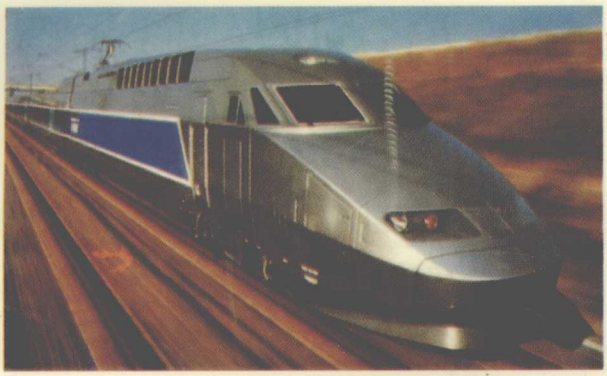
西南交通大学出版社

铁路继续教育系列教材

现代铁路信号技术

铁道部人事司
铁道部人才交流培训中心 组织编写



铁路继续教育系列教材

现代铁路信号技术

铁道部人事司
组织编写
铁道部人才交流培训中心

郎宗棪　郜成缙　主编

胡东源　谢肇桐　主审

西南交通大学出版社
·成都·

铁路继续教育系列教材
现代铁路信号技术
铁道部人事司
铁道部人才交流培训中心 组织编写
出版人 宋绍南
责任编辑 吴晓黎
封面设计 郑宏
*
西南交通大学出版社出版发行
（成都二环路北一段111号 邮政编码:610031 发行科电话:7600564）
http://press.swjtu.edu.cn
E-mail:cbs@center2.swjtu.edu.cn
四川森林印务有限责任公司印刷
*
开本:787mm×1092mm 1/16 印张:32.125
字数:775千字 印数:5001～7000册
1998年12月第1版 2000年5月第2次印刷
ISBN 7-81057-234-2/T·303
定价:31.00元

前　言

在铁道部和北京局人才交流中心的领导和支持下，我们编写了这本《现代铁路信号技术》，本书作为供铁路信号工程技术人员继续教育的主要教材，具有起点高、内容新、范围广等特点。

改革开放以来铁路信号技术发展非常迅速，微机联锁、多信息自动闭塞、超速防护、行车调度指挥管理系统、列车运行自动控制、自动化驼峰、微机监测等新技术层出不穷。这些新技术所涉及的基础技术又非常广泛，这本书对此也花了一定的篇幅进行了介绍。

因为不少新技术正在发展之中，有些还不够成熟，有些多种制式五彩缤纷，加上编者手头掌握的资料有限，这些因素造成了呈现在读者面前的本书还存在着这样那样的不足之处。编者恳切地希望广大从事信号和其它领域的读者提出宝贵的意见。

本书的编写者是：第一章为郎宗棪，第二章为任轶凝；第三章为苗国栋；第四章为郝云岗；第五章为郭秀清；第六章为秦钟芳；第七章为郎宗棪；第八章为蔡维娜；第九章为徐玉华；第十章为徐金祥；第十一章为郜成缙。全书主编为郎宗棪，副主编为郜成缙。

在编写过程中，得到铁道部电务局、全路通信信号研究设计院、成都铁路局电务处、上海铁路局电务处、北方交通大学等单位大力支持，对此深表感谢。

编　者

一九九八年十二月

序　言

《铁路继续教育系列教材》，是对铁路专业技术人员进行继续教育的基础读本。它的问世，对于抓好铁路继续教育，提高铁路专业技术队伍的素质是有益的。

铁路是我国交通运输的骨干。在加快改革开放和发展社会主义市场经济的新形势下，铁路面临着新的机遇和挑战。为把我国铁路现代化建设事业全面推向21世纪，我们必须以十五大精神为指导，加快铁路改革与发展，实施科教兴路战略，使铁路从传统产业逐步走向现代化。

实现铁路现代化，关键是科技，基础在教育。加快铁路科技进步，提高铁路专业技术队伍的素质，直接关系到铁路现代化的进程，现代科技发展日新月异，世界铁路在高速技术、重载技术、管理技术、安全技术和信息技术等方面取得了重大进展。为了适应新的形势，必须对全路专业技术人员广泛开展继续教育。

