信息与编码理论

[illegible]

[illegible]

信息与编码理论

—— 用于通信的数学结构

〔美〕R.J.麦克埃里斯著
刘立柱　译
米鹤颐审校

中国人民解放军工程技术学院情报室
1985

译 者 序

人类社会的文明进步，今天将迈进高度发展的信息化时代。对信息合理的存储、处理和利用是现代社会的标志，信息的概念渗透到自然科学和社会科学的各个领域，以至于人们的日常生活当中。因此，信息论和编码理论普遍受到人们的关注，翻译这本书的目的意在适应这种需求。

MCEliece博士写的"信息论与编码"一书是美国"数学及其应用的百科全书"的第三卷，这本书反映了作者1972—1976年在加利福尼亚理工学院的教学经验和创造性的研究成果，在选材和编写上独具匠心，较好地体现了教学法、持久性和关联性；对该领域的几乎所有的基本课题给出了最新颖而又深入浅出的论述。具有普通数学基础知识的读者是可以理解课文的(然而，有些习题的证明和解答也许是困难的)。而具有概率论和线性代数知识的读者会更容易读。因此，该书对想涉入这个领域的初学者和有一定基础的深造者都是适用的，既可作大学生或研究生的教材，同样可供其他科技工作者参考。

在翻译过程中，我院胡东荣副教授、三系张玉琨副主任给予了热情鼓励和支持，周卓韧、赵人杰副教授，长春邮电学院胡士琪副教授给予了热情的鼓励和指导，孙天茂、魏振军老师分别审校过部分初稿，在此表示感谢。由于译者水平有限，译文中不当甚至错误之处在所难免，欢迎读者批评指正。

译者　1984、11于郑州

前　言

信息传输是我们所说的通信的核心。作为一个引人注目的领域，它的重要性使自然科学家全神贯注，从而产生了一个蓬勃发展的技术分支。

我们应感谢仙农的创造性工作，他发现了关于编码、传输和译码信息可通过系统的和制式的方法进行研究；他在1948年发表的著名论文，标志着一个数学新篇章的创立。

在过去三十年来，这个新领域中的文献多得使人震惊，它的一部分术语已变成我们日常用语的一部分。

这本专著(实为两个专题论文的结合)是对通信的两个方面，即编码和传输是一个杰出的导论。

第一（指第二部分课题），它充分显示出代数的威力和优越性；第二，它属于概率论，仙农开创了这个领域，而该书以新颖和想象不到的方法丰富了这个领域。

概率论部分的总编辑　马克·卡克

序　言

本书试图对信息和编码理论的基本成果进行全面的介绍，它写作于1972——1976年期间。当时，我在加利福尼亚理工学院讲授这一课程。我的学生，大约一半是电子工程研究生，其余的都是其他专业（数学，物理，生物，甚至还有一名是英语专业！）的学生，因此该课程既是针对专业人员的，也是面向非专业人员的，这本书也是如此。

本书有三部分：引论，第一部分（信息理论）和第二部分（编码理论）。先阅读引论是必要的，因为它给出了全课程的概貌。在第一部分，第1章是基础，但首先读这一章可能会误解，因为实际上它是熵、互信息以及其它技术成就的汇集。最好把它作为参考性的章节，为了搞懂2——5章，必要时可查阅第1章。第6章是新成果综述，可单独阅读，在第二部分，第7章是基础，读第八章之前必读之；但是第9章几乎与第7章无关，第10章与第7章则完全无关，第11章是第二部分另一个独立的综述。

每一章末尾的习题是很重要的。它包括许多在正文中略去的证明细节和重要结果。建议至少阅读一遍这些习题。

有四个附录，附录A给出了概率论扼要的综述，对第一部分来说是重要的。附录B讨论了凸函数与颜森不等式。在第一部分经常用到它，不熟悉的读者应首先读附录B。附录C摘选了第8章要用的有限域的主要结论。附录D描述了在第9章中用到的有向图中计算路径的算法。

