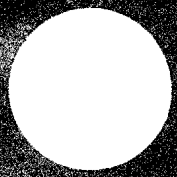


宋焕章 编著



计算机纠错编码

JISUANJI
JIUCUO BIANMA

国防科技大学出版社

919.3

内 容 简 介

本书是为计算机专业研究生和高年级本科生编写的教材。作者结合多年从事纠错编码教学的经验，广泛吸收国内外特别是国防科技大学计算机系在纠错编码领域的理论研究和应用成果，在试用讲义的基础上修订而成。

本书理论与应用并重，概念清晰，例题丰富。全书共分为八章：一、纠错码的基本概念；二、纠错码的数学基础；三、线性分组码；四、循环码基础；五、一些重要的循环码；六、算术码；七、主存贮器和网络系统错误控制；八、外存贮器错误控制。

计算机纠错编码

宋焕章 编著

责任编辑 王金荣

封面设计 宁建国

*

国防科技大学出版社 出版发行

湖南省新华书店经销

国防科技大学印刷厂印装

*

开本：787×1092 1/16 印张：15 字数：334千
1990年6月第一版 1990年6月第一次印刷 印数：1200册

ISBN 7-81024-110-9
TP·19 定价：3.00元

前 言

在电子数字计算机系统中，由于各种原因，运算、存贮及传输的信息都可能发生错误。这类错误，并非计算机的误差。对于二进制信息，0错成1，或1错成0，结果便可能截然不同。如不采取措施去避免或纠正这些错误，则机器的速度再高、容量再大也都失去了意义。

最常见的措施是设置纠错编码。它将运算、存贮和传输的彼此互不相关的信息依一定规则进行组织，使之具有一定的相关性，从而自动纠正或检测错误。因此，纠错编码是一种容错技术。纠错编码源于数字通信，是信息论的重要组成部分。多年来的研究与实践表明，在计算机系统内部或系统之间，纠错编码对提高系统的可靠性成效显著。所以纠错编码在计算机领域得到越来越广泛的应用。

研究纠错编码，主要是研究码的构造规律，即码的数学特性。纠错编码较多地涉及到线性代数、近世代数等数学知识，因而将其强调为“代数编码”并非言过其实。编码虽未必单纯求助于代数，但数学方法却更深刻地反映其本质，也是最方便有效的途径。然而，纠错编码的迅速发展更重要的是在于应用。通信和计算机的蓬勃发展及VLSI的发展为纠错编码提供了广阔的天地。

本书旨在讨论纠错编码的基本概念及其在计算机领域的应用。笔者从事计算机专业的纠错编码教学多年，1986年油印讲义印出后，曾广泛征求学生及老师的意见，特别是得到中科院计算所沈理、武汉大学张焕国、国防科工委指挥技术学院饶世麟及本系黄克勋等专家教授的指导与帮助。在编写过程中，参阅了王新梅教授的《纠错码》、饶世麟教授的《编码原理》及其他文献资料。何自强副教授及吴玲达、唐玉华、张春元硕士认真审阅了全稿。在此，特向他们致以深切的谢意。

纠错编码的理论研究和工程应用发展迅速，资料非常丰富。因笔者水平有限，使本书在选材和阐述等方面难免有不当和错误，敬请读者批评指正。

作 者

1989年12月

目 录

第一章 纠错码的基本概念

1.1 数字通信系统及其信道模型	1
1.2 纠错码和错误控制	3
1.2.1 纠错码及其分类	3
1.2.2 错误控制	5
1.3 分组码	5
1.4 信道编码定理	8
1.5 常用检错码	9
1.5.1 水平一致监督码	9
1.5.2 水平垂直一致监督码 (方阵码)	9
1.5.3 横向斜向一致监督码	10
1.5.4 定比码	10
1.5.5 群计数码	11
习题	12

第二章 纠错码的数学基础

2.1 代数结构	13
2.1.1 群	13
2.1.2 环	14
2.1.3 域	14
2.2 矩阵和线性空间	15
2.2.1 线性空间	15
2.2.2 矩阵	17
2.3 子群、陪集和子环	21
2.4 域上的多项式环	23
2.4.1 有限域上的多项式	23
2.4.2 多项式剩余类环	28
2.5 孙子定理	30
2.6 平方剩余	32
习题	35

第三章 线性分组码

3.1 线性分组码的基本概念	35
3.2 距离、重量和纠错能力	36
3.3 线性分组码的编码	38
3.3.1 一致校验矩阵	38
3.3.2 生成矩阵	41

3.3.3 对偶码和缩短码	43
3.4 线性分组码的译码	44
3.4.1 伴随式	44
3.4.2 陪集和标准阵列	48
3.5 Hamming 码	51
3.6 修正码	53
3.6.1 扩展码和删余码	53
3.6.2 增删码	55
3.7 最佳奇权码	56
3.7.1 H 矩阵的特性和构成	56
3.7.2 循环向量法	57
3.7.3 分解合并法	61
3.8 分组码的性能界	64
3.8.1 Plotkin界	65
3.8.2 Hamming界	65
3.8.3 Varsharmov-Gibert界	66

习题	67
----	----

第四章 循环码基础

4.1 理想和循环码	69
4.2 循环码的编码	71
4.2.1 一般循环码的 G 矩阵和 H 矩阵	71
4.2.2 系统循环码的编码	73
4.3 用多项式的根定义循环码	75
4.4 缩短循环码和对偶循环码	78
4.5 多项式运算电路	79
4.5.1 多项式乘法电路	80
4.5.2 多项式除法电路	82
4.6 编码器	84
4.6.1 用 $g(x)$ 电路构成的 r 级 编码器	84
4.6.2 用 $h(x)$ 电路构成的 k 级编码器	86
4.7 循环码的译码	87
4.7.1 伴随式计算和一般	

