

信息论与编码方法

在计算机·通信中的应用

目 录

第一章 绪 论	
第一节 信息与编码	
一、 信息时代与编码技术	
二、 信息系统模型	2
三、 模拟信号的数字化	5
四、 数字信号的类型	7
五、 数字信号的调制	10
第二节 数字编码系统	11
一、 进位制的不同表示	11
二、 数字的二进制表示	15
三、 八进制数与十六进制数	16
四、 二进制编码的十进制数	18
五、 原码、反码和补码	19
六、 负二进制数表示法	23
七、 数的阶乘表达方法	25
八、 余数表示方法	26
九、 格雷码	27
第三节 计算机系统编码的特点	29
一、 信源编码	30
二、 差错控制编码	32
三、 数据加密编码	38
习 题	42
第二章 信息论基础	44
第一节 信息与概率	44

一、信息论发展简史	44
二、信息的概率含义	45
第二节 平均信息量——熵	49
第三节 二维离散概率量的熵	58
第四节 信道干扰特性	63
一、离散无干扰信道	66
二、输入—输出相互独立的信道	67
三、熵间的相互关系	69
第五节 互信息量	71
一、互信息量的定义	71
二、熵与集合图的类比	73
三、信息处理中熵的变化	78
第六节 离散信道的信道容量	80
一、二进对称信道 BSC	81
二、二进删除信道 BEC	82
三、具有对称噪声特性的信道	83
四、一般二进信道的拉格朗日乘数法	85
第七节 连续信道的信道容量	87
一、连续随机变量的熵	87
二、连续信道的信道传输率	91
三、连续信道的信道容量	94
习 题	97
第三章 信源编码	99
第一节 编码的意义	99
第二节 编码定义	101
第三节 非续长码	105
第四节 平均编码长度	107
第五节 最佳编码方法	110
一、仙农-范诺编码方法	110

二、霍夫曼编码方法	113
三、吉尔伯特-穆尔字母码	115
第六节 马尔可夫信源	118
第七节 离散无干扰编码基本定理	124
习 题	126
第四章 差错控制一般原理	129
第一节 计算机系统可靠性	129
第二节 差错的统计特性	131
第三节 级联式二进对称信道	139
第四节 差错控制的主要形式	142
一、前向纠错	142
二、自动回询重传	143
三、混合式 ARQ	145
第五节 网络链路层传输控制	146
第六节 简单差错控制方法	149
一、定比码	149
二、群计数码	151
三、模 P 方法	151
四、正反码	153
第七节 差错控制码分类	155
第八节 有干扰时离散编码基本定理	156
习 题	160
第五章 线性码及其应用	162
第一节 码距和码重	162
第二节 检错能力与纠错能力	165
第三节 奇偶监督码	168
第四节 二维奇偶监督码	171
第五节 监督矩阵与生成矩阵	174
第六节 伴随式与标准阵列	182

第七节 汉明码	186
第八节 计算机存储器的差错控制	188
一、IBM 系列计算机内存差错控制	191
二、AM2960 级联式检错纠错集成电路芯片	193
第九节 卷积码的基本概念	196
一、编码电路	197
二、监督矩阵	200
三、第一截分组码	201
四、生成矩阵	202
五、译码方法	204
习 题	209
第六章 循环码与 BCH 码	211
第一节 基本定义	211
第二节 有限域中的运算规则	213
第三节 循环码多项式的基本特性	218
第四节 循环码的编码方法	220
第五节 循环码的编码电路	223
一、多项式除法电路	223
二、自动乘 x^r 的除法电路	224
三、编码电路	225
第六节 循环码的译码电路	227
一、自发运算电路	227
二、纠正一位错误的 $(7,4)$ 码译码电路	229
第七节 BCH 码	230
一、最小多项式	231
二、码的主要特性	232
三、戈雷码	235
四、BCH 码的译码方法	236
五、里德-索洛蒙码	239
第八节 在计算机网络中的应用	240

第九节 法尔码及在磁盘纠错中的应用	247
习 题	251
第七章 组合编码方法	253
第一节 组合编码的特点	253
第二节 基本组合设计方法	255
一、组合运算公式	255
二、组合求序公式	256
三、生成函数	260
四、平方剩余	261
五、射影几何	262
六、哈达玛矩阵	263
第三节 $S(U, V)$ 阵列与关联矩阵	265
第四节 SBIBD 组合码	271
一、差集码	271
二、 $(22, 11, 7)$ 码	274
三、广义正交码	276
第五节 DBBD 组合码	280
第六节 在内存纠错中的应用	284
习 题	286
第八章 复数旋转码及其应用	288
第一节 基本概念	288
一、码的定义与结构	288
二、复转编码方法	291
三、旋转运算矩阵	292
第二节 复数旋转码的组合特性	297
第三节 译码原则	300
第四节 超限译码与自适应差错控制	304
一、复数旋转码的超限译码能力	304
二、自适应差错控制	306

