

1. 第一次课后作业

单选题

概率分布 $\bar{p} = \{p_1, p_2, \dots, p_a\}$ 是一个确定性分布为熵 $H(p_1, p_2, \dots, p_a) = 0$ 的 () 条件.

(A) 充分条件; (B) 必要条件; (C) 充分必要条件; (D) 既不充分也不必要.

概率分布 $\bar{p} = \{p_1, p_2, \dots, p_a\}$ 是一个确定性分布, 即所有的概率都为 1 或 0, 因此熵 $H(p_1, p_2, \dots, p_a) = 0$.

反之, 若 $H(p_1, p_2, \dots, p_a) = 0$, 则由 $H(p_1, p_2, \dots, p_a)$ 的定义可知, $\forall i, p_i \log_c p_i = 0$, 或者 $p_i = 0$, 或者 $\log_c p_i = 0$, 由于 $\sum_{i=1}^a p_i = 1, p_i \geq 0$, 存在 i 使得 $p_i = 1$, 而其它 $p_j = 0$, 因此 \bar{p} 必为确定型分布. 所以, 答案是: (C) 充分必要条件

单选题

设 ξ 是一个二元随机变量, 即 $\mathcal{X} = \{0, 1\}$, 令 $p(\xi = 1) = p, p(\xi = 0) = 1 - p$. 则有二元熵函数 $H(p) = p \log_2 \frac{1}{p} + (1 - p) \log_2 \frac{1}{1-p}$, 则当 $p = ()$ 时, $H(p)$ 达到最大值.

(A) 0 (B) $\frac{1}{4}$; (C) $\frac{1}{2}$; (D) 1.

首先, 计算 $H(p)$ 的导数:

$$\begin{aligned} H(p) &= -p \log_2 p - (1 - p) \log_2 (1 - p) \\ H'(p) &= -\log_2 p - p \cdot \frac{1}{\ln 2 \cdot p} + \log_2 (1 - p) + \frac{1}{1 - p} \cdot \frac{1 - p}{\ln 2} \\ &= -\log_2 p - \frac{1}{\ln 2} + \log_2 (1 - p) + \frac{1}{\ln 2} \\ &= -\log_2 p + \log_2 (1 - p) \\ &= \log_2 \frac{1 - p}{p} \end{aligned}$$

令导数等于零, 解方程 $\log_2 \frac{1-p}{p} = 0$, 得到 $p = \frac{1}{2}$.

接下来, 我们来验证 $p = \frac{1}{2}$ 是 $H(p)$ 的最大值点还是最小值点. 我们可以通过二阶导数的符号来判断. 计算二阶导数:

$$\begin{aligned} \frac{d^2 H(p)}{dp^2} &= \frac{d}{dp} \left[\log_2 \frac{1-p}{p} \right] \\ &= \frac{1}{p(p-1) \ln 2} \end{aligned}$$

当 $p = \frac{1}{2}$ 时, $\frac{1}{p(p-1) \ln 2} < 0$, 所以 $p = \frac{1}{2}$ 是 $H(p)$ 的最大值点.

因此, 当 $p = \frac{1}{2}$ 时, $H(p)$ 达到最大值. 选项 (C) $\frac{1}{2}$ 是正确答案.

单选题

若 $H(\xi, \eta) = H(\xi) + H(\eta)$, 则随机变量 ξ 与 η 的关系 ().

- A. ξ 由 η 决定;
- B. η 由 ξ 决定;
- C. ξ 与 η 相互独立.

当两个随机变量 ξ 和 η 相互独立时，它们的联合概率分布可以表示为它们各自的边缘概率分布的乘积，即 $p(\xi, \eta) = p(\xi) \cdot p(\eta)$ 。根据熵的定义，随机变量的熵可以表示为 $H(\xi) = - \sum_X p(x) \log p(x)$ ，其中 x 是随机变量 ξ 的取值。同样地， $H(\eta) = - \sum_Y p(y) \log p(y)$ ，其中 y 是随机变量 η 的取值。当两个随机变量相互独立时，它们的联合熵可以表示为 $H(\xi, \eta) = - \sum_X \sum_Y p(x, y) \log p(x, y)$ 。由于它们相互独立，联合概率分布可以拆分为各自的边缘概率分布的乘积，即 $p(x, y) = p(x) \cdot p(y)$ 。代入联合熵的定义中，我们有：

$$\begin{aligned}
 H(\xi, \eta) &= - \sum_X \sum_Y p(x, y) \log p(x, y) \\
 &= - \sum_X \sum_Y p(x) \cdot p(y) \log(p(x) \cdot p(y)) \\
 &= - \sum_X \sum_Y p(x) \cdot p(y) (\log p(x) + \log p(y)) \\
 &= - \sum_X \sum_Y p(x) \cdot p(y) \log p(x) - \sum_X \sum_Y p(x) \cdot p(y) \log p(y) \\
 &= - \sum_X p(x) \log p(x) - \sum_Y p(y) \log p(y) \\
 &= H(\xi) + H(\eta)
 \end{aligned}$$

因此，当 $H(\xi, \eta) = H(\xi) + H(\eta)$ 时，可以得出 ξ 和 η 是相互独立的。

单选题

$H(\xi, \eta) = H(\xi)$ ，则随机变量 ξ 与 η 的关系 ()。

- A. ξ 由 η 决定；
- B. ξ 与 η 相互独立；
- C. η 由 ξ 决定。

根据题目中的信息 $H(\xi, \eta) = H(\xi)$ ，这意味着给定 ξ 的情况下， η 的条件熵为零，即 $H(\eta|\xi) = 0$ 。这表明在已知 ξ 的情况下， η 是确定的，因此可以得出结论： η 由 ξ 决定。因此，答案是 C. η 由 ξ 决定。

计算题

计算 $H\left(\frac{1}{a}, \frac{1}{a}, \dots, \frac{1}{a}, \frac{2}{a}, \frac{2}{a}\right)$

由 $\sum P_i = 1$ 知, 含 $(a-4)$ 个 $\frac{1}{a}$, 2 个 $\frac{2}{a}$, 总共 $(a-2)$ 项, 于是

$$\begin{aligned}
 H\left(\frac{1}{a}, \frac{1}{a}, \dots, \frac{1}{a}, \frac{2}{a}, \frac{2}{a}\right) &= \sum_{i=1}^{a-2} p_i \cdot \log \frac{1}{p_i} \\
 &= \sum_{i=1}^{a-4} \frac{1}{a} \log a + 2 \cdot \frac{2}{a} \log \frac{a}{2} \\
 &= \frac{a-4}{a} \cdot \log a + \frac{4}{a} \log \frac{a}{2} \\
 &= \frac{a-4}{a} \cdot \log a + \frac{4}{a} \log a - \frac{4}{a} \log 2 \\
 &= \log a - \frac{4}{a} \log 2
 \end{aligned}$$

计算题

设两只口袋中各有 20 个球, 第一支口袋中有 10 个白球, 5 个黑球和 5 个红球; 第二只口袋中有 8 个白球, 8 个黑球和 4 个红球, 从每只口袋中各取一个球, 试判断哪一个结果的不肯定性更大.

当我们要判断哪个结果的不确定性更大时, 可以使用熵来衡量. 首先, 我们将第一只口袋的球的颜色作为随机变量 ξ_1 , 它的概率分布为:

$$\xi_1 \sim \begin{pmatrix} \text{白} & \text{黑} & \text{红} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

其中, $\frac{1}{2}$ 表示白球的概率, $\frac{1}{4}$ 表示黑球的概率, $\frac{1}{4}$ 表示红球的概率.

计算第一只口袋的熵 $H(\xi_1)$:

$$H(\xi_1) = \frac{1}{2} \log 2 + 2 \times \frac{1}{4} \log 4 = \frac{1}{2} + 1 = 1.5 \text{ bits}$$

接下来, 我们将第二只口袋的球的颜色作为随机变量 ξ_2 , 它的概率分布为:

$$\xi_2 \sim \begin{pmatrix} \text{白} & \text{黑} & \text{红} \\ \frac{2}{5} & \frac{2}{5} & \frac{1}{5} \end{pmatrix}$$

其中, $\frac{2}{5}$ 表示白球的概率, $\frac{2}{5}$ 表示黑球的概率, $\frac{1}{5}$ 表示红球的概率.

计算第二只口袋的熵 $H(\xi_2)$:

$$\begin{aligned}
 H(\xi_2) &= \frac{4}{5} \log \frac{5}{2} + \frac{1}{5} \log 5 \\
 &= \frac{4}{5} (\log 5 - \log 2) + \frac{1}{5} \log 5 \\
 &= \frac{4}{5} \log 5 + \frac{1}{5} \log 5 - \frac{4}{5} \\
 &= \log 5 - \frac{4}{5} \approx 2.32 - 0.8 \\
 &= 1.52 \text{ bits}
 \end{aligned}$$

比较 $H(\xi_1)$ 和 $H(\xi_2)$ 的值, 我们可以得出结论: 第二只口袋的结果的不确定性更大, 因为它的熵值更大.

2. 第二次课后作业

单选题

互信息 $I(\xi; \eta) = 0$ 的充分必要条件是随机变量 ξ 与 η 的关系为 ().

- A. η 由 ξ 决定
- B. 相互独立
- C. ξ 由 η 决定

根据互信息与联合熵的关系可知, $I(\xi, \eta) = H(\xi) + H(\eta) - H(\xi, \eta) = 0$, 于是我们有 $H(\xi) + H(\eta) = H(\xi, \eta)$. 由前面知 η 与 ξ 相互独立. 因此, 互信息为零是 ξ 和 η 相互独立的充分必要条件.

填空题

令 ξ 是一个离散随机变量, 它服从的概率分布是 $\bar{p} = (p_1, p_2, \dots, p_a)$, 则 ξ 的熵 $H(\xi) = \underline{\hspace{2cm}}$, 它在 $\underline{\hspace{2cm}}$ 条件下达到最大值, 最大值 = $\underline{\hspace{2cm}}$.

对于离散随机变量 ξ , 其熵 $H(\xi)$ 定义为:

$$H(\xi) = - \sum_{i=1}^a p_i \log p_i$$

其中, p_i 是 ξ 取第 i 个值的概率, a 是 ξ 可能取的值的个数.

当 ξ 的概率分布是均匀分布时, 即所有可能取值的概率相等, 即 $p_i = \frac{1}{a}$, 此时熵 $H(\xi)$ 达到最大值. 在这种情况下, 熵的最大值为:

$$H_{\max} = - \sum_{i=1}^a \frac{1}{a} \log \frac{1}{a} = -a \cdot \frac{1}{a} \log \frac{1}{a} = \log a$$

因此, 当 ξ 的概率分布是均匀分布时, 熵 $H(\xi)$ 达到最大值, 最大值为 $\log a$.

填空题

设 $p(x), q(x)$ 是离散信源 \mathcal{X} 上的两个概率分布, 则它们的互熵 $H(p||q) = 0$ 的充分必要条件是 $\underline{\hspace{2cm}}$.

当 $H(p||q) = 0$ 时, 根据互熵的定义, 我们有:

$$H(p||q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)} = \sum_{x \in \mathcal{X}} p(x) [\log p(x) - \log q(x)] = 0$$

因此, 当且仅当对任意 $q(x) \neq 0$ 的 x , 满足 $p(x) = q(x)$ 时 $H(p||q) = 0$.

填空题

互信息 $I(\xi; \eta)$ 与熵 $H(\xi), H(\eta)$ 及联合熵 $H(\xi, \eta)$ 满足关系式 $\underline{\hspace{2cm}}$.

$$\begin{aligned}
I(\xi; \eta) &= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x)q(y)} \\
&= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) [\log p(x, y) - \log p(x)q(y)] \\
&= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) [\log p(x, y) - \log p(x) - \log q(y)] \\
&= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y) - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x) - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log q(y) \\
&= -H(\xi, \eta) + H(\xi) + H(\eta) = H(\xi) + H(\eta) - H(\xi, \eta)
\end{aligned}$$

即 $I(\xi; \eta) = H(\xi) + H(\eta) - H(\xi, \eta)$.