译码器·····	88	6.4.4 子码和复合码·····	145
4.7.2 Meggit通用译码器·····	91	6.4.5 最小距离·····	148
4.8 捕错译码·····	92	6.4.6 译码方法·····	148
4.8.1 系统循环码的捕错译码 ·····	92	习题·····	150
4.8.2 改进的捕错译码·····	94	第七章 主存贮器和网络系统的错误控制	
习题·····	96	7.1 存贮器错误类型·····	152
第五章 一些重要的循环码		7.1.1 随机错误·····	152
5.1 循环Hamming码·····	97	7.1.2 B 邻接片错误·····	152
5.2 Golay码·····	98	7.1.3 消失错误·····	152
5.3 BCH码·····	101	7.1.4 单向错误·····	152
5.3.1 基本概念·····	101	7.2 随机错误控制·····	153
5.3.2 BCH码的译码·····	105	7.2.1 奇偶码·····	153
5.4 RS码·····	109	7.2.2 Hamming码·····	153
5.5 大数逻辑可译码·····	113	7.2.3 最佳奇权码·····	154
5.5.1 一步大数逻辑可译码·····	113	7.2.4 多个随机错误的纠正·····	159
5.5.2 L 步大数逻辑可译码·····	118	7.3 B 邻接片错误控制·····	160
5.6 Fire码·····	120	7.3.1 b 邻接位错和 B 邻接片 错码的概念·····	160
5.6.1 码的突发错误纠正能力·····	120	7.3.2 单错纠正/双错检测/ 单字节错检测码·····	161
5.6.2 Fire码的基本概念·····	122	7.3.3 单字节错纠正码(SBC)·····	162
5.6.3 Fire码的编译码器·····	123	7.3.4 单字节纠正/双字节错检测 码(SBC/DBD)·····	168
习题·····	128	7.3.5 多字节错纠正和检测码·····	168
第六章 算术码		7.4 消失错误控制·····	169
6.1 算术重量和算术距离·····	129	7.4.1 错误定位方法·····	169
6.2 倍数码·····	131	7.4.2 译码算法·····	169
6.2.1 AN 码的基本概念·····	131	7.4.3 单随机错单消失错纠正/单 随机错双消失错检测码 ·····	170
6.2.2 AN 码的纠错能力·····	132	7.5 单向错误控制·····	170
6.2.3 AN 码与其他线性码 比较·····	135	7.5.1 单向错误的基本概念·····	170
6.2.4 $AN+B$ 码·····	137	7.5.2 SEC/AUED码·····	172
6.2.5 AN 码的实现·····	138	7.5.3 Berger码·····	176
6.2.6 伴随式译码·····	139	7.5.4 循环 AN 码·····	177
6.3 剩余码·····	140	7.5.5 推广Berger码·····	178
6.3.1 剩余码的基本概念·····	140	7.6 网络系统错误控制·····	181
6.3.2 剩余码检测错误·····	140	7.7 复数旋转码·····	184
6.3.3 剩余码的实现·····	141	7.7.1 复数旋转因子·····	184
6.4 循环 AN 码·····	141	7.7.2 复数旋转码及其结构·····	184
6.4.1 循环 AN 码的概念·····	141	7.7.3 编码方法·····	187
6.4.2 循环 AN 码的生成·····	142		
6.4.3 循环 AN 码的循环周期 ·····	144		

7.7.4 译码方法	187	8.4.2 $g(x)$ 电路的自发运算规律	206
7.7.5 复数旋转码特性分析	190	8.4.3 快速移位纠错译码	208
习题	191	8.4.4 译码流程和实例分析	209
第八章 外存储器错误控制		8.5 采用孙子定理快速译码	211
8.1 磁带循环冗余校验	192	8.6 Fire码的反向快速移位译码	214
8.1.1 基本思想	192	8.7 FMG码	218
8.1.2 实现方法	193	8.7.1 码的构成	218
8.1.3 采用长除法求校验字符	194	8.7.2 采用孙子定理快速译码	219
8.1.4 反读纠错	197	8.7.3 反向快速移位译码	219
8.2 磁带最佳矩形码	197	8.8 $GF(2^6)$ 上突发错误纠错码	220
8.2.1 编码	197	8.8.1 $GF(2^8)$ 上RS码	220
8.2.2 译码	199	8.8.2 $GF(2^{16})$ 上线性分组码	222
8.2.3 单道错误纠正	200	8.8.3 $GF(2^{16})$ 上四度交错的独立编码	226
8.2.4 双道删除错误纠正	201	8.9 光盘错误控制	229
8.3 海量宽带存储器的BCH码	202	习题	230
8.3.1 磁带数据格式	202	参考文献	231
8.3.2 编码	202		
8.3.3 译码	203		
8.4 磁盘Fire码的快速移位译码	205		
8.4.1 快速移位的基本思想	205		

第一章 纠错码的基本概念

纠错编码最初源于通信系统。因此，首先简介数字通信系统及其信道模型，然后讨论差错控制的基本思想，最后归纳一下常用的简单检错码。

1.1 数字通信系统及其信道模型

采用某种方法、借助某种媒质将信息从甲地传送到乙地的过程叫通信。甲地发送信息者叫信源，乙地接收信息者叫信宿。若传送是连续的电信号，则叫模拟通信，如由电话、广播传送的声音信息，由电视、传真传送的文字图象信息等。若传送的是数字信号，则叫数字通信，如电报、数据通信等。

