量子计算与量子信息 Notes

Flower CA77

目　录

第一部分　基础概念

第一章　简介与概述

1.1 全貌

1.2 量子比特

1.3 量子计算

1.4 量子算法

1.5 实验量子信息处理

1.6 量子信息

第二章　量子力学引论

2.1 线性代数

2.2 量子力学的假设

2.3 应用: 超密编码

2.4 密度算子

2.5 Schmidt 分解与纯化

2.6 EPR 和 Bell 不等式

第三章　计算机科学简介

3.1 计算模型

3.2 计算问题的分析

3.3 关于计算科学的观点

第二部分　量子计算

第四章　量子电路

4.1 量子算法

4.2 单量子比特操作

4.3 受控操作

4.4 测量

4.5 通用量子门

4.6 量子计算电路模型总结

4.7 量子系统的模拟

第五章　量子 Fourier 变换及其应用

5.1 量子 Fourier 变换

5.2 相位估计

5.3 应用: 求阶与因子分解问题

5.4 量子 Fourier 变换的一般应用

第六章　量子搜索算法

6.1 量子搜索算法

6.2 作为量子模拟的量子搜索

6.3 量子计数

6.4 NP 完全问题解的加速

6.5 无结构数据库的量子搜索

6.6 搜索算法的最优性

6.7 黑盒算法的极限

第七章　量子计算机: 物理实现

7.1 指导性原则

7.2 量子计算的条件

7.3 谐振子量子计算机

7.4 光学光量子计算机

7.5 光学腔量子电动力学

7.6 离子阱

7.7 核磁共振

7.8 其他实现方案

第三部分　量子信息

第八章　量子噪声与量子操作

8.1 经典噪声与 Markov 过程

8.2 量子操作

8.3 量子噪声与量子操作的例子

8.4 量子操作的应用

8.5 量子操作形式体系的局限

第九章　量子信息的距离度量

9.1 经典信息的距离度量

9.2 两个量子态有多接近

9.3 量子信道保护信息的效果怎么样

第十章　量子纠错

10.1 背景介绍

10.2 Shor 编码

10.3 量子纠错理论

10.4 构造量子编码

10.5 稳定子编码

10.6 容错量子计算

第十一章　熵与信息

11.1 Shannon 熵

11.2 熵的基本性质

11.3 von Neumann 熵

11.4 强次可加性

第十二章　量子信息论

12.1 量子态的区分与可达信息

12.2 数据压缩

12.3 噪声信道上的经典信息

12.4 有噪声量子信道的量子信息

12.5 作为一种物理资源的纠缠

12.6 量子密码学

附录

附录 A　概率论基础

随机变量 X 取值 x 的概率为 $p(X=x)$:

- 如果 X 是离散型随机变量, 则 $p(X=x)$ 为 $X=x$ 的概率
- 如果 X 是连续型随机变量, 则 $p(X=x)=0$, 因为一个点在一个连续区域内的测度为零, 此时我们引入概率密度 $\rho(x)$, 使得 $p(x\leqslant X<x+dx)=\rho(x)dx$

我们简记 $p(X=x)$ 为 $p_X(x)$, 不引起混淆时进一步简记为 $p(x)$。

概率密度的概念是始终有效的, 对离散型随机变量 X, 我们可以取 $\rho(x)=\sum_{x'}p(X=x')\delta(x-x')$, 其中求和 x' 取遍 X 的所有值, δ 为 Dirac 的 δ 函数。进一步, 当 x' 不是 X 可取的值时 $p(X=x')=0$, 求和 x' 可以取遍全部值。

一组随机变量 $X_1,X_2,\cdots,X_n$ 组成随机向量 $\boldsymbol{X}=(X_1,X_2,\cdots,X_n)$, 联合分布 $p(\boldsymbol{X}=\boldsymbol{x})=p(X_1=x_1,X_2=x_2,\cdots,X_n=x_n)$ 也简记为 $p_{\boldsymbol{X}}(\boldsymbol{x})$, 不引起混淆时简单记作 $p(\boldsymbol{x})$。

条件概率 $p(Y=y\mid X=x)=p(X=x,Y=y)/p(X=x)$, 简记为 $p_{Y|X}(y\mid x)=p_{(X,Y)}(x,y)/p_X(x)$, 其中分子是随机向量 (X,Y) 的联合分布。不引起混淆时我们简单记作 $p(y\mid x)$。

