高等学校
工科电子类 规划教材

GH

信息论与编码

方 军 俞槐铨 编著

電子工業出版社

内 容 提 要

本书主要内容为信息论和纠错编码两大部分。信息论部分包括信息论的基本概念、离散源无失真编码、离散信道的编码定理、连续信源和信道、率失真理论、多终端信息论和保密通信系统及其信息论基础。纠错编码部分包括线性分组码、循环码、卷积码、几何码和算术码。

本书可作为高等工科院校的高年级本科生和硕士研究生的教材，亦可供从事无线电技术和通信工程的技术人员参考。

信息论与编码

方 军　俞槐铨编

责任编辑　陆伯雄

电子工业出版社出版(北京市万寿路)

电子工业出版社发行　各地新华书店经销

北京科技印刷厂印刷

开本:787×1092毫米　1/16　印张:15.5　字数:360千字

1994年9月第1版　1994年9月第1次印刷

印数:2000册　定价:12.00元

ISBN 7-5053-2455-1/TP·722

出 版 说 明

根据国务院关于高等学校教材工作的规定，我部承担了全国高等学校和中等专业学校工科电子类专业教材的编审、出版的组织工作。由于各有关院校及参与编审工作的广大教师共同努力，有关出版社的紧密配合，从1978～1990年，已编审、出版了三个轮次教材，及时供给高等学校和中等专业学校教学使用。

为了使工科电子类专业教材能更好地适应“三个面向”的需要，贯彻国家教委《高等教育“八五”期间教材建设规划纲要》的精神，“以全面提高教材质量水平为中心，保证重点教材，保持教材相对稳定，适当扩大教材品种，逐步完善教材配套”，作为“八五”期间工科电子类专业教材建设工作的指导思想，组织我部所属的八个高等学校教材编审委员会和四个中等专业学校专业教学指导委员会，在总结前三轮教材工作的基础上，根据教育形势的发展和教学改革的需要，制订了1991～1995年的“八五”（第四轮）教材编审出版规划。列入规划的，以主要专业主干课程教材及其辅助教材为主的教材约300余种。这批教材的评选推荐和编审工作，由各编委会或教学指导委员会组织进行。

这批教材的书稿，其一是从通过教学实践、师生反应较好的讲义中经院校推荐，由编审委员会（小组）评选择优产生出来的，其二是在认真遴选主编人的条件下进行约编的，其三是经过质量调查在前几轮组织编写出版的教材中修编的。广大编审者、各编审委员会（小组）、教学指导委员会和有关出版社，为保证教材的出版和提高教材的质量，作出了不懈的努力。

限于水平和经验，这批教材的编审、出版工作还可能有缺点和不足之处，希望使用教材的单位，广大教师和同学积极提出批评和建议，共同为不断提高工科电子类专业教材的质量而努力。

电子工业部教材办公室

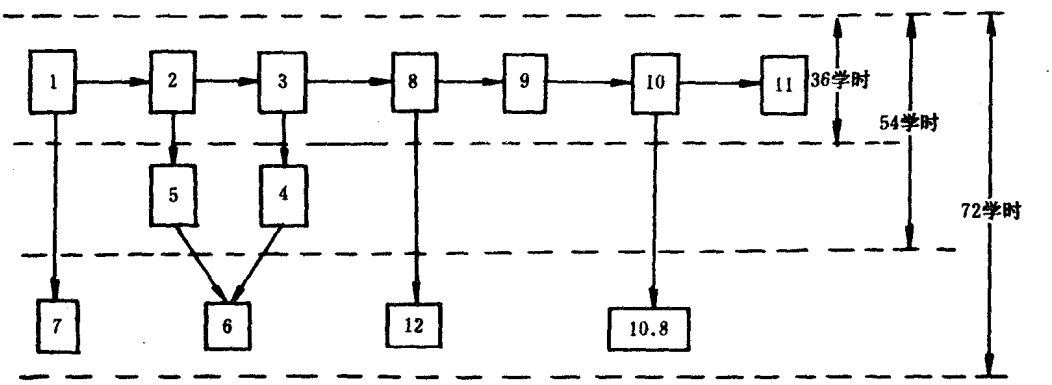
前　言

本教材系按电子工业部的工科电子类专业教材 1991～1995 年编审出版规划，由无线电技术与信息系统教材编审委员会通信教材编审小组征稿并推荐出版。责任编委为洪福明教授。