完成数字通信的有关部件构成数字通信系统。无论是数据通信、雷达、遥测遥控，还是电子数字计算机系统内部或系统之间的信息存贮或传输，均可用图1.1所示模型描述。

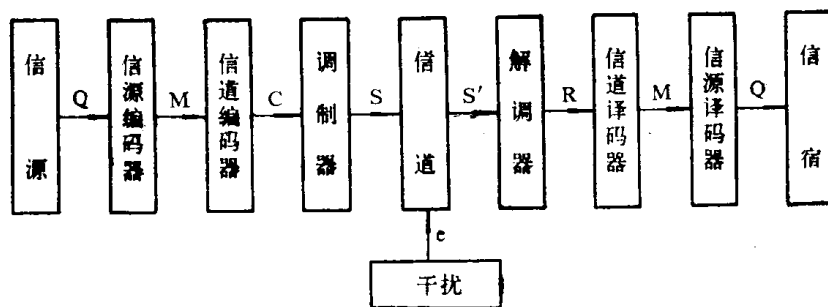


图 1.1 数字通信系统模型

信源发出的消息 Q 如语言、文字、图象等经信源编码器转换成离散的数字信息序列 M ，然后经信道编码器变换成一定的编码序列 C ，最后经调制器调制成便于传输或存贮的形式送往传送信息的通道——信道。由于信道常受到干扰，因而解调器接收的可能叠加有错误的信息 $S' = S + e$ ，送给信道译码器的则是 $R = C + e$ ，信道译码器力图检测或纠正错误，以恢复成 M 或其近似值，最后经信源译码器还原成 Q 送给信宿。

上述过程中，涉及到两类不同的编码：信源编码和信道编码。信源按一定规律进行数字变换的过程即信源编码 (Information Source Coding)，它主要解决模拟信号的数字化和提高数字信号的有效性。为提高信息传输的可靠性而采用的编码叫信道编码 (Channel Coding)，它是根据信道的概率特性进行抗干扰编码，又称为纠错编码 (Error Correcting Code)。

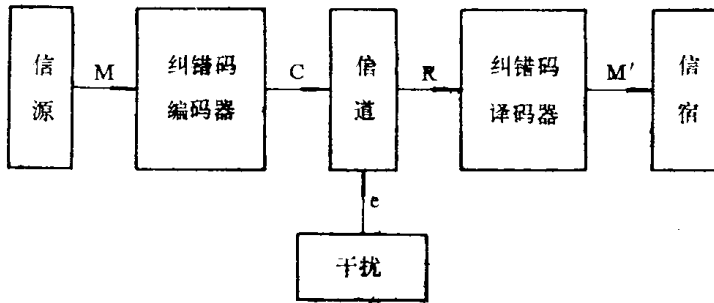


图 1.2 简化的通信系统模型

在计算机系统中,运算、传输和存贮的均是二元(或二进制)数字信息,且特别注重其可靠性,故仅讨论纠错编码。此时,系统模型可简化成图 1.2 所示。

图中信源可以是计算机及其外围设备,其输出为二元数字序列 M。信道是传输信息的媒介,既包括传输信息的通道或存贮信息的介质,也包括调制和解调装置。信宿亦指计算机或外围设备,以及可接收信息的其它装置。

我们不考虑连续波形的信道,仅讨论编码信道即离散信道。离散信道可分为无记忆信道和有记忆信道。无记忆信道又称**随机信道**(Random Channel),它产生随机错误,这种错误的特点是各码元是否出错是相互独立的,即每一个差错的出现与其前后是否有错无关。有记忆信道又称**突发信道**或**猝发信道**(Burst Channel),它产生突发错误。这种错误是固定不变、前后相关、密集成串的。在一个突发错误持续长度内,开头和末尾的码元总是错误的,中间的码元则不一定都错,但错误的码元相对较多。在数据传输中,如在含有错误位的一串信号中,两个相邻错误位之间正确位的数目小于规定的标准,则可将这些错误位当作一个突发错误处理。

由于实际信道干扰的复杂性,错误往往不是一种,而是两种并存。随机错误与突发错误并存的信道叫**组合信道**或**复合信道**。

最简单最典型的理想信道是二元对称信道BSC(Binary Symmetric Channel),如图 1.3(a)所示。这种信道中,1错成0或0错成1的概率相等,均为 q 。于是 q 就是码元错误概率,或称**误码率**(Error Rate),而码元正确接收的概率即**正码率**为 $p=1-q$ 。

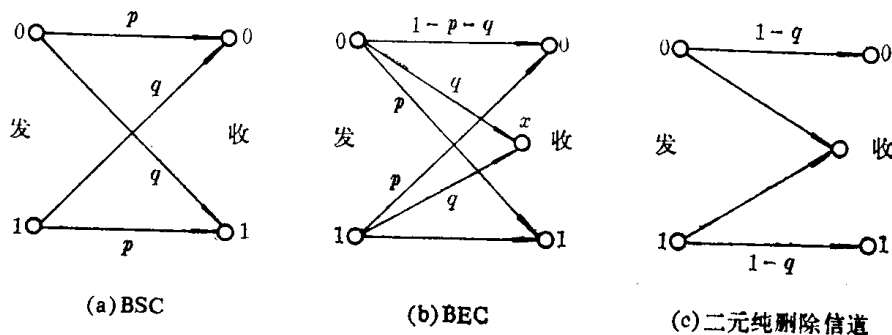


图 1.3 二元对称信道

经二元对称信道传输 n 比特(bit)信息序列出现 t 个错误的概率 p_t ,据贝努利定理为

$$p_t = \binom{n}{t} p^{n-t} q^t = \binom{n}{t} p^{n-t} (1-p)^t = \binom{n}{t} (1-q)^{n-t} q^t \quad (1.1)$$

其中二项式系数

$$\binom{n}{t} = \frac{n!}{t!(n-t)!} = \frac{n(n-1)\cdots(n-t+1)}{t \cdot (t-1) \cdots 3 \cdot 2 \cdot 1}$$

