

清华大学电子与信息技术系列教材

# 应用信息论基础

朱雪龙 编著

清华大学出版社

(京)新登字 158 号

## 内 容 简 介

本书从基本概念、基本方法和基本应用三个方面较系统全面地介绍了信息理论。本书取材既重视基础理论,又面向实际应用;既讲述成熟的原理,又适当介绍发展中的前沿课题。全书共分 9 章。第 1 章和第 2 章分别为概述和基本概念,第 3 章至第 6 章分别介绍信源的冗余度压缩编码、熵压缩编码和信道的容量与信道编码。第 7 章讨论最大熵与最小鉴别信息原理及其应用。第 8 章讨论非统计意义下的信息理论,内容包括组合信息、算法信息与通用编码。最后在第 9 章中简要介绍了通信网中的信源编码与信道容量问题。各章附有习题。

本书可作为高等学校与科研院所信息类专业研究生教材或教学参考书使用,也可供有关科技人员在学习专业基础理论时参考。

## 图书在版编目(CIP)数据

应用信息论基础/朱雪龙编著. —北京:清华大学出版社,2000

清华大学电子与信息技术系列教材

ISBN 7-302-04154-7

. 应... . 朱... . 信息学-高等学校-教材 . G201

中国版本图书馆 CIP 数据核字(2000)第 78583 号

出版者:清华大学出版社(北京清华大学学研大厦,邮编 100084)

<http://www.tup.tsinghua.edu.cn>

印刷者:北京市清华园胶印厂

发行者:新华书店总店北京发行所

开 本:787 × 960 1/16 印张:22 字数:394 千字

版 次:2001 年 3 月第 1 版 2001 年 5 月第 2 次印刷

书 号:ISBN 7-302-04154-7/TN · 116

印 数:3001 ~ 6000

定 价:26.00 元

(京)新登字 158 号

## 内 容 简 介

本书从基本概念、基本方法和基本应用三个方面较系统全面地介绍了信息理论。本书取材既重视基础理论,又面向实际应用;既讲述成熟的原理,又适当介绍发展中的前沿课题。全书共分 9 章。第 1 章和第 2 章分别为概述和基本概念,第 3 章至第 6 章分别介绍信源的冗余度压缩编码、熵压缩编码和信道的容量与信道编码。第 7 章讨论最大熵与最小鉴别信息原理及其应用。第 8 章讨论非统计意义下的信息理论,内容包括组合信息、算法信息与通用编码。最后在第 9 章中简要介绍了通信网中的信源编码与信道容量问题。各章附有习题。

本书可作为高等学校与科研院所信息类专业研究生教材或教学参考书使用,也可供有关科技人员在学习专业基础理论时参考。

## 图书在版编目(CIP)数据

应用信息论基础/朱雪龙编著. —北京:清华大学出版社,2000

清华大学电子与信息技术系列教材

ISBN 7-302-04154-7

. 应... . 朱... . 信息学-高等学校-教材 . G201

中国版本图书馆 CIP 数据核字(2000)第 78583 号

出版者:清华大学出版社(北京清华大学学研大厦,邮编 100084)

<http://www.tup.tsinghua.edu.cn>

印刷者:北京国马印刷厂

发行者:新华书店总店北京发行所

开 本:787 × 960 1/16 印张:22 字数:394 千字

版 次:2001 年 3 月第 1 版 2001 年 3 月第 1 次印刷

书 号:ISBN 7-302-04154-7/TN · 116

印 数:0001 ~ 3000

定 价:26.00 元

# 前 言

自香农(C . E . Shannon)提出信息理论以来,在大学中开设信息理论课已有近半个世纪的历史。尽管课程的中心内容都离不开香农提出的基本概念、方法和定理,但课程设置的对象、目的、课程内容的组织、取舍以至讲授的方式方法都因校、因时、因人而异,存在众多显著的差别。

信息理论涉及两个学科是造成上述差别的主要原因。在数学界,信息理论被看成是概率论的分支,是遍历性理论的分支,一个涉及不变变换理论的分支。所以在数学系,这一课程是为统计数学专业的学生开设的。而在工学界,信息理论被看成是通信理论的一部分,是通信的统计理论,是数字通信的基础理论。因此在电气或电子工程系内它是为通信专业的学生开设的。了解同一名称的课程在不同系开设时的差异不但是有益的,而且是必要的,这可使授课者或学习者都能把他们的精力有效地放在他们关心的问题 and 关心的方向上。这一本书是从工程应用的角度编写的,所以我们在信息论前加上应用两字,以明确本书的性质和特点。

其次,正如汉明(R . W . Hamming)所说,从逻辑上讲是编码理论导致信息理论,而信息理论又给出编码的性能极限。因此信息理论常和编码理论放在一起讲授,甚至把课程称为信息与编码理论。但目前这样做时其中的编码理论往往只指基于近世代数的信道编码构造理论。由于迄今在信源编码方面尚没有一个统一的构造性理论,因此目前还难于开设一个在内容上组织均衡的本来意义上的信息与编码理论。基于这一考虑,本书对信道编码的构造理论仅作简单的介绍,也不把编码理论四字纳入教材名称,以明确本书完全以信息理论为中心。

香农提出的信息理论是一种基于统计意义上的信息理论。这一理论对通信技术的发展产生了持久和深刻的影响,但它对信息技术的其他一些方面,如人工智能等,则很少有理论指导作用。所以自香农以来,人们对更广泛意义下的信息的研究一直没有停止。迄今为止,较为成熟的研究成果有:E . T . Jaynes 在 1957 年提出的最大熵原理的理论,S . K . Kullback 在 1959 年首次提出后又为 J . S . Shore 等人在 1980 年后发展了的鉴别信息及最小鉴别信息原理的理论,A . N . Kolmogorov 在 1965 年提出的关于信息量度定义的三种方法——概率

法,组合法,计算法,A . N . Kolmogorov 在 1968 年阐明并为 J . Chaitin 在 1987 年系统发展的关于算法信息的理论。这些成果大大丰富了信息理论的概念、方法和应用范围。首先,它把信息的统计定义进一步推广并对非统计意义的信息给出了一种量度。其次,信息量度的意义已不再限于信源编码和信道编码。信息的量度已系统地发展成为信息处理的一种准则,这一准则在信息技术领域正逐渐取代代表功率的最小均方误差准则。可以认为信息理论已从通信的数学理论发展成为信号与信息处理的基础理论。基于这一考虑,本书对上述列举的研究成果也作了系统的介绍。

本书共分 9 章,第 1 章介绍信息论和信息论方法。通过这一章读者可以明了在学习信息理论后什么是他们可以得到的,什么是不能得到的,以及为了他自己的学习目的,他应该如何学习。第 2 章介绍信息论的基本概念:熵、互信息和鉴别信息。这是学习本书的基础。第 3 章至第 6 章介绍香农的信源编码和信道编码理论,同时对实用的信源编码方法(如矢量量化、线性预测编码、变换编码)和信道编码方法(如线性码等)作简单的介绍。主要目的是说明信息理论如何应用于实际以及理论与实际之间存在什么差距。第 7 章介绍最大熵与最小鉴别信息原理。这一章具体体现了熵与鉴别信息作为准则在信息处理中的作用。非统计意义上的信息理论在第 8 章中介绍。这一章同时给出了通用编码方法的代表——Lempel-Ziv 编码方法及其性能界。第 9 章介绍网络中的信源编码与信道容量问题。这些内容主要针对以电路交换为基础的通信网,但不适用于以分组交换为基础的通信网。在以分组交换为基础的通信网中信息传输的载体——信号,除了在信号幅度上受到干扰外还在信号传输的延迟时间上受到干扰,这两者都对信号携带的信息量起到限制作用。它们的分析方法与这一章介绍的方法差异很大,限于篇幅,这部分内容在书中未作介绍。

作者希望通过这 9 章的内容能为读者提供有关信息理论的比较全面和比较系统的知识。在全书各章的叙述中作者都尽可能地使基本概念和基本方法的描述清晰易懂,为此省略了某些数学细节。少数不涉及基本概念且较深入的内容在目录中用 \* 号标出。全书除第 1, 2, 8 章外其余各章都有一些内容涉及信号处理和通信技术,这对了解信息理论的应用是有益的。为此学习本书时除了需要有概率论、随机过程的必要基础知识外,还需具有信号处理和通信技术方面的基础知识。

我国已故院士常迥教授,信息科学界的前辈周炯 院士,吴佑寿院士以及知名学者仇佩亮、章照止、钟义信、周荫清、孟庆生、王新梅、贾世楼、金振玉、方军、

姜丹等都在信息理论方面有很好的著作或教材。国外学者如 T . M . Cover, T . Berger, R . E . Blahut, R . G . Gallager 等也都有很好的专著或教材。作者在编写此书时得益于早期对他们著作的学习,在此顺表谢意。

作者感谢清华大学电子工程系对作者的信任,使作者有机会多年担任此课程的讲授。本书正是在这一基础上写成的。

作者还感谢艾红梅、邓北星及郁杨在整理出版本书中的帮助。

本书不当之处,敬请来函赐教。

朱雪龙

2000 年 7 月

于清华大学电子工程系



# 目 录

第 1 章	信息论与信息论方法概述.....	1
1.1	信息、信息科学和信息论.....	1
1.2	信息论方法的应用及其取得的成果 .....	3
1.3	信息论的形成与发展 .....	7
1.3.1	通信技术的理论基础.....	7
1.3.2	统计数学的一个分支 .....	11
1.3.3	信号与信息处理的一般理论基础 .....	12
第 2 章	信息论的基本概念 .....	14
2.1	离散熵.....	14
2.1.1	熵的定义 .....	14
2.1.2	熵函数的性质 .....	19
2.1.3	熵函数形式的唯一性 .....	23
2.1.4	联合熵与条件熵 .....	26
2.2	离散互信息.....	29
2.2.1	互信息的定义 .....	29
2.2.2	多个随机变量下的互信息 .....	31
2.2.3	互信息函数的性质 .....	35
2.3	连续随机变量下的熵与互信息.....	38
2.3.1	连续随机变量下的微分熵 .....	38
2.3.2	随机变量函数的微分熵 .....	40
2.3.3	连续随机变量下的互信息 .....	42
2.4	鉴别信息 .....	44
2.4.1	鉴别信息的定义 .....	44
2.4.2	Kullback 与香农两种信息量度之间的关系 .....	47
2.4.3	鉴别信息的性质 .....	51
* 2.4.4	鉴别信息函数形式的唯一性 .....	57
2.5	对信息论基本概念的若干评注.....	70



习题 .....	71
第 3 章 信源的熵率、冗余度与冗余度压缩编码.....	74
3.1 信源、信源模型与信源编码 .....	74
3.1.1 信源 .....	74
3.1.2 信源模型 .....	75
3.1.3 信源编码 .....	77
3.2 离散稳恒信源的熵率与冗余度.....	78
3.3 离散无记忆信源的渐近等同分割性与信源的定长编码定理.....	82
3.3.1 渐近等同分割性 .....	82
3.3.2 定长编码定理 .....	84
3.4 离散无记忆信源的变长编码.....	86
3.4.1 前缀码与 Kraft 定理 .....	87
3.4.2 唯一可译码定理 .....	89
3.5 变长编码的平均码长与最优编码.....	90
3.5.1 变长编码的平均码长 .....	90
3.5.2 最优编码 .....	92
3.6 离散无记忆信源的变长树码.....	95
3.6.1 算术码 .....	95
3.6.2 算术码的存在性 .....	97
3.7 离散马尔可夫信源的熵率 .....	100
3.7.1 马尔可夫链的基本概念.....	100
3.7.2 离散马尔可夫信源熵率的计算.....	102
3.8 离散马尔可夫信源的编码定理与最优编码 .....	105
习题.....	108
第 4 章 信道、信道容量与信道的有效利用 .....	110
4.1 信道、信道模型与信道分类.....	110
4.1.1 信道.....	110
4.1.2 信道模型与信道分类.....	111
4.2 离散无记忆信道及其信道容量 .....	112
4.3 离散无记忆信道容量的计算 .....	116
4.3.1 信道容量解的充要条件.....	116
4.3.2 某些简单情况下信道容量的解.....	119

4 3 3	一般情况下信道容量的解.....	122
4 3 4	信道容量的迭代解法 .....	124
4 4	级联信道和并联信道的信道容量 .....	125
4 4 1	级联信道.....	125
4 4 2	并联信道.....	128
4 5	信道达到充分利用时输入输出字母概率分布的唯一性 .....	131
4 6	连续信道的信道容量 .....	135
4 6 1	无记忆加性噪声信道的信道容量费用函数.....	136
4 6 2	无记忆加性高斯噪声信道的信道容量费用函数.....	137
4 6 3	一般无记忆加性噪声信道的信道容量费用函数的界.....	141
4 6 4	无记忆加性高斯噪声信道的级联和并联.....	142
4 7	模拟信道的信道容量 .....	145
4 7 1	模拟随机信号的正交展开.....	145
4 7 2	模拟信道下的信道容量费用函数及其计算.....	148
4 8	限带加性白色高斯噪声信道的极限性能及其与传输要求的 匹配 .....	156
4 8 1	限带加性白色高斯噪声信道的性能及其极限.....	157
4 8 2	信道与信息传输要求的匹配.....	160
4 9	限带模拟信道的数字化 .....	163
4 10	蜂窝移动通信条件下信道的有效利用 .....	165
4 10 1	蜂窝移动通信与系统的频谱利用效率 .....	165
4 10 2	不同接入方法下蜂窝移动通信系统的频谱利用 效率及其比较 .....	167
	习题.....	171
第 5 章	信道编码.....	173
5 1	信道编码概述 .....	173
5 2	信道译码准则 .....	176
5 3	联合典型序列与联合渐近等同分割定理 .....	179
5 4	信道编码定理 .....	181
5 5	信道编译码方法的最初范例——汉明码 .....	183
5 6	分组码之一:线性码.....	185
5 6 1	线性码的定义、编码与生成矩阵 .....	185

5.6.2	线性码的伴随式与伴随式译码.....	187
* 5.7	分组码之二:循环码.....	190
5.7.1	循环码的定义.....	191
5.7.2	循环码的编码与生成多项式.....	191
5.7.3	循环码的伴随式与译码原理.....	193
5.8	树码、网格码与卷积码.....	195
5.9	关于信道编码理论的若干评注 .....	199
	习题.....	200
第6章	信源的信息速率失真函数与熵压缩编码.....	203
6.1	熵压缩编码和信源的信息速率失真函数 .....	204
6.1.1	熵压缩编码.....	204
6.1.2	离散无记忆信源的熵压缩分组编码及信源的信息 速率失真函数.....	204
6.2	信息速率失真函数的性质 .....	206
6.3	离散无记忆信源下的信息速率失真函数的计算 .....	211
6.3.1	信息速率失真函数解的充要条件及参数方程 .....	211
* 6.3.2	求解信息速率失真函数的迭代算法 .....	217
6.3.3	信息速率失真函数解的唯一性问题 .....	220
6.3.4	乘积信源的信息速率失真函数 .....	222
6.4	连续无记忆信源的信息速率失真函数 .....	224
6.4.1	连续无记忆信源信息速率失真函数的定义及其解 的充要条件.....	224
6.4.2	差值失真量度下连续无记忆信源信息速率失真 函数的计算.....	226
6.5	标量量化 .....	233
6.5.1	均匀量化.....	235
6.5.2	Lloyd-Max 算法.....	235
6.6	有记忆连续信源与模拟信源的信息速率失真函数 .....	236
6.6.1	有记忆连续信源的信息速率失真函数的定义.....	236
6.6.2	模拟信源的信息速率失真函数的定义.....	237
6.6.3	高斯有记忆连续信源的信息速率失真函数.....	237
6.6.4	高斯模拟信源的信息速率失真函数.....	240

6.7	变换编码——实用的熵压缩分组编码 .....	242
6.8	预测编码——实用的熵压缩树码 .....	248
6.8.1	最小均方误差预测器.....	249
6.8.2	最小平均绝对误差预测器.....	249
6.8.3	最大零误差概率预测器.....	249
	习题.....	251
第7章	最大熵原理与最小鉴别信息原理.....	254
7.1	非适定问题与最大熵和最小鉴别信息原理 .....	254
7.1.1	非适定问题的提出.....	254
7.1.2	最大熵原理与最小鉴别信息原理.....	255
7.2	最大熵原理的合理性 .....	258
7.3	最小鉴别信息原理与最大熵原理的公理化推导 .....	261
7.3.1	最小鉴别信息原理的推导.....	261
7.3.2	最大熵原理的推导.....	269
7.4	最小失真意义下的最大熵原理与最小鉴别信息原理 .....	269
7.4.1	方向正交与投影失真.....	270
7.4.2	投影失真的一般形式.....	272
7.4.3	最小失真准则与熵准则.....	274
7.5	最大熵与最小鉴别信息原理的应用及其解的分布 .....	276
7.5.1	最大熵与最小鉴别信息原理的应用.....	276
7.5.2	最大熵分布与最小鉴别信息分布.....	281
	习题.....	282
第8章	组合信息、算法信息与通用编码 .....	284
8.1	信源统计特性不确定时的信源编码问题 .....	284
8.1.1	统计特性失配时统计编码的性能.....	285
8.1.2	自适应统计编码.....	285
8.2	基于组合的信息量度与通用编码 .....	287
8.2.1	基于组合的信息量度.....	287
8.2.2	通用编码.....	288
8.2.3	Fitingof 通用编码的性能 .....	289
8.3	算法信息量 .....	292
8.3.1	单一事件或数值下的信息量度问题.....	292

8 3 2	Kolmogorov 算法熵 .....	293
8 4	二元字符序列的算法熵 .....	294
8 5	算法熵的不可计算性 .....	296
8 6	有限状态压缩编码器 .....	298
8 7	Lewpel-Ziv 编码 .....	302
8 8	LZ 编码压缩比与香农熵 .....	305
	习题 .....	306
第 9 章	通信网中的信源编码与信道容量 .....	309
9 1	概述 .....	309
9 2	反馈信道 .....	314
9 3	多个随机变量下的联合典型序列 .....	316
9 4	多源接入信道 .....	320
9 4 1	多源接入信道的容量 .....	320
9 4 2	相关信源输入下的多源接入信道 .....	324
9 5	高斯多源接入信道 .....	324
9 5 1	高斯多源接入信道的容量域 .....	324
9 5 2	对高斯多源接入信道容量域的讨论 .....	326
9 5 3	多源接入信道容量域与多址方法的关系 .....	327
9 6	分布信源编码 .....	329
	习题 .....	333
	参考文献 .....	335
	索引 .....	336

# 第 1 章 信息论与信息论方法概述

顾名思义,信息论是关于信息的理论,应有自己明确的研究对象和适用范围。但从信息论诞生的那时起人们就对它有不同的理解。随着信息和信息科学对现代社会生活各方面影响的不断加大和深化,人们对信息论的意义的认识 and 价值的估计也不断变化。在这一章中,我们将简要地从工程技术或技术科学的角度讨论一下什么是信息,什么是信息科学和信息论,并对信息论形成、发展的过程及其已取得的应用成果作简要的回顾。我们的目的主要是通过历史发展的实际过程来说明信息论的研究对象、方法和适用的范围。

## 1.1 信息、信息科学和信息论

什么是信息?信息一词在我国由来已久。据辞海记载,我国南唐诗人李中有诗云“梦断美人沉信息,目穿长路依楼台”,可见信息泛指音讯和消息。在近代,信息一词又被用作英语中 information 的译名,information 在英语中来自词根 inform(通知),乃指被告知的事实或知识。information 在牛津英文字典里给出的解释是“某人被通知或告知的内容、情报、消息”。在这样的解释中,信息一词显然不是作为科学名词或技术术语来定义的,因此无法对信息一词作更深入的推敲。实际上在不同的字典中对信息一词还有不同的解释,更不用说工作在不同领域的人们对信息有不同的理解了。

尽管信息一词的含义模糊和难于捉摸,但人人都感觉到它的存在。每时每刻我们都在通过对周围世界的观察去获取它,并且通过一定的方法把它传送给别人、进行交换或把它存储起来留作以后使用。这种目前尚难明确定义的信息我们暂时可以把它称为广义理解的信息。对这种广义的信息自然是值得研究的,实际上语言学家已经对其作了认真的研究,如 Zellig Harris 的著作《语言和信息的理论》就是这方面的代表。但迄今为止尚未有得到普遍接受的有关广义信息的定义。

信息作为技术术语广泛使用是在计算机特别是微处理器得到广泛应用以后的事。在计算机发展的早期,计算机处理的对象仍沿用过去的名词,如数据、记

录、报表、文字等等。但随着计算机的不断发展,无论在计算机学术界或工业界都产生一种明显的倾向,即希望有一个名称能把所有这些处理对象统统包含在内。信息这一名称恰好符合这一要求,因为只有这样一个含糊的术语才能对多种多样且在不断涌现的对象得到一个统一的、全面的、不需时时改变的表达。作为一个技术术语的信息其意义当然要比前面广义信息的含义具体得多,但仍然是比较笼统和含混不清的。

信息作为一个可以用严格的数学公式定义的科学名词首先出现在统计数学中,随后又出现在通信技术中。无论是在统计数学中还是在通信技术中定义的信息都是一种统计意义上的信息,我们可以把它简称为统计信息。统计信息是非常明确的,同时其适用范围要比广义信息狭隘得多。我们在本书中讨论的信息论正是关于这种统计信息的理论。

统计信息是一个抽象的然而明确的概念,它与作为技术术语用的信息仍有很大的区别。后者比较笼统,没有确切定义但却比较具体。有一种意见认为作为技术术语用的信息实际上是指一切符号、记号、信号等表达信息所用的形式或载体,这种意见实际上把信息的形式或载体和它的具体内容区分开来。计算机所能处理的(特别是通信所能传送的)都是信息的载体或表达形式。计算机可把信息的一种形式转换成另一种形式,如把英语文本翻译成法语文本,把数据库中的数据整理成所需形式的报表,或把气象数据进行处理后给出某一地区的气温等,而通信则把信息的具体载体或形式从甲地传送到乙地。这种看法虽然未得到广泛的承认,但基本上反映了目前的实际情况。