为了搞好铁路专业技术人员的继续教育，编写一套好的教材是非常重要的。《铁路继续教育系列教材》反映了现代科学技术发展的水平和铁路企业技术进步的特点，兼顾了教材理论体系的系统性和专业人员选修的适用性，对专业技术人员了解和把握本专业学科领域国内外科技发展动态，学习掌握先进的技术、理论和方法等会有帮助。希望全路各级组织、各级领导都来关心继续教育工作。各单位要根据实际，以这套教材为基础读本，切实抓好继续教育工作。全路广大专业技术人员要通过继续教育，不断更新知识内容，拓宽知识面，为我国铁路现代化建设事业作出新贡献。

这套教材由铁道部人事司、人才交流培训中心组织各方面的专家、教授和学者编写，部机关有关司局进行指导和审定，在此，我谨向为这套教材的编写、出版倾注了大量心血的所有工作人员表示衷心的感谢。

一九九七年十二月一日

目　　录

第一章　信息传输安全技术

第一节　信道模型及错误图样

数字信号在信道中传输时会受到各种干扰而产生差错，干扰对差错的影响与判决的方法有很大关系。通常有三种判决方法：第一种称为硬判决，即收到一个码元不是判定为 1 信号就是判定为 0 信号；第二种是软判决，在判定为 1 信号或 0 信号的同时还附带一个可信程度的指标；第三种在可以作出正确判决的情况下就判定为 1 信号或 0 信号，没有把握时就暂时不作判决，用 X 来表示，称为删除符号。

一、二进制对称信道 BSC

最常见的信道是二进制对称信道，也是最简单最典型的信道，称 BSC(Binary Symmetric Channel)信道。其信道模型见图 1-1。对于高斯白噪声干扰的信道。BSC 是很好的信道模型，随机差错硬判决译码用的就是这种信道模型。

二、离散无记忆信道 DMC

离散无记忆信道，简称 DMC(Discrete Meneryless Channel)信道。对随机差错进行软判决译码时，为了从解调器得到输出码元的可信度信息，输出常常被量化成 q 个电平，一般 q 为 8，即输出为 0、1、2、…、7，其中 0 是可信度最高的 0 码元，7 是可信度最高的 1 码元。当 4、5、6 被译成 1 码元时，4 的可信度最低。同样，当 1、2、3 被译成 0 码元时，3 的可信度最低。这种信道称为离散无记忆信道，简称 DMC 信道。图 1-2 是它的信道模型。

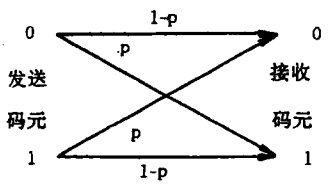


图 1-1　二进制对称信道 BSC

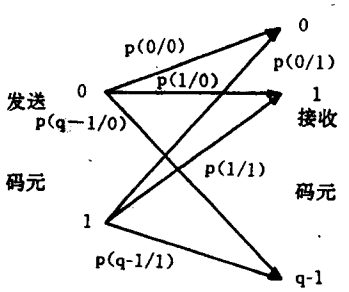


图 1-2　离散无记忆信道模型

三、二进制删除信道 BEC

在二进制删除信道 BEC(Binary Erasure Channel)中，当发现某位码元的可信度不够，不能确定是什么码元时，暂时将该位用“X”标出，然后分别将该位用 $X=0$ 和 $X=1$ 代入进行最大似

然译码。卷积码的序列译码就是采用这种信道模型。图 1-3 是二进制删除信道的信道模型。

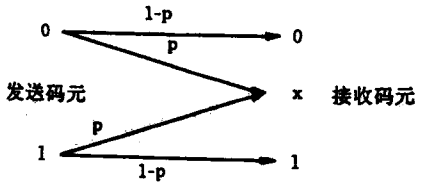


图 1-3　二进制删除信道模型

四、二进制混合信道 BHC

二进制混合信道 BHC(Binary Hybrid Channel) 兼有二进制对称信道和二进制删除信道的性质。既有 1 错成 0 和 0 错成 1 的情况，也有不能确定而暂时删除的情况。例如，在 8 量化电平情况下，如果将 0、1、2 译成 0，5、6、7 译成 1，3 和 4 暂时删除。图 1-4 是这种信道的信道模型。例如，发送 0，接收到 2 译成 0，接收到 3 暂时删除，接收到 5 就错译成 1。

