量子信息与量子密码

Quantum Information & Quantum Cryptology

[第2次课]数学、物理预备知识

授课教师：杨理

授课时间：2022年3月14日

内容概要

§3.1 线性代数

一、矩阵的分解；二、矩阵的直积；三、矩阵的酉对角化；四、两矩阵同时酉对角化；五、教材上的其它内容

§3.2 量子力学基础

一、基本假设；二、基本概念；三、量子测量；四、密度算符；五、复合体系；六、Bell定理

一、矩阵的分解

二、矩阵的直积

三、矩阵的酉对角化

四、两矩阵同时酉对角化

五、教材上的其它内容

一、矩阵的分解

n 阶Hermitian阵 A 可以酉对角化：$A = U^{\dagger} D U$ 。

问题：

1. 若 A 为一般 矩阵，有无类似的定理？
2. 什么样的两个矩阵可以同时对角化？

任意矩阵的奇异值分解

- **定理（1939）** 设 A 为一 (m,n) 矩阵，$Rank\ A = r$，总可以找到一个 n 阶酉阵 U 和一个 m 阶酉阵 V 以及对角阵 $S_0 = \begin{pmatrix} S_1 & \ddots & 0 \\ 0 & & S_r \end{pmatrix}$，$S_1 \geq S_2 \geq \cdots \geq S_r > 0$，使表达式 $A = VSU$ 成立，其中 $S = \begin{pmatrix} S_0 & 0 \\ 0 & 0 \end{pmatrix}$。

- 此即为矩阵 A 的奇异值分解。数 $S_1, \cdots, S_r (> 0)$ 称为矩阵 A 的奇异值（即是 $A^\dagger A$ 的特征值的算术根）。

极式分解

- **定理**（极式分解） 令A是向量空间V上的线性算子，则存在酉算子U和半正定算子J和K使得

$$A = UJ = KU$$

其中J和K是唯一满足这些方程的半正定算子，定义为$J \equiv \sqrt{A^+ A}$和$K \equiv \sqrt{AA^+}$。如果A可逆，U是唯一的。

- $A = UJ$为A的左极式分解，$A = KU$为A的右极式分解。

方阵的奇异值分解

- **推论（奇异值分解）** 令 A 是一方阵，则必存在酉矩阵 U、V 和一个非负对角阵 D 使得

$$A = UDV$$

D 的对角元称为A 的奇异值。

注意：奇异值分解不只适用于方阵。

Schmidt 分解定理

- 应用：证明 Schmidt 分解定理：

$$
\begin{aligned}
|\Psi\rangle &= \sum_{j,k} a_{jk} |j\rangle |k\rangle \\
&= \sum_{i,j,k} v_{ji} s_i u_{ik} |j\rangle |k\rangle \\
&= \sum_{i} s_i |A_i\rangle |B_i\rangle
\end{aligned}
$$

其中 $|A_i\rangle = \sum_j v_{ji} |j\rangle$， $|B_i\rangle = \sum_k u_{ik} |k\rangle$ ，此正是 Schmidt 分解。

- 矩阵 A 的秩即是两体纯态的 Schmidt 数，大于1即为纠缠态。

二、矩阵的直积（张量积）

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B \cdots & A_{1n}B \\ \vdots & & \\ A_{m1}B & A_{m2}B \cdots & A_{mn}B \end{bmatrix}$$

- 直积的性质：
  1. $0 \otimes A = A \otimes 0 = 0$
  2. $(A_1 + A_2) \otimes B = A_1 \otimes B + A_2 \otimes B,\ A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$
  3. $(\zeta A) \otimes (\eta B) = \zeta\eta (A \otimes B)$
  4. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$

矩阵的直积

例：

$$A \otimes B \equiv \overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}}^{nq} \left.\vphantom{\begin{bmatrix} A \\ A \\ \vdots \\ A \end{bmatrix}}\right\} mp$$

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1\times 2 \\ 1\times 3 \\ 2\times 2 \\ 2\times 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}, \quad X \otimes Y = \begin{bmatrix} 0\cdot Y & 1\cdot Y \\ 1\cdot Y & 0\cdot Y \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$$

矩阵的直积

5. $(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_1A_2) \otimes (B_1B_2)$
6. $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$
7. $(A \otimes B)^{\mathrm{T}} = A^{\mathrm{T}} \otimes B^{\mathrm{T}}$
8. 两上（下）三角阵的直积是上（下）三角阵。
9. 两酉阵的直积是酉阵。
10. $\det(A \otimes B) = (\det A)^n (\det B)^m \qquad A \in C^{mm}, B \in C^{nn}$
11. $tr(A \otimes B) = (trA)(trB)$
12. $rank(A \otimes B) = (rankA)(rankB)$
13. $A^2 = A,\ B^2 = B \Rightarrow (A \otimes B)^2 = A \otimes B$

