

实用编码技术

蔡宗蔚编著

人民邮电出版社

实用编码技术

蔡宗蔚 编著

人民邮电出版社

内 容 提 要

本书比较通俗地全面地介绍编码的基本概念并以大量的实例阐述各种常用的码,例如汉明码、线性码、循环码、m 序列和卷积码等。

读者对象主要是初学编码技术的人员也可供从事数据传输、数据处理、电子计算机等方面的工程技术人员参考。

实 用 编 码 技 术

蔡宗蔚 编著

*

人民邮电出版社出版

北京东长安街27号

北京印刷一厂印刷

新华书店北京发行所发行

各地新华书店经售

*

开本: 787×1092 1/32 1983年2月第一版

印张: 9 4/32 页数: 146 1983年2月北京第一次印刷

字数: 208 千字 印数: 1—12,000 册

统一书号: 15045·总2653-有5273

定价: 1.15 元

前 言

随着通信的数字化和高速化，以及数据交换及传输技术的应用，产生了如何克服信息和数据在传输中出现差错的问题。解决这个问题有两种方法：一种是设法制造能避免差错的设备，另一种是采用编码的方法来发现和纠正差错，人们发现后一种途径是经济而且实用的。

人们常根据码的特性和用途进行分类，例如循环码、卷积码等是按其特性命名的；而同步码、测距码、线路传输码、地址码、纠错码等是按其用途命名的。在本书中，我们主要介绍一些常用的纠错码。

全书共分七章。第一、二章主要介绍码的基本概念，并且通过实用例子分析一些码的初步演变和发展。

第三章是本书的中心，介绍变形的汉明码和线性码是怎样演变过来的以及怎样完成纠错检差作用的，还叙述了线性码的几种不同划方式。

第四章介绍的循环码是目前在电子计算机和数据通信中被广泛采用的一种纠错码，它既能用来纠正随机差错，也可用来纠错突发差错。

第五章介绍了一种特殊的循环码—— m 序列以及它在扰乱器方面的应用。

第六章我们仿照线性码研究正在结构上较为复杂的卷积码。

第七章扼要地叙述了有关有限域的一些常识，并引入了纠

2 错 BCH 码。

本书在编写上着重采用以具体例子引入新问题的办法，因此在学习时必须弄懂每一个例子，并注意举例后所作的结论，这些结论代表着较一般的规律。我们的意图是通过举例，代替较复杂的数学分析或推导，从而引出规律，达到进一步应用的目的。根据作者的经验，很多简单例子往往是理论证明的重要启示。反过来，列举简单例子从各方面去说明理论又常常是消化理论的重要手段之一。

本书前身虽曾以讲义的形式使用过几次，并作了多次修改，力求通俗易懂，较容易地被初学者所接受，但由于作者水平和经验的限制，还存在着不少问题、缺点和错误，殷切希望读者批评指正。

蔡宗蔚

1982 年 12 月

目 录

第一章 绪论	1
1. 数字通信的简介	1
2. 二元对称信道	2
3. 噪声和引起的错型	3
4. 编码的目的和要求	4
5. 小结	6
第二章 码的基本概念	8
1. 普通码	9
2. 检错码	19
3. 小结	32
第三章 汉明码和线性码	33
1. 线性码	33
2. 研究码的工具——矩阵	37
3. 线性码的一致监督矩阵和纠检差错的规律性	47
4. 监督子的作用	51
5. 纠 1 错码和纠 1 检 2 错码的作法	56
6. 线性码的生成矩阵	67
7. 矩阵化为标准形式的方法	75
8. 线性码实现方式举例	79
9. 线性码在电子计算机的磁带机中的应用	84
10. 分组纵横监督码	87
11. 小结	93

第四章 循环码	96
1. (7,3)线性码	96
2. 码多项式与循环码的生成多项式	97
3. 循环码的生成多项式和生成矩阵	106
4. 循环码的一致监督矩阵和一致监督多项式	114
5. 除法电路	118
6. 利用除法电路编循环码的方法	125
7. 除法电路的变形	127
8. 梅吉特译码法	132
9. 捕错译码法	138
10. 小结	142
第五章 m 序列	144
1. 线性移位寄存器的状态和状态的转移	144
2. 线性移位寄存器状态的转移矩阵	146
3. 线性移位寄存器序列的递推关系	151
4. 转移矩阵的特征多项式	154
5. 用母函数研究特征多项式	165
6. m 序列的伪随机性	169
7. m 序列的用途	174
8. 扰乱器及其作用	177
9. 带循环输入的扰乱器的转移矩阵	180
10. 扰乱器的不利起动状态	188
11. 带有特殊循环输入的扰乱器	196
12. 小结	201
第六章 卷积码	202
1. 关于作卷积码的想法	202
2. 卷积码的生成矩阵	207

