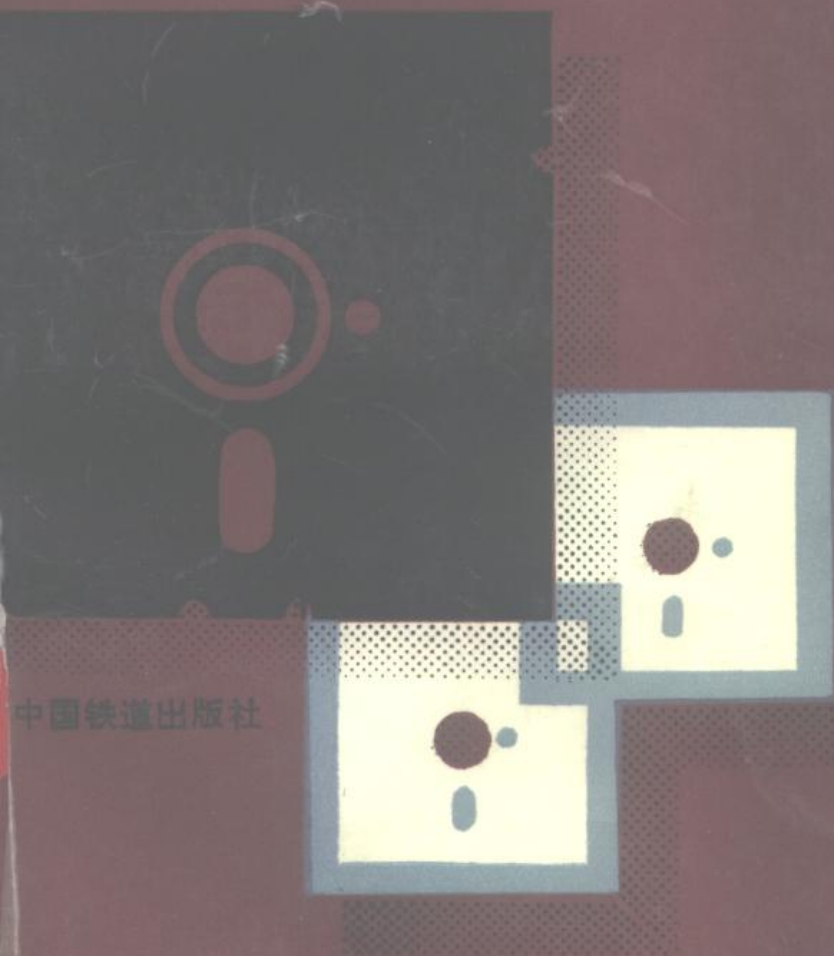


现代通信中的 编码技术

李振玉 卢玉民 编著



中国铁道出版社

(京)新登字 063 号

内 容 简 介

本书共分七章,内容包括:现代通信系统及编码技术、数字通信中的信源编码、选址通信中的地址编码、数字通信中的纠错编码、密码通信中的密钥编码、计算机通信中的混合编码、加密与纠错相结合系统在数字通信中的应用。

本书可作为从事通信工程、计算机工程工作人员的参考书,也可作为高校通信专业及计算机工程专业高年级学生、研究生教材,以及教师的教学参考资料。

现代通信中的编码技术

李振玉 卢玉民 编著

中国铁道出版社出版发行

(北京市东单三条 14 号)

责任编辑 黄成士 封面设计 赵敬宇

各地新华书店经售

中国铁道出版社印刷厂印

开本:787×1092 毫米 1/32 印张:13.25 字数:292 千

1996 年 5 月 第 1 版 第 1 次印刷

印数:1—3000 册

ISBN7-113-02247-2/TP·228 定价:16.70 元

前 言

随着改革开放不断地深化,社会主义现代化建设的飞速发展,要求现代通信要先行,而无线移动通信又是通信发展中的热点。也由此而带来了通信中的抗干扰、安全性和可靠性,以及密码、纠错技术等问题。传统的通信方式已远远不能满足现代通信的要求。近几年来发展起来的蜂窝式重复利用频率和共用频率的集群通信方式,也都不能满足通信迅速发展的需要。尤其是对通信安全性、可靠性的要求。国内、外新发展起来的纠错、编码技术,应用在数字通信、选址通信、密码通信,不但能缓解通信的紧张问题,而且也解决了通信中的抗干扰、加密纠错传输的技术问题,先进的加密、纠错技术也符合无线数字通信的发展方向。