矩阵的直积

- 试证： $$rank\left(A\otimes B\right)=\left(rankA\right)\left(rankB\right).$$

- 证明： $$A=V_AS_AU_A\text{，}\ B=V_BS_BU_B.$$

$$\begin{aligned}A\otimes B&=\left(V_A\otimes V_B\right)\left(S_A\otimes S_B\right)\left(U_A\otimes U_B\right)\\&\equiv VSU.\end{aligned}$$

$$rankS=\left(rankS_A\right)\left(rankS_B\right).$$

- 因为与可逆阵相乘不改变矩阵的秩，知

$$\begin{aligned}rank\left(A\otimes B\right)&=rankS\\&=\left(rankS_A\right)\left(rankS_B\right)\\&=rank\left(V_AS_AU_A\right)rank\left(V_BS_BU_B\right)\\&=\left(rankA\right)\left(rankB\right).\end{aligned}$$

三、矩阵的酉对角化

- 酉变换：保持内积不变的变换 $(Ux,Uy)=(x,y)$。
- 酉矩阵：U 变换在标准正交基下的矩阵。
- **定理** 矩阵 A 可以酉相似于对角矩阵的充分必要条件是 $A^{+}A=AA^{+}$（即 A 是正规矩阵）。

矩阵的酉对角化

- [证] 必要性：即 A 酉相似于对角阵 $\rightarrow$ $A^{+}A = AA^{+}$ 。

  设 T 为酉矩阵，则 $T^{-1} = T^{+}$ ，

$$TAT^{-1} = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix},$$

则

$$\left(T^{-1}\right)^{+} A^{+}T^{+} = TA^{+}T^{-1} = \begin{bmatrix} \lambda_1^* & & \\ & \ddots & \\ & & \lambda_n^* \end{bmatrix},$$

$$AA^{+} = T^{-1}\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}T\,T^{-1}\begin{bmatrix} \lambda_1^* & & \\ & \ddots & \\ & & \lambda_n^* \end{bmatrix}T = T^{-1}\begin{bmatrix} \lambda_1^* & & \\ & \ddots & \\ & & \lambda_n^* \end{bmatrix}\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}T$$

$$= A^{+}A$$

矩阵的酉对角化

- 充分性：即 $A^{+}A = AA^{+} \rightarrow A$ 酉相似于对角阵。
- 递归构造证明：

$i=1$ 时，显然；　设 $i=n-1$ 时命题成立。

当 $i=n$ 时，取 A 的某一特征值 λ_n ，归一化特征向量 X_n，

则有 $AX_n = \lambda_n X_n$ ，$X_n^{+} X_n = 1$ 。

矩阵的酉对角化

补充 $X_1, X_2, \cdots, X_{n-1}$ 与 X_n 构成一组标准正交基，则存在酉矩阵 S ， 使得矩阵 A 在新基下为

$$A' = \begin{bmatrix} A_{n-1} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ C & \lambda_n \end{bmatrix},$$

（使 S^{-1}的第 j 列是第 j 个基矢量即有 $SAS^{-1} = A'$ ）

矩阵的酉对角化

- 由此得

$$AA^+ = S^{-1}\begin{bmatrix} A_{n-1}A_{n-1}^+ & A_{n-1}C^+ \\ CA_{n-1}^+ & CC^+ + \lambda_n\lambda_n^* \end{bmatrix}S, \qquad A^+A = S^{-1}\begin{bmatrix} A_{n-1}^+A_{n-1} + C^+C & C^+\lambda_n \\ \lambda_n^*C & \lambda_n^*\lambda_n \end{bmatrix}S,$$

- 由利用 $A^+A = AA^+$，得 $CC^+ + \lambda_n\lambda_n^* = \lambda_n^*\lambda_n$，从而有 $C=0$ 和 $A_{n-1}^+A_{n-1} = A_{n-1}A_{n-1}^+$，即 A_{n-1} 是正规矩阵，因此知存在酉阵 P 使得

$$PA_{n-1}P^{-1} = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_{n-1} \end{bmatrix}。$$

矩阵的酉对角化

- 命 $Q=\begin{bmatrix} P & 0 \\ 0 & 1 \end{bmatrix}$，于是

$$QSAS^{-1}Q^{-1}=\begin{pmatrix} P & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} A_{n-1} & 0 \\ 0 & \lambda_n \end{pmatrix}\begin{pmatrix} P^{-1} & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} PA_{n-1}P^{-1} & 0 \\ 0 & \lambda_n \end{pmatrix}=\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