本教材由上海交通大学电子信息学院电子工程系方军副教授和俞槐铨副教授担任主编，成都电子科技大学洪福明教授担任主审。

本课程的参考教学时数为 72 小时，其主要内容为信息论和纠错编码两大部分。信息论部分的前四章是基础知识，包括信息论基本概念，离散无记忆信源编码定理和变长编码算法，以及离散无记忆信道的编码定理的近代形式，第 4 章是对连续信源与信道的一个简洁的数学处理，但要点是所导出结果的物理意义；第 5 章介绍率失真理论，它是数据压缩的基础；第 6 章简要介绍多用户信息论的基础成果；第 7 章讨论保密通信的信息论基础。纠错编码部分包括分组码和卷积码，分组码重点介绍循环码及其最重要的子类：BCH 码，实用性强的 RS 码在讲授时应予强调，交替码和 Goppa 码亦作了简介；第 11 章是对卷积码的全面介绍，重点放在卷积码的各种描述法及它们之间的联系和实用性强的维特比软判决译码算法上，其它译码技术也作了简单介绍；几何码与算术码在第 12 章里讨论。各附录包含了必要的数学基础知识的复习，对学习正文是极其重要的。虽然网格编码调制(TCM)未能成为本教材的一部分，但如果牢固掌握了本课程中信息传输理论和卷积码原理，迅速读懂有关 TCM 的论文应当是可能的。

使用本教材时请注意，本教材是为高等工科院校硕士研究生和高年级本科生设计的，经使用者的选择取舍，可以适应各种规模的教学需要：



[i]表示第 i 章，[i.j]表示第 i 章第 j 节

编者在编著过程中遵循的原则是尽量采用新的数学处理方法，这在第 1 章内表现得较为明显。各篇后附有习题与思考题，包括练习性质和扩展性质两类，前者为提高熟练程度，后者则是对正文的补充和扩展。编者希望本教材能被灵活地使用，在详细讲清基本内容的基础上，在有限的时间内牢固掌握信息论中关于信息传输的概念，学会对通信系统的基本界限进行估计；

对于编码部分，在打好代数基础后，则注重实用性。

本教材由方军编写第1至7章，以及10.8节；其余部分由俞槐铨编写。徐黎昊同志为本教材的编写做了大量实际工作，编者对他表示衷心的感谢；参加审阅工作的还有吴伟陵同志等，他们都为本书提出了许多宝贵意见，这里表示诚挚的谢意。由于编者水平有限，书中还存在着一些缺点和错误，殷切希望广大读者批评指正。

目　录

第一篇　信息论

第二篇 纠错编码

第一篇　信息论

第 1 章　信息论的基本概念

1.1　引言：通信系统的统计模型和性能估计

信息论是一门应用概率统计方法来研究信息的传输、存储和处理的学科。自从 1948 年美国学者 E. C. Shannon 发表了他的关于信息论的重要著作《通信的数学理论》以来，信息论就开始形成了一门新的学科，引起了世界各国通信学界的学者和数学家们的重视和高度的研究兴趣，因而在近几十年里获得了迅速的发展。

在信息论的研究中，人们为解决通信理论中的一些基本问题找到了正确的方法，大量的研究成果为这些基本问题提供了解答，对通信理论和技术的成熟发展起到了极为重要的推动作用。信息论为通信理论提出了各种理论界限和关于改善系统性能的启示，被认为是通信理论中的基础分枝之一。从 50 年代到现在，信息论本身经历了一个发展和成熟的过程，其中的主要经典结果又被用严格的数学方法进行了新的处理和推广，成为目前的近代信息论。近几十年来，信息论又随着通信技术的发展，朝着网络化——分散信息处理模型等方向继续发展。

尽管信息论是一门诞生仅仅四十多年的新学科，但是它已经对现代科学技术的发展产生了重大的影响。近年来，人类已经认识到信息对于社会生活的高度重要性，它同物质、能量一样，是维持生物社会的生存和进化的基本因素。

目前，世界已经进入了信息时代的初期。衡量一个国家或民族的科学技术发展水平的标志之一，是掌握对信息的传输、存储、交换和处理的能力。因此，信息论的学习对从事通信、计算机信息技术领域工作的学生和研究人员来说都是十分重要的。

在第 1 章里，我们将引入信息论的基本概念，并对整个课程作一个简单的介绍。

让我们先从通信的基本问题谈起。

信息论的奠基人 E. C. Shannon 曾经写道：

"The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point."