解答题

令 (ξ, η) 具有如下联合分布

$\xi \backslash \eta$	1	2	3	4
1	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{32}$
2	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{32}$
3	$\frac{1}{8}$	$\frac{1}{8}$	0	0
4	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$

试求: (1) $H(\xi), H(\eta)$; (2) $H(\xi | \eta), H(\eta | \xi)$; (3) $H(\xi, \eta)$; (4) $H(\eta) - H(\eta | \xi)$; (5) $I(\xi; \eta)$.

$\xi \backslash \eta$	1	2	3	4	Σ
1	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{4}$
2	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{4}$
3	$\frac{1}{8}$	$\frac{1}{8}$	0	0	$\frac{1}{4}$
4	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{4}$
Σ	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	1

对 $\xi: p(x) = \sum_{y \in \mathcal{Y}} p(x, y)$, 则有:

$$\begin{aligned}
p(1) &= p(1, 1) + p(1, 2) + p(1, 3) + p(1, 4) = \frac{1}{8} + \frac{1}{16} + \frac{1}{8} + \frac{3}{8} = \frac{3}{8} \\
p(2) &= p(2, 1) + p(2, 2) + p(2, 3) + p(2, 4) = \frac{1}{16} + \frac{1}{8} + \frac{1}{8} + \frac{1}{16} = \frac{3}{8} \\
p(3) &= p(3, 1) + p(3, 2) + p(3, 3) + p(3, 4) = \frac{1}{32} + \frac{1}{32} + 0 + \frac{1}{16} = \frac{1}{8} \\
p(4) &= p(4, 1) + p(4, 2) + p(4, 3) + p(4, 4) = \frac{1}{32} + \frac{1}{32} + 0 + \frac{1}{16} = \frac{1}{8}
\end{aligned}$$

因此 ξ 的边缘分布为 $(\frac{3}{8}, \frac{3}{8}, \frac{1}{8}, \frac{1}{8})$. 同理对 $\eta: p(y) = \sum_{x \in \mathcal{X}} p(x, y)$, 也可求得 η 的边缘分布为

$(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$. 于是

$$\begin{aligned}
 H(\xi) &= \sum_{i=1}^4 p_i \log \frac{1}{p_i} = 2 \cdot \frac{3}{8} \cdot \log_2 \frac{8}{3} + 2 \cdot \frac{1}{8} \cdot \log_2 8 = 3 - \frac{3}{4} \log_2 3 \\
 H(\eta) &= \sum_{i=1}^4 p_i \log \frac{1}{p_i} = 4 \cdot \frac{1}{4} \log_2 4 = 2 \\
 H(\xi, \eta) &= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \cdot \log_2 \frac{1}{p(x, y)} = 4 \cdot \frac{1}{8} \cdot \log_2 8 + 6 \cdot \frac{1}{16} \cdot \log_2 16 + 4 \cdot \frac{1}{32} \log_2 32 \\
 &= \frac{3}{2} + \frac{3}{2} + \frac{5}{8} = \frac{29}{8} \\
 H(\xi | \eta) &= H(\xi, \eta) - H(\eta) = \frac{29}{8} - 2 = \frac{13}{8} \\
 H(\eta | \xi) &= H(\xi, \eta) - H(\xi) = \frac{29}{8} - (3 - \frac{3}{4} \log_2 3) = \frac{5}{8} + \frac{3}{4} \log_2 3 \\
 H(\eta) - H(\eta | \xi) &= 2 - (\frac{5}{8} + \frac{3}{4} \log_2 3) = \frac{11}{8} - \frac{3}{4} \log_2 3 \\
 I(\xi; \eta) &= H(\xi) + H(\eta) - H(\xi, \eta) = 3 - \frac{3}{4} \log_2 3 + 2 - \frac{29}{8} = \frac{11}{8} - \frac{3}{4} \log_2 3
 \end{aligned}$$

解答题

设两只口袋中各有 20 个球，第一支口袋中有 10 个白球，5 个黑球和 5 个红球；第二只口袋中有 8 个白球，6 个黑球和 6 个红球，从每只口袋中各取一个球，试判断哪一个结果的不肯定性更大（已知： $\log_2 5 = 2.322, \log_2 3 = 1.585$ ）。

当我们要判断哪个结果的不肯定性更大时，可以使用熵来衡量。首先，我们将第一只口袋的球的颜色作为随机变量 ξ_1 ，它的概率分布为：

$$\xi_1 \sim \begin{pmatrix} \text{白} & \text{黑} & \text{红} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

其中， $\frac{1}{2}$ 表示白球的概率， $\frac{1}{4}$ 表示黑球的概率， $\frac{1}{4}$ 表示红球的概率。

计算第一只口袋的熵 $H(\xi_1)$ ：

$$H(\xi_1) = \frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 4 + \frac{1}{4} \cdot \log_2 4 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 1.5 \text{ bits}$$

接下来，我们将第二只口袋的球的颜色作为随机变量 ξ_2 ，它的概率分布为：

$$\xi_2 \sim \begin{pmatrix} \text{白} & \text{黑} & \text{红} \\ \frac{2}{5} & \frac{3}{10} & \frac{3}{10} \end{pmatrix}$$

其中， $\frac{2}{5}$ 表示白球的概率， $\frac{3}{10}$ 表示黑球的概率， $\frac{3}{10}$ 表示红球的概率。

计算第二只口袋的熵 $H(\xi_2)$ ：

$$\begin{aligned}
H(\xi_2) &= \frac{2}{5} \log_2 \frac{5}{2} + \frac{3}{10} \log_2 \frac{10}{3} + \frac{3}{10} \log_2 \frac{10}{3} \\
&= \frac{2}{5} (\log_2 5 - 1) + \frac{3}{5} (\log_2 10 - \log_2 3) \\
&= \frac{2}{5} (\log_2 5 - 1) + \frac{3}{5} (1 + \log_2 5 - \log_2 3) \\
&= \log_2 5 - \frac{3}{5} \log_2 3 + \frac{1}{5} \\
&\approx 2.322 - 0.6 \times 1.585 + 0.2 \\
&= 1.571 \text{ bits}
\end{aligned}$$

所以我们得到 $H(\xi_1) = 1.5 < 1.571 = H(\xi_2)$ ，比较 $H(\xi_1)$ 和 $H(\xi_2)$ 的值，我们可以得出结论：第二只口袋的结果的不肯定性更大，因为它的熵值更大。

3. 第三次课后作业

2024-03-11

设 ξ 和 η 联合分布 $p(0,0) = \frac{1}{3}, p(0,1) = \frac{1}{3}, p(1,0) = 0, p(1,1) = \frac{1}{3}$ ，试求：

- (1) $H(\xi), H(\eta)$;
- (2) $H(\xi | \eta), H(\eta | \xi)$;
- (3) $H(\xi, \eta)$;
- (4) $H(\eta) - H(\eta | \xi)$;
- (5) $I(\xi; \eta)$;
- (6) 画出上述各信息之间关系的韦恩图。

$\xi \backslash \eta$	0	1	Σ
0	$\frac{1}{3}$	0	$\frac{1}{3}$
1	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{2}{3}$
Σ	$\frac{2}{3}$	$\frac{1}{3}$	1

$$\Rightarrow \xi \sim \begin{pmatrix} 0 & 1 \\ \frac{2}{3} & \frac{1}{3} \end{pmatrix}, \quad \eta \sim \begin{pmatrix} 0 & 1 \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

(1)

$$H(\xi) = \sum_{i=0}^1 p_i \log_2 \frac{1}{p_i} = \frac{2}{3} \log_2 \frac{3}{2} + \frac{1}{3} \log_2 3 = \frac{2}{3} \log_3 - \frac{2}{3} \log_2 + \frac{1}{3} \log_2 3 = \log_2 3 - \frac{2}{3}$$

$$H(\eta) = \sum_{i=0}^1 p_i \log_2 \frac{1}{p_i} = \frac{1}{3} \log_2 3 + \frac{2}{3} \log_2 \frac{3}{2} = \frac{1}{3} \log_2 3 + \frac{2}{3} \log_2 3 - \frac{2}{3} \log_2 2 = \log_2 3 - \frac{2}{3}$$

(3)

$$H(\xi, \eta) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \frac{1}{p(x, y)} = 3 \cdot \frac{1}{3} \log_2 3 = \log_2 3$$

(2)

$$H(\eta | \xi) = H(\xi, \eta) - H(\xi) = \log_2 3 - \left(\log_2 3 - \frac{2}{3} \right) = \frac{2}{3}$$

$$H(\xi | \eta) = H(\xi, \eta) - H(\eta) = \log_2 3 - \left(\log_2 3 - \frac{2}{3} \right) = \frac{2}{3}$$

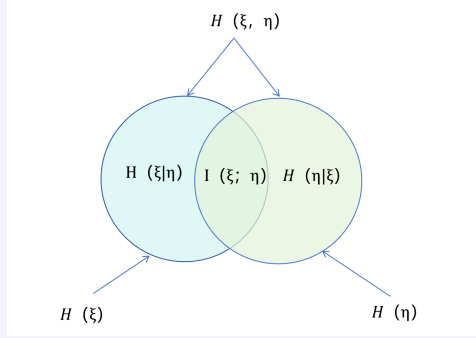
(4)

$$H(\eta) - H(\eta | \xi) = \log_2 3 - \frac{2}{3} - \frac{2}{3} = \log_2 3 - \frac{4}{3}$$

(5)

$$I(\xi; \eta) = H(\xi) + H(\eta) - H(\xi, \eta) = (\log_2 3 - \frac{2}{3}) + (\log_2 3 - \frac{2}{3}) - \log_2 3 = \log_2 3 - \frac{4}{3}$$

(6)



2024-03-11

设 ξ 是取 m 个值 x_1, x_2, \dots, x_m 的随机变量, $p(\xi = x_m) = a$. 证明:

$$H(\xi) = a \log \frac{1}{a} + (1-a) \log \frac{1}{1-a} + (1-a)H(\eta),$$

其中 η 是取 $m-1$ 个值 x_1, x_2, \dots, x_{m-1} 的随机变量.

$$p(\eta = x_j) \stackrel{\text{def}}{=} \frac{p(\xi = x_j)}{(1-a)}, 1 \leq j \leq m-1.$$

进一步, 证明: $H(\xi) \leq a \log \frac{1}{a} + (1-a) \log \frac{1}{a} + (1-a) \log(m-1)$, 并确定其中等号成立的条件.

证明: 由 $p(\eta = x_j) \stackrel{\text{def}}{=} \frac{p(\xi = x_j)}{(1-a)} \Rightarrow p(\xi = x_j) = (1-a)p(\eta = x_j), j = 1, \dots, m-1$.

$$\begin{aligned} \text{故 } H(\xi) &= a \log \frac{1}{a} + \sum_{j=1}^{m-1} p(\xi = x_j) \log \frac{1}{p(\xi = x_j)} \\ &= a \log \frac{1}{a} + \sum_{j=1}^{m-1} (1-a)p(\eta = x_j) \log \frac{1}{(1-a)p(\eta = x_j)} \\ &= a \log \frac{1}{a} + \sum_{j=1}^{m-1} (1-a)p(\eta = x_j) \log \frac{1}{1-a} + \sum_{j=1}^{m-1} (1-a)p(\eta = x_j) \log \frac{1}{p(\eta = x_j)} \\ &= a \log \frac{1}{a} + (1-a) \log \frac{1}{1-a} \sum_{j=1}^{m-1} p(\eta = x_j) + (1-a) \sum_{j=1}^{m-1} p(\eta = x_j) \log \frac{1}{p(\eta = x_j)} \\ &= a \log \frac{1}{a} + (1-a) \log \frac{1}{1-a} + (1-a)H(\eta) \end{aligned}$$

根据熵的最大值定理有 $H(\eta) \leq \log(m-1)$. 因此有

$$H(\xi) \leq a \log \frac{1}{a} + (1-a) \log \frac{1}{a} + (1-a) \log(m-1)$$

等号成立的条件是 $p(\eta = x_j)$ 为等概率分布, 即有

$$p(\eta = x_j) = \frac{1}{m-1}$$

此时

$$p(\xi = x_j) = \frac{1-a}{m-1}, \quad j = 1, 2, \dots, m-1.$$

4. 第四次课后作业

单选题

码 C 是前缀码是码 C 是即时码的 ().

