z = \begin{pmatrix}1&0\\0&-1\end{pmatrix} \Longrightarrow \begin{cases}|0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle\end{cases}$ 相位反转.

$\sigma_y = i\sigma_x\sigma_z$ 比特相位反转.

量子Hadamard变换. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$



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

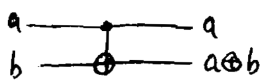
$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

$\hat{\sigma}_z = \hat{H}\hat{\sigma}_x H$

$\hat{\sigma}_x = H\sigma_z H$.

② 关于双比特的操作. (最重要的子集为控制U门). $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U$)

XOR (CNOT)



4×4 在 ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$ 基下)

$U_{CNOT} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$ $|x\rangle|y\rangle \xrightarrow{CNOT} |x\rangle|y\oplus x\rangle$

例：$(a|0\rangle+b|1\rangle)_A(c|0\rangle+d|1\rangle)_B$

$\xrightarrow{CNOT} ac|00\rangle + bc|11\rangle + ad|01\rangle + bd|10\rangle$

③ 3比特的操作 (控制-控制U门).

Δ. 量子Toffoli门操作 (控制-控制非门操作)

$|x, y, z\rangle \xrightarrow{\theta^{(3)}} |x\rangle|y\rangle|z\oplus xy\rangle$

Toffoli门在可逆计算中有很重要的作用，是最简单的普适门操作.

Δ. Deutsch门操作. (非SU)

在 $x=y=1$ 时, z 发生一个 R 操作. $R = -iR_x(\theta) = -i\exp(i\frac{\theta}{2}\sigma_x)$

要求. θ/π 为无理数 (不可公度)

Deutsch证明了普适量子计算机的存在。Deutsch门是一种普适量子逻辑门：任意n个比特，对其做任意幺正变换，都可以通过Deutsch门组联生成.

§1.5. 广义测量和广义演化.

§1.5.1 正交测量 (Von Neumann 测量)

Von Neumann 对测量的观点：将经典观量与系统的状态同宏观经典变量的值联系起来是可能的。我们先想当然地认为，我们可以察觉经典变量的值.

我们用一个自由粒子作为指针，探测这个指针的位置 (x)。现在，我们考虑测量精度的限制.

$t=0$: $\Delta x(0)$ 测不准关系 $\Delta x \Delta p \sim \hbar$

$$\Delta v = \frac{\Delta p}{m} \sim \frac{\hbar}{m\Delta x}$$

t. $\Delta x(t) \sim \Delta x + \frac{\hbar t}{m\Delta x} - 2\sqrt{\frac{\hbar t}{m}} + 2\sqrt{\frac{\hbar t}{m}} \geq 2\sqrt{\frac{\hbar t}{m}}$

$$[\Delta x(t)]^2_{min} \sim \frac{\hbar t}{m}$$

$$\Delta x(t) > (\Delta x(t))_{SQL} \sim \sqrt{\frac{\hbar t}{m}}$$

现在，我们看这个自由粒子作为指针，同一个量子系统发生耦合.

$$H = H_0 + \frac{1}{2m}\hat{p}^2 + \lambda \hat{M}\hat{p} \qquad H_0 \text{ 是系统的自由 Hamiltonian.}$$

$$U(t) = e^{-iHt/\hbar} = e^{-\frac{i}{\hbar}t(H_0+\lambda MP)} e^{-\frac{i}{\hbar}t\frac{1}{2m}p^2}$$

为了简化分析，我们令 $[H_0, M]=0$ (或是这个测量经历的时间非常短)

$\because [H_0, M]=0$. $U(t) = e^{-i\lambda\hat{M}\hat{p}t/\hbar} e^{-iH_0t/\hbar} e^{-i\frac{p^2}{2m\hbar}t}$

$$|\psi(0)\rangle = \sum_a \alpha_a |a\rangle|\psi(0)\rangle$$

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle = e^{-i\lambda\hat{M}pt/\hbar}\sum_a \alpha_a e^{-iE_at/\hbar}|a\rangle|\psi(x)\rangle$$

$$= e^{-i\lambda\hat{M}pt/\hbar}\sum_a \alpha_a'|a\rangle|\psi(x)\rangle$$

$$\hat{M} = \sum_a m_a|a\rangle\langle a|$$

$$\hat{p} = -i\hbar\frac{\partial}{\partial x}$$

$$e^{-i\lambda\hat{M}pt/\hbar} = e^{-\sum_a m_a\lambda t|a\rangle\langle a|\frac{\partial}{\partial x}}$$

$$e^{-i\lambda\hat{M}pt/\hbar}\sum_a \alpha_a'|a\rangle|\psi(x)\rangle = \sum_a \alpha_a'|a\rangle \otimes |\psi(x - m_a\lambda t)\rangle$$

如 $\Delta x \le \lambda m_a t$，则我们就可以分辨不同的 m_a 的值。同时，以 $|\alpha_a|^2$ 的几率使得系统处于 $|a\rangle$.

例如: Stern-Gerlach 实验. 被测量: σ_z.

它通过一个梯度磁场 $B = \lambda\hat{z}$ $\qquad H = -\lambda\mu\hat{z}\hat{\sigma}_3$

$\hat{z}$ 产生动量的平移.

一个问题：我们在讨论易擦除时应注意，建立上面的测量系统的解释为什么测量前制备到 $\hat{M}$ 的本征态，为什么不是 $\hat{M}$ 的叠加呢？为什么 $|\psi(x)\rangle$ 有特殊的地位？

力学量 $\hat{A}=\sum_a \alpha_a|a\rangle\langle a|=\sum_a\alpha_a\hat{P}_a$

$\hat{P}_a$：①.正定性 ②厄米性 ③完备性 ④正交性.

i) 测量结果为 α_a 的几率 $Prob(\alpha_a)=tr(\hat{P}_a\rho)$

ii) 选择性测量，输出为 α_a，则末态为 $|a\rangle$

iii) 非选择性测量 $\rho_{out}=\sum_a \hat{P}_a\rho\hat{P}_a=\sum_a Prob(\alpha_a)\hat{P}_a$

§1.5.2 广义测量：

问题的引入：考虑 Hilbert 空间 H_A 是大的空间 H 的一部分，它们之间存在直和结构。

$$H=H_A\oplus H_A^\perp$$

我们的观察者生活在 H_A 中，他的观测量 M_A 满足：

$$M_A|\psi^\perp\rangle=0=\langle\psi^\perp|M_A \qquad M_A\in H_A,\ |\psi^\perp\rangle\in H_A^\perp$$

当实施一个 H 中的正交测量，处于 H_A 中的观测者仅仅知道他所处的空间 H_A 中的态的成分，而这些成分是可以不正交的，于是，该观测者可以认为是测量过程制备了一套非正交态的集合。

$$E_a=|u_a\rangle\langle u_a| \qquad |u_a\rangle\in H$$

$$|u_a\rangle=|\tilde{\varphi}_a\rangle+|\tilde{\varphi}_a^\perp\rangle \qquad |\tilde{\varphi}_a\rangle\in H_A,\ |\tilde{\varphi}_a^\perp\rangle\in H_A^\perp$$

$$\rho_A\in H_A.$$

$$\langle u_a|\rho_A|u_a\rangle=(\langle\tilde{\varphi}_a|+\langle\tilde{\varphi}_a^\perp|)\rho_A(|\tilde{\varphi}_a\rangle+|\tilde{\varphi}_a^\perp\rangle)=\langle\tilde{\varphi}_a|\rho_A|\tilde{\varphi}_a\rangle$$

观测者不知道 $H_A^\perp$ 中的情况，对他而言，$|u_a\rangle$ 与 $|\tilde{u}_a\rangle$ 是无法区分的。

$|\tilde{\varphi}_a\rangle=\sqrt{\lambda_a}|\varphi_a\rangle$，$|\varphi_a\rangle$ 为 H_A 中的归一化矢量，我们可以称输出为 $|\varphi_a\rangle$ 的几率为：

$$\langle\tilde{\varphi}_a|\rho_A|\tilde{\varphi}_a\rangle=\lambda_a\langle\varphi_a|\rho_A|\varphi_a\rangle$$

定义算符 $\hat{F}_a=I_AE_aI_A=|\tilde{\varphi}_a\rangle\langle\tilde{\varphi}_a|=\lambda|\varphi_a\rangle\langle\varphi_a|$

$$\sum_a\hat{F}_a=\sum_a I_AE_aI_A=I_AI_aI_A=I_A$$

★ 用非负算符来分割单位算符，这种分割定义一种测量，称为正定算符值的测量（Positive Operator-valued measure POVM），也称为广义测量。（注：并不仅仅局限于以上的直和形式）

★ 广义测量的特点 $\{F_a\}$：

①.正定性 $F_a\ge 0$. ②厄米性 $F_a^+=F_a$ ③完备性 $\sum_a F_a=I$.

④ 正交性 ✗

测量结果的几率：$\mathrm{Prob}(a)=\mathrm{Tr}(\rho\hat{F}_a)$

关于测量后的末态：对于一维算符的情况，若 $\hat{F}_a=\lambda_a|\psi_a\rangle\langle\psi_a|$，并且，对于 $\hat{F}_a$，输出为 $|\psi_a\rangle$，

则 $\hat{\rho}\xrightarrow{\text{POVM}}\rho'=\sum_a \mathrm{tr}(\rho\hat{F}_a)\,|\psi_a\rangle\langle\psi_a|$

$$
\begin{aligned}
&=\sum_a \lambda_a\langle\psi_a|\rho|\psi_a\rangle|\psi_a\rangle\langle\psi_a| \\
&=\sum_a \sqrt{\lambda_a}\,|\psi_a\rangle\langle\psi_a|\rho\left(\sqrt{\lambda_a}\,|\psi_a\rangle\langle\psi_a|\right) \\
&=\sum_a \sqrt{F_a}\,\rho\,\sqrt{F_a}.
\end{aligned}
$$

但是，在一般情况下，我们仅知道测量的几率，而不能给出测量末态的显式表示。

例子：构造单qubit的POVM.

有N个测量结果联系着Bloch球上的N个单位矢量 $\{\hat{n}_a\}$

要求 $\sum_a \lambda_a\hat{n}_a=0$ 成立，另外 $0<\lambda_a\le 1$ $\quad\sum_a\lambda_a=1$

令 $\hat{F}_a=\lambda_a(I+\hat{n}_a\cdot\hat{\sigma}_a)=2\lambda_a E(\hat{n}_a)$

$\sum_a \hat{F}_a=(\sum_a\lambda_a)I+(\sum_a\lambda_a\hat{n}_a)\cdot\hat{\sigma}_a=I$

$\therefore\{\hat{F}_a\}$ 定义了一个POVM。

§1.5.3. Neumark定理.

定理：任何由N个一维算符构成的广义测量，总可以用扩展Hilbert空间的正交测量来实现。

证明：　考虑一个Hilbert空间 H.　$\dim H=N$.

一个POVM. $\{F_a\}$　$a=1,2,\cdots n>N$.

$F_a=|\tilde{\varphi}_a\rangle\langle\tilde{\varphi}_a|$

$$\sum_{a=1}^{N}(F_a)_{ij}=\sum_{a=1}^{N}\tilde{\varphi}_{ai}^{*}\tilde{\varphi}_{aj}=\delta_{ij}$$

$$\tilde{\varphi}_{aj}\quad\begin{pmatrix}\varphi_{11}&\cdots&\varphi_{1N}\\ \vdots&&\\ \varphi_{n1}&\cdots&\varphi_{nN}\end{pmatrix}_{(n\times N)}\qquad\sum_{a=1}^{n}\tilde{\varphi}_{ai}^{*}\tilde{\varphi}_{aj}=\left(N\times n\right)\left(n\times N\right)=\left(N\times N\right)$$

我们从n维空间中可以找到N个矢量 u_i　$i=1,2,\cdots N$.

令 $u_{ai}=\tilde{\varphi}_{ai}$

则 $\sum_a u_{ai}^{*}u_{aj}=\delta_{ij}$　对 $i,j=1,2,\cdots N$.

$\therefore$ 有 $U^{+}U=I=UU^{+}$

$$\begin{bmatrix}\left[\;N\times n\;\right]\\ \left[\;(n-N)\times n\;\right]\end{bmatrix}\begin{bmatrix}\left[\;n\times N\;\right]&\left[\;n\times(n-N)\;\right]\end{bmatrix}=\begin{bmatrix}I_{N\times N}&0\\ 0&I_{(n-N)\times(n-N)}\end{bmatrix}$$

于是 $\tilde{\varphi}_{aj}$ 可以扩展 $(n-N)$ 维构成么正矩阵.