上述讨论归纳起来可以说:广义信息是把信息的形式、内容等全都包含在内的最广泛意义上的信息。作为技术术语的信息主要指信息的具体表达形式,虽然信息的形式总是与信息的内容有一定的联系,且不可能存在没有内容的形式,但作为技术术语的信息的确不考虑信息的内容。而统计信息则是一种有明确定义的科学名词,它与内容无关,而且不随信息具体表达形式的变化(如把文字翻译成二进制码)而变化,因而也独立于形式。它反映了信息表达形式中统计方面的性质,是一个统计学上的抽象概念。

现在我们转过来讨论信息科学和信息理论,但为此我们必须先谈谈信息技术。什么是信息技术?对此我们又无法给予明确的回答。但在实际中我们知道它是泛指计算机所涉及的各种各样的技术。有意思的是这一名词的笼统和不明确反倒成为一个优点,使它能对计算机涉及的种类繁多且在不断发展的技术得到一个统一的、全面的、高层次的表述。信息技术的出现当然使人们联想到信息

科学,因为所谓技术乃是对科学原理加以应用的具体实践。我们知道能源技术和材料技术都是有相应的科学原理作为基础的,但信息技术迄今为止还没有上述意义的信息科学作为基础,或者确切地说系统的信息科学迄今还没有完全成熟。信息科学作为一个名词来看,最早出现在图书馆学中,主要研究图书文献的检索。在计算机出现以后,信息科学被赋予新的含义,但在不同国家中它的含义不尽相同。在日本信息科学的含义和美国的计算机科学的含义相似,主要研究科学计算的理论和方法。而在美国信息科学原先主要指科学计算以外,如商业、服务业、管理统计部门等所需要的涉及大量数据但计算比较简单的数据处理问题。20 世纪 80 年代以来,信息科学的含义不断扩大,不但逐渐把计算机科学的内容统一包含在内,而且有把信息技术涉及的所有科学理论统统包含在内的趋势。20 世纪 80 年代初美国信息科学学会就曾多次举行学术讨论会研究这种意义上的信息科学,即作为信息技术理论基础的信息科学。因此,尽管人们还在不同意义上使用信息科学这一名词,但从发展和长远的观点来看,把信息科学理解成能与信息技术相对应的基础科学可能是合适的。在这样的理解下信息科学与信息理论的关系又如何呢?在美国信息科学学会所组织的一次学术讨论会上这一问题成为讨论的中心问题之一。有一部分人的意见认为统计信息理论不能解决诸如人工智能中如何进行启发式搜索和学习等问题,因此在未来的信息科学中没有信息理论的位置。但多数人的意见认为信息理论尽管有其局限性和不足,但仍然是未来信息科学所不可缺少的一块基石。近年来信息论的发展和信息论方法的逐渐广泛应用表明后一种看法是比较全面和客观的看法,我们有理由相信今后的发展还会证明这一点。

## 1.2 信息论方法的应用及其取得的成果

信息论从它诞生的那时起就吸引了众多领域学者的注意,他们竞相应用信息论的概念和方法去理解和解决本领域中的问题。50 年过去了,这期间虽有失败的教训但也不乏成功的例子,下面我们就列举若干成功的范例。

### (1) 语音信号压缩

语音信号一直是通信网中传输的主要对象。自从通信网数字化以来,压缩语音信号的编码速率就成为通信中的一个重要问题。根据信息理论的分析,语音信号所需的编码速率可以远远低于仅按 Nyquist 采样定理和量化噪声分析所决定的编码速率。几十年来的工作已在这方面取得巨大的进展:长途电话网标



准的语音编码速率已从 1972 年 CCITT G.711 标准中的  $64 \text{ kbit/s}$  降低到 1992 年 CCITT 标准中的  $16 \text{ kbit/s}$ 。在移动通信中 1988 年欧洲 GSM 标准中的语音编码速率为  $13.2 \text{ kbit/s}$ , 而 1989 年美国 CTIA 标准中的速率为  $7.95 \text{ kbit/s}$ 。对语音质量要求较低的军用通信, 美国 NSA 标准的速率在 1975 年时已达到  $2.4 \text{ kbit/s}$ 。目前, 在实验室中已实现  $600 \text{ bit/s}$  的低速率语音编码, 特别是按音素识别与合成原理构造的声码器其速率可低于  $100 \text{ bit/s}$ , 已接近信息论指出的极限。

## (2) 图像信号压缩

图像信号的信息量特别巨大, 这对图像信号的传输及存储都带来极大的不便。经过多年的研究, 到 20 世纪 80 年代时图像压缩逐步进入建立标准的阶段。1989 年 CCITT 提出电视电话/ 会议电视的压缩标准 H.261, 其压缩比达到  $25:1$  到  $48:1$  左右。1991 年 CCITT 与 ISO 联合提出的“多灰度静止图像压缩编码”标准 JPEG, 其压缩比为  $24:1$ 。对常规电视信号的压缩在 1991 年提出的国际标准 MPEG-1 中其平均压缩比可达  $50:1$ 。这些巨大的进展为图像信号进入通信领域以及多媒体计算机的发展创造了条件。此外, 随着全数字高清晰度电视技术的发展, 相应的压缩编码研究也已取得进展, 这就是 1993 年提出的 MPEG-2。

## (3) 计算机文件的压缩

由于数据库的广泛应用, 存储计算机文件所需的存储量问题日益突出。在过去的二十多年中对计算机文件的压缩已发展了至少二十余种不同的算法。1988 年澳大利亚举行的压缩算法对抗赛对各种算法进行了一次大检阅。竞赛所用的文件内容多种多样, 如各种高级语言的源程序、目标码、论文、小说、科学数据、图书目录等等。压缩工作全在当时比较典型的微机上进行。测试结果表明, 其中较好的算法都能使各种文件压缩后所需的存储量只为原文件的  $25\%$  到  $50\%$ , 其平均值约为  $30\%$  左右。压缩所需的时间和存储器开销都不大。目前, 各种压缩算法已在计算机中得到广泛的应用。

## (4) 模拟话路中数据传输速率的提高

20 世纪 50 年代初计算机开始在美国联网, 当时模拟话路是传输计算机数据的几乎唯一可用的信道。最早的调制器其速率只有  $300 \text{ bit/s}$ , 而信息论指出, 标称带宽为  $4 \text{ kHz}$ , 信噪比为  $25 \text{ dB}$  的话路信道的极限速率应在  $25 \text{ kbit/s}$  左右。所以在以后的三十多年中就开始了提高速率的长期的、现在看来是极其成功的工作。1967 年速率为  $4800 \text{ bit/s}$ , 1971 年为  $9600 \text{ bit/s}$ , 1980 年开始进

入 14.4 kbit/s, 1985 年时利用多维网格编码调制的调制器 Codex 2680 使速率达到 19.2 kbit/s, 非常接近于理论极限。信息论在模拟话路数据传输中获得的巨大成功, 其意义远远超出模拟话路本身。实际上由于模拟话路中所用的调制器可用 VLSI 电路实现, 价格低廉, 因而实际上成了信息论方法的试验场。各种在话路调制器中获得成功的调制方法都很快被推广应用到载波的高次群信道及数字微波、数字卫星信道中, 他们都同样获得了成功。

#### (5) 降低信息传输所需的功率

在远距离无线通信, 特别是深空通信中如何降低信息传输所需的功率至关重要, 因为在这种情况下发送设备的功率和天线的尺寸都已成为设备生产和使用中的一个困难问题。幸运的是正是在这个领域信息论获得了它第一批令人信服的成果。从 20 世纪 60 年代后期起, NASA 发射的所有深空探测器无一例外地在其通信设备中采取了信道编码措施, 因为根据信息理论的分析, 采用低码率的信息编码可以降低传送单位比特所需的能量  $E_b$  与噪声功率谱密度  $N_0$  之比。现在利用不太复杂的信道编码就可以使同样误码率下所需的  $E_b/N_0$  比不采用信道编码时低 6 dB 左右。其中一些好的方案(如用 RS 码作为外码、卷积码作为内码的方案)可以使误码率在  $10^{-5}$  的情况下所需的  $E_b/N_0$  降到 0.2 dB, 比不用信道编码时所需的 10.5 dB 降低了近 10 dB。

#### (6) 计算机网中数据传输可靠性的保证

随着计算机技术的发展, 计算机设备的布局变得愈来愈分散, 各种终端及外围设备离主机也越来越远, 这就产生了计算机网。近年来, 计算机网还与分布式计算机系统相联系而变得更为重要。在用各种电缆联接而成的计算机网中电噪声和各种外界的电磁干扰是不能不考虑的, 因为它使传输的信息发生差错。一般情况下局域网中的差错率在  $10^{-8}$  左右, 广域网中的差错率在  $10^{-3} \sim 10^{-5}$ 。这样高的差错率在实际应用中是无法接受的。

目前普遍采用的解决办法是带自动重发请求的差错检测码。差错检测的方法从最简单的奇偶检验到比较复杂的循环冗余检验都被采用, 但较大的网一般都用循环冗余检验。这种方法已被各种网络通信协议采用并成为标准。例如 ISO 制定的高级数据链路协议 HDLC 就采用 CCITT V.41 的 CRC 码进行循环冗余检验。HDLC 在全世界已被广泛采用, 这一标准有很广的应用领域, 许多协议都是从它派生出来的。

#### (7) 计算机中的容错问题

计算机的存储器是计算机的重要组成部分。随着计算机技术的发展无论是

内存或外存其存取速度以及存储密度等都在不断提高,如何保证存取的正确性已成为越来越突出的问题。特别是在外存中,由于存储量大,而且存储体的表面难免有缺损,要保证绝对不发生差错已不可能,现在广泛采取的解决办法是增加适当的检错纠错装置。例如 IBM4300, Cray-1 等大型机的内存都有较简单的检错纠错措施。而在外存中,根据不同的情况和要求从较简单的 Fire 码到 BCH 码以及 RS 码等都被广泛使用,例如在 IBM360 的光盘存储器中就采用了 RS 码。

#### (8) 图像信号的复原与重建

图像的复原与重建是图像信号处理的一个重要内容,在实用中有很大的价值。20 世纪 80 年代以来,最大熵方法在图像复原与重建中取得了很大的成功。在退化图像复原中,图像退化的原因是多种多样的,如由于景物的运动、光学系统的不理想、噪声等等。图像重构的形式也很多,如计算机层析图像、合成孔径射电望远镜图像、结晶学研究中用的光学干涉仪或无线电干涉仪的图像、核磁共振波谱仪图像等。在这些应用中最大熵方法较其他方法优越的主要原因是其合理性,即所得结果是我们希望可以而且能够期望的最好结果。同时也有一些派生的好处,如在盲解卷时同时给出卷积函数,在重建图像中可以同时对仪器中的某些参数进行校正等等。

虽然最大熵法在这些应用中目前还不能给出性能的解析表达式,但算法已比较成熟,如常用的剑桥算法等。

#### (9) 模式分类问题与树分类器的设计

模式分类是一个在很多学科中都遇到的问题,具有相当普遍的意义。按照这一概念相同类别的模式在空间中有较短的距离,但什么是距离一直是一个令人困惑的问题。从统计分类以及统计信息的观点来看,熵、鉴别信息(交叉熵)与互信息是各种不同情况下可以选用的比较合理的距离量度。20 世纪 80 年代以来,这一观点在模式分类中得到广泛承认并有重要的应用。例如利用互信息作准则的自顶向下法设计树分类器等效于设计香农-Fano 前缀码,在语音识别中广泛使用的 Itakura-Saito 距离实际上就是鉴别信息的一种具体形式等。此外,信息论方法在汉字识别的具体应用中也取得了很好的结果。

#### (10) 其他应用成果

信息论方法的应用领域相当广泛,有时甚至出乎我们的预料。我们知道在语言学、生物学、医学方面早已有大量论文甚至专著讨论信息论方法的应用,最近在研究人工神经网络作为联想存储器的存储容量以及分析动力系统吸引子的

分形性质时也都利用了信息论的方法。最后我们还可以提一下在经济学方面的应用成果,这就是美国经济学家 K . J . Arrow 所开创的“信息经济学”,他因在这方面的研究成果而获得诺贝尔经济学奖。至于其他种种应用我们就不一一列举了。

当信息论方法用于具体学科时,信息无疑会有其特殊的具体内容,并且会有某种概念上的发展,但信息的基本统计学性质却是一样的。例如 K . J . Arrow 在《信息经济学》的中译本序言中是这样说的:“大多数经济决策都是在具有相当的不确定性的条件下作出的,一旦不确定性的存在在形式上可以分析,信息在经济作用就变得十分重要了。人们可以花费人力及财力来改变经济领域所面临的不确定性,这种改变恰好就是信息的获得。……所以把信息作为一种经济物品来加以分析,既是可能的,也是非常重要的。”这些话,只要我们把其中的“经济”两字改成“通信”就和通信工程师说的话几乎没有什么不同。

所以,我们相信信息论方法有相当普遍的意义和价值,它在各种有关学科中的应用还会不断发展。

## 1 3 信息论的形成与发展

了解信息论的形成过程对于我们进一步了解信息论有很大的好处。从历史上看信息论的形成是两部分人共同努力的结果,一部分是通信工程方面的学者,另一部分是统计数学家。这两部分人虽然研究的是同一领域的问题,但他们感兴趣的方面和侧重点是有差异的。这种情况从信息论产生时起一直保持到现在,今天从事信息论研究工作的人仍然由这两部分人组成。根据这一实际情况我们在下面分三个方面来介绍信息论的形成与发展。

### 1 3 1 通信技术的理论基础

信息论的形成与发展最主要是以通信技术基础理论的形式逐步形成和发展起来的。这一点有它内在的原因:一方面如我们在 1.1 节中所述,广义信息的含义极其复杂,而通信本身只涉及信息的表现形式或者说只对信息的表现形式感兴趣,而这是广义信息最简单最基础的方面。因此我们可以认为正是从这最简单的方面得到突破,形成了信息论。另一方面,当通信技术得到广泛发展和应用以致形成通信网以后,人们自然要问:既然交通解决物质的运输,电网解决能量

(电力)的传输,那么通信传送的究竟是什么?而信息论正是对这一问题的全面和系统的回答。

但是不要以为人们只要想到“通信传送的究竟是什么?”就会自然地导致信息论的诞生。因为通信关心的是信息的表现形式,这种形式在通信的传输过程中可能经过多次的变换,只要通信设备还能够把发送端输入的形式足够精确地在接收端输出处再现,人们是不会进一步追根究底的。只有当人们无法实现“准确再现”时,理论上的追根究底也才有了动力,并导致信息论的诞生。下面我们就来看一看电信技术发展的过程及信息论的形成。

电信技术发展的历史可以上溯到 19 世纪 30 年代。1832 年 J. Henry 发明电报和 1838 年 F. B. Morse 发明电码使信息获得了电气的表现形式。1876 年 Bell 发明电话使人类语言第一次获得电信号的形式。1895—1896 年 Marconi 和 Popov 的工作使电报和电话可以通过电波加以传送。1904 年 Fleming 发明的二极管和 1906 年 deForest 发明的三极管放大器使电报电话的有线和无线长距离传输成为可能。可以认为电信技术在 19 世纪时所面临的主要问题是获得信息的电气表现形式以及如何将它们进行远距离传输。

进入 20 世纪后电信技术获得快速发展,如何提高信道利用率的问题开始提上日程。1917 年 G. A. Campbell 申请了第一个关于滤波器的专利,为频分复用信道提供了条件。1922 年 J. R. Carson 分析了振幅调制信号,开始明确上下边带的概念。1924 年 H. Nyquist 开始分析电报信号传输中脉冲速率与信道带宽的关系。这一结果稍后又在 1928 年的论文中得到发展,建立了限带信号的采样定理。20 世纪 20 年代电信号理论的最后一个重要发展是 R. V. L. Hartley 取得的,他在 1928 年发表的论文“信息的传输”中第一次从通信的观点出发对信息量作了定义。Hartley 的工作是在 Nyquist 已取得的结果上进行的,他的新贡献是引入了接收机在估计接收脉冲幅度时只有有限精确度的概念。按照这一概念,接收机只能分辨有限数目的脉冲幅度。假设这一数目是  $M$ , 则  $N$  个脉冲所可能组成的不同序列的总数是  $M^N$ , Hartley 就把信息量  $H$  定义为  $H = N \log M$ 。这样,通过信道传输的信息量就与信道带宽和传输总时间的积成正比。从上面这些进展可以看出,在 20 世纪 30 年代以前通信的主要目标还集中在如何使发送信号无失真地送到接收端,所用的分析方法还是分析确定性信号的方法。所以虽然 Hartley 定义了信息量,但这还不是一个统计的概念,因此其意义还是相当有限的。

20 世纪 30 年代,由于通信技术水平的提高以及随后第二次世界大战的爆

发,使通信中的噪声和抗干扰问题逐渐突出。1930年维纳(N. Wiener)开始把Fourier分析方法全面引入到随机信号的研究中来,1936年V. D. Landon发表他第一篇有关噪声的论文。与此同时抗干扰的通信方法先后出现,1936年E. H. Armstrong提出频率调制,1939年H. Dudley发明声码器,1939年H. Reeve提出了具有强抗干扰能力的脉冲编码调制。对噪声的研究到1945年时由S. O. Rice作了全面的总结。所以20世纪40年代中通信的理论已经全面走上统计分析的道路,抗干扰已经取代抗失真成为通信研究中的中心问题。在这样的背景下香农和维纳几乎同时提出了信息的统计定义。关于这一概念的产生过程,维纳在其1948年发表的《控制论》中是这样说的,“这样一来,我们就把通信工程变成为一门统计科学,变成为统计力学的一个分支。在通信工程的场合,统计因素的意义是直接明了的,信息的传递除非作为二择一的事件的传递,否则是不可能的。……为了概括通信工程的这个局面,我们必须发展一个关于信息量的统计理论。在这个理论中单位信息量就是对具有相等概率的二择一事件作选择时所传递出去的信息。这个思想差不多在同一个时候由好几位科学家提出来,其中有统计学家R. A. Fisher, Bell电话研究所的香农和作者自己。Fisher研究这题目的动机来自古典统计理论,香农的动机来自信息编码问题,作者本人的动机则来自电气滤波中的噪声与消息问题……信息量的概念非常自然地隶属于统计力学中的一个古典概念——熵。正如一个系统中的信息量是它的组织化程度的度量”。香农本人没有正面阐述这一想法的来源,但W. Weaver在其1949年与香农合写的著作中曾这样介绍过:“香农的工作植根于玻耳兹曼(Boltzman)1894年在统计物理方面的工作。玻耳兹曼已经把熵看作是‘失去的信息’,这一想法后来在1925年经L. Szilard、1932年经V. Neuman先后进一步发展。……香农的工作与R. V. L. Hartley的工作也有直接的联系。”不过应该指出的是香农在其1948年发表的信息论奠基性论文“通信的数学理论”一文中只定义了熵和互信息,而没有单独定义一个信息量。关于这一差别香农在1971年回答M. Tribus的问题时是这样说的:“我最关心的是给它取个什么名称好?我曾经想把它称为‘信息’,但这一名称有点过份,所以我决定叫它‘不确定性’。当我把这一想法和V. Neuman讨论时,他提了个好主意。他说,你应该称它为熵。理由有两条:第一,你的不确定性函数在统计力学中已经被称为熵,所以它早已有名称了。第二,更重要的是没有人知道熵到底是什么,这样在有争论时你就永远立于不败之地。”上述我们提到的两个文献,即香农的“通信的数学理论”和维纳的《控制论》后来被公认为信息论的经典著作,但后

者讨论的范围更广,它更主要的是控制论的经典著作。

在 1948 年以后的十余年中,香农对信息论的发展作出了巨大的贡献。在 1973 年出版的信息论经典论文集中,香农是 49 篇(总数)论文中 12 篇论文的作者。迄今为止,信息论的主要概念除通用编码外几乎都是香农首先提出的。除一系列基本的概念外香农的贡献还在于证明了一系列编码定理,这些定理不但给出了某些性能的理论极限,而且实际上也是对香农所给基本概念的重大价值的证明。由于香农的这一系列贡献,香农被认为是信息论的创始人。

值得指出的是,香农在给出一系列编码定理时所用的证明方法是非常独特的,他使用了他自己创造的随机编码的方法。这一方法的优点是能够给出极限性能的数学表达式,但缺点是对如何构造一个好的编码不能给出具体的指导。所以从 20 世纪 50 年代起,通信技术界就把主要的精力转向信源编码和信道编码的具体构造方法上。四十多年来,这方面取得了稳步的进展。首先,在无失真信源编码方面,香农本人提出的香农编码方法已经成为历史。1952 年 D. A. Huffman 提出的 Huffman 编码方法,1963 年 P. Elias 提出的算术编码方法,1965 年 A. N. Kolmogorov 提出的通用编码方法等现在都已有重大的改进而先后实用化。例如 Huffman 编码用于传真图像的压缩标准,算术编码用于二值图像的压缩标准 JBIG,通用编码用于计算机文件的压缩等。其次,在有失真信源编码方面,量化这一最古老的方法经过发展现在已经成为语音和图像压缩的最重要的手段。例如北美移动通信标准 IS-54 中语音压缩的标准算法就是矢量量化算法。1969 年由 T. S. Huang 首先提出的分组变换与量化方法经过发展现在已在电视图像压缩的各种标准如 H. 261, JPEG, MPEG 中得到应用,1955 年 P. Elias 提出的预测编码经过发展现在已成为美国军用通信中语音压缩的标准算法。第三,在面向数字信道的信道编码方面,20 世纪 40 年代末由 M. J. E. Golay 和汉明最早提出的分组编码技术已经发展成为系统的编码理论,成为代数学的一个分支。分组码中的不少码,如汉明码、Golay 码、Fire 码、BCH 码等都在通信、计算机技术中获得广泛应用。分组编码理论中关于能否构造出渐近好码使其极限性能满足香农编码定理的问题已由 J. Justeseu 在 1972 年的工作得到初步解决。1954 年由 P. Elias 首先提出的卷积码虽然在理论上未能获得系统的发展,但依靠计算机搜索找到的部分好码已在陆地移动通信以及卫星通信和深空通信中获得重要的应用。1993 年提出的 Turbo 码在性能上已非常接近理论极限。最后,在面向模拟信道的信道编码方面,1974 年 J. L. Massey 最早提出将编码与调制统一考虑的概念。1982 年这一想法在 G. Ungerboeck 等

人的研究下终于得到突破,这就是网格编码调制。网格编码调制实用中发生的相位含糊问题在 1984 年被 L. F. Wei 所解决,这一方法随即被 CCITT 所采纳成为一种标准。现在,网格编码调制正在向卫星通信、磁记录等领域扩展其应用范围。

