5.6 线性分组码

- 信道编码的目的是为了降低平均差错率，又称纠错编码。
- 香农的有噪声信道定理的意义在于，它告诉我们什么是通过努力可以做到的事情，什么是不可能做到的事情。但香农并没有给出切实可行的实现方法。
- 香农提出的随机编码方法，是一种为避免寻找好码而采取的权宜之计，有理论意义而无实用价值。
- 有实用价值的码须用适当的数学工具来构造，使得构造出的码具有很好的结构特性，以便于译码。
- 纠错编码理论几乎与信息论同时创立，创始人是汉明。
- 纠错编码理论发展到现在，已形成以近世代数为理论基础的系统编码理论，又称代数编码理论。

纠错编码的基本概念

- 纠错编码的基本思路：引入可控冗余，即在信息序列中加入一些冗余码元（或称校验码元）。
- 译码：利用码元之间的相关性质来检测错误和纠正错误。
- 分组码：先将信息序列分成*K*个符号一组，称为信息组，然后在信息组中加入一些校验码元组成N长码字，由此得到的码称为（*N*，*K*）分组码。分组码中的任一码字的码长为N，所含的信息位数目为*K*、校验位数目为*N*-*K*。
- 线性码：线性码的最重要性质是线性特性，即信息位和监督位之间的关系为线性关系，码中任意两个码字的和仍为该编码的码字。否则为非线性码。
- 循环码：循环码是线性码的一个子集。循环码中任一码字循环移位后仍为该码的码字。否则为非循环码。

1、线性分组码的生成矩阵和校验矩阵

（以（5，2）分组码为例）

信息组长度 $K=2$：

$$\boldsymbol{m}=[m_1 \quad m_2];\ m_i \in \{0,1\}$$

码字长度$N=5$：

$$\boldsymbol{c}=[c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5]$$

编码函数：

$$f:\begin{cases} c_1 = m_1 \\ c_2 = m_2 \\ c_3 = m_1 \oplus m_2 = c_1 \oplus c_2 \\ c_4 = m_1 = c_1 \\ c_5 = m_1 \oplus m_2 = c_1 \oplus c_2 \end{cases}$$

码字由信息元的模2线性组合生成，因此是二元线性分组码，简称为线性码。

编码函数的矩阵表示：$[c_1 \quad c_2 \quad c_3 \quad c_4 \quad c_5]=[m_1 \quad m_2]\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

$$\boxed{\boldsymbol{c}=\boldsymbol{m}\boldsymbol{G}}$$

生成矩阵$\boldsymbol{G}$

校验方程的矩阵表示：

$$\begin{cases} c_3 = m_1 \oplus m_2 = c_1 \oplus c_2 \\ c_4 = m_1 = c_1 \\ c_5 = m_1 \oplus m_2 = c_1 \oplus c_2 \end{cases} \Longrightarrow \begin{cases} c_1 \oplus c_2 \oplus c_3 = 0 \\ c_1 \oplus c_4 = 0 \\ c_1 \oplus c_2 \oplus c_5 = 0 \end{cases} \Longrightarrow \begin{cases} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix}=\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \\ \boxed{\boldsymbol{H}\boldsymbol{c}^T=\boldsymbol{0}} \quad \boxed{\boldsymbol{c}\boldsymbol{H}^T=\boldsymbol{0}} \end{cases}$$

一致性校验矩阵$\boldsymbol{H}$

二元（N，K）线性码

信息组，K 维行阵：$\boldsymbol{m}=\begin{bmatrix} m_1 & m_2 & \cdots & m_K \end{bmatrix}$，$m_i \in \{0,1\}$

码字，N 维行阵：$\boldsymbol{c}=\begin{bmatrix} c_1 & c_2 & \cdots & c_N \end{bmatrix}$，$c_i \in \{0,1\}$

码字生成式：$\boxed{\boldsymbol{c}=\boldsymbol{m}\boldsymbol{G}}$

$\boldsymbol{G}$：$K\times N$ 生成矩阵，其元素取值于二元集合 {0，1}。

校验方程：$\boxed{\boldsymbol{H}\boldsymbol{c}^T=0}$　　$\boxed{\boldsymbol{c}\boldsymbol{H}^T=\boldsymbol{0}}$

$\boldsymbol{H}$：$r\times N$ 校验矩阵，其元素取值于二元集合 {0，1}。

$r=N-K$：校验位数目。

二元（N，K）线性码（续一）

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{g}_1\\ \boldsymbol{g}_2\\ \vdots\\ \boldsymbol{g}_K\end{bmatrix}=\begin{bmatrix}g_{11} & g_{12} & \cdots & g_{1N}\\ g_{21} & g_{22} & \cdots & g_{2N}\\ \vdots & \vdots & \vdots & \vdots\\ g_{K1} & g_{K1} & \cdots & g_{KN}\end{bmatrix}\qquad \boldsymbol{c}=\boldsymbol{m}\boldsymbol{G}=m_1\boldsymbol{g}_1\oplus m_2\boldsymbol{g}_2\oplus\cdots\oplus m_K\boldsymbol{g}_K$$

（1）$\boldsymbol{G}$ 的每个向量都是一个码字。

例：$m_1=1,\quad m_2=m_3=\cdots=m_K=0 \Longrightarrow \boldsymbol{c}=\boldsymbol{g}_1$

(2) 二元(N，K)线性码C={c}可看成一个N重维线性空间，　G的K个相互独立的行向量是它的一组基底。

(3) 任意K个相互独立的N长码字都可作为N重维码空间的一组基底，用这个码字当作行向量组成生成矩阵，即可生成所有码字。

二元（*N*，*K*）线性码（续二）

系统码：码字的前（或后）K 位照搬信息组的K个信息元

对于前K位为信息元的系统码，生成矩阵G可分成2块：

$$G=[I_{K\times K}\quad A_{K\times r}]=\begin{bmatrix}1 & 0 & \cdots & 0 & a_{11} & a_{12} & \cdots & a_{1r}\\ 0 & 1 & \cdots & 0 & a_{21} & a_{22} & \cdots & a_{2r}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \cdots & 1 & a_{K1} & a_{K2} & \cdots & a_{Kr}\end{bmatrix}=\begin{bmatrix}g_1\\ g_2\\ \vdots\\ g_K\end{bmatrix}$$

校验方程：$\boxed{cH^T=0}$

g_i 是码字，满足校验方程 。

$$g_iH^T=0\ ,\quad i=1,2,\cdots,K$$

$$\left.\begin{aligned}GH^T&=0\\ G&=[I_{K\times K}\quad A_{K\times r}]\end{aligned}\right\}\Rightarrow H=[A_{K\times r}^T\quad I_{r\times r}]$$

验证：$GH^T=[I_{K\times K}\quad A_{K\times r}][A_{K\times r}^T\quad I_{r\times r}]^T=[I_{K\times K}\quad A_{K\times r}]\begin{bmatrix}A_{K\times r}\\ I_{r\times r}\end{bmatrix}=A_{K\times r}\oplus A_{K\times r}=0$