令 $|u_a\rangle = |\tilde{\varphi}_a\rangle + |\tilde{\varphi}_a^{\perp}\rangle$ $\quad |\tilde{\varphi}_a\rangle \in H \quad |\tilde{\varphi}_a^{\perp}\rangle \in H^{\perp}$

(n维中) (N维中) ($n-N$维中)

$E_a = |u_a\rangle\langle u_a|$ $\quad |u_a\rangle$ 构成了 n维空间中的正交基，通过投影到空间H，产生了 POVM $\{F_a\}$

$$\begin{aligned} & I_N E_a I_N \\ = & I_N (|\tilde{\varphi}_a\rangle + |\tilde{\varphi}_a^{\perp}\rangle)(\langle\tilde{\varphi}_a| + \langle\tilde{\varphi}_a^{\perp}|) I_N \\ = & |\tilde{\varphi}_a\rangle\langle\tilde{\varphi}_a| = F_a. \end{aligned}$$

§1.5.4. 直积空间中的正交测量.

§1.5.4. 直积空间中的正交测量

投影算符 $E_a \in H_A \otimes H_B$. $\sum_a E_a = I$

让我们考虑最初的量子系统是没有关联的.

$$\rho_{AB} = \rho_A \otimes \rho_B$$

$$Prob(a) = Tr_{AB}[E_a(\rho_A \otimes \rho_B)]$$

(AB末态) $$\rho'_{AB}(a) = \frac{E_a(\rho_A \otimes \rho_B)E_a}{Tr_{AB}[E_a(\rho_A \otimes \rho_B)]}$$

(A末态) $$\rho'_A(a) = Tr_B\,\rho'_{AB}(a) = \frac{Tr_B[E_a(\rho_A \otimes \rho_B)E_a]}{Tr_{AB}[E_a(\rho_A \otimes \rho_B)]}$$

$$Prob(a) = Tr_A[Tr_B(E_a(\rho_A \otimes \rho_B))]$$

这里: $Tr_B[E_a(\rho_A \otimes \rho_B)]$

$$= \sum_{ii'jj'\mu\mu'\nu\nu'\tau} (E_a)_{j\nu;i\mu}(\rho_A)_{i'j'}(\rho_B)_{\mu'\nu'}\langle\tau|(|j\rangle|\nu\rangle\langle i|\langle\mu|)(|i'\rangle\langle j'|)(|\mu'\rangle\langle\nu'|)|\tau\rangle$$

$$= \sum_{ii'jj'\mu\mu'\nu\nu'\tau} (E_a)_{j\nu;i\mu}(\rho_A)_{i'j'}(\rho_B)_{\mu'\nu'}\,\delta_{\tau\nu}\,\delta_{ii'}\,\delta_{\mu\mu'}\,\delta_{\nu'\tau}\,|j\rangle\langle j'|$$

$$= \sum_{i\mu jj'\nu} (E_a)_{j\nu;i\mu}(\rho_A)_{ij'}(\rho_B)_{\mu\nu}\,|j\rangle\langle j'|$$

$$= \sum_{ijj'}\Big(\sum_{\mu\nu}(E_a)_{j\nu;i\mu}(\rho_B)_{\mu\nu}\Big)(\rho_A)_{ij'}\,|j\rangle\langle j'|$$

$$Tr_A\Big(\sum_{ijj'}\Big(\sum_{\mu\nu}(E_a)_{j\nu;i\mu}(\rho_B)_{\mu\nu}\Big)(\rho_A)_{ij'}\,|j\rangle\langle j'|\Big)$$

$$= \sum_{kijj'}\Big(\sum_{\mu\nu}(E_a)_{j\nu;i\mu}(\rho_B)_{\mu\nu}\Big)(\rho_A)_{ij'}\,\langle k|j\rangle\langle j'|k\rangle$$

$$= \sum_{ij}\Big(\underbrace{\sum_{\mu\nu}(E_a)_{j\nu;i\mu}(\rho_B)_{\mu\nu}}_{F_{ji}}\Big)(\rho_A)_{ij}$$

$$= \sum_{ij}F_{ji}(\rho_A)_{ij} = Tr(F_a\rho_A)$$

令 $(F_a)_{ji} = \sum_{\mu\nu}(E_a)_{j\nu;i\mu}(\rho_B)_{\mu\nu}$

即 $\hat{F}_a = Tr_B(E_a(I \otimes \rho_B))$

$\hat{F}_a$ ①.厄米的. ②正定的. ③完备的. 构成H_A中的POVM.

$$(F_a)^*_{ij} = \sum_{\mu\nu}(E_a)^*_{i\nu;j\mu}(\rho_B)^*_{\mu\nu}$$
$$= \sum_{\mu\nu}(E_a)_{j\mu;i\nu}(\rho_B)_{\nu\mu}$$
$$= (F_a)_{ji}$$

注意：一般情况下，根据 ρ_A 与 F_a 无法给出 ρ_A' 的表达。对于POVM，我们仅关心输出结果的几率。

问题：如果有一个一维的 POVM $\{F_a\}_{a=1}^{n}$（在空间 H_A 中），那么，能否通过引入一个 ρ_B，从而通过在 $H = H_A\otimes H_B$ 中实施一个正交测量来实现该POVM呢？

即：$Tr\, E_a(\rho_A\otimes\rho_B) = Tr(F_a\rho_A)$ 能否成立？

答案是肯定的。

证明：i) 首先我们考虑 $n=rN$ 的情况。

$\{F_a\}_{a=1}^{n}$ $\quad dim\, H_A = N$ $\quad F_a = |\tilde{\varphi}_a\rangle\langle\tilde{\varphi}_a|$

根据 Neumark 定理，

$|u_a\rangle = |\tilde{\varphi}_a\rangle + |\tilde{\varphi}_a^{\perp}\rangle$ $\quad |\tilde{\varphi}_a^{\perp}\rangle \in H_A^{\perp}$ $\quad dim(H_A^{\perp}) = (r-1)N$

$|u_a\rangle$ 构成 n 维空间中的一组正交基

$|u_a\rangle \in H$ $\quad H = H_A\oplus H_A^{\perp}$

现将 $H_A^{\perp}$ 划分成 $(r-1)$ 个正交子空间

$$H_A^{\perp} = H_{A1}^{\perp}\oplus H_{A2}^{\perp}\oplus\cdots\oplus H_{A,r-1}^{\perp}$$

$$|\tilde{\varphi}_a^{\perp}\rangle = |\tilde{\varphi}_{1a}^{\perp}\rangle\oplus|\tilde{\varphi}_{2a}^{\perp}\rangle\oplus\cdots\oplus|\tilde{\varphi}_{r-1,a}^{\perp}\rangle \quad \text{且} \quad |\tilde{\varphi}_{ia}^{\perp}\rangle\in H_{Ai}^{\perp}$$

$$\delta_{ab} = \langle u_a|u_b\rangle = \langle\tilde{\varphi}_a|\tilde{\varphi}_b\rangle + \sum_{\mu=1}^{r-1}\langle\tilde{\varphi}_{\mu a}^{\perp}|\tilde{\varphi}_{\mu b}^{\perp}\rangle$$

现在，我们选择一个具有 r 维的空间 H_B，其正交基 $\{|\mu_B\rangle\}_{\mu=0}^{r-1}$

我们在一个直积空间 $H_A\otimes H_B$ 中定义矢量：

$$|\Phi_{AB}\rangle_a = |\tilde{\varphi}_a\rangle_A|0\rangle_B + \sum_{\mu=1}^{r-1}|\tilde{\varphi}_{\mu a}^{\perp}\rangle_A|\mu_B\rangle \qquad a=1,2,\cdots n.$$

${}_a\langle\Phi_{AB}|\Phi_{AB}\rangle_b = \delta_{ab}$. $\quad E_a = |\Phi_a\rangle_{AB}\langle\Phi_a|$ $\quad \{E_a\}$ 构成一套正交测量.

引入子系 B $\quad$ 令 $\rho_B = |0\rangle_B\langle 0|$

则 $H_A\otimes H_B$ 中的状态 $\rho_{AB} = \rho_A\otimes|0\rangle_B\langle 0|$

我们对 ρ_{AB} 做正交测量 $\{E_a\}$.

$$\text{则}\ {}_{AB}\langle\Phi_a|\rho_{AB}|\Phi_a\rangle_{AB} = {}_A\langle\tilde{\varphi}_a|\rho_A|\tilde{\varphi}_a\rangle_A = Tr(F_a\rho_A)$$

如测量结果为 a，则 $\rho_{AB}' = |\Phi_a\rangle_{AB}\langle\Phi_a|$

$$\rho_A' = Tr_B(|\Phi_a\rangle_{AB}\langle\Phi_a|) = |\tilde{\varphi}_a\rangle\langle\tilde{\varphi}_a| + \sum_{\mu=1}^{r-1}|\tilde{\varphi}_{\mu a}^{\perp}\rangle\langle\tilde{\varphi}_{\mu a}^{\perp}|$$

ii). 对于 $n = rN - c$ 的情况

我们只需选择 $|\tilde{\varphi}_{r-1,a}^{\perp}\rangle$ 的最后 c 个成分为 0，$|\Phi_{AB}\rangle_a$ 仍仍然相互正交。

补充 c 个相互正交的矢量

$|e_i\rangle_A|r-1\rangle_B \qquad i=N-c+1,\ N-c+2,\cdots,N.$

$|e_i\rangle$ 表示在基 $\{|j\rangle_A\}_{j=1}^N$ 下，仅有第 i 个分量不为0.

这样，$|\Phi_a\rangle_{AB}$ 和 $|e_i\rangle_A|r-1\rangle_B$ 构成 rN 维空间的一组正交基，从而可以实现POVM$\{F_a\}$.

§1.5.5. 超算符

如果A、B系统的演化是幺正的，如何来描述A系统的演化呢？

△. 算符和的表示：

初态：$\rho_A\otimes|0\rangle_B\langle 0|$

演化：$U_{AB}(\rho_A\otimes|0\rangle_B\langle 0|)U_{AB}^+$

$$\rho_A'=Tr_B(U_{AB}(\rho_A\otimes|0\rangle_B\langle 0|)U_{AB}^+)$$
$$=\sum_\mu {}_B\langle\mu|U_{AB}|0\rangle_B\,\rho_A\,{}_B\langle 0|U_{AB}^+|\mu\rangle_B$$

令 $M_\mu={}_B\langle\mu|U_{AB}|0\rangle_B$

于是：$\$(\rho_A)=\rho_A'=\sum_\mu M_\mu\rho_A M_\mu^+ \qquad (1)$

这里有 $\sum_\mu M_\mu^+M_\mu=\langle 0|U_B^+\sum_\mu|\mu\rangle\langle\mu|U_B|0\rangle=\langle 0|U_{AB}^+U_{AB}|0\rangle=I_A \quad (2)$

线性映射\$：映射线性算符到线性算符。这样的一种映射，如(2)式被满足，我们称其为超算符；(2)式称为这个超算符的算符和表示。(M_μ，M_μ^+ 称为Kraus算符)

△ 给定一个算符和的表示，创造一个相应的幺正表示总是可能的。

H_A 中的算符 $(M_\mu,M_\mu^+)_{\mu=1}^r$，选取一个Hilbert空间 H_B，满足 $dim(H_B)\geq r$。

任意一个 $|\varphi_A\rangle\in H_A$，$\{|\mu_B\rangle\}$ 为 H_B 中的一组正交态，$|0\rangle_B$ 为 H_B 中的某一标准化态，

现定义 U_{AB} 满足：

$$U_{AB}(|\varphi_A\rangle\otimes|0\rangle_B)=\sum_\mu M_\mu|\varphi_A\rangle|\mu_B\rangle$$

为了验证 U_{AB} 是否为幺正，我们看内积是否保持

$$\left(\sum_\nu {}_A\langle\varphi_2|M_\nu^+\otimes\langle\nu|\right)\left(\sum_\mu M_\mu|\varphi_1\rangle_A\otimes|\mu\rangle\right)$$
$$={}_A\langle\varphi_2|\sum_\mu M_\mu^+M_\mu|\varphi_1\rangle=\langle\varphi_2|\varphi_1\rangle={}_B\langle 0|{}_A\langle\varphi_2|\varphi_1\rangle_A|0\rangle_B$$

∴ U_{AB} 可以扩展为作用在 $H_A\otimes H_B$ 上的幺正矩阵。(利用作业中的结论)

$$tr_B\left(U_{AB}|\varphi_A\rangle\otimes|0\rangle_B\right)\left({}_A\langle\varphi|\otimes{}_B\langle 0|U_{AB}\right)$$

$$=\sum_\mu M_\mu\left(|\varphi_A\rangle{}_A\langle\varphi|\right)M_\mu^+$$

而 ρ_A 可以表示为纯态的系综，于是可以有 $\$(\rho)=\sum_\mu M_\mu\rho M_\mu^+$.