S,Q 为酉阵 $\Rightarrow T=QS$ 亦为酉阵，即： $A^+A=AA^+ \to A$ 酉相似于对角阵。

谱分解定理

- **定理** 向量空间 V 上的任意正规算子 M，在 V的某个标准正交基下可对角化。反之，任意可对角化的算子都是正规的。
- 采用对空间 V 维数 d 的归纳法证明。 $d=1$ 的情况是平凡的。
- 令 λ 是 M 的一个特征值， P 是到 λ 特征空间的投影， Q 是到正交补的投影，于是 $M=(P+Q)M(P+Q)=PMP+QMP+PMQ+QMQ,$
显然 $MP=\lambda P$， 故 $QMP=0$. 令 $|\upsilon\rangle$ 为 λ 特征空间中的元素，则由 M的正规性， $MM^{+}|\upsilon\rangle=M^{+}M|\upsilon\rangle=\lambda M^{+}|\upsilon\rangle$,
可得 $QM^{+}P=0$， 即 $PMQ=0$，于是 $M=PMP+QMQ$.
- 证明中用到：$P^{+}=P, Q^{+}=Q.$

谱分解定理

- 由 $QM = QM(P+Q) = QMQ$, $QM^{+} = QM^{+}(P+Q) = QM^{+}Q$,

$$\begin{aligned} QMQQM^{+}Q &= QMQM^{+}Q \\ &= QMM^{+}Q \\ &= QM^{+}MQ \\ &= QM^{+}QMQ \\ &= QM^{+}QQMQ \end{aligned}$$

- 故 QMQ 是正规的。由归纳假设，QMQ 对子空间 Q 的某个标准正交基是可对角化的，而 PMP 已经是对于 P 的标准正交基对角化的。可知 $M = PMP + QMQ$ 相对全空间的某个标准正交基可对角化。

四、两矩阵同时酉对角化

- **定理** 两个可交换的正规矩阵可以同时酉对角化。

- 证明： ① 当 $AB=BA$ 时， A, B 至少有一个共同的特征向量。设 $AX=\lambda_1 X$ ，构造 $\left[X, BX, B^2X, \cdots\right]$，为 C_n 的子空间，B 为该子空间的线性变换，则存在 X_1，使 $BX_1=\mu_1 X_1$，同时有 $AX_1=\lambda_1 X_1$ 。

两矩阵同时酉对角化

② 类似前一节定理的证明

补充向量 $Y_2,\cdots,Y_n$ ， 与 X_1 构成一组标准正交基。

$$SAS^{-1}=\begin{bmatrix}\lambda_1 & F\\ 0 & A_{n-1}\end{bmatrix},\qquad SBS^{-1}=\begin{bmatrix}\mu_1 & G\\ 0 & B_{n-1}\end{bmatrix}.$$

由 $AA^{+}=A^{+}A,\ BB^{+}=B^{+}B$ 可推出 $F,G=0$ ， 从而

$$SAS^{-1}=\begin{bmatrix}\lambda_1 & 0\\ 0 & A_{n-1}\end{bmatrix},\qquad SBS^{-1}=\begin{bmatrix}\mu_1 & 0\\ 0 & B_{n-1}\end{bmatrix},$$

$\Rightarrow$ $A_{n-1},\ B_{n-1}$ 为可交换的正规矩阵。

两矩阵同时酉对角化

③由此可逐步得到标准正交基 $\{X_1,\cdots,X_n\}$，

在这一组基下，A, B 对角化为：

$$UAU^{-1}=\begin{bmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{bmatrix},\qquad UBU^{-1}=\begin{bmatrix}\mu_1 & & \\ & \ddots & \\ & & \mu_n\end{bmatrix}.$$

两Hermitian阵可对易的充要条件

- **定理**　设 A 和 B 是 Hermitian 矩阵，当且仅当存在一组标准正交基，使 A 和 B 在这组基下同时是对角的，有 $[A,B]=0$，即 A 和 B 可对易。

- 这是教材中的定理。如果考虑的是正规阵，是否有同样结果？

五、教材上的其它内容

- Gram-Schmidt正交化方法
- Dirac符号表示的完备条件
- 算子的矩阵表示
- Cauchy-Schwarz不等式
- 算子函数

Gram-Schmidt正交化方法

- 逐步生成一组标准正交基的方法：

$$
取\ |\upsilon_1\rangle \equiv \frac{|w_1\rangle}{\left\| \ |w_1\rangle \ \right\|},\quad |\upsilon_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^{k} \langle \upsilon_i | w_{k+1}\rangle |\upsilon_i\rangle}{\left\| \ |w_{k+1}\rangle - \sum_{i=1}^{k} \langle \upsilon_i | w_{k+1}\rangle |\upsilon_i\rangle \ \right\|}
$$