信息论在近半个世纪的历程中所取得的上述这些进展说明信息论作为通信技术基础理论的意义已经有了重大的发展。从最初形成时提供性能极限和进行概念方法性指导发展到今天具体指导通信系统的结构组织和部件的设计,这种趋势势必还会进行下去,而信息论也将在与通信理论、通信系统设计的理论日益融合的过程中得到进一步的发展。

### 1.3.2 统计数学的一个分支

从历史上看信息作为一个科学名词最早出现在统计数学中。1925 年,即 R. V. L. Hartley 发表信息量定义的前 3 年,统计数学家 R. A. Fisher 就从古典统计理论的角度定义了一种信息量,这种信息量现在一般被称为 Fisher 信息量。Fisher 信息量在估计问题中迄今仍有重要的价值。

香农的论文“通信的数学理论”发表以后,一方面由于文中出现的“信息”一词引起各相关应用领域的兴趣,同时由于文中所涉及的数学问题而引起统计数学家的兴趣。如前所述,信息作为一个科学名词对统计数学家并不陌生。对数学家来说,香农工作的意义在于把熵、互信息和遍历性理论联系起来,用随机编码这一独创的方法证明了一系列编码定理,这些定理同时又说明了熵、互信息这两个概念的重要性。但香农最初的工作集中在无记忆信源和无记忆信道,虽然他也讨论了马尔可夫信源,但这与一般的稳恒信源还有相当距离。所以数学家们如 A. J. Khinchine、A. Feinstein、J. Wolfowitz 纷纷把香农的基本概念和编码定理推广到更一般的信源模型、更一般的编码结构和性能量度,并给出严格的证明。在发展信息论的概念方面,苏联数学家 A. N. Kolmogorov 有突出贡献。1956 年他提出信息量的一般定义,1958 年他指出熵相等是动力系统同构的必要条件,这一工作开辟了遍历理论的一个新方向,即动力系统的熵及其在同构中的应用。1968 年他又提出定义信息量的三种途径,首次提出序列复杂度的概念并把它和香农熵相互联系起来,这一工作后来得到 G. J. Chaitin 的发展并在 1987 年建立了算法信息理论。在数学家中我们要提到 S. K. Kullback,他在 1959 年系统地论述了鉴别信息(现在又被称为相对熵、交叉熵等)的概念、定义



及其和 Fisher 信息量、香农熵的关系。由于香农熵的概念在连续随机变量下失去意义,因此鉴别信息在这种情况下具有特别重要的价值。

以上这些进展不仅对数学本身而且对信息技术也有重大的影响。例如,动力系统同构问题的研究使人们对信源编码有了更深刻的认识并获得了一些新的结果和编码方法;序列复杂度的概念已导致通用编码,这对非遍历信源来讲是非常重要的;鉴别信息的概念为估计问题、识别问题带来了理想的数学工具,在信号处理中获得了重要的应用。

除以上这些已获重要结果的进展外,统计数学家对熵的定义作了很多推广,其中较重要的是 A . N . Kolmogorov 在 1958 年引入的 熵。熵不但解决了连续随机变量下香农熵定义推广时的困难,而且导致率失真理论的建立。此外, A . Renyi 在 1961 年时认为香农熵只是在编码问题中才是唯一可取的形式,在其他情况下其他信息度量同样可用甚至更好。Renyi 具体提出所谓  $\alpha$  阶熵,香农熵可看成是  $\alpha$  阶熵的一种极限形式因而被包括在  $\alpha$  阶熵的概念之内。自 Renyi 以后 J . Havrda 在 1967 年提出  $\alpha$  次熵, S . Arimoto 在 1971 年提出  $\alpha$  熵, S . Guiasu 在 1968、1977 年提出加权熵, B . D . Sharma 和 D . P . Mittal 于 1975 年提出  $\alpha$  阶  $\alpha$  次熵, C . Ferreri 于 1980 年引入次熵等等。这些熵在统计模式识别及模糊集理论中有某些应用,但其重要性均远不如香农熵。

香农在 1961 年最早提出的多用户信息论在 20 世纪 70 年代由于卫星通信的发展而引起广泛的讨论,特别是引起了数学家们的兴趣。这一研究一时形成高潮并在数学上取得了很多成果,但这些结果在工程问题中尚未得到成功的应用。相反,利用分组交换的多用户通信却取得了成功的应用。对于这样一些目前尚未获得重要应用的研究进展我们就不再赘述了。

### 1 3 3 信号与信息处理的一般理论基础

如前所述,信息论的基本概念最初是从古典的统计理论与通信工程中提出的。但自从信息论产生以后它的一些基本概念与方法就在一般的信号与信息处理中获得应用,并在应用过程中逐步丰富和发展了信息论的内容。今天,这方面的内容虽然还没有形成非常系统的理论或理论分支,但取得的成果是明显的。1925 年 Fisher 提出的信息量不但在估计理论中占有地位,而且迄今还在各种信号处理中获得应用。1949 年香农把他在“通信的数学理论”一文中发展起来的概念用于保密系统,发表了“保密系统的通信理论”。这一论文提出了完全保密

性等重要概念,从而奠定了密码学的理论基础。1957 年 E . T . Jaynes 发表“ 信息论与统计力学 ”, 该文提出的最大熵原理不但对统计力学有重要意义, 而且在随后的几十年中对信号处理产生了很大影响, 成为信号处理的一个重要方法。最大熵谱估计是这一原理获得成功应用的一个突出例子, 它标志着熵作为一种标准开始取代其他标准在信号处理中发挥作用。20 世纪 60 年代人们又开始在模式识别与分类中应用信息论, 其中较突出的代表是 S . Watanabe, 他最早用熵去解释模式分类过程。1969 年他发表《认识与猜测》一书, 较系统地总结了他的研究成果。到 20 世纪 80 年代时分类器特别是树分类器的设计以及模式识别器的设计已相当普遍地采用了信息论的方法, 并获得满意的结果。20 世纪 80 年代的另一个重要发展是鉴别信息或交叉熵这一概念所受到的广泛重视和研究。在这一方面, J . E . Shore 和 R . W . Johnson 的工作最有代表性, 他们发展和完善了最早由 Kullback 提出的概念, 并将其成功地应用于信号处理的各个方面。今天, 随着信号与信息处理的深入, 人们已经越来越深刻地认识到信号与信息处理的中心问题是信息。在非线性非高斯信号处理问题、在信号分类识别问题和信号重建复原等问题中信息论的方法应该取代诸如最小二乘误差等准则和方法, 信息论应该成为信号与信息处理的一个理论基础。

## 第2章 信息论的基本概念

1925年, R. A. Fisher 给出了“信息”的定义。它是从古典统计理论的角度定义的一种信息量, 又称 Fisher 信息量。Fisher 信息量在估计理论中具有重要价值, 并且在各种信号处理中获得了应用。其后, 信息论的创始人香农在其1948年发表的信息论奠基性论文“通信的数学理论”中提出了两个重要的概念熵(entropy)和互信息(mutual information)。利用这两个概念, 香农对通信系统进行理论分析, 取得了通信技术史上划时代的重要成果。1959年, S. K. Kullback 提出了另一个重要概念——鉴别信息(discrimination information), 他认为这一概念可以统一 Fisher 在1925年定义的信息以及后来由香农定义的信息。由于香农熵在连续随机变量下失去了意义, 因此鉴别信息在此情况下具有特别重要的价值。此后的几十年中对信息的研究有了很多进展, 但迄今为止在实际问题中得到最广泛应用的仍然是上述三个概念。

在这一章中, 我们将利用概率论中已经发展起来的一整套描述随机事件的理论和方法, 对离散和连续情况下的熵、互信息、鉴别信息这三个基本概念及其主要性质进行介绍和讨论。

### 2.1 离散熵

熵的概念在离散随机变量的情况下可以得到最清楚的表述, 而且不会遇到数学上的困难, 所以我们先从离散随机变量开始引入熵的概念。

#### 2.1.1 熵的定义

##### 2.1.1.1 熵的引入

设有一个离散随机变量  $X$ , 它有  $N$  个可能取值, 分别为  $a_1, a_2, \dots, a_N$ , 各种取值出现的概率分别为  $p_1 = P(a_1), p_2 = P(a_2), \dots, p_N = P(a_N)$  且

$$\sum_{n=1}^N p_n = 1$$

对这种简单的离散型随机变量,我们一般用下述分布列或密度矩阵来加以描述:

$$\begin{array}{c} X \\ P(x) \end{array} = \begin{array}{ccccc} a_1 & a_2 & \dots & a_N \\ p_1 & p_2 & \dots & p_N \end{array}$$

信息论所关心的是这一随机变量的不确定性,即我们在对这一随机变量进行观察、测量、记录(在概率论中称为“试验”)时,其结果的不确定性。因为正是这种不确定性,才驱使我们对于随机变量进行观察、记录,并从中获取信息。显然,随机变量的不确定程度越高,我们从试验中可能获取的信息也就越多。

直观地看来,随机变量的不确定程度并不都是一样的。例如,3 个随机变量  $X, Y, Z$  的密度矩阵分别为

$$\begin{array}{c} X \\ P(x) \end{array} = \begin{array}{cc} a_1 & a_2 \\ 0.01 & 0.99 \end{array}$$

$$\begin{array}{c} Y \\ P(y) \end{array} = \begin{array}{cc} b_1 & b_2 \\ 0.4 & 0.6 \end{array}$$

$$\begin{array}{c} Z \\ P(z) \end{array} = \begin{array}{cc} c_1 & c_2 \\ 0.5 & 0.5 \end{array}$$

在这 3 个随机变量  $X, Y, Z$  中,不确定性程度由小到大的排列顺序是  $X, Y, Z$ , 因为等概分布时,随机变量的不确定性程度最大。

又如,两个随机变量  $X, Y$  的密度矩阵分别为

$$\begin{array}{c} X \\ P(x) \end{array} = \begin{array}{ccccc} a_1 & a_2 & a_3 & a_4 & a_5 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \end{array}$$

$$\begin{array}{c} Y \\ P(y) \end{array} = \begin{array}{cc} b_1 & b_2 \\ 0.5 & 0.5 \end{array}$$

在这两个随机变量中,  $X$  的不确定程度比  $Y$  更高。

那么,能否严格给出这种不确定性的量度呢? 又该如何严格给出这种不确定性的度量呢?

香农指出,存在这样的不确定性的量度,它是概率分布  $p_1, p_2, \dots, p_N$  的函数  $f(p_1, p_2, \dots, p_N)$ , 且该函数满足以下 3 个先验条件:

(1) 连续性条件:  $f(p_1, p_2, \dots, p_N)$  应是  $p_n (n=1, 2, \dots, N)$  的连续函数;

(2) 等概时为单调增函数:  $f\left(\frac{1}{N}, \frac{1}{N}, \dots, \frac{1}{N}\right) = g(N)$  应是  $N$  的增函数;

(3) 可加性条件: 当随机变量的取值不是通过一次试验而是若干次试验才最后得到时,随机变量在各次试验中的不确定程度应该可加,且其和始终与通过

一次试验取得结果的不确定程度相同,即

$$f(p_1, p_2, \dots, p_N) = f((p_1 + p_2 + \dots + p_K), p_{K+1}, \dots, p_N) \\ + (p_1 + p_2 + \dots + p_K) f(p_1, p_2, \dots, p_K)$$

其中

$$p_k = \frac{p_k}{(p_1 + p_2 + \dots + p_K)}, \quad k = 1, 2, \dots, K$$

香农的研究证明,当函数  $f(p_1, p_2, \dots, p_N)$  满足上述 3 个条件时,其形式唯一,如下所示:

$$f(p_1, p_2, \dots, p_N) = - \sum_{n=1}^N p_n \log p_n$$

其中  $C = \text{常数} > 0$ 。香农把这一函数称为熵,它是随机变量不确定性的量度(关于熵中对数的底,在介绍熵的单位时再说明,这里暂时省略),并记作  $H(p_1, p_2, \dots, p_N)$  或  $H(\mathbf{p})$ ,即

$$H(p_1, p_2, \dots, p_N) = - \sum_{n=1}^N p_n \log p_n \quad (2.1)$$

当有多个随机变量时,为区别不同随机变量的熵,可将熵写成  $H(X)$ ,  $H(Y)$ ,以分别表示  $X$  或  $Y$  的熵,但是,这并不表示  $X$  或  $Y$  是熵  $H$  的宗量。

### 2.1.1.2 香农熵与热力学中热熵的关系

熵这一名称并不是香农首先提出的。最先提出熵这一名称的是物理学家 R. Clausius,他提出的熵现在称其为热熵,它是热力学系统的一个状态函数,即

$$S = \frac{dQ}{T}$$

其中  $Q$  是热量,  $T$  是绝对温度。以后不久,玻耳兹曼给出了热熵  $S$  与热力学概率的关系

$$S = k \ln \Omega$$

其中  $\Omega$  是指一个物理系统所处宏观状态所对应的微观状态数。1900 年,普朗克引进玻耳兹曼常数  $k$  后,得到玻耳兹曼关系式

$$S = k \ln \Omega$$

热熵是物理系统无序性的量度。 $\Omega$  越大,表明物理系统可能的微观状态数也就越多,从微观上看,系统就越变化多端,越没有秩序。

香农在研究随机变量不确定性量度时所得的式(2.1)在数学模型层次上与热熵完全相同,所以香农根据 V. Neumann 的意见,也把它称作熵,现在一般称

其为信息熵或香农熵。

若把系统分子的相空间作为系统宏观状态的状态空间,则按分子在相空间中的分布而求得的香农熵  $H$  与其热熵  $S$  有如下的关系:

$$S = kH$$

因此,可以认为热熵是香农熵的一个特例,它仅仅是分子在相空间所处位置的不确定性的量度。

然而,热熵是有量纲的,而香农熵是无量纲的,这是两者的重大差别。

### 2.1.1.3 熵可以作为信息的量度

对于随机变量而言,其取值是不确定的。在做随机试验之前,我们只了解各取值的概率分布,而做完随机试验后,我们就确切地知道了取值,不确定性完全消失。这样,通过随机试验我们获得了信息,且该信息的数量恰好等于随机变量的熵。在这个意义上,我们可以把熵作为信息的量度。

例 2.1 掷一枚色子,各个点数出现的概率相等,用随机变量  $X$  表示为

$$\begin{array}{c} X \\ P(x) \end{array} = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 \end{array}$$

则该随机变量  $X$  的熵为

$$H(X) = - \sum_{n=1}^6 p_n \log p_n = \log 6$$

当掷出色子,得知点数为 2 时,该随机变量的不确定性完全消除,此时概率分布为

$$\begin{array}{c} X \\ P(x) \end{array} = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{array}$$

则随机变量  $X$  在做完试验后,其熵变为

$$H(X) = 0$$

在此过程中,试验者获得的信息量为

$$H(X) - H(X) = \log 6$$

例 2.2 同时掷两枚色子,设各个点数出现的概率相等,用随机变量  $Y$  表示两个色子面朝上的点数之和时,有

$$\begin{array}{c} Y \\ P(y) \end{array} = \begin{array}{cccccccccccc} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ \frac{1}{36} & \frac{2}{36} & \frac{3}{36} & \frac{4}{36} & \frac{5}{36} & \frac{6}{36} & \frac{5}{36} & \frac{4}{36} & \frac{3}{36} & \frac{2}{36} & \frac{1}{36} \end{array}$$

则该随机变量  $Y$  的熵为

$$H(Y) = - \sum_{n=1}^{11} p_n \log p_n = 3.2744$$

当掷出色子,得知点数之和为 8 时,随机变量  $Y$  的不确定性已经消除,试验者获得的信息量为  $H(Y)$ 。但若要确定色子各自朝上的点数  $X_1 X_2$ ,则仍存在不确定性,因为它们可能是

$$X_1: \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$$

$$X_2: \quad 6 \quad 5 \quad 4 \quad 3 \quad 2$$

5 种等概情况之一,得知点数之和为 8 时系统  $X_1 X_2$  的熵由原来的  $\log 36$  变为

$$H(X_1 X_2) = - \sum_{n=1}^5 \frac{1}{5} \log \frac{1}{5} = \log 5$$

在此过程中,试验者获得的信息量为  $\log 36 - H(X_1 X_2)$ 。

熵与信息的关系曾被利用来为“麦克斯韦(J. C. Maxwell)妖”这一悖论提供一种解释。该悖论认为,麦克斯韦妖能使物理系统的热熵在没有能量交换的情况下自动减小。

1929 年, L. Szilard 指出“麦克斯韦妖”一定是把信息转换成了负熵; 1930 年, G. N. Lewis 进一步指出熵的增加是由于系统从已知分布进入到一个未知分布,熵的增加只是意味着信息的丢失而已; 1943 年, E. Schrödinger 指出生命物质从环境中引出“有序”,以负熵为生。以上这些讨论中指出的信息和熵都不是香农信息论中的信息和熵。1951 年, L. Brillian 在研究香农信息论以后,才把香农的信息量与热力学熵联系起来,建立了信息负熵原理,并称其为广义第二定律:

“信息与负熵之间可以相互转换。物理系统的热力学熵在没有能量交换情况下的自动减小,实际上是由于信息转换成了负熵的缘故。”

然而,对此仍存在争议,表现在:

(1) 对香农熵和热力学熵存在联系的质疑: 1963 年, Jaynes 认为香农量度和热力学熵是完全不同的概念,“我们的工作决不应是主张或主观认为这两者有什么关系,需要的倒是从已知的数学和物理事实中看看这之间会有什么关系存在。”

(2) 对广义第二定律的质疑: 1984 年, K. G. Dewbig 指出“负熵原理只在启发性的意义上有用,而远非一条规律。所谓信息和负熵之间的转换带有一定的欺骗性,因为这一转换实际上是不可逆的。”因为生命物质从无序(负熵)到有

序(信息),熵是减小的,反之则不成立。

应该指出,香农本人并没有把  $H(X)$  称为信息,因为他认为信息一词的含义过于广泛和含糊,他也没有像后来很多著作中那样,把  $-\log p_n$  称为“自信息”,然后把  $H(X)$  看成是自信息的均值。继香农之后,对熵的定义在概念上又有很多发展,最重要的是 Kolmogorov 熵。迄今,物理学界仍在讨论 Clausius、玻耳兹曼、J. W. Gibbs、香农、Kolmogorov 等人所定义的各种熵在概念上的关系。

## 2.1.2 熵函数的性质

香农熵是概率矢量的非负的上凸函数。

**性质 2.1** 熵函数具有非负性,即  $H(\mathbf{p}) \geq 0$ 。

证明 注意

$$H(\mathbf{p}) = - \sum_{n=1}^N p_n \log p_n$$

而

$$0 \leq p_n \leq 1$$

故

$$\log p_n \leq 0$$

所以

$$H(\mathbf{p}) \geq 0$$

另外,对任意  $x > 0$ , 有

$$\log x \leq x - 1 \quad \text{或} \quad \log \frac{1}{x} \geq 1 - x$$

所以

$$H(\mathbf{p}) = - \sum_{n=1}^N p_n \log \frac{1}{p_n} = \sum_{n=1}^N p_n (1 - p_n) \geq 0 \quad \text{证毕}$$

在讨论熵函数的凸性之前,首先让我们回顾一下有关凸性的概念。

若对区域  $D$  中任意两点  $\mathbf{x}$  和  $\mathbf{y}$ ,  $\mathbf{x}, \mathbf{y} \in D$ , 均有

$$\lambda \mathbf{x} + (1 - \lambda) \mathbf{y} \in D, \quad \lambda \in [0, 1]$$

则称区域  $D$  是凸域。我们可以这样理解,若两点  $\mathbf{x}$  和  $\mathbf{y}$  在凸域  $D$  内,则  $\mathbf{x}$  和  $\mathbf{y}$  之间的线段也整个在区域  $D$  内。

凸域的例子很多,例如实数域是凸域,但整数、有理数不是凸域;由  $N$  个概



率分量组成的概率矢量的集合

$$S_P = \{ \mathbf{p}; p_n \geq 0, n = 1, 2, \dots, N, \sum_{n=1}^N p_n = 1 \}$$

是一个  $N - 1$  维的凸域。如  $N = 2$  时, 设

$$\mathbf{p}_1 = (0.5, 0.5), \quad \mathbf{p}_2 = (0.4, 0.6)$$

则有

$$\lambda \mathbf{p}_1 + (1 - \lambda) \mathbf{p}_2 = (\lambda p_{11} + (1 - \lambda) p_{21}, \lambda p_{12} + (1 - \lambda) p_{22})$$

此时仍然有

$$\lambda p_{11} + (1 - \lambda) p_{21} + \lambda p_{12} + (1 - \lambda) p_{22} = \lambda + (1 - \lambda) = 1$$

故

$$\lambda \mathbf{p}_1 + (1 - \lambda) \mathbf{p}_2 \in S_P$$

若在凸域  $D$  上的  $f(\mathbf{x})$  满足关系式

$$f(\lambda \mathbf{x} + (1 - \lambda) \mathbf{y}) \leq \lambda f(\mathbf{x}) + (1 - \lambda) f(\mathbf{y}), \quad \mathbf{x}, \mathbf{y} \in D, \quad 0 \leq \lambda \leq 1$$

则称函数  $f(\mathbf{x})$  为凸函数。若上式中的不等式是严格不等式, 则称  $f(\mathbf{x})$  是定义在凸域  $D$  上的严格凸函数。

若在凸域  $D$  上的函数  $f(\mathbf{x})$  满足关系式

$$f(\lambda \mathbf{x} + (1 - \lambda) \mathbf{y}) \geq \lambda f(\mathbf{x}) + (1 - \lambda) f(\mathbf{y}), \quad \mathbf{x}, \mathbf{y} \in D, \quad 0 \leq \lambda \leq 1$$

则称函数  $f(\mathbf{x})$  为凹函数。若上式中的不等式是严格不等式, 则称  $f(\mathbf{x})$  是定义在凸域  $D$  上的严格凹函数。