※ 给定一个超算符后，算符和的表示不唯一。

$M_\mu={}_B\langle\mu|U_{AB}|0\rangle_B$ 　但基 $\{|\mu\rangle_B\}$ 的选择可以是任意的.

于是：$\$(\rho_A)=\sum_\mu M_\mu\rho M_\mu^+=Tr_B\left(U_{AB}|0\rangle_B\langle 0|\otimes\rho_A U_{AB}^+\right)$

$$=\sum_\mu {}_B\langle\mu|U_{AB}|0\rangle_B\,\rho_A\,{}_B\langle 0|U_{AB}^+|\mu\rangle_B$$

$$=\sum_\nu {}_B\langle\nu|U_{AB}|0\rangle_B\,\rho_A\,{}_B\langle 0|U_{AB}^+|\nu\rangle_B$$

$$=\sum_\nu N_\nu\rho_B N_\nu^+$$

~~[illegible]~~ 则 $N_\nu=U_{\nu\mu}M_\mu$.

幺正演化形成群，但超算符定义了一个半群（定义了乘法（乘法运算是封闭的），满足结合律）

超算符 \$（映射）　$\rho\longrightarrow\rho'$　（最一般的演化）

它满足：(1) 线性性　$\$(\rho_1+\rho_2)=\$(\rho_1)+\$(\rho_2)$

(2) \$ 是保厄米的.（如 ρ 是厄米的，则 $\$(\rho)$ 也是厄米的）

(3) \$ 是保迹的　$Tr\rho'=1$　if $Tr\rho=1$.

(4) \$ 是正定的.　$\rho\geq 0\implies\$(\rho)\geq 0$.

为什么要要求线性性？这主要是维系系综解释的合理性.

以下的非线性映射满足 (2)、(3)、(4) 的要求：

$$\$(\rho)=\exp\left(i\pi\sigma_x tr(\sigma_x\rho)\right)\rho\exp\left(-i\pi\sigma_x tr(\sigma_x\rho)\right)$$

如 $\rho=\frac{1}{2}\left(|\uparrow_z\rangle\langle\uparrow_z|+|\downarrow_z\rangle\langle\downarrow_z|\right)\longrightarrow\$(\rho)=\rho$.

如 $\rho=\frac{1}{2}\left(|\uparrow_z\rangle\langle\uparrow_z|+|\uparrow_x\rangle\langle\uparrow_x|\right)\longrightarrow\$(\rho)=\frac{1}{2}\left(|\downarrow_z\rangle\langle\downarrow_z|+|\uparrow_x\rangle\langle\uparrow_x|\right)$

那么，如满足条件 (1)—(4)，是否就一定有算符和的表示，并且可以通过两子系的幺正演化来实现？

(4′) 完全正定性：考虑 H_A 的任意可能的扩展 $H_A\otimes H_B$，如果 $\$_A\otimes I_B$ 对这种扩展是正定的，则称 $\$_A$ 在 H_A 上是完全正定的。

增加 (4′) 的合理性：对于 A 的演化，我们不能确定是否有某一系统 B 与 A 是否有耦合。完全正定性是说：如果 A 演化而 B 不演化，那么最初 A、B 系统的密度矩阵也将演化到另外一个密度矩阵。

例子：转置算符（正定，但不是完全正定）

$$\hat{T}\rho = \rho^T$$

$$\rho = U\,\mathrm{diag}\{\lambda_1, \lambda_2, \dots \lambda_n\}\,U^+$$

$$T\rho = U^*\,\mathrm{diag}\{\lambda_1, \lambda_2, \dots \lambda_n\}\,(U^*)^+$$

算符的转置并不改变本征值。∴转置算符是正定的。

但它不是完全正定的

∵ $\hat{T}_A \otimes I_B$ 为非正定算符

$\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$ $\qquad \rho = \frac{1}{2}\left(|0\rangle\langle 0|\otimes|1\rangle\langle 1| + |1\rangle\langle 1|\otimes|0\rangle\langle 0| + |0\rangle\langle 1|\otimes|1\rangle\langle 0| + |1\rangle\langle 0|\otimes|0\rangle\langle 1|\right)$

$$T\rho = \frac{1}{2}\left(|0\rangle\langle 0|\otimes|1\rangle\langle 1| + |1\rangle\langle 1|\otimes|0\rangle\langle 0| + |1\rangle\langle 0|\otimes|1\rangle\langle 0| + |0\rangle\langle 1|\otimes|0\rangle\langle 1|\right)$$

$$\rho^T = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 \end{pmatrix} \qquad \det \rho^T = -\tfrac{1}{16}$$

※ POVM ~~是~~ 超算符的演化

（一个幺正变换将 A、B 系统纠缠起来，然后对 B 系统实施一个正交测量，可以描述为实施在 A 上的 POVM）

∵ 有一个算符和的表示，总可以构造一个幺正变换，满足：

$$|\varphi\rangle_A|0\rangle_B \xrightarrow{U} \sum_\mu M_\mu|\varphi_A\rangle|\mu\rangle_B$$

测 B 系统 $Prob(\mu) = \langle\varphi_A|M_\mu^+ M_\mu|\varphi_A\rangle$

定义 $F_\mu = M_\mu^+ M_\mu$ $\qquad Prob(\mu) = Tr(F_\mu \rho_A)$

F_μ：厄米的，正定的，完备的。

如果 M_μ 也是厄米的 $\quad M_\mu = M_\mu^+ = \sqrt{F_\mu}$

$$\rho \longrightarrow \sum_\mu \sqrt{F_\mu}\,\rho\sqrt{F_\mu}$$

对于 $\rho_\mu' = \dfrac{\sqrt{F_\mu}\,\rho\sqrt{F_\mu}}{Tr(F_\mu\rho_A)}$ $\qquad Prob(\mu) = Tr(F_\mu\rho)$

于是：对一个系统 A 的最一般性的测量可以是，先将 A 与系统 B 相纠缠，再对 B 实施一个正交测量。

※ 算符的极性分解和奇异值分解

算符的极性分解：A 为矢量空间 V 上的线性算符，那么就存在幺正算符 U 和正定算符 J 和 K，使得，$A = UJ = KU$ $\qquad J = \sqrt{A^+A} \qquad K = \sqrt{AA^+}$

且，如果 A 是可逆的，则 U 是唯一确定的。

证明: $J=\sqrt{A^+A}$ 为正定算符

$J=\sum_i a_i |i\rangle\langle i|$ $\quad a_i\geq 0$.

定义: $|\psi_i\rangle = A|i\rangle$.

$\langle\psi_i|\psi_i\rangle = \langle i|A^+A|i\rangle = \langle i|J^2|i\rangle = a_i^2$

$\langle\psi_j|\psi_i\rangle = \delta_{ij} a_i^2$

于是找出 $a_i\neq 0$ 的基矢量 $|i\rangle$, 对应的令 $|e_i\rangle = |\psi_i\rangle/a_i$

则 $\langle e_i|e_j\rangle = \delta_{ij}$.

利用 Gram-Schmidt 程序, 将 $|e_i\rangle$ 扩展为正交基.

令 $U=\sum_i |e_i\rangle\langle i|$ $\qquad UU^+ = \sum_i |e_i\rangle\langle e_i| = \sum_i |i\rangle\langle i| = U^+U = I$.

$UJ = \sum_i |e_i\rangle\langle i| \sum_j a_j |j\rangle\langle j| = \sum_i a_i |e_i\rangle\langle i| = \sum_i |\psi_i\rangle\langle i| = A$.

$\because A=UJ$ $\quad A^+=JU^+$ $\therefore A^+A=J^2$ $\quad \therefore J=\sqrt{A^+A}$.

$\therefore A$可逆 $\Rightarrow J$可逆. $\Rightarrow U=AJ^{-1}$

$A=UJ = UJU^+U = KU$

$A^+=U^+K \quad \Rightarrow AA^+=K^2 \Rightarrow K=\sqrt{AA^+}$

奇异值分解定理: A为方阵, 那么存在幺正矩阵U和V, 和非负对角阵D,

满足$A=UDV$. $\quad D$中的对角元称为A的奇异值.

$A=SJ$ $\quad S$为幺正阵, J为正定

$J=TDT^+ \Longrightarrow A=\underbrace{ST}_{U}D\underbrace{T^+}_{V}$

§1.5.6 Kraus表示理论

任意满足以下四条性质的超算符，总可以写成算符和的形式：

(1) 线性性 (2) 保厄米性 (3) 保迹性 (4) 完全正定性

$$\hat{\$}(\rho) = \sum_\mu M_\mu \rho M_\mu^+ \qquad (\sum_\mu M_\mu^+ M_\mu = I)$$

~~[illegible]~~ 简介： 相对态方法

该方法将

作用在子空间A上的算符 M_A $\xleftrightarrow{\text{建立对应关系}}$ 作用在空间 $H_A \otimes H_B$ 中的最大纠缠态上的算符 $M_A \otimes I_B$

$\dim H_B \geq \dim H_A = N$

现定义一个未归一化的最大纠缠态 $|\tilde{\varphi}\rangle_{AB} = \sum_{i=1}^{N} |i\rangle_A \otimes |i'\rangle_B$ $\{|i\rangle\}$ H_A的正交基 $\{|i'\rangle\}$ 彼此正交

对于 H_A中任意一个态 $|\varphi\rangle_A = \sum_i a_i |i\rangle_A$ 定义 $|\varphi^*\rangle_B = \sum_{i=1}^{N} a_i^* |i'\rangle_B$

则 $|\varphi_A\rangle = {}_B\langle\varphi^*|\tilde{\varphi}\rangle_{AB} = \sum_{i=1}^{N} a_i |i\rangle_A$

$$|\varphi_A\rangle^{(H_A)} \xrightarrow[\text{反线性}]{} |\varphi_B^*\rangle^{(H_B)}$$

$$(c_1|\varphi_1\rangle_A + c_2|\varphi_2\rangle_A \longrightarrow c_1^*|\varphi_1^*\rangle_B + c_2^*|\varphi_2^*\rangle_B)$$

M_A为H_A空间中的算符

现在 $(M_A \otimes I_B)|\tilde{\varphi}_{AB}\rangle = \sum_i M_A |i\rangle_A \otimes |i'\rangle_B$

则 $M_A|\varphi_A\rangle = \langle\varphi_B^*|(M_A \otimes I)|\tilde{\varphi}\rangle_{AB}$ 称为算符的相对态表示
(等价的数学表示)

制备态 ~~[illegible]~~ $|\varphi_A'\rangle \Longleftrightarrow$ 用 $|\varphi_B'^*\rangle$ 向 $|\tilde{\varphi}_{AB}\rangle$ 投影

制备出 $|\varphi_A'\rangle$；用 M_A作用于其上 $\Longleftrightarrow$ 用 $M_A \otimes I$ 作用于 $|\tilde{\varphi}_{AB}\rangle$，再用 $|\varphi_B'^*\rangle$ 进行投影

现在我们将相对态的数学方法用于证明超算符的表示

证明： $\because$ $\underline{\hat{\$}_A\text{完全正定}}$ $\therefore$ $\hat{\$}_A \otimes I_B$ 也是正定的

于是 $\hat{\$}_A \otimes I_B(\hat{\rho}_{AB})$ 是正定算符

$$(\hat{\$}_A \otimes I_B)(|\tilde{\varphi}\rangle_{AB}\langle\tilde{\varphi}|) = \sum_\mu q_\mu |\tilde{\Phi}_\mu\rangle_{AB}\langle\tilde{\Phi}_\mu| \qquad (\text{厄米的})$$

$$q_\mu > 0 \quad \sum_\mu q_\mu = 1 \quad \langle\tilde{\Phi}_\mu|\tilde{\Phi}_\mu\rangle = N$$

应用相对态方法，

$$\hat{\$}_A(|\phi\rangle_A\langle\phi|) = {}_B\langle\phi^*|(\hat{\$}_A \otimes I_B)(|\tilde{\varphi}_{AB}\rangle\langle\tilde{\varphi}_{AB}|)|\phi^*\rangle_B$$

$$= \sum_\mu q_\mu \, {}_B\langle\phi^*|\tilde{\Phi}_\mu\rangle_{AB}\langle\tilde{\Phi}_\mu|\phi^*\rangle$$

定义. H_A中的算符M_μ:

$$M_\mu|\phi_A\rangle = \sqrt{q_\mu}\,{}_B\langle\phi^*|\tilde{\Phi}_\mu\rangle_{AB}$$

则 M_μ 满足.