第五节 增加码率与实现不等保护	307
一、增加编码效率	307
二、实现不等保护	310
第六节 复数旋转码的主要特性	312
第七节 微机自动纠错机	314
习 题	318
第九章 算术运算校验码	320
第一节 算术运算与差错控制	320
一、组合逻辑电路检错	320
二、时序电路检错	321
三、运算器检错	322
第二节 奇偶校验方式	323
第三节 余码的基本概念	325
一、同余运算规则	326
二、余码的定义和性质	327
三、余码的校验能力	328
四、余码编码方式	331
第四节 算术重量与距离	334
第五节 AN 码	337
习 题	342
第十章 数据加密编码方法	344
第一节 计算机系统数据的安全	344
第二节 传统密码编制方法	347
一、移位法加密	348
二、代替法加密	349
三、代数法加密	350
第三节 伪随机序列的产生	352
第四节 标准数据加密算法	354
一、加密过程	354

二、 初始置换 IP 和逆初始置换 IP^{-1}	356
三、 子密钥的产生	357
四、 加密函数	359
第五节 中国剩余定理	363
第六节 公开密钥密码体制	367
一、 公开密钥密码体制的基本特征	367
二、 RSA 公开密钥密码体制	369
三、 背包公开密钥密码体制	373
第七节 数字签名	377
第八节 通信密钥分散管理	378
一、 多项式的中国剩余定理方案	378
二、 全组合分散保管方案	381
第九节 复数旋转码在数据加密中的应用	383
一、 单向加密函数与模二方程求解	384
二、 行列互换性与密标的设置	386
三、 密钥分散管理功能的实现	389
习 题	391
附录一 ASCII 字符码与部标字符码	392
附录二 五单位数字保护电码	394
附录三 复数旋转码的编码译码程序	395
参考文献	399

第一章 绪 论

第一节 信息与编码

一、 信息时代与编码技术

当前,一个以 3C(即**计算技术 Computation**、**通信技术 Communication** 和**自动控制 Control** 三个英文名词的第一个字母)为特征的世界范围内的信息革命正在到来,信息与能源、材料并驾齐驱,成为新的经济技术革命的三大支柱。建立在微电子技术基础上的数字式集成电路的诞生和成熟,引起信息传输领域中的现代数字通信技术和信息处理领域中的数字电子计算机技术迅猛发展。它们互相结合和渗透,形成了远程的和局部的计算机网络,并正在进一步向多功能的**综合业务数字网络**(Integrated Services Digital Networks,简称 ISDN)过渡,从而使人类进入一个崭新的信息时代。

自从信息论的奠基人仙农(Claude E. Shannon)1948 年首次发表有名的论文《通信的数学原理》后,信息理论的发展和编码理论的发展始终是相互依赖、相互促进的。著名编码学者汉明(R. W. Hamming)曾经说过:“从逻辑上来说,编码理论导致信息理论,信息理论则为适当的信息编码提供了所能达到的限度”。

信息的价值来源于它的共享性和可交换性。由于数字式集成电路技术发展,一切生产和生活中的机器和设备都在朝着数字化方向过渡。如同我们在后面将要看到的那样,数字化的信息就是编码的信息。人与机器、机器与机器之间,都要依

靠编码这个环节来进行信息交换(图1—1)。实际上,在信息技术的各个环节,即信息的提取、采集、发送、传递、接收、检测、量度、变换、存储、显示和处理中,都存在不同形式和不同用途的编码方法。

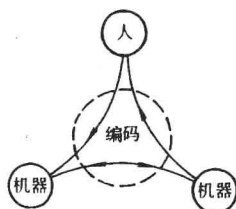


图 1—1 编码在信息

交换中的作用

二、 信息系统模型

随着科学技术的发展,人们传递

消息的方式也在不断进步。从人和人之间面对面的谈话,到经过电话信道由一个城市到另一个城市的通话,从架空明线、电缆到光纤通信和卫星通信。尽管所利用的物理原理和设备各不相同,它们都可以归纳为图 1—2 所示的简单模型。即它由信源、信道和信宿(又称收信者)三个基本部分组成。例如在课堂上,教师是信源或发信者,消息以声波的方式经过空气构成的信道,传到收信者即学生们的耳中。当人们通电话时,消息由声音转换成电信号后,在导线通道中传送。此外,信道中还存在着各种干扰。