("通信的基本问题是要在某一端准确地或近似地再现从另一端选择出来的消息。")

这一描述虽然通俗简洁，却涉及到了通信问题的本质。通信正是一个对信息的载体——消息信号的表示或复制体——进行传输、交换和存储的过程。为了定量地研究信息在通信系统中的传输过程，Shannon 建立了通信系统的统计模型，并引入了信息的度量和熵等基本概念。

通信系统的统计模型包含信源、信道、编码器、译码器、用户等基本部分。这是一个对各种实际系统的抽象。信息的传输是这一模型中的中心问题。

Shannon 引入的统计模型可以用图 1-1 表示。

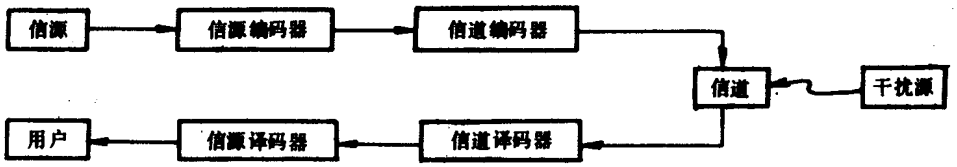


图 1-1　通信系统的统计模型

Shannon 对这一系统中的各个基本部分都作了数学描述，我们将在本书第 1 到第 5 章中详细讨论。

信源是产生消息的机构，**消息**中包含着信息，是用户所关心的部分。消息本身在系统其他部分被转换、复制并处理。实际中的信源是高度复杂的物理现象，例如人类的语言和文字显示、图像、声响，甚至于各种控制系统中的传感器等。但是在信息论里，信源被抽象成一个产生信息的随机过程。

尽管到现在，人们仍然无法在信息本身的属性这一问题上达成一致的意见，但是在 Shannon 以前的通信学家就开始试图对信息进行度量。长期以来，人们认识到，任何随机事件都包含有某种未知的不确定性因素，称为**不确定性**(uncertainty)。当这一事件发生后，人们在这个过程中获得了关于它的知识，从而去除或减少了不确定性。通常说，人们在这一过程中获得了**信息**。但是，不同的随机现象中包含的不确定性是不同的，因而信息的多少也是不同的。所以，信息的度量是信息论的最基本的问题。Shannon 在前人工作的基础上，采用事件概率的负对数作为信息的度量。我们将在 1.4 和 1.5 节中专门讨论这一问题。在成功地解决了信息度量问题之后，就有可能定量地研究它的传输问题。

信息传输和存储的媒介称为**信道**(channel)。实际中的信道也是极其广泛复杂的，例如各种通信线路、大气、水以及空间、存储介质等。在通信线路上信息从一地向另一地进行空间上的传输，而在存储器中信息则是从现在向未来进行时间上的传输。信道上不可避免地存在各种干扰源，其特性对用户而言也是未知的，通常也是用一个随机过程来描述。这样，信道的统计模型就是一个概率映射。

信息论的另一中心概念是**编码**。在经典信息论中，编码分为**信源编码**和**信道编码**两类。

由于信源产生的是信息载体——消息信号，而信号携带信息的方式是由信源的性质决定的，往往不一定利于信息的有效传输和用户的理解。为了说明这一问题，我们举一个不同语言对话者的例子。A 与 B 进行对话，如果 A 与 B 讲不同的语言，那么他们之间虽然能通信但无法理解。如果 A 与 B 都讲第三种语言，则他们往往要花更多的力气来表达以互相交流，比较起说他们各自的母语来说，通信的效率就低得多。因此，为了有效地传输信息，有必要对消息信号进行处理。这种以提高信息传输的效率为目的的信号处理称为**信源编码**。

另一方面，由于信道上存在干扰，传输的信号必然受到不同程度的影响，其结果是信号中含有的有用信息丢失，使通信的可靠性降低。为了抵抗信道干扰，提高通信的可靠性，又产生了对信号进行处理的需要。这种以提高信道上信息传输的可靠性为目的的信号处理称为**信道编码**。

在以上的统计模型的基础上，Shannon 引入了差错概率和平均失真作为通信系统的性能的度量，建立了定量的理论。首先，Shannon 为了抓住信源和信道上信息传输的本质，定义了信

源的平均信息量：**信源的熵**(source entropy)，以及**信道的容量**(channel capacity)两个关键概念，使得信源和信道的特性得以用两个物理不变量：**熵**和**容量**来刻画。这两个量又进一步地用**信息传输率**(以后将简称为**传信率**)联系起来。信息传输率与信源的熵和信道的容量的关系就是 Shannon 信息论中的主要成果：编码定理的内容。