作者从事现代通信、通信中的编码与纠错技术的教学、科研已有 20 余年,曾发表了几十篇论文,以及类似的有关著作;由于作者教学和科研的需要,不断跟踪了学术领域中的先进科学技术,收集和翻译了大量地有关科技新资料,尤其是近五年来现代通信和加密、纠错技术的情报。经过对上述教学、科研及对收集的情报的分析研究,而编写了这本科技书,提供给广大无线通信专业和计算机通信专业的学生、工程技术人员和科技工作者参考,为现代通信的发展贡献微薄之力。

本书共分七章,第一章到第四章由李振玉编写;第五到第七章由卢玉民编写,全书由李振玉统编。在本书的编写过程中,得到了许多同志的支持,林少军、岳路凯、康群、董志刚、李岷提供了部分资料,在此表示感谢。

目 录

第一章 现代通信系统及编码技术	1
第一节 现代通信系统	1
一、现代通信系统的现状与发展	1
二、现代通信系统的组成	3
三、现代通信系统的性能指标	5
四、现代通信系统的类型	8
第二节 现代通信系统中的编码技术	27
一、引言	27
二、线性码(PN 序列)	29
三、非线性码	46
第二章 数字通信中的信源编码	57
第一节 信源编码	57
一、信源编码的概念	57
二、最佳的二进制编码	66
第二节 文件传真编码	68
一、分辨率和压缩比	69
二、极限压缩比	71
三、空白编码	73
四、长度编码	76
第三节 话音编码	82
一、话音编码的特点	82
二、话音预测编码	83
三、话音的树图编码	87

第四节 脉冲数字调制编码	90
一、脉冲编码调制(PCM)	90
二、增量调制(ΔM)	109
三、改进的增量调制	114
四、PCM 和 ΔM 的比较	120
第五节 图象编码	122
一、图象编码概述	122
二、预测变换原理	124
三、图象编码方法	125
第三章 选址通信中的编码	140
第一节 选址通信的理论基础	140
一、信号设计	140
二、信号正交分割原理	142
三、信号分割的严格条件	144
第二节 选址通信中的地址编码	147
一、码分选址通信	147
二、码分通信中的地址编码	153
三、跳频通信中的地址编码	167
第三节 集群通信系统中的信令编码	176
一、集群通信的概念	176
二、集群通信系统控制方式	183
三、系统控制信令编码	184
四、MPT—1327 信令码	185
五、随路信令—LTR 信令码	189
六、美国的 QTR 信令码	194
七、美国 Motorola 智慧网集群系统信令	196
第四节 无线寻呼系统编码	198
一、POCSAG 编码	198

二、汉字信息编码	210
三、无线寻呼系统标准	218
第四章 数字通信中的纠错编码	226
第一节 数字通信中的纠错技术	226
一、差错控制方式	226
二、信道编码定理	232
三、数字通信中的抗干扰码	236
四、纠错码分类	241
第二节 数字通信中的纠错码	243
一、线性分组码	243
二、循环码	253
三、BCH 码	257
第三节 数字通信中的随机错误和突发错误码	265
一、乘积码	266
二、交错码	270
三、戈莱码	272
四、RS 码	276
第五章 密码通信中的编码	280
第一节 密码通信中的加密系统	280
一、引言	280
二、密码通信的加密系统	281
第二节 密码通信中的加密方式	283
一、话音加密方式	283
二、伪随机编码加密方式	288
第三节 密码通信中的加密方法	295
一、引言	295
二、加密过程	295
三、加密的主要方法	301