一般均有 $q \ll 1$, 故

$$p_i = \binom{n}{t} q^t \quad (1.2)$$

在接收信息时, 译码判决非 0 即 1, 这是一种“硬判决”。如对接收的某位码元暂不作判决, 而是输出一个未知或待定的信号 x , 则称之为“删除”符号。在作删除判决时, 信道可用图 1.3(b) 表示, 称之为二元删除信道 BEC(Binary Elimination Channel)。这也是一种二元对称信道。图中的 p 为信道转移概率, q 为删除概率。在作删除处理时, p 一般很小而忽略不计, 则 BEC 可用图 1.3(c) 代替, 称为二元纯删除信道, 一般说到 BEC 即指这种信道。

1.2 纠错码和错误控制

1.2.1 纠错码及其分类

什么是纠错码? 为什么它能自动检测或纠正错误呢? 为说明问题, 我们先考察最简单的检错码——奇偶校验码。

众所周知, 所谓奇偶校验码是对传输的每一组信息都设置一个校验位, 使每一组信息中 1 的个数都为奇数或偶数。接收时如果一组信息中 1 的个数不是奇数或偶数, 则该组信息出现了错误。但是, 这时无法确定这一组信息中究竟是哪一位出错, 故仅能检错而不能纠错。

例如对八单位纸带设置奇偶校验可作如下处理: 每一排孔中用七个表示一组二进制信息, 而用一个孔作为校验孔。长度为 7 的所有二进制信息组合可看成是二元域上的 7 维向量空间 $V_7(F_2)$, 每一排孔中的七位原始信息组就是一个 7 维行向量, 设为 $(c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ 。增加一位奇偶校验位, 就将一个 7 维行向量扩充成为了一个 8 维行向量

$$\alpha: (c_0, c_1, c_2, c_3, c_4, c_5, c_6) \rightarrow (c_0, c_1, c_2, c_3, c_4, c_5, c_6, \sum_{i=0}^6 c_i)$$

其中求和是二元域 $GF(2)$ 即 F_2 中定义的运算, 即半加。这样, 记录在纸带上的便是一组一组的八位二进制信息, 它们集合即为

$$V_8(F_2) = (c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7 = \sum_{i=0}^6 c_i)$$

显然, $V_8(F_2)$ 中的向量有一重要特征, 即其八个分量之和一定等于零, 即

$$\sum_{i=0}^7 c_i = 0 \quad (1.3)$$

当从纸带上读出一排孔信息不满足上述特征时, 就说明读出有错。设读出一排孔信息即接收向量为

$$R = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7)$$

则应有

$$\sum_{i=0}^7 r_i = 0$$

否则说明有一个或奇数个位发生了错误。

可见，奇偶校验码之所以可检测奇数个错误，是它将毫无关联的一组信息通过设置校验位后满足方程(1.3)，从而使这一组信息具有了一定的相关性。根据这一相关性对接收信息译码，就可判断是否发生了错误。

通过设置附加的校验位，即使传输的信息增加了一定的冗余度。这种冗余度使原来无规律或规律性不强的一组信息具有了某种相关性，接收信息时再依据这种相关性译码从而检错或纠正错误，这就是错误控制的基本思想。用来检测或纠正信息错误的冗余码就是所谓纠错码。

一般地，设信源的原始数字信息的集合是 $V_k(F_q)$ ， q 是一个素数的幂， n 是大于 k 的一个整数，如 α 是从 $V_k(F_q)$ 映入 $V_n(F_q)$ 的一个一一映射， $\alpha: V_k(F_q) \rightarrow V_n(F_q)$ ，记 $C = \alpha(V_k(F_q))$ ，则 $C \subset V_n(F_q)$ ，称 C 为码， C 中的向量叫码字或码组，码字的分量叫码元。码元在二元域 F_2 中取值，则称码为二源码。 n 叫码长， $V_n(F_q)$ 中的向量叫字。显然，所有码字的集合是 $V_n(F_q)$ 的子集。

如果在发送一个码字后，在传输过程中有 $\leq t$ 个位置的码元或分量出错，而接收译码时可以判断出这种错误，则 C 叫码长为 n 的可检测 t 个差错的检错码， α 叫检错编码；若接收时还可正确译出原发送的码字，则 C 叫码长为 n 的可纠正 t 个错误的纠错码，而 α 叫纠错编码。检错编码和纠错编码有时统称为纠错编码。

前述奇偶校验码对无错或偶数个错误，译码时均满足其编码规则，而单个或奇数个错误则使编码规则遭到破坏，故奇偶码是一个可检测单个或奇数个差错的检错码。

纠错码是十分活跃的学科，在信息、通信和计算机领域中广为应用。除据纠错能力可分为检错码和纠错码外，还可从不同角度进行分类，如图1.4所示。

(1) 根据校验元与信息元之间的关系分为线性码与非线性码。校验元与信息元之间呈线性关系，即可把校验规则用线性方程组表示的叫线性码 (Linear Code)，如不存在线性关系则叫非线性码。

(2) 按对信息处理方法的不同可分为分组码与卷积码。对信源输出的序列，按 k 个信息元进行分组，每组设置 r 个校验元，形成一个长为 $n = k + r$ 的码字，该码字的校验元仅与本码字的 k 个信息元有关，与别的码字无关，这样按组分别处理的编码是分组码 (Block Code)。若码长为 n 位，校验元为 r 位，如此 r 个校验元不仅与本组的 k 个信息元有关，而且也与前 m 组的信息元有关，则称之为卷积码 (Convolutional Code)或连环码 (Recurrent Code)。