3. 卷积码的一致监督矩阵	214
4. 卷积码的第一截分组码	217
5. 卷积码的一致监督矩阵与生成矩阵的关系	220
6. 卷积码的生成多项式组, 哈夫曼时延算子表示法 ...	224
7. 卷积码的生成元和子生成元	232
8. 纠 1 错威纳——阿什码的作法	239
9. 择多逻辑译码法	248
10. 小结.....	253

第七章 关于有限域的一些知识与纠 2 错 BCH 码的引进

.....	255
1. 模 2 运算	255
2. 关于群的概念	256
3. 群码	258
4. 关于域的概念	260
5. 关于自然数的欧几里得算法	261
6. 模 p (p 为质数) 剩余代表所构成的有限域 $GF(p)$...	266
7. 有限域 $GF(2^n)$	268
8. 关于纠 2 错 BCH 码的引进.....	272
9. 有限域 $GF(2^n)$ 中元素的表达法	281
10. 小结.....	283

第一章 绪 论

1. 数字通信的简介

通信系统是用来传送消息的。为了传送消息，它通常必须通过末端设备将消息变为电信号。这样的电信号通常可分为两类：一类是模拟信号，又称连续信号，如电话机送话器输出的语言信号、摄像管产生的图象信号等，它们的电压（电流）取值为连续的时间函数；另一类是数字信号，又称离散信号，如电报数字和文字、雷达数据、遥控指令等，它们仅可能有有限个离散的取值。通常，我们把传输模拟信号的系统称为模拟通信系统，把传送数字信号的系统称为数字通信系统。

在模拟通信系统中，传输的是一个连续的模拟波形。这时，要求接收机能以较高的保真度来复现原发送的消息波形，因为我们考虑的是输出信噪比。而在数字通信系统中，传输的是有限个离散取值的信号之一。要求接收机能在存在各种干扰的条件下，正确判决（或检测）出当时发送的是哪一个离散值，因此我们关心的主要是错误概率。

数字传输的一个主要优点是在信道中可采用再生中继器。数字再生中继器对每个数据数字作出正确的判决，根据判决结果产生新的脉冲，并把它发送到线路上去，这样，由信道引起的失真或噪声就不会被累积。因此，只要在每隔适当距离就配置一个中继器，那末数字传输就可达到很长的距离。

第二个优点是，不论数字信号是代表离散数据还是数字模拟量，都可进行同样的处理，这就有助于实现自动转接。

第三个优点是，能使用数字集成电路，体积小，成本低，而且还易于进行保密通信。

在通信中，总是要求有发送和接收信息的人或机器，我们把它们分别叫做信源和受信者（信宿）。另外，还必须在信源和受信者之间插入一个供信息传输的通信线路，称为信道。信息在信道中传输时，我们会不可避免地遇到内部和外界的干扰而形成所谓噪声。这些联系在一起就构成一个简单、粗糙的通信模型，如图 1.1 所示。

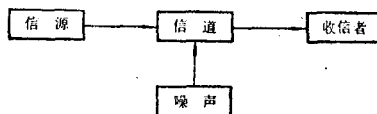


图 1.1 简单的通信系统模型

通常遇到的信源有：

- ① 人的语言；
- ② 温度、压强、水位、速度、流量、容量、

重量等人们需要预测的物理量；

- ③ 图象，表格；
- ④ 计算机处理的数据，等等。

为了研究实际信道，我们常常作出模拟实际信道的几种理想化信道，其中一种常用的是所谓二元对称信道。

2. 二元对称信道

设进入信道的数字为“1”，经信道传送后，由于噪声的影响，信道输出端得到的可能为“1”，也可能为“0”。如果进入信道时的数字为“1”（或“0”），而信道输出端得到的是“0”（或“1”），则称数字“1”（或“0”）经过信道传输后发生差错。假定数字经过信道后，不发生差错的概率为 $1-p$ ，发生差错的概率为 p ，那末这种信道通常称为二元对称信道，如图 1.2 所示。它的特点是：

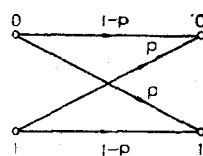


图 1.2 二元对称信道

- ① 信道中传送的信号只有“0”和“1”两种；
- ② “1”误为“0”，或“0”误为“1”这两事件都是互相独立的随机事件，它们所发生的概率相等，都等于 p ；
- ③ 数字“1”或“0”保持正确的概率也相等，都等于 $1-p$
 $\left(1-p > \frac{1}{2}\right)$ 。