四、关于二进制信息的加密方法	304
五、对加密处理要求	310
第四节 现代密码体制	314
一、DES 体制	314
二、RSA 体制	328
三、陷门背包体制	332
第六章 计算机通信中的混合编码	338
第一节 加密、纠错相结合的基本理论	338
一、引言	338
二、密码体制	339
三、纠、检错码	347
四、加密、纠错相结合系统	352
第二节 神经网络译码原理	357
一、神经网络基本原理	357
二、竞争学习算法	359
三、线性分组码的神经网络译码	361
第三节 加密、纠错相结合系统的设计与实现	364
一、加密、纠错相结合系统的设计	364
二、用软件方法实现加密、纠错相结合系统	373
三、用硬件方法实现加密、纠错相结合系统	381
第四节 加密、纠错相结合系统性能分析	389
一、安全性分析	389
二、可靠性分析	392
三、讨论	394
第七章 加密纠错相结合系统在数字通信中的应用	396
第一节 在远程通信中的应用	396

一、应用目的、意义	396
二、加密算法	397
三、总体结构及系统框图	398
四、应用环境	399
五、通信过程	399
六、结果分析	400
第二节 在计算机网络通信中的应用	401
一、计算机网络概述	402
二、计算机网络通信中数据的 安全性和可靠性	403
三、应用于计算机网络通信中 有关问题的研究	409
参考文献	414

第一章

现代通信系统及编码技术

第一节 现代通信系统

一、现代通信系统的现状与发展

所谓通信,主要是指消息的传递和交换,即互通信息。在近代通信中,要传送的信息有文字、语音、图像、数据及符号等各种类型。

最早的通信方式是比较简单的,通信内容都很单一,并且受环境距离等条件的限制,不可能在比较辽阔的领域内进行广泛的通信。

真正的通信技术是从 19 世纪 30 年代发明电报后才开始的。它是利用导线中有无电流来区分传号和空号,然后再根据传号和空号的长短来组成点和划,并且编码成不同的电报符号。实际上,它就是利用电流(或电磁波)来传递消息,这就给通信技术的发展奠定了良好的基础。

19 世纪 70 年代在发明电报之后不久,人们又利用电磁感应的原理发明了电话机。电报和电话是组成通信的基本内容,一直到现在还大量应用。到 19 世纪末期,人们在长期实践中利用电磁波辐射原理发明了无线电报。这就精简了大量通信线路,节省投资和建设时间,并为无线通信开辟了道路。

20 世纪初开始发明电子管,它又为无线电话提供了实现的基础。当时主要是利用长波、中波和短波,并采用调幅制,因

此通信质量不高。

本世纪 20 年代开始,随着科学技术的发展,相继出现广播、传真等技术,因此通信的内容就扩大了。不仅文字、语言可以作为传递消息的对象,而且包括音乐、图片、报纸在内的消息也属于通信的范畴。

本世纪 30 年代还相继发明了电视和调频技术,后者利用超短波或微波可以传递各种信号。这就进一步扩大了通信的内容。另外,值得一提的是在 30 年代中期出现了脉冲编码技术,它为数字通信开辟了新的广泛的领域。因此,几乎所有的通信内容都可以在数字通信系统内实现。

本世纪 40 年代出现的晶体管和电子计算机也是对通信技术的发展起到决定性的作用。由于电子计算机的功能不断发展,无论是用于计算或者用于数据处理和实时控制,它都要求有许多终端来配套。这样一来,通信的内容已经突破了人与人之间通信的概念,而且扩展到人与机器和机器与机器之间的通信,并将逐步成为近代通信的主要内容。

本世纪 60 年代出现的光通信和卫星通信,它们都为大量的、综合性的通信系统提供了广阔的信道。尤其是卫星通信在解决国际通信中的通信质量方面作出了突出的贡献。它不仅使得设备小型化,而且寿命长、可靠性高,适合于在空间通信中应用。

通信学科的发展,除了由于新的电子器件问世以及技术水平的提高外,还不能忽视在通信理论方面的突出成果。在信息论的基础上又逐步地形成最佳接收理论、编码理论、信号和噪声理论等,都曾给提高通信质量和创造新的通信体制作出重大贡献。