(3) 按照码字的循环结构可分为循环码和非循环码。在循环码中，任一码字循环移位得到的仍是其中一个码字。而非循环码中，一个码字的循环移位后不一定是该码的一个码字。

(4) 根据所纠错误类型可分为纠正随机错误码、纠正突发错误码、纠正随机与突发错误码等。

(5) 按研究码的数学方法分类，有代数码、几何码、算术码等。

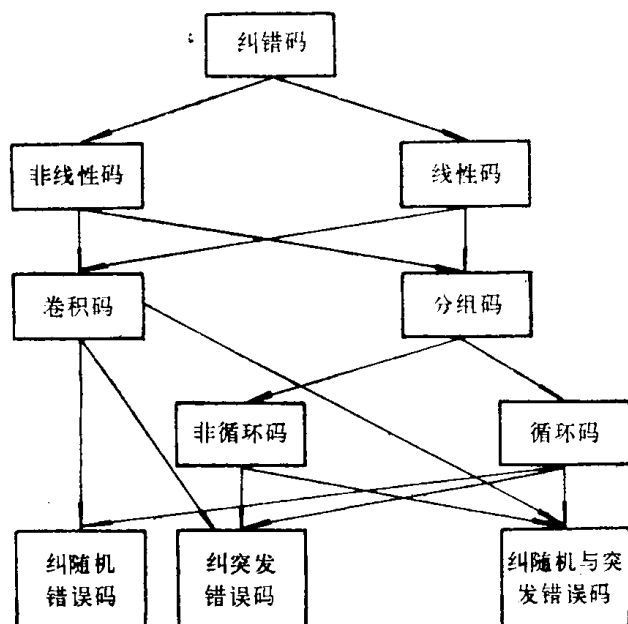


图 1.4 纠错码分类

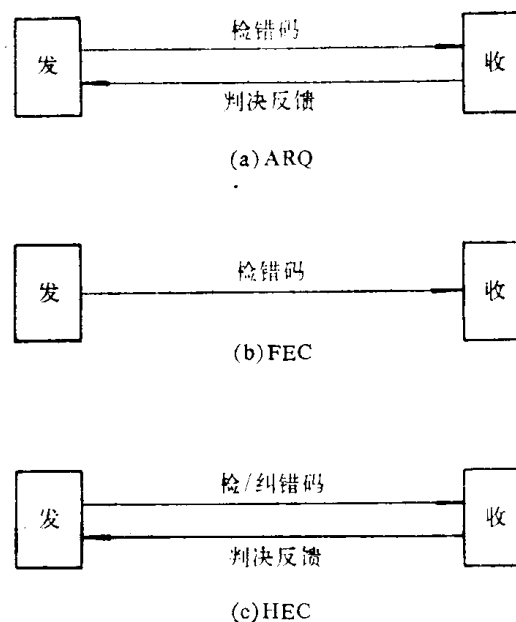


图 1.5 错误控制方式

1.2.2 错误控制

应用纠错码进行错误控制，一般有三种方式。

一、自动重发请求方式ARQ

采用ARQ(Automatic Repeat Request)方式时,发方发送的是经过检错编码的码字,收方译码时判断接收字是否有错,并将结果反馈告知发方。若无错则继续发送新的码字,否则请求重发,直至收方认为正确为止,如图1.5(a)所示。

二、前向纠错方式FEC

如图1.5(b)所示,采用FEC (Forward Error Control) 方式时,发方发送的是可纠正错误的码字,收方译码时,根据编码规则可自动纠正传送中出现的差错。显然,要可自动纠错,编译码装置均比ARQ方式复杂。但随着LSI 的不断发展,这种方式应用愈来愈多。

三、混合纠错方式HEC

HEC(Hybrid Error Control)是上述两种方式的综合。发方发送的是既可检错又可纠错的码字,收方译码时若发现出错的个数在码的纠错能力之内,则自动纠正;若出错个数超过码的纠错能力不能纠正,但可检测,则反馈告知发方重发,如图1.5(c)所示。

实际应用中,怎样选择错误控制方式呢?一般而言,应根据系统要求,结合信道出错概率及所使用的设备、器件等因素综合考虑。

1.3 分组码

计算机系统中,信息均按字节或字组织,故一般采用分组码。

对信源输出的序列,若按每组长 k 位进行分组,则在二进制情况下共有 2^k 个不同组

合。若按某一种规则,将每一组 k 位增加 r 位校验位, $r=n-k$,使之成为具有一定纠错或检错能力的码字,则此 2^k 个码字集合构成**分组码**。若对每一码长为 n 的码字,前面 $k=n-r$ 位是原始的信息组,后 r 位是校验位且是信息位的线性函数,则称该码为**系统线性分组码**记为 (n, k) 。

一个长为 n 的序列称为 **n 重**。在二进制情况,共有 2^n 个 n 重。而符合一定编码规则的 2^k 个 n 重称为**许用码字**(Permissible Code)或合法码字,简称码字。而余下的 $2^n - 2^k$ 个 n 重是不符合编码规则的非法码字称为**禁用码字**(NonPermissible Code)。发方发送的是许用码字,若收方收到的是禁用码字,则说明传输发生了错误。

在 (n, k) 线性分组码中,常用**编码效率**衡量码的有效性,它定义为信息位在码字中所占比重

$$R = \frac{k}{n} \quad (1.5)$$

编码效率 R 又称**传信率**,简称**码率**或**速率**, R 愈大,表明码的冗余度愈小。

若 C 是一个码字,由于信道存在干扰,接收时变成了字 $R=C+E$,这里 E 为错误模式或错误图形(Error Pattern)。对于一个经信道传输的码字,若在发生错误的码元位置上用“1”表示,在未发生错误的码元位置用“0”表示,则可以构成一个新的 n 重,这就是错误模式。若 $C=11111000$,而 $R=10110101$,则 $E=01001101$,即是发送码字的第二、五、六、八位产生了错误。