除了上面所列举的属于空间传输的信息系统外,还有时间传输的信息系统。例如我们在计算机存储系统中

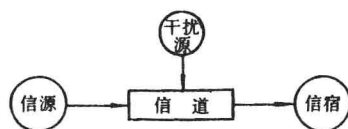


图 1—2 简单信息系统模型

存入信息,过一定的时候又

将它们输出来,这时存储信息的介质就相当于通信的传输线。实际的数字信息传输系统或存储系统模型要比图 1—2 中的简单信息系统模型复杂些。图 1—3 中表示出典型的信息传输(或存储)系统结构框图。其各部分的作用和特点简述如下。

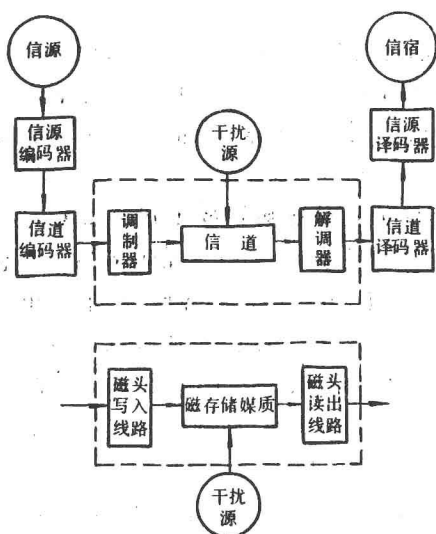


图 1-3 典型的数字信息传输或存储系统框图

减少每个消息、字符所需的平均码元数,从而提高信息传输或存储的有效性。第三章将专门讨论信源编码问题。

对于输出为模拟量的信源来说,在信源编码中要完成模拟量到数字量的变换。对于某些用户来说,信源编码中还包含数据加密的功能。

信道编码器的作用是对信源编码器的输出进行变换,用增加多余度的方法提高对信道干扰的抗击能力。由于实际的信道中都不可避免地存在各种原因所引起的干扰,所以信道编码的原理、方法和应用,一直是编码学科领域中探讨得最为热烈和深入的主题。本书中也将用相当的篇幅对信道编码问题进行分析讨论。

调制器将信道编码器输出的数字序列变换为振幅、频率或相位受到调节控制的波形,以适合在信道中作较长距离的

信源是产生消息的来源,消息可以是离散的,也可以是连续的。它可以是数据、文字,也可以是语言、图象。通常信源的消息是随机发生的,因而需要用随机变量或随机过程来描述。

信源编码器将信源的输出变换为数字信息序列,信源编码的目的通常是降低信源输出中的多余度,

传输。

信道是信号由发送端传输到接收端的媒介。典型的传输信道有明线、电缆、高频无线通道、微波通道和光导纤维通道等。典型的存储媒质有磁芯、磁鼓、磁盘、磁带、半导体存储器 and 光盘存储器等。

干扰源是对传输信道或存储媒质构成干扰的来源的总称。实际信道中干扰(有时又叫噪声)的种类是很多的。天电干扰、电机或电器设备的火花、电子器件的热噪声、来自相邻线路的串音等,是传输信道中常见到的干扰。磁存储介质的固有缺陷、磁层表面磨损、盘面游离磁粉污染、磁头放大器波形不对称、外来电磁场的干扰,以及 α 粒子对半导体存储单元的作用等,则是存储媒质中常见到的干扰来源。

一般说来,干扰可以分为两类。一类是由外界原因所产生的随机干扰,它与在信道中传送的信号统计无关,因而信道的输出是输入和干扰的叠加,称为**加性干扰**。另一类是信号受某些物理条件的变化影响(如无线通信中电离层位置的随机变化等),引起信号参量(如频率色散、相位偏移等)随机变化,此时信道的输出信号可看成是输入信号与一个时变参量相乘的结果,因而称为**乘性干扰**。