Dirac符号表示的完备条件

- 由 $\{|i\rangle\}$ 为一组完备基，有：

$$\left(\sum_i |i\rangle\langle i|\right)|\upsilon\rangle = \sum_i |i\rangle\langle i|\upsilon\rangle = \sum_i \upsilon_i |i\rangle = |\upsilon\rangle$$

可知：

$$\sum_i |i\rangle\langle i| = I$$

此即为Dirac符号表示的完备条件。

算子的矩阵表示

- 设 A 是从 V 到 W 的线性算子，则有 A 的矩阵表示如下：

$$
\begin{aligned}
A &= I_W \ A \ I_V \\
&= \sum_{ij} \left| w_j \right\rangle \left\langle w_j \right| A \left| \upsilon_i \right\rangle \left\langle \upsilon_i \right| \\
&= \sum_{ij} \left\langle w_j \right| A \left| \upsilon_i \right\rangle \left| w_j \right\rangle \left\langle \upsilon_i \right|
\end{aligned}
$$

Cauchy-Schwarz不等式

Cauchy-Schwarz 不等式：对于Hilbert 空间任意两向量 $|v\rangle$ 和 $|w\rangle$ ，有

$$\left|\langle v|w\rangle\right|^2 \le \langle v|v\rangle\langle w|w\rangle.$$

证明：基于 Gram-Schmidt 方法构造向量空间的一组标准正交基 $\{|i\rangle\}$ 时，取这组基的第一个成员为 $|w\rangle/\sqrt{\langle w|w\rangle}$.

利用完备条件 $\sum_i |i\rangle\langle i| = I$，只保留第一项，可得

Cauchy-Schwarz不等式

$$\langle v|v\rangle\langle w|w\rangle=\sum_i\langle v|i\rangle\langle i|v\rangle\langle w|w\rangle$$

$$\geq\frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle}\langle w|w\rangle$$

$$=\langle v|w\rangle\langle w|v\rangle=\left|\langle v|w\rangle\right|^2$$

可以看出，当且仅当 $|v\rangle$ 和 $|w\rangle$ 有线性关系时，上式取等号。

Cauchy-Schwarz不等式

- 另一种证明方法：对于任意复数 λ ，显然有

$$\left(\langle\psi| - \lambda^* \langle\varphi|\right)\left(|\psi\rangle - \lambda|\varphi\rangle\right) \geq 0.$$

即

$$\langle\psi|\psi\rangle + \lambda^*\lambda\langle\varphi|\varphi\rangle - \lambda\langle\psi|\varphi\rangle - \lambda^*\langle\varphi|\psi\rangle > 0,$$

取

$$\lambda = \langle\varphi|\psi\rangle / \langle\varphi|\varphi\rangle,$$

即得：

$$\langle\psi|\psi\rangle\langle\varphi|\varphi\rangle - \langle\psi|\varphi\rangle\langle\varphi|\psi\rangle > 0.$$

算子函数

- 令 $A=\sum_a a|a\rangle\langle a|$ 是正规算子 A 的一个谱分解，定义算子函数：

$$f(A)=\sum_a f(a)|a\rangle\langle a|$$

- 一个不在上述表述范围内的重要矩阵函数是矩阵的迹：

$$tr(A)\equiv\sum_i A_{ii}$$
$$tr(AB)=tr(BA)$$
$$tr(A+B)=tr(A)+tr(B)$$
$$tr(\lambda A)=\lambda\, tr(A)$$

算子函数

- 矩阵的迹在酉相似变换 $A \to UAU^{+}$ 下不变：

$$tr\left(UAU^{+}\right)=tr\left(U^{+}UA\right)=tr\left(A\right).$$

迹在酉相似变换下的不变性保证算子的迹是与基的选取无关的。

- 等式

$$tr\left(A|\psi\rangle\langle\psi|\right)=\sum_i\langle i|A|\psi\rangle\langle\psi|i\rangle=\langle\psi|A|\psi\rangle$$

是一个常用的结果。

一、基本假设

二、基本概念

三、量子测量

四、密度算符

五、复合体系

六、Bell定理

一、基本假设

1. 波函数假设 系统状态为$|\psi\rangle$，坐标表象中为$\psi(\mathbf{r},t)$。对于孤立系统，波函数为完全描述，并有几率波解释。

- 波函数的引入必然导致态叠加原理和纠缠态问题，而这正是量子物理全部神秘和神奇之源。

- 量子信息理论主要涉及由有限维复向量空间上的线性变换所表述的“简易量子力学”，态叠加原理和纠缠态问题却更加凸现出来，量子力学的神秘和神奇丝毫不减。

Richard Feynman:

- “We choose to examine a phenomenon which is impossible, absolutely impossible, to explain in any classical way, and which has in it the heart of quantum mechanics.
- “In reality, it contains the only mystery.
- “We cannot make the mystery go away by “explaining” how it works. We will just tell you how it works.
- “In telling you how it works we will have told you about the basic peculiarities of all quantum mechanics.”