根据通信发展史可以看到,通信这门学科是逐渐由低级到高级,内容由简单到复杂发展成长起来的。

二、现代通信系统的组成

通信的目的就是为了交换消息(单向或双向),因此一个通信系统最概括的组成可用图 1.1 来表示。

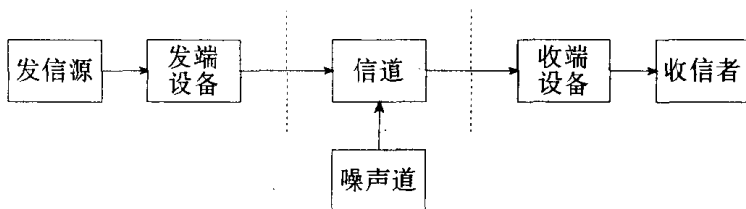


图1.1 通信系统的组成

这里发信源是指消息的产生来源,并且将消息变换成电信号。例如,它包括电话机、电报机、话筒、摄像机等。由于数据通信的开展,各种数字终端以及计算机本身也都可看作是发信源。通常将它们当作确知信号来处理。

发端设备所要完成的功能也很多,例如调制、放大、滤波、发射等,在数字通信系统内还包括编码。由发信源发出的信号通常称为基带信号,它的特点是频谱由零频附近开始。基带信号直接在信道内传输,称为基带传输系统。

实际上,大量的通信系统是建立在各种调制的基础上的,例如调幅、调频或脉冲调制等。调制的根本任务是将基带信号变换为更适合于在不同信道内传输的信号,并且有可能实现信道多路复用或者提高抗干扰能力。

信道的种类也很多,但概括起来只有两种,即有线信道和无线信道。前者例如架空明线、对称电缆、同轴电缆等;它们都是作为通信系统中的传输媒介,传输性能的好坏直接影响到通信质量,信道中产生噪声的来源很多,而且也很分散。例如,在各种电子器件内有噪声,导线内也会产生噪声,此外还包括

来自宇宙空间的各种噪声。在图 1.2 内把它们都集中在一起，并且加在信道上，这是表示在信号传输过程中随时随地有可能叠加噪声的影响。实际上，信道中除了有噪声以外，还有各种干扰。例如，工业干扰、电台干扰、雷电磁暴等干扰。

至于接收端设备和受信者则是完成与发送端设备和发信源相反的任务，当然，这里所谓的受信者也不一定是人，可以是其它各种终端设备。

图 1.1 是各种通信系统的概括说明。如果结合模拟通信系统的要求，则可将图 1.1 化为最简化的模拟通信系统。而现代通信已向数字通信发展，数字通信系统的模型如图 1.2。

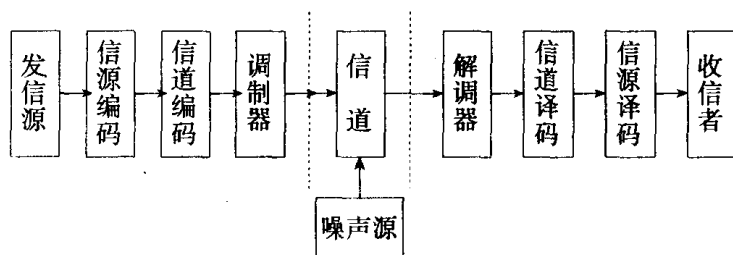


图1.2 数字通信系统的模型

所谓数字通信是指在该通信系统内所传输的是二进(元)或多进(元)制数字信号。这里的特点是在实现调制之前先要经过二次编码，即信源编码和信道编码。相应地在接收端于解调后要有二次译码。

所谓信源编码是指将原来不适于在数字通信系统内传输的信号，变换为比较理想和有效的数字信号。例如，将原来属于模拟信号的话音数字化就是信源编码器的任务；又如发信源是并行输出的计算机，则需要通过并串变换形成串行数据后才能进行数字通信，这也是信源编码器的任务。此外，如数据扰乱，数话加密，编码电视比特压缩等也都是在信源编码器

内完成的。简单地说,信源编码器就是实现信号处理的功能,使得处理后的信号更适宜于在数字通信系统内传输。

所谓信道编码是指在原来的数字信号序列中引进某些作为误差控制用的数码,以实现自动检错和纠错的目的。因此,通过信道编码器后的数码序列要加长,即提高数字信号传输可靠性是用降低传输速率的办法来换取的。

图 1.2 内的信源编码和信道编码并不是每个数字通信系统都必须的。不过应强调两点,即图 1.2 采用的是数字调制和解调,它们与模拟调制和解调有所区别;另外一点是在数字通信系统中同步系统是不可缺少的,在图 1.2 中虽然没有画出,但绝对不能忽略。因此,数字通信系统的组成要比模拟通信系统更复杂,这是在比较两种通信制式时应该考虑到的。

至于接收端和收信者则是完成与发送端和发信源相反的任务,这里不再重述。

三、现代通信系统的性能指标

通信系统组成后必然要提到通信质量问题,如何来衡量通信系统的质量?