解调器将从信道中传送过来的信号波形,还原为调制器以前的数字序列。由于信道中干扰的影响,还原的数字序列往往和原来输入调制器的数字序列有差别,这就是误码现象。

信道译码器的作用和信道编码器相反,它利用信道编码时所提供的多余度,检查或纠正解调器还原的数字序列中的错误,并把有用的信息序列送往信源译码器。

信源译码器的作用和信源编码器相反,它把经过信道译码器核对后的信息序列转换为适合受信者接收的消息形式。例如,对接收模拟量的受信者来说,数字信息要转换为模拟

量。

信宿或收信者,就是消息要送往的目的地,如计算机、终端、存储器、遥控对象和收信设备等。

在数字信息传输系统中,如果仅着眼于编码和译码问题,则如图 1—3 中虚线方框所示的,包括调制器、信道、解调器部分,称为编码信道。

三、模拟信号的数字化

表达各种物理量的电信号有两类:一类称为模拟信号,又称连续信号,其特点是信号电压(电流)的取值是连续的时间函数。如电话机送出的话音信号、摄象管产生的图象信号、以及反映心脏功能的心电图信号等。另一类是数字信号,它们只能有有限个离散的取值,如电报符号和遥控指令等。模拟信号虽然能变换为适当的光信号或声信号,为人的视觉、听觉系统所接受,但却不适合于在数字通信系统中传输,也不适合于在数字式计算机中进行处理和存储。因此,有必要将模拟信号数字化。模拟信号数字化的方法很多,如脉冲编码调制(简称脉冲调制,缩记为 PCM)、增量调制(ΔM)、差分脉码调制

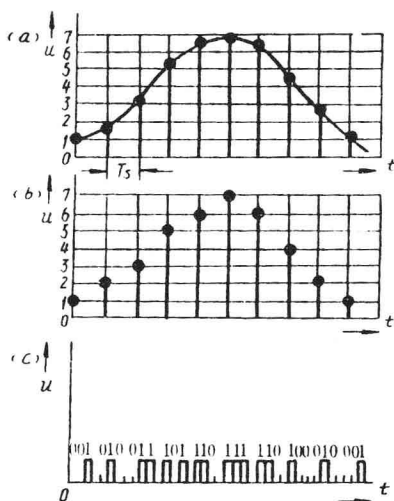


图 1—4 脉码调制的抽样(a)

量化(b) 与编码(c)过程

(DPCM)等。

下面,我们以目前应用很广的脉码调制方式为例,说明模拟信号的数字化编码的基本原理和步骤。图 1—4(a)(b)(c)分别表示抽样、量化和编码三个主要过程。

对于图 1—4(a)中所示的连续信号,在抽样脉冲的作用下,每隔 T_s 秒进行一次抽样,抽样所得到的周期为 T_s 秒的样值脉冲序列,就是原来连续信号在各抽样时刻的瞬时幅值。这样,就把连续信号变成时间离散信号。

可以想到,只有抽取的样值足够密时,才能从离散的样值脉冲序列恢复出原来连续信号而不致丢失信息。根据著名的奈奎斯特(Nyquist)抽样定理:

如果给定的连续信号全部能量包括在零到 W Hz 频带内,则当抽样频率至少为 $2W$ Hz 时,可以由样值脉冲序列无失真地恢复原信号。

当抽样周期

$$T_s = \frac{1}{2W} \quad (1-1)$$

时,抽样出来的样值脉冲序列包含有连续信号 $f(t)$ 的全部信息, T_s 就称为奈奎斯特抽样间隔。

对于话音信号,国际电报电话咨询委员会(简称 CCITT)规定,包括保护频带在内共 4000Hz,因此话音抽样频率定为 8000Hz。

抽样后的离散脉冲序列的幅度取值仍是连续的,称为脉冲幅度调制(PAM)信号。为了方便于进一步编码处理,PAM 信号的幅度取值还要进一步离散化,这就是图 1—4(b)所示的量化过程。具体地说,在信号幅值的取值范围内,按一定的原则分为若干层,称为量化级,每个量化级都用一个量化值来代表。PAM 信号的幅值就用最接近它的量化值来代表。

显然,这种类似于“四舍五入”的归并方式,必然会产生误差。原值与量化值之差称为量化误差。量化过程不同于抽样处理,量化误差将造成信息不可复原的损失。在工作范围一定的情况下,量化级愈多,量化误差就愈小。

经过量化后的 PAM 信号在时间和幅值上都是离散化了的,但幅度上的多种取值仍不便于进行传输、处理或存储。所以,还需要进一步将每个样值所取的量化值编成一组二进制数字,这就是编码。如同我们在后面将要讨论的那样,二进制中只有“0”和“1”两个数字, n 个二进制数字称为 n bit,它可以表示 2^n 个不同的数值。图 1—4(c)中用 $n=3\text{bit}$,就可以表示 $2^3=8$ 种量化值。

根据抽样频率和样值量化级所需的比特数,就可以算出每秒所需传输二进制码的比特数。例如,带宽约 6MHz 的彩色电视信号,抽样频率为 13.3MHz,每个量化样值按 9bit 编码(即有 $2^9=512$ 个量化值),则编成二进制码的传输速率为 119.7Mbit/s。