基本假设

2. 算符假设　力学量可用线性厄密算符表示。一对共轭力学量算符的不可对易性是量子力学的基本特征。

基本算符：$\mathbf{r}$, $\mathbf{p} \equiv -i\hbar\nabla$，由此可构造：

$$\hat{T} = \frac{\hat{\mathbf{p}}^2}{2m} = -\frac{\hbar^2}{2m}\Delta, \quad \hat{V} = V(\mathbf{r}),$$

$$\hat{\mathbf{L}} = \mathbf{r}\times\hat{\mathbf{p}} = -i\hbar\mathbf{r}\times\nabla, \quad \hat{E} = i\hbar\frac{\partial}{\partial t},$$

……

基本假设

3. 测量假设 对力学可观测量的测量使系统随机落入该力学量的一个本征态 $|\varphi_m\rangle$，概率为 $|\langle\varphi_m|\psi\rangle|^2$。

平均值： $\bar{\Omega}_\psi = \int \psi^*(\mathbf{r})\,\Omega\,\psi(\mathbf{r})\,d\mathbf{r}$， 用Dirac 符号写为

$$\bar{\Omega} = \langle\Omega\rangle_\psi = \langle\psi|\Omega|\psi\rangle,$$

不必指出具体采用哪个基展开。

基本假设

- 量子系综：大量处于相同的量子态的系统构成量子系综。量子态上的平均值是在量子系综上的平均值。

- 两力学量可同时观测的充分必要条件：
  两力学量算符可对易：$\left[\hat{A},\hat{B}\right]=0$，则有共同本征函数系，可以进行同时测量，测量后系统进入两力学量的一个共同本征态。

基本假设

4. 态演化假设 Schrödinger绘景下量子态演化所遵循的方程是Schrödinger方程：

$$i\hbar\frac{\partial}{\partial t}\left|\psi(t)\right\rangle = \hat{H}(p,q,t)\left|\psi(t)\right\rangle,$$

其中 $\hat{H}(p,q,t)$ 为系统的哈密顿算符。

5. 全同性假设 全同粒子体系的波函数对于任意两粒子的交换是对称的（玻色子情形）或是反对称的（费米子情形），即自然界存在的态 $\left|\psi\right\rangle$ 必须是所有交换算符的本征态：$P_{ij}\left|\psi\right\rangle = \pm\left|\psi\right\rangle, (i,j=1,2,\cdots,N)$.

二、基本概念

- Dirac采用了抽象的态矢量符号，以与基选取无关的方式表达量子体系的状态及其演化，更凸现了物理本质。
- 严格来讲，连续谱态空间超出了Hilbert空间。
- 量子力学独立于波动力学和矩阵力学的表述方式：费曼量子最小作用量原理。

右矢，左矢，标量积

1. 右矢、左矢、标量积

右矢：$|A\rangle$，如：$|\mathbf{r}\rangle, |\mathbf{p}\rangle, |\psi_{nlm}(t)\rangle, |\psi_{nlm}\rangle, |nlm\rangle, \cdots$

左矢：$\langle A| = (|A\rangle)^{+}, \Rightarrow (\langle A|)^{+} = |A\rangle$

标量积：$\langle B|A\rangle =$ 对由态矢$|A\rangle$描述的物理系统测量，发现该系统处于状态$|B\rangle$的几率幅。

用波函数表示，则为：$\langle B|A\rangle = \int \varphi_B^*(\mathbf{r})\varphi_A(\mathbf{r})d\mathbf{r}$ 。

标积的厄密性质：$\langle B|A\rangle = \langle A|B\rangle^*$ 。

- 为了能在态矢空间中进行定量计算，需要选取一组特定的态矢作为基矢，以展开任意态矢。

对易式和反对易式

- 对易式定义为 $[A,B]\equiv AB-BA$ 。

  反对易式定义为 $\{A,B\}\equiv AB+BA$ 。
- 设 A 和 B 为厄密算符，$\langle\psi|AB|\psi\rangle = x+iy$,

  有：$\langle\psi|[A,B]|\psi\rangle = 2iy, \langle\psi|\{A,B\}|\psi\rangle = 2x$. 于是有

$$\left|\langle\psi|[A,B]|\psi\rangle\right|^2 + \left|\langle\psi|\{A,B\}|\psi\rangle\right|^2 = 4\left|\langle\psi|AB|\psi\rangle\right|^2.$$