(i) 线性映射 $|\phi_A\rangle \xrightarrow{\text{反线性映射}} |\phi_B^*\rangle \xrightarrow{\text{反线性映射}} {}_B\langle\phi^*|\tilde{\Phi}_\mu\rangle_{AB}$
(对态矢)

(ii) $\forall\, |\phi\rangle_A \in H_A$

$$\$_A(|\phi\rangle_A\langle\phi|) = \sum_\mu M_\mu(|\phi_A\rangle\langle\phi_A|)M_\mu^\dagger \qquad \text{(正半的)}$$

(iii) ∵ $\$$为线性算符 $\rho_A = \sum_i p_i|\phi_i\rangle\langle\phi_i|$ (线性的).

$$\hat{\$}(\rho_A) = \sum_\mu M_\mu \rho_A M_\mu^\dagger$$

(iv) $\hat{\$}$是保迹的. $\Longrightarrow$ $\sum_\mu M_\mu^\dagger M_\mu = I$ (保迹的)

这样,我们就建立了$\$_A$的算符和表示.

推论1: 线性独立的M_μ的最大个数为N^2个. ∵ $\dim H_A = N$. $\tilde{\rho}_{AB}$的最大秩为N^2.
$|\tilde{\Phi}_\mu\rangle_{AB}$的个数最大为$N^2$个.

推论2: 不同算符和的表示,可以对应同一个$\$$。两个算符和的表示$\{N_a\}$ $\{M_\mu\}$表示等价的充要条件是: $N_a = \sum_\mu M_\mu U_{\mu a}$.

小结: 如果有完全正定的超算符(对应于合理的物理作用) $\Longrightarrow$ 有算符和的表示.
$\Longrightarrow$ 可以对应扩展空间的么正演化.

A) 在量子信息中, Von Neumann 测量, U演化是不够普遍的;

B) 最普遍的测量是POVM测量, 最普遍的演化是算符和的演化;

C) POVM测量与算符和的演化分别对应扩展Hilbert空间的Von Neumann测量和U演化。

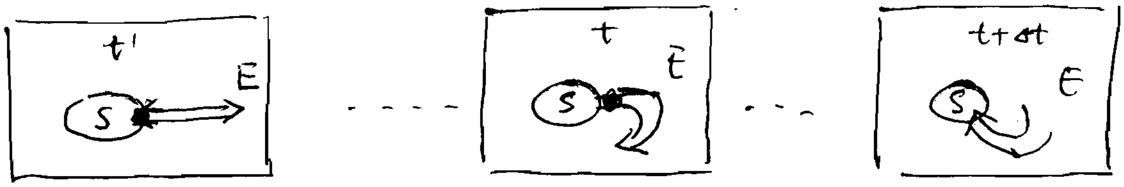
§1.5.7. 主方程

△ Markov近似。

微分方程所描述的过程在时间上是局域的,即系统$t+dt$时刻的状态完全由系统t时刻的状态决定。即:将来的状态只决定于现在的状态,与更前面的历史无关。

显然,孤立系统的演化是满足这一条件的.

但是,对子系统的演化是否同样满足呢! 举例:小封闭环境中的回声、旷野里说话.



$$\rho_S(t+\Delta t) = f(t, t-\Delta t, t-2\Delta t, \cdots t')$$

在这种情况下，建立描述子系统演化的微分方程是不行的.

Markov近似：系统流入环境的信息不会再流回来影响系统，即：系统对过去的历史是无记忆的.

什么是过去、现在、将来!

粗粒时间的概念：　环境的记忆时间 $(\Delta t)_{res}$

系统演化的特征时间 $(\Delta t)_{coarse}$ (相对于系统状态的变化，它可看成是很小)

$(\Delta t)_{coarse} \gg (\Delta t)_{res} \Longrightarrow$ Markov近似　(一般是弱耦合、环境自由度→∞)

※ Lindblad方程

要使 $\rho_A(t+dt) = \$_{dt}(\rho(t))$ 成立　$\rho(t+dt) = \sum_\mu M_\mu(dt)\rho(t)M_\mu^\dagger(dt)$

必须要求 初始时刻的系统与环境是没有纠缠的.

如果有纠缠，$c_1\rho_1 + c_2\rho_2$ 的线性演化特性就会遭到破坏.

按照Markov近似，我们对 $\rho_A(t)$ 的演化做一个形式的推导

$$\rho(dt) = \$_{dt}(\rho(0)) = \sum_\mu M_\mu(dt)\rho(0)M_\mu^\dagger(dt)$$

$$\$_{t=0} = I.$$

于是 $\rho(dt) = \rho(0) + O(dt)$

于是，我们得一个Kraus算子设为 $\hat{M}_0 = I + O(dt)$

余下的Kraus算子 M_μ　$\mu\neq0$ 将有 $\sqrt{dt}$ 的数量级.

如果系统经受量子跃迁，那么跃迁仅能以与 dt 成比例的概率出现.

令 $\begin{cases} \hat{M}_0 = I + (-iH+K)dt. & H.\ K.\ \text{厄米的} \\ \hat{M}_\mu = \sqrt{dt}\,\hat{L}_\mu & \mu = 1, 2, \ldots \end{cases}$

$$\sum_{\mu=0} M_\mu^\dagger M_\mu = I + \left(2K + \sum_{\mu\neq0} L_\mu^\dagger L_\mu\right)dt = I$$

$$\Longrightarrow K = -\frac{1}{2}\sum_{\mu\neq0} L_\mu^\dagger L_\mu.$$

$$\dot{\rho}(t) = \frac{\rho(t+dt) - \rho(t)}{dt} = -i[H,\rho] + \sum_{\mu\neq0}\left(L_\mu\rho L_\mu^\dagger - \frac{1}{2}L_\mu^\dagger L_\mu\rho - \frac{1}{2}\rho L_\mu^\dagger L_\mu\right)$$

这就是Lindblad主方程，其中 L_μ 称为跳跃算符.

§1.6. EPR佯谬，Bell不等式、CHSH不等式

1. EPR佯谬

※局域实在论的观点：

①.引入物理实在的定义：在系统没有被干扰的情况下，如果我们能确定地预言下一个物理量的值，那么这个物理量就必定是客观实在，对应着一个物理实在的元素。

②定义完备的物理理论：一个完备的理论应当包括所有的物理实在元素.

③局域性假定：对于两个分开的并没有相互作用的系统，对其中一个的测量必定不能修改关于另一个的描述，即：不存在超距的相互作用。

※从局域实在论出发来论去量子力学.

在量子力学中 $[\hat{x},\hat{p}]=i\hbar$.

但 $[\hat{x}_1-\hat{x}_2,\ \hat{p}_1+\hat{p}_2]=0$. 于是，$|\psi\rangle$可以处于$\hat{x}_1-\hat{x}_2$和$\hat{p}_1+\hat{p}_2$的本征态

由于两个"粒子1"和"粒子2"的分离距离非常远，对1的测量无法干扰粒子2（用了假定③）

但测量"1"的x_1，可以相应地确定x_2；测量"1"的p_1，可以相应地确定p_2。

也就是说，对于一个遥远的体系2，我们可以不扰动它，从而预言出它的x_2，p_2，于是，由假定①，我们可以推出x_2，p_2是物理实在。同样的推理，x_1，p_1也是物理实在。

但是，由假定②完备的理论应当包含所有物理实在的完备的描述。但在量子力学中，x,p不对易，不能同时精确地预言x，p，于是量子力学是不完备的。

$$\psi=\delta(x_1-x_2-L)\,\delta(p_1+p_2)$$

Bohm得到一个极化的EPR系统

$|\psi_{AB}\rangle=\frac{1}{\sqrt{2}}(|10\rangle-|01\rangle)$ 它是$\sigma_{x_1}\sigma_{x_2}$与$\sigma_{z_1}\sigma_{z_2}$的共同本征态.

Bohm给出了局域隐变量理论（存在经典随机变量+局域性假定），不需要引入量子纠缠.

2. Bell不等式与CHSH型不等式 (Clauser – Horne – Shimony – Holt)

目的：用于比较局域隐变量理论与量子力学哪个正确.

证明：$\vec{e}^{(1)}$，$\vec{e}^{(2)}$为沿着空间任意方向的两个单位矢量，测量电子1沿$\vec{e}^{(1)}$方向的自旋分量$\vec{\sigma}^{(1)}\cdot\vec{e}^{(1)}$的值记为$A(\vec{e}^{(1)})$，测量电子2沿$\vec{e}^{(2)}$方向的自旋分量$\vec{\sigma}^{(2)}\cdot\vec{e}^{(2)}$的值记为$B(\vec{e}_2)$

按照隐参数理论 $A(\vec{e}^{(1)})$, $B(\vec{e}^{(2)})$ 应由隐参数决定.

于是, $A(\vec{e}^{(1)},\lambda)\in\{\pm1\}$ $\quad B(\vec{e}^{(2)},\lambda)\in\{\pm1\}$

设 $\rho(\lambda)$ 是λ的归一化分布函数 $\int\rho(\lambda)d\lambda=1$.

按照局域性假定, 粒子1和2 在 $\vec{\sigma}^{(1)}\cdot\vec{e}^{(1)}$ 和 $\vec{\sigma}^{(2)}\cdot\vec{e}^{(2)}$ 再两个局域测量下的相关函数为:

$$P(\vec{e}^{(1)},\vec{e}^{(2)})=\int d\lambda\,\rho(\lambda)\underbrace{A(\vec{e}^{(1)},\lambda)\,B(\vec{e}^{(2)},\lambda)}_{\text{该处体现了局域性}}$$

我们先制备一个纠缠态系综(量子力学将之描绘为: $|\psi^-\rangle=\frac{1}{\sqrt2}(|0\rangle|1\rangle-|1\rangle|0\rangle)$), 但,我们暂时不知, 该系综满足 $A(\vec{e}^{(1)},\lambda)=-B(\vec{e}^{(1)},\lambda)$ 的特性.

现在,我们来计算下面的关联函数的差:

$$\begin{aligned}
&P(\vec{e}^{(1)},\vec{e}^{(2)})-P(\vec{e}^{(1)},\vec{e}^{\prime(2)})\\
&=\int d\lambda\,\rho(\lambda)\left[A(\vec{e}^{(1)},\lambda)B(\vec{e}^{(2)},\lambda)-A(\vec{e}^{(1)},\lambda)B(\vec{e}^{\prime(2)},\lambda)\right]\\
&=\int d\lambda\,\rho(\lambda)A(\vec{e}^{(1)},\lambda)B(\vec{e}^{(2)},\lambda)\left[1+A(\vec{e}^{(2)},\lambda)B(\vec{e}^{\prime(2)},\lambda)\right]
\end{aligned}$$

于是:
$$\begin{aligned}
&\left|P(\vec{e}^{(1)},\vec{e}^{(2)})-P(\vec{e}^{(1)},\vec{e}^{\prime(2)})\right|\\
&=\left|\int d\lambda\,\rho(\lambda)A(\vec{e}^{(1)},\lambda)B(\vec{e}^{(2)},\lambda)\underbrace{\left[1+A(\vec{e}^{(2)},\lambda)B(\vec{e}^{\prime(2)},\lambda)\right]}_{\geq 0}\right|\\
&\leqslant\int d\lambda\,\rho(\lambda)\left|A(\vec{e}^{(1)},\lambda)B(\vec{e}^{(2)},\lambda)\right|\left(1+A(\vec{e}^{(2)},\lambda)B(\vec{e}^{\prime(2)},\lambda)\right)\\
&=1+P(\vec{e}^{(2)},\vec{e}^{\prime(2)})
\end{aligned}$$

以上为经典局域隐变量理论的预言.