- A. 充分条件
- B. 充分必要条件
- C. 必要条件

(B)

\Leftarrow : 假设 C 是一个码元集, 若 C 不是前缀码, 则存在码字 c_i, c_j , 使得 c_i 是 c_j 的前缀, 在一个含有 c_i 的码字串中, 从左到右, 当 c_i 出现时, 只有当 c_i 后面出现部分, 连同 c_i 不是 c_j 时才能把 c_i 还原; 若 c_i 以及连同后面部分是 c_j 时, 不能把 c_i 还原, 应该把 c_j 还原, 因此 C 不是即时码, 矛盾. 故即时码一定为前缀码.

\Rightarrow : 若 C 不是即时码, 则从左到右, 出现一个码字 c_i , 还原为消息字母时, 依赖于后面的字符串, 即存在另一个码字 c_j , 使得 c_i 是 c_j 的前缀, 从而 C 不是前缀码.

单选题

码字长度为 $\{\ell_1, \ell_2, \dots, \ell_a\}$ 的码为即时码是 $\{\ell_1, \ell_2, \dots, \ell_a\}$ 满足 Kraft 不等式的 ().

- A. 充分条件
- B. 充分必要条件
- C. 必要条件

若 $\ell_1, \ell_2, \dots, \ell_a$ 满足 Kraft 不等式, 则必存在码字长度为 $\ell_1, \ell_2, \dots, \ell_a$ 的即时码. 如果一个码的码字长度满足 Kraft 不等式, 但它不一定是即时码.

如: 考虑二元码 $C = \{0, 11, 100, 110\}$, 码字长度分别为 1, 2, 3, 3, 因为 $|\mathcal{X}| = 2$, 我们有

$$\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} = 1,$$

所以, 它的码字长度满足 Kraft 不等式. 但这个码并不是即时的 (不是前缀码), 因为码字 11 是码字 110 的前缀. 但根据 1, 2, 3, 3 可构造一个即时码, 如 $\{0, 10, 110, 111\}$ 或 $\{1, 01, 001, 000\}$.

因此码字长度为 $\{\ell_1, \ell_2, \dots, \ell_a\}$ 的码为即时码是 $\{\ell_1, \ell_2, \dots, \ell_a\}$ 满足 Kraft 不等式的充分条件.(A)

解答题

下面的码是否是即时码? 是否是唯一可译码?

(1) $C = \{0, 10, 1100, 1101, 1110, 1111\}$.

(2) $C = \{0, 10, 110, 1110, 1011, 1101\}$.

(1) 在这个码集中, 没有任何码字是另一个码字的前缀. 因此, 每个码字的开始都唯一标识了一个码字, 没有歧义, 因此是即时码. 由于是即时码, 它自然也是唯一可译码. 即时码的属性保证了解码过程中的唯一性. 故 C 是前缀码, 是即时码, 是唯一可译码.

(2) C 不是前缀码, 因为码字 10 是码字 1011 的前缀, 故 C 不是即时码. C 不是唯一可译码. 因为根据如下字符串得知: 一个给定的编码序列中可能会解码出两种不同的消息, 表明在这个特定的码集不是唯一可译码.

$$\begin{array}{cccccc} 0 & 10 & 110 & 1110 & 1011 & 1101 \\ \hline a & b & c & d & e & f \\ 0 & 1011 & 0 & 1110 & 1011 & 1101 \\ \hline a & e & a & d & e & f \end{array}$$

解答题

判断是否存在即时码具有以下的基数和码字长度, 如果有, 试构造出一个这样的码.

(1) $r = 2$, 长度: 1, 3, 3, 3, 4, 4.

(2) $r = 3$, 长度: 1, 1, 2, 2, 3, 3, 3.

(3) $r = 5$, 长度: 1, 1, 1, 1, 1, 8, 9.

(1) $r = 2$, 长度: 1, 3, 3, 3, 4, 4.

首先, 我们计算 Kraft 和:

$$\sum_{i=1}^6 2^{-\ell_i} = 2^{-1} + 3 \times 2^{-3} + 2 \times 2^{-4} = 1$$

Kraft 和等于 1, 满足 Kraft 不等式, 因此存在即时码. 下面构造一个即时码:

长度 1 的码字: 0

长度 3 的码字: 100, 101, 110

长度 4 的码字: 1110, 1111

$$\begin{array}{llll} u_{1,1} = 0 & 0 & & \\ u_{3,1,1} = 1 & u_{3,1,2} = 0 & u_{3,1,3} = 0 & (1, 0, 0) \\ u_{3,2,1} = 1 & u_{3,2,2} = 0 & u_{3,2,3} = 1 & (1, 0, 1) \\ u_{3,3,1} = 1 & u_{3,3,2} = 1 & u_{3,3,3} = 0 & (1, 1, 0) \\ u_{4,1,1} = 1 & u_{4,1,2} = 1 & u_{4,1,3} = 1 & u_{4,1,4} = 0 \quad (1, 1, 1, 0) \\ u_{4,2,1} = 1 & u_{4,2,2} = 1 & u_{4,2,3} = 1 & u_{4,2,4} = 1 \quad (1, 1, 1, 1) \end{array}$$

故此即时码为

$$\{0, 100, 101, 110, 1110, 1111\}$$

(2) $r = 3$, 长度: 1, 1, 2, 2, 3, 3, 3.

接下来, 我们计算 Kraft 和:

$$\sum_{i=1}^7 3^{-\ell_i} = 2 \times 3^{-1} + 2 \times 3^{-2} + 3 \times 3^{-3} = \frac{2}{3} + \frac{2}{9} + \frac{3}{27} = \frac{2}{3} + \frac{2}{9} + \frac{1}{9} = 1$$

Kraft 和等于 1, 满足 Kraft 不等式, 因此存在即时码. 下面构造一个即时码:

长度 1 的码字: 0,1

长度 2 的码字: 20,21

长度 3 的码字: 220, 221, 222

$$\begin{array}{lll}
 u_{1,1} = 0 & u_{1,2} = 1 & 0, 1 \\
 u_{2,1,1} = 2 & u_{2,1,2} = 0 & (2, 0) \\
 u_{2,2,1} = 2 & u_{2,2,2} = 1 & (2, 1) \\
 u_{3,1,1} = 2 & u_{3,1,2} = 2 & u_{3,1,3} = 0 \quad (2, 2, 0) \\
 u_{3,2,1} = 2 & u_{3,2,2} = 2 & u_{3,2,3} = 1 \quad (2, 2, 1) \\
 u_{3,3,1} = 2 & u_{3,3,2} = 2 & u_{3,3,3} = 2 \quad (2, 2, 2)
 \end{array}$$

故此即时码为

$$\{0, 1, 20, 21, 220, 221, 222\}$$

(3) 我们计算 Kraft 和:

$$\sum_{i=1}^7 5^{-\ell_i} = 5 \times \frac{1}{5} + \frac{1}{5^8} + \frac{1}{5^9} > 1$$

故这样的即时码不存在.

5. 第五次课后作业

解答题

对下面给定的概率分布和基数, 找出一个 Huffman 编码, 并求平均码长.

$$p = \{0.1, 0.1, \dots, 0.1\}, r = 3.$$

解: 首先确定 k 的值, $a = 10, r = 3$.

$$k = \text{Int}_+ \left(\frac{a-1}{r-1} \right) = \text{Int}_+ \frac{9}{2} = 5.$$

再确定第一列最后几个分量相加: $a - (k-1)r + k - 1 = 10 - (5-1) \times 3 + 5 - 1 = 2$. 从第三列开始每次将最后 r 个分量相加, 并按大小排序放入下一奇数列. 于是我们构造 Huffman 编码为

概率	码	概率	码	概率	码	概率	码	概率	码
0.1	01	0.2	00	0.3	2	0.3	1	0.4	0
0.1	02	0.1	01	0.2	00	0.3	2	0.3	1
0.1	10	0.1	02	0.1	01	0.2	00	0.3	2
0.1	11	0.1	10	0.1	02	0.1	01		
0.1	12	0.1	11	0.1	10	0.1	02		
0.1	20	0.1	12	0.1	12				
0.1	21	0.1	20	0.1					
0.1	22	0.1	21						
0.1	000	0.1	22						
0.1	001								

平均码长:

$$L(\mathcal{S}, f) = 0.8 \times 2 + 0.2 \times 3 = 2.2$$

解答题

对下面给定的概率分布和基数, 找出一个 Huffman 编码, 并求平均码长.

$$p = \{0.3, 0.1, 0.1, 0.1, 0.1, 0.06, 0.05, 0.05, 0.05, 0.04, 0.03, 0.02\}, \quad r = 4.$$

解: 首先确定 k 的值, $a = 12, r = 4$.

$$k = \text{Int}_+ \left(\frac{a-1}{r-1} \right) = \text{Int}_+ \frac{11}{3} = 4.$$

再确定第一列最后几个分量相加: $a - (k-1)r + k - 1 = 12 - (4-1) \times 4 + 4 - 1 = 3$. 从第三列开始每次将最后 $r = 4$ 个分量相加, 并按大小排序放入下一奇数列, 用方框标出. 于是我们构造 Huffman 编码为

概率	码	概率	码	概率	码	概率	码
0.3	1	0.3	1	0.3	1	0.39	0
0.1	3	0.1	3	0.21	2	0.3	1
0.1	00	0.1	00	0.1	3	0.21	2
0.1	01	0.1	01	0.1	00	0.1	3
0.1	02	0.1	02	0.1	01		
0.06	20	0.09	03	0.1	02		
0.05	21	0.06	20	0.09	03		
0.05	22	0.05	21				
0.05	23	0.05	22				
0.04	030	0.05	23				
0.03	031						
0.02	032						

平均码长:

$$L(\mathcal{S}, f) = 0.4 \times 1 + 0.51 \times 2 + 0.09 \times 3 = 1.69$$

解答题

判断是否存在即时码具有以下的基数和码字长度, 如果有, 试构造出一个这样的码. $r = 3$, 长度 1, 1, 2, 4, 4, 5.

我们计算 Kraft 和:

$$\sum_{i=1}^6 3^{-\ell_i} = 2 \times 3^{-1} + 1 \times 3^{-2} + 2 \times 3^{-4} + 1 \times 3^{-5} = \frac{2}{3} + \frac{1}{9} + \frac{2}{81} + \frac{1}{243} = \frac{196}{243} < 1$$

满足 Kraft 不等式, 因此存在即时码. 下面构造一个即时码:

$$\begin{array}{llllll} u_{1,1} = 0 & u_{1,2} = 1 & & & & 0, 1 \\ u_{2,1,1} = 2 & u_{2,1,2} = 0 & & & & (2, 0) \\ u_{4,1,1} = 2 & u_{4,1,2} = 1 & u_{4,1,3} = 0 & u_{4,1,4} = 0 & & (2, 1, 0, 0) \\ u_{4,2,1} = 2 & u_{4,2,2} = 1 & u_{4,2,3} = 0 & u_{4,2,4} = 1 & & (2, 1, 0, 1) \\ u_{5,1,1} = 2 & u_{5,1,2} = 1 & u_{5,1,3} = 1 & u_{5,1,4} = 0 & u_{5,1,5} = 0 & (2, 1, 1, 0, 0) \end{array}$$

故此即时码为

$$\{0, 1, 20, 21, 2100, 2101, 21100\}$$

解答题

对下面给定的概率分布和基数, 找出一个 Huffman 编码, 并求平均码长.

$$p = \{0.3, 0.2, 0.2, 0.1, 0.1, 0.1\}, \quad r = 2.$$

解: 首先确定 k 的值, $a = 6, r = 2$.

$$k = \text{Int}_+ \left(\frac{a-1}{r-1} \right) = \text{Int}_+ \frac{5}{1} = 5.$$

再确定第一列最后几个分量相加: $a - (k-1)r + k - 1 = 6 - (5-1) \times 2 + 5 - 1 = 2$. 从第三列开始每次将最后 $r = 2$ 个分量相加, 并按大小排序放入下一奇数列, 用方框标出. 于是我们构造 Huffman 编码为

概率	码	概率	码	概率	码	概率	码	概率	码
0.3	01	0.3	01	0.3	00	0.4	1	0.6	0
0.2	11	0.2	10	0.3	01	0.3	00	0.4	1
0.2	000	0.2	11	0.2	10	0.3	01		
0.1	001	0.2	000	0.2	11				
0.1	100	0.1	001						
0.1	101								

平均码长:

$$L(\mathcal{S}, f) = 0.5 \times 2 + 0.5 \times 3 = 2.5$$

判断题

无噪声信道的容量是 $\log a$, 其中 a 是输入字母表的大小.