凸函数和凹函数如图 2.1 所示。在有的书中, 凸函数和凹函数又分别称为下凸函数和上凸函数。

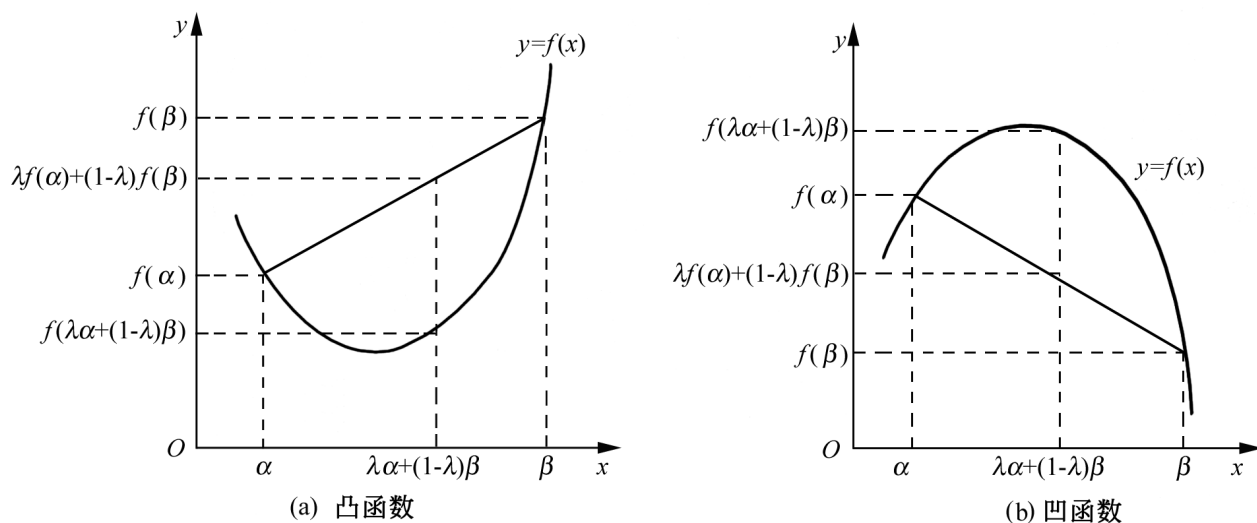


图 2.1 凸函数和凹函数示意图

设  $f(\mathbf{x})$  是凸域  $D$  上的凸函数, 且  $\mathbf{x}_m \in D, m = 1, 2, \dots, M$ , 则对  $\theta \in [0, 1]$

$$\theta \in [0, 1], \sum_{m=1}^M \theta_m = 1, \text{ 有}$$

$$f\left(\sum_{m=1}^M \theta_m \mathbf{x}_m\right) \leq \sum_{m=1}^M \theta_m f(\mathbf{x}_m) \quad (2.2)$$

这一结果被称为 Jensen 不等式。Jensen 不等式可以根据凸函数的定义和数学归纳法来证明。

若将  $(\theta_1, \theta_2, \dots, \theta_M)$  看成是由概率值组成的概率矢量, 将  $(\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M)$  看成是随机矢量  $\mathbf{X}$  可能取的值, 则 Jensen 不等式可以写成如下的形式:

$$f(E[\mathbf{X}]) \leq E[f(\mathbf{X})] \quad (2.3)$$

性质 2.2 熵函数具有凸性, 即  $H(\mathbf{p})$  是  $\mathbf{p}$  的上凸函数。

证明 我们可以分两步进行证明。

(1) 设概率矢量  $\mathbf{p} = (p_1, p_2, \dots, p_N)$  的集合组成一个区域 (记作  $D$ ),  $\mathbf{p}, \mathbf{p}'$  是区域  $D$  中的任意两个概率矢量,  $\mathbf{p} = (p_{11}, p_{12}, \dots, p_{1N})$ ,  $\mathbf{p}' = (p_{21}, p_{22}, \dots, p_{2N})$ , 则对  $\theta \in [0, 1]$  有

$$\theta \mathbf{p} + (1 - \theta) \mathbf{p}' = (\theta p_{11} + (1 - \theta) p_{21}, \theta p_{12} + (1 - \theta) p_{22}, \dots, \theta p_{1N} + (1 - \theta) p_{2N})$$

且

$$\begin{aligned} & \theta p_{11} + (1 - \theta) p_{21} + \theta p_{12} + (1 - \theta) p_{22} + \dots + \theta p_{1N} + (1 - \theta) p_{2N} \\ &= (\theta p_{11} + p_{12} + \dots + p_{1N}) + (1 - \theta)(p_{21} + p_{22} + \dots + p_{2N}) \\ &= \theta + (1 - \theta) \\ &= 1 \end{aligned}$$

所以有  $\theta \mathbf{p} + (1 - \theta) \mathbf{p}' \in D$ 。这说明概率矢量  $\mathbf{p} = (p_1, p_2, \dots, p_N)$  的集合组成的区域  $D$  是一个凸域。可令  $\mathbf{p} = \theta \mathbf{p} + (1 - \theta) \mathbf{p}'$ 。

(2) 证明不等式

$$H(\theta \mathbf{p} + (1 - \theta) \mathbf{p}') \geq \theta H(\mathbf{p}) + (1 - \theta) H(\mathbf{p}') \quad (2.4)$$

成立。因为

$$\begin{aligned} & H(\theta \mathbf{p} + (1 - \theta) \mathbf{p}') - \theta H(\mathbf{p}) - (1 - \theta) H(\mathbf{p}') \\ &= - \sum_{n=1}^N (\theta p_{1n} + (1 - \theta) p_{2n}) \log(\theta p_{1n} + (1 - \theta) p_{2n}) \\ &\quad + \sum_{n=1}^N p_{1n} \log p_{1n} + (1 - \theta) \sum_{n=1}^N p_{2n} \log p_{2n} \end{aligned}$$

$$\begin{aligned}
&= \sum_{n=1}^N p_{1n} \log \frac{p_{1n}}{p_{1n} + (1 - p_{1n}) p_{2n}} + (1 - p_{1n}) \sum_{n=1}^N p_{2n} \log \frac{p_{2n}}{p_{1n} + (1 - p_{1n}) p_{2n}} \\
&= \sum_{n=1}^N p_{1n} \log \frac{1 - \frac{p_{1n} + (1 - p_{1n}) p_{2n}}{p_{1n}}}{1} + \sum_{n=1}^N (1 - p_{1n}) \log \frac{1 - \frac{p_{1n} + (1 - p_{1n}) p_{2n}}{p_{2n}}}{1} \\
&= \sum_{n=1}^N (p_{1n} - p_{0n}) + \sum_{n=1}^N (1 - p_{1n}) (p_{2n} - p_{0n}) \\
&= \sum_{n=1}^N p_{1n} - \sum_{n=1}^N p_{0n} + \sum_{n=1}^N (1 - p_{1n}) p_{2n} - \sum_{n=1}^N p_{0n} \\
&= 0
\end{aligned}$$

所以, 式(2.4)成立, 即  $H(\mathbf{p})$  是  $\mathbf{p}$  的上凸函数。

证毕

**例 2.3** 二元熵函数是对随机变量  $X$  的如下概率分布所求的熵:

$$P(x) = \begin{matrix} X & 0 & 1 \\ & p & 1-p \end{matrix}$$

则

$$H(X) = -p \log p - (1-p) \log(1-p) = H(p) \quad (2.5)$$

而

$$H(p) = -\log p - \frac{p}{p} + \log(1-p) + \frac{1-p}{1-p} = \log \frac{1-p}{p}$$

可以证明,  $p = \frac{1}{2}$  时,  $H(p)$  取最大值, 为  $\log 2$ 。而  $p = 0$  或  $1$  时,  $H(p) = 0$

因为  $\lim_{p \rightarrow 0} p \log p = \lim_{p \rightarrow 0} \frac{\log p}{1/p} = \frac{-1/p}{-1/p^2} = -p \rightarrow 0$ , 所以二元熵函数的曲线如图 2.2 所示。

从该曲线可以看出, 等概时随机变量具有最大的不确定性, 而在  $p = 0$  或  $1$  时, 随机变量的随机性完全消失。这与我们对不确定性量度的要求是一致的。

对一般的熵函数, 我们有下述定理。

**定理 2.1** 对于离散随机变量, 当其可能的取值等概分布时, 其熵达到最大值, 即

$$\max H(X) = \log N$$

其中  $N$  为  $X$  可能取值的个数。

关于熵的单位, 由于二元概率空间是最简单的概率空间, 所以我们可以取二

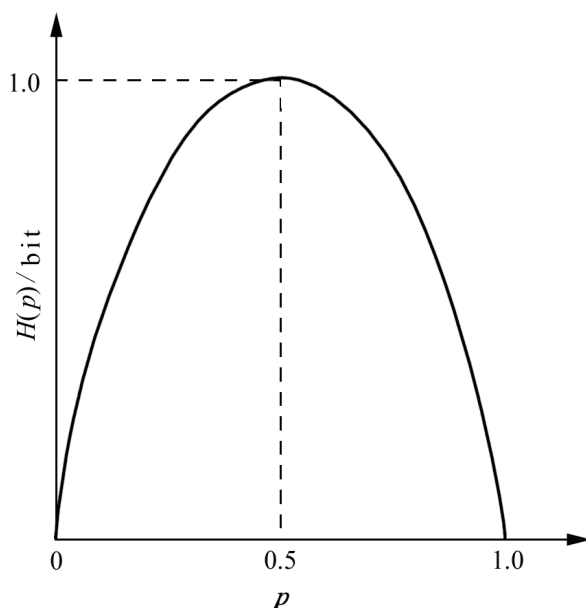


图 2.2 二元熵函数曲线

元概率空间在等概时的熵值作为单位熵。该单位就称为 bit(比特),相应的对数底应取为 2。bit 在一些二元数字系统,如数字计算机和数字通信系统的分析设计中使用相当合适。

除此之外,还有前面介绍过的以  $e$  为底的熵单位 nat(奈特),以 10 为底的熵单位 Hartley(哈特利)。在信息论的一些理论推导中使用以  $e$  为底的自然对数更加方便。

### 2.1.3 熵函数形式的唯一性

在 2.1.1 节中我们已经提到香农熵函数形式的唯一性,下述定理证明了这一结论。

**定理 2.2** 设离散随机变量的密度矩阵为

$$\begin{array}{cccc} a_1 & a_2 & \dots & a_N \\ p_1 & p_2 & \dots & p_N \end{array}$$

函数  $f(p_1, p_2, \dots, p_N)$  是随机变量不确定性的量度,若此函数满足条件

- (1) 连续性;
- (2) 等概时的单调增函数性;
- (3) 可加性。

则此函数必为

$$f(p_1, p_2, \dots, p_N) = -C \sum_{n=1}^N p_n \log p_n \quad (2.6)$$

其中  $C$  为常数。

证明 (1) 考虑随机变量  $X$  等概分布的情况, 这时有  $p_n = \frac{1}{N}$  ( $n = 1, 2, \dots, N$ )。令  $f\left(\frac{1}{N}, \frac{1}{N}, \dots, \frac{1}{N}\right) = g(N)$ , 由条件(3)可知

$$\begin{aligned} g(MN) &= f\left(\frac{1}{MN}, \frac{1}{MN}, \dots, \frac{1}{MN}\right) \\ &= g(M) + \sum_{i=1}^M \frac{1}{M} g(N) \\ &= g(M) + g(N) \end{aligned}$$

则有

$$\begin{aligned} g(s^m) &= mg(s) \\ g(t^n) &= ng(t) \end{aligned}$$

其中  $s, t, m, n$  都是正整数。

显然, 我们可以选择  $m, n$ , 使之满足

$$s^m t^n < s^{m+1}$$

对上式取对数, 有

$$m \log s + n \log t < (m+1) \log s$$

将上式两边除以  $n \log s$ , 得

$$\frac{m}{n} + \frac{\log t}{\log s} < \frac{m+1}{n}$$

所以有

$$\left| \frac{m}{n} - \frac{\log t}{\log s} \right| < \frac{1}{n} \quad (2.7)$$

由条件(2)可得

$$mg(s) + ng(t) = (m+1)g(s)$$

将上式两边除以  $ng(s)$ , 得

$$\frac{m}{n} + \frac{g(t)}{g(s)} < \frac{m+1}{n}$$

所以有

$$\left| \frac{m}{n} - \frac{g(t)}{g(s)} \right| < \frac{1}{n} \quad (2.8)$$

综合式(2.7)和式(2.8), 并根据  $|a \pm b| \leq |a| + |b|$ , 即有

$$\left| \frac{g(t)}{g(s)} - \frac{\log t}{\log s} \right| < \frac{2}{n}$$

由于  $s, t$  任意,  $n$  可任意大, 所以有

$$\frac{g(t)}{g(s)} = \frac{\log t}{\log s}$$

即

$$g(t) = C \log t$$

其中  $C$  为常数。

(2) 考虑随机变量  $X$  非等概分布, 但此时概率为有理数的情况, 此时概率可表示为

$$p_n = \frac{m_n}{N}$$

其中  $m_n$  为整数。令  $M = \sum_{n=1}^N m_n$ , 由条件(3),  $g(M)$  可以写成

$$g(M) = f(p_1, p_2, \dots, p_N) + \sum_{n=1}^N p_n g(m_n)$$

于是

$$\begin{aligned} f(p_1, p_2, \dots, p_N) &= g(M) - \sum_{n=1}^N p_n g(m_n) \\ &= C \log M - \sum_{n=1}^N p_n C \log m_n \\ &= C \log M \sum_{n=1}^N p_n - C \sum_{n=1}^N p_n \log m_n \end{aligned}$$

则

$$f(p_1, p_2, \dots, p_N) = -C \sum_{n=1}^N p_n \log \frac{m_n}{M} = -C \sum_{n=1}^N p_n \log p_n$$

(3) 考虑随机变量  $X$  非等概分布, 但此时概率为无理数的情况。根据无理数可以用有理数逼近以及条件(1), 可以证明在此情况下仍然有

$$f(p_1, p_2, \dots, p_N) = -C \sum_{n=1}^N p_n \log p_n$$

综合以上所述, 可以得出结论

$$f(\mathbf{p}) = - \sum_{n=1}^N p_n \log p_n = H(\mathbf{p}) = H(X) \quad \text{证毕}$$

由于  $H(\mathbf{p})$  只与概率分布有关, 而与所取的可能值无关, 所以为了加以区分, 可将  $H(\mathbf{p})$  记作  $H(X)$ ,  $H(Y)$  等。对于二元随机变量, 其密度矩阵为

$$\begin{pmatrix} 0 & 1 \\ p & 1-p \end{pmatrix}$$

时,  $H(\mathbf{p})$  可以简记作  $H(p)$ 。

值得一提的是, 熵函数形式的唯一性是受上述 3 个条件限制的。当然, 这些限制条件可以有所变化, 但均可以得到熵函数的唯一形式。例如 D. A. Fadiev 给出的 3 个条件如下:

(1) 连续性;

(2) 可加性;

(3) 对称性:  $f(p_1, p_2, \dots, p_N) = f(p_2, p_3, \dots, p_N, p_1) = \dots = f(p_N, p_{N-1}, \dots, p_2, p_1)$

而 A. I. Khinchin 给出的 4 个条件则分别为:

(1) 连续性;

(2) 可加性;

(3) 极值条件: 等概时熵函数最大, 即

$$\max f(p_1, p_2, \dots, p_N) = f\left(\frac{1}{N}, \frac{1}{N}, \dots, \frac{1}{N}\right)$$

(4) 事件集合中零概率事件集不影响不确定性, 即

$$f(p_1, p_2, \dots, p_N) = f(p_1, p_2, \dots, p_N, 0)$$

若把限制条件放得更宽, 则可以得到其他形式的熵函数, 如 Fisher 熵、阶熵、次熵、熵、广义相加熵、一次熵、二次熵、三角熵、加权熵等形式。

## 2.1.4 联合熵与条件熵

在前面我们已知道, 一个随机变量的不确定性可以用熵来表示。这一概念可以方便地推广到多元随机变量。利用多元随机变量的联合概率分布和条件概率分布, 可以相应得到联合熵与条件熵。本节我们将只讨论两个随机变量的情形, 因为由此就不难导出多个随机变量时相似的一些结论。

设二元随机变量  $(X, Y)$  可能的取值为  $(a_k, b_j)$ ,  $k=1, 2, \dots, K$ ,  $j=1, 2, \dots, J$ ,

其联合概率分布为

$$p(a_k, b_j) \quad \begin{matrix} k=1, 2, \dots, K \\ j=1, 2, \dots, J \end{matrix}$$

仿照一元随机变量定义熵的办法, 可以定义

$$H(XY) = - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(a_k, b_j) \quad (2.9)$$

则称  $H(XY)$  为二元随机变量  $(X, Y)$  的联合熵, 它是二元随机变量的不确定性的量度。

根据

$$\begin{aligned} p(a_k) &= \sum_{j=1}^J p(a_k, b_j), \quad p(b_j) = \sum_{k=1}^K p(a_k, b_j) \\ p(a_k, b_j) &= p(a_k) p(b_j | a_k) = p(b_j) p(a_k | b_j) \end{aligned}$$

式(2.9)可以转化为

$$\begin{aligned} H(XY) &= - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(a_k) p(b_j | a_k) \\ &= - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(a_k) - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(b_j | a_k) \\ &= - \sum_{k=1}^K p(a_k) \log p(a_k) + \sum_{k=1}^K p(a_k) H(Y | a_k) \end{aligned}$$

故有

$$H(XY) = H(X) + H(Y | X) \quad (2.10)$$

我们称  $H(Y | X)$  为条件熵, 它是  $X$  取值  $a_k$  条件下  $Y$  的熵  $H(Y | a_k)$  的平均值,  $H(Y | a_k)$  称为  $X$  取值  $a_k$  条件下  $Y$  的条件熵, 即

$$\begin{aligned} H(Y | X) &= - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(b_j | a_k) \\ &= \sum_{k=1}^K p(a_k) H(Y | a_k) \end{aligned} \quad (2.11)$$

类似地, 可以得到

$$H(XY) = H(Y) + H(X | Y) \quad (2.12)$$

条件熵表示在已知一随机变量的情况下, 对另一随机变量的不确定性的量度。

下面我们对联合熵、条件熵作一下简单讨论。当二元随机变量的两个分量  $X, Y$  相互独立时, 有



$$p(a_k, b_j) = p(a_k) p(b_j)$$

$$p(a_k | b_j) = p(a_k)$$

$$p(b_j | a_k) = p(b_j)$$

于是有

$$H(XY) = H(X) + H(Y) \quad (2.13a)$$

$$H(X | Y) = H(X) \quad (2.13b)$$

$$H(Y | X) = H(Y) \quad (2.13c)$$

这表明,当随机变量相互独立时,其联合熵等于单个随机变量的熵之和,而条件熵等于无条件熵。

在一般情况下,联合熵、条件熵和无条件熵存在下列不等关系:

$$H(XY) \geq H(X) + H(Y) \quad (2.14a)$$

$$H(X | Y) \leq H(X) \quad (2.14b)$$

$$H(Y | X) \leq H(Y) \quad (2.14c)$$

其证明如下:

$$\begin{aligned} & H(XY) - H(X) - H(Y) \\ &= - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(a_k, b_j) + \sum_{k=1}^K p(a_k) \log p(a_k) + \sum_{j=1}^J p(b_j) \log p(b_j) \\ &= - \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log \frac{p(a_k) p(b_j)}{p(a_k, b_j)} \\ &= \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \left( \frac{p(a_k) p(b_j)}{p(a_k, b_j)} - 1 \right) \\ &= 0 \end{aligned}$$

于是

$$H(XY) \geq H(X) + H(Y)$$

又考虑到

$$H(XY) = H(X) + H(Y | X) = H(Y) + H(X | Y)$$

所以

$$H(X | Y) \leq H(X)$$

$$H(Y | X) \leq H(Y)$$

证毕

这表明条件熵在一般情形下总是小于无条件熵。从直观上说,由于事物总是有联系的,因此对随机变量  $X$  的了解平均来讲总能使  $Y$  的不确定性减少。同

样,对  $Y$  的了解也会减少  $X$  的不确定性。

注意,条件熵总是小于无条件熵是平均意义上的。对随机变量  $X$  取某一特定值,如  $a_k$  时, $Y$  的不确定性完全有可能增加、减少或不变,这取决于  $x = a_k$  时, $Y$  取值的概率分布情况。也就是说  $H(Y|a_k) > H(Y)$ , 或  $H(Y|a_k) = H(Y)$ , 或  $H(Y|a_k) < H(Y)$  均可能出现。

同样  $H(X|b_j) > H(X)$ , 或  $H(X|b_j) = H(X)$ , 或  $H(X|b_j) < H(X)$  均可能出现。

若  $X$  和  $Y$  有确定的函数关系,且  $X$  可以完全确定  $Y$  (或  $Y$  完全确定  $X$ ), 则有

$$H(Y|X) = 0 \text{ (或 } H(X|Y) = 0 \text{)}$$

于是

$$H(XY) = H(X) \text{ (或 } H(XY) = H(Y) \text{)}$$

## 2.2 离散互信息

互信息是信息论中的第二个重要概念。本节只限于离散随机变量之间的互信息。

### 2.2.1 互信息的定义

由于事物是普遍联系的,因此,对于两个随机变量  $X$  和  $Y$ , 它们之间在某种程度上也是相互联系的,即它们之间存在统计依赖(或依存)关系。于是在获知一随机变量(如  $Y$ )的取值的条件下的条件熵  $H(X|Y)$  总是不大于另一随机变量(如  $X$ )的无条件熵  $H(X)$ 。也就是说,未知  $Y$  时, $X$  的不确定度为  $H(X)$ , 已知  $Y$  时, $X$  的不确定度变为  $H(X|Y)$ , 且有  $H(X|Y) \leq H(X)$ 。这说明  $H(X|Y)$  表示了已知  $Y$  后  $X$  “残留”的不确定度。这样,在了解  $Y$  以后, $X$  的不确定度的减少量为  $H(X) - H(X|Y)$ , 这个差值实际上也是已知  $Y$  的取值后所提供的有关  $X$  的信息。

同样,在了解  $X$  以后, $Y$  的不确定度的减少量为  $H(Y) - H(Y|X)$ , 这个差值实际上也是已知  $X$  的取值后所提供的有关  $Y$  的信息。