由于特点①，信道称为二元的，由于特点②、③，信道称为对称的。

3. 噪声和引起的错型

一般地说，通信信道中的噪声可以分为两种：一种是高斯噪声，它是在设计调制解调器时所关心的重要对象。高斯噪声的来源是多方面的，而且是不可避免地存在着的。高斯噪声包括从发送和接收设备来的热噪声和散弹噪声、由传输媒介引起的热噪声以及由收信天线传来的辐射等。另一种是脉冲噪声，它的特征是信道在长时间的安静之后出现突发脉冲，其幅度远大于按正态分布律预测的幅度。这种噪声的来源有天然的也有人为的，包括雷电、开关瞬态、微波衰落以及维护工作中的偶然碰撞。在电话通信网里，低速和中速数据传输中的多数差错是由于脉冲噪声引起的。

由于噪声的存在，不论应用什么样的调制方式和解调方法，在接收端解调后的数据中都不可避免地会出现差错。通常，我们遇到的差错有两种。一种是随机差错，这时接收序列中前后位发生差错与否是互相独立的。产生随机差错的信道称为无记忆信道或随机信道，例如卫星信道等；另一种是突发差错，这时一个差错的出现往往影响到后面一串数字，也就是说，它们是统计相关的。这种信道称为有记忆信道，其特殊情形是突

发信道。设信道中传送的数据序列为 0 0 0 0 0 0 0 0 ……，由于噪声干扰变为 0 1 0 0 1 1 0 0 ……，则这种差错形式就是一个突发差错，第一个差错与最后一个差错数字之间的长度“5”称为突发长度，而差错形式“1 0 0 1 1”称为突发错型。短波、散射信道或存贮系统中磁带的缺陷或读写头的接触不良所引起的差错都属于这种差错。由于实际信道的复杂性，所遇到的差错也可能不是单纯的随机差错和突发差错，而是两者兼有，这种信道称为混合信道。

4. 编码的目的和要求

由上知，在信息传输过程中不可避免地会发生差错。人们自然会想，在收到一个数据序列后，如何判断它有无差错，又如何纠正这些差错？人们在实践的过程中不断地总结经验，逐步得到了一套“编码”的办法，即在发送端根据要传输的信息序列，通过编码器以一定的规则产生一些附加数字（称为监督数字或多余度数字），使原来不相关的信息序列变为相关的新的序列（称为码序列或码字），然后把新序列发送出去。人们可以通过编码的方法使信息具有纠检差错的能力。在码字到达接收端时，由于信道中干扰的影响，在码字 C 上已附加上一定的差错，称为错型 E ，所以接收端收到的是 $C + E$ ，它未必是一个码字，为此我们把 $C + E$ 称为接收序列（或接收矢量） R 。在一定条件下，这个接收序列 R 可通过译码器把差错自动纠正，恢复原来发送的码字（或者把接收序列中的差错检查出来，然后通知对方重新发送这个码字，直到正确地接收到有关码字为止）。这时的通信模型可粗糙地用图 1.3 表示。一般的编码器的编码都分两步进行，第一步把信源送来的信息编成二进制数字构成的序列，这部分设备称为信源编码器，第二步再把二进制

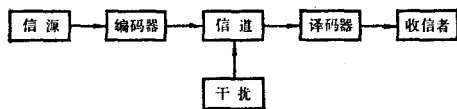


图 1.3 数据通信系统模型

序列编成具有纠检能力的二进制序列，这部分设备称为信道编码器，本书研究的只限于信道编码。事实上信道编码器的输出还得通过调制器使二进制序列转化为更适应于信道传输的信号。在接收端的译码器，也相应地由解调器、信道译码器、接收译码器等组成。这样，通信模型又可进一步画成如图 1.4 所示。

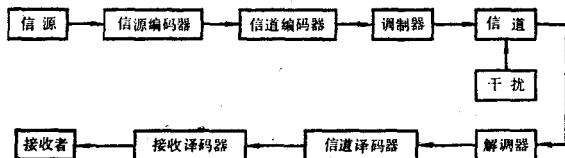


图 1.4 实用数据通信系统方框图

在编码的过程中，人们又产生了这样的问题，就是：

什么样的码，怎样编码才能既提高纠检差错的能力，又保证尽可能高的通信效率？这种码应具有什么样的构造规律才能使编、译码器的设计简单实用？

研究码的构造规律，一种方便的方法是研究码的构造的数学特性，即研究码的数学结构。例如可以用生成矩阵或一致监督矩阵来反映线性码和卷积码的数学结构，也可用转移矩阵或递推关系反映最长线性移位寄存器序列的数学结构，又可利用