注意　在略去概率 p 的角标时 [即简记 $p_X(x)$ 为 $p(x)$] 必须要规范标记变量, 即用单个大写字母 X 表示随机变量, 其小写值 x 表示对应的 X 的取值, 这个规定也是 $p(x)$ 的缺省标准。在表达式比较复杂时, 可以显式写出随机变量 $p(X=x)$。

习题 (教材 A.1)　证明 Bayes 定律 $p(x\mid y)=p(y\mid x)\dfrac{p(x)}{p(y)}$

证明　把待证等式改写为 $p(x\mid y)p(y)=p(y\mid x)p(x)$，可以看到等式两边都是联合分布概率 $p(x,y)$，这就证明了待证方程。

习题 (教材 A.2)　全概率公式 $p(y)=\sum_x p(y\mid x)p(x)$

证明　$\sum_x p(y\mid x)p(x)=\sum_x p(x,y)=p(y)$

期望 $\mathbb{E}X\equiv\sum_x xp(x)$, 方差 $\operatorname{var}X\equiv\mathbb{E}\Big[(X-EX)^2\Big]=\mathbb{E}(X^2)-(\mathbb{E}X)^2$, 标准差 $\Delta X\equiv\sqrt{\operatorname{var}X}$

习题 (教材 A.3)　证明 $\exists x\geqslant\mathbb{E}X$, s.t. $p(x)>0$

证明　反证，只要证明命题 $\forall x\geqslant\mathbb{E}X: p(x)=0$ 是伪命题即可。考虑到

$$\mathbb{E}X=\sum_x xp(x)=\sum_{x<\mathbb{E}X}xp(x)+\sum_{x\geqslant\mathbb{E}X}xp(x)=\sum_{x<\mathbb{E}X}xp(x)<\mathbb{E}X\sum_{x<\mathbb{E}X}p(x)\leqslant\mathbb{E}X\sum_x p(x)=\mathbb{E}X$$

习题 (教材 A.4)　证明 $\mathbb{E}X$ 对 X 是线性的。

证明　$\mathbb{E}(kX)=\sum_x kxp(x)=k\sum_x xp(x)=k\mathbb{E}X$

习题 (教材 A.5)　证明 X,Y 独立时 $\mathbb{E}(XY)=\mathbb{E}X\cdot\mathbb{E}Y$

证明　$\mathbb{E}(XY)=\sum_{x,y}xyp(x,y)\overset{X,Y\text{ 独立}}{=\!=\!=}\sum_{x,y}xyp(x)p(y)=\sum_x xp(x)\sum_y yp(y)=\mathbb{E}X\cdot\mathbb{E}Y$

习题 (教材 A.6, Cheybshev 不等式)　$\forall\lambda>0$ 和有限方差的 X，$p(|x-\mathbb{E}X|\geqslant\lambda\Delta X)\leqslant\dfrac{1}{\lambda^2}$

证明 我们设概率密度为 $\rho(x)$，则

$$
\begin{aligned}
\Delta X^2 = \operatorname{var} X = \mathbb{E}\Big[(X-\mathbb{E}X)^2\Big] = \int (x-\mathbb{E}X)^2\rho(x)dx \\
&= \int_{x-\mathbb{E}X\leqslant -\lambda\Delta X}(x-\mathbb{E}X)^2\rho(x)dx + \int_{\mathbb{E}X-\lambda\Delta X}^{\mathbb{E}X+\lambda\Delta X}(x-\mathbb{E}X)^2\rho(x)dx + \int_{x-\mathbb{E}X\geqslant \lambda\Delta X}(x-\mathbb{E}X)^2\rho(x)dx \\
&\geqslant \lambda^2\Delta X^2\int_{x-\mathbb{E}X\leqslant -\lambda\Delta X}\rho(x)dx + 0 + \lambda^2\Delta X^2\int_{x-\mathbb{E}X\geqslant \lambda\Delta X}\rho(x)dx = \lambda^2\Delta X^2\int_{|x-\mathbb{E}X|\geqslant \lambda\Delta X}\rho(x)dx
\end{aligned}
$$

则 $p(|X-\mathbb{E}X|\geqslant \lambda\Delta X) = \displaystyle\int_{|x-\mathbb{E}X|\geqslant \lambda\Delta X}\rho(x)dx \leqslant \frac{\Delta X^2}{\lambda^2\Delta X^2} = \frac{1}{\lambda^2}$