于是我们定义离散随机变量  $X$  和  $Y$  之间的互信息  $I(X; Y)$  为

$$I(X; Y) = H(X) - H(X|Y) \quad (2.15a)$$

或定义互信息  $I(Y; X)$  为

$$I(Y; X) = H(Y) - H(Y/X) \quad (2.15b)$$

可以证明, 互信息  $I(X; Y)$  和互信息  $I(Y; X)$  是相等的, 证明过程如下:

$$\begin{aligned} I(X; Y) &= H(X) - H(X/Y) \\ &= - \sum_{k=1}^K p(a_k) \log p(a_k) + \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(a_k / b_j) \\ &= \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log \frac{p(a_k, b_j)}{p(a_k) p(b_j)} \\ &= - \sum_{j=1}^J p(b_j) \log p(b_j) + \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log p(b_j / a_k) \\ &= H(Y) - H(Y/X) \\ &= I(Y; X) \end{aligned}$$

因此  $I(X; Y)$  和  $I(Y; X)$  是随机变量  $X$  和  $Y$  之间相互提供的信息量, 把它们称为互信息是完全确切的。

互信息的另一种定义方法是直接定义  $X$  和  $Y$  之间的互信息为

$$I(X; Y) = \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log \frac{p(a_k, b_j)}{p(a_k) p(b_j)} \quad (2.16)$$

由式(2.16)可以得到

$$I(X; Y) = H(X) + H(Y) - H(XY) \quad (2.17)$$

可以看出, 在这一表达式中,  $X$  和  $Y$  的位置是完全对称的。这一点与互信息这一名称完全一致。

在一般情况下, 互信息的值满足关系式

$$0 \leq I(X; Y) \leq \min(H(X), H(Y)) \quad (2.18)$$

证明 由于

$$H(X) \geq H(X/Y), \quad H(Y) \geq H(Y/X)$$

于是, 由定义式(2.15)可得

$$I(X; Y) \geq 0$$

这说明了解一事物总对另一事物的了解有所帮助。

由于

$$H(X/Y) \geq 0, \quad H(Y/X) \geq 0$$

又由定义式(2.15)可知

$$I(X; Y) \leq H(X)$$

$$I(X; Y) = H(Y)$$

于是可以得到

$$I(X; Y) = \min(H(X), H(Y))$$

证毕

前面已经知道,当随机变量  $X$  和  $Y$  之间统计独立时,有

$$H(X/Y) = H(X), \quad H(Y/X) = H(Y)$$

于是得到

$$I(X; Y) = 0$$

而当随机变量  $X$  和  $Y$  之间有确定的函数关系时,分如下两种情况:

(1)  $X$  可以唯一确定  $Y$ , 此时  $H(Y/X) = 0$ , 故

$$I(X; Y) = H(Y)$$

(2)  $Y$  可以唯一确定  $X$ , 此时  $H(X/Y) = 0$ , 故

$$I(X; Y) = H(X)$$

所以,互信息  $I(X; Y)$  是对  $X$  和  $Y$  之间统计依存程度的信息量度,这也是互信息的另一层含义。

互信息的上述定义和理解在信息传输和处理问题中具有很大的理论意义和实用价值。本书将在后面陆续介绍。

值得一提的是,有些书上给出“单个互信息”的定义如下:

$$I(a_k; b_j) = \log \frac{p(a_k, b_j)}{p(a_k)p(b_j)} = \log \frac{p(a_k/b_j)}{p(a_k)} = \log \frac{p(b_j/a_k)}{p(b_j)}$$

它代表已知随机变量  $Y$  取值为  $b_j$  后所获得的关于  $X$  取值为  $a_k$  的信息量。在这一定义下,互信息  $I(X; Y)$  是单个互信息的数学期望,即

$$I(X; Y) = E \log \frac{p(a_k, b_j)}{p(a_k)p(b_j)} = E \log \frac{p(a_k/b_j)}{p(a_k)}$$

当  $X$  和  $Y$  为同一随机变量,且  $b_j = a_k$  时,有

$$I(a_k; a_k) = \log \frac{p(a_k/a_k)}{p(a_k)} = \log \frac{1}{p(a_k)} = H(a_k)$$

而  $H(a_k)$  的数学期望就是熵,即

$$H(X) = E\{I(a_k; a_k)\} = E\{H(a_k)\}$$

所以由互信息也可以导出熵。

## 2.2.2 多个随机变量下的互信息

前面我们讨论了两个随机变量之间的互信息。现在我们来考虑三个或三个

以上随机变量之间的互信息。

与多个随机变量的熵相比,三个或三个以上随机变量之间的互信息要复杂得多,因为前者只要把多个随机变量作为一个多元随机矢量来考虑就可以完全解决,而后者则可以从三个角度来考虑。

### (1) 两组多元随机矢量之间的互信息

为简单具体起见,我们考虑随机变量  $X$  和二元随机矢量  $(Y, Z)$  之间的互信息。设这三个随机变量的密度矩阵分别是

$$\begin{aligned} X &= \begin{matrix} a_1 & a_2 & \dots & a_K \\ p(a_1) & p(a_2) & \dots & p(a_K) \end{matrix} \\ Y &= \begin{matrix} b_1 & b_2 & \dots & b_J \\ p(b_1) & p(b_2) & \dots & p(b_J) \end{matrix} \\ Z &= \begin{matrix} c_1 & c_2 & \dots & c_L \\ p(c_1) & p(c_2) & \dots & p(c_L) \end{matrix} \end{aligned}$$

其联合分布密度矩阵为

$$p(a_k, b_j, c_l) \quad \begin{matrix} k=1, 2, \dots, K \\ j=1, 2, \dots, J \\ l=1, 2, \dots, L \end{matrix}$$

仿照前面定义两个随机变量之间的互信息的方法,可以定义随机变量  $X$  和二元随机矢量  $(Y, Z)$  之间的联合互信息  $I(X; YZ)$  为

$$\begin{aligned} I(X; YZ) &= H(X) - H(X | YZ) \\ &= H(YZ) - H(YZ | X) \end{aligned} \quad (2.19)$$

以及

$$I(X; YZ) = H(X) + H(YZ) - H(XYZ) \quad (2.20)$$

由前面讨论可知

$$I(X; YZ) = I(YZ; X)$$

联合互信息  $I(X; YZ)$  表示随机变量  $X$  与随机矢量  $YZ$  之间相互可能提供的信息量,或者说  $I(X; YZ)$  是  $X$  与  $YZ$  之间统计依存程度的信息量度。

### (2) 条件互信息

类似于研究熵时引入条件熵的方法,在研究互信息时我们可以引入条件互信息。

在已知随机变量  $Z$  的条件下定义随机变量  $X$  和  $Y$  之间条件互信息  $I(X; Y | Z)$  为

$$I(X; Y / Z) = \sum_{k=1}^K \sum_{j=1}^J \sum_{l=1}^L p(a_k, b_j, c_l) \log \frac{p(a_k, b_j / c_l)}{p(a_k / c_l) p(b_j / c_l)} \quad (2.21)$$

由此定义式可以推导得到下列关系式:

$$I(X; Y / Z) = H(X / Z) - H(X / YZ) \quad (2.22a)$$

$$I(X; Y / Z) = H(Y / Z) - H(Y / XZ) \quad (2.22b)$$

$$I(X; Y / Z) = H(X / Z) - H(XY / Z) + H(Y / Z) \quad (2.22c)$$

$$\begin{aligned} I(X; Y / Z) &= H(XZ) - H(Z) - H(XYZ) + H(Z) + H(YZ) - H(Z) \\ &= H(XZ) + H(YZ) - H(XYZ) - H(Z) \end{aligned} \quad (2.22d)$$

可以看出, 式(2.22a)至式(2.22c)除了有条件  $Z$  以外, 都与  $I(X; Y)$  类似的等式的含义相似。

可以证明, 条件互信息也是非负的, 即

$$I(X; Y / Z) \geq 0 \quad (2.23)$$

利用条件互信息, 就可以把联合互信息  $I(X; YZ)$  做如下展开:

$$\begin{aligned} I(X; YZ) &= H(X) - H(X / YZ) \\ &= H(X) - H(X / Y) + H(X / Y) - H(X / YZ) \\ &= I(X; Y) + I(X; Z / Y) \end{aligned} \quad (2.24a)$$

该式的含义是随机矢量  $(Y, Z)$  所提供的关于  $X$  的信息量等于  $Y$  所提供的关于  $X$  的信息量加上在已知  $Y$  的条件下  $Z$  所提供的关于  $X$  的信息量。

同理, 存在关系式

$$I(X; YZ) = I(X; Z) + I(X; Y / Z) \quad (2.24b)$$

而两组随机矢量之间的互信息的更一般的表达式为

$$I(XY; UVW) = I(XY; W) + I(XY; V / W) + I(XY; U / VW) \quad (2.25)$$

该式的推导和含义类似前面所讨论的, 不再讨论。

### (3) 随机矢量中各随机变量相互之间的互信息

当从该角度考虑时, 我们希望如此定义的互信息是各随机变量所共有的, 所以应对各随机变量呈现出对称性。研究表明这样的定义是可以找到的。

以三个随机变量  $X, Y$  和  $Z$  为例。三个随机变量相互之间的互信息  $I(X; Y; Z)$  为

$$I(X; Y; Z) = \sum_{k=1}^K \sum_{j=1}^J \sum_{l=1}^L p(a_k, b_j, c_l) \log \frac{p(a_k, b_j, c_l)}{p(a_k) p(b_j) p(c_l)} \quad (2.26)$$

上式是仿照  $I(X; Y)$  的直接定义式(2.16)给出的。经过变形, 式(2.26)可以化

为

$$\begin{aligned}
 I(X; Y; Z) &= \sum_{k=1}^K \sum_{j=1}^J \sum_{l=1}^L p(a_k, b_j, c_l) \log \frac{p(a_k, b_j)}{p(a_k) p(b_j)} \\
 &\quad - \sum_{k=1}^K \sum_{j=1}^J \sum_{l=1}^L p(a_k, b_j, c_l) \log \frac{p(c_l) p(a_k, b_j, c_l)}{p(b_j, c_l) p(c_l, a_k)} \\
 &= I(X; Y) - I(X; Y | Z)
 \end{aligned} \quad (2.27a)$$

同理有

$$I(X; Y; Z) = I(Y; Z) - I(Y; Z | X) \quad (2.27b)$$

$$I(X; Y; Z) = I(Z; X) - I(Z; X | Y) \quad (2.27c)$$

按照这一方法可以得到更多随机变量之间的这种互信息。

需要说明的是, 互信息  $I(X; Y; Z)$  没有明确的物理意义, 且  $I(X; Y; Z)$  可以大于零、小于零或等于零。  $I(X; Y; Z)$  在数学上有一定的价值, 可以帮助我们推导一些关系式。除此之外,  $I(X; Y; Z)$  很少在实际问题中应用。

**例 2.4** 求证: 当随机变量  $X$  和  $Z$  统计独立时, 有

$$I(X; Y) = I(X; Y | Z)$$

**证明** 由已知, 可得  $I(X; Z) = 0$ 。利用式(2.27), 有

$$\begin{aligned}
 I(X; Y) - I(X; Y | Z) &= I(Z; X) - I(Z; X | Y) \\
 &= -I(Z; X | Y)
 \end{aligned}$$

又由条件互信息  $I(Z; X | Y) = 0$ , 所以

$$I(X; Y) - I(X; Y | Z) = 0 \quad \text{证毕}$$

当  $X, Y, Z$  两两统计独立时, 因为  $I(X; Y) = I(Y; Z) = I(Z; X) = 0$ , 于是得到

$$I(X; Y | Z) = I(Y; Z | X) = I(Z; X | Y)$$

$I(X; Y; Z)$  可正可负, 是由于条件互信息  $I(X; Y | Z)$  可能大于、等于或小于互信息  $I(X; Y)$ , 即在已知  $Z$  的条件下  $X$  与  $Y$  的统计依存程度既有可能增加, 也有可能减小。

不难证明,  $I(X; Y; Z)$  的取值范围为

$$\begin{aligned}
 -\min\{I(X; Y | Z), I(Y; Z | X), I(Z; X | Y)\} &\leq I(X; Y; Z) \\
 &\leq \min\{I(X; Y), I(Y; Z), I(Z; X)\}
 \end{aligned} \quad (2.28)$$

我国学者胡国定早在 1962 年时就已指出香农的熵与互信息可以对应于集合的某种测度, 从而可以在信息论和集合论之间建立一种关系。具体来说, 设  $A, B$  是对应于  $X$  和  $Y$  的集合变量, 利用集合  $A \cap B$  上的代数

$$F = \{A \cup B, A \cap B, A - B, B - A, \overline{A \cap B}, \overline{A \cup B}\}$$

可以定义测度  $\mu$  如下:

$$\mu(A \cup B) = H(XY), \mu(A) = H(X),$$

$$\mu(B) = H(Y), \mu(A \cap B) = I(X; Y)$$

$$\mu(A - B) = H(X|Y), \mu(B - A) = H(Y|X),$$

$$\mu(\overline{A \cap B}) = H(X|Y) + H(Y|X)$$

$$\mu(\emptyset) = 0, \text{ 其中 } A - B = A \cap \overline{B}, B - A = B \cap \overline{A}$$

这样,在信息量度和集合测度之间就可以有一种形式上的对应关系。这一关系可以推广到多个随机变量。图 2.3 给出了三个随机变量时的这种对应关系。

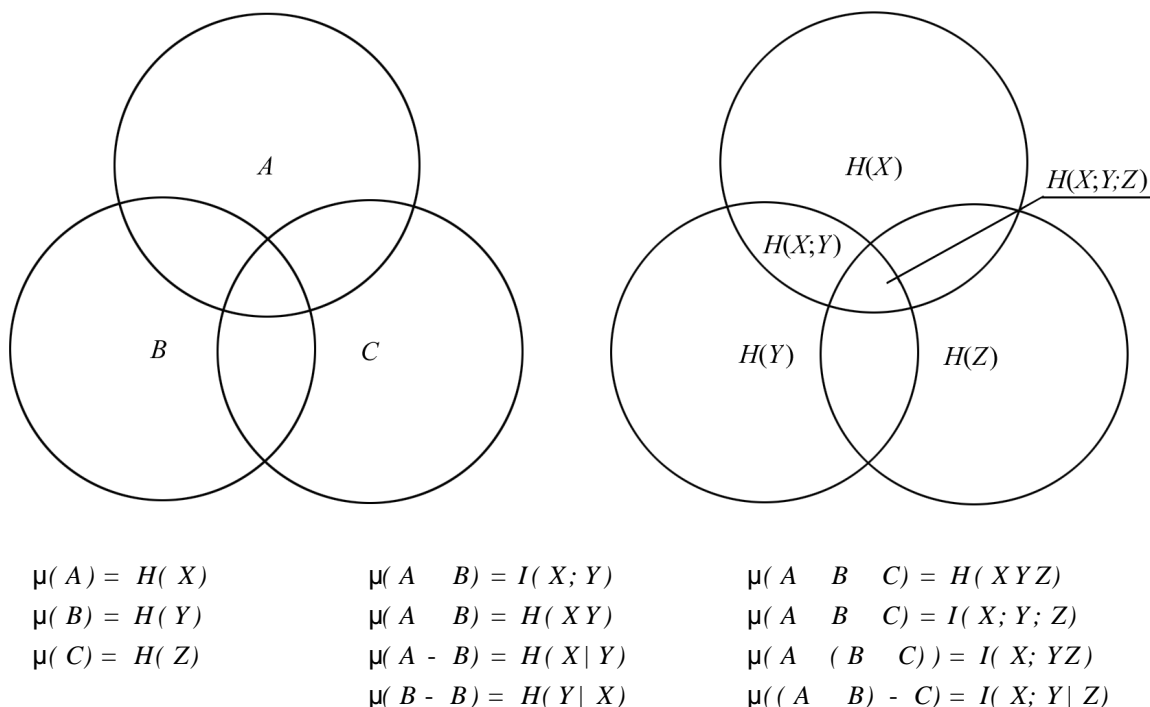


图 2.3 集合论与信息论公式对应关系的示意图

### 2.2.3 互信息函数的性质

两个变量之间的互信息在信息传输和处理中有着重要的应用,因此我们需要讨论该函数的性质。

根据互信息的定义可以知道,两个随机变量  $X$  和  $Y$  之间的互信息函数  $I(X; Y)$  为



$$I(X; Y) = \sum_{k=1}^K \sum_{j=1}^J p(a_k, b_j) \log \frac{p(a_k, b_j)}{p(a_k) p(b_j)}$$

由于

$$p(a_k) = \sum_{j=1}^J p(a_k, b_j)$$

$$p(b_j) = \sum_{k=1}^K p(a_k, b_j)$$

所以,  $I(X; Y)$  实际上是两个随机变量  $X$  和  $Y$  的联合分布密度矩阵  $(p(a_k, b_j))_{k,j}$  的函数。在实际应用中, 还可以将  $I(X; Y)$  的表达式写成

$$I(X; Y) = \sum_{k=1}^K \sum_{j=1}^J p(a_k) q(b_j | a_k) \log \frac{q(b_j | a_k)}{p(a_i) q(b_j | a_i)}$$

于是,  $I(X; Y)$  就成了随机变量  $X$  的概率矢量  $\mathbf{p} = (p(a_1), p(a_2), \dots, p(a_K))$  和条件概率矩阵  $\mathbf{Q} = (q(b_j | a_k))_{k,j}$  的函数, 可以记作  $I(\mathbf{p}, \mathbf{Q})$ 。互信息作为  $\mathbf{p}, \mathbf{Q}$  的函数, 具有凸函数的性质。

**性质 2.3** 互信息  $I(\mathbf{p}, \mathbf{Q})$  是  $\mathbf{p}$  的上凸函数。

**证明** 按凸函数的定义, 这就是要证明对 " $\mathbf{p}, \mathbf{p}' \in D$  及 " $0 \leq \lambda \leq 1$ , 有

$$I(\mathbf{p}, \mathbf{Q}) + (1 - \lambda) I(\mathbf{p}', \mathbf{Q}) \leq I(\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}', \mathbf{Q}) \quad (2.29)$$

由于  $\mathbf{p}, \mathbf{p}' \in D$ , 所以  $\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}' \in D$ , 并令  $\mathbf{p}_0 = \lambda \mathbf{p} + (1 - \lambda) \mathbf{p}'$ 。引入随机变量  $Z$ , 其密度矩阵为

$$P(z) = \begin{matrix} & d_1 & d_2 \\ \begin{matrix} Z \\ P(z) \end{matrix} & \lambda & 1 - \lambda \end{matrix}$$

并将  $Z, X, Y$  看成是如图 2.4 所示的输入与输出关系, 并假设  $X$  的概率分布由随机变量  $Z$  来控制, 即

$z = d_1$  时,  $X$  的概率分布为  $\mathbf{p} = \{p_1(a_k)\} = \{p_{x|z=d_1}(x = a_k | z = d_1)\}$

$z = d_2$  时,  $X$  的概率分布为  $\mathbf{p}' = \{p_2(a_k)\} = \{p_{x|z=d_2}(x = a_k | z = d_2)\}$

图 2.4  $Z, X$  与  $Y$  构成的输入与输出关系示意图

所以  $\mathbf{p}, \mathbf{p}'$  就成了  $Z$  取不同值时  $X$  取值的条件概率矢量。但是, 此时条件概率矩阵  $\mathbf{Q}$  与随机变量  $Z$  的取值无关, 于是有

$$I(\mathbf{p} + (1 - \alpha)\mathbf{p}, \mathbf{Q}) = I(\mathbf{p}, \mathbf{Q}) = I(X; Y)$$

而

$$\begin{aligned} & I(\mathbf{p}, \mathbf{Q}) + (1 - \alpha) I(\mathbf{p}, \mathbf{Q}) \\ &= p(d_1) I(\mathbf{p}, \mathbf{Q}) + p(d_2) I(\mathbf{p}, \mathbf{Q}) \\ &= p(d_1) I(X; Y | Z = d_1) + p(d_2) I(X; Y | Z = d_2) \\ &= I(X; Y | Z) \end{aligned}$$

由于  $Z$  与  $\mathbf{Q}$  无关, 所以在给定  $X$  的条件下,  $Z$  与  $Y$  统计独立, 即

$$I(Z; Y | X) = 0$$

根据  $I(X; Y; Z)$  的一组公式(2.27), 可以知道

$$I(X; Y) - I(X; Y | Z) = I(Z; Y) - I(Z; Y | X) = I(Z; Y)$$

又由互信息的非负性, 可以知道  $I(Z; Y) \geq 0$ , 所以

$$I(X; Y) \geq I(X; Y | Z)$$

即

$$I(\mathbf{p}, \mathbf{Q}) + (1 - \alpha) I(\mathbf{p}, \mathbf{Q}) \leq I(\mathbf{p} + (1 - \alpha)\mathbf{p}, \mathbf{Q}) \quad \text{证毕}$$

性质 2.4 互信息  $I(\mathbf{p}, \mathbf{Q})$  是  $\mathbf{Q}$  的下凸函数。

证明 按凸函数定义, 这就是要证明对任给的两个条件概率矩阵  $\mathbf{Q}$  和  $\mathbf{Q}$  及  $\alpha \in [0, 1]$ , 有

$$I(\mathbf{p}, \mathbf{Q}) + (1 - \alpha) I(\mathbf{p}, \mathbf{Q}) \leq I(\mathbf{p}, \alpha \mathbf{Q} + (1 - \alpha) \mathbf{Q}) \quad (2.30)$$

首先, 条件概率矩阵的特点是其元素满足关系式

$$\sum_{j=1}^J q(b_j | a_k) = 1, \quad k = 1, 2, \dots, K$$

故

$$\begin{aligned} & \sum_{j=1}^J [ \alpha q(b_j | a_k) + (1 - \alpha) q(b_j | a_k) ] \\ &= \sum_{j=1}^J \alpha q(b_j | a_k) + (1 - \alpha) \sum_{j=1}^J q(b_j | a_k) \\ &= \alpha + (1 - \alpha) = 1 \end{aligned}$$

所以, 对  $\alpha \in [0, 1]$ ,  $\mathbf{Q} \in D$ ,  $\mathbf{Q} \in D$ , 有  $\alpha \mathbf{Q} + (1 - \alpha) \mathbf{Q} \in D$ , 故条件概率矩阵组成的集合  $D$  是一个凸域。令  $\mathbf{Q} = \alpha \mathbf{Q} + (1 - \alpha) \mathbf{Q}$ 。