前后参照脚标的顺序是：节、图、例、定理、公式和习

题，它们按章进行连续地双重编号。因此“节2·3”，“定理3·4”，“习题4·17”分别表示第2章的第3节，第3章的定理4，第4章的习题17。附录将参照字母，例如“式B·4”指附录B的第4个公式。

下述特殊符号要说明：$\lfloor x \rfloor$表示$\leqslant x$的最大整数；$\lceil x \rceil$表示$\geqslant x$的最小整数。

最后，我高兴地感谢我的支援者：Gus solomon，第一个引导我搞这个课题；John pierce给了我在加州理工学院授课的机会；Gian—Carlo Rota鼓励我写这本书；Len Baumert，Stan Butman，Gene Rodemich以及Howard Rumsey为本书绞了不少脑汁；Jim Lesh和Jerry Heller为我提供了图6.7和11.2的数据；Bob Hall为我草绘了图；我的打字员Ruth Stratton，Lillian Johnson，特别是Dian Rapchak，和Ruth Flohn为我们抄写了编注。

然而，我最大的支援者是我的妻子Jeannette，她容忍并支持了我这个心不在焉的不尽心的作者——丈夫。谨将本书奉献给她作为一个不恰当的，然而却是真诚的感谢和爱的表达。

罗伯特J·麦克埃里斯

目　录

第二部分 编码理论

引　论

一九四八年，仙农[1]*在他的经典论文“通信的数学理论”的引言中写道：

“通信的基本问题是在一地准确地或近似地恢复在另一地所选用的消息。”

为了解决这个问题，接下去他在这篇论文中创立了一个崭新的应用数学的分支——今天称为**信息理论**和**编码理论**。本书是想在这个理论经历了30年的历史发展之后，对它的主要成果作一介绍。

在这一章里，我们借助于一对特定的数学模型——**二元对称信源**和**二元对称信道**，来阐明信息理论的中心思想。

二元对称信源（简称信源）是一个**客体**，它以每单位时间R个符号的速率发出“0”和“1”符号。我们称这些符号为**bits**，它是**binary digtis**的缩写。由信源发出的这些比特（bits）是随机的，而且发出“0”和“1”的可能性是相等的。我们设想信源的速率R是连续变量，即R可取任意非负数。

二元对称信道（简记为BSC[2]）是一个客体，它每单位时间可传输一个比特。但是，信道并不是完全可靠的：存在一个固定的概率p，$0 \leqslant p \leqslant \frac{1}{2}$（称为**原误码率**[3]或**原比特错误**

*注，上标给出的注释列在每一章的末尾。

概率），即输出比特不等同于输入比特。

我们设想有一个发送者和一个接收者。发送者必然力求把信源的输出尽可能准确地传送给接收者，而二者之间使用的通信线路只是BSC。（但是，在信源接通前，接收者与发送者之间予先知道对方使用的数据处理策略）。我们假定发送者和接收者都拥有足够的计算能力和储存容量，都得到政府的大量资金和其他物资的资助。

现在要问，对于给定的信源速率R，发送者和接收者在BSC上进行通信有多高的准确性？对这个问题，我们终久要给出一个准确的一般答复，但是，我们首先考虑一些特殊情形。

设R=1/3，意即，信道上传送的比特速率是信源产生比特速率的三倍，因此信源输出在传输之前可按每比特重复三次而编码。例如，信源输出的前5个比特为10100，则编码流为111000111000000。接收者收到的将是这个编码流，而由于信道“噪声”的干扰，可能使与每一信源比特相对应的三个码流比特不尽相同。若信道干扰使第2、第5、第6、第12和第13个传输比特发生错误，则接收者收到的是101011111001100。不难想到，在这种情况下，接收者译出一个给定的信源比特的最佳译码策略是对它的三次重复码采取择多判决。在上述例子中，应将接收到的消息译为11100，这时对第二个比特作出了错误判决。一般地说，一个信源比特三次重复中的两个或三个受到信道干扰的话，它将被错误地接收。于是，若用Pe表示误码率，则

$$Pe = P\{2个传输错误\} + P\{3个传输错误\}$$
$$= 3p^2(1-p) + p^3 = 3p^2 - 2p^3 \qquad (0.1)$$