对. 无噪声信道等价条件是, 存在一个 $\mathcal{U} \rightarrow \mathcal{V}$ 的 $1-1$ 映射 ϕ , 使得 $p(\phi(u) | u) = 1$ 对所有 u 成立, 从而 $a = b$. 因此 $C = \log a = \log b$.

判断题

无用信道的容量是 0 .

对. 无用信道意味着输出不依赖于输入, 或者说输出对于输入的选择完全没有信息. 在这种情况下, 无论输入是什么, 输出的分布都保持不变, 因此 $H(\eta|\xi) = H(\eta)$. $I(\xi;\eta) = H(\xi) - H(\xi | \eta) = H(\xi) - H(\xi) = 0$. (注意 ξ 与 η 是相互独立的.)

判断题

无丢失信道的容量是 $\log a$, 其中 a 是输入字母表的大小.

对. 因 ξ 完全由 η 决定, 即 $H(\xi | \eta) = 0$.

$$I(\xi;\eta) = H(\xi) - H(\xi | \eta) = H(\xi) - 0 = H(\xi) \leq \log a$$

$H(\xi)$ 的最大值 $\log a$.

解答题

写出二元对称信道的信道矩阵, 并利用信道容量的定义求它的信道容量.

记输入输出字母表 $\mathcal{U} = \mathcal{V} = \{0, 1\}$. 信道转移概率分布为

$$p(0 | 1) = p(1 | 0) = p, p(0 | 0) = p(1 | 1) = 1 - p$$

则二元对称信道的信道矩阵如下所示:

$$\begin{array}{cc} & \begin{matrix} 0 & 1 \end{matrix} \\ \begin{matrix} 0 \\ 1 \end{matrix} & \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \end{array}$$

下面利用信道容量的定义求它的信道容量.

$$C = \max \{I(\xi;\eta) | \xi \in \mathcal{P}_{\mathcal{U}}\} = \max \{H(\eta) - H(\eta | \xi) | \xi \in \mathcal{P}_{\mathcal{U}}\}$$

设入口分布为 (p_0, p_1) , 对应的出口分布为 (q_0, q_1) , 则

$$(q_0, q_1) = (p_0, p_1) \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} = (p_0(1-p) + p_1p, \quad p_0p + p_1(1-p))$$

不妨设 $p_0 = \theta$, 则 $p_1 = 1 - \theta, 0 \leq \theta \leq 1$.

$$\begin{aligned} q_0 &= \theta(1-p) + (1-\theta)p = \theta + p - 2\theta p \\ q_1 &= \theta p + (1-\theta)(1-p) = 1 - \theta - p + 2\theta p \\ H(\eta) &= -q_0 \log_2 q_0 - q_1 \log_2 q_1 \\ &= -q_0 \log_2 q_0 - (1-q_0) \log_2 (1-q_0) \\ &= H(q_0) \end{aligned}$$

根据熵函数的性质 q_0 取 $\frac{1}{2}$ 时 $H(\eta)$ 最大且取值为 1, 此时 $q_0 = \theta + p - 2\theta p = \frac{1}{2}$, 化简即得 $\theta = \frac{1}{2}$. 由于

$$\begin{aligned} H(\eta | \xi = 0) &= p(0|0) \log \frac{1}{p(0|0)} + p(1|0) \log \frac{1}{p(1|0)} \\ &= (1-p) \log \frac{1}{1-p} + p \log \frac{1}{p} = H(p) \\ H(\eta | \xi = 1) &= p(0|1) \log \frac{1}{p(0|1)} + p(1|1) \log \frac{1}{p(1|1)} \\ &= p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p} = H(p). \end{aligned}$$

所以

$$H(\eta | \xi) = \sum_{u \in \mathcal{U}} p(u) H(\eta | \xi = u) = \sum_{u \in \mathcal{U}} p(u) H(p) = \left(\sum_{u \in \mathcal{U}} p(u) \right) H(p) = H(p)$$

因此二元对称信道的信道容量为

$$C = \max \{H(\eta) - H(\eta | \xi)\} = 1 - H(p)$$

解答题

考虑离散无记忆信道 $Y = (X + Z) \bmod 11$, 其中

$$Z = \begin{pmatrix} 1 & 2 & 3 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

$X \in \{0, 1, \dots, 10\}$. 假设 X 和 Z 独立.

- (1) 求这个信道的容量.
- (2) 找出达到信道容量的输入分布.

(1) $Y = (X + Z) \bmod 11$, 输入为 X , 输出为 Y, Z 为噪声信道, 而 $Z = \begin{pmatrix} 1 & 2 & 3 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$, $X \in \{0, 1, \dots, 10\}$. 所以 $Y \in \{0, 1, \dots, 10\}$,

因为 Z 可以取三个值 $(1, 2, 3)$, 每个都有 $\frac{1}{3}$ 的概率, 所以对于每个 X 的值, Y 可以是三个可能的结果之一, 这取决于 Z 的值. 信道矩阵 $P(Y | X)$ 将具有 11 行 (对应于 X 的可能值) 和 11 列 (对应于 Y 的可能值). 每个元素 P_{ij} 表示给定输入 $X = i$ 时输出 $Y = j$ 的概率.

由于 Z 的作用是加在 X 上然后对 11 取模, 每个 X 值将映射到三个不同的 Y 值, 每个的概率都是 $\frac{1}{3}$. 例如, 如果 $X = 0$, 则 Y 可以是 1, 2 或 3, 每个都有 $\frac{1}{3}$ 的概率, 因为 Z 分别加 1, 2 或 3. 因此, 信道矩阵的一般形式将是每行有三个 $\frac{1}{3}$ 的条目, 分别对应于 X 加上 1, 2, 3 和模 11 的结果, 而其他位置为 0. 对于 $X = 0: Y$ 的可能值是 1, 2, 3, 每个概率为 $\frac{1}{3}$. 对于 $X = 1: Y$ 的可能值是

2, 3, 4, 每个概率为 $\frac{1}{3}$. 以此类推, 直到 $X = 10$. 每行的具体值会随着 X 的增加而“滚动”, 并在达到 10 并绕回 0 时循环. 这种模式的重复构成了完整的信道矩阵:

$$\begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{array} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} \end{pmatrix}$$

得到一个对称信道, 在这种情况下,

$$H(Y | X) = H(Z | X) = H(Z) = \left(\frac{1}{3} \log 3 + \frac{1}{3} \log 3 + \frac{1}{3} \log 3 \right) = \log 3,$$

与 X 的分布无关, 因此信道的容量为

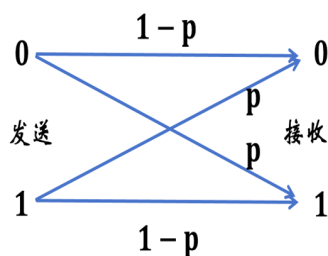
$$\begin{aligned} C &= \max_{p(x)} I(X; Y) = \max_{p(x)} H(Y) - H(Y | X) \\ &= \max_{p(x)} H(Y) - \log 3 \\ &= \log 11 - \log 3 = \log \frac{11}{3} \end{aligned}$$

(2) 当 Y 具有均匀分布时达到最大值, 根据对称性知道, 这发生在 X 具有均匀分布时, 即

$$p(X) = \frac{1}{11}, \quad X \in \{0, 1, \dots, 10\}.$$

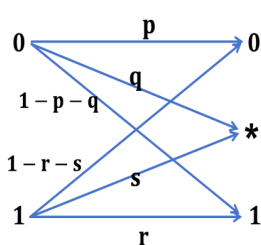
解答题

写出二元对称信道, 二元擦除信道及 M 信道的信道矩阵.



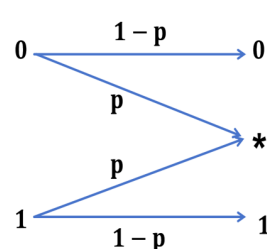
$$\begin{array}{c} 0 \\ 1 \end{array} \begin{pmatrix} 0 & 1 \\ 1-p & p \\ p & 1-p \end{pmatrix}$$

(a) 二元对称信道



$$\begin{array}{c} 0 \\ 1 \end{array} \begin{pmatrix} 0 & * & 1 \\ p & q & 1-p-q \\ 1-r-s & s & r \end{pmatrix}$$

(b) 二元擦除信道



$$\begin{array}{c} 0 \\ 1 \end{array} \begin{pmatrix} 0 & * & 1 \\ 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix}$$

(c) M 信道

解答题

写出二元对称信道的信道矩阵, 并利用极值法求它的信道容量.

二元对称信道的信道矩阵为 $\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$. 设入口分布为 (p_0, p_1) , 对应的出口分布为 (q_0, q_1) , 则 $(q_0, q_1) = (p_0, p_1) \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} = (p_0(1-p) + p_1 \cdot p, p_0p + (1-p)p_1)$

$$\begin{aligned} C &= \sum_{j=1}^b p(v_j | y_i) \log \frac{p(v_j | u_i)}{q(v_j)} \\ &= (1-p) \log \frac{1-p}{q_0} + p \log \frac{p}{q_1} \\ &= p \log \frac{p}{q_0} + (1-p) \log \frac{1-p}{q_1} \end{aligned}$$

展开有 $\log \frac{1-p}{q_0} - p \log \frac{1-p}{q_0} + p \log \frac{p}{q_1} = p \log \frac{p}{q_0} + \log \frac{1-p}{q_1} - p \log \frac{1-p}{q_1}$

$$\begin{aligned} \log \frac{q_1}{q_0} + p \log \frac{q_0}{q_1} + p \log \frac{q_0}{q_1} &= 0 \\ (2p-1) \log \frac{q_0}{q_1} &= 0 \end{aligned}$$

则 $p = \frac{1}{2}$ 或 $q_0 = q_1$. 由 $q_0 = q_1$ 知 $p_0(1-p) + p_1 - p = p_0p + (1-p)p_1 \Rightarrow p = \frac{1}{2}$ 或 $p_1 = p_0$. 由 $p_0 + p_1 = 1$ 知 $p_0 = p_1 = \frac{1}{2}$ 进而 $q_0 = q_1 = \frac{1}{2}$ 于是

$$\begin{aligned} C &= p \log \frac{p}{\frac{1}{2}} + (1-p) \log \frac{1-p}{\frac{1}{2}} \\ &= p \log 2p + (1-p) \log 2(1-p) \\ &= p + p \log p + 1 - p + (1-p) \log(1-p) \\ &= 1 + p \log p + (1-p) \log(1-p) \\ &= 1 - H(p) \end{aligned}$$

解答题

写出 M 信道的信道矩阵, 并利用极值法求它的信道容量.

M 信道的信道矩阵为 $\begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix}$. 设入口分布为 (p_0, p_1) , 对应的出口分布为 (q_0, q_1, q_2) ,

且 $q(v_j) = \sum_{i=1}^a p(u_i) p(v_j | u_i)$ 则有

$$(q_0, q_1, q_2) = (p_0, p_1) \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix} = (p_0(1-p), (p_0+p_1)p, p_1(1-p))$$

$$\begin{aligned} C &= \sum_{j=1}^b p(v_j | u_i) \log \frac{p(v_j | u_i)}{\sum_{l=1}^a p(u_l) p(y_j | u_l)} \\ &= \sum_{j=1}^b p(v_j | u_i) \log \frac{p(v_j | u_i)}{q(v_j)} \\ &= (1-p) \cdot \log \frac{1-p}{q_0} + p \log \frac{p}{p_i} \\ &= p \log \frac{p}{q_1} + (1-p) \cdot \log \frac{1-p}{q_2} \end{aligned}$$

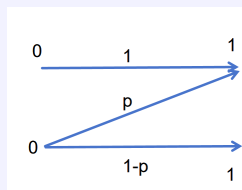
根据上面等式, 比对后有 $(1-p) \log \frac{1-p}{q_0} = (1-p) \cdot \log \frac{1-p}{q_2}$. 即得 $q_0 = q_2$.

