线性码

信息系统的基础编码之一：差错控制编码

引言

问题：信道是不完善的，影响因素很多。若将信道看成一个系统，则系统的输入在统计意义上决定输出。（强调：不是确定性的）

信息论的贡献：
在互信息的基础上，计算信道容量。
建立了信道编码定理：只要传输速率不超过信道容量，则在分块编码的长度足够大时，可以达到任意小的错误概率。

Theorem 7.7.1 (*Channel coding theorem*)

For a discrete memoryless channel, all rates below capacity C are achievable. Specifically, for every rate $R < C$, there exists a sequence of $(2^{nR}, n)$ codes with maximum probability of error $\lambda^{(n)} \to 0$.

Conversely, any sequence of $(2^{nR}, n)$ codes with $\lambda^{(n)} \to 0$ must have $R \leq C$.

信道编码定理指明了方向，后来的研究者沿着该方向寻找和设计“好码（good codes）”

分块编码的基本思路可以从噪声打字机信道得到启发：仅仅使用输入符号的一个子集（subset），可以形成无噪信道。
对于二元通信的场合，只有两个符号 0 和 1，无法选取子集。
变通一下，对于通信做n次扩展，每次不是发一个符号，而是发一个长度为n的符号序列（符号串）。如此做法使得我们可从 2^n个输入符号串中选择一个子集（subset）参与通信。相当于我们找到了一种输入分布，子集内的符号串的发送概率值不为零且相等，子集外的符号串的发送概率值为 0。

基本思想：将表示信息的数据看成符号序列，引入冗余符号，要求冗余符号与原始数据符号序列之间具有确定性的依赖关系。

简单重复

编码：每一个符号，重复奇数次 $2k+1$。例如：$1 \to 11111$， $0 \to 00000$

译码：采用择多逻辑判决（大数逻辑判决）。若有至少 $k+1$ 个 1，译为 1，反之译为 0.

容错能力：检测并纠正不超过 k 个错误。

奇偶校验

编码：$x_1x_2...x_k \to x_1x_2...x_kx_{k+1}$，附加的 x_{k+1} 被称为校验符号位，原始数据 $x_1x_2...x_k$ 称为信息符号位。将这些符号位看成有限域 $GF(2)$ 中的元素，附加的校验符号位 x_{k+1} 满足 $x_1+x_2+...+x_k+x_{k+1}=0$，其中的加法是 $GF(2)$ 上的加法，即模 2 加。

译码：若接收到 $r_1r_2...r_kr_{k+1}$，验证 $r_1+r_2+...+r_k+r_{k+1}=0$ 是否成立，若成立，则提取前 k 位，将其认定为发送方发出的信息位，即 $x_1x_2...x_k \cong r_1r_2...r_k$。若不成立，则表明出错，应该丢弃数据。

注解：

$String1 \cong String2$，将右边的符号串认定为左边的符号串。

$x_1x_2...x_{k+1} \cong r_1r_2...r_{k+1}$ 不能断定没有出错，因为若出现偶数个错，则

$r_1+r_2+...+r_k+r_{k+1}=0$ 依然成立。

若出现奇数个错，则 $r_1+r_2+...+r_k+r_{k+1}=1$

线性码

高等代数的有关结论：

定理 1：向量组的极大线性无关组都含有相同个数的向量。
定义 1：向量组的秩（rank）是指向量组的极大线性无关组所含有的向量的个数。
定义 2：矩阵的行秩是指矩阵的行向量组的秩。
定义 3：矩阵的列秩是指矩阵的列向量组的秩。
定理 2：矩阵的行秩与列秩相等。