- 根据Cauchy-Schwarz不等式，

$$\left|\langle\psi|AB|\psi\rangle\right|^2 \le \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle,$$

  得到：

$$\left|\langle\psi|[A,B]|\psi\rangle\right|^2 \le 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle.$$

不确定性原理

- Suppose C and D are two observables. Substituting $A=C-<C>$ and $B=D-<D>$ into the last equation, we obtain Heisenberg's uncertainty principle as it is usually stated:

$$\Delta(C)\Delta(D) \geq \frac{\left|\left\langle \psi \middle| [C,D] \middle| \psi \right\rangle\right|}{2}$$

- 上式其实只是一个定理，应该称之“测不准关系”。不确定性原理是一个物理定律，不是可以推导出来的。

正交归一条件

2、正交归一性和完备性

- 正交归一条件

离散编号（分立谱）：

$$\langle \xi_i | \xi_j \rangle = \delta_{ij}$$

$$\langle nlm | n'l'm' \rangle = \delta_{nn'}\delta_{ll'}\delta_{mm'}$$

连续编号（连续谱）：

$$\langle \xi' | \xi'' \rangle = \delta(\xi' - \xi'')$$

$$\langle \mathbf{r}' | \mathbf{r}'' \rangle = \delta(\mathbf{r}' - \mathbf{r}'')$$

$$\langle \mathbf{p}' | \mathbf{p}'' \rangle = \delta(\mathbf{p}' - \mathbf{p}'')$$

完备条件

- 完备条件

$$\sum_i |\xi_i\rangle\langle\xi_i| = I \qquad \text{(离散）}$$

$$\int |\xi\rangle d\,\xi \langle\xi| = I \qquad \text{(连续）}$$

- 普遍形式：

$$\sum_i |\xi_i\rangle\langle\xi_i| + \int |\xi'\rangle d\,\xi' \langle\xi'| = I \qquad (1)$$

完备条件

- （1）式的证明：设

$$\left|A\right\rangle = \sum_i a_i \left|\xi_i\right\rangle + \int a(\xi)\left|\xi\right\rangle d\,\xi,$$

由正交归一性，有

$$\left\langle \xi_j \middle| A\right\rangle = \sum_i a_i \left\langle \xi_j \middle| \xi_i \right\rangle = \sum_i a_i \delta_{ij} = a_j$$

$$\left\langle \xi' \middle| A\right\rangle = \left\langle \xi' \right| \left\{ \int a(\xi'') \left|\xi''\right\rangle d\,\xi'' \right\}$$

$$= \int a(\xi'')\,\delta(\xi' - \xi'')\,d\,\xi'' = a(\xi').$$

完备条件

所以有

$$
\begin{aligned}
|A\rangle &= \sum_i \langle \xi_i | A\rangle |\xi_i\rangle + \int \langle \xi | A\rangle |\xi\rangle \, d\xi \\
&= \sum_i |\xi_i\rangle\langle \xi_i | A\rangle + \int |\xi\rangle \, d\xi \langle \xi | A\rangle \\
&= \left(\sum_i |\xi_i\rangle\langle \xi_i| + \int |\xi\rangle \, d\xi \langle \xi| \right) |A\rangle,
\end{aligned}
$$

故知

$$
\sum_i |\xi_i\rangle\langle \xi_i| + \int |\xi\rangle \, d\xi \langle \xi| = \hat{I},
$$

即（1）式成立。

标积

- 标积的计算：设

$$\left|A\right\rangle = \sum_i a_i \left|\xi_i\right\rangle + \int a(\xi)\left|\xi\right\rangle d\,\xi$$

$$\left\langle B\right| = \sum_i b_i^* \left\langle\xi_i\right| + \int b^*(\xi')\left\langle\xi'\right| d\,\xi'$$

则

$$\left\langle B\middle|A\right\rangle = \sum_{ij} b_i^* a_j \delta_{ij} + \int b^*(\xi') a(\xi)\,\delta(\xi'-\xi)\,d\,\xi' d\,\xi$$

$$= \sum_i b_i^* a_i + \int b^*(\xi) a(\xi)\,d\,\xi$$

- 标积的意义：$\left\langle \mathbf{r}\middle|A\right\rangle = \psi_A(\mathbf{r})$ 表示处于$\left|A\right\rangle$ 态的系统，在点 $\mathbf{r}$ 的几率幅。