在有必要从经过抽样、量化和编码的二进制脉冲序列恢复原来的模拟信号时,可根据二进制码字恢复所对应的量化值,即量化了的 PAM 信号。PAM 信号经过低通滤波器去掉高频分量,从而将脉冲平滑成原来的模拟信号。^①

四、 数字信号的类型

表示二进制“0”和“1”的数字信号有不同的形状。图 1—5 中表示出几种不同的数字信号编码形式。

(一)不回零(NRZ)信号

它又可以分为 L 型(图 1—5(a))(1=高电平,0=低电

① 关于 PCM 的更详细的说明,参考文献[5]

平)、M 型(图 1—5(b))(1=间隔开始处有跃变,0=无跃变)和 S 型(图 1—5(c))(1=无跃变,0=间隔开始处有跃变)。不回零信号实现容易,带宽利用好,其中 M 和 S 型是差分码,它们的信号编码是根据相邻信号位的极性比较进行的,因而在有干扰时,察觉一个跃变要比门槛值判别方法容易。它的缺点是有直流成分,无同步能力。

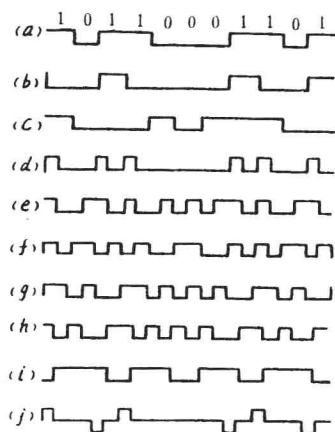


图 1—5 二进制数字信号的
编码形式

(二)回零(RZ)信号(图 1—5(d))

回零信号的 1=间隔的前一半有脉冲,0=无脉冲。由于脉冲宽度比码元时间间隔窄,在每个脉冲之后总要回到零位。这种信号比较简单,易于实现,但存在直流成分,对带宽的要求也高些。

(三)双相信号

它又有 L 型(图 1—5(e))(称为 Manchester 码,1=间隔中点有从高电平向低电平的跃变,0=间隔中点有从低电平向高电平的跃变)、M 型(图 1—5(f))(1=在间隔中点有跃变,0=在间隔中点无跃变。此外,在间隔开始处总是有跃变)、S 型(图 1—5(g))(1=在间隔中点无跃变,0=在间隔中点有跃变。此外,在间隔开始处总是有跃变)和差分曼彻斯特型(图 1—5(h))(1=在间隔开始处无跃变,0=在间隔开始处有跃变。此外,在间隔中点处总是有跃变)。这种双相码在每一比

特的开始或中间有一次跃变,便于接收端同步,因此又称为半时钟码。它无直流成分,跃变特性有利于差错检测,因此常用于网络传输或磁带记录中,例如它用于 629 位/厘米的 IBM 兼容磁带上。

(四)延迟调制信号(图 1—5(i))

又名密勒(Miller)编码方法。它的 1=在间隔中点有跃变,0=如后随“1”,无跃变;如后随“0”,在间隔终点处有跃变。由于每两比特中至少包含一次跃变,因此具有同步能力。它对带宽的要求较双相信号为低。

(五)双极性回零信号(图 1—5(j))

它的 1=间隔的前一半有脉冲,并且交替地变更极性,0=无脉冲。可以看出,在相邻脉冲间恒留有零电位的间隙,无直流成分,且由于连续的“1”具有相异的极性,因而具有一定的检错能力。

除了上述几种一个二进制符号对应一个脉冲的信号外,还有多于一个二进制符号对应一个脉冲的情形,称为多值信号波形或多电平信号波形。图 1—6 表示一个具有 4 个电平的信

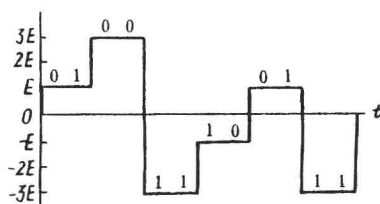


图 1—6 多电平信号波形

号波形。其中 00 对应 $+3E$, 01 对应 $+E$, 10 对应 $-E$, 11 对应 $-3E$ 。由于这种波形的一个脉冲可代表多个二进制符号,故它适宜于在高速率数据传输系统中使用。

这里需要特别指出的是,应当区分开信息传输速率(又称信息速率、传信率)和码元传输速率(又称信号速率、传码率)两个容易混淆的概念。信息传输速率定义为每秒钟传递的信