由上述定理，可用矩阵的秩统称矩阵的行秩和列秩。

通过校验矩阵定义线性码

将奇偶校验的思想进行推广。

将方程式 $x_1+x_2+\ldots+x_k+x_{k+1}=0$ 改写为

$$H\vec{x}=0$$

其中 $x=(x_1,x_2,\ldots,x_k,x_{k+1})^T$， $H=[1,1,\ldots,1,1]$

从改写后的方程式可以看出：

其中涉及到的矩阵 $H=[1,1,\ldots,1,1]$ 是非常特殊的形式：仅由一行全 1 向量组成。每个 1 表示对应的符号参加运算，受到监督保护。

1 个方程式对应一个校验符号 x_{k+1}、对应 H 矩阵的一行

一个符号对应 H 矩阵的一列

换成一般的矩阵

$$H=\begin{pmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{n-k\,1} & \cdots & h_{n-k\,n} \end{pmatrix}$$

称该矩阵为码的校验矩阵。

校验矩阵的含义解释如下：

它有 n 列，对应 n 个符号 $x_1x_2\ldots x_kx_{k+1}\ldots x_n$；不能出现全 0 的列，否则该列对应的符号取值对运算结果无影响，从而得不到监督保护；

它有 $n-k$ 行，对应 $n-k$ 个独立方程式、对应 $n-k$ 个校验符号 $x_{k+1}\ldots x_n$；其秩为 $n-k$，即 $rank(H)=n-k$，在矩阵论中，称这样的矩阵为行满秩矩阵。

从上述解释，我们看出，校验矩阵给出了码的很多知识，下面我们通过给出有限域上的行满秩矩阵 $H=\begin{pmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{n-k\,1} & \cdots & h_{n-k\,n} \end{pmatrix}$ 来定义一个线性码

定义【线性码】：线性码是指$C \triangleq \{\vec{x}: H\vec{x}=\vec{0}, \vec{x}\in GF^n(2), \vec{0}=(0,...,0)^T\}$。
由定义知：
线性码是校验矩阵H的核空间$H^{-1}(\vec{0})$----所有被H变成零向量的向量构成的集合。
C是$GF^n(2)$的线性子空间

C是齐次线性方程组$H\vec{x}=\vec{0}$的解空间

定理　若以行满秩矩阵$H_{n-k,n}$作为校验矩阵定义线性码C，则C是$GF^n(2)$的k维线性子空间，即$\dim(C)=k=n-rank(H)$

通过校验矩阵获得生成矩阵

由于$H_{n-k,n}$是行满秩矩阵，则它可以通过初等变换改变成如下分块形式：

$$[B_{n-k,k} \mid I_{n-k}]$$

将$\vec{x}=(x_1,x_2,...,x_k,x_{k+1},...,x_n)^T$作对应分块

$$\vec{x}=\begin{bmatrix}\overrightarrow{x^1}\\ \overrightarrow{x^2}\end{bmatrix}$$

其中

$$\overrightarrow{x^1}=(x_1,x_2,...,x_k)^T$$

$$\overrightarrow{x^2}=(x_{k+1},...,x_n)^T$$

$$[B_{n-k,k} \mid I_{n-k}]\begin{bmatrix}\overrightarrow{x^1}\\ \overrightarrow{x^2}\end{bmatrix}=B_{n-k,k}\overrightarrow{x^1}+I_{n-k}\overrightarrow{x^2}=B_{n-k,k}\overrightarrow{x^1}+\overrightarrow{x^2}=0$$

$$\overrightarrow{x^2}=-B_{n-k,k}\overrightarrow{x^1}$$

做转置

$$(x_{k+1},...,x_n)=(x_1,x_2,...,x_k)(-B^T_{n-k,k})$$

记 $G \triangleq [I_{k,k} \mid -B_{n-k,k}^{T}]$

则 $(x_1, x_2, ..., x_k, x_{k+1}, ..., x_n) = (x_1, x_2, ..., x_k)G$

上式表明，可以由矩阵 G 和原始信息符号分组 $(x_1, x_2, ..., x_k)$，生成有待发送的符号分组 $(x_1, x_2, ..., x_k, x_{k+1}, ..., x_n)$，故称矩阵 G 为码的生成矩阵。