于是 $p_0(1-p) = p_1(1-p) \Rightarrow p_0 = p_1$ 由 $p_0 + p_1 = 1$ 知 $p_0 = p_1 = \frac{1}{2}$, 则 $q_0 = p_0(1-p) = \frac{1-p}{2}$. 同理 $q_1 = p, q_2 = \frac{1-p}{2}$, 将 q_0, q_1, q_2 的值代入等式中, 于是

$$\begin{aligned} C &= p \log \frac{p}{q_1} + (1-p) \log \frac{1-p}{q_2} \\ &= p \log \frac{p}{p} + (1-p) \log \frac{1-p}{\frac{1-p}{2}} \\ &= (1-p) \log 2 = 1-p \end{aligned}$$

解答题

Z 信道如下图所示, 写出它的信道矩阵并求其信道容量.



信道矩阵为 $\begin{pmatrix} 1 & 0 \\ p & 1-p \end{pmatrix}$. 设入口分布为 (p_0, p_1) , 对应的出口分布为 (q_0, q_1) , 则

$$(q_0, q_1) = (p_0, p_1) \begin{pmatrix} 1 & 0 \\ p & 1-p \end{pmatrix} = (p_0 + p_1 p, p_1(1-p))$$

$$\begin{aligned} c &= \sum_{j=1}^b p(v_j | v_i) \log \frac{p(v_j | u_i)}{q(v_j)} \\ &= 1 \cdot \log \frac{1}{q_0} \\ &= p \cdot \log \frac{p}{q_0} + (1-p) \log \frac{1-p}{q_1} \end{aligned}$$

根据等式有 $-\log q_0 = p \cdot \log \frac{p}{q_0} + (1-p) \cdot \log \frac{1-p}{q_1}$

$$-\log q_0 = p \log p - p \log q_0 + (1-p) \log(1-p) - (1-p) \log q_1$$

$$H(p) = (1-p) \log \frac{q_0}{q_1}$$

于是 $\frac{q_0}{q_1} = e^{\frac{H(p)}{1-p}}$. 由于 $q_0 + q_1 = 1$, 所以 $\frac{1-q_1}{q_1} = e^{\frac{H(p)}{1-p}}$, 令 $\lambda = \frac{H(p)}{1-p}$ 解得 $q_1 = \frac{1}{1+e^\lambda}$, 则 $q_0 = \frac{e^\lambda}{1+e^\lambda}$

$$\begin{aligned} C &= \log \frac{1}{q_0} = \log \frac{1+e^\lambda}{e^\lambda} = \log \left(1 + \frac{1}{e^\lambda} \right) \\ &= \log \left(1 + e^{-\frac{H(p)}{1-p}} \right) \end{aligned}$$

6. 第八次课后作业

选择题

设 C 是一个 q 元 (n, M, d) 码, 则 C 的码率是 ()

- A. $\frac{M}{n}$ B. $\frac{\log_q M}{n}$

对于一个 q 元 (n, M, d) 码, 其中 n 为码字长度, M 为码字个数, d 为最小距离, 码率 $R(C)$ 定义为有效信息位与总位数之比, 即 $R(C) = \frac{k}{n}$, 其中 $k = \log_q M$ 为每个码字中的有效信息位数. 因此, 码率 $R(C)$ 可表示为 $R(C) = \frac{\log_q M}{n}$, 选项 B. $\frac{\log_q M}{n}$ 是正确的.

选择题

设二元码 $C = \{1100, 0101, 1010\}$, 则码 C 的最小距离是 ()

- A.1 B.2 C.3

对于二元码 $C = \{1100, 0101, 1010\}$, 我们需要计算所有可能的码字对之间的 Hamming 距离, 并找出最小的距离. 给定码 C , 我们可以计算得到: $d(1100, 0101) = 2$, $d(1100, 1010) = 2$, $d(0101, 1010) = 4$. 因此, 码 C 的最小距离为 $d(C) = 2$. 所以选项 B.2 是正确的.

选择题

设 C 是一个二元 $(5, 4, 3)$ 码, 则 C 至多可纠正的错误个数 ()

- A.1 B.2 C.3

对于一个二元 (n, M, d) 码, 其最大可纠正的错误个数为 $t = \lfloor \frac{d-1}{2} \rfloor$. 在这里, $d = 3$, 所以最大可纠正的错误个数为 $t = \lfloor \frac{3-1}{2} \rfloor = 1$.

因此, C 是一个二元 $(5, 4, 3)$ 码, 至多可纠正的错误个数为 1, 选项 A.1 是正确的.

(定理: 码 C 至多可纠正 t 个错误的充分必要条件为 $d(C) = 2t + 1$ 或 $d(C) = 2t + 2$.)

选择题

设 C 是一个二元 $(7, 16, 3)$ 码 (如三阶二元 Hamming 码), 则 C 至多可检查的错误个数是 ()

- A.1 B.2 C.3

根据定理: 码 C 至多可检查 t 个错误的充分必要条件为 $d(C) = t + 1$.

因此, 对于二元 $(7, 16, 3)$ 码, 至多可检查的错误个数为 2, 选项 B.2 是正确的.

解答题

设 $C = \{11100, 01001, 10010, 00111\}$ 是一个二元 $(5, 4)$ 码

(1) 求码 C 的最小距离.

(2) 根据最小距离译码原则, 对接收到的字 10000, 01100, 00100 分别进行译码.

(3) 计算码 C 的码率.

(1) 要求码 C 的最小距离, 我们需要计算所有可能的码字对之间的 Hamming 距离, 并找出最小的距离. 给定码 $C = \{11100, 01001, 10010, 00111\} \subset V(5, 4)$, 令 $x_1 = 11100, x_2 = 01001, x_3 = 10010, x_4 = 00111$. 我们可以计算得到:

$$d(x_1, x_2) = 3, d(x_1, x_3) = 3, d(x_1, x_4) = 4$$

$$d(x_2, x_3) = 4, d(x_2, x_4) = 3, d(x_3, x_4) = 3$$

因此 $d(C) = \min \{d(x_i, x_j) \mid x_i, x_j \in C, x_i \neq x_j, i, j = 1, 2, 3, 4\} = 3$

(2) 根据最小距离译码原则, 我们选择收到的字与码 C 中距离最近的码字进行译码. 对于接收到的字 10000: 设 $x = 10000$, 则

$$d(x, x_1) = 2, d(x, x_2) = 3, d(x, x_3) = 1, d(x, x_4) = 4$$

因此将 x 译为 x_3 , 即接收到的字 10000 应当译码为 10010

对于接收到的字 01100: 设 $y = 01100$, 则

$$d(y, x_1) = 1, d(y, x_2) = 2, d(y, x_3) = 4, d(y, x_4) = 3$$

因此将 y 译为 x_1 . 即 $01100 \rightarrow 11100$

对于接收到的字 00100: 设 $z = 00100$, 则 $d(z, x_1) = 2, d(z, x_2) = 3, d(z, x_3) = 3, d(z, x_4) = 2$ 因此将 z 译为 x_1 或 x_4 , 即 $00100 \rightarrow 11100$ 或 $00100 \rightarrow 00111$

(3) 对于二元 $(5, 4)$ 码 C , 其中 $M = 4$ (共有 4 个码字), $n = 5$ (每个码字长度为 5 位). 根据码率公式 $R(C) = \frac{\log_2 M}{n}$, 我们有:

$$R(C) = \frac{\log_2 4}{5} = \frac{2}{5}$$

因此, 码 C 的码率为 $\frac{2}{5}$.

解答题

设 $C = \{00000000, 00001111, 00110011, 00111100\}$ 是一个二元 $(8, 4)$ 码.

(1) 计算码 C 中不同码字的 Hamming 距离和码 C 的最小距离.

(2) 在一个二进制中, 如果把某一个码字中的 0 和 1 互换, 即将 0 换为 1, 1 换为 0, 则我们将所得的字称为原码字的补. 一个二进制的所有码字的补构成的集合称为原码的补码. 求码 C 的补码, 并求补码中所有不同码字之间的 Hamming 距离和补码的最小距离. 它们与 (1) 中的结果有什么关系?

(3) 将 (2) 中的结果推广到一般的二进制.

(1) 令 $x_1 = 00000000, x_2 = 00001111, x_3 = 00110011, x_4 = 00111100$

$$d(x_1, x_2) = 4, d(x_1, x_3) = 4, d(x_1, x_4) = 4$$

$$d(x_2, x_3) = 4, d(x_2, x_4) = 4, d(x_3, x_4) = 4$$

因此 $d(C) = 4$

(2) 设补码 $\bar{C} = \{11111111, 11100000, 11001100, 11000011\}$, \bar{C} 中的码字分别记作 y_1, y_2, y_3, y_4 , 则

$$d(y_1, y_2) = 4, d(y_1, y_3) = 4, d(y_1, y_4) = 4$$

$$d(y_2, y_3) = 4, d(y_2, y_4) = 4, d(y_3, y_4) = 4$$

因此 $d(\bar{C}) = 4$, 对比 (1) 可知, C 的补码中码字间的 Hamming 距离与 C 相对应的码字间 Hamming 距离相同且 C 的补码的最小距离与 C 的最小距离相同.

(3) 对于一般的二进制, 任取原码中两个不同码字 $x = x_1x_2 \dots x_n$ 和 $y = y_1y_2 \dots y_n$, 其补码分别为 $\bar{x} = \bar{x}_1\bar{x}_2 \dots \bar{x}_n$ 和 $\bar{y} = \bar{y}_1\bar{y}_2 \dots \bar{y}_n$. 其中 $x_i, y_i \in \{0, 1\}$, $\bar{x}_i = 1 - x_i$, $\bar{y}_i = 1 - y_i$. $i = 1, 2, \dots, n$. 原码 x 和 y 之间的 Hamming 距离为 $d(x, y) = \sum_{i=1}^n |x_i - y_i|$, 补码 \bar{x} 和 \bar{y} 之间的 Hamming 距离为 $d(\bar{x}, \bar{y}) = \sum_{i=1}^n |\bar{x}_i - \bar{y}_i| = \sum_{i=1}^n |(1 - x_i) - (1 - y_i)| = \sum_{i=1}^n |y_i - x_i| = d(x, y)$. 因此, 原码 x 和 y 之间的 Hamming 距离与其补码 \bar{x} 和 \bar{y} 之间的 Hamming 距离相等. 根据 x, y 的任意性进而得知而补码的最小距离与原码的最小距离相同.

7. 第八次课后作业

填空题

码 C 至多可纠正 t 个错误的充分必要条件是码 C 的最小距离 $d(C) = \underline{\hspace{2cm}}$.

定理：码 C 至多可纠正 t 个错误的充分必要条件为 $d(C) = 2t + 1$ 或 $d(C) = 2t + 2$.

填空题

对于任意二元 $(3, M, 2)$ 码, 一定有 $M \leq \underline{\hspace{2cm}}$.

使用 Singleton 界定理可以帮助我们确定编码理论中线性码的一个上界. Singleton 界定理指出, 对于任意的 q -元 (n, M, d) 码, 其码长为 n 、码字数为 M 以及最小汉明距离为 d , 我们有:

$$M \leq q^{n-d+1}$$

对于一个二元 $(3, M, 2)$ 码, 其中 $q = 2$ (因为是二进码)、 $n = 3$ (码字长度为 3) 和 $d = 2$ (最小汉明距离为 2), 因此

$$M \leq 2^{3-2+1} = 2^2 = 4$$

填空题

设二元 $[4, 2]$ 线性码 $L = \{0000, 1100, 0011, 1111\}$, 则 L 的最小距离为 $\underline{\hspace{2cm}}$.

为了找出给定的二元线性码 $L = \{0000, 1100, 0011, 1111\}$ 的最小距离, 我们需要计算码集中任意两个不同码字之间的汉明距离, 然后找出这些距离中的最小值.

汉明距离是指两个码字在相应位上不同的位数. 对于线性码, 最小距离也可以通过找出除了零码字以外的码字的最小重量 (即非零位的数量) 来得到, 因为线性码的任意两个码字的差也是该码中的一个码字.