下面我们来看量子力学的预言:

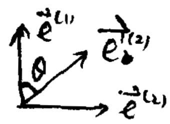
对于量子力学的自旋单重态 $|\psi^-\rangle=\frac{1}{\sqrt2}(|0\rangle|1\rangle-|1\rangle|0\rangle)$

$$(\vec{\sigma}^{(1)}+\vec{\sigma}^{(2)})|\psi^-\rangle=0\implies\vec{\sigma}^{(1)}|\psi^-\rangle=-\vec{\sigma}^{(2)}|\psi^-\rangle$$

于是:
$$\begin{aligned}
P(\vec{e}^{(1)},\vec{e}^{(2)})&=\langle\psi^-|(\vec{\sigma}^{(1)}\cdot\vec{e}^{(1)})(\vec{\sigma}^{(2)}\cdot\vec{e}^{(2)})|\psi^-\rangle\\
&=-\langle\psi^-|(\vec{\sigma}^{(1)}\cdot\vec{e}^{(1)})(\vec{\sigma}^{(1)}\cdot\vec{e}^{(2)})|\psi^-\rangle\\
&=-\sum_{ij}\langle\psi^-|\sigma_i^{(1)}e_i^{(1)}\sigma_j^{(1)}e_j^{(2)}|\psi^-\rangle\\
&=-\sum_{ij}e_ie_j\langle\psi^-|\sigma_i^{(1)}\sigma_j^{(1)}|\psi^-\rangle\\
&=-\sum_{ij}e_ie_j\delta_{ij}=-\vec{e}^{(1)}\cdot\vec{e}^{(2)}=-\cos(\vec{e}^{(1)},\vec{e}^{(2)})
\end{aligned}$$

那么，对于上面探讨的关联函数的关系，在量子力学情况，就应为：

$$\left|\mathrm{Cos}(\vec e^{(1)},\vec e^{(2)})-\mathrm{Cos}(\vec e^{(1)},\vec e'^{(2)})\right|\le 1-\mathrm{Cos}(\vec e'^{(2)},\vec e^{(2)})$$

现选择  $\cos\theta\le 1-\sin\theta$ （θ为锐角）

显然，上面的不等式是不成立的，于是量子力学的结果与局域隐变量的结果是相互矛盾的！

② CHSH型的不等式 （不依赖于系综选取）

$$P(\vec e^{(1)},\vec e^{(2)})-P(\vec e^{(1)},\vec e'^{(2)})$$

$$=\int d\lambda\,\rho(\lambda)\left[A(\vec e^{(1)},\lambda)B(\vec e^{(2)},\lambda)-A(\vec e^{(1)},\lambda)B(\vec e'^{(2)},\lambda)\right]$$

$$=\int d\lambda\,\rho(\lambda)\,A(\vec e^{(1)},\lambda)B(\vec e^{(2)},\lambda)\left[1\pm A(\vec e'^{(1)},\lambda)B(\vec e'^{(2)},\lambda)\right]$$

$$-\int d\lambda\,\rho(\lambda)\,A(\vec e^{(1)},\lambda)B(\vec e'^{(2)},\lambda)\left[1\pm A(\vec e'^{(1)},\lambda)B(\vec e^{(2)},\lambda)\right]$$

$\because\ A,B=\pm1$

$$\therefore\ \left|P(\vec e^{(1)},\vec e^{(2)})-P(\vec e^{(1)},\vec e'^{(2)})\right|$$

$$\le\int d\lambda\,\rho(\lambda)\left[1\pm A(\vec e'^{(1)},\lambda)B(\vec e'^{(2)},\lambda)\right]+\int d\lambda\,\rho(\lambda)\left[1\pm A(\vec e'^{(1)},\lambda)B(\vec e^{(2)},\lambda)\right]$$

$$\le 2\pm\left[P(\vec e'^{(1)},\vec e'^{(2)})+P(\vec e'^{(1)},\vec e^{(2)})\right]$$

~~※ CHSH不等式是最大违背~~ $\Longrightarrow \underbrace{\left|P(\vec e^{(1)},\vec e^{(2)})-P(\vec e^{(1)},\vec e'^{(2)})+P(\vec e'^{(1)},\vec e'^{(2)})+P(\vec e'^{(1)},\vec e^{(2)})\right|\le 2}_{\text{CHSH 不等式}}$

※ CHSH不等式的最大违背

$$\hat C=\hat a\hat b-\hat a\hat b'+\hat a'\hat b'+\hat a'\hat b$$

$\hat a,\hat a'\to$ 粒子1的算符，$\hat b,\hat b'$ 为粒子2的算符

$[a,b]=[a',b]=[a,b']=[a',b']=0\qquad a^2=b^2=a'^2=b'^2=I$

$$\hat C^2=4\cancel{-\hat b\hat b'}+\hat a\hat a'\hat b\hat b'\cancel{+\hat a\hat a'}\cancel{-\hat b'\hat b}\cancel{-\hat a\hat a'}-\hat a\hat a'\hat b'\hat b$$

$$+\hat a'\hat a\hat b'\hat b\cancel{-\hat a'\hat a}\cancel{+\hat b'\hat b}\cancel{+\hat a'\hat a}-\hat a'\hat a\hat b\hat b'\cancel{+\hat b\hat b'}$$

$$=4+aa'bb'-aa'b'b+a'ab'b-a'abb'$$

$$=4+aa'[b,b']+a'a[b',b]=4+[a,a'][b,b']$$

任意算符 $\hat M$ 的模定义：

$$\|\hat M\|=\sup_{|\psi\rangle}\frac{\|M|\psi\rangle\|}{\||\psi\rangle\|}\qquad \||\psi\rangle\|=\sqrt{\langle\psi|\psi\rangle}\qquad \|M\| \text{ 对应于}M\text{的最大本征值.}$$

算符模的性质

$\|MN\|\le\|M\|\cdot\|N\|.\qquad \|M+N\|\le\|M\|+\|N\|.$

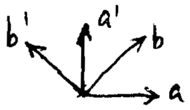
$$\|[M,N]\| \le \|MN\| + \|NM\| \le 2\|M\|\cdot\|N\|$$

$$\therefore \|C^2\| \le 4+4\|a\|\|a'\|\|b\|\|b'\| = 8 \qquad \therefore \|C\| \le 2\sqrt{2}.$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$(\vec{\sigma}_A + \vec{\sigma}_B)|\Psi^-\rangle = 0 \Longrightarrow \vec{\sigma}_A|\Psi^-\rangle = -\vec{\sigma}_B|\Psi^-\rangle$$

$$\langle\Psi^-|(\vec{n}\cdot\vec{\sigma}_A)(\vec{m}\cdot\vec{\sigma}_B)|\Psi^-\rangle = -\vec{m}\cdot\vec{n} = -\cos\theta.$$



$$\left|\langle\Psi^-|\hat{C}|\Psi^-\rangle\right| = 2\sqrt{2} \quad > 2.$$

3. 无不等式形式的Bell定理.

GHZ态: $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$.

对于量子力学

$$\sigma_x^1\sigma_y^2\sigma_y^3|GHZ\rangle = |GHZ\rangle$$
$$\sigma_y^1\sigma_x^2\sigma_y^3|GHZ\rangle = |GHZ\rangle$$
$$\sigma_y^1\sigma_y^2\sigma_x^3|GHZ\rangle = |GHZ\rangle$$
$$\sigma_x^1\sigma_x^2\sigma_x^3|GHZ\rangle = -|GHZ\rangle$$

四组力学量都对易, GHZ态为其共同本征态.

按照定域实在论的观点. 对于处于$|GHZ\rangle$ 测 2.3粒子的 $\sigma_y^2\sigma_y^3 = \begin{cases}1 \longrightarrow \sigma_x^1 = 1 \\ -1 \longrightarrow \sigma_x^1 = -1.\end{cases}$

$\sigma_y^1\sigma_y^2\sigma_y^3$

于是 σ_x^1为物理实在, 同样 σ_x^2、σ_x^3 也为物理实在。

$$\left.\begin{array}{l} m_{x1}\, m_{y2}\, m_{y3} = 1 \\ m_{y1}\, m_{x2}\, m_{y3} = 1 \\ m_{y1}\, m_{y2}\, m_{x3} = 1 \end{array}\right. \Longrightarrow m_{x1}m_{x2}m_{x3} = 1.$$

但是, 事实上 $\langle GHZ|\sigma_x^1\sigma_x^2\sigma_x^3|GHZ\rangle = -1$

GHZ定理: 对于GHZ态, 存在一组对易的可观测量, 对于这组力学量的测量, 量子力学将给出与定域实在论不相容的测量结果。

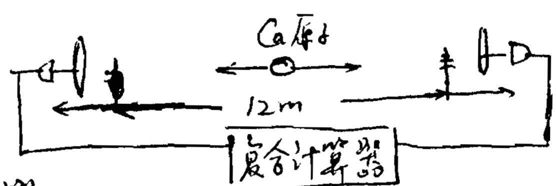
4. Bell不等式的实验研究.

80年代以前 ——

1982. CHSH型Bell不等式.

80-90年代. Ou, Shih.

a) 定域性漏洞. b) 探测效率漏洞.



§1.7 Von Neumann熵及其性质

1. Von Neumann熵

$$S(\rho) = -Tr(\rho\log_2\rho)$$

ρ 的谱分解：$\rho = \sum_a |\lambda_a|^2 |a\rangle\langle a|$ $\quad S(\rho) = -\sum_a |\lambda_a|^2 \log_2 |\lambda_a|^2$

2. Von Neumann熵的性质

① $S(\rho)=0$. 对 $\rho = |\psi\rangle\langle\psi|$

② $S(U\rho U^{-1}) = S(\rho)$ 在正交变换下 $S(\rho)$ 不变.

③ $S(\rho)$ 的最大值 $\quad S(\rho) \le \log_2 D \quad$ D为 ρ 的非零本征值的最大个数.

④ 如 ρ_{AB} 为纯态，则 $S(\rho_A) = S(\rho_B)$

⑤. 上凸性.

对任意的 $\lambda_1\lambda_2,\cdots\lambda_n \ge 0$. 且 $\lambda_1+\lambda_2+\cdots+\lambda_n = 1$.

$$S(\lambda_1\rho_1+\lambda_2\rho_2+\cdots+\lambda_n\rho_n) \ge \lambda_1 S(\rho_1)+\lambda_2 S(\rho_2)+\cdots+\lambda_n S(\rho_n)$$

⑥. 测量熵.

态 ρ，测量力学量 $A = \sum_y a_y |y\rangle\langle y|$，得到结果为 y 的几率 $P_y = \langle y|\rho|y\rangle$

对 $\{P_y\}$ 可定义 Shannon entropy

$H(Y) = -\sum_y P_y \log_2 P_y \quad$ 则 $H(Y) \ge S(\rho) \quad$ 等号仅当 $[A,\rho]=0$.

$H(Y)$ 代表测量值的混乱程度（混乱程度越大，获得的信息越少）

A 如果作测量，对 $[A,\rho]=0$.（这时测量所引起的不确定性最小）

⑦ 制备熵. （制备态的系综）

对于经典的随机变量 $\{p_i\}$，制备一个态系综. $\{p_i, |\psi_i\rangle\}$. $|\psi_i\rangle$ $|\psi_j\rangle$ 之间不一定正交

$H(x) = -\sum_i p_i \log_2 p_i \qquad \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$H(x) \ge S(\rho)$. 等号仅当 $|\psi_i\rangle$ 彼此正交.

意义：当我们混合非正交态时，我们不能够识别了（经典信息丢失）

⑧. 次加性. (subadditivity)

对于双粒子系统的态 ρ_{AB}. $\rho_A = Tr_B\rho_{AB}$

$S(\rho_{AB}) \le S(\rho_A)+S(\rho_B) \quad$ 等号仅当 $\rho_{AB} = \rho_A\otimes\rho_B$.

⑨ 强次加性.

对于 ρ_{ABC} $\quad S(\rho_{ABC})+S(\rho_B) \le S(\rho_{AB})+S(\rho_{BC})$

如. $\rho_{ABC} = \rho_{AC}\otimes|0\rangle_B\langle 0|$ $\quad S(\rho_B)=0$. 则退化为次加性.

⑩ 三角不等式

$$S(\rho_{AB}) \geq |S(\rho_A) - S(\rho_B)|$$

Von Neumann熵与 Shannon熵之间并不对应. ∵ $H(X,Y) \geq H(X), H(Y)$ 但 $S(X,Y)$不一定.

对于纠缠纯态. $S(\rho_{AB})=0$. $S(\rho_A)=S(\rho_B)>0$.

而 $H(X|Y) = H(X,Y) - H(Y) \geq 0$.

3. 熵与热力学的关系.

设系统为A, 环境为E, 初态 $\rho_{AE} = \rho_A \otimes \rho_E$.

Markov近似, 在任意时刻近似 $\rho_{AE} = \rho_A \otimes \rho_E$.