熵是信源中所含平均信息量的度量。但是，信源的任何一种表示的符号序列中，每符号携带的信息量，即信源的传信率是一定的。记信源的熵为 H。某种表示法或称某种信源编码的传信率为 R，那么当 $R > H$ 时，就说明这种表示方法的效率不是最优的，这种表示的符号序列中含有**冗余度**(redundancy)。为了表示同一信源，冗余度小的编码的效率较高。信源编码的目的是尽可能多地去除冗余度，提高信源的表示或描述的效率。

但是，在保证信息的完全输运的前提下，传输率可以降低的程度是有限的。Shannon 证明了，这一基本界限是信源的熵 H。当 $R > H$ 时，一定存在某种信源编码方式使信息能够完全输运；否则，当 $R \leqslant H$，就是不可能的。这一结论就是**信源编码定理**。

另一方面，任何实际的信道上所能输运的信息是一定的。对于任何信道，我们当然希望可靠地输运尽可能多的信息。但在保证可靠性的前提下，信道的传输率可以提高的程度也是有限的，其上界就是信道的容量 C。为了提高传输的可靠性，一个有效的方法就是对信息进行处理，将它的载体信号变换成能够抵抗信道干扰的形式，这就是信道编码。信道编码必然在信号中引入冗余度。一个好的信道编码是保证足够的可靠性又使信道的传输率 R 尽可能高。

但是，在保证信息的可靠输运的前提下，R 可以高到多少呢？Shannon 又证明了，这一基本界限是信道的容量 C，当 $R < C$，一定存在某种信道编码方法，使信息能够可靠输运；否则，当 $R \geqslant C$，这就是不可能的。这一结论就是**信道编码定理**。

在上面的讨论中，我们并未给出信息的“完全输运”和“可靠输运”的确切定义，这是过于抽象的定性描述。为了进一步清楚地表达这些概念，要涉及到通信系统的**性能估计**(performance evaluation)问题。

通信过程是一个统计学过程。在任何通信过程中，接收端不可能预先知道发送端信源的确切内容。因此，只有在引入一定的**准则**(criteria)的前提下，才能够知道所设计的系统的性能的好坏，以及同用信息论研究该系统得到的基本界限比较，可以知道实际系统离理想程度的差距有多远，应该如何努力得到进一步的改进。信息论中应用得最基本的性能准则是**差错概率**和**平均失真量度**。

应用了这些性能准则，就可以准确地表达信源编码中信息的“完全输运“以及信道编码中信息的“可靠输运“的概念。差错概率是指发送和接收的消息信号不一致的概率。当发送和接收信号不一致时，表明信息不能够完全地传输给用户。当这种概率可以做到任意小时，就是“完全输运”信息的真实意义。同样，在信道上的信息传输中，如果发送和接收的信号不一致，则说明由于信道干扰使信息遭到破坏，如果这种不一致的概率可以做到任意小时，就是“可靠输运”的真实意义。

在信道编码定理中，证明了当 $R \geqslant C$ 时，差错概率就不可能做到任意小。但是 60 年代末期的研究进一步表明，即使当 $R < C$ 时，可靠性也随着 R 与 C 的接近程度而降低。所以提高可靠性的代价是降低传信率。这一点已经被差错控制编码的理论与技术证实。

在信源编码定理中，当 $R \leqslant H$ 时，差错是不可避免的。在这种情况下，Shannon 又进一步引入了失真度量准则，研究了当有差错时，如何使其影响尽可能小，以及在限制平均失真的条件

下尽可能地降低传信率的问题。这方面的成果是第 5 章将要介绍的**率失真理论**(rate distortion theory),它是**数据压缩**的理论基础。

综上所述,在这个引言中,我们对于通信系统的统计模型和性能估计问题作了一个简短的介绍,并叙述了经典信息论中的主要结果:信源与信道编码定理的意义。这一节论述的各个观点,都将在后续各章节中逐步得到具体化。我们将会看到,在信息论中的最关键的概念是传信率。

前五章是信息论的经典内容。第 6 章是关于多终端信息论的一个引论。第 7 章则介绍保密通信的信息论基础。本书中将要学习的信息论仅仅涉及信息的传输问题,限于以通信系统为背景,称为**狭义信息论**。目前正处于探索阶段的**广义信息论**则是在更广泛深刻的背景下研究信息的各方面的问题,本书就不作介绍了。