我们用两种方法分别来计算:

1. 码字重量分析:

0000 的重量为 0 (无需考虑, 因为我们寻找的是非零码字的最小重量).

1100 的重量为 2.

0011 的重量为 2.

1111 的重量为 4.

2. 码字间的汉明距离:

从 0000 到 1100, 距离为 2.

从 0000 到 0011, 距离为 2.

从 0000 到 1111, 距离为 4.

从 1100 到 0011, 距离为 4.

从 1100 到 1111, 距离为 2.

从 0011 到 1111, 距离为 2.

由上面的计算可见, 码字之间的最小汉明距离是 2, 这也是该码的最小距离. 因此, 给定的二元线性码 L 的最小距离为 2.

填空题

对于任意 $n \geq 1$, $A_q(n, n) = \underline{\hspace{2cm}}$.

设 C 是一个 q 元 (n, M, n) 码, 则 $\forall x, y \in C, x = (x_1, \dots, x_n), y = (y_1, \dots, y_n), x_i \neq y_i, i = 1, \dots, n$, 因此, 所有码字在一个固定分量位置上出现的字符一定互不相同, 于是 $M \leq q$. 由此可知 $A_q(n, n) \leq q$, 又码长为 n 的 q 元重复码是一个 q 元 (n, q, n) 码, 故 $A_q(n, n) = q$.

解答题

- (1) 证明: 对任意三元 $(3, M, 2)$ 码, 一定有 $M \leq 9$.
 (2) 证明: 三元 $(3, 9, 2)$ 码一定存在. 于是, $A_3(3, 2) = 3^2$.
 (3) 证明: $A_q(3, 2) = q^2$, 其中 $q \geq 2, q$ 是素数的幂次方.

(1) 对于任意的三元 $(3, M, 2)$ 码, 根据 Singleton 界, $A_q(n, d) \leq q^{n-d+1}$, 将 $n = 3, d = 2, q = 3$ (因为是三元码, 所以 $q = 3$) 代入上述公式: $A_3(3, 2) \leq 3^{3-2+1} = 3^2 = 9$. 这表明在保证任意两个码字之间的汉明距离至少为 2 的情况下, 码字总数 M 不能超过 9. 因此, 任何 $(3, M, 2)$ 码的码字数量 M 最大为 9, 这就证明了 $M \leq 9$.

(2) 为了证明, 我们需要构造一个具体的 $(3, 9, 2)$ 码. 考虑以下码集 C :

$$C = \{000, 111, 222, 012, 021, 120, 102, 210, 201\}$$

这 9 个码字确保了任意两个码字之间的汉明距离至少为 2. 由于我们找到了一个有效的 $(3, 9, 2)$ 码, 因此 $A_3(3, 2) \geq 9$. 结合前面的 Singleton 界结果 $A_3(3, 2) \leq 9$, 可以断定 $A_3(3, 2) = 9$.

(3) 使用 Singleton 界:

$$A_q(3, 2) \leq q^{3-2+1} = q^2$$

我们需要构造一个 q 元 $(3, q^2, 2)$ 码来证明存在性. 考虑码集:

$$C = \{(a, b, a+b) \mid a, b \in \mathbb{F}_q\}$$

其中 \mathbb{F}_q 是有 q 个元素的有限域. 这种构造中, 每个码字形式为 $(a, b, a+b)$, 其中每个 a 和 b 可以独立选择, 因此共有 q^2 个码字. 即 $|C| = q^2$. 由于对于任何两个不同的码字 $(a, b, a+b)$ 和 $(a', b', a'+b')$, 至少在两个坐标上有不同 (如果 $a \neq a'$ 那么 $a+b \neq a'+b'$), 所以这种码的最小汉明距离 $d(C) = 2$. 因此, $A_q(3, 2) = q^2$.

解答题

试说明对于二元重复码 $C = \{00 \dots 0, 11 \dots 1\}$, 它是一个二元 $(n, 2, n)$ 码, 当 n 为奇数时, C 是完备码. 另外, 只含一个码字的码以及由 $V(n, q)$ 构成的 q 元 $(n, q^n, 1)$ 码都是完备码.

设 C 是一个 q 元 $(n, M, 2t+1)$ 码. 如果

$$M \left\{ \binom{n}{0} + \binom{n}{1} (q-1) + \binom{n}{2} (q-1)^2 + \dots + \binom{n}{t} (q-1)^t \right\} = q^n,$$

则称 C 为完备码 (perfect code).

(1) 对于码长为 n 的二元重复码

$$\begin{aligned}
 C_1 &= \{\underbrace{00 \cdots 0}_n, \underbrace{11 \cdots 1}_n\}. \\
 &2 \left\{ \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right\} \\
 &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{l} + \binom{n}{t+1} + \cdots \\
 &\quad + \binom{n}{n-2} + \binom{n}{n-1} + \binom{n}{n} \\
 &= (1+1)^n \\
 &= 2^n.
 \end{aligned}$$

因此, 当码长 n 为奇数时, 二元重复码 C_1 是一个完备的 $(n, 2, n)$ 码.

(2) 对于只含有一个码字的码 $C_2 = \{x\} \subset V(n, q)$, 当在信道发送端发送码字 x 后, 在信道接收端不管接收到什么向量都将译为码字 x . 这就是说, 码 C_2 可以检查和纠正码字在信道传输过程中发生的任何数目的错误. 因此, 码 C_2 可纠正的错误数目为 $t = n$. 显然,

$$\begin{aligned}
 &\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{n}(q-1)^n \\
 &= (1 + (q-1))^n \\
 &= q^n.
 \end{aligned}$$

因此, 只含有一个码字的码 C_2 是完备码.

(3) 对于码 $C_3 = V(n, q)$, 其码字个数为 q^n . 最小距离为 1, 可纠正的错误数目为 $t = 0$. 显然, 对于 q 元 $(n, q^n, 1)$ 码 C_3 . 满足定义. 因此, $C_3 = V(n, q)$ 是完备码.

解答题

对于任意 $n \geq 1$, 试确定 $A_q(n, n)$.

设 C 是一个 q 元 (n, M, n) 码, 则 C 中任意两个不同的码字 \mathbf{x} 和 \mathbf{y} 的 Hamming 距离都是 n , 也就是说, \mathbf{x} 和 \mathbf{y} 的 n 个分量一定互不相同. 于是, 对于任意一个分量位置 i , C 中 M 个码字的第 i 个分量一定互不相同. 因此, $M \leq q$. 另一方面, 我们已经知道码长为 n 的 q 元重复码是一个 (n, q, n) 码. 因此, $A_q(n, n) = q$.

解答题

试说明对于二元重复码 $C = \{00 \cdots 0, 11 \cdots 1\}$, 它是一个二元 $(n, 2, n)$ 码, 当 n 为奇数时, C 是完备码. 另外, 只含一个码字的码以及由 $V(n, q)$ 构成的 q 元 $(n, q^n, 1)$ 码都是完备码.

(1) 二元重复码 $C = \{00 \cdots 0, 11 \cdots 1\}$ 是一个二元 $(n, 2, n)$ 码, 当 n 为奇数时, C 是完备码.

二元重复码 C 包含两个码字: 全 0 和全 1, 每个码字长度为 n . 最小汉明距离 $d = n$ 是因为两个码字在每个位上都不同.

验证完备码条件: 完备码的定义要求:

$$M \left(\sum_{i=0}^t \binom{n}{i} \right) = 2^n,$$

其中 $M = 2$ 是码字数量, $t = \frac{n-1}{2}$.

由于二项式定理给出:

$$\sum_{i=0}^n \binom{n}{i} = 2^n,$$

利用对称性, 当 n 为奇数时:

$$\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} = \sum_{i=\frac{n+1}{2}}^n \binom{n}{i},$$

因此,

$$2 \left(\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} \right) = 2^n,$$

满足完备码的条件. 因此, 当 n 为奇数时, 二元重复码 C 是完备码.

(2) 只含一个码字的码 $C_2 = \{x\}$ 以及由 $V(n, q)$ 构成的 q 元 $(n, q^n, 1)$ 码都是完备码.

只含一个码字的码 C_2 : 任何接收的向量都被解释为唯一的码字 x . 纠正的错误数目 $t = n$ (最大可能的错误数目).

完备码条件为:

$$\left(\sum_{i=0}^n \binom{n}{i} (q-1)^i \right) = q^n.$$

由于二项式定理, 上式变为 $(1 + (q-1))^n = q^n$, 显然满足. 因此 C_2 是完备码.

(3) 由 $V(n, q)$ 构成的 q 元 $(n, q^n, 1)$ 码 C_3 : 包括所有 n -维向量, 错误纠正个数 $t = 0$. 由于覆盖了整个 n -维空间, 满足完备码条件, 即有 $q^n = q^n$, 所以 C_3 也是完备码.

填空题

设二元 $[4, 2]$ 线性码 $L = \{0000, 1100, 0011, 1111\}$, 则 L 的对偶码为 ____.

一个线性码 L 的对偶码 L^\perp 定义为所有与 L 中所有码字正交的码字的集合. 对于一个二码, 如果两个码字 $x = (x_1, x_2, \dots, x_n)$ 和 $y = (y_1, y_2, \dots, y_n)$ 的点积 $x \cdot y = x_1y_1 + x_2y_2 + \dots + x_ny_n = 0$ (模 2 计算), 则这两个码字正交.

对于给定的线性码 $L = \{0000, 1100, 0011, 1111\}$, 我们需要找到所有与 L 中每个码字都正交的码字构成的集合 L^\perp .

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

L 的生成矩阵为 $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.

$L^\perp = \{xG^T = 0 \mid x \in V(n, q)\}$. 即 $\begin{cases} x_1 + x_2 = 0 \\ x_3 + x_4 = 0 \end{cases}$ 解得 $\xi_1 = (1, 1, 0, 0), \xi_2 = (0, 0, 1, 1), \xi_3 = (1, 1, 1, 1), \xi_4 = (0, 0, 0, 0)$. $L^\perp = L, L^\perp$ 也是 $[4, 2]$ 线性码. $L^\perp = \{0000, 1100, 0011, 1111\}$

解答题

设 E_n 是 $V(n, 2)$ 中所有具有偶数重量的向量的集合. 证明: E_n 是线性码, 确定 E_n 的参数 $[n, k, d]$ 以及其标准型的生成矩阵.

证明: $\forall x, y \in E_n, d(x, y) = \omega(x - y), \omega(x - y) = \omega(x) + \omega(y) - 2\omega(x \cap y)$. 故 $\omega(x + y)$ 为偶数, $x + y = x - y, x + y \in E_n, E_n$ 是线性码. 由上一章课后题知 E_n 是一个 $[n, n - 1, 2]$ 线性码, 标准生成阵为

$$G = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$$

设 $L = \{xG \mid \forall x \in V(n - 1, q)\}$, 对 n 用归纳法证明, 则 L 中的元均具有偶重量, 从而 $L \subseteq E_n$. 又 $\dim L = \dim E_n = n - 1$, 故 $L = E_n$. ($\forall x \in L, x = v_{j1} + v_{j2} + \cdots + v_{jk}$, 系数取在 F_2 中 $\{0, 1\}$, $k = 2$ 时, $x = v_{j1} + v_{j2}, \omega(x) = \omega(v_{j1}) + \omega(v_{j2}) - 2\omega(v_{j1} \cap v_{j2})$ 为偶数容易用归纳法证得)

解答题

设 E_n 是 $V(n, 2)$ 中所有具有偶数重量的向量的集合. 证明: E_n 是线性码, 确定 E_n 的参数 $[n, k, d]$ 以及其标准型的生成矩阵.

(1) 要证明 E_n 是线性码, 我们需要证明对于任意两个向量 $x, y \in E_n$, 它们的加法 $x+y$ (在 \mathbb{F}_2 上是按位异或) 仍然在 E_n 中. 对于任何二元向量, 其重量的公式 $\omega(x+y)$ 可以通过 $\omega(x) + \omega(y) - 2\omega(x \cap y)$ 来计算, 其中 $\omega(x \cap y)$ 是 x 和 y 同时为 1 的位置数. 因 x, y 的重量都是偶数, $\omega(x) + \omega(y)$ 也是偶数. 由于 $\omega(x \cap y)$ 是整数, $2\omega(x \cap y)$ 一定是偶数, 从而 $\omega(x+y)$ 是偶数, 证明 $x+y$ 也在 E_n 中. 得证.