这里所谓通信质量是指整个通信系统的性能,不是指某个局部。另外,对通信系统的质量要求也很多,包括电气性能、工艺结构、操作维修等,但我们主要讨论通信系统的电气性能。

从信号传输的角度分析,通信系统的质量最主要的是有效性和可靠性。所谓传输信号的有效性就是指在给定的信道内能够传输更多的信息内容;而所谓传输信号的可靠性是指在给定的信道内接收到信息的准确程度。在实际的通信系统内这两个要求经常是有矛盾的,亦即传输信号的有效性提高会使传输信号的可靠性下降,反之亦然。例如,上面提到的信

道编码器是在原来的数字信号序列中引进一些监督码元,以实现自动检错和纠错,因此它可以使传输信号的可靠性提高。但是,由于监督码元的加入使信号长度增加,因此信号传输的速率就要降低,亦即传输信号的有效性要下降。在处理这对矛盾时我们经常是用牺牲一方来换取另一方的办法来解决,因此必须根据具体情况而定。

1. 模拟通信系统的质量要求

(1)在模拟通信系统中,信号传输的有效性通常可用有效传输频带来衡量。当给定信道的容许传输带宽后,它被每路信号的有效传输带宽来除,就可确定信道容许同时传输的最大通路数目,这就称为多路频率复用。显然,信道复用的程度越高,则信号传输的有效性就越好。信号的有效传输带宽还与调制方式有关,例如调频波的频带就要比调幅波宽得多。因此在同样的传输线路上传输调频波的有效性就不如调幅波。

(2)模拟通信系统的传输可靠性通常可用整个通信系统的输出信噪比来衡量。由于信道内存在噪声,因此接收到的波形实际上是信号和噪声的混合物,它们经过解调后同时在通信系统的输出端出现。因此,噪声对模拟信号的影响可用信号功率与噪声功率之比(在同一点上)来衡量,这就是输出信噪比。显然,信噪比越高,通信质量就越好,信息内容的准确性也就越高。输出信噪比一方面与信道内噪声大小和信号功率有关,同时又和调制方式有很大关系。不同的调制方式采用不同的解调器,而后者对处理噪声的能力是大不相同的。例如,在调频系统内采用鉴频器就具有抑制噪声的能力,因此输出信噪比可以提高;而在调幅系统内采用包络检波器来解调就没有提高输出信噪比的能力,因此调频通信系统的传输可靠性往往比调幅系统好。但是,调频系统的传输有效性不如调幅系统,这里又出现了传输可靠性与有效性之间的矛盾。

2. 数字通信的质量要求

(1) 数字通信系统有效性。由于数字通信系统内都是传输离散的数字信号,因此传输有效性可用信号(或符号)传输速率来衡量。如果数字信号采用的是二进制信号,则信号传输速率(简称传信率)可用比特/秒(bit/s)作单位。比特是一种计算信息量的单位,在这里可理解为二进制脉冲的数量。例如,传信率是 4800bit/s 可理解为每秒内传送 4800 个二进制脉冲数。显然,传信率越高,信号传输的有效性就越好。如果采用的是多进制数字信号,这时信号传输速率可用波特(Baud)作单位。这里每个波特就是指传输一个多进制数字信号。例如,传信率是 75Bd 可理解为每秒内传送 75 个多进制数字信号。显然,波特和比特是可以相互转换的。

