

### 第 04 周作业

练习 1. 设  $A = \begin{pmatrix} 1 & -4 & 2 \\ -1 & 4 & -2 \end{pmatrix}$ ,  $B = \begin{pmatrix} 1 & 2 \\ -1 & 3 \\ 5 & -2 \end{pmatrix}$ ,  $C = \begin{pmatrix} 2 & 2 \\ 1 & -1 \\ 1 & -3 \end{pmatrix}$ , 计算  $B + C$ ,  $AB$ ,  $BA$ ,  $AC$ ,  $CA$  和  $A(2B - 3C)$ 。

练习 2. 设  $A = \begin{pmatrix} 2 & 1 & 4 \\ -3 & 0 & 2 \end{pmatrix}$ , 计算  $AA^T$  及  $A^T A$ 。

练习 3. 若  $A = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}$  和  $AB = \begin{pmatrix} -1 & 2 & -1 \\ 6 & -9 & 3 \end{pmatrix}$ , 求  $B$ 。

以下是附加题，做出来的同学下次课交，可以加分。注意解答过程要详细。

**练习 4.** (关于纠错码) 在这个练习中，我们不使用实数，而使用二进制数字 0 和 1。在这种数字系统中，加法、减法、乘法定义为： $1+1=0$ ,  $1+0=1$ ,  $0-1=1$ ,  $1\cdot 1=1$ ,  $0\cdot 1=0$  等等。用  $\mathbb{F}$  表示这种数字系统，即  $\mathbb{F} = \{0, 1\}$ 。(题外话，实数系统则记为  $\mathbb{R}$ 。)

把分量均为  $\mathbb{F}$  中的 0 和 1 的  $n$  维向量的全体，定义为  $\mathbb{F}^n$ 。不难知道， $\mathbb{F}^n$  只包含  $2^n$  个向量。在信息通信中， $\mathbb{F}^8$  中的一个向量就是一个字节 (byte)。例如，向量

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

就是一个字节。

计算机中信息储存的形式是 0 和 1 的字符串。例如

$$\cdots 101100011110010010101110 \cdots$$

通常把该字符串以 8 个数字为一段加以断开。例如上述字符串就断开成：

$$\cdots | 10110001 | 11100100 | 10101110 | \cdots$$

这样，每一段的 8 个数字正好构成 1 个字节，也就是  $\mathbb{F}^8$  中的一个向量。通信时，每次传输 1 字节的信息。

通信的过程有时会出错，例如，把字节 10110001 发送出去，但接受方可能收到的是字节 10110101。那么，有没有一种办法，让接收方自行判断收到的字节是否正确？这是有的，其中一种办法是采用“纠错码”。这种方法会涉及到线性代数中矩阵的乘积。以上就是本题的背景和说明。

下面介绍纠错码时，我们假设字符串是以 4 个数字为一段进行断开，而不是通常的 8 个数字。这样做是为了叙述简单。

首先给出一些定义。定义矩阵

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

该矩阵称为 Hamming 矩阵。定义  $\mathbb{F}^7$  中四个向量：

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

**验证：**乘积  $Hv_1, Hv_2, Hv_3, Hv_4$  均为  $\mathbb{F}^7$  中的零向量。

定义矩阵

$$M = (v_1, v_2, v_3, v_4).$$

(即：矩阵  $M$  为  $7 \times 4$  矩阵，各列依次为： $v_1, v_2, v_3, v_4$ ) 则上述所验证的结论说明  $HM = O$ 。

现在假设 Coco 要发送信息  $u \in \mathbb{F}^4$  给 Cici。纠错码的办法是：

1. 首先 Coco 计算乘积  $v := Mu$ 。(注意  $v \in \mathbb{F}^7$ 。) **验证**:  $v$  的后四位数字正好就是  $u$ 。
2. 然后, Coco 把  $v$  发送给 Cici。(注意不是发送原信息  $u$ 。)
3. 假设 Cici 收到的信息是  $w \in \mathbb{F}^7$ 。(如果  $w \neq v$ , 则说明发送过程出错。但 Cici 现在还不知道收到的  $w$  究竟有错没错。)

4. 假设传输过程信息**最多出错一个数字**。例如, 假设发送的是  $v = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ , 那么收到的可能是

$$w = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \quad (\text{第 2 位数字出错}) \text{ 或者 } w = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad (\text{第 6 位数字出错}) \text{ 等等, 但不可能收到 } w = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

(第 2, 6 位数字同时出错)。

4. Cici 开始验证了: 计算乘积  $Hw$ 。请你**验证**: 如果  $Hw = 0$ , 则说明传输过程没错, 即  $w = u$ 。这时  $w$  的后 4 位数字正好就是原信息  $u$ 。如果  $Hw \neq 0$ , 则说明传输过程出错, 即  $w \neq v$ 。

5. 即便传输过程出错, 也是有办法在错误中把原信息恢复出来。请你以这个例子想一想: 假设收到

$$w = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \text{ 那么原信息 } u \text{ 是什么?}$$

最后, 想一想“纠错码”体现在哪里?