(2) 码的长度 n : 码的长度 n 指的是每个码字的位数, 由于 E_n 包括 $V(n, 2)$ 中所有具有偶数重量的向量, 每个向量自然是长度为 n 的向量.

维数 k 表示线性码的生成矩阵的行数, 也即是该码作为向量空间的基的向量数目. 在 E_n 的情况中, 生成矩阵 G 可以构造为长度为 n 且每行保证向量总重量为偶数的矩阵, 具体形式如下

$$G = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$$

这个矩阵的每一行代表一个基向量, 其中最后一个元素是其它所有元素的和 (确保总重量为偶数). 考虑到 E_n 是所有偶数重量向量的集合, 若 n 是奇数, 则所有 n 位向量中重量为奇数的向量不能直接包含在 E_n 中, 但可以通过其它向量的线性组合得到 (例如全 “1” 向量可以通过其它所有位为 1 且总数为奇数的向量异或得到).

因此, E_n 实际能够生成的独立向量数为 $n-1$, 即除去一个线性相关的向量 (例如, 全 “1” 向量), 余下的向量能够生成所有偶数重量的向量. 这意味着 E_n 作为子空间的维数是 $n-1$.

最小汉明距离 d 是指码中任意两个不同码字间至少有 d 个位是不同的. 对于 E_n , 因为所有码字的重量都是偶数, 所以任何两个不同的码字至少要在两个位置上有差异, 以确保它们的总重量变化保持为偶数 (如果仅一个位不同, 一个码字的重量将由偶数变为奇数或反之, 不满足偶数重量的要求). 因此, E_n 的最小汉明距离至少是 2.

综上所述, E_n 是一个 $[n, n-1, 2]$ 线性码.

(3) 标准型的生成矩阵 G 的具体形式是: $G = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$

这里, G 是一个 $(n-1) \times n$ 矩阵, 其中前 $n-1$ 列是 I_{n-1} ($n-1$ 阶单位矩阵), 最后一列是全 1 (如果 n 是奇数) 或全 0 列 (如果 n 是偶数), 以保持每行的重量为偶数.

解答题

证明: 对于任意一个二元线性码 L , 一定满足下列条件之一.

- (1) L 中所有码字都具有偶数重量;
- (2) L 中一半码字具有偶数重量, 另一半码字具有奇数重量.

证明: 设 L 是一个二元 $[n, k]$ 线性码, 且 L 中存在码字 x_0 , 使得 $\omega(x_0)$ 为奇数. 令 $L_1 = \{x \in L \mid \omega(x) \text{ 是偶数}\}$, $L_2 = \{x \in L \mid \omega(x) \text{ 是奇数}\}$, $x_0 + L_1 = \{x_0 + x \mid \forall x \in L_1\}$, $x_0 + L_1$ 中元素重量为奇数, $x_0 + L_1 \subseteq L_2$ 同理 $x_0 + L_2 \subseteq L_1$. $|L_2| \geq |x_0 + L_1| = |L_1| \geq |x_0 + L_2| = |L_2| \Rightarrow |L_1| = |L_2|$. (否定一个证另一个)

解答题

证明: 对于任意一个二元线性码 L , 一定满足下列条件之一.

- (1) L 中所有码字都具有偶数重量;
- (2) L 中一半码字具有偶数重量, 另一半码字具有奇数重量.

给定条件是 L 是一个二元 $[n, k]$ 线性码. 这意味着 L 包含 2^k 个码字, 每个码字长度为 n .

定义两个集合: $L_1 = \{x \in L \mid \omega(x) \text{ 是偶数}\}$, $L_2 = \{x \in L \mid \omega(x) \text{ 是奇数}\}$.

假设在 L 中存在至少一个码字 x_0 使得 $\omega(x_0)$ 是奇数. 我们将使用这个码字来构建集合映射.

对于 L_1 中的任意码字 x , 由于 x_0 是奇数重量, x 是偶数重量, 那么 $x_0 + x$ 将是奇数重量 (偶数与奇数相加结果为奇数). 因此, $x_0 + L_1 = \{x_0 + x \mid x \in L_1\} \subseteq L_2$.

同样, 对于 L_2 中的任意码字 y , $x_0 + y$ 将是偶数重量 (奇数与奇数相加结果为偶数). 因此, $x_0 + L_2 = \{x_0 + y \mid y \in L_2\} \subseteq L_1$.

由于 $x_0 + L_1 \subseteq L_2$ 且 $x_0 + L_2 \subseteq L_1$, 我们知道 $x_0 + L_1$ 和 $x_0 + L_2$ 分别是 L_2 和 L_1 的一部分, 且由于码的线性属性, 加法 $x_0 + x$ (其中 x 是 L 的任意成员) 是双射的 (即一一对应且可逆). 因此, $|x_0 + L_1| = |L_1|$ 和 $|x_0 + L_2| = |L_2|$.

由 $|L_2| \geq |x_0 + L_1| = |L_1|$ 和 $|L_1| \geq |x_0 + L_2| = |L_2|$, 我们得出 $|L_1| = |L_2|$.

这表明如果 L 中存在至少一个奇数重量的码字, 那么偶数重量的码字和奇数重量的码字数量必然相等, 即 $|L_1| = |L_2|$. 如果 L 中所有码字都具有偶数重量, 那么 L_2 为空集, 从而也满足题目中的条件之一.

综上所述, 对于任意一个二元线性码 L , 要么所有码字都具有偶数重量, 要么一半码字具有偶数重量, 另一半码字具有奇数重量.

解答题

设三元线性码 L 的生成矩阵为 $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$. 试求 L 的最小距离, 并证明 L 是完备码.

$$G = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array} \right) = (I_2 | A), \text{ 故 } L \text{ 的校验阵 } H = (-A^T | I_2) = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}.$$

H 中任意两列线性无关, 存在第 1, 2, 4 列线性相关, 根据定理知, $d(L) = 3$.

$|L| = q^k = 3^2 = 9$, 因此 L 为一个三元 $(4, 9, 3)$ 码, 由于

$$3^2 \left(\binom{4}{0} + \binom{4}{1}(3-1) \right) = 3^4$$

因此, L 是完备码.

解答题

设二元线性码 L 的生成矩阵为 $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$. 试求 L 的标准阵, 并对信道接收端接收到的字 11111 和 10000 分别进行译码.

易知 L 为一个 2 元 $[5, 2]$ 线性码, $|L| = q^k = 2^2 = 4$. $L = xG = (x_1, x_2) \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$, (x_1, x_2) 分别取 $(0, 0), (0, 1), (1, 0), (1, 1)$. 计算可得 $L = \{00000, 01010, 11010, 10000\}$, $|V(5, 2)| = 2^5 = 32$, 于是标准阵:

00000	01010	11010	<u>10000</u>	
01000	00010	10010	11000	$a_1 + L$
00100	01110	11110	10100	$a_2 + L$
00001	01011	11011	10001	$a_3 + L$
01100	00110	10110	11100	$a_4 + L$
01001	00011	10011	11001	$a_5 + L$
00101	01111	<u>11111</u>	10101	$a_6 + L$
01101	00111	10111	11101	$a_7 + L$

11111 在第 7 行第 3 列, 将 11111 译为第 3 列中最顶端的码字 11010, 同理将 10000 译为 10000.

解答题

设三元线性码 L 的生成矩阵为 $G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$.

- (1) 试求 L 的标准型的生成矩阵.
- (2) 试求 L 的标准型的校验矩阵.
- (3) 试利用伴随式译码方法对信道接收端接收到的字 2121、1201、2222 分别进行译码.

$$(1) G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{array} \right) = G'$$

G' 为 L 的标准型的生成矩阵.

$$(2) G' = \left(\begin{array}{cc|cc} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{array} \right) = (I_2 | A), \text{ 故 } L \text{ 的标准型的校验矩阵为 } H = (-A^T | I_2) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

- (3) 码 L 的伴随式列表为

陪集头	伴随式 xH^T
0000	00
1000	11
0100	12
0010	10
0001	01
2000	22
0200	21
0020	20
0002	02

设信道接收端接收到的字 2121、1201、2222 分别为 x_1, x_2, x_3 ,

$$x_1 H^T = 22, \quad a_1 = 2000, \quad a_1 H^T = 22, \quad x_1 - a_1 = 0121$$

$$x_2 H^T = 00, \quad a_2 = 0000, \quad a_2 H^T = 00, \quad x_2 - a_2 = 1201.$$

$$x_3 H^T = 02, \quad a_3 = 0002, \quad a_3 H^T = 02, \quad x_3 - a_3 = 2220.$$

因此, 2121 译码为 $2121 - 2000 = 0121$. 1201 译码为 $1201 - 0000 = 1201$, 2222 译码为 $2222 - 0002 = 2220$.

解答题

设二元线性码 L 的生成矩阵为 $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$. 试求 L 的重量分布.

$G = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array} \right) = (I_3 | A)$, 故 L 的校验阵 $H = (-A^T | I_3) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$. 根据定义知, H 为线性码 L 的对偶码 L^\perp 的生成矩阵, 于是 $L^\perp = \{00000, 10010, 11101, 01111\}$. 由于 L^\perp 是一个二元 $[5, 2]$ 线性码, 则有

$$W_{L^\perp}(z) = 1 + z^2 + z^4 + z^4$$

L 是一个二元 $[5, 3]$ 线性码, 则由二元线性码的 Mac Williams 恒等式知

$$\begin{aligned} W_L(z) &= \frac{1}{2^2} (1+z)^5 W_{L^\perp} \left(\frac{1-z}{1+z} \right) \\ &= \frac{1}{4} (1+z)^5 \left[1 + \left(\frac{1-z}{1+z} \right)^2 + 2 \left(\frac{1-z}{1+z} \right)^4 \right] \\ &= 1 + 3z^2 + 3z^3 + z^5. \end{aligned}$$

因此线性码 L 的重量分布为

$$A_0 = 1, A_1 = 0, A_2 = 3, A_3 = 3, A_4 = 0, A_5 = 1.$$

解答题

试求二元 Hamming 码 Ham(3,2) 的包含陪集头和对应伴随式列表, 并对在信道接收端接收到的字 0000011, 1111111, 1100110, 1010101 分别进行译码.

二元 Hamming 码 Ham(3,2) 的校验矩阵为 $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

伴随式列表:

陪集头 x_i	伴随式 $x_i H^T$
1000000	001
0100000	010
0010000	011
0001000	100
0000100	101
0000010	110
0000001	111

$$(0000011)H^T = 001 \Rightarrow 000011 \text{ 译为 } 1000011.$$

$$(1111111)H^T = 000 \Rightarrow 1111111 \text{ 译为 } 1111111.$$

$$(1100110)H^T = 011 \Rightarrow 1100110 \text{ 译为 } 1110110.$$

$$(1010101)H^T = 000 \Rightarrow 1010101 \text{ 译为 } 1010101.$$

解答题

写出七元 Hamming 码 Ham(2,7) 的校验矩阵 H , 并对在信道接收端接收到的字 35234106 和 10521360 分别进行译码.

七元 Hamming 码 Ham(2,7) 的校验矩阵为 $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

$$x_1 H^T = (35234106) \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 5 \\ 1 & 6 \end{pmatrix} = (0 \ 0), \quad x_2 H^T = (10521360) \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 5 \\ 1 & 6 \end{pmatrix} = (3 \ 6) = 3(1 \ 2)$$

因此, x_1 没有发生错误, 即 35234106 译为 35234106. x_2 在第 4 个位置发生错误, 10521360 译为 10521360 - 00030000 = 10561360.

解答题

设二元 Hamming 码 $\text{Ham}(4, 2)$ 的校验矩阵为

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

试对在信道接收端接收到的字 011011001111000 和 001100110011000 分别进行译码.

$$(011011001111000) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = (0110), (001100110011000) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = (1111)$$

第 6 个位置发生错误, 于是 011011001111000 译为 011010001111000 .

第 15 个位置发生错误, 于是 001100110011000 译为 001100110011001 .