(2) 数字通信系统内的传输可靠性可用误码率来衡量,它代表接收到的数字信号出现错误的程度。如果数字信号是采用二进制,则误码率可用 P_b 表示

$$P_b = \frac{\text{错误比特数}}{\text{传输总比特数}} \quad (1.1)$$

相应地,在多进制数字通信系统内误码率就可用 P_c 表示

$$P_c = \frac{\text{错误码元数}}{\text{传输总码元数}} \quad (1.2)$$

这里码元就代表多进制数字信号。

在 P_b 和 P_c 之间也有相互转换关系,但它与译码方法、选用码型等都有关系,因此比较复杂。在一般情况下总是 $P_b < P_c$,只有在二进制数字通信系统内 $P_b = P_c$ 。

在数字通信系统内误码率越低就说明数字信号传输的可靠性越高,因此通信质量越好。在有线信道内通常要求误码率小于 10^{-6} ,亦即在传输 10^6 个数字信号中只容许出现一个错误信号,显然这样的要求是很高的。在无线短波信道内,由于

存在着衰落和多径效应等特点,信道特性对于数字信号的传输非常不利,通常要求误码率在 10^{-3} 以下。

四、现代通信系统的类型

1. 数字通信

(1) 数字通信的概念

“通信”简单的说就是信息的交换和传递,它在人们的工作和生活中占有十分重要的地位。现代化的通信都是指用电子技术完成通信任务,简称“电信”。电信技术发展到了电话通信、电报通信、图象通信(如传真和电视等)。在传输的信号波形上又可分为模拟通信和数字通信。

什么是数字通信呢?就是把需要传送的原始信号变成一系列数字脉冲来传输的通信方式,称为数字通信。它包括数字电话、数字电报、数字传真、数字电视等等。

随着科学技术的发展,近年来又出现了一种新的数字通信方式——数据通信。所谓数据通信,它具有数字通信的一系列特点和优点,不过它传送的信息形式,或者本来就是一些数据数字,或者是由其它信息形式转化而来的数据。现代的通信,根据对象区分有:人与人的通信、人与机的通信、机与机的通信。数据通信的一个主要特点,即通信方式是伴随着电子计算机的发展而出现的,它是一种电子计算机与通信信道相结合的数字通信方式。这里所谈的通信信道,可以是有线、无线、微波或卫星通信线路等。为突出其人与机、机与机通信的特点也有专门称之为数据通信的。此外有的数据通信传送的可能是模拟信号,这种数据通信并不等于一般的数据通信,只是其通信对象是人与机、或机与机,这是数据通信的特例。通常说的数据通信都是指有电子计算机参加的人与机、机与机的通信,而且传输的又是数字信号。

关于人与人的通信象电话、电报、传真、广播、电视等。人与机、机与机的数据通信。例如：舰艇与岸上的无线通信，根据现代的测定技术，只要连续通信 3 秒钟，就会被敌人测出位置而无藏身之地，所以要求潜艇与岸上的通信最好在零点几秒以内完成。再如火箭导弹的飞行速度是很高的，可达每分钟几百公里，从发现情况到报知、直至采取应急和反击措施真是“秒不容缓”。要完成上述的通信与指挥的任务，用人对人的电话或电报通信方式是行不通的。因此必须采用电子计算机控制的高度自动化的“人与机”或“机与机”的通信，可见数据通信也是势在必行。

人与机或机与机的数据通信从发展国民经济中用途也十分广泛。例如：企业管理、火车调度、地质勘探、油田管理、电力网控制、银行结算等等都可应用数据通信。如气象观测站分布在全国各地，要把各地的气象数据及时而准确的汇集起来，进行分析、综合计算以后，才能及时而准确的实施气象预报。如果采用数据通信，让全国各地的气象观测站向计算中心传递数据，经计算中心自动的进行综合、分析、计算以后，就可以及时而准确的向全国发出气象预报。地震的预报也是如此。这些都说明数据通信必将是今后的一种重要的通信方式。

(2) 数字通信系统的组成

图 1.1 示出一个单向数字通信系统的框图，下面讨论各组成部分的作用，如图 1.3 所示。

① 信源

信源可以是模拟的或离散的。模拟信源给出时间连续的信号，离散信源的输出是离散符号的序列。语音信号、雷达输出信号、照片扫描后的数据都是模拟信源信号。电传打印终端的计算机数据文件与报文，则是离散信源符号。

通常，用取样及模数转换器将模拟信号表示为数字符号