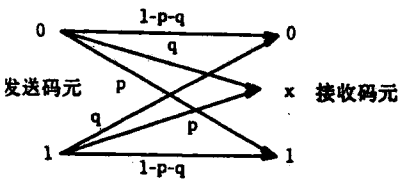


图 1-4　二进制混合信道模型

五、二进制 Z 信道

在二进制 Z 信道中，两种码元出错的概率相差很大。大规模集成电路和磁带、磁盘等因缺陷所造成的差错就属于这种单向差错。图 1-5 是二进制 Z 信道模型。

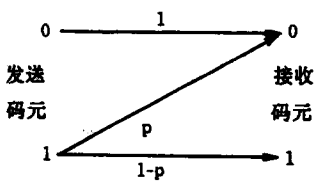


图 1-5　二进制 Z 信道模型

六、记忆信道

以上五种信道都是无记忆信道，实际上大多数信道都是有记忆的。即差错的出现不是独立的随机事件而与前面码元是否出现差错有关，其中仅受前一码元影响的称为单纯马尔科夫过程。图 1-6 是单纯马尔科夫过程的信道模型。

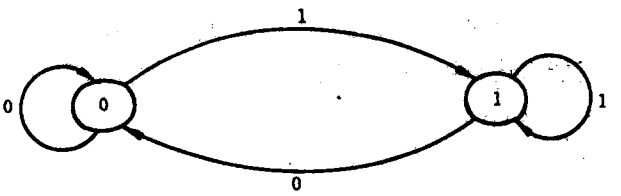


图 1-6 单纯马尔科夫过程的信道模型

第二节 线性分组码及循环码

一、线性分组码

(一) 线性分组码概述

1. 线性分组码的构成

在信道中传送的数字信号都是由 0 码元和 1 码元组成的二元序列。长度为 k 的二元序列可以传送 2^k 种不同的消息。因为这 k 个码元都可以是 0 码元或 1 码元，每个码元都带有信息量，我们称它们为信息码元。全部由信息码元组成的二元序列不具备任何防护出差错的能力。我们可以在信息元序列后面按照一定的编码规则增加若干不带信息量的冗余码元。这些冗余码元称为校验元。如果在信息序列中取 k 个信息元为一组。按编码规则增加 r 个校验元，成为长度为 $n=k+r$ 的码字，就构成了分组码。我们常用(n,k)来表示长度为 n 信息位数为 k 的分组码。

分组码分为线性和非线性两大类。定比码和群计数码都属于非线性分组码，它们都比较简单，性能也比较差。线性分组码的实用价值较高，它的 r 位校验元都是 k 位信息元中某些码元的模 二和。即校验元是部分信息元的线性组合，所以称之为线性分组码。在编码过程中如果 k 位信息元的顺序和取值都不变，就叫做系统码，否则叫做非系统码。

2. 奇偶校验码

最简单的二进制线性分组码就是奇偶校验码。它是$(n,n-1)$系统线性分组码。它的前 $n-1$位是信息元，最后一位是校验元。如果是奇校验码，则校验元的取值保证了全部码元中 1 码元的个数为奇数。如果是偶校验码，则校验元的取值保证了全部码元中 1 码元的个数为偶数。如(5,4)偶校验码可以写成

$$C=C_4C_3C_2C_1C_0$$

这里，C_4、C_3、C_2、C_1 是信息元，C_0 是校验元。

$$C_0=C_4\oplus C_3\oplus C_2\oplus C_1 \tag{1-1}$$

符号⊕表示模二加。如果是奇校验码，则校验元

$$C_0=C_4\oplus C_3\oplus C_2\oplus C_1\oplus 1 \tag{1-2}$$

我们定义信息元数 k 与码长 n 的比值

$$R=k/n \tag{1-3}$$

为编码效率，简称码率。奇偶校验码的编码效率很高，$R=(n-1)/n$，但性能很差，只能发现奇数位差错而不能纠正差错。

3. 能纠正差错的线性分组码

奇偶校验码只有一位校验元，只能发现奇数位差错而不能纠错，我们只要增加校验元的数目就能改善码的抗干扰能力达到纠正差错的目的，(7,4)线性分组码的码字为

$$C=(C_6、C_5、C_4、C_3、C_2、C_1、C_0)$$

其中，$C_6、C_5、C_4、C_3$ 是信息元，$C_2、C_1、C_0$ 是校验元。

$$C_2=C_6\oplus C_5\oplus C_4$$
$$C_1=C_5\oplus C_4\oplus C_3$$
$$C_0=C_6\oplus C_5\oplus C_3$$

