线性分组码

May 30, 2023

Yimin Zhao
ym-zhao.com

线性分组码（Linear Block Code）

- 一个二元 (n, k) 线性分组码有 k 个信息位，$n - k$ 个校验位。根据某种数学关系构成总长度为 n 的码字，码率为 $\frac{k}{n}$
- 校验位是信息位的线性组合
- 码字最大数量为 2^k

性质：对于 (n, k) 线性分组码，设 $d_{\min}$ 为最小汉明距离，那么

1. $d_{\min} \geq 2t + 1$ iff 能 **纠正** t 个错误
2. $d_{\min} \geq l + 1$ iff 能 **检测** l 个错误
3. $d_{\min} \geq t + l + 1$ iff 能 **纠正** t 个错误且能 **检测** l 个错误

生成矩阵（Generator Matrix）

(n, k) 线性分组码的本质是把 k 维的信息向量 u 通过线性变换 G 扩张成 n 维的码字 C, G 称为生成矩阵，对于 C 中任意一个码字 c, 其满足

$$
\begin{aligned}
c_{1\times n} &= u_{1\times k} \cdot G_{k\times n} \\
&= (u_1, u_2, ..., u_k)\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} \\
&= \left(\sum_{i=1}^{k} u_i g_{i1}, ..., \sum_{i=1}^{k} u_i g_{i1}\right)
\end{aligned}
$$

性质：

1. 每个码字都是 G 各行的线性组合
2. G 的各行线性无关
3. G 的各行都在 C 空间中
4. 如果对 G 进行初等行变换得到 G', 那么其对应的 C' 空间与 C 完全相同，且不会改变校验矩阵 H

系统码（Systematic Code）

对于线性分组码而言，如果码字 c 的开头 k 位是信息位，剩下的校验位，那么称为系统码。

意义：对于系统码而言，G 才具有唯一性。

性质：

1. G 此时前 k 列构成单位矩阵，即

$$G_{k\times n} = \left(I_{k\times k}, Q_{k\times(n-k)}\right)$$

2. c 此时前 k 行就是信息向量 u，即

$$c_{1\times n} = \left(u_{1\times k}, p_{1\times(n-k)}\right)$$

校验矩阵（Parity Check Matrix）

对于系统码而言，校验位也是对信息位的线性组合，因此，可以把校验过程也写成矩阵形式，称为校验矩阵。 对于 C 中任意一个码字 c, 都满足

$$H_{(n-k)\times n}\cdot c^T=0$$

性质：

1. H 的各行线性无关
2. 如果 C 的 $d_{\min}$ 表示最小汉明距离，那么 H 的任意 $d_{\min}-1$ 列线性无关，反之也成立
3. 因为 G 的每一行都在 C 空间中，因此

$$H_{(n-k)\times n}\cdot G^T=0$$

4. $\operatorname{rank}(H)=n-k$, 可以化简为 $H=\left(P_{(n-k)\times k},I_{n-k}\right)$, 注意到如果 G 是系统码生成矩阵，有 $G=\left(I_k,Q_{k\times(n-k)}\right)$, 因此

$$P=Q^T$$

G 与 *H* 互相推导

$$G\leftrightarrow G^{'}\leftrightarrow G^{''}\leftrightarrow H^{''}\leftrightarrow H^{'}\leftrightarrow H$$

其中（只介绍一侧方向，反向同理）

1. $G\to G^{'}$ 是通过初等行变换变为行简化阶梯形（Row Reduced Echelon, RRE）
   1. 矩阵的每一行的第一个非零元素为1，称为该行的主元
   2. 每一行的主元所在列的其余元素全为0
   3. 主元所在列的序号随着行数增加而增加
   4. 零行在最下方
2. $G^{'}\to G^{''}$ 是通过列交换变为$\left(I_k,Q_{k\times(n-k)}\right)$的形式
3. $H^{''}=\left(Q^T,I_{n-k}\right)$
4. $H^{''}\leftrightarrow H^{'}$ 通过与第2步相反的列交换进行
5. H 可以认为是 $H^{'}$ 本身或者其通过初等行变换得到的任意结果

伴随式（Syndrome）

在信道中，假设发送端将信息 x 发出，接受端收到为 y, 那么可以用校验矩阵检查是否发生了错误:

$$s_{1\times(n-k)}=H\mathrm{y}^T$$

s 被称为校验子或伴随式，如果为0则没有错误，如果非0则认为发生了错误，若把信道造成的错误影响记为 z, 那么有

$$\mathrm{y}=\mathrm{x}+\mathrm{z}$$

因此有

$$\begin{aligned}s&=H\mathrm{y}^T\\&=H(\mathrm{x}+\mathrm{z})^T\\&=\underbrace{H\mathrm{x}^T}_{=0}+H\mathrm{z}^T\\&=H\mathrm{z}^T\end{aligned}$$

根据伴随式改错

关注形状：

$$
\begin{aligned}
s &= H\mathbf{z}^T \\
&= (r_1, r_2, ..., r_k)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix}
\end{aligned}
$$

当码元仅为0/1时，可以确认信道错误图样（error pattern）即 $\mathtt{z}$ 的值：

- 如果 s 等于 H 的某一行 r_i, 这意味着错误出现在 e_i, 即 $e_i = 1$, 其余为0
- 如果 s 等于 H 的某两行之和 $r_i + r_j$, 这意味着错误出现在 e_i 与 e_j, 即 $e_i = e_j = 1$, 其余为0

此时由于 $\mathtt{z}$ 和 $\mathtt{y}$ 已知，可以直接计算出正确信息 $\mathtt{x} = \mathtt{y} - \mathtt{z}$