一般,若发送码字为 $C=c_{n-1}c_{n-2}\cdots c_1c_0$,而接收字为 $R=r_{n-1}r_{n-2}\cdots r_1r_0$,错误模式为 $E=e_{n-1}e_{n-2}\cdots e_1e_0$,则 R 就是 C 与 E 模2加的结果。即

$$R = C + E \quad \text{mod } 2 \quad (1.6)$$

或
$$C = R + E \quad \text{mod } 2 \quad (1.7)$$

对于突发错误,常用**突发错误长度** b 表示错误持续的时间或位数。如 $E=100101$,则 $b=6$ 。对于一个长度 $\leq b$ 的错误模式,其错误模式的类型共 $2^b - 1$ 个。例如对于 $b \leq 4$ 的错误模式共有 $2^4 - 1 = 8$ 种,即1111,1011,1001,1101,111,101,11,1。

两个相邻突发错误之间正确码元的位数叫**保障区间**(Ensure Area)。

码元被错误接收的概率叫**误码率**(Error Rate),是反映信道传输可靠性的参数,通常为

$$P_e = \frac{\text{错误接收的码元数}}{\text{接收的码元总数}} \quad (1.8)$$

分组码中,重复码和奇偶码是两个最简单的例子。

例1.1 $(n, 1)$ 重复码

该码信息位数 $k=1$,校验位数 $r=n-k=n-1$,因校验元是信息元的重复,故称之为重复码。如设 $n=3$,则是三重码,其许用码字有 $2^1=2$ 个:000,111。而禁用码字有 $2^3 - 2^1=6$ 个:001,010,100,011,101,110。该码效率为 $R=1/3$ 。

显而易见,对于 $(n, 1)$ 重复码, n 愈大,则 R 愈小。此意味着校验位增多,冗余度加大,照理码的抗干扰能力愈大。

例如 $(2, 1)$ 码,许用码字为00和11。它们以码元相等的可能性,即等概率发送时 $p(0)$

$=p(1)=1/2$. 经二元对称信道传输, 码元发生错误彼此独立, 且一般错误概率 $q < 1/2$. 无论发送00还是11, 若出现一位错, 则收方接收为01或10, 均是非法码字, 故可发现错误. 但收方收到01或10时, 译码判决是应为00还是11呢? 无法确定. 因此, 译码时不能纠错判决, 故(2,1)码是可检测一位错误的分组码, 其实质就是偶校码.

但前述(3,1)码不同, 若收方接收是001, 010, 100之一时, 译码可判为000; 而接收是011, 101, 110时, 则译码可判为111. 为什么前一情况会判为000而不是111呢? 这是因为收到001, 010, 100之一时, 经判决发现它们与000只相差一位, 而与111相差2位, 即“最象”000而“不象”111. 同样在后一情况则可判为111而非000. 可见, (3,1)码可以纠正单个错误. 当仅用于检错, 则接收只要不是000或111均报告有错, 因此, 它可检测1个和2个错误. 这说明(3,1)码的抗干扰能力比(2,1)码强, 但(3,1)码效率比(2,1)码的要低.

上述根据接收字“最象”哪个码字就译码判决为哪个码字的方法叫最大似然译码。(Maximum Likelihood Decode). 它是基于这一前提: 一个码字在传送时出错个数较少的可能性比一个码字传送时出错个数较多的可能性要大. 从直观上看, 要求信道正确传送的可能性大于错误传送的可能性, 这是合乎情理的. 否则, 信道可靠性太低, 还有什么实用价值呢?

若用概率表示似然函数, 则当发送码字 C_i 后, 根据接收字 R_j 计算条件概率 $p(R_j|C_i)$. 若条件概率 $p(R_j|C_i)$ 最大, 即若 $p(R_j|C_i) > p(R_j|C_i), \forall i \neq i$, 则译码判决是条件概率最大者, 即 R_j 译为 C_i .

若(3,1)码每位码元的出错概率为 q , 正确接收的概率为 p , 则任何一码元被正确接收三次的概率为 p^3 , 错一次正确二次的概率为 p^2q . 一个码字错一个的概率为 $3p^2q$, 故能正确接收及单错纠错的概率共为 $p^3 + 3p^2q$, 而错误接收的概率为 $3pq^2 + q^3$. 若单个码元出错概率为 $q=0.1$, 则经编码后单错概率减为

$$p_e = q^3 + 3pq^2 = 0.1^3 + 3 \times 0.9 \times 0.1^2 = 2.8 \times 10^{-2}$$

可靠性提高的代价是效率降低了2/3, 即 $R=1/3$.

例1.2 $(n, n-1)$ 奇偶码

奇偶码是只有一个校验元的线性分组码, 设校验元为 c_0 , 则编码规则为

$$c_{n-1} + c_{n-2} + \dots + c_1 + c_0 = 0 \quad \text{mod } 2 \quad (1.9)$$

$$\text{或} \quad c_{n-1} + c_{n-2} + \dots + c_1 + c_0 = 1 \quad \text{mod } 2 \quad (1.10)$$

式(1.9)保证每个码字中“1”的个数为偶数, 故称偶校码; (1.10)式保证每个码字中“1”的个数为奇数, 故称奇校码.

如(3,2)偶校码, 对于 $2^2=4$ 个信息组可据式(1.9)得到相应4个码字

$$00 \rightarrow 000, 01 \rightarrow 011, 10 \rightarrow 101, 11 \rightarrow 110,$$

该码的 $R=2/3$, 也检测一个错误. 译码的误码率为

$$P_e = \binom{3}{2} pq^2 = 3 \times 0.9 \times 0.1^2 = 2.7 \times 10^{-2}$$

综上所述不难看出: 随着 n 的增大, 重复码的抗干扰能力愈来愈强, 但 R 愈来愈小, 即当 $n \rightarrow \infty$ 时, $R \rightarrow 0$. 而对奇偶码, 当 n 增大时, R 愈来愈大, 即 $n \rightarrow \infty$ 时, $R \rightarrow 1$, 但抗