因为原误码率$p\leqslant\frac{1}{2}$，所以Pe小于p；这个简单的编码方法已提高了信道的可靠性，而当p很小时，可靠性的提高是显著的。

不难看出，用多次重复每个比特的方法可以获得更高的可靠性。因此，若对某一整数n，$R=1/(2n+1)$，在传输之前可以重复每一信源比特$(2n+1)$次（见习题0.2），应用上述的择多判决译码，由此不难得到所产生的误码率$P_e^{(2n+1)}$的公式：

$$P_e^{(2n+1)}=\sum_{k=n+1}^{2n+1}P\{2n+1\text{个传输比特中}k\text{个传输错误}\}$$

$$=\sum_{k=n+1}^{2n+1}\binom{2n+1}{k}p^k(1-p)^{2n+1-k}$$

$$=\binom{2n+1}{n+1}p^{n+1}+p\text{的更高次幂项。}\qquad(0.2)$$

若$n>1$，当$p\to 0$时，$P_e^{(2n+1)}$比$n=1$时更迅速地趋于0。[4]因而，在这个意义上，较长的重复码比较短的更有效。但是，我们希望得出一个更强的论断：对一个确定的BSC，它有确定的原误码率$p<\frac{1}{2}$，则当$n\to\infty$时，$P_e^{(2n+1)}\to 0$，也就是说，通过这种重复码，信道可以得到所需要的可靠性。考察$P_e^{(2n+1)}$的表示式（0.2），我们说，可以做到这一点，但并不容易。因此，我们将用另外的方法。**弱大数定律***指出，若在信道上传输N个比特，则对任意的$\varepsilon>0$，

---

* 在附录A中讨论。

$$\lim_{N\to\infty} P\left\{ \left| \frac{\text{传输错误的个数}}{N} - p \right| > \varepsilon \right\} = 0。(0.3)$$

换言之，当N大时，被错误接收的比特的比例与p不会有很大的差异。于是我们对$P_e^{(2n+1)}$可作如下估算：

$$\begin{aligned} P_e^{(2n+1)} &= P\left\{ \text{错误接收比特的比例} \geqslant \frac{n+1}{2n+1} \right. \\ &\quad \left. = \frac{1}{2} + \frac{1}{4n+2} \right\} \\ &\leqslant P\{\text{比例} > \tfrac{1}{2}\} \\ &\leqslant P\{\,|\text{比例} - p| > \tfrac{1}{2} - p\} \end{aligned}$$

而由（0.3）式，当$n\to\infty$时，$P_e^{(2n+1)}\to 0$。于是，我们得到了这样的结论：若R很小，即使信道自身是强干扰的，也可能使总的错误概率很小。当然，这并不十分意外。

对于信源速率小于1的情况暂且讨论到此。当R>1时，情况怎样呢？我们怎样进行准确的通信呢？

例如，若R>1，我们只能传送信源输出比特的1/R，而要求接收者猜测其余部分，这种猜测就象猜一枚翻转的硬币的正反面一样。对这种不太高明的方案，不难算出所产生的误码率p_e。

$$\begin{aligned} P_e &= \frac{1}{R} \times p + \frac{R-1}{R} \times \frac{1}{2} \\ &= \frac{1}{2} - \left(\frac{1}{2} - p\right)/R \end{aligned} \qquad (0.4)$$

当R>1时，采用另一种稍好一点的方法，以R=3为例说明之。若R=3，在信道传送的比特数只是信源发出比特数的1/3，因此发送者将信源输出比特分为三个一组，且仅

传送三个一组的择多判决符号。例如，信源输出为101110101000101，发送者在信道上传送11101。接收者只要对接收到的每一比特进行三次重复。这时，若信道干扰歪曲了第2个传输比特，接收者将收到10101，他把它扩展为1110001110 00111，从而造成5个比特错误。一般地，由此所产生的误码率为