引入随机变量  $Z$ , 其密度矩阵为

$$P(z) = \begin{matrix} Z & d_1 & d_2 \\ & \alpha & 1 - \alpha \end{matrix}$$

设  $Z$  的取值与随机变量  $X$  无关, 只影响条件概率矩阵  $\mathbf{Q}$ , 即

当  $z = d_1$  时, 条件概率矩阵  $\mathbf{Q} = \mathbf{Q}_1$

当  $z = d_2$  时, 条件概率矩阵  $\mathbf{Q} = \mathbf{Q}_2$

于是

$$\begin{aligned} & I(\mathbf{p}, \mathbf{Q}_1) + (1 - \alpha) I(\mathbf{p}, \mathbf{Q}_2) \\ &= p(d_1) I(\mathbf{p}, \mathbf{Q}_1 / z = d_1) + p(d_2) I(\mathbf{p}, \mathbf{Q}_2 / z = d_2) \\ &= I(X; Y / Z) \end{aligned}$$

而

$$I(\mathbf{p}, \alpha \mathbf{Q}_1 + (1 - \alpha) \mathbf{Q}_2) = I(\mathbf{p}, \mathbf{Q}) = I(X; Y)$$

由于  $Z$  与  $X$  无关, 即  $I(X; Z) = 0$ , 则

$$\begin{aligned} I(X; Y; Z) &= I(X; Y) - I(X; Y / Z) \\ &= I(X; Z) - I(X; Z / Y) \\ &= -I(X; Z / Y) = 0 \end{aligned}$$

所以

$$I(X; Y / Z) = I(X; Y)$$

即

$$I(\mathbf{p}, \mathbf{Q}_1) + (1 - \alpha) I(\mathbf{p}, \mathbf{Q}_2) = I(\mathbf{p}, \alpha \mathbf{Q}_1 + (1 - \alpha) \mathbf{Q}_2) \quad \text{证毕}$$

## 2.3 连续随机变量下的熵与互信息

在研究离散随机变量下的熵与互信息后, 自然想到连续随机变量下的熵与互信息该如何表示? 因为在实际问题中经常遇到的是连续随机变量。在微积分中我们已熟悉如何把连续问题看成是某种函数问题的极限。但是, 从离散熵和互信息到连续熵和互信息不仅涉及到数学处理上的问题, 而且还涉及到熵和互信息本身的概念和含义。

### 2.3.1 连续随机变量下的微分熵

回顾离散随机变量  $X$  的熵为

$$H(X) = - \sum_{k=1}^K p(a_k) \log p(a_k)$$

根据该公式可以知道, 当随机变量为离散的, 且仅有有限个可能取值时, 熵肯定存在。当  $K \rightarrow \infty$  时, 则该级数和存在收敛性问题, 不一定存在极限。而当随机变

量取值为连续分布时,按离散熵概念推导过来的熵,此时必将趋于无穷,这一点不难证明。

设连续随机变量  $X$  的可能取值在整个实数域上,即  $x \in (-\infty, +\infty)$ , 其概率密度函数为  $p(x)$ 。若将  $X$  的值域分成间隔为  $\Delta x$  的小区间,则  $X$  的值在小区间  $(x_i, x_i + \Delta x)$  内的概率近似为  $p(x_i) \Delta x$ 。于是,熵的近似值为

$$H_{\Delta x}(X) = - \sum_{i=-\infty}^{+\infty} p(x_i) \Delta x \log(p(x_i) \Delta x)$$

当  $\Delta x \rightarrow 0$  时,有

$$\begin{aligned} \lim_{\Delta x \rightarrow 0} H_{\Delta x}(X) &= \lim_{\Delta x \rightarrow 0} - \sum_{i=-\infty}^{+\infty} p(x_i) \Delta x \log(p(x_i) \Delta x) \\ &= - \int_{-\infty}^{+\infty} p(x) \log p(x) dx - \lim_{\Delta x \rightarrow 0} \log \Delta x \int_{-\infty}^{+\infty} p(x) dx \\ &= - \int_{-\infty}^{+\infty} p(x) \log p(x) dx - \lim_{\Delta x \rightarrow 0} \log \Delta x \end{aligned}$$

可以看出,当  $\Delta x \rightarrow 0$  时,上式中的后一项极限值为无穷大。因此,按照离散熵的概念,连续随机变量的熵应为无穷大,失去意义。但上式中的第一项仍存在一定的意义和价值,在历史上曾一再被利用。

1866年,玻耳兹曼用力学观点研究麦克斯韦分布的唯一性时,得到了分布函数随时间变化的玻耳兹曼方程式,并定义了物理量  $E$  为

$$E = - \int_{-\infty}^{+\infty} f(x, t) \log f(x, t) dx$$

其中  $f(x, t)$  是单原子分子气体中原子速度的分布函数。玻耳兹曼证明物理量  $E$  对时间的导数决不为正。这就是著名的  $H$  定理。由  $H$  定理可以知道,气体向平衡分布接近时,熵不断增大。

1948年,维纳在其《控制论》一书中定义

$$H = - \int_{-\infty}^{+\infty} f(x) \log f(x) dx$$

为信息量,其中  $f(x)$  为概率密度函数。维纳认为“这是在通常情况下定义为熵的那个量的负数。虽然这个定义是个统计学上的定义,而且能替代 R. A. Fisher 统计方法中的定义,但与 Fisher 定义不同。”

1948年,香农在他的论文中直接定义连续分布随机变量的熵为

$$h(X) = - \int_{-\infty}^{+\infty} p(x) \log p(x) dx$$

该定义现在已被广泛接受。为了区别该定义量与(离散)熵的定义,我们称其为

“微分熵”。

连续分布随机变量  $X$  的微分熵定义为

$$h(X) = - \int_{-\infty}^{+\infty} p(x) \log p(x) dx \quad (2.31)$$

其中  $p(x)$  为  $X$  的概率密度函数。

应该说,连续分布随机变量的微分熵与离散随机变量的熵在概念上是不同的。前者去掉了无穷大项,而仅保留有限值的那一项。尽管如此,微分熵仍可以作为连续分布随机变量的不确定程度的一种相对量度。因为在实际应用中,数据都只有有限精度,在同样的精度下,连续随机变量的熵  $H(X)$  中的第二项  $\log x$  取相同的值,因此微分熵可以作为连续随机变量不确定程度的相对量度。

微分熵的概念可以推广到多个随机变量。以两个连续随机变量  $X$  和  $Y$  的情况为例,设它们的概率密度函数分别为  $p(x)$ ,  $p(y)$ , 其联合概率密度函数为  $p(x, y)$ , 条件概率密度函数分别为  $q(y|x)$ ,  $q(x|y)$  则连续随机变量  $X$  和  $Y$  的联合微分熵  $h(XY)$  定义为

$$h(XY) = - \int p(x, y) \log p(x, y) dx dy \quad (2.32)$$

连续随机变量  $X$  和  $Y$  的条件微分熵  $h(X|Y)$  定义为

$$\begin{aligned} h(X|Y) &= - \int p(x, y) \log p(x|y) dx dy \\ &= - \int p(y) dy \int p(x|y) \log p(x|y) dx \end{aligned} \quad (2.33)$$

显然,多个随机变量下的这些微分熵作为不确定程度的量度也都仅有相对的意义。

多个随机变量下离散熵之间的一些关系式在连续随机变量下仍然成立,例如

$$h(XY) = h(X) + h(Y|X) = h(Y) + h(X|Y) \quad (2.34a)$$

$$h(X|Y) \leq h(X), h(Y|X) \leq h(Y) \quad (2.34b)$$

$$h(XY) \geq h(X) + h(Y) \quad (2.34c)$$

这些关系式的证明与离散熵时相似,此处不再赘述。

## 2.3.2 随机变量函数的微分熵

随机变量经变换后可以得到新的随机变量,如何求变换后的随机变量的熵

或微分熵是一个理论上和实际中都有意义的问题。

对于离散随机变量而言,经变换后其离散熵值一般保持不变。但对于连续随机变量,变换后的微分熵值一般都有变化。

设有连续随机向量  $(X, Y)$ , 其联合分布密度函数为  $p(x, y)$ , 边缘分布密度函数分别为  $p(x)$ ,  $p(y)$ 。 $(X, Y)$  经变换

$$U = u(X, Y)$$

$$V = v(X, Y)$$

后,得到新的随机向量  $(U, V)$ , 其联合分布密度函数为  $p(u, v)$ , 边缘分布密度函数分别为  $p(u)$ ,  $p(v)$ 。变换前后的随机向量的关系如下所示:

$$(X, Y) \xrightarrow[u(X, Y)]{u(X, Y)} (U, V)$$

$$\text{取值} \begin{matrix} (x, y) \\ (u, v) \end{matrix}$$

由概率论可以知道,若变换  $u(X, Y)$ ,  $v(X, Y)$  各存在唯一的反变换,且正、反变换函数均连续,并有连续的偏导数,即

$$u = u(x, y) \quad x = x(u, v)$$

$$v = v(x, y) \quad y = y(u, v)$$

则可以由  $p(x, y)$  求出  $p(u, v)$  为

$$p(u, v) = p(x, y) \left| J \frac{x, y}{u, v} \right| \quad (2.35)$$

其中  $J$  为雅可比行列式

$$J \frac{x, y}{u, v} = \begin{vmatrix} \frac{\partial x}{\partial u} & \frac{\partial x}{\partial v} \\ \frac{\partial y}{\partial u} & \frac{\partial y}{\partial v} \end{vmatrix}$$

且

$$J \frac{x, y}{u, v} = \frac{1}{J \frac{u, v}{x, y}}$$

于是变换后,  $U$  和  $V$  的联合微分熵为

$$h(UV) = - \int \int p(u, v) \log p(u, v) du dv$$

$$= - \int \int p(x, y) \left| J \frac{x, y}{u, v} \right| \log p(x, y) \left| J \frac{x, y}{u, v} \right| du dv$$

考虑到

$$du dv = \left| J \frac{u, v}{x, y} \right| dx dy$$

用  $J$  表示  $J \frac{x, y}{u, v}$ , 则有

$$h(UV) = - \int p(x, y) \log p(x, y) dx dy - \int p(x, y) \log |J| dx dy$$

故

$$h(UV) = h(XY) - \int p(x, y) \log |J| dx dy \quad (2.36)$$

若变换是线性的, 即

$$\begin{pmatrix} U \\ V \end{pmatrix} = \mathbf{A} \begin{pmatrix} X \\ Y \end{pmatrix}$$

其中  $\mathbf{A}$  为线性变换矩阵。于是该条件下的雅可比行列式为常数, 即

$$J \frac{x, y}{u, v} = \frac{1}{\det \mathbf{A}} = \det \mathbf{A}^{-1}$$

其中  $\det \mathbf{A}$  表示  $\mathbf{A}$  的行列式值。于是

$$h(UV) = h(XY) - \log |\det \mathbf{A}^{-1}| = h(XY) + \log |\det \mathbf{A}| \quad (2.37)$$

若变换不仅是线性变换, 且仅有平移和旋转, 则有

$$\det \mathbf{A} = 1$$

于是

$$h(UV) = h(XY)$$

由于微分熵仅在非常特殊的变换下才具有不变性, 使得微分熵独立应用的价值受到极大限制。

### 2.3.3 连续随机变量下的互信息

对于连续随机变量之间的互信息, 可以按照离散互信息的概念进行推广。

设有两个连续分布的随机变量  $X$  和  $Y$ , 其联合概率密度函数为  $p(x, y)$ , 边缘分布密度函数分别为  $p(x)$  和  $p(y)$ , 则连续随机变量  $X$  和  $Y$  的互信息为

$$I(X; Y) = \lim_{\substack{x \rightarrow 0 \\ y \rightarrow 0}} \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} p(x_i, y_j) \log \frac{p(x_i, y_j)}{p(x_i) p(y_j)}$$

其中,  $p(x_i, y_j)$ ,  $p(x_i)$ ,  $p(y_j)$  分别是相应量化区间中所对应的概率密度函数的中值。

当取极限时,有

$$I(X; Y) = \int \int p(x, y) \log \frac{p(x, y)}{p(x)p(y)} dx dy \quad (2.38)$$

这就是两个连续分布的随机变量之间的互信息的表达式。

连续随机变量的互信息表示了随机变量之间相互提供的信息量,故有

$$I(X; Y) = I(Y; X)$$

该互信息还表示了随机变量之间统计依存程度的信息量度。

可以看到,连续随机变量的互信息的概念在从离散推广到连续时不存在数学上的困难,其原因可以这样来理解:

(1) 互信息的概念从根本上讲具有相对意义,其数学表达式中对数的宗量即是一个比值量。

(2) 在求连续随机变量的互信息的过程中,连续随机变量的熵中趋于无穷的那一项在这里被抵消了,即

$$\begin{aligned} I(X; Y) &= \lim_{x \rightarrow 0} [h(X) - \log x - h(X/Y) + \log x] \\ &= h(X) - h(X/Y) \end{aligned}$$

或

$$\begin{aligned} I(X; Y) &= \lim_{x \rightarrow 0, y \rightarrow 0} [h(X) - \log x + h(Y) - \log y - h(XY) + \log x + \log y] \\ &= h(X) + h(Y) - h(XY) \end{aligned}$$

当然,从数学上讲,上述阐述是不严格的。严格定义连续随机变量的互信息应该如下:

连续随机变量  $X$  和  $Y$  的互信息  $I(X; Y)$  为

$$I(X; Y) = \sup I([X]; [Y]) \quad (2.39)$$

其中,  $[X], [Y]$  是对应于  $X, Y$  的离散随机变量,且  $[X]$  满足

$$P\{[X] = i\} = P\{X \in S_i\} = \int_{S_i} dF(x)$$

这里,  $S_i (i = 1, 2, \dots)$  是  $X$  所取值域的一个有限分割,且  $S_i \cap S_j = \emptyset (i \neq j)$ ,  $\bigcup_i S_i = X$  的全部值域,  $F(X)$  是  $X$  的分布函数。 $[Y]$  满足的关系式类似于  $[X]$ 。

按照这一定义式,在一般情况下连续随机变量之间总存在有限的互信息。这点与熵不同。

对于多个连续随机变量下的互信息,我们也可以得到与离散互信息时完全相似的表达式和关系式,例如

$$I(X; YZ) = h(X) - h(X/YZ)$$



$$I(X; Y | Z) = h(X | Z) - h(X | YZ)$$

等等。

## 2.4 鉴别信息

鉴别信息的概念是在 20 世纪 50 年代由 I. J. Good, L. J. Savage 和 S. Kullback 等发展起来的。1959 年, Kullback 以著作的形式系统地阐述了这一概念。70 年代末, J. E. Shore 和 R. W. Johnson 的工作使鉴别信息在信号处理中的应用得到了很大的推广, 从而使得鉴别信息这一概念的重要性得到了普遍承认, 成为现代信息论重要而不可分割的一部分。

鉴别信息(discrimination information)一词来自 Kullback, 现在有些文献中又称它为交叉熵(cross-entropy)、Kullback 熵(Kullback entropy)、相对熵(relative entropy)、方向散度(directed divergence)、K-L 数等。我们在这里采用 Kullback 最早取的名称。

### 2.4.1 鉴别信息的定义

#### (1) 离散随机变量的情形

设随机变量  $X$  的可能取值为  $\{a_1, a_2, \dots, a_K\}$ , 且  $X$  的概率分布情况与假设  $H_1$  和  $H_2$  有关, 即在假设  $H_1$  下,  $X$  的概率分布为

$$P_1(x) = \begin{matrix} X & a_1 & a_2 & \dots & a_K \\ p_1(a_1) & p_1(a_2) & \dots & p_1(a_K) \end{matrix}$$

在假设  $H_2$  下,  $X$  的概率分布为

$$P_2(x) = \begin{matrix} X & a_1 & a_2 & \dots & a_K \\ p_2(a_1) & p_2(a_2) & \dots & p_2(a_K) \end{matrix}$$

另外, 假设  $H_1$  和  $H_2$  成立的概率分别为  $p(H_1)$  和  $p(H_2)$ , 则根据条件概率公式及全概率公式, 有

$$p(H_1 | a_k) = \frac{p(H_1) p_1(a_k)}{p(H_1) p_1(a_k) + p(H_2) p_2(a_k)} \quad (2.40a)$$

$$p(H_2 | a_k) = \frac{p(H_2) p_2(a_k)}{p(H_1) p_1(a_k) + p(H_2) p_2(a_k)} \quad (2.40b)$$

其中,  $p_1(a_k) = p(a_k | H_1)$ ,  $p_2(a_k) = p(a_k | H_2)$ ; 而  $p(H_1 | a_k)$  和  $p(H_2 | a_k)$  分别是

$X$  取  $a_k$  的条件下, 假设  $H_1$  和  $H_2$  成立的条件概率。

由式(2.40a)和式(2.40b), 可以知道

$$\log \frac{p_2(a_k)}{p_1(a_k)} = \log \frac{p(H_2/a_k)}{p(H_1/a_k)} - \log \frac{p(H_2)}{p(H_1)} \quad (2.41)$$

上式右边第一项是已知  $X$  取  $a_k$  时, 假设  $H_2$  和  $H_1$  的对数似然比, 右边第二项是未知  $X$  取  $a_k$  时, 假设  $H_2$  和  $H_1$  的对数似然比。可以看出, 对数似然比

$\log \frac{p_2(a_k)}{p_1(a_k)}$  刚好等于随机变量  $X$  在取  $a_k$  前后假设  $H_2$  和  $H_1$  的对数似然比之差。

我们定义  $\log \frac{p_2(a_k)}{p_1(a_k)}$  为随机变量  $X$  取  $a_k$  时所提供的在鉴别假设  $H_1$  和  $H_2$  时倾向于  $H_2$  的信息。

可以看出, 对数似然比  $\log \frac{p_2(a_k)}{p_1(a_k)}$  所给出的信息量可正可负。但是, 为避免出现除数为零的情况, 必须假定所有概率恒为正, 当然, 该正值可以任意小, 这种假定不会给研究工作带来多大损失。

对数似然比  $\log \frac{p_2(a_k)}{p_1(a_k)}$  在假设  $H_2$  下的数学期望就称为鉴别信息, 记作  $I(p_2, p_1; X)$ , 即

$$I(p_2, p_1; X) = \sum_{k=1}^K p_2(a_k) \log \frac{p_2(a_k)}{p_1(a_k)} \quad (2.42)$$

在不需要指明随机变量的情况下, 鉴别信息  $I(p_2, p_1; X)$  一般简记作  $I(p_2, p_1)$ 。

鉴别信息  $I(p_2, p_1)$  是为鉴别  $H_2$  和  $H_1$  而对随机变量  $X$  在  $H_2$  假设的分布下进行观察所平均得到的倾向于  $H_2$  的信息量。也可以理解为: 观察者对随机变量  $X$  的了解由分布  $p_1(x)$  和  $p_2(x)$  时所获得的信息量, 此时  $p_1(x)$  相当于先验概率分布,  $p_2(x)$  则是观察后所得到的后验概率分布。

注意, 鉴别信息  $I(p_2, p_1)$  是有方向的, 故又叫做方向散度, 因为在一般情况下,  $I(p_2, p_1) \neq I(p_1, p_2)$ 。

在此基础上, 我们可以定义两个概率分布之间的散度 (divergence)  $J(p_2, p_1; X)$  为

$$J(p_2, p_1; X) = I(p_2, p_1; X) + I(p_1, p_2; X) \quad (2.43)$$

在不指明随机变量  $X$  而不会引起混淆的情况下,  $J(p_2, p_1; X)$  也可以简记为  $J(p_2, p_1)$ 。

散度  $J(p_2, p_1)$  是对两个概率分布之间的差别的一种量度, 它具有以下 3 个

性质:

$J(p_2, p_1)$  是无方向性的, 对其两个概率分布是对称的, 即  $J(p_1, p_2) = J(p_2, p_1)$

$$J(p_2, p_1) \geq 0$$

$$J(p_2, p_1) = 0 \quad p_2 = p_1$$

但  $J(\cdot, \cdot)$  不满足三角不等式

$$J(p_2, p_1) \leq J(p_2, p_0) + J(p_0, p_1)$$

所以, 除三角不等式以外,  $J(p_2, p_1)$  具有一个距离所具有的其他 3 个性质。

## (2) 连续随机变量的情形

设有连续随机变量  $X$ , 其概率分布密度函数与假设  $H_1, H_2$  有关, 即在假设  $H_1$  下,  $X$  的概率密度函数为  $p_1(x)$ ; 在假设  $H_2$  下,  $X$  的概率密度函数为  $p_2(x)$ 。仿照离散随机变量时的情形, 可以有

$$\log \frac{p_2(x)}{p_1(x)} = \log \frac{p(H_2 | x)}{p(H_1 | x)} - \log \frac{p(H_2)}{p(H_1)} \quad (2.44)$$

其中,  $p(H_2 | x)$  和  $p(H_1 | x)$  分别是  $X$  取  $x$  的条件下, 假设  $H_2$  和  $H_1$  的条件概率。

对数似然比  $\log \frac{p_2(x)}{p_1(x)}$  在假设  $H_2$  下的数学期望定义为连续随机变量下的鉴别信息, 记作  $I(p_2, p_1; X)$ , 即

$$I(p_2, p_1; X) = \int p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \quad (2.45)$$

连续随机变量下的鉴别信息的含义与离散随机变量下的鉴别信息相同。对鉴别信息而言, 它在离散和连续两种随机变量的情况下的形式完全相似, 且含义相同。这正是鉴别信息优越于熵的方面。后面将介绍这两者的关系。

## (3) 多个随机变量的情形

与香农理论中的联合熵和条件熵类似, 我们可以定义联合鉴别信息和条件鉴别信息。我们以离散随机变量为例, 连续随机变量则与此类似。

设有两个离散随机变量  $X, Y$ , 其取值分别为

$$X: \{a_1, a_2, \dots, a_K\}$$

$$Y: \{b_1, b_2, \dots, b_J\}$$

$X, Y$  的联合概率分布在假设  $H_1$  下为  $p_1(a_k, b_j) = g_1(a_k) q_1(b_j | a_k)$ , 在假设  $H_2$  下为  $p_2(a_k, b_j) = g_2(a_k) q_2(b_j | a_k)$ , 其中,  $k = 1, 2, \dots, K$ ,  $j = 1, 2, \dots, J$ 。则定义随机变量  $X$  和  $Y$  的联合鉴别信息为

$$I(p_2, p_1; XY) = \sum_{k=1}^K \sum_{j=1}^J p_2(a_k, b_j) \log \frac{p_2(a_k, b_j)}{p_1(a_k, b_j)} \quad (2.46)$$