三个校验元分别由三个不同的校验方程式给出，每个信息元至少在两个校验方程式中出现，即至少接受两个校验元的检查。

(二) 线性分组码的生成矩阵和校验矩阵

1. 线性分组码的生成矩阵

线性分组码是由一组信息元的线性方程式生成，它可以用图 1-7 所示的编码器实现。

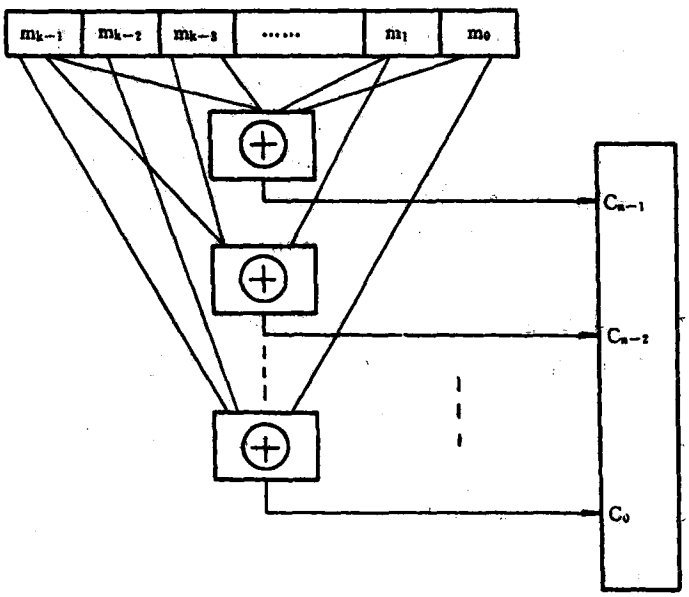


图 1-7 (n,k)线性码的编码器

以上编码器可用 n 个线性方程式表示成

$$\begin{aligned}
C_{n-1}&=m_{k-1}g_{k-1,n-1}\oplus m_{k-2}g_{k-2,n-1}\oplus\cdots\oplus m_0g_{0,n-1}\\
C_{n-2}&=m_{k-1}g_{k-1,n-2}\oplus m_{k-2}g_{k-2,n-2}\oplus\cdots\oplus m_0g_{0,n-2}\\
&\vdots\qquad\qquad\vdots\\
C_0&=m_{k-1}g_{k-1,0}\oplus m_{k-2}g_{k-2,0}\oplus\cdots\oplus m_0g_{0,0}
\end{aligned}\qquad(1\text{-}4)$$

这里，对所有 k 和 i 都有 $g_{ki}\in\{0,1\}$，只有 $g_{ki}=1$ 时，该信息元才参加该方程的校核。因为模二乘法和普通乘法是相同的，(1-4)式中乘积项可用普通乘法表示。(1-4)式中的系数可以用矩阵来表示

$$G=\begin{bmatrix} g_{k-1,n-1} & g_{k-1,n-2} & \cdots & g_{k-1,0} \\ g_{k-2,n-1} & g_{k-2,n-2} & \cdots & g_{k-2,0} \\ \vdots & & & \vdots \\ g_{0,n-1} & g_{0,n-2} & \cdots & g_{0,0} \end{bmatrix} \tag{1-5}$$

该矩阵叫做线性分组码的生成矩阵。

(1-4)式可用矩阵形式来表示

$$C=mG \tag{1-6}$$

同一个码可以有许多生成矩阵，我们把其中具有下列形式的生成矩阵称为系统码的生成矩阵。

$$G=\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & g_{k-1,n-k-1} & g_{k-1,n-k-2} & \cdots & g_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & g_{k-2,n-k-1} & g_{k-2,n-k-2} & \cdots & g_{k-2,0} \\ \vdots & & & & & & & \vdots & \\ 0 & 0 & 0 & \cdots & 1 & g_{0,n-k-1} & g_{0,n-k-2} & \cdots & g_{0,0} \end{bmatrix}=[I_kP] \tag{1-7}$$