对于算符和的演化, 可以扩展空间, 使 U_{AE}成立.

$$\rho_{AE}' = U_{AE} \rho_{AE} U_{AE}^\dagger$$

$$\therefore S(\rho_{AE}') = S(\rho_{AE}) = S(\rho_A) + S(\rho_E)$$

但, 由次加性 $S(\rho_{AE}') \leq S(\rho_A') + S(\rho_E')$

$\therefore S(\rho_A) + S(\rho_E) \leq S(\rho_A') + S(\rho_E')$ 总熵总是在增加的.

§1.8. 量子信息论简介

§1.8.1 可提取的信息和 Holevo 极限定理 (用量子比特容载经典信息)

经典信源: $\{X, p_x\}$ $\quad H(X) = -\sum_x p_x \log_2 p_x$

量子信源. $\mathcal{E} = \{\rho_x, p_x\}$ 包含多少信息呢? $\rho = \sum_x p_x \rho_x$

定义 Holevo 信息. $\chi(\mathcal{E}) = S(\rho) - \sum_x p_x S(\rho_x)$

它与经典的互信息量有密切联系.

$\chi(\mathcal{E})$的特性.

(1) 正定性 $\chi(\mathcal{E}) \geq 0$. $\Longleftrightarrow$ $S(\rho)$的凹性.

(2) 单调性. 一个超算符的演化不能使 $\chi(\mathcal{E})$增加.

Lindblad - Uhlmann 定理: 对于一般的超算符的演化 $\hat{\$}$, 演化后的信源 $\mathcal{E}' = \{\hat{\$}(\rho_x), p_x\}$

$$\rho' = \sum_x p_x \hat{\$}(\rho_x) = \hat{\$}(\rho)$$

$$\chi(\mathcal{E}') = S(\rho') - \sum_x p_x S(\hat{\$}(\rho_x))$$

则 $\chi(\mathcal{E}') \leq \chi(\mathcal{E})$. 等号对应于幺正演化.

※ 定义可提取的信息：

$$\text{经典}\{p_x\} \Longrightarrow \boxed{\text{编码}} \xrightarrow{\ \mathcal{E}=\{p_x,\rho_x\}\ } \underset{\text{量子噪声信道}}{\overset{\hat{\$}}{=\!=\!=}} \ \mathcal{E}'=\{p_x,\hat{\$}(\rho_x)\} \longrightarrow \text{测量、提取，恢复到经典信息 } \{Y\}$$

A：（制备）量子信源 $\mathcal{E}=\{p_x,\rho_x\}$

B：（测量）POVM测量 $\{F_y\}$，$\sum_y F_y = I$

A制备 ρ_x，而B测量出 F_y 的联合概率 $\quad p(x,y)=p_x \operatorname{Tr}(\rho_x F_y)$

则 $p(x)=p_x$ $\qquad p(y)=\sum_x p(x,y)$

$H(X)=-\sum_x p(x)\log_2 p(x) \qquad H(Y)=-\sum_y p(y)\log_2 p(y)$

$H(X,Y)=-\sum_{xy} p(x,y)\log_2 p(x,y)$

A、B之间的互信息量 $\quad I(X,Y)=H(X)+H(Y)-H(X,Y)$

定义可提取的信息量 $\quad Acc(\mathcal{E})=\max\limits_{\{F_y\}} I(X,Y)$

Holevo极限定理：$\quad Acc(\mathcal{E}) \le \chi(\mathcal{E})$

证明：

引理：两子系A、B的量子互熵在 $\$_B$ 操作下非增。$S(A':B') \le S(A:B)$

Von Neumann互熵：$\quad S(A:B)=S(\rho_A)+S(\rho_B)-S(\rho_{AB})$

$\rho_{AB}'=\$_B\otimes I_A(\rho_{AB})=\operatorname{Tr}_C\left(U_{BC}\,\rho_{AB}\otimes|0\rangle_C\langle 0|\,U_{AB}^{+}\right)$

$$\left.\begin{aligned} S(\rho_A)&=S(\rho_A') \\ S(\rho_{BC})&=S(\rho_{BC}') \\ S(\rho_{ABC})&=S(\rho_{ABC}') \end{aligned}\right. \Longrightarrow \begin{aligned} S(\rho_A)+S(\rho_{BC})-S(\rho_{ABC}) &= S(\rho_A')+S(\rho_{BC}')-S(\rho_{ABC}') \\ \| \qquad\qquad & \\ S(\rho_A)+S(\rho_B)-S(\rho_{AB}) & \end{aligned}$$

根据强次加性：$\quad S(\rho_{ABC}')+S(\rho_B')\le S(\rho_{AB}')+S(\rho_{BC}')$

$$\Longrightarrow \quad S(\rho_A')+S(\rho_B')-S(\rho_{AB}')\le S(\rho_A')+S(\rho_{BC}')-S(\rho_{ABC}')$$

于是，有 $\quad \underline{S(\rho_A)+S(\rho_B)-S(\rho_{AB}) \ge S(\rho_A')+S(\rho_B')-S(\rho_{AB}')}$（去掉子系统不能增加信息）

证明：$\quad \rho^{PQM}=\sum_x p_x|x\rangle\langle x|\otimes\rho_x\otimes|0\rangle\langle 0|$

正交$\{|x\rangle\}$对应经典信号，Alice以 p_x 的概率产生 $|x\rangle$，于是对应地制备一个 ρ_x。

现在Bob收到 ρ_x 的子系，再加上自己手头上的 $|0\rangle$，他想对 ρ_x 部分实施一个广义测量 $\{E_y\}$

于是，我们可以定义一个作用在QM上的超算符，使之恰好对 $\{E_y\}$ 测量。

我们定义QM上的超算符为 $\$_{QM}$. 其Kraus算子为. $\{\sqrt{E_y}\otimes U_y\}$

其中 $U_y|y'\rangle = |y'+y\rangle$

$\because \sum_y \sqrt{E_y}\otimes U_y^\dagger \cdot \sqrt{E_y}\otimes U_y = \sum_y E_y \otimes I_M = I_Q\otimes I_M$. $\therefore$ $\$_{QM}$的算符和表示为.

$$\rho'_{QM} = \sum_y \sqrt{E_y}\otimes U_y\, \rho_{QM} \sqrt{E_y}\otimes U_y^\dagger$$

$$\rho_{QM} = \rho\otimes|0\rangle\langle 0|$$

$$\mathrm{Prob}(y) = \mathrm{Tr}_{QM}\, \sqrt{E_y}\otimes U_y\, \rho\otimes|0\rangle\langle 0|\sqrt{E_y}\otimes U^\dagger$$

$$= \mathrm{Tr}_{QM}\, \sqrt{E_y}\rho\sqrt{E_y}\otimes|y\rangle\langle y| = \mathrm{Tr}_Q \sqrt{E_y}\rho\sqrt{E_y} = \mathrm{Tr}_Q\, \rho E_y$$

该超算符等价于 $\{E_y\}$ 对 Q 系的测量.

于是. $\rho^{P'Q'M'} = \sum_{xy} p_x |x\rangle\langle x| \otimes \sqrt{E_y}\rho_x\sqrt{E_y}\otimes|y\rangle\langle y|$

$$\rho^{P'M'} = \mathrm{Tr}_Q\, \rho^{P'Q'M'} = \sum_{xy} p_x(\mathrm{Tr}\,\rho_x E_y)\,|x\rangle\langle x|\otimes|y\rangle\langle y| = \sum_{xy} p(xy)\,|x\rangle\langle x|\otimes|y\rangle\langle y|$$

$$S(P':M') = I(P':M') \le \underbrace{S(P':Q',M')}_{\text{根据强次加性}} \le \underbrace{S(P:Q,M)}_{\text{引理}} = S(P:Q)$$

于是: $\max I(P':M') \le S(P:Q) = \underset{\underset{H(\{p_x\})}{\parallel}}{S(\rho^P)} + \underset{\underset{S(\rho)}{\parallel}}{S(\rho^Q)} - S(\rho^{PQ})$

$$\rho^{PQ} = \sum_x p_x|x\rangle\langle x|\otimes\rho_x = \sum_{xk} p_x \delta_k\, |x\rangle\langle x|\otimes|k\rangle_x\langle k|$$

$$S(\rho^{PQ}) = -\sum_{xk} p_x\delta_k \log_2 p_x\delta_k$$

$$= H(x) - \sum_{xk} p_x\delta_k\log_2\delta_k$$

$$= H(x) + \sum_x p_x S(\rho_x)$$

$$\therefore \quad \max I(P':M') \le H(x) + S(\rho) - H(x) - \sum_x p_x S(\rho_x) = S(\rho) - \sum_x p_x S(\rho_x)$$

应用Holevo定理的一个例子:

纯态信源. $\{|\psi_x\rangle, p_x\}$.

$\chi(\varepsilon) = S(\rho)$.

$Acc(\varepsilon) \le S(\rho)$.

$\therefore$ 一个qubit不能容载超过一个bit的经典信息.

§1.8.2. 量子信源编码

量子信源 $\varepsilon=\{p_x, |\psi_x\rangle\}$ $\rho=\sum_x p_x|\psi_x\rangle\langle\psi_x|$

用尽可能少的量子比特作为信息的载体。

首先考虑扩展信源，发送一群信号 $\rho^n=\rho\otimes\rho\otimes\cdots\otimes\rho$，最少可用多少qubit表示出来？要求不失真，保真度→1.

Schumacher的无噪信道的编码理论（对信源进行压缩）

量子信源的n次扩展信源，$n\to\infty$时，可用 $nS(\rho)$个量子比特表示信源符号序列，则保真度→1。

△ 关于典型序列和典型子空间

典型序列：信源$X=\{x_i, p_i\}$，对于其N次扩展信源X^N中的符号序列，如果该序列很可能出现，我们称其为典型序列；反之，我们称其为非典型序列。

当n非常大的时候：$p(x_1,x_2,\ldots x_n)=p(x_1)p(x_2)\cdots p(x_n)\approx p^{np}(1-p)^{(1-p)n}$

$$-\log_2 p(x_1,x_2,\ldots x_n)\approx -np\log_2 p-n(1-p)\log(1-p)=nH(X)$$

$$p(x_1,x_2,\ldots x_n)\approx 2^{-nH(X)}$$

如果我们将$2^{-nH(X)}$作为一个典型序列出现的概率，那么，至多有$2^{nH(X)}$个典型序列。于是，这些典型序列可以用$nH(X)$个bit进行编码。（$n\to\infty$时，几乎都是典型序列）

如果序列的概率$p(x_1,x_2,\cdots x_n)$满足：$2^{-n(H(X)+\varepsilon)}\le p(x_1,x_2,\cdots x_n)\le 2^{-n(H(X)-\varepsilon)}$，则所有满足以上约束的序列的集合，我们称为 ε 典型序列。

关于典型序列的一些结论：

(1). 给定$\varepsilon>0$，则对于任意的$\delta>0$，只要n足够长，所有ε典型序列的概率之和至少为$1-\delta$

(2). 对于任意给定的$\varepsilon>0$和$\delta>0$，对于充分大的n，ε典型序列的数目$|T(n,\varepsilon)|$满足

$$(1-\delta)2^{n(H(X)-\varepsilon)}\le|T(n,\varepsilon)|\le 2^{n(H(X)+\varepsilon)}$$

(3). 让$S(n)$为2^{nR}个序列的集合，$R<H(X)$。那么，对于任意的$\delta>0$，对于充分大的n

$$\sum_{x\in S(n)}p(x)\le\delta.$$

（假设$S(n)$中所有序列都是典型序列，一个典型序列的概率为$2^{-nH(X)}$，则$2^{n(R-H(X))}$为全部概率，当$n\to\infty$，$2^{n(R-H(X))}\to 0$.）

典型空间：对应于量子情况 $\rho=\sum_x p_x|x\rangle\langle x|$ （本征分解） $S(\rho)=-\sum_x p_x\log_2 p_x = H(\{p_x\})$.

定义ε典型态 $|x_1\rangle|x_2\rangle,\cdots|x_n\rangle$ 对应ε典型序列 $x_1,x_2,\cdots x_n$.