1.2 信　　源

在 1.1 节中我们已经叙述了信源的统计模型的概念。我们知道,尽管实际中的信源是高度复杂的,但它们的共同特征是它们产生随机的输出信号。因此,用随机过程来描述信源的统计特性是合适的。

一般情况下,记一个信源为$\{X(t,\omega),P_X(X,t)\}$,其中 $X(t,\omega)$ 表示一个随机过程,$P_X(X,t)$ 表示它的分布。

按照 $X(t,\omega)$ 的不同情况,信源可以分成很多类。

首先,如果 $X(t,\omega)$ 取值的字符集 X 为离散集合,我们称信源为**离散信源**,否则就是**连续信源**。这分别对应于空间离散的和空间连续的随机过程。

在时间上,如果过程 $X(t,\omega)$ 为时间离散的,就是**时间离散信源**,这时将信源输出写为序列 $\{Xn(\omega)\}$ 的形式。时间连续的信源常常称作**波形信源**(waveform source)。

于是,时间与空间的离散和连续就产生了四种不同的信源的类。时间与空间都离散的信源在数字通信系统、数字电子系统中比较普遍。例如,一个连续信源的输出经过取样和量化之后就成为时间、空间都离散的信源。时间离散但空间连续的信源的例子是各种取样信号。另一方面,时间连续信源也大量存在于实际系统中,但正如随机过程的情况一样,这类波形信源在描述和处理上都不如离散情况方便。在第 5 章中将讨论这类信源。连续信源的编码技术称为**数据压缩**(data compression),这是本课程的后续课题。

从信源的统计特性来看,又有几种不同的情况。下面我们对时间离散信源情况进行讨论。

当$\{Xn\}$ 中各时刻的 Xn 互相独立时,称为**无记忆源**。进一步,如果 Xn 为独立同分布(independent and identically distributed;i. i. d.),则称$\{Xn\}$ 为**独立同分布源**,即 i. i. d. 源,简记为$\{X,P_X(\cdot)\}$。

当$\{Xn\}$ 中各时刻的随机变量互相相关时,称为**有记忆源**。有记忆源的数学描述相当复杂,通常要用联合概率空间来描述。

记长为 L 的输出矢量为:

$$\boldsymbol{X}=(X_1,X_2,\ldots,X_L)\in X^L$$

那么,我们要研究联合分布函数:

$$P_{\boldsymbol{X}}(\boldsymbol{X})=Pr\{X_1<a_1,X_2<a_2,\cdots,X_L<a_L\}\quad a_i\in X,\quad i=1,\ldots,L$$

如果 $P_X(X)$ 与起始下标无关，则称为**平稳信源**：

$\forall t \in N, Pr\{X_1 < a_1, \cdots, X_L < a_L\} = Pr\{X_{t+1} < a_1, \cdots, X_{t+L} < a_L\}$，

如果 $Pr(X_L < a_L | X_1 < a_1, \cdots, X_{L-1} < a_{L-1}) = Pr(X_L < a_L | X_{L-1} < a_{L-1})$ 成立时，称信源为**马尔可夫信源**，这时：

$$Pr(X_1 < a_1, \cdots, X_L < a_L) = Pr(X_L < a_L | X_{L-1} < a_{L-1}) Pr(X_{L-1} < a_{L-1} | X_{L-2} < a_{L-2}) \cdots \cdots Pr(X_2 < a_2 | X_1 < a_1) Pr(X_1 < a_1)$$

成立。

关于平稳源我们在第 2 章中还要详细讨论。

下面介绍二个例子。

[例 1.1] 二进制对称源(BSS:Binary Symmetric Source) 记为：

$\{X, P_X(\cdot)\} = \{X \in \{0,1\}, P_X(\cdot) = (p, 1-p)\}$

其中，$Pr\{X = 0\} = p, Pr(X = 1\} = 1 - p, X$ 为 i. i. d. 过程。

[例 1.2] 离散无记忆源(DMS:Discrete Memoryless Source)X 为取值于字符集 $X = \{a_0 \cdots, a_1, \cdots, a_{K-1}\}$ 的 i. i. d. 过程。