式中，I_k 是 k 阶单位矩阵；P 为$(n-k)\times k$ 阶矩阵；G 为$(n\times k)$阶矩阵。前面介绍的(7,4) 线性分组码的系统码生成矩阵为：

$$G=\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

用生成矩阵编成的码字为：

$$C=mG=[m_3 \quad m_2 \quad m_1 \quad m_0][I_4P]$$

可以得到

$$C_6=m_3$$
$$C_5=m_2$$
$$C_4=m_1$$
$$C_3=m_0$$
$$C_2=m_3\oplus m_2\oplus m_1$$
$$C_1=m_2\oplus m_1\oplus m_0$$
$$C_0=m_3\oplus m_2\oplus m_0$$

任何非系统码的生成矩阵都可以通过行的初等变换化成系统码的生成矩阵。这里，行的初等变换是指对矩阵的任意两行交换位置，在某一行上加上另一行等。

2. 线性分组码的校验矩阵

由(1-6)式可以得到系统码的校验元

$$C_i=\sum_{j=k-1}^{0} m_jg_{ji} \qquad i=n-k-1、n-k-2、\cdots、0 \tag{1-8}$$

移项可得

$$0=\sum_{j=k-1}^{0} m_jg_{ji}\oplus C_i \qquad i=n-k-1、n-k-2、\cdots、0 \tag{1-9}$$

注意到 $m_{k-1}=C_{n-1}$、$m_{k-2}=C_{n-2}$、$\cdots$、$m_0=C_{n-k}$

(1-9)式可以写为矩阵形式

$$0=CH^T \tag{1-10}$$

这里 H 是 $r\times n$ 阶矩阵，称为校验矩阵。系统码的校验矩阵

$$H=\begin{bmatrix} g_{k-1,n-k-1} & g_{k-2,n-k-1} & \cdots & g_{0,n-k-1} & 1\ 0\ 0\ \cdots\ 0 \\ g_{k-1,n-k-2} & g_{k-2,n-k-2} & \cdots & g_{0,n-k-2} & 0\ 1\ 0\ \cdots\ 0 \\ \vdots & & & \vdots & \\ g_{k-1,0} & g_{k-2,0} & \cdots & g_{0,0} & 0\ 0\ 0\ \cdots\ 1 \end{bmatrix}=[P^T I_r] \tag{1-11}$$

从(1-9)式可以看出，任何码字和 H 矩阵的转置矩阵相乘，结果都是 r 位全零序列，因此用 H 矩阵来检查任意一个二元序列是不是码字就十分方便，校验矩阵的名称也就是这样得来的。系统码的校验矩阵可以很方便地由它的生成矩阵得到。由(1-10)和(1-6)式可得

$$CH^T=mGH^T=0$$

所以

$$GH^T=HG^T \tag{1-12}$$

前面介绍的(7,4)线性分组码的系统码校验矩阵为

$$H=\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}=[P^T I_3] \tag{1-13}$$

（三）线性分组码的伴随式

为了能够纠正码字在传送过程中产生的差错，必须使每一种差错在译码过程中产生的标志各不相同，这个标志就是伴随式。假设一个码字

$$C=C_{n-1}C_{n-2}\cdots C_0$$

在传送过程中由于噪声干扰产生差错又称错误图样

$$E=e_{n-1}e_{n-2}\cdots e_0$$

接收端收到的二元序列为：

$$R=C\oplus E=r_{n-1}r_{n-2}\cdots r_0 \tag{1-14}$$

其中，$r_{n-1}=C_{n-1}\oplus e_{n-1}$，$r_{n-2}=C_{n-2}\oplus e_{n-2}$，$\cdots$，$r_0=C_0\oplus e_0$。