$$P_e=\frac{1}{4}\times(1-p)+\frac{3}{4}\times p$$

$$=\frac{1}{4}+\frac{p}{2} \qquad (0.5)$$

注意，它小于1/3+p/3，后者是当R=3时，我们采用原始的“硬币翻转”策略时所产生的错误概率。当R取其它整数时，这个策略的一般形式留作习题（见习题0.4）。

至此，我们所考虑的方案都是极平凡的，但并非完全无意义。下面，让我们给出一个不平凡的例子，它在1948年之前实际上还不知道。

设R=4/7，由此可知，对信源发出的每4个比特在信道上传送时只能发送3个附加比特。我们将精心地选择这3个附加比特：若4个信源比特用x_0,x_1,x_2,x_3表示，则附加的或冗余的或一致校验比特，标记为x_4，x_5，x_6，且由如下方程决定，

$$\begin{aligned} x_4&\equiv x_1+x_2+x_3 \quad (\mathrm{mod}2),\\ x_5&\equiv x_0+x_2+x_3 \quad (\mathrm{mod}_2), \qquad (0.6)\\ x_6&\equiv x_0+x_1+x_3 \quad (\mathrm{mod}_2)。\end{aligned}$$

因此，若$(x_0, x_1, x_2, x_3)=(0110)$，则$(x_4, x_5, x_6)=(011)$，而在信道上传输的7比特码字为0110011。

为了叙述接收者如何由受到干扰而被歪曲的7比特码字作出对4个信源比特的估计，即，叙述它的**译码算法**，我们用下面的方式重新写出一致校验方程式（0.6）

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0, \\ x_0 + x_2 + x_3 + x_5 &= 0, \\ x_0 + x_1 + x_3 + x_6 &= 0。 \end{aligned} \qquad (0.7)$$

（在（0.7）式中，运算是模2运算），用略有不同的方式来叙述，若矩阵H定义为

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

可看出，16个可能的码字中的每一个$x=(x_0, x_1, x_2, x_3, x_4, x_5, x_6)$都满足矩阵矢量方程

$$\mathbf{H}x^{T} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}。 \qquad (0.8)$$

（式中的上标T表示“转置”。）

设想对于在BSC上传输的比特按下述原则加上(mod2)0或1：若该比特未发生错误时加0，否则加1。这种作法证明是有效的。若传输矢量为$x=(x_0, x_1, x_2, \cdots, x_6)$，则接收矢量为$y=(x_0+z_0, x_1+z_1, \cdots, x_6+z_6)$，其中$z_i=1$，若第i分量发生了传输错误；否则$z_i=0$。于是，若$z=(z_0, \cdots, z_6)$表示**错误模式**，则$y=x-z$。接收者只知道y，但他想知道x，这时他做一件很巧妙的事：他计算下面的矢量$S=(s_0, s_1, s_2)$：

$$S^{T} = Hy^{T}$$
$$H(x+z)^{T}$$

$$= Hx^T + Hz^T$$

$$= Hz^T \quad (\text{见}(0.8)) \qquad (0.9)$$

这里，s称之为y的校正子[5]，在校正子中，0表示y满足相应的一致校验方程，而1表示不满足。根据（0.9）式，校正子不取决于发送的码字，而仅与错误模式z有关。但是，因为 $x = y + z$，若接收者能求出z，他也就求得了x，因此，他把注意力集中在求z上。方程 $S^T = Hz^T$ 表明S是H与z中的1相对应的那些列的（二进制）和，即，与被信道歪曲的码字的比特相对应的那些列的和：

$$S^T = Z_0\begin{vmatrix}0\\1\\1\end{vmatrix} + Z_1\begin{vmatrix}1\\0\\1\end{vmatrix} + \cdots + Z_6\begin{vmatrix}0\\0\\1\end{vmatrix} \qquad (0.10)$$

在已计算出S的情况下，接收者的任务就是要解出关于z的方程 $S^T = HS^T$。可惜，未知元为7而只有三个方程，因此，对任一S，z有16种可能性。对于z的验前有128种可能性，这点已是明确的。但是，接收者在剩下的16个中如何选择呢？例如，设接收到的y =（0111001），则S =（101），于是，16种可供选择的z为

0100000	0010011
1100011	0001010
0000101	0111001
0110110	1010000
0101111	1001001
1000110	1111010
1110101	0011100
1101100	1011111