附录 B　群论

B.1 基本定义

定义 B.1 (群)　(1) 封闭性 (2) 结合律 (3) 单位元 (4) 逆元

定义 B.2 (有限群)　若群 G 有限, 则其成员个数 $|G|$ 称为阶数。

定义 B.3 (Abel 群)　运算 **可交换** 的群, 如整数模 n 的加法群 $\mathbb{Z}_n$。

定义 B.4 (阶数)　若 $g \in G$, 使得 $g^r = e$ 的最小正整数 $r \in \mathbb{Z}_{>0}$ 称为其阶数。

定义 B.5 (子群)　$H \leqslant G$ 是指 $H \subset G$ 且 H 在 G 运算下构成群。容易看出单位元 $e \in G$。

习题 (教材 B.1)　证明有限群的成员都有阶数，即 $\forall g \in$ 有限群, $\exists r \in \mathbb{Z}_{>0}$, s.t. $g^r = e$。

证明　若某个成员 g 没有阶数，则群 G 有无限大的子集 $\{g^r : r \in \mathbb{Z}_{>0}\}$，矛盾。进一步，我们知道群 G 的任何成员的阶数不超过 $|G|$。

习题 (教材 B.2, Lagrange 定理)　若 $H \leqslant$ 有限群 G，则 $|H|$ 可整除 $|G|$，除数 $[G:H] = \dfrac{|G|}{|H|}$ 称为子群 H 的 Lagrange 指数。

为了证明此定理我们需要引入一些概念:

定义 B.6 (陪集)　设 $H \leqslant g$, 集合 $gH = \{gh : h \in H\}$, $Hg = \{hg : h \in H\}$ 称为 g 对 H 的 **左陪集** 和 **右陪集** 。

命题 1　$gH = H \iff g \in H$

证明　$g \in H \implies gH = H$ 是显然的，反过来时注意到 $e \in H$，则 $g = ge \in gH = H$。

命题 2　$g_1H \cap g_2H = \begin{cases} \text{非空集合} & (g_1H = g_2H) \\ \varnothing & (g_1H \neq g_2H) \end{cases}$

证明　对 $\forall g \in g_1H$ 有 $g = g_1h = g_2(g_2^{-1}g_1h)$ $(h \in H)$。若 $\exists$成员 $g \in g_1H \cap g_2H$，则有 $h_1, h_2 \in H$ s.t. $g = g_1h_1 = g_2h_2 \implies g_2^{-1}g_1 = h_2h_1^{-1} \in H$，由此 $g = g_2(g_2^{-1}g_1h) \in g_2H$。类似的 $\forall g \in g_2H \implies g \in g_1H$，这就证明了 $g_1H = g_2H$。

命题 3　全部陪集的并 $\bigcup\limits_{g \in G} gH = G$。

证明　由 $gH \subset G$ 可知 $\bigcup\limits_{g \in G} gH \subset G$。

另一方面，由于 $e \in H$，故 $\forall g \in G, g = ge \in gH$，这说明 $\forall g \in G : G \subset gH \implies g \subset \bigcup\limits_{g \in G} gH$。

综合上述所论，$\bigcup\limits_{g \in G} gH \subset G$ && $g \subset \bigcup\limits_{g \in G} gH \implies G = \bigcup\limits_{g \in G} gH$。

证明 (教材习题 B.2, Lagrange 定理)　我们知道全部陪集 $\{gH : g \in G\}$ 是一组不交的集合，容易看出 $\bigcup \{gH : g \in G\} = G$，即 $G = \bigsqcup \{gH : g \in G\} = \bigsqcup gH$，这说明 $|G| = \sum |gH|$。容易证明 $|gH| = |H|$，这说明 $|G| = \sum |gH| = \sum |H| = |H| \sum 1$，由此命题得证。

习题 (教材 B.3) 证明每个成员 $g \in G$ 的阶数可以整除 $|G|$。

证明 令 $H = \{g^r : 1 \leqslant r \leqslant r_k\} = \{g, g^2, \cdots, g^{r_k - 1}, g^{r_k} = e\}$，则容易看出 $H \leqslant G$，根据 Lagrange 定理，H 的指数 $[G:H] = \dfrac{|G|}{|H|} \in \mathbb{Z}_{>0}$，即 $|G| = [G:H] \cdot |H| = [G:H] r_k \implies r_k \mid |G|$。