令 $$S=RH^T=(C\oplus E)H^T=CH^T\oplus EH^T$$

因 C 是码字，故有 $CH^T=0$，得

$$S=EH^T \tag{1-15}$$

这里 S 称之为伴随式。(1-14)式表明伴随式 S 只和错误图样 E 有关，而和发送的是什么码字无关。由(1-14)式可知，第 i 位出差错，即 $e_i=1$ 的伴随式就是 H 矩阵的第 i 列。只要 H 矩阵的每列都不相同，就可以纠正任何单错，在长为 n 的错误图样中，单错有 n 种加上无差错一种，共需要 $n+1$ 种伴随式。伴随式是长为 $r=n-k$ 的二元序列，共有 2^r 种不同的组合。因此，(n,k)码要能纠正任何单错，它的校验元数目，即 H 矩阵每一列的元数必须满足

$$2^r\geqslant n+1 \tag{1-16}$$

同样，(n,k)码要能够纠正全部单错和双错，则任何单错和双错的伴随式都应不同。因此校验元数目必须满足

$$2^r \geqslant C_n^2 + C_n^1 + 1 \tag{1-17}$$

依此类推，(n,k)码要能够纠正 t 位和少于 t 位的全部差错，其校验元数目必须满足

$$2^r \geqslant C_n^t + C_n^{t-1} + \cdots + C_n^2 + C_n^1 + 1 \tag{1-18}$$

这就是有名的汉明界。

（四）汉明距离和汉明重量

码的汉明距离是两个码字之间差别程度的标志。任何(n,k)码都是从 2^n 个长为 n 的二元序列中按编码规则挑选出 2^k 个二元序列作为码字的。编码的方法要使码字间的差别程度尽可能大。码字间的差别程度的量度是汉明距离。它定义为两码字对应位相异码元的个数。即

$$d(a,b) = \sum_{i=0}^{n-1} (a_i \oplus b_i) \tag{1-19}$$

例如 $a=1\,0\,1\,0\,1\,1\,1$，$b=1\,1\,0\,0\,1\,1\,0$，

则 $d(a,b)=1\oplus1+0\oplus1+1\oplus0+0\oplus0+1\oplus1+1\oplus1+1\oplus0=3$

我们把某种编码中任意两个码字间距离的最小值称为码的最小矩离 d，(n,k)码的任一码字和全零码字间的汉明距离称为该码字的汉明重量，一个码字的汉明重量就是该码字中 1 码元的数目。记为 $wt(x)$。上例中 $wt(a)=5$，$wt(b)=4$。非零码字中汉明重量最小的码字的汉明重量称为码的最小重量。记为 $wt(C)$。

由 $CH^T=0$ 可知，如果码的最小重量为 $wt(C)$，则 H 矩阵中至少存在一种 $wt(C)$列线性相加结果为零的情况。而任何少于 $wt(C)$列线性相加结果一定不为零。因为不存在重量少于 $wt(C)$的码字。

在线性码中，任意两个码字按位模二加的结果必定是一码字。可见码的最小重量就是码的最小矩离。码的最小矩离 d 与码的纠错和检错能力有很大的关系。

如果要检出 e 个错，码的最小矩离 d 必须满足下式

$$d \geqslant e+1 \tag{1-20}$$

如果要纠正 t 个错，码的最小矩离 d 必须满足下式

$$d \geqslant 2t+1 \tag{1-21}$$

如果要纠正 t 个错并检出 e 个错，这里 $e>t$，码的最小矩离 d 必须满足下式

$$d \geqslant t+e+1 \tag{1-22}$$

（五）汉明码

汉明码是最简单的纠错码，它只能够纠单个错误。前面介绍的(7,4)线性分组码就是最简单的汉明码。汉明码的码长 $n=2^r-1$，信息元数 $k=2^r-r-1$，校验元数为 $n-k=r$。汉明码的校验矩阵有 r 行 n 列，任何一列都不为零并且任何两列都不相等，所以能够纠正任何单错。H 矩阵一般有三种形式：

(1) 按二进制的自然顺序从左到右排列 H 矩阵的各列；

(2) 系统码标准形式；

(3) 循环码显式表达形式。

(7,4)汉明码 H 矩阵的第二种形式就是(1-13)式。

第一种形式是

$$H_1=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}$$

第三种形式是

$$H_3=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\end{bmatrix}$$

如果我们分别取 $r=4、5、6、\cdots$ 可以构成(15,11)、(31,26)、(63,57)、…长度不同的汉明码。关于汉明码的循环特性我们将在后面讨论。