对式(2.46)进行展开,可以得到

$$I(p_2, p_1; XY) = \sum_{k=1}^K g_2(a_k) \log \frac{g_2(a_k)}{g_1(a_k)} + \sum_{k=1}^K g_2(a_k) \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{q_1(b_j | a_k)}$$

上式第一项等于  $I(g_2, g_1; X)$ , 第二项等于  $I(q, q; Y | X)$ , 其中  $\sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{q_1(b_j | a_k)}$  等于  $I(q, q; Y | X = a_k)$ , 我们称  $I(q, q; Y | X = a_k)$  为  $X = a_k$  条件下的条件鉴别信息, 即

$$I(q, q; Y | X = a_k) = \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{q_1(b_j | a_k)} \quad (2.47)$$

我们称  $I(q, q; Y | X)$  为平均条件鉴别信息, 它是  $X = a_k$  条件下的条件鉴别信息的数学期望, 即

$$I(q, q; Y | X) = \sum_{k=1}^K g_2(a_k) \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{q_1(b_j | a_k)} \quad (2.48)$$

于是可以得到联合鉴别信息与条件鉴别信息之间的关系式

$$I(p_2, p_1; XY) = I(g_2, g_1; X) + I(q, q; Y | X) \quad (2.49)$$

注意此时鉴别信息中必须指明随机变量。

与离散随机变量的情形相似, 我们可给出连续随机变量  $X, Y$  下联合鉴别信息和条件鉴别信息的定义及其关系式

$$I(p_2, p_1; XY) = \int p_2(x, y) \log \frac{p_2(x, y)}{p_1(x, y)} dx dy \quad (2.50)$$

$$I(q, q; Y | X) = \int g_2(x) q(y | x) \log \frac{q(y | x)}{q_1(y | x)} dx dy \quad (2.51)$$

$$I(p_2, p_1; XY) = I(g_2, g_1; X) + I(q, q; Y | X) \quad (2.52)$$

联合鉴别信息中随机变量  $X$  和  $Y$  的位置是对称的, 所以也可以有

$$I(p_2, p_1; XY) = I(g_2, g_1; Y) + I(q, q; X | Y)$$

但需注意此式中的  $g_2, g_1$  和  $q, q_1$  分别是  $Y$  的概率密度和  $X$  的条件概率密度。

## 2.4.2 Kullback 与香农两种信息量度之间的关系

### (1) 鉴别信息与香农熵的关系

香农首先定义的是不确定性的量度——熵, 然后利用熵得到信息的量度。

也就是说, 观察者通过试验消除或减少随机变量取值的不确定性, 从而使熵减少, 随机变量熵的减少量即等于观察者获得的信息量

信息量 = 熵的减少量

Kullback 首先定义的是鉴别信息, 然后利用鉴别信息得到不确定性的量度。具体讨论如下。

设离散随机变量  $X$  的先验概率分布为

$$\begin{array}{ccccccc} X & & a_1 & & a_2 & & \dots & & a_K \\ P_0(x) & = & p_0(a_1) & & p_0(a_2) & & \dots & & p_0(a_K) \end{array}$$

经过试验后,  $X$  的概率分布为  $P(x)$ , 此时观察者所获得的鉴别信息为  $I(p, p_0)$ 。假如观察者通过试验所可能获得的最大鉴别信息为  $I(p_m, p_0)$ , 则二者的差值

$$I(p_m, p_0) - I(p, p_0)$$

表示我们尚未获得的信息, 这个未获得的信息就是  $X$  的概率分布  $P(x)$  中所蕴含的不确定性。若记概率分布  $P(X)$  的不确定性为  $U(\mathbf{p})$ , 则有

$$U(\mathbf{p}) = I(p_m, p_0) - I(p, p_0) \quad (2.53)$$

此即 Kullback 的不确定性的量度, 它表示了随机变量  $X$  在概率分布为  $P(x)$  时的不确定程度。

同样, 对连续随机变量  $X$  而言, 其概率密度为  $p(x)$  时的不确定性量度为

$$\begin{aligned} U(p) &= \int p_m(x) \log \frac{p_m(x)}{p_0(x)} dx - \int p(x) \log \frac{p(x)}{p_0(x)} dx \\ &= I(p_m, p_0) - I(p, p_0) \end{aligned}$$

Kullback 的这一不确定性量度与香农不确定性量度形式不同, 但有联系。

对离散随机变量而言, 若  $X$  的先验概率分布为

$$p_0(a_k) = \frac{1}{K}, \quad k = 1, 2, \dots, K$$

而  $p_m$  对应完全确定的概率分布, 即

$$p_m(a_k) = \begin{cases} 1, & k = j \\ 0, & k \neq j, \quad j = 1, 2, \dots, K \end{cases}$$

则

$$\begin{aligned} U(\mathbf{p}) &= I(p_m, p_0) - I(p, p_0) \\ &= \sum_{k=1}^K p_m(a_k) \log \frac{p_m(a_k)}{1/K} - \sum_{k=1}^K p(a_k) \log \frac{p(a_k)}{1/K} \\ &= \sum_{k=1}^K p_m(a_k) \log p_m(a_k) + \sum_{k=1}^K p_m(a_k) \log K \end{aligned}$$

$$\begin{aligned}
 & - \sum_{k=1}^K p(a_k) \log p(a_k) - \sum_{k=1}^K p(a_k) \log K \\
 & = - \sum_{k=1}^K p(a_k) \log p(a_k) \\
 & = H(\mathbf{p})
 \end{aligned}$$

因此,在上述特定的先验概率分布  $p_0$  和  $p_m$  的条件下, Kullback 的不确定性量度  $U(\mathbf{p})$  等于香农熵  $H(\mathbf{p})$ 。

对连续随机变量而言,若  $X$  的取值范围为  $[a, b]$ , 其先验概率密度为

$$p_0(x) = \frac{1}{b-a}$$

而  $p_m(x)$  为

$$p_m(x) = \frac{(x)}{L}$$

其中,  $(x)$  取 0 或者 1, 且  $\int_a^b (x) dx = \int_a^b (x) dx = L$ , 则有

$$\begin{aligned}
 U(p) &= \int_a^b p_m(x) \log \frac{p_m(x)}{1/(b-a)} dx - \int_a^b p(x) \log \frac{p(x)}{1/(b-a)} dx \\
 &= \int_a^b p_m(x) \log p_m(x) dx + \int_a^b p_m(x) \log(b-a) dx \\
 &\quad - \int_a^b p(x) \log p(x) dx - \int_a^b p(x) \log(b-a) dx \\
 &= \int_a^b \frac{(x)}{L} \log \frac{(x)}{L} dx - \int_a^b p(x) \log p(x) dx \\
 &= \int_a^b \frac{(x)}{L} \log (x) dx - \int_a^b \frac{(x)}{L} \log L dx - \int_a^b p(x) \log p(x) dx
 \end{aligned}$$

所以

$$U(p) = - \int_a^b p(x) \log(Lp(x)) dx \quad (2.54)$$

可以看出,在特定的概率分布下, Kullback 对连续随机变量的不确定性量度类似于微分熵,但存在以下的重大区别:

$U(p)$  没有量纲上的问题,由于  $p(x)$  是概率密度,所以  $Lp(x)$  是没有量纲的量。

$L \rightarrow 0$  时,  $U(p) \rightarrow \infty$ , 这是合理的,因为  $L \rightarrow 0$  时,  $X$  取值的精度将无限地提高。这样,从  $p(x)$  改变到无限精确的取值就需要无穷大的信息量,所以分布密度  $p(x)$  可以有无穷大的不确定性。

综上所述, 香农熵可以看成是 Kullback 不确定性量度的一个特例, 而且 Kullback 不确定性量度在连续随机变量下也没有量纲上的问题, 可以很直接地说明为什么连续随机变量的不确定性会趋于无穷。因此, 从理论上讲, 鉴别信息的定义比香农熵的定义有更普遍的意义。

鉴别信息与香农离散熵的关系还可以通过下面的分析得到。

按照鉴别信息的最初定义, 有对数似然比

$$\log \frac{p_1(x)}{p_0(x)} = \log \frac{p(H_1/x)}{p(H_0/x)} - \log \frac{p(H_1)}{p(H_0)}$$

它表示  $X=x$  时所提供的倾向于  $H_1$  假设的信息量。

假设  $H_0 = \{H_1, H_2, \dots, H_K\}$  是由  $K$  个互不相容的假设  $H_k, k=1, 2, \dots, K$  组成的一个集合, 故假设  $H_0$  为必然事件。  $X$  为随机变量, 其分布列为

$$\begin{array}{ccccccc} X & & a_1 & & a_2 & & \dots & & a_K \\ P(x) & = & p(a_1) & & p(a_2) & & \dots & & p(a_K) \end{array}$$

观察  $X$  的取值, 可唯一地确定何假设为真, 即

$$\begin{aligned} p(H_k/a_k) &= 1, \quad k=1, 2, \dots, K \\ p(H_0) &= 1 \end{aligned}$$

代入对数似然比中, 有

$$\log \frac{p_1(a_k)}{p_0(a_k)} = \log \frac{p(H_1/a_k)}{p(H_0/a_k)} - \log \frac{p(H_1)}{p(H_0)}$$

当  $a_k = a_1$  时, 有

$$\log \frac{p_1(a_1)}{p_0(a_1)} = \log \frac{1}{1} - \log \frac{p(H_1)}{1} = -\log p(H_1)$$

此即  $X=a_1$  时所提供的倾向于假设  $H_1$  的信息量, 即  $X$  取  $a_1$  所提供的信息量。

以此类推,  $X=a_k$  时所提供的信息量为

$$\log \frac{p_k(a_k)}{p_0(a_k)} = -\log p(H_k)$$

于是, 对  $X$  的观察所得的平均信息量为

$$-\sum_{k=1}^K p(a_k) \log p(H_k) = -\sum_{k=1}^K p(a_k) \log p(a_k)$$

此值即等于离散随机变量  $X$  的熵。

## (2) 从鉴别信息到互信息

互信息对离散和连续随机变量的定义是一致的, 因此我们以连续随机变量为例。

两个连续随机变量  $X$  和  $Y$  的鉴别信息为

$$I(p_2, p_1; XY) = \int p_2(x, y) \log \frac{p_2(x, y)}{p_1(x, y)} dx dy$$

现设在假设  $H_1$  下,  $X$  和  $Y$  互相独立, 其联合概率密度函数为

$$p_1(x, y) = g(x)h(y)$$

又设在假设  $H_2$  下,  $X$  和  $Y$  不独立, 但联合概率密度函数满足条件

$$p_2(x, y) dx = h(y)$$

$$p_2(x, y) dy = g(x)$$

则此时的鉴别信息为

$$I(p_2, p_1; XY) = \int p_2(x, y) \log \frac{p_2(x, y)}{g(x)h(y)} dx dy$$

此即两个连续随机变量的互信息。这说明, 当  $X$  和  $Y$  的联合概率分布由独立变为不独立时, 所得到的鉴别信息即等于  $X$  和  $Y$  不独立时香农定义意义下的互信息。

鉴别信息不仅与香农定义的信息有着密切的关系, 而且与 R. A. Fisher 在 1925 年所定义的 Fisher 信息有密切的关系。有兴趣的读者可以参阅 Kullback 的有关著作。

### 2.4.3 鉴别信息的性质

鉴别信息具有作为一个信息的量度所应具有很多性质, 其中主要的性质如下。

#### 2.4.3.1 非负性

**性质 2.5** 鉴别信息是非负的, 当且仅当两个概率分布相等时鉴别信息才等于零。

**证明** 这一性质在离散和连续随机变量下都成立。这里只给出离散随机变量下的证明。

利用不等式  $\ln x \leq x - 1$  或  $\ln x \geq x - 1$  (当且仅当  $x = 1$  时等号成立), 则有

$$I(p_2, p_1; X) = \sum_{k=1}^K p_2(a_k) \log \frac{p_2(a_k)}{p_1(a_k)}$$



$$\sum_{k=1}^K p_2(a_k) - 1 - \frac{p_1(a_k)}{p_2(a_k)} = 0$$

当且仅当  $p_1(a_k) = p_2(a_k) \quad (k=1, 2, \dots, K)$  时等式成立。

证毕

## 2.4.3.2 凸性

性质 2.6 离散随机变量下的鉴别信息是其宗量的下凸函数, 即 "

$$I(p_2 + (1 - \alpha)p_1, p_1) \leq \alpha I(p_2, p_1) + (1 - \alpha)I(p_1, p_1) \quad (2.55a)$$

及

$$I(p_2, p_1 + (1 - \alpha)p_1) \leq \alpha I(p_2, p_1) + (1 - \alpha)I(p_2, p_1) \quad (2.55b)$$

其中,  $p_1, p_1, p_1$  分别表示概率分布  $\{p_1(a_k)\}, \{p_1(a_k)\}, \{p_1(a_k)\}$ ;  $p_2, p_2, p_2$  分别表示概率分布  $\{p_2(a_k)\}, \{p_2(a_k)\}, \{p_2(a_k)\}$ ;  $p_1 + (1 - \alpha)p_1$  表示概率分布  $\{p_1(a_k) + (1 - \alpha)p_1(a_k)\}$ ;  $p_2 + (1 - \alpha)p_2$  表示概率分布  $\{p_2(a_k) + (1 - \alpha)p_2(a_k)\}$ 。

证明 (1) 证明式(2.55a), 令  $\alpha = p_2 + (1 - \alpha)p_2$ , 则

$$\begin{aligned} I(p_2 + (1 - \alpha)p_1, p_1) &= I(p_2, p_1) - (1 - \alpha)I(p_2, p_1) \\ &= \sum_{k=1}^K p_2(a_k) \log \frac{p_2(a_k)}{p_2(a_k)} + (1 - \alpha) \sum_{k=1}^K p_2(a_k) \log \frac{p_2(a_k)}{p_2(a_k)} \\ &= \sum_{k=1}^K p_2(a_k) \frac{p_2(a_k)}{p_2(a_k)} - 1 + (1 - \alpha) \sum_{k=1}^K p_2(a_k) \frac{p_2(a_k)}{p_2(a_k)} - 1 \\ &= 0 \end{aligned}$$

(2) 证明式(2.55b), 由于  $\log x$  是上凸函数, 所以有

$$\log(p_1(a_k) + (1 - \alpha)p_1(a_k)) \geq \alpha \log p_1(a_k) + (1 - \alpha)\log p_1(a_k)$$

故

$$\begin{aligned} I(p_2, p_1 + (1 - \alpha)p_1) &= \sum_{k=1}^K p_2(a_k) \log p_2(a_k) - \sum_{k=1}^K p_2(a_k) \log(p_1(a_k) + (1 - \alpha)p_1(a_k)) \\ &= \sum_{k=1}^K p_2(a_k) \log p_2(a_k) - \sum_{k=1}^K p_2(a_k) \log p_1(a_k) \\ &\quad - (1 - \alpha) \sum_{k=1}^K p_2(a_k) \log p_1(a_k) \end{aligned}$$

$$= I(p_2, p_1) + (1 - )I(p_2, p_1) \quad \text{证毕}$$

在连续随机变量时, 鉴别信息的凸性如性质 2.7 所示。

**性质 2.7** 任给一连续随机变量  $X$ , 其概率密度函数为  $p(x)$ , 以及  $X$  值域中的一个非空子集  $E$ , 恒有

$$\int_E p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \leq p_2(E) \log \frac{p_2(E)}{p_1(E)} \quad (2.56)$$

其中,  $p_2(E) = \int_E p_2(x) dx$ ,  $p_1(E) = \int_E p_1(x) dx$ , 当且仅当

$$\frac{p_2(E)}{p_1(E)} = \frac{p_2(x)}{p_1(x)}$$

时等式成立。

**证明** (1) 当  $E$  为  $X$  的整个值域时, 有

$$p_1(E) = p_2(E) = 1$$

于是式(2.56)变为

$$\int p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \leq 0$$

由性质 2.5 可知, 该式是成立的。

(2) 当  $E$  为整个值域的真子集时, 对  $E$  上的概率密度函数进行归一化, 得

$$g_1(x) = \frac{p_1(x)}{p_1(E)}, \quad g_2(x) = \frac{p_2(x)}{p_2(E)}$$

由鉴别信息的非负性可以知道

$$\int_E g_2(x) \log \frac{g_2(x)}{g_1(x)} dx \geq 0$$

当且仅当  $g_1(x) = g_2(x)$  时取等号。代入  $g_1(x)$  和  $g_2(x)$  的表达式, 即得

$$\frac{1}{p_2(E)} \int_E p_2(x) \log \frac{p_2(x)}{p_1(x)} dx - \log \frac{p_2(E)}{p_1(E)} \geq 0$$

故有

$$\int_E p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \leq \int_E p_2(x) \log \frac{p_2(E)}{p_1(E)} dx = p_2(E) \log \frac{p_2(E)}{p_1(E)}$$

当且仅当  $g_1(x) = g_2(x)$ , 或  $\frac{p_2(x)}{p_1(x)} = \frac{p_2(E)}{p_1(E)}$  时等式成立。 证毕

进一步, 若将  $X$  的整个值域划分成  $N$  个两两互不相交的子集  $E_1, E_2, \dots, E_N$ , 则性质 2.7 可以表述为

$$I(p_2, p_1; X) = \int p_2(x) \log \frac{p_2(x)}{p_1(x)} dx$$

$$\begin{aligned}
&= \sum_{n=1}^N \int_{E_n} p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \\
&\quad \sum_{n=1}^N p_2(E_n) \log \frac{p_2(E_n)}{p_1(E_n)}
\end{aligned} \tag{2.57}$$

当且仅当  $\frac{p_2(x)}{p_1(x)} = \frac{p_2(E_n)}{p_1(E_n)}$  ( $x \in E_n, n=1, 2, \dots, N$ ) 时等式成立。

### 2.4.3.3 可加性

**性质 2.8** 多个随机变量的鉴别信息在各随机变量互相独立时等于各随机变量的鉴别信息之和。

**证明** 以只有两个连续随机变量的情况为例, 对多个随机变量时的证明方法相同。

设连续随机变量  $X$  和  $Y$  的联合概率密度函数为  $p(x, y)$ , 且满足

$$p_2(x, y) = g_2(x) h_2(y)$$

$$p_1(x, y) = g_1(x) h_1(y)$$

则

$$\begin{aligned}
I(p_2, p_1; XY) &= \int_{x, y} g_2(x) h_2(y) \log \frac{g_2(x) h_2(y)}{g_1(x) h_1(y)} dx dy \\
&= \int_{x, y} g_2(x) h_2(y) \log \frac{g_2(x)}{g_1(x)} dx dy + \int_{x, y} g_2(x) h_2(y) \log \frac{h_2(y)}{h_1(y)} dx dy \\
&= I(g_2, g_1; X) + I(h_2, h_1; Y)
\end{aligned} \tag{证毕}$$

下面我们讨论一下, 当随机变量的概率分布从  $p_0$  变为  $p_1$ , 又从  $p_1$  变为  $p_2$  时, 鉴别信息  $I(p_2, p_0)$  是否等于  $I(p_1, p_0) + I(p_2, p_1)$ ? 即分步可加性问题。

对香农定义的信息量度而言, 由  $p_0$  到  $p_1$  获得的信息量为  $I_s(p_1, p_0)$ , 即

$$H(p_0) - H(p_1) = I_s(p_1, p_0)$$

同理还可有

$$H(p_1) - H(p_2) = I_s(p_2, p_1)$$

$$H(p_0) - H(p_2) = I_s(p_2, p_0)$$

由此可得

$$I_s(p_2, p_0) = I_s(p_1, p_0) + I_s(p_2, p_1)$$

所以在香农的定义下, 由  $p_0$  到  $p_2$  一步获得的信息量与  $p_0$  分几步到达  $p_2$  所获得的总信息量是相等的, 即分步可加性成立。

但对 Kullback 定义的鉴别信息而言, 分步可加性却不一定成立。下面的例子说明了这一点。

**例 2.5** 掷色子, 设色子面朝上的点数用随机变量  $X$  来表示, 则  $X$  可能有以下几种概率分布

$$\mathbf{p} = \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}$$

$$\mathbf{p} = 0, \frac{1}{3}, 0, \frac{1}{3}, 0, \frac{1}{3}$$

$$\mathbf{p} = 0, 0, 0, \frac{1}{2}, 0, \frac{1}{2}$$

$$\mathbf{p} = 0, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}$$

对每种概率分布, 其香农熵分别为  $H(\mathbf{p}) = \log 6$ ,  $H(\mathbf{p}) = \log 3$ ,  $H(\mathbf{p}) = \log 2$ ,  $H(\mathbf{p}) = \log 5$ 。从而

$$I_s(p_1, p_0) = H(\mathbf{p}_0) - H(\mathbf{p}) = \log 2$$

$$I_s(p_2, p_1) = H(\mathbf{p}) - H(\mathbf{p}) = \log \frac{3}{2}$$

$$I_s(p_3, p_1) = H(\mathbf{p}) - H(\mathbf{p}) = \log \frac{3}{5}$$

于是

$$I_s(p_2, p_0) = H(\mathbf{p}_0) - H(\mathbf{p}) = \log 3 = I_s(p_1, p_0) + I_s(p_2, p_1)$$

$$I_s(p_3, p_0) = H(\mathbf{p}_0) - H(\mathbf{p}) = \log \frac{6}{5} = I_s(p_1, p_0) + I_s(p_3, p_1)$$

同样

$$I_s(p_3, p_0) = I_s(p_2, p_0) + I_s(p_3, p_2)$$

如果从香农熵的减少等于获得的信息量来理解上面的等式, 会发现实际上成立

$$I_s(p_3, p_2) < 0$$

$$I_s(p_3, p_1) < 0$$

这说明当概率分布从  $\mathbf{p}$  到  $\mathbf{p}$ ,  $\mathbf{p}$  到  $\mathbf{p}$  时, 试验者获得了负信息, 这是不合理的。

另一方面, 对 Kullback 定义的鉴别信息而言, 有

$$I(p_1, p_0) = \log 2, \quad I(p_2, p_1) = \log \frac{3}{2}$$

于是

$$I(p_2, p_0) = \log 3 = I(p_1, p_0) + I(p_2, p_1)$$

而  $I(p_3, p_1) = \quad$ , 即  $\mathbf{p} \quad \mathbf{p}$  不合理, 所以有

$$I(p_3, p_0) = \log \frac{6}{5} = I(p_1, p_0) + I(p_3, p_1)$$

因此, 虽然分步可加性对香农信息总是成立, 但并不合理。而对 Kullback 鉴别信息而言, 分步可加性不一定成立。只有对随机变量的了解逐步精确化时, Kullback 鉴别信息才具有分步可加性。所以这是合理的。

