量子计算与量子信息 Notes

Flower CA77

目　录

附录

1 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 $\rho(x)=\sum\limits_{x'}p(X=x')\delta(x-x')$, 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, 可以显示写出随机变量 $p(X=x)$。

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

证明 $\sum\limits_x p(y\mid x)p(x)=\sum\limits_x p(x,y)=p(y)$

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

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

证明 反证, 只要证明命题 $\forall x\geqslant\mathbb{E}X,\ \text{s.t.}\ \ p(x)=0$ 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 (A.4) 证明 $\mathbb{E}X$ 对 X 是线性的。

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

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

证明 $\mathbb{E}(XY)=\sum\limits_{x,y}xyp(x,y)\overset{X,Y\ \text{独立}}{=\!=\!=\!=}\sum\limits_{x,y}xyp(x)p(y)=\sum\limits_x xp(x)\sum\limits_y yp(y)=\mathbb{E}X\cdot\mathbb{E}Y$

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

2 群论

2.1 基本定义

定义 (群) (1) 封闭性 (2) 结合律 (3) 单位元 (4) 逆元

定义 (有限群) 若群 G 有限, 则其成员个数 $|G|$ 称为阶数。

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

定义 (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 (子群) $H \leqslant G$ 是指 $H \subset G$ 且 H 在 G 运算下构成群。

习题 (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 (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 (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 $gH = H \iff g \in H$

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 $g_1 H \cap g_2 H = \begin{cases} \text{非空集合} & (g_1 H = g_2 H) \\ \varnothing & (g_1 H \neq g_2 H) \end{cases}$

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

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

定义 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 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:

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

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:

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

第一部分　基础概念