$\forall i \in \{0,1,\cdots,K-1\}, Pr\{X = a_i\} = P_i$，且 $\sum_i P_i = 1$。

1.3 信　　道

作为信息传输媒介的信道也是高度复杂的物理对象。首先，信道有输入端和输出端，以及一个干扰源，如图 1-2 所示。

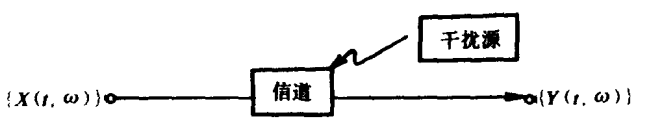


图 1-2　一般信道模型

输入、输出分别为两个随机过程，记为$\{X(t,\omega)\}$ 和$\{Y(t,\omega)\}$。

进一步考虑干扰源对输入过程的作用方式，有加性与乘性(additive and multiplicative) 两种。我们将主要讨论加性信道，它的模型可用图 1-3 表示。

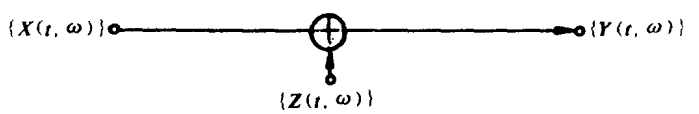


图 1-3　加性信道模型

将干扰源看作一个随机过程，它往往与输入过程独立。Shannon 进一步将图 1-2 的模型数字化，把干扰源的作用通过一个概率映射来表示。这样，输入过程的样本点以一定的概率映射为输出过程的样本点，如图 1-4 表示。

记一个信道为三元集合：$\{X, Y, P_{Y|X}(\cdot|\cdot)\}$，其中 X 为输入过程，Y 为输出过程，

$P_{Y|X}(\cdot|\cdot)$ 为信道的概率映射的统计描述，称为**信道的转移函数**。

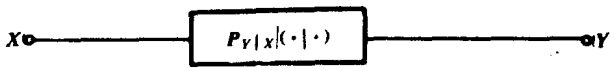


图 1-4　干扰源的概率映射表示

信道也可以按各种不同特性分类。首先，按照输入过程和输出过程取值的状态空间或字符集 X 和 Y 的离散或连续，可以分为以下几种：

(1) 当 X 和 Y 均为离散集合时，称为**离散信道**。

(2) 当 X 和 Y 均为连续集合时，称为**连续信道**。

(3) 当 X 和 Y 中一个为离散，一个为连续集合时，称为**半连续信道**。

(4) 时间离散、空间连续的信道。通常的例子是**取样信道**(sampled channel)，它是从时间、空间都连续的信道通过取样(sampling) 得到的。

(5) 时间连续信道，又称为**波形信道**(waveform channel)。

其次按统计特性又可作一些分类：

(6) 无记忆信道：输入、输出和干扰源都是独立同分布的 i. i. d. 过程。

(7) 有记忆信道：输入、或干扰源、或输出过程至少有一个不是 i. i. d. 的。其中又有平稳源与马尔可夫源以及非平稳源等。

(8) 恒参信道：信道统计特性不随时间变化。

(9) 变参信道：信道统计特性随时间变化。

恒参信道多为有线信道，如同轴电缆、光纤等，卫星信道的 C- 波段也被认为是恒参的。变参信道的例子有短波无线信道、移动通信信道等。

下面我们再举一些信道模型的例子。

[**例 1.3**]　二进制对称信道(BSC：Binary Symmetric Channel)。

$X = Y = \{0,1\}$，X 与 Y 为 i. i. d.，$P_{Y|X}(0|0) = P_{Y|X}(1|1) = 1-\varepsilon$，

$P_{Y|X}(0|1) = P_{Y|X}(1|0) = \varepsilon$，如图 1-5 所示。

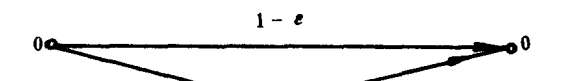


图 1-5　BSC

[**例 1.4**]　离散无记忆信道(DMC：Discrete Memoryless Channel)。

$X = \{a_0, a_1, \cdots, a_{K-1}\}$，$Y = \{b_0, b_1, \cdots, b_{J-1}\}$，$X$ 与 Y 为 i. i. d.，$P_{Y|X}(\cdot|\cdot)$ 表示为以下的转移概率矩阵。

$$\{P_{Y|X}(\cdot|\cdot)\} = \begin{bmatrix} Pr(b_0|a_0) & \cdots & Pr(b_{J-1}|a_0) \\ Pr(b_0|a_1) & \cdots & Pr(b_{J-1}|a_1) \\ Pr(b_0|a_{K-1}) & \cdots & Pr(b_{J-1}|a_{K-1}) \end{bmatrix}$$

通常 DMC 可以画为图 1-6。

下面再举几个更复杂但实际上具有重大意义的信道模型的例子。