二、循环码

(一) 循环码的基本概念

循环码是线性分组码中应用最广的子类。它有完整的代数结构，可以用近世代数来描述。码长在 1000 以下时有较大的纠错能力，并可以用移位寄存器电路来实现编码和译码，设备简单，价格便宜。

(n,k)循环码除了具有线性分组码的全部性质外，还具有循环特性，即它的任意一个码字向左或向右循环移位后仍然是它的码字。即如果

$$C=C_{n-1}C_{n-2}\cdots C_1C_0$$

是一码字，则向左循环移一位，用 $L(C)$表示，后可得

$$L(C)=C_{n-2}C_{n-3}\cdots C_0C_{n-1} \tag{1-23}$$

仍是一个码字，同理

$$L^2(C)=C_{n-3}C_{n-4}\cdots C_{n-1}C_{n-2}$$

$$L^{n-1}(C)=C_0C_{n-1}\cdots C_2C_1$$

都是该码字集合中的码字。最后

$$L^n(C)=C_{n-1}C_{n-2}\cdots C_1C_0=C$$

即向左循环移 n 位后，又回到原来的码字。同样我们可以用 $R(C)$来表示向右循环移位。循环码的最大循环周期和它的码长 n 相同，其它循环周期是码长 n 的因数。为了用近世代数来表述循环码，可把码字中的码元看作为有限域上变元 X 的$(n-1)$次多项式的系数。我们可以用码多项式 $C(X)$来表示码字

$$C(X)=C_{n-1}X^{n-1}+C_{n-2}X^{n-2}+\cdots C_1X+C_0 \tag{1-24}$$

码字 C 向左循环移 i 位相当于 X^i 乘以 $C(X)$后再模$(X+1)^n$。同样，向右循环移 i 位相当于 X^{-i}乘以 $C(X)$后再模$(X+1)^n$。这样一来，编码和译码都可以用近世代数的加法和乘法运算来实现了。

(二) 有限域计算

用 GF(q)表示的有限域又称为伽罗华(Galois)域。域元素有 0、1、2、…、$q-1$ 等 q 个。其中最常用的是 $q=2$ 的 GF(2)域及其扩展域 GF(2^m)。

1. 有限域的定义

一切有限域都有加法和乘法两种运算，并满足下列条件：

(1) 封闭性：

若任意两个元素 a、$b \in GF(q)$，则有

$$a+b=c \in GF(q)$$

$$a \cdot b=d \in GF(q)$$

(2) 结合律：

若任意三个元素 a、b、$c \in GF(q)$，则有

$$(a+b)+c=a+(b+c)$$

$$(a \cdot b) \cdot c=a \cdot (b \cdot c)$$

(3) 交换律：

若任意两个元素 a、$b \in GF(q)$，则有

$$a+b=b+a$$

$$a \cdot b=b \cdot a$$

(4) 有加法单位元(又称零元)0 和乘法单位元(又称么元)e，使任意元素 $a \in GF(q)$ 都有

$$a+0=a$$

$$a \cdot e=a$$

有时乘法单位元用 1 来表示。

(5) 对任意元素 $a \in GF(q)$，都有加法负元$(-a)$，使

$$a+(-a)=0$$

对任意非零元素 $a \in GF(q)$，都有乘法逆元 a^{-1}，使

$$a \cdot a^{-1}=e$$

(6) 乘法对加法满足分配律：

对任意三个元素 a、b、$c \in GF(q)$，都有

$$a(b+c)=a \cdot b+a \cdot c$$

有限域元素的个数一定是素数或素数的整数次幂。常用的是 GF(2)及 $GF(2^m)$，我们称 $GF(2^m)$ 为 GF(2) 的扩展域。$GF(2^3)$ 是以系数取自 GF(2) 的 3 次本原多项式 $p(x)=x^3+x+1$ 为模所构成的多项式域。它的 8 个元素是 0、1、α、$\alpha+1$、α^2、α^2+1、$\alpha^2+\alpha$、$\alpha^2+\alpha+1$。这里 α 是 $p(X)$ 的根。因此有 $\alpha^3+\alpha+1=0$，由于它的素域是 GF(2)，故有 $\alpha^3=\alpha+1$。