举例

- 例如：
$$\langle \mathbf{r} | \mathbf{p} \rangle = \frac{1}{(2\pi\hbar)^{3/2}} e^{i\mathbf{p}\cdot\mathbf{r}/\hbar} ,$$
$$\langle \mathbf{p} | \mathbf{r} \rangle = \frac{1}{(2\pi\hbar)^{3/2}} e^{-i\mathbf{p}\cdot\mathbf{r}/\hbar} = \langle \mathbf{r} | \mathbf{p} \rangle^* ,$$

易于验证：
$$\begin{aligned}\langle \mathbf{r} | \mathbf{r}' \rangle &= \int \langle \mathbf{r} | \mathbf{p} \rangle d\mathbf{p} \langle \mathbf{p} | \mathbf{r}' \rangle \\ &= \frac{1}{(2\pi\hbar)^3} \int e^{i(\mathbf{p}\cdot\mathbf{r}-\mathbf{p}\cdot\mathbf{r}')/\hbar} d\mathbf{p} \\ &= \delta(\mathbf{r} - \mathbf{r}') .\end{aligned}$$

例题

- 现证明：

$$\langle \mathbf{r}'|\mathbf{p} = -i\hbar \frac{\partial}{\partial \mathbf{r}'}\langle \mathbf{r}'| \qquad (2)$$

- 对任意态 $|A\rangle$ 有：

$$\langle \mathbf{r}'|\mathbf{p}|A\rangle = \int \langle \mathbf{r}'|\mathbf{p}|\mathbf{p}'\rangle\langle \mathbf{p}'|A\rangle d\mathbf{p}'$$

$$= \int \mathbf{p}' e^{i\mathbf{p}'\cdot\mathbf{r}'/\hbar}\psi_A(\mathbf{p}')\frac{d\mathbf{p}'}{(2\pi\hbar)^{3/2}}$$

$$= -i\hbar\frac{\partial}{\partial \mathbf{r}'}\int e^{i\mathbf{p}'\cdot\mathbf{r}'/\hbar}\psi_A(\mathbf{p}')\frac{d\mathbf{p}'}{(2\pi\hbar)^{3/2}}$$

$$= -i\hbar\frac{\partial}{\partial \mathbf{r}'}\psi_A(\mathbf{r}') = -i\hbar\frac{\partial}{\partial \mathbf{r}'}\langle \mathbf{r}'|A\rangle$$

作业

- 由 $|A\rangle$ 的任意性，知有等式（2）成立。

- **[作业]** 证明

$$\begin{cases} \hat{\mathbf{r}}\left|\mathbf{p}'\right\rangle = -i\hbar\dfrac{\partial}{\partial\mathbf{p}'}\left|\mathbf{p}'\right\rangle \\ \left\langle\mathbf{p}'\right|\hat{\mathbf{r}} = i\hbar\dfrac{\partial}{\partial\mathbf{p}'}\left\langle\mathbf{p}'\right| \end{cases}$$

三、量子测量

1. 测量的形式理论：设测量算子集合为 $\{M_m\}$.

对于测量 $\{M_m\}$ 有：以概率 $p(m)=\langle\psi|M_m^+M_m|\psi\rangle$

测到编号为 m 的结果，并使系统进入状态

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

由 $\sum_m p(m)=1$ 可得 $\sum_m M_m^+M_m=I$. 此即为测量算子的完备性关系。

量子测量

2. 正交投影测量：

可观测量 M 有谱分解$M=\sum_m \lambda_m P_m$，其中 $P_m=|m\rangle\langle m|$ 是到特征值为λ_m的特征子空间的投影算符。

测量状态$|\psi\rangle$时将以概率 $p(m)=\langle\psi|P_m|\psi\rangle$ 得到编号为m的测量结果，测量完成后系统进入状态 $P_m|\psi\rangle/\sqrt{p(m)}$.

量子测量

① 由于$P_m = P_m^2 = P_m^+ P_m$，可取 $M_m = P_m$， 此时 M_m 满足正交投影算子条件：$M_m M_n = \delta_{mn} M_m$.

② M 在 $|\psi\rangle$ 下的平均值为

$$\langle M\rangle = \sum_m mp(m) = \sum_m m\langle\psi|P_m|\psi\rangle$$
$$= \langle\psi|\sum_m mP_m|\psi\rangle = \langle\psi|M|\psi\rangle.$$

量子测量

- 实际测量过程的刻画：

设初始时刻系统 A 处于叠加态 $|\varphi\rangle=\sum_m \alpha_m |m\rangle$， 指示器状态 $|\psi(x)\rangle$，大系统处于可分离态：

$$|\varphi\rangle\otimes|\psi\rangle=\sum_m \alpha_m |m\rangle\otimes|\psi(x)\rangle,$$

经 t 时刻演化后，大系统演化为纠缠态：

$$U(t)\{|\varphi\rangle\otimes|\psi(x)\rangle\}=\sum_m \alpha_m |m\rangle\otimes|\psi(x,m)\rangle.$$

量子测量

- 在读出测量结果 m 之时被测系统坍缩到被测力学量的本征态 $|m\rangle$。
- Stern-Gerlach 实验：

$$H=\frac{p^2}{2m}-\mu B(x)\sigma_x \qquad (\text{质量为}m,\ \text{磁矩为}\mu)$$

取一级近似：

$$B(x)=\left.\frac{\partial B}{\partial x}\right|_{x=0} x \rightarrow H=\frac{p^2}{2m}-fx\sigma_x\ ,$$

其中 $f=\mu\dfrac{\partial B}{\partial x}$.