总结如下

利用校验矩阵，接收方可以做符号的校验工作：$H\vec{x} = \vec{0}$

利用生成矩阵，发送方可以做符号的生成工作：

$(x_1, x_2, ..., x_k, x_{k+1}, ..., x_n) = (x_1, x_2, ..., x_k)G$

例题：Hamming 码

（7，4）Hamming 码的校验矩阵如下

$$\begin{array}{cc} & \begin{array}{ccccccc}1&2&3&4&5&6&7\end{array} \\ H= & \left[\begin{array}{ccccccc}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{array}\right]_{3\times7}\end{array}$$

变动列的位置可以得到

$$\begin{array}{cc} & \begin{array}{ccccccc}3&5&6&7&4&2&1\end{array} \\ H= & \left[\begin{array}{cccc|ccc}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{array}\right]_{3\times7}\end{array}$$

进一步可以得到生成矩阵

$$G=\left[\begin{array}{cccc|ccc}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{array}\right]_{4\times7}$$

练习：构造 (15,11) Hamming 码的校验矩阵和生成矩阵。

$$\begin{array}{cc} & \begin{array}{ccccccccccccccc}1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\end{array} \\ H= & \left[\begin{array}{ccccccccccccccc}0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\end{array}\right]_{4\times15}\end{array}$$

变动列的位置可以得到

$$
\begin{array}{c c}
 & \begin{array}{ccccccccccc|cccc} 3 & 5 & 6 & 7 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 8 & 4 & 2 & 1 \end{array} \\
H = & \left[\begin{array}{ccccccccccc|cccc}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1
\end{array}\right]_{4\times 15}
\end{array}
$$

$$
G = \left[\begin{array}{ccccccccccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{array}\right]
$$

生成矩阵和校验矩阵之间的关系

由 $H\vec{x}=\vec{0}$ 和 $(x_1,x_2,...,x_k,x_{k+1},...,x_n)=(x_1,x_2,...,x_k)G$，可得

$(x_1,x_2,...,x_k)GH^T=0$

由于 $(x_1,x_2,...,x_k)$ 的任意性，$GH^T=0$

由此可见，G 的行空间与 H 的行空间是正交的。

$$
G=\begin{pmatrix} g_1 \\ \vdots \\ g_i \\ \vdots \\ g_k \end{pmatrix},\ H=\begin{pmatrix} h_1 \\ \vdots \\ h_j \\ \vdots \\ h_{n-k} \end{pmatrix},\quad g_i h_j^T=0\ (i=1,...,k;\ j=1,...,n-k)
$$

例题：验证（7，4）-Hamming 码的 $GH^T=0$。

$$G=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}_{4\times 7}$$

$$H=\begin{bmatrix}0\,1\,1\,1\,1\,0\,0\\1\,0\,1\,1\,0\,1\,0\\1\,1\,0\,1\,0\,0\,1\end{bmatrix}_{3\times 7}$$

仅以 G 的第四行与 H 的第二行为例验证如下，注意其中的加法和乘法都是有限域$GF(2)$上的加法和乘法，也可以理解为命题逻辑中的“异或”与“合取”。

$$\begin{aligned}&(0\quad 0\quad 0\quad 1\quad 1\quad 1\quad 1)(1\quad 0\quad 1\quad 1\quad 0\quad 1\quad 0)^T\\&=0\bullet 1+0\bullet 0+0\bullet 1+1\bullet 1+1\bullet 0+1\bullet 1+1\bullet 0\\&=0+0+0+1+0+1+0=1+1=0\end{aligned}$$