干扰能力愈来愈差。前者是低效码，后者则是低可靠性码，两者都不理想。那么是否存在一种码，随着 n 的增加，其纠错能力和传信率都保持一定呢。也就是说，能否找到一种码，既有高的传信率，又有强的抗干扰能力呢？Shannon 的信道编码定理对此作了肯定的回答。

1.4 信道编码定理

信道传输信息的最大能力或传输信息的最大值叫信道容量，它定义为单位时间内信道上所能传输的最大信息量。由信息论知，对高斯白噪声信道，其信道容量为

$$C = W \log_2 \left(1 + \frac{P_s}{W N_0} \right) \quad (\text{位/秒}) \quad (1.11)$$

式中 W 是信道可提供的带宽； $P_s = E_s/T$ 是信号功率， E_s 为信号能量， T 是分组码信号的持续时间即信号宽度，因此 P_s/W 是单位频带的信号功率； N_0 是单位频带的噪声功率，故 $P_s/W N_0$ 是信噪比。

从上式易知：增加系统的带宽或信噪比，均可增加信道容量 C ，且三者之间可以转换。例如 C 保持一定，增加信道带宽 W ，则可降低信噪比的要求，即信号功率 P_s 可以减小；反之亦然。

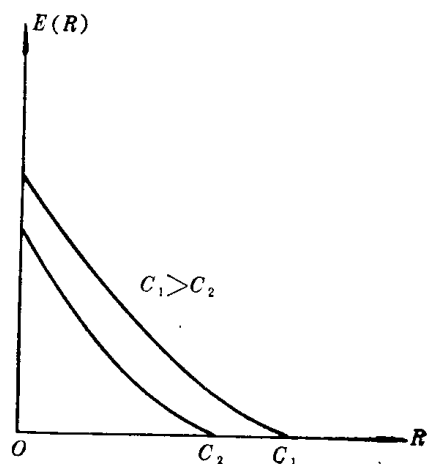


图 1.6 $E(R)$ 与 R 的关系

对于二元对称信道

$$E(R) = -R + \ln 2 - \ln(1 + 2\sqrt{p(1-p)}) \quad (1.13)$$

如果是线性分组码，则

$$P_e = \sum_{k=2}^N e^{-W_k \ln 2 \sqrt{p(1-p)}} \quad (1.14)$$

式中， N 是码字集合的码字总数； W_k 是非零码字的重量。

对于一个系统，为满足一定误码率 P_e 的要求，可采用两种方法。方法之一是增加信道容量 C ，从而使 $E(R)$ 增加。由式(1.11)知，加大信道带宽或增加信噪比可增大 C ，即从根本上改善信道的特性，以增强传输的可靠性。方法之二是在 R 一定时，增加分组信

如果信道的传信率 R 超过了信道容量 C ，则信息传送将很不可靠，这就有着名的 Shannon 信道编码定理。

对一个给定的有扰离散信道，只要发方以任何小于信道容量 C 的速率 R 发送信息，则必存在速率为 R 、码长为 n 的分组码。若采用最大似然译码，可使译码错误概率 P_e 随码长 n 的增加而按指数规律降至任意小。即

$$P_e \leq e^{-nE(R)} \quad (1.12)$$

式中 $E(R)$ 是误差函数或随机编码指数，它与 R 和 C 的关系如图 1.6 所示。图中 C_1 和 C_2 均为信道容量，且 $C_1 > C_2$ 。 $E(R)$ 随着 R 接近于 C 而单调下降，当 $R = C$ 时， $E(R) \rightarrow 0$ 。

号的持续时间 T ，对于分组码即增加分组码长度 n 。但是，随着 n 的增加，将增加码的冗余度及编译码设备的复杂性。研究纠错编码的意义就在于：在一定的传信率下，尽量降低误码率，以实现可靠通信；或在给定误码率下，尽量提高传信率，以实现有效通信；力求编译码器结构简单且易于实现。

Shannon的信道编码定理表明：通信系统中有效性和可靠性是一对主要矛盾，为了提高可靠性要牺牲有效性。它指明了为提高可靠性进行纠错编码的方向，但并未提供怎样构造纠错编码的方法。

1.5 常用检错码

本节介绍的检错码，虽不一定纳入纠错编码理论讨论，但由于结构简单，实现容易，抗干扰能力较强，故得到广泛的应用。

1.3节所述 $(n, n-1)$ 奇偶码是计算机内部及其输入输出设备中最常用的检错码。在信道干扰不严重和码长 n 不大的情况下，应用它是非常有效的。而 $(n, 1)$ 重复码，则不但可检错，而且可能纠错。除此而外，还有如下常用的检错编码。

1.5.1 水平一致监督码

该码先按适当长度对数据序列分组，并按照列的顺序排列构成 m 列 k 行方阵。然后对每行码元进行奇偶校验，得到 k 个校验元形成新的一列附于其它各列之后。最后按列的顺序传送，得到一个 $((m+1)k, mk)$ 分组码。

表 1.1 水平一致监督码

信 息 元										校 验 元
1	2	3	4	5	6	7	8	9	10	11
1	1	1	0	0	1	1	0	0	0	1
1	0	1	0	1	1	0	0	1	1	0
0	0	1	0	0	1	1	0	1	1	1
0	0	0	0	1	0	0	1	0	0	0
1	0	1	1	0	1	1	1	1	0	1

(55, 50)码的一个码字

如表1.1所示， $m=10$ ， $k=5$ ，这是(55, 50)水平奇偶监督码的一个码字。该码字传送顺序是：11001, 10000, 11101, ..., 01101, 01100, 10101。接收时仍按此方阵排列，译码时检查各行的奇偶校验关系是否满足，从而判断是否有错。该码可检测所有长度 $\leq k$ 的突发错及其它错误模式。

1.5.2 水平垂直一致监督码 (方阵码)