于是，我们定义 $T(n,\varepsilon)$ 为ε典型子空间，其空间投影子为 $P(n,\varepsilon)$.

$$P(n,\varepsilon)=\sum_{x\in\text{典型序列}}|x_1\rangle\langle x_1|\otimes|x_2\rangle\langle x_2|\otimes\cdots\otimes|x_n\rangle\langle x_n|$$

则典型空间有以下结论：

(1) 给定 $\varepsilon>0$，则对于任意的 $\delta>0$，对于充分大的 n，有 $Tr(P(n,\varepsilon)\rho^{\otimes n})\geq 1-\delta$

(2) 对于任意给定的 $\varepsilon>0$，$\delta>0$，对于充分大的 n，则典型空间 $T(n,\varepsilon)$ 的维数满足：

$$(1-\delta)2^{n(S(\rho)-\varepsilon)}\leq|T(n,\varepsilon)|\leq 2^{n(S(\rho)+\varepsilon)}$$

(3) 记 $S(n)$ 为投影到 $H^{\otimes n}$ 的子空间的投影子，维数至多为 2^{nR} 维，$R<S(\rho)$。那么，对于任意 $\delta>0$，对于充分大的 n，$Tr(S(n)\rho^{\otimes n})\leq\delta$

证明 Schumacher 的理论：

给定 $H^{\otimes n}=\Lambda\oplus\Lambda^\perp$ 　Λ 为典型空间. E 为 Λ 的投影子.

思路：将典型空间中的量子态真实地发送。先将 $\rho^{\otimes n}$ 向 Λ 和 $\Lambda^\perp$ 投影，则投影到 Λ 的概率为 $P_\Lambda=Tr(\rho^{\otimes n}E)>1-\delta$，然后，我们对 Λ 中的态进行编码、发送；而投影到 $\Lambda^\perp$ 中的部分 $P_{\Lambda^\perp}<\delta$ 可忽略.

Λ 中的编码变换：U_Λ（幺正的）

$$U_\Lambda|\psi_{typical}\rangle=\underbrace{|\psi_{comp}\rangle}_{n(S(\rho)+\varepsilon)\uparrow}|0_{rest}\rangle \quad |0_{rest}\rangle\to|0\rangle|0\rangle\cdots|0\rangle$$

Alice 将 $|\psi_{comp}\rangle$ 发送给 Bob.

Bob $U_\Lambda^{-1}|\psi_{comp}\rangle|0_{rest}\rangle\longrightarrow|\psi_{typical}\rangle$

对于实际的操作：

Alice 先作幺正变换 U，再测量 rest 部分的比特，~~[illegible]~~（U 为 U_Λ 的扩展幺正变换）.

$\Updownarrow$

先投影 Λ. $\Lambda^\perp$，再对 Λ 中的部分做 U_Λ

∵ 仅有典型空间的状态，经 U 变换后 rest 部分为0；对于 $\Lambda^\perp$ 中的态，经 U 后，rest 为非0.

假定，待传的某个态 $|\psi_i\rangle=|\psi_{x_1}^{(i)}\rangle|\psi_{x_2}^{(i)}\rangle\cdots|\psi_{x_n}^{(i)}\rangle$.

Alice 做幺正变换，再测量 rest 部分，发送给 Bob. Bob 借助辅助比特，做 U^{-1}，恢复量子态.

$$|\psi_i\rangle\langle\psi_i|\longrightarrow\rho_i'=E|\psi_i\rangle\langle\psi_i|E+\rho_{i,Junk}\langle\psi_i|(I-E)|\psi_i\rangle$$

则平均保真度：（保源 $\{p_i, |\varphi_i\rangle\} \longrightarrow \{p_i, \rho_i'\}$）

$$F = \sum_i p_i \langle\varphi_i|\rho_i'|\varphi_i\rangle$$

$$= \sum_i p_i \langle\varphi_i|E|\varphi_i\rangle\langle\varphi_i|E|\varphi_i\rangle + \sum_i p_i \langle\varphi_i|\rho_{i,junk}|\varphi_i\rangle\langle\varphi_i|I-E|\varphi_i\rangle$$

$$\geq \sum_i p_i \| E|\varphi_i\rangle \|^4 \geq \sum_i p_i (2\langle\varphi_i|E|\varphi_i\rangle - 1) = 2Tr\,\rho^{\otimes n}E - 1 > 2(1-\delta) - 1 = 1-2\delta.$$

假定 ρ_{comp} 被压缩到 $n(S-\varepsilon)$ 个 qubit 里，其 Hilbert 空间为 Λ' $\dim\Lambda' =$ [redacted] $2^{n(S-\varepsilon)}$

输入为 $|\varphi_i\rangle$

Bob 的重建态为 $\rho_i'' = \sum_{a_i} \lambda_{a_i}|a_i\rangle\langle a_i|$

$$F_i = \langle\varphi_i|\rho_i''|\varphi_i\rangle$$

$$= \sum_{a_i}\lambda_{a_i}\langle\varphi_i|a_i\rangle\langle a_i|\varphi_i\rangle$$

$$\leq \sum_{a_i}\langle\varphi_i|a_i\rangle\langle a_i|\varphi_i\rangle \leq \langle\varphi_i|E'|\varphi_i\rangle$$

$$F = \sum_i p_i F_i \leq \sum_i p_i\langle\varphi_i|E'|\varphi_i\rangle = Tr(\rho^{\otimes n}E')$$

由典型空间的结论 当 $n\to\infty$ 时，[redacted] $F\to 0$

$\therefore$ $S(\rho)$ 个 qubit 是量子信号的最佳压缩

（量子传输与经典不同的是，Bob 可以拥有这个量子态，但他不能读（测量））

§1.8.3. 噪声量子信道的经典信息容量

（没有讨论量子信道传送量子信息和量子纠缠）

Holevo – Schumacher – Westmoreland 定理：

$\mathcal{E}$ 为保迹的量子操作，定义 $C(\mathcal{E}) = \max\limits_{\{p_j,\rho_j\}} \left[S\left(\mathcal{E}\left(\sum_j p_j\rho_j\right)\right) - \sum_j p_j S(\mathcal{E}(\rho_j))\right]$

这里，最大值求遍所有可能输入态的所有的系综。

$C(\mathcal{E})$ 称为信道 $\mathcal{E}$ 的直积态容量。

※ 信息论，经典与量子的对比

	经典	量子
熵	Shannon 熵 $H(X) = -\sum_x p_x\log_2 p_x$	Von Neumann 熵 $S(\rho) = -Tr\,\rho\log_2\rho$
可提取信息	可把字写出可以识别的	Holevo 极限 $\chi(\rho)$. $Acc \leq \chi(\rho)$. $\chi(\rho) = S(\rho) - \sum_x p_x S(\rho_x)$
无噪信道编码	Shannon I. $n_{bit} = H(X)$	Schumacher 定理. $n_{qubit} = S(\sum_x p_x\rho_x)$
噪声信道的经典信道容量	Shannon II. $C = \max\limits_{\{p_x\}} I(X,Y)$	HSW定理. $C(\mathcal{E}) = \max\limits_{\{p_x,\rho_x\}}\left[S\left(\mathcal{E}\left(\sum_x p_x\rho_x\right)\right) - \sum_x p_x S(\mathcal{E}(\rho_x))\right]$ 噪声信道的量子信道容量尚未完全解决

§1.9. 量子纠缠简介.

§1.9.1. 量子纠缠的定义和特性.

量子纠缠的历史，及其在量子信息中的重要性.

EPR → Bell不等式 → 量子密钥 (92 Ekert) → 量子 teleportation. dense coding

→ 量子纠缠作为 source → 通讯 / → 计算　导致纠缠的分类、定量化的研究.

量子编码、多方计算中通讯复杂度的降低、利用纠缠做量子计算 (少体)
(多体) → one way 量子计算.

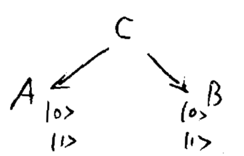
→ 多体纠缠与多体物理的联系. (量子相变中的纠缠)

△ 什么是纠缠态:

① 对于纯态，纠缠态是指不能表示为两个(多个)子系统直积形式的态.

② 对于混和态 ρ: 区分量子纠缠与经典关联

$$\rho_{AB} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$$



$\rho_{AB} = \sum_x p_x \rho_{xA} \otimes \rho_{xB}$ 表示一般的具有经典关联性质的态.

一个 center，选择一个经典的随机过程，再利用经典通讯，可以通过局域的态制备来实现该量子系统。 (所谓经典关联是指可以用 LOCC 来建立的关联)

若 ρ_{AB} 不能表示为 $\sum_x p_x \rho_{xA} \otimes \rho_{xB}$ 的形式，则称 ρ_{AB} 为量子纠缠态；否则，则称为可分量子态.

③ 纠缠的特性. 在 LOCC 下 纠缠不能增加.

(i) LO (Local Operations) (包括局域的 POVM 及广义演化)，纠缠的总量不能增加。
如局域操作为幺正演化，则纠缠不变

(ii) 通过经典通信 (Classical Communications) 纠缠不能增加.

§1.9.2 纠缠的度量.

△ 度量纠缠的必要性和重要性:

当两地分享一定的纠缠的时候，纠缠的所有者可以通过对纠缠态做局域操作并辅以经典通讯的手段来进行像量子通信、量子计算的功能，这都只要以消耗两地共享的纠缠态为代价的。所以对纠缠进行量化非常必要。

最初在研究纠缠定量化的时候，物理上的动机在于纠缠分类、以及评估实验中产生的纠缠量。但在随后的研究中发展起来的一些数学工具对于研究量子信道容量的加性，理解量子相变中的关联行为，限定容错量子计算的阈值等非常重要。（可参考 quant-ph/0504163 中的 references）

Δ. 定量化纠缠的基本原则 (bipartite)

① $E(\rho)$ 是一个从密度矩阵到正实数的映射.

$$\rho \to E(\rho) \in R^+$$

$d\times d$ 维系统的最大纠缠态为 $|\psi^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle_A|i\rangle_B$ $\quad E(|\psi_d^+\rangle)=\log d$

② if ρ 为可分，则 $E(\rho)=0$.

③ 在 LOCC 下，平均纠缠不能增加.

$$E(\rho) \geq \sum_i p_i E\left(\frac{A_i\rho A_i^\dagger}{\mathrm{tr}A_i\rho A_i^\dagger}\right) \qquad p_i=\mathrm{tr}A_i\rho A_i^\dagger$$

A_i 为描述 LOCC 运算的 Kraus 算符.

④ 对于纯态 $|\psi\rangle_{AB}$，纠缠度退化为子系约化密度矩阵的 Von Neumann 熵

$$E(|\psi\rangle_{AB}\langle\psi|) = (S\circ \mathrm{tr}_B)(|\psi\rangle_{AB}\langle\psi|)$$

由以上原则、两子系复合系统的纯态的纠缠度量已经有了.

$$|\psi\rangle_{AB} = \sum_{i=1}^N a_i|i\rangle_A|i\rangle_B \qquad \rho_A=\sum_{i=1}^N |a_i|^2|i\rangle_A\langle i| \qquad S(\rho_A)=S(\rho_B)=E(|\psi\rangle_{AB}) = -\sum_{i=1}^N |a_i|^2\log_2|a_i|^2$$

对于 Bell 态 $|\psi^\pm\rangle = (|01\rangle\pm|10\rangle)/\sqrt{2}$ $\quad |\Phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$ $\quad E=1$

称为 1 ebit.

Δ. 两子系复合系统混态的纠缠度量.

① 生成纠缠 (entanglement of formation)

两粒子态 ρ_{AB} 的生成纠缠定义为通过 LOCC 过程，从制备 ρ_{AB} 所消耗的 Bell 基的平均最小数目.

A.B 首先共享 Bell 基，他们要制备出 ρ_{AB}，$\rho_{AB}^{\otimes n}$ 如需要 k 个 Bell 基，则生成纠缠 $E_F=\lim_{n\to\infty}\frac{k_{min}}{n}$

② 蒸馏纠缠 (entanglement of distillation)

ρ_{AB} 的蒸馏纠缠 E_D 定义为通过 LOCC 过程可以从 ρ_{AB} 中提取的最大的 Bell 基数目。有 n 个 ρ_{AB}，可以提取出 k' 个 Bell 基，则蒸馏纠缠为 $E_D=\lim_{n\to\infty}\frac{k'_{max}}{n}$

为什么要用渐近性定义？

度量的目标是在某种意义下 [redacted] 建立等价性。态之间的转换，由 LOCC 操作来完成。但是，在有限态情况下，无法从一个态确定地转化到另一个态（尝试无限也不行）。但是，可以借鉴香农熵的定义，

在渐近意义下 $\frac{\varepsilon}{n}\to 0$.

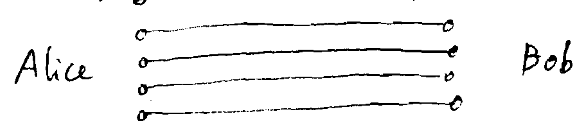
纠缠纯化：通过LOCC过程，从部分纠缠态中提取最大纠缠态（Bell基）的过程称为纠缠纯化。如部分纠缠态为纯态，则此过程也称为纠缠浓缩。

△ 对于纯态 $|\psi\rangle_{AB}$　$E_F = E_D = S(\rho_A)$.