有限域的全部元素构成一个循环群，并可用 α 的幂表示全体元素，因此我们又称 α 为生成元。

2. 有限域的运算

模 $p(X)$ 运算的规则是先做普通加法运算或乘法运算，然后用 $p(X)$ 除，得到的余式就是所求的结果。例如用 α 的幂表示 GF(8)的各元素时有：α、α^2、$\alpha^3=\alpha+1$、$\alpha^4=\alpha \cdot \alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha$、$\alpha^5=\alpha \cdot \alpha^4=\alpha^2+\alpha+1$、$\alpha^6=\alpha \cdot \alpha^5=\alpha^2+1$。

域元素还可表示成泽奇(Zech)函数的形式，称为泽奇对数，用 $Z(n)$ 表示

$$\alpha^{z(n)}=\alpha^n+1 \tag{1-25}$$

可以利用泽奇函数进行加法运算

$$\alpha^m+\alpha^n=\alpha^m(1+\alpha^{n-m})=\alpha^{m+z(m-n)} \tag{1-26}$$

以上我们介绍了 $GF(2^m)$ 域元素的多项式表示法，幂表示法和泽奇对数表示法。多项式表示法还可用其系数表示成 m 重，幂表示法还可用其对数表示。表 1-1 列出 GF(8) 域元素的 5

种表示形式。

表 1-1 GF(8)域元素的表示形式

多 项 式	3 重	对 数	幂	$Z(n)$
0	000	$-\infty$	0	0
1	001	0	1	$-\infty$
α	010	1	α	3
α^2	100	2	α^2	6
$\alpha+1$	011	3	α^3	1
$\alpha^2+\alpha$	110	4	α^4	5
$\alpha^2+\alpha+1$	111	5	α^5	4
α^2+1	101	6	α^6	2

表中的多项式表示法和 $m=3$ 重表示法便于加法运算，对数表示法和幂表示法便于乘法运算，泽奇对数表示法便于混合运算。上述关于域的构成原则可以推广到 GF(2^m)，任何 m 次本原多项式的根 α，它的幂一定能生成 GF(2^m)的全部非零元素。本原多项式一定是不可约的，但不可约多项式不一定就是本原多项式。例如 x^4+x+1 和 x^4+x^3+1 都是本原多项式，但 $x^4+x^3+x^2+x+1$ 却只是不可约多项式而非本原多项式。因此它不能生成 GF(16)的全部元素。表 1-2 列出由 $p(x)=x^4+x+1$ 生成的域元素的 5 种表示形式。

表 1-2 GF(16)域元素的表示形式

多 项 式	4 重	对 数	幂	$Z(n)$
0	0000	$-\infty$	0	0
1	0001	0	1	$-\infty$
α	0010	1	α	4
α^2	0100	2	α^2	8
α^3	1000	3	α^3	14
$\alpha+1$	0011	4	α^4	1
$\alpha^2+\alpha$	0110	5	α^5	10
$\alpha^3+\alpha^2$	1100	6	α^6	13
$\alpha^3+\alpha+1$	1011	7	α^7	9
α^2+1	0101	8	α^8	2
$\alpha^3+\alpha$	1010	9	α^9	7
$\alpha^2+\alpha+1$	0111	10	α^{10}	5
$\alpha^3+\alpha^2+\alpha$	1110	11	α^{11}	12
$\alpha^3+\alpha^2+\alpha+1$	1111	12	α^{12}	11
$\alpha^3+\alpha^2+1$	1101	13	α^{13}	6
α^3+1	1001	14	α^{14}	3

3. 最小多项式和分圆陪集

GF(2)及 GF(2^m)域上多项式有一重要性质：如果 β 是多项式的根，则 β^2、β^4、$\beta^{2^{(m-1)}}$ 等也是它的根。例如设 α 是

$$f(x)=x^3+x+1$$

的根，则有

$$f(\alpha)=\alpha^3+\alpha+1=(011)+(010)+(001)=(000)=0$$

运用以上性质，α^2、α^4 也应是它的根，即

$$f(\alpha^2)=\alpha^6+\alpha^2+1=(101)+(100)+(001)=(000)=0$$