在水平一致监督基础上，再垂直对列的信息元进行一次奇偶校验。因此，该码码长为 $n = mk + k + m$ ，校验元长 $k + m$ ，故构成 $(mk + k + m, mk)$ 分组码。传送时既可按列的次序也可按行的次序进行，接收时仍按此方阵排列译码。

表 1.2 水平垂直一致监督码

		信 息 元 列										校验元列
		1	2	3	4	5	6	7	8	9	10	11
信息元行	1	<u>1</u>	1	<u>1</u>	0	0	1	1	0	0	0	1
	2	1	0	1	0	1	1	0	0	1	1	0
	3	0	0	1	0	0	1	1	0	1	1	1
	4	<u>0</u>	0	<u>0</u>	0	1	0	0	1	0	0	0
	5	1	0	1	1	0	1	1	1	1	0	1
校验元行	6	1	1	0	1	0	0	1	0	1	0	

表1.2是该码的一个例子，它是 (65,50) 分组码的一个码字。这类码可检测长度 $\leq k+1$ 或 $\leq m+1$ 的突发错，视依列或行的传输次序而定；根据某行某列的校验关系，可判断该行该列交叉处码元有错，从而可纠正一位错。但有一种偶数个错无法检测。如某两行都在同一列位置出错，则因行和列的奇偶校验关系都可满足，因而无法检测。尽管如此，这种码的检错能力之强不容怀疑，在ARQ系统中应用较多。

1.5.3 横向斜向一致监督码

水平垂直一致监督码是一种横向纵向奇偶校验码。与此类似，还有一种横向斜向一致监督码，它们均是二维奇偶校验码。

如表1.3所示，除对横向的信息元设置一列校验元外，还对斜向组合的信息元也设置校验元。这样，可得到两列校验元附于信息元之后，得到一个(40,30) 分组码。对于一个 m 例 k 行的信息组，可按规则构成 $(mk+2k, mk)$ 分组码。与方阵码类似，它也可纠正一位错误，但当出现双向成偶错误时亦会发生检测不出错误的漏检现象。

表 1.3 横向斜向一致监督码

信 息 元							校验元	
1	0	1	0	1	0		1	0
0	1	1	0	1	1		0	1
0	0	0	1	1	1		1	0
1	1	0	0	1	0		1	1
1	0	1	1	0	0		1	0

1.5.4 定比码

这类码中，所有码字中码元取值为“1”和“0”的位数保持相同比例，即码字中“1”的个数相同，故称为定比码、等重码、定权码及 m 中取 n 码。它是一种非线性码。

若码长为 m ，码字中“1”的个数为 n ，则许用码字的个数为 $\binom{m}{n}$ ，禁用码字个数为 $2^m - \binom{m}{n}$ 。例如，我国电传通信采用的3比2码，即5中取3码，共有许用码字

$\binom{5}{3} = 5! / 3!(5-3)! = 10$ 个，正好用来表示 10 个阿拉伯数字。再用 4 个数字组成一个汉字，从而实现汉字信息传输。表 1.4 给出了电传打字机所用 5 中取 3 码的几种方案。

表 1.4 电传通信用 5 中取 3 码

	方案一	方案二	方案三	方案四
0	0 1 1 0 1	0 1 1 0 1	0 1 1 0 1	0 1 1 0 1
1	0 1 0 1 1	1 1 0 1 0	0 0 1 1 1	1 0 1 1 0
2	1 1 0 0 1	1 1 0 0 1	1 1 0 0 1	1 1 0 0 1
3	1 0 1 1 0	1 0 1 1 0	1 0 1 1 0	1 1 0 1 0
4	1 1 0 1 0	0 1 0 1 1	1 1 0 1 0	0 1 0 1 1
5	0 0 1 1 1	1 0 0 1 1	1 0 0 1 1	0 0 1 1 1
6	1 0 1 0 1	1 0 1 0 1	1 0 1 0 1	1 0 1 0 1
7	1 1 1 0 0	1 1 1 0 0	1 1 1 0 0	1 1 1 0 0
8	0 1 1 1 0	0 1 1 1 0	0 1 1 1 0	0 1 1 1 0
9	1 0 0 1 1	0 0 1 1 1	0 1 0 1 1	1 0 0 1 1

又如国际电报用的 ARQ 通信系统，采用 7 中取 3 码，共有许用码字 $\binom{7}{3} = 7! / 3!(7-3)! = 35$ 个，正好用来代表电传机中的 32 个数字与符号。实践证明，它能使国际电报的误码率保持在 10^{-6} 以下。

定比码可检测所有非对称性错即所谓单向错，即 0 错成 1 和 1 错成 0 的数目不相等的错误。而 0 错成 1 和 1 错成 0 数目相等的对称性错误无法检测，而这种对称性错误的概率是极小的。

1.5.5 群计数码

对传送的信息组计算重量即 1 的个数，并用二进制数字表示，然后根据需要取其部分或全部作为校验元附加在该信息组之后，从而组成一个码字，如表 1.5 所示。和定比码一样，它也是一种非线性码。

表 1.5 群计数码

码字	信 息 元							校 验 元			重 量
C_1	1	0	0	0	1	1	0	0	1	1	3
C_2	0	1	0	0	0	1	0	0	1	0	2
C_3	1	1	0	0	1	1	1	1	0	1	5
C_4	0	0	1	1	0	1	0	0	1	1	3
C_5	1	0	1	0	1	1	0	1	0	0	4

接收时先计算接收字信息组的重量，并与接收字的校验元比较，若符合，则传送正确，否则传送出错。这种码也可检测对称性错误以外的大量错误，适用于磁带记录系统。

如将群计数码与水平一致监督码结合起来形成所谓水平群计数码，则能检测较长的突发错误。如表 1.6 所示五个码字，每个码字有八位信息元，另设两位校验元，按模 4 计算信息组中 1 的个数。传送时按列的顺序发送，即先是 11101，接着是 11001，…，最后是 11001。