解答题

写出三元 Hamming 码 $\text{Ham}(3, 3)$ 的校验矩阵 H , 并对在信道接收端接收到的字 0122100110022 和 2211001012020 分别进行译码.

$$n = \frac{3^3 - 1}{3 - 1} = \frac{26}{2} = 13$$

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

$$x_1 = 0122100110022 \quad x_1 H^\top = (111)$$

$$x_2 = 2211001012020 \quad x_2 H^\top = (010)$$

x_1 在第 9 个位置发生错误, 于是译为 $x_1 - 0000000010000 = 0122100100022$

x_2 在第 2 个位置发生错误, 于是译为 $x_2 - 0100000000000 = 2111001012020$

解答题

试求二元 Hamming 码 $\text{Ham}(4,2)$ 中重量分别为 1, 2, 3, 4 的码字的个数.

$r = 4$, 于是 $n = 2^r - 1 = 15$, 代入重量分布多项式中得:

$$W_{\text{Ham}(4,2)}(z) = \frac{1}{2^4} \left[(1+z)^{15} + 15(1-z^2)^7(1-z) \right]$$

由二项式展开定理, 计算整理得:

$$W_{\text{Ham}(4,2)}(z) = 1 + 35z^3 + 105z^4$$

于是, 二元 Hamming 码 $\text{Ham}(4,2)$ 中重量为 1, 2, 3, 4 的码字的个数分别为 0, 0, 35, 105.

解答题

确定二元 Hamming 码 $\text{Ham}(r,2)$ 中重量为 3 的码字的个数 A_3 .

二元 Hamming 码 $\text{Ham}(r,2)$ 的重量分布多项式为 $W_L(z) = \frac{1}{2^r} \left[(1+z)^n + n(1-z^2)^{\frac{n-1}{2}}(1-z) \right]$, 其中, $n = 2^r - 1$, 由二项式展开定理, 计算整理得:

$$W_L(z) = \frac{1}{2^r} \left[(\cdots + C_n^3 z^3 + \cdots) + (\cdots + nC_{\frac{n-1}{2}}^1 z^3 + \cdots) \right]$$

z^3 的系数为 $\frac{1}{2^r} \left(C_n^3 + nC_{\frac{n-1}{2}}^1 \right) = \frac{1}{n+1} \cdot \frac{(n-1)n(n+1)}{6} = \frac{n(n-1)}{6}$. 故重量为 3 的码字的个数 $A_3 = \frac{n(n-1)}{6}$.

解答题

设 p 是一个素数.

- (1) 在 F_p 上将 $x^p - 1$ 分解成不可约多项式的乘积.
- (2) 在 F_p 上将 $x^{p-1} - 1$ 分解成不可约多项式的乘积.

当 p 是素数时, 我们可以利用特征为 p 的有限域 F_p 上的性质来分解多项式 $x^p - 1$ 和 $x^{p-1} - 1$.

(1) 对于 $x^p - 1$, 我们可以利用二项式定理展开 $(x-1)^p$. 在有限域 F_p 中, 二项式系数 $\binom{p}{k}$ 对 p 取模后都为 0 (当 $1 < k < p$). 因此, 展开后除了首尾两项, 其他所有的项都被 p 整除, 而首尾两项就是 x^p 和 -1 , 因此我们可以得到:

$$x^p - 1 = (x-1)^p$$

(2) 对于 $x^{p-1} - 1$, 我们可以利用费马小定理. 根据费马小定理, 对于任意 $a \in F_p$ 且 $a \neq 0$, 都有 $a^{p-1} \equiv 1 \pmod{p}$. 因此, $x^{p-1} - 1$ 在 F_p 上有 $p-1$ 个根, 分别是 $1, 2, \dots, p-1$. 因此, 我们可以将其分解为一次多项式的乘积:

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$$

这样, 我们就完成了 $x^p - 1$ 和 $x^{p-1} - 1$ 在有限域 F_p 上的分解.

解答题

在 F_3 上将 $x^4 - 1$ 分解成不可约多项式的乘积, 确定所有码长为 4 的三元循环码, 并写出每一个码的生成矩阵和校验矩阵.

在三元域 F_3 上

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) = (x + 2)(x + 1)(x^2 + 1)$$

$x + 2$ 是一个一次多项式. 在任何域上, 一次多项式都是不可约的, 因为它们没有非平凡的因子. 所以在 F_3 上, $x + 2$ 是不可约的. 同理, $x + 1$ 也在 F_3 上不可约. 对于 $x^2 + 1$, 我们需要检查它是否有在 F_3 上的根. 如果它没有根, 那么它就是不可约的. 我们检查 F_3 中的所有元素:

1. $x = 0 : 0^2 + 1 = 1 \neq 0$
2. $x = 1 : 1^2 + 1 = 1 + 1 = 2 \neq 0$
3. $x = 2 : 2^2 + 1 = 4 + 1 = 5 \equiv 2 \pmod{3} \neq 0$

由于 $x^2 + 1$ 在 F_3 上没有根, 所以它在 F_3 上是不可约的.

长为 4 的三元循环码的生成多项式、生成矩阵、校验矩阵和对应的码如下:

生成多项式	生成矩阵	校验多项式	校验矩阵	$V(4, 3)$ 中的码
1	I_4	$x^4 - 1 = 0$	$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$	$V(4, 3)$
$x - 1$	$\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$	$x^3 + x^2 + x + 1$	$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$	{0000, 2100, 0210, 0021, 1002, 1200, 0120, 0012, 2001, 1020, 0102, 2010, 0201, 1110, 0111, 1011, 1101, 2220, 0222, 2022, 2202, 2211, 1221, 1122, 2112, 2121, 1212}
$x + 1$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$	$x^3 - x^2 + x - 1$	$\begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$	{0000, 1100, 0110, 0011, 1001, 2200, 0220, 0022, 2002, 1020, 0102, 2010, 0201, 1210, 0121, 1012, 2101, 2120, 0212, 2021, 1202, 2112, 2211, 1221, 1122, 1111, 2222}
$x^2 + 1$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$	$x^2 - 1$	$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$	{0000, 1010, 0101, 2020, 0202, 1212, 2121, 1111, 2222}
$x^2 - 1$	$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$	$x^2 + 1$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$	{0000, 2010, 0201, 1020, 0102, 1122, 2112, 2211, 1221}
$x^3 - x^2 + x - 1$	$\begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix}$	$x + 1$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$	{0000, 2121, 1212}
$x^3 + x^2 + x + 1$	$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$	$x - 1$	$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$	{0000, 1111, 2222}
$x^4 - 1 = 0$	$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$	1	I_4	{0000}

解答题

在 F_2 上将 $x^5 - 1$ 分解成不可约多项式的乘积, 确定所有码长为 5 的二元循环码, 并写出每个码的生成矩阵和校验矩阵.

在 F_2 上, $x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$ 所有码长为 5 的二元循环码的生成多项式, 生成矩阵和校验矩阵如下:

生成多项式	生成矩阵	校验矩阵	$V(5, 2)$ 中的码
1	I_5	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$V(5, 2)$
$x + 1$	$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$	$\left\{ \begin{array}{l} 00000, 11000 \\ 01100, 00110 \\ 00011, 10001 \\ 10010, 01001 \\ 10100, 01010 \\ 00101, 11110 \\ 01111, 10111 \\ 11011, 11101 \end{array} \right\}$
$x^4 + x^3 + x^2 + x + 1$	$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	$\{00000, 11111\}$
$x^5 - 1$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	I_5	$\{00000\}$

解答题

在 \mathbb{F}_2 上把 $x^3 - 1$ 分解成不可约多项式的乘积, 确定所有码长是 3 的二元循环码, 并写出每个码的生成矩阵和校验矩阵.

先将 $x^3 - 1$ 在二元域 \mathbb{F}_2 上分解为不可约多项式的乘积,

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x + 1)(x^2 + x + 1).$$

因为 0 和 1 都不是多项式 $x^2 + x + 1$ 的根, 所以 $x^2 + x + 1$ 在 \mathbb{F}_2 上是不可约的. 因此 $x + 1$ 和 $x^2 + x + 1$ 都是 \mathbb{F}_2 上的不可约多项式.

生成多项式	R_3 中的码	$V(3, 2)$ 中的码	生成矩阵	校验矩阵
1	R_3	$V(3, 2)$	I_3	$\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$
$1 + x$	$\{0, 1 + x, x + x^2, 1 + x^2\}$	$\{000, 110, 011, 101\}$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$
$1 + x + x^2$	$\{0, 1 + x + x^2\}$	$\{000, 111\}$	$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$
$x^3 - 1$	$\{0\}$	$\{000\}$	$\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$	I_3

写出 R_4 中的码长为 4 的所有三元循环码.

列表:

生成多项式	R_4 中的码	$V(4, 3)$ 中的码
1	R_4	$V(4, 3)$
$2 + x$	$3^3 = 27$ 个元	{0000, 2100, 0210, 0021, 1002, 1200, 0120, 0012, 2001, 1020, 0102, 2010, 0201, 1110, 0111, 1011, 1101, 2220, 0222, 2022, 2202, 2211, 1221, 1122, 2112, 2121, 1212}
$1 + x$	$3^3 = 27$ 个元	{0000, 1100, 0110, 0011, 1001, 2200, 0220, 0022, 2002, 1020, 0102, 2010, 0201, 1210, 0121, 1012, 2101, 2120, 0212, 2021, 1202, 2112, 2211, 1221, 1122, 1111, 2222}
$1 + x^2$	$3^2 = 9$ 个元	{0000, 1010, 0101, 2020, 0202, 1212, 2121, 1111, 2222}
$2 + x^2$	$3^2 = 9$ 个元	{0000, 2010, 0201, 1020, 0102, 1122, 2112, 2211, 1221}
$2 + x + 2x^2 + x^3$	$3^1 = 3$ 个元	{0000, 2121, 1212}
$1 + x + x^2 + x^3$	$3^1 = 3$ 个元	{0000, 1111, 2222}
$x^4 - 1$	{0}	{0000}

$(a + bx + cx^2)(2 + x), a, b, c \in F_3, 3^3 = 27$ 个元;

$(a + bx)(1 + x^2), a, b \in F_3, 3^2 = 9$ 个元;

$a(2 + x + 2x^2 + x^3), a \in F_3, 3^1 = 3$ 个元.

在 F_3 上将 $x^4 - 1$ 分解成不可约多项式的乘积, 确定所有码长为 4 的三元循环码, 并写出每一个码的生成矩阵和校验矩阵.

生成多项式	R_4 中的码	$V(4, 3)$ 中的码
1	R_4	$V(4, 3)$
$x + 1$	27 个元	{0000, 1100, 0110, 0011, 1001, 2200, 0220, 0022, 2002, 1020, 0102, 2010, 0201, 1210, 0121, 1012, 2101, 2120, 0212, 2021, 1202, 2112, 2211, 1221, 1122, 1111, 2222}
$x - 1$	27 个元	{0000, 2100, 0210, 0021, 1002, 1200, 0120, 0012, 2001, 1020, 0102, 2010, 0201, 1110, 0111, 1011, 1101, 2220, 0222, 2022, 2202, 2211, 1221, 1122, 2112, 2121, 1212}
$x^2 + 1$	9 个元	{0000, 1010, 0101, 2020, 0202, 1212, 2121, 1111, 2222}
$x^2 - 1$	9 个元	{0000, 2010, 0201, 1020, 0102, 1122, 2112, 2211, 1221}
$x^3 + x^2 + x + 1$	3 个元	{0000, 1111, 2222}
$x^3 - x^2 + x - 1$	3 个元	{0000, 2121, 1212}
$x^4 - 1$	{0}	{0000}

长为 4 的三元循环码的生成多项式, 生成矩阵和校验矩阵如下:

特征多项式	生成矩阵	校验多项式	校验矩阵
1	I_4	$x^4 - 1 = 0$	$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$
$x - 1$	$\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$	$x^3 + x^2 + x + 1$	$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$
$x + 1$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$	$x^3 - x^2 + x - 1$	$\begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$
$x^2 + 1$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$	$x^2 - 1$	$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$
$x^2 - 1$	$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$	$x^2 + 1$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$
$x^3 - x^2 + x - 1$	$\begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix}$	$x + 1$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$
$x^3 + x^2 + x + 1$	$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$	$x - 1$	$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$
$x^4 - 1 = 0$	$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$	1	I_4