从通信的角度看，发送方发送的是 G 的行空间的向量，接收方用对 H 的行空间（其代表向量就是 H 的行向量）来检验。

通过校验矩阵获得最小重量与最小距离

对于C中的任意码字，定义

Hamming 重量$wt(x)$=码字x的非 0 分量的个数，例如$wt(0010111)=4$

码的最小重量=C中的所有非零码字的 Hamming 重量的最小值

Hamming 距离$dist(x,y)$=码字x和y具有不相同分量的位置的个数，例如

$dist(0010111,1011001)=5$

码的最小距离=C中的任意码字间的 Hamming 距离的最小值

对于线性码，码的最小距离=码的最小重量（思考：为什么相等？）

给出校验矩阵，如何考察其最小距离？

考察$H\vec{x}=0$，将其改写为

$$\begin{pmatrix} h_1 & \ldots & h_i & \ldots & h_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{pmatrix} = 0$$

h_i 是校验矩阵的第 i 个列向量，于是有

$$x_1 h_1 + \ldots + x_i h_i + \ldots + x_n h_n = 0$$

左边是校验矩阵列向量的线性组合，方程式表明这些列向量是线性相关的。
如果线性码的某个码字的重量为 w，则存在 w 个列向量，其和为零向量。
如果任何 w-1 个列向量线性无关，而存在 w 个列向量线性相关，则码的最小重量为 w。

考察（7，4）Hamming 码的校验矩阵，其最小重量为 3

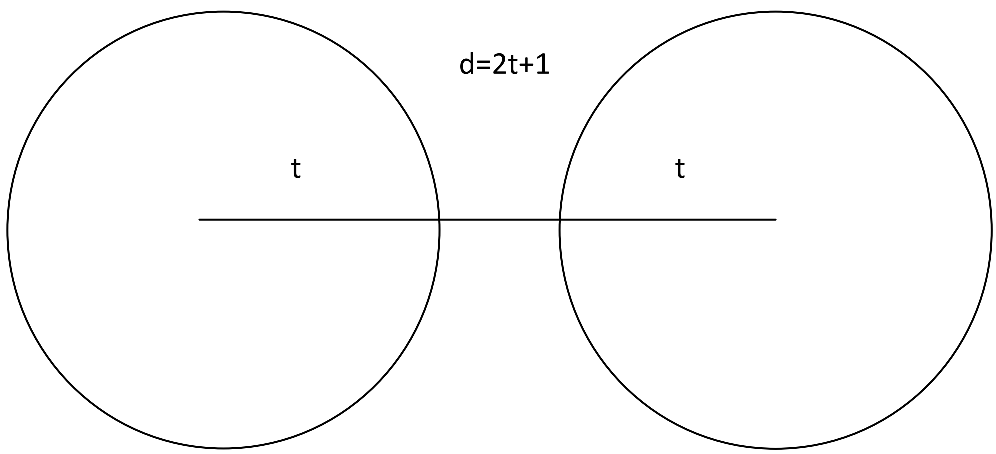
最小距离与容错能力

容错：检错、纠错

最小距离给出了检错、纠错能力。

码的三个参数 (n,k,d)

例如 Hamming 码的三个参数为 $(2^k - 1, 2^k - 1 - k, 3)$



Hamming 的纠错方法

Hamming 码的纠错方法是：校验矩阵的每一个列向量对应一个错误位置。数学推导：

令 $\vec{c}$：码字向量，

$\vec{r}$：接收向量

$\vec{e_i}$：错误向量，第 i 个分量为 1，其余分量为 0，表达单个错误模式

$\vec{r}=\vec{c}+\vec{e_i}$

$H\vec{r}=H(\vec{c}+\vec{e_i})=H(\vec{c})+H(\vec{e_i})=0+H(\vec{e_i})=H(\vec{e_i})=h_i$

由此可见，接收方做校验运算的结果是校验矩阵的第 i 个列向量，只要列向量之间两两互不相同，则可以定位相应的错误。就 Hamming 码的构造而言，每列相当于 $1\sim 2^k-1$ 的 k 位二进制展开，保证了两两互不相同。