量子测量

- 设系统初态为

$$\langle x|\Psi(0)\rangle=\left(C_+|\uparrow\rangle+C_-|\downarrow\rangle\right)\otimes\psi(x),$$

取 $\psi(x)=\left(\frac{1}{2\pi a^2}\right)^{\frac{1}{4}}e^{-\frac{x^2}{4a^2}}$ 是一个高斯波包，在磁场中，处于 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 状态的粒子接受到方向相反的力 $\pm f$ 的作用，因而分裂为两束，有

量子测量

$$\left|\Psi(t)\right\rangle = e^{-iHt}\left|\Psi(0)\right\rangle$$

$$= C_+\left|\uparrow\right\rangle e^{-i\left(\frac{p^2}{2m}-fx\right)t}\left|\psi\right\rangle + C_-\left|\downarrow\right\rangle \otimes e^{-i\left(\frac{p^2}{2m}+fx\right)t}\left|\psi\right\rangle.$$

在坐标表象中，可以得到：

$$\left\langle x\middle|\Psi(t)\right\rangle = C_+\left|\uparrow\right\rangle \otimes \psi_+(x) + C_-\left|\downarrow\right\rangle \otimes \psi_-(x),$$

量子测量

其中

$$\psi_{\pm}(x)=\frac{\left(a^2/2\pi\right)^{\frac{1}{4}}}{\sqrt{a^2+\frac{it}{2m}}}\exp\left\{-\frac{if^2t^3}{6m}-\frac{\left(x\mp\frac{ft^2}{2m}\right)^2}{4\left(a^2+\frac{it}{2m}\right)}\pm iftx\right\}$$

是分别与 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 态相关联的空间分布。

理想测量：要能区分 $\psi_+(x)$ 和 $\psi_-(x)$，即 $\langle\psi_+|\psi_-\rangle\to 0.$

量子测量

- 实验中，

$$\left|\langle\psi_+|\psi_-\rangle\right| = \exp\left(-2a^2f^2t^2 - \frac{f^2t^4}{8a^2m^2}\right),$$

显然 $\left|\langle\psi_+|\psi_-\rangle\right| \xrightarrow{t\to\infty} 0$，

即 $S-G$ 实验实现了一个**理想测量**。

- 这正是量子测量过程导致 $\sum c_n|n\rangle|e\rangle \to \sum_n c_n|n\rangle|e_n\rangle$ 的例子。

量子测量

3. 广义测量与POVM：

广义测量：在大系统上进行正交投影测量时，在子系统上所观察到的测量，是前面给出的测量形式理论的具体实现。

POVM：一组能对单位算符做分解的非负的厄密算符。

量子测量

- Neumark定理

  任何给定的POVM都可以通过将态空间扩展到某一更大的态空间，并在其上施行正交投影测量的方法实现。

- POVM元定义为：$E_m \equiv M_m^+ M_m$，半正定算子 E_m 满足

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

- 集合 $\{E_m\}$ 即称为一个POVM。

量子测量

例1. $\left\{\mathbf{n}_\alpha \middle| \left|\mathbf{n}_\alpha\right|^2 = 1, \alpha = 1, 2, \cdots, N\right\}$ 满足 $\sum_\alpha \lambda_\alpha \mathbf{n}_\alpha = 0$， 其中 $0 < \lambda_\alpha < 1$，$\sum_\alpha \lambda_\alpha = 1$. 构造 $\hat{F}_\alpha = \lambda_\alpha\left(\mathrm{I} + \mathbf{n}_\alpha \cdot \hat{\boldsymbol{\sigma}}\right)$， 可知 $\hat{F}_\alpha$ 非负，厄密，并且 $\sum_\alpha F_\alpha = \hat{\mathrm{I}}$. 故知 $\left\{\hat{F}_\alpha \middle| \alpha = 1, \cdots, N\right\}$ 在一个量子位的二维态空间中定义了一个POVM。

作业：证明上述POVM元的半正定性。

量子信息与量子密码

[第2次课] 数学、物理预备知识

Q&A