某种多项式的倍式按 X^n-1 求余式而得到的集合来反映循环码的数学规律等等，有时把部分编码问题强调为“代数编码方法”就是这个道理。虽然编码未必求助于数学方法，更未必单纯地求助于代数，但是寻求编码的规律总是客观的需要，而借助于数学方法只是一种方便，但决不是唯一的途径。

由于生产实践上的需要人们常对编码提出一定的要求，例如：

- ① 码长尽量短；
- ② 信息率尽量高；
- ③ 纠检能力尽量大；
- ④ 编码规律尽量简单；
- ⑤ 具体实现的设备要求简单易做，费用节省；
- ⑥ 与信道的差错统计特性尽量匹配等。

5. 小 结

这一章主要是介绍一些有关编码问题的预备知识。

通信系统由信源、信道和信宿三者构成。信息在信道中传输时，由于受到各种干扰而不可避免地引起差错。通常遇到的差错有随机差错和突发差错两种。为了判断差错的有无以及确定存在差错后如何纠正，人们提出了“编码”的要求，同时也逐步总结了一些“编码”的方法。

为了简化对问题的研究，人们常常把许多实际信道理想化为二元对称信道。普通的编码问题都是在二元对称信道中考虑的。

学习本章要求了解：

1. 通信系统的简单框图。
2. 二元对称信道的特征。

3. 两种差错的特征和区别。
4. 为什么要编码？什么是编码？
5. 编码有哪些要求？

第二章 码的基本概念

我国古代以烽火为号，就是用符号代表消息的一个先例，可以认为它就是今天的“码”的最原始的一种形式。但是，接近于今天的码的形式应该追溯到由莫尔斯发明的电码，即莫尔斯电码，它被广泛使用于早期的电报通信中。在采用电传打字机后，人们又引进了五单位电码。这些在通信初期引进的码，只是用来代表某些消息，没有纠正或发现差错的能力，在人们发现差错时，可以采取另外的一些辅助措施来纠正这些差错。这种没有纠正和发现差错的能力的码叫普通码。莫尔斯电码、五单位电码、8421 码、等都是普通码。随着通信速率的不断提高，人们对通信质量的要求也越来越迫切，要求码的本身能具有发现差错和纠正差错的能力。偶监督码、奇监督码、定重码就是人们最初找到的具有发现差错能力的码，但是这些码没有纠正差错的能力。第一个引进具有纠正差错能力的码的是汉明，为了纪念他，人们把这码叫做汉明码，我们把它简记作 H 码。H 码的编译（把消息编成 H 码，以及由 H 码译成原来的消息）过程并不方便。后来，人们在改进它们的过程中逐步得到了具有纠错能力的循环码、BCH 码和卷积码的简单的编译码电路，才使码的实用问题得到了充分的肯定。这种具有纠正差错能力的码叫做纠错码，单单具有发现差错的能力而不能纠正差错的码叫做检错码。人们也常把纠错码用来检错。从第三章起我们主要分析上述这些重要的纠错码。

在本章中我们先介绍一些普通码，并通过它说明有关码的一些基本概念。然后介绍一些检错码，使我们从中看到它们的

演变过程。

1. 普通码

在本节中我们介绍几种常用的普通码，通过它们来说明：什么叫一个码？什么叫码字？什么叫码元？码字和码的区别和关系如何？同时还可看到，由于实际使用的目的不同，码可以具有各种不同的形式，并带有各种不同的特点。

例 1 莫尔斯电码

莫尔斯电码是以不同长度、不同数量的电脉冲的各种组合来区别各种符号的，例如：

A	• —
B	— • • •
C	— • — •
D	— • •
E	•
⋮	⋮
⋮	⋮
⋮	⋮
数字 0	— — — — —
⋮	⋮
⋮	⋮
⋮	⋮

其中短的脉冲称为点，长的脉冲称为划。点是最短的信号，称为基本信号。一划等于三点的长度。点与划、划与划、或点与点之间的间隔等于一点的长度。字母或数字之间的间隔等于三点或一划的长度。字与字之间，留出五点的长度。

字母“E”的长度等于 4 个基本信号。

数字“0”的长度等于 22 个基本信号。

关于基本信号的每个具体的组合叫做一个码字。例如“• —”是一个码字，而每一个符号（字母或数字）与一组基本信号