定义 B.7 若 $\exists g \in G$, s.t. 群成员 $a, b \in G$ 满足 $b = g^{-1} a g$, 则称 a, b 为共轭成员。

命题 4 群成员间的共轭是等价关系。

证明 1. 任意成员 a 与其自身共轭:

$$a = e^{-1} a e$$

2. 若成员 a 与成员 b 共轭，则成员 b 与成员 a 共轭:

$$(b = g^{-1} a g) \implies \left[a = (g^{-1})^{-1} b (g^{-1})\right]$$

3. 若成员 a 与成员 b 共轭，成员 b 与成员 c 共轭，则成员 a 与成员 c 共轭:

$$(b = g^{-1} a g) \,\&\&\, (c = g'^{-1} b g') \implies \left[c = g'^{-1} g a g g' = (g g')^{-1} a (g g)\right]$$

定义 B.8 (正规子群) 若 $H \leqslant G$ 且 $\forall g \in G : g^{-1} H g = H$ (或等价的 $Hg = gH$), 则称 H 为 G 的 **正规子群** , 记作 $H \trianglelefteq G$, 记号 $H \triangleleft G$ 表示 $H \neq G$ 的正规子群。

我们指出, Abel 群的任何子群都是正规子群。设 $H \leqslant$ Abel 群 G, 由于子群 H 的成员也是其继承的 Abel 群的成员, 这些成员与 G 中任意成员 g 也是可交换的, 故 $Hg = gH$ 显然成立。

对群 G, $x \in G$ 的共轭类定义为 $G_x \equiv \left\{g^{-1} x g : g \in G\right\}$。容易看出 $y \in G_x \implies x \in G_y$。注意到

$$\begin{aligned} y \in G_x &\implies \exists g \in G : y = g^{-1} x g \\ &\implies \exists g \in G : x = g y g^{-1} = \left(g^{-1}\right)^{-1} y \left(g^{-1}\right) \\ &\xrightarrow{g^{-1} \in G} \exists g \in G : x = g^{-1} y g \implies x \in G_y \end{aligned}$$

习题 (教材 B.4) $y \in G_x \implies G_y = G_x$

证明 由于 $y \in G_x$，$\exists g_0 \in G : y = g_0^{-1} x g_0$ 或 $x = g_0 y g_0^{-1}$。现在设 $t \in G_y$，即 $\exists g \in G : t = g^{-1} y g = g^{-1} g_0^{-1} x g_0 g = (g_0 g)^{-1} x (g_0 g) \implies t \in G_x$，这就证明了 $G_y \subset G_x$。反过来设 $t \in G_x$，即 $\exists g \in G : t = g^{-1} x g = g^{-1} g_0 y g_0^{-1} g = \left(g_0^{-1} g\right)^{-1} y \left(g_0^{-1} g\right) \implies t \in G_y$。这就证明了 $G_x \subset G_y$。综合上述，我们有 $G_y = G_x$。

习题 (教材 B.5) $x \in$ Abel 群 $G \implies G_x = \{x\}$

定义 B.9 (生成元) 设 $g_1, g_2, \cdots, g_\ell \in$ 群 G, 则 G 中全部可以写成 $g_1, g_2, \cdots, g_\ell$ 中若干个成员之乘积的群成员构成 G 的一个子集, 叫做 $g_1, g_2, \cdots, g_\ell$ 所生成的子群 H, 记作 $H = \langle g_1, g_2, \cdots, g_\ell \rangle$, 即

$$\langle g_1, g_2, \cdots, g_\ell \rangle = \left\{ g_1^{n_1} g_2^{n_2} \cdots g_\ell^{n_\ell} = \prod_{k=1}^{\ell} g_k^{n_k} : (n_1, n_2, \cdots, n_\ell) \in (\mathbb{Z}_{\geqslant 0})^\ell \right\}$$

$g_1, g_2, \cdots, g_\ell$ 称为子群 $\langle g_1, g_2, \cdots, g_\ell \rangle$ 的生成元。

如果基群 G 是很大的或平凡的, 那么由给定成员生成的继承 G 的子群也称为 (G 的) 一个 **生成群** , 我们可以略去 G 的表述。容易看出生成一个阶数为 n 的生成群至少需要 $\log(n)$ 个成员。

附录 C　Solovay-Kitaev 定理

附录 D　数论

附录 E　公钥密码和 RSA 密码系统

附录 F　Lieb 定理的证明