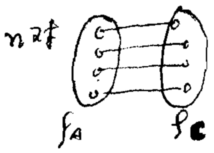
下面来验证上述论断

※ 首先考虑生成纠缠（Schumacher压缩和Teleportation）

A、B 分享 $k=n(S(\rho_A)+\delta)$ 个Bell态.



i) Alice局域制备 $|\psi\rangle_{AC}^{\otimes n}$



$S(\rho_C) = S(\rho_A)$

ii) 按照Schumacher压缩理论，C的n份拷贝处于空间$(H_C^{\otimes n})$，其典型子空间的维数小于$2^{n(S(\rho)+\delta)}$，于是，我们可以实施幺正变换，将典型子空间的状态压缩到 $n(S(\rho)+\delta)$ 个qubit的空间 $\tilde{H}_C$.

（典型空间的特性：解码出的$(\rho_C)^{\otimes n}$与$(\rho_C)^{\otimes n}$之间的保真度$\to 1$.

iii) 现在Alice和Bob用$n(S(\rho_A)+\delta)$对Bell态，将$\tilde{H}_C$中的态teleport到空间$\tilde{H}_B$中去，teleportation的保真度原则上可以达到1。在A、B共享Bell态的情形，teleportation仅需局域操作和经典通讯即可完成.

iv) 最后，Bob作一个解码，于是AB共享 ρ_{AB}^{out}，在渐近意义下，ρ_{out}与 $|\psi_{AB}\rangle^{\otimes n}$的保真度$\to 1$.

※ 浓缩纠缠　（这里，我们大致说明典型空间的趋势$\to 1$）

例　$|\psi(\theta)\rangle_{AB} = \cos\theta|00\rangle + \sin\theta|11\rangle$

$$|\psi(\theta)\rangle_{AB}^{\otimes n} = (\cos\theta|00\rangle + \sin\theta|11\rangle)^{\otimes n}$$

A子系　$\rho_A^{\otimes n} = (\cos^2\theta|0\rangle\langle 0| + \sin^2\theta|1\rangle\langle 1|)^{\otimes n}$

我们可以以$|1\rangle$的数目划分子空间　$H^{\otimes n} = H_0^{|1\rangle} \oplus H_1^{|1\rangle} \oplus \cdots \oplus H_n^{|1\rangle}$

则 $P(m) = \binom{n}{m}(\sin^2\theta)^m(\cos^2\theta)^{n-m}$　为 $\rho_A^{\otimes n}$ 投影到 $H_m^{|1\rangle}$ 中的几率.

随着n的增加，几率分布$P(m)$越来越锐，几率峰值趋近于 $m/n = \sin^2\theta \Rightarrow m = n\sin^2\theta$.

$$P(m=n\sin^2\theta) = \binom{n}{m}(\cos^2\theta)^{n-m}(\sin^2\theta)^m = \frac{n!}{m!(n-m)!}(\cos^2\theta)^{n-m}(\sin^2\theta)^m$$

String公式
$n! \sim n^n e^{-n}$
$(n\to\infty)$

$$\approx \frac{n^n e^{-n}(\cos^2\theta)^{n\cos^2\theta}(\sin^2\theta)^{n\sin^2\theta}}{(n\sin^2\theta)^{n\sin^2\theta}e^{-n\sin^2\theta}(n\cos^2\theta)^{n\cos^2\theta}e^{-n\cos^2\theta}} = 1.$$

投影到 $H_{n\sin^2\theta}^{|1\rangle}$ 中的项数.　$\binom{n}{m} = \frac{n!}{m!(n-m)!} \approx \frac{n^n e^{-n}}{(n\sin^2\theta)^{n\sin^2\theta}(n\cos^2\theta)^{n\cos^2\theta}e^{-n}}$

$$= \frac{1}{(\sin^2\theta)^{n\sin^2\theta}(\cos^2\theta)^{n\cos^2\theta}} = 2^{nS(\rho_A)}$$

确切地 $n\to\infty$ $(1-\delta)2^{n(S(\rho)-\epsilon)} < \binom{n}{m} < 2^{n(S(\rho)+\epsilon)}$

$\epsilon\to 0,\ \delta\to 0.\quad 2^{k'}\sim\binom{n}{m}.\qquad E_D=\lim_{n\to\infty}\frac{k'}{n}=S(\rho_A)$

所以，对于上例的浓缩过程，我们只需向典型子空间投影，再经过适当的幺正变换可实现浓缩的目的。

对于混和态，E_F，E_D不一定相等，$E_F\geq E_D$.

※ 任意2-qubit的生成纠缠 $E_F(\rho)=\min_{\{\rho=\sum p_i\rho_i\}} p_iE(\rho_i)$ (PRL 80, 2245, 1998)

Concurrence (共生)

$\tilde{\rho}=(\sigma_y\otimes\sigma_y)\rho^*(\sigma_y\otimes\sigma_y)\qquad R=\sqrt{\sqrt{\rho}\,\tilde{\rho}\sqrt{\rho}}$

或称 $\rho\tilde{\rho}$ 的平方根本征值 $\lambda_1,\lambda_2,\lambda_3,\lambda_4$.

Concurrence: $C(\rho)=\max\{0,\lambda_1-\lambda_2-\lambda_3-\lambda_4\}$ $\lambda_1\geq\lambda_2\geq\lambda_3\geq\lambda_4$ 为R的本征态.

则 $E_F(\rho)=h\left(\frac{1-\sqrt{1-C(\rho)^2}}{2}\right)\qquad h(x)=-x\log_2x-(1-x)\log_2(1-x)$

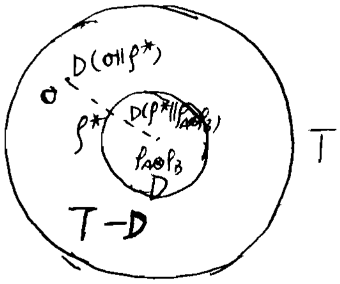
③ 基于距离的纠缠度定义

设两子系量子系统所有量子态的集合为T，T分成两个不相交的子集：非纠缠态的子集D，和所有纠缠态的子集E=T−D，其中T和D都是凸集：

$\forall\rho_1,\rho_2\in T(D)\Longrightarrow\lambda\rho_1+(1-\lambda)\rho_2\in T(D)$

密度矩阵σ的纠缠度定义为：

$$E(\sigma)=\min_{\rho\in D}D(\sigma\|\rho)$$



基于距离的纠缠度示意图

- Von Neumann 相对熵

$S(\sigma\|\rho)=\mathrm{Tr}(\sigma\log_2\sigma/\rho)$

在纯态限制下 $E(\sigma)=\min_{\rho\in D}S(\sigma\|\rho)$

退化为Von Neumann熵.

④ Negativity:

$\rho=\sum_{ij,kl}\rho_{ij,kl}|i\rangle\langle j|\otimes|k\rangle\langle l|$

$\rho^{T_B}=\sum_{ij,kl}\rho_{ij,kl}|i\rangle\langle j|\otimes|l\rangle\langle k|$ 它的谱是不依赖于基矢的选择的.

如ρ为可分，则 ρ^{T_B} 仍为密度矩阵。$\rho^{T_B}\geq 0$ 为ρ为可分的必要条件.

可以证明 $\rho^{T_B}\geq 0$ 也是 $E_D(\rho)=0$ 的充分条件.

$N(\rho)=\frac{\|\rho^{T_B}\|-1}{2}.\qquad \|X\|=\mathrm{Tr}\sqrt{X^\dagger X}.$

Logarithmic Negativity:

$E_N(\rho)=\log_2\|\rho^{T_B}\|$

△ 多体的纠缠度量：（尚未完成）

~~进展~~ 若干进展：

① 最小纠缠生成集：Bennett 等人定义了一组态 $G=\{\psi_1,\psi_2,\ldots,\psi_k\}$ 为最小可逆的纠缠生成集。他们设想任何一个多子系系统的纯纠缠态可由这组生成集以渐近可逆的方式生成。每个元素着一个纠缠度.

② Entanglement of Assistance (3 party), Localizable entanglement (multi party)
(DiVincenzo, et. al 2001)　　(F. Verstraete, et al. 2004)

一个问题：在多粒子复合体系中，我们怎样来标记两点的纠缠？

如 $|\psi\rangle=\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)$　我们看任意的两点约化密度矩阵 $\rho_{12}=\frac{1}{2}|00\rangle\langle 00|+\frac{1}{2}|11\rangle\langle 11|$.

按照两体的纠缠度的计算，它是可分的.

但是，对这样一个多体系统，我们可以通过对除这两点之外的其它系统作LOCC操作，进而最大化两点的纠缠。在最佳的LOCC下，两点所获得的最大纠缠称为 Localizable entanglement.

如 $\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$　通过测 $\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$ 可以将两体的态制备成最大纠缠态.

Localizable entanglement 显示同凝聚态系统的关联函数有一定的关系。

③ Tangle.（纠缠的一夫一妻制）.（Wootters et. al. 2000）.

例如一个三体的纯态.（A.B.C）. 如 A与B很纠缠，则C与A或B只会有很弱的纠缠，

如 A.B为Bell态，则C不可能同A.B纠缠。

用单点的性质来标记空间两体纠缠.（~~一个……~~ 一个 $2\times n$ 体系的 ρ.

$$\tau(\rho)=\{\inf\sum_i p_i C^2(|\psi_i\rangle\langle\psi_i|)\}$$

对于3qubit纯态，定义 τ_3.（它是一个局域幺正不变量，并且独立于A.B.C的选择）

$$\tau_3=\tau(A:BC)-\tau(A:B)-\tau(A:C)\quad\text{（可以描述三体纠缠）}$$

另，已证明. $\tau(A:BCD\cdots)\geq\tau(A:B)+\tau(A:C)+\tau(A:D)+\cdots$

§1.9.3. 纠缠态的判别及其分类.

△. 判别两子系系统为可分的必要条件 — Peres-Horodecki 判据 (1996).

对于二粒子系统的量子态 ρ_{AB}，如 ρ_{AB} 为可分态（非纠缠态），则其部分转置算符 σ_{AB} 为正定。

$$\sigma_{mn,\mu\nu}=\langle m_A|\langle\nu_B|\rho|n\rangle_A|\mu\rangle_B=\rho_{mn,\nu\mu}=\rho^{T_B}_{mn,\mu\nu}.$$

证明：$\rho_{AB}=\sum_{ijkl}\rho_{ij;kl}\,|i\rangle_A\langle j|\otimes|k\rangle\langle l|$

$\rho_{AB}^{T_B}=\sigma_{AB}=\sum_{ijkl}\rho_{ij;lk}\,|i\rangle\langle j|\otimes|k\rangle\langle l|$.

如 ρ_{AB} 为可分，则 $\rho_{AB}=\sum_x p_x\,\rho_{Ax}\otimes\rho_{Bx}$.

$$\sigma_{AB} = \rho_{AB}^{T_B} = \sum_x p_x \rho_{Ax}\otimes\rho_{Bx}^{T}$$

$$\rho_{Bx} = U\,\mathrm{diag}\{\lambda_1,\lambda_2,\cdots\lambda_n\}U^+$$

$$\rho_{Bx}^{T_B} = U^*\,\mathrm{diag}\{\lambda_1,\lambda_2,\cdots\lambda_n\}(U^*)^+$$

∴ σ_{AB}仍然是密度矩阵，显然是正定的.

部分转置为正定，我们记为PPT.

Horodecki et.al. 随后证明了：对于2×2和2×3系统，P-H判据为可分性判定的充要条件.

$PPT \Longrightarrow E_D(\rho)=0$

但是，这时 $E_F(\rho)$可以不为0，Horodecki et.al.将这种态称为"束缚纠缠态".

但随后，人们发现即使为NPT，也可以有束缚纠缠态.

$$\text{纠缠态}\begin{cases}\text{束缚纠缠态} & (PPT.\ NPT)\\ \text{可蒸馏的纠缠态} & (NPT)\end{cases}$$

束缚纠缠态：展现了信息的不可逆过程，可以类比热力学的熵增现象.

4. Entanglement Witness (纠缠目击) 算符W. 满足. $W=W^+$

$\forall \rho\in D$. $\mathrm{Tr}\,W\rho \geq 0$ 但. $\sigma\notin D$. $\mathrm{Tr}\,W\sigma<0$.

则W为σ的纠缠目击算符.