#### 2.4.3.4 不变性

前面已经讨论过, 离散随机变量经变换后, 其熵不变。而连续随机变量经变换后, 新随机变量的微分熵一般不等于原随机变量的微分熵。这是微分熵的缺点, 限制了它的应用。

对鉴别信息而言, 它仍保持不变性, 即连续随机变量经变换后, 新随机变量的鉴别信息在一定条件下保持不变。

**性质 2.9** 设随机变量  $X$  及可逆变换  $T$ , 有  $Y = T(X)$ , 则  $X$  的鉴别信息与相应  $Y$  的鉴别信息相等, 即

$$I(g_2, g_1; X) = I(h_2, h_1; Y)$$

其中,  $g_2(x), g_1(x)$  是  $X$  的概率密度函数,  $h_2(x), h_1(x)$  是相应  $Y$  的概率密度函数。

**证明** 根据概率论, 若函数  $f(y)$  是  $y$  的实函数, 则有

$$\int_E f(y) h_2(y) dy = \int_{T^{-1}(E)} f(T(x)) g_2(x) dx$$

其中  $E$  是  $y$  的取值域。因而有

$$\int_E h_2(y) \log \frac{h_2(y)}{h_1(y)} dy = \int_{T^{-1}(E)} g_2(x) \log \frac{h_2(T(x))}{h_1(T(x))} dx$$

根据随机变量变换前后概率密度函数的关系, 有

$$g_2(x) = h_2(T(x)) \frac{dy}{dx}$$

$$g_1(x) = h_1(T(x)) \frac{dy}{dx}$$

于是

$$\frac{h_2(T(x))}{h_1(T(x))} = \frac{g_2(x)}{g_1(x)}$$

代入前式, 即得

$$h_2(y) \log \frac{h_2(y)}{h_1(y)} dy = g_2(x) \log \frac{g_2(x)}{g_1(x)} dx$$

即

$$I(h_2, h_1; Y) = I(g_2, g_1; X) \quad \text{证毕}$$

性质 2.9 可以推广到随机矢量及其非奇异变换的情况, 此时变换的雅可比行列式代替了上述微分  $\frac{dy}{dx}$ 。

性质 2.5 至性质 2.9 表明, 鉴别信息可以对离散随机变量和连续随机变量给出统一的信息定义, 且具有人们对信息量度所期望的所有重要性质, 即非负性、凸性、可加性和变换下的不变性。

#### \* 2.4.4 鉴别信息函数形式的唯一性

弄清鉴别信息函数形式在什么样的条件下是唯一的, 对我们正确理解这一定义的意义和适用范围是很有好处的。

对于鉴别信息这一定义的唯一性, 历史上曾有很多人作过研究, 如 R. L. Kashyap, P. Kannappan 给出了最初的研究结果。而完整的阐述是由 R. W. Johnson 在 1979 年给出的。下面用定理形式表述这一结果。

**定理 2.3** 设  $F(p_2, p_1)$  是概率密度函数  $p_2(x), p_1(x)$  的泛函, 有

$$F(p_2, p_1) = \int f(p_2(x), p_1(x)) dx$$

若要求此泛函具有下述特性:

- (1) 有限性: 对任何概率密度函数  $p(x)$  恒有  $F(p, p) < \infty$ 。
- (2) 可加性: 设  $p_2(x, y) = g_2(x)h_2(y), p_1(x, y) = g_1(x)h_1(y)$ , 则有

$$F(p_2, p_1) = F(g_2, g_1) + F(h_2, h_1)$$

- (3) 半有界性: 设  $p_2(x) \geq p_1(x)$ , 则有  $F(p_2, p_1) \geq F(p_1, p_1)$ 。

则  $F(p_2, p_1)$  必取如下形式:

$$F(p_2, p_1) = B \int p_2(x) \log \frac{p_2(x)}{p_1(x)} dx + C \int p_1(x) \log \frac{p_1(x)}{p_2(x)} dx \quad (2.58)$$

其中,  $B, C$  为常数,  $B \geq 0, C \geq 0$ , 且  $B, C$  不同时为零。

为证明该定理, 先给出 4 个引理。

**引理 2.1** 设泛函  $F$  满足有限性和可加性, 取概率密度函数  $g_2(x)$  和

$g_1(x)$ , 满足  $F(g_2, g_1) < \frac{1}{2}$ , 则有

$$\int_{\mathbb{R}} f(g_2(x), g_1(x)) dx = \frac{1}{2} \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx \quad (2.59)$$

其中,  $\frac{1}{2}$  为常数, 且  $\frac{1}{2} > 0$ 。

证明 (1) 设有概率密度函数  $g_2(x)$ ,  $g_1(x)$  及  $h(y)$ , 其中  $h(y)$  除满足概率密度函数的条件外, 还满足

当  $0 \leq y \leq a$  时,  $h(y) = \frac{1}{a}$ , 且  $a < 1$

记  $A = [0, a]$ ,  $\bar{A}$  表示  $A$  的补集, 则有

$$\begin{aligned} & \int_{\mathbb{R}} \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx dy \\ &= \int_{\bar{A}} dy \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx + a \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx \end{aligned}$$

又由可加性, 有

$$\begin{aligned} & \int_{\mathbb{R}} \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx dy \\ &= \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx + \int_{\bar{A}} f(h(y), h(y)) dy + af(\frac{1}{2}, \frac{1}{2}) \end{aligned}$$

则

$$\begin{aligned} & \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx + \int_{\bar{A}} f(h(y), h(y)) dy + af(\frac{1}{2}, \frac{1}{2}) \\ &= \int_{\bar{A}} dy \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx + a \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx \quad (2.60) \end{aligned}$$

(2) 另取概率密度函数  $h(y)$ , 且  $h(y)$  满足

$$h(y) = \begin{cases} h(y), & y < 0 \\ \frac{1}{a}, & 0 \leq y \leq a \\ h(y + a - a'), & y > a \end{cases}$$

按照与第 1 步证明相同的推理, 可以得到

$$\begin{aligned} & \int_{A'} dy \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx + \frac{a}{2} \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx \\ &= \int_{\mathbb{R}} f(g_2(x), g_1(x)) dx + \int_{A'} f(h(y), h(y)) dy + \frac{a}{2} f(\frac{1}{2}, \frac{1}{2}) \end{aligned}$$

其中  $A' = [0, \frac{1}{2}]$ ,  $\overline{A'}$  表示  $A'$  的补集。

(3) 注意到有限性, 本引理中  $F(g_2, g_1) < \frac{1}{2}$  的假设, 以及

$$\int_{\bar{A}} dy \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx = \int_{A'} dy \int_{\mathbb{R}} f(g_2(x)h(y), g_1(x)h(y)) dx$$

和

$$\int_{\mathcal{A}} f(h(y), h(y)) dy = \int_{\mathcal{A}} f(h(y), h(y)) dy$$

即得

$$\begin{aligned} \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx &= \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx \\ &= \int_{\mathcal{A}} f(1, 1) - \int_{\mathcal{A}} f(1, 1) \end{aligned} \quad (2.61)$$

若令  $\mathcal{A} = 1$ , 则有

$$\int_{\mathcal{A}} f(g_2(x), g_1(x)) dx = \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx = f(1, 1) - \int_{\mathcal{A}} f(1, 1) \quad (2.62)$$

(4) 现取概率密度函数  $p_2(x)$  和  $p_1(x)$ , 使

$$p_2(x) = g_2(x), p_1(x) = g_1(x),$$

显然,  $F(p_2, p_1) < \infty$ , 故式(2.62)对  $p_2(x)$  和  $p_1(x)$  也成立, 即有

$$\begin{aligned} \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx &= \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx \\ &= f(1, 1) - \int_{\mathcal{A}} f(1, 1) \end{aligned} \quad (2.63)$$

另一方面, 若对式(2.61)作变量置换, 令  $x = x$ , 则有

$$\begin{aligned} \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx &= \int_{\mathcal{A}} f(g_2(x), g_1(x)) dx \\ &= f(1, 1) - \int_{\mathcal{A}} f(1, 1) \end{aligned} \quad (2.64)$$

比较式(2.63)与式(2.64), 可以得到

$$\int_{\mathcal{A}} f(1, 1) - \int_{\mathcal{A}} f(1, 1) = \int_{\mathcal{A}} f(1, 1) - f(1, 1) \quad (2.65)$$

(5) 定义新函数  $f(t)$ , 使之对所有  $t > 0$  满足

$$f(t) = \frac{f(t, t)}{t} - f(1, 1)$$

则式(2.65)可以写成

$$f(t) - f(t) = f(t) \quad (2.66)$$

在节“2.1.3 熵函数形式的唯一性”中已经证明了满足式(2.66)的函数必取

$$f(t) = k \log t$$

的形式, 其中  $k$  为任意常数。故



$$f(t, t) = kt \log t + f(1, 1)t$$

从而

$$F(p, p) = k \int p(x) \log p(x) dx + f(1, 1) \int p(x) dx$$

上式中  $\int p(x) dx = 1$ 。根据有限性假设有  $F(p, p) < \infty$ ，但  $\int p(x) \log p(x) dx$  在某些概率密度函数下可以取无穷大，故必有  $k = 0$ 。所以得

$$F(p, p) = f(1, 1)$$

又由可加性假设，当  $p$  为二元概率密度函数时，应有

$$F(p, p) = f(1, 1) + f(1, 1)$$

故必有

$$f(1, 1) = 0, \quad F(p, p) = 0 \quad (2.67)$$

于是

$$f(t, t) = kt \log t + f(1, 1)t = 0 \quad (2.68)$$

将式(2.68)代入式(2.61)中，即得到

$$\int f(g_2(x), g_1(x)) dx = \frac{1}{J} \int f(g_2(x), g_1(x)) dx \quad \text{证毕}$$

**引理 2.2** 设  $F$  满足可加性及有限性，则  $F$  在随机矢量作非奇异线性变换时保持不变，即设随机矢量  $\mathbf{X}$  及其概率密度  $p_2(x)$  和  $p_1(x)$ ，经非奇异线性  $\mathbf{T}$  变换后的随机矢量  $\mathbf{Y} = \mathbf{TX}$  有对应的概率密度  $p_2(y)$  及  $p_1(y)$ ，则

$$F(p_2, p_1) = F(p_2, p_1) \quad (2.69)$$

**证明** 设  $F(p_2, p_1) < \infty$ ，由引理 2.1 可以知道

$$F(p_2, p_1) = \int f(p_2(\mathbf{x}), p_1(\mathbf{x})) d\mathbf{x} = \frac{1}{J} \int f(p_2(\mathbf{x}), p_1(\mathbf{x})) d\mathbf{x} \quad (2.70)$$

由概率论可以知道，变换前后的概率密度存在关系式

$$p_2(\mathbf{x}), p_1(\mathbf{x}) = p_2(\mathbf{Tx}) \det \mathbf{T}, \quad p_1(\mathbf{x}) = p_1(\mathbf{Tx}) \det \mathbf{T} \quad (2.71)$$

其中行列式  $\det \mathbf{T} \neq 0$ 。故可以令  $J = 1/\det \mathbf{T}$ 。

将式(2.71)代入式(2.70)中，即得

$$\begin{aligned} F(p_2, p_1) &= (\det \mathbf{T}) \int f(p_2(\mathbf{Tx}), p_1(\mathbf{Tx})) d\mathbf{x} \\ &= \int f(p_2(\mathbf{y}), p_1(\mathbf{y})) d\mathbf{y} \\ &= F(p_2, p_1) \end{aligned} \quad (2.72)$$

反过来,若设  $F(p_2, p_1) < \infty$ , 因  $T$  是非奇异线性变换, 此时可以取逆变换  $T^{-1}$ , 同样可以得到

$$F(p_2, p_1) = F(p_2, p_1)$$

若令两者均取无穷, 则

$$F(p_2, p_1) = \infty = F(p_2, p_1)$$

则定理的结论仍然成立。

证毕

引理 2.3 设  $f$  是单变量实函数, 满足

$$\frac{p_2(x)}{p_1(x)} p_2(x) dx = 0 \quad (2.73)$$

其中,  $p_2(x)$ 、 $p_1(x)$  是概率密度函数, 且满足  $F(p_2, p_1) < \infty$ ,  $F$  满足有限性假设, 则  $f$  必取以下形式

$$f(t) = D \frac{1}{t} - 1 \quad (2.74)$$

其中,  $t > 0$ ,  $D$  是常数。

证明 令  $u, v$  是两个任意正实数, 满足  $u + v > 0$ , 而

$$r = \frac{1 - v}{u + v}$$

则  $0 \leq r \leq 1$ , 且

$$ru + (1 - r)v = 1$$

取集合  $M$  及其子集  $A$ , 满足

$$\int_M dx = m, \quad \int_A dx = rm, \quad \text{且 } 0 \leq m \leq 1$$

取概率密度  $p_2(x)$  和  $p_1(x)$ , 使满足

$$\begin{aligned} p_1(x) &= 1, & \text{当 } x \in M \text{ 时} \\ &= u, & x \in A \\ p_2(x) &= v, & x \in M - A \\ &= p_1(x), & x \in \text{补} \end{aligned} \quad (2.75)$$

则

$$\begin{aligned} \int p_2(x) dx &= \int_A u dx + \int_{M-A} v dx + \int_{\text{补}} p_1(x) dx \\ &= urm + v(m - rm) + (1 - m) \\ &= 1 \end{aligned}$$

即  $p_2(x)$  满足概率密度函数的要求, 且

$$F(p_2, p_1) = \int_M f(p_2(x), p_1(x)) dx + \int_{\text{补}} f(p_2(x), p_1(x)) dx <$$

因为上式的第一项是在有限测度集合  $M$  上的有界积分, 由该引理的有限性假设可以知道, 第二项也必为有限值, 所以,  $p_2(x), p_1(x)$  满足该引理的要求。将式(2.75)代入式(2.73)中, 得

$$\begin{aligned} & \int \frac{p_2(x)}{p_1(x)} p_2(x) dx \\ &= \int_A (u) u dx + \int_{M-A} (v) v dx + \int_{\text{补}} (1) p_1(x) dx \\ &= r m u(u) + (1-r) m v(v) + (1-m)(1) = 0 \end{aligned} \quad (2.76)$$

当  $v=1$  时,  $r = \frac{1-v}{u-v} = 0$ , 则必有  $(1) = 0$ , 于是,

$$r m u(u) + (1-r) m v(v) = 0 \quad (2.77)$$

代入  $r = \frac{1-v}{u-v}$ , 得到当  $v \neq 1$  时有

$$\frac{u(u)}{1-u} = \frac{v(v)}{1-v} \quad (2.78)$$

该式两端各与变量  $u, v$  有关, 故必有

$$\begin{aligned} (u) &= D \frac{1}{u} - 1 \\ (v) &= D \frac{1}{v} - 1 \end{aligned}, \text{ 当 } u > 1, 0 < v < 1 \text{ 时} \quad (2.79)$$

又  $(1) = 0$ , 故得到对所有  $t > 0$  有

$$(t) = D \frac{1}{t} - 1, D \text{ 为常数} \quad \text{证毕}$$

**引理 2.4** 设  $F$  满足线性变换下的不变性、有限性和半有界性, 则  $f(u, v)$  函数必具有形式

$$f(u, v) = u - \frac{u}{v} \quad (2.80)$$

其中  $\phi$  为某种特定形式的函数。

**证明** 该引理的证明主要利用线性变换下的不变性。

(1) 考虑最简单的线性变换, 即乘以常数  $t$  的情形。作变换  $x = tx$ , 变换后的概率密度函数为  $p_2(x), p_1(x)$ 。由引理 2.1 可以知道

$$\int f(p_2(x), p_1(x)) dx = \frac{1}{t} \int f(tp_2(x), tp_1(x)) dx \quad (2.81)$$

用  $x = tx$  替换, 有

$$\begin{aligned} f(p_2(x), p_1(x))dx &= f(tp_2(tx), tp_1(tx))dx \\ &= f(tp_2(tx), tp_1(tx))dx \end{aligned} \quad (2.82)$$

(2) 取两组概率密度函数。先取  $p_2(x)$  及  $p_1(x)$ , 使其满足  $F(p_2, p_1) < \frac{1}{2}$ , 且分别满足

$$\begin{aligned} p_2(x) &= \frac{1}{a}, \text{ 当 } 0 \leq x \leq a < 1, \\ p_1(x) &= 1, \text{ 当 } 0 \leq x \leq a < 1, \end{aligned}$$

再取  $p_2(x)$  及  $p_1(x)$ , 使其满足

$$\begin{aligned} p_2(x) &= \begin{cases} \frac{1}{a}, & x < 0 \\ 0, & 0 \leq x \leq a' \\ \frac{1}{a-a'}, & x > a' \end{cases} \\ p_1(x) &= \begin{cases} \frac{1}{a}, & x < 0 \\ 0, & 0 \leq x \leq a' \\ \frac{1}{a-a'}, & x > a' \end{cases} \end{aligned} \quad (2.83)$$

显然,  $p_2(x)$  和  $p_1(x)$  满足  $\int p_2(x)dx = 1$  及  $\int p_1(x)dx = 1$ , 且有  $F(p_2, p_1) < \frac{1}{2}$ 。

由引理 2.1 的证明可以知道, 这两组概率密度函数满足

$$\begin{aligned} \int f(p_2(x), p_1(x))dx &= \int f(p_2(x), p_1(x))dx \\ &= af(1, 1) - \frac{a}{t}f(t, t) \end{aligned} \quad (2.84)$$

及

$$\begin{aligned} \frac{1}{t} \int f(tp_2(x), tp_1(x))dx &= \frac{1}{t} \int f(tp_2(x), tp_1(x))dx \\ &= \frac{a}{t}f(t, t) - \frac{a}{t}f(t, t) \end{aligned} \quad (2.85)$$

由第(1)步证明中的式(2.81)和式(2.82)可以知道, 式(2.84)与式(2.85)相等, 即

$$af(1, 1) - \frac{1}{t}f(t, t) = \frac{1}{t}f(t, t) - \frac{1}{t}f(t, t) \quad (2.86)$$

(3) 定义当  $t$  取某恒定值时, 式(2.86)左端的值为  $k(t)$ , 即设

$$k(\cdot) = \frac{1}{f(\cdot, 1)} - \frac{1}{f(\cdot, \cdot)} \quad (2.87)$$

于是利用函数  $k(\cdot)$ , 可以将式(2.86)表示成

$$k(\cdot) = k(\cdot/t) - k(t)$$

或

$$k(\cdot) + k(t) = k(\cdot/t) \quad (2.88)$$

该式对所有  $\cdot > 0$  和  $t > 0$  成立, 故函数  $k(\cdot)$  必取

$$k(\cdot) = C \log \quad (2.89)$$

其中  $C$  为固定  $\cdot$  取某值时的常数。当  $\cdot$  取不同值时,  $C$  的值可能会随之改变, 故记作  $C(\cdot)$ , 于是, 式(2.87)可写成

$$\frac{1}{f(\cdot, 1)} - \frac{1}{f(\cdot, \cdot)} = C(\cdot) \log \quad (2.90)$$

定义

$$(\cdot) = \frac{1}{f(\cdot, 1)}$$

并令式(2.90)中  $\cdot = u/v$ ,  $\cdot = v$ , 则对任意  $u > 0, v > 0$ , 有

$$f(u, v) = u \frac{u}{v} - C \frac{u}{v} u \log v \quad (2.91)$$

(4) 现设  $p_2(x), p_1(x)$  为任意能满足  $F(p_2, p_1) < \infty$  的概率密度函数。由式(2.81), 有

$$\begin{aligned} & \frac{p_2(x)}{p_1(x)} - C \frac{p_2(x)}{p_1(x)} \log p_1(x) p_2(x) dx \\ = & \frac{tp_2(x)}{tp_1(x)} - C \frac{tp_2(x)}{tp_1(x)} \log tp_1(x) tp_2(x) \frac{1}{t} dx \end{aligned}$$

化简得

$$\log t - C \frac{p_2(x)}{p_1(x)} p_2(x) dx = 0 \quad (2.92)$$

由引理 2.3 可以知道

$$C(t) = D \frac{1}{t} - 1 \quad (2.93)$$

其中  $D$  为常数。将式(2.93)代入式(2.91)中, 得

$$f(u, v) = u \frac{u}{v} + D(u - v) \log v \quad (2.94)$$

(5) 证明式(2.94)中的  $D$  必为零。对随机变量  $X$  作非线性变换  $T(X)$ 。设

$T$  及其逆  $T^{-1}$  均可微, 导数为正。则变换前后的概率密度函数为

$$p_2(x) = p_2(T(x)) \frac{dT(x)}{dx}$$

$$p_1(x) = p_1(T(x)) \frac{dT(x)}{dx}$$

由式(2.94)可以知道

$$\begin{aligned} & f(p_2(x), p_1(x)) \\ &= p_2(x) \frac{p_2(x)}{p_1(x)} + D(p_2(x) - p_1(x)) \log p_1(x) \\ &= p_2(T(x)) \frac{dT(x)}{dx} \frac{p_2(T(x))}{p_1(T(x))} \\ &\quad + D[p_2(T(x)) - p_1(T(x))] \frac{dT(x)}{dx} \log p_1(T(x)) \frac{dT(x)}{dx} \\ &= p_2(T(x)) \frac{p_2(T(x))}{p_1(T(x))} \\ &\quad + D[p_2(T(x)) - p_1(T(x))] \log p_1(T(x)) \frac{dT(x)}{dx} \\ &\quad + D[p_2(T(x)) - p_1(T(x))] \log \frac{dT(x)}{dx} \frac{dT(x)}{dx} \end{aligned} \quad (2.95)$$

于是

$$\begin{aligned} & F(p_2, p_1) \\ &= F(p_2, p_1) - D[p_2(T(x)) - p_1(T(x))] \log \frac{dT^{-1}(x)}{dx} \frac{dT(x)}{dx} dx \\ &= F(p_2, p_1) - D(p_2(x) - p_1(x)) \log \frac{dT^{-1}(x)}{dx} dx \end{aligned} \quad (2.96)$$

若  $D > 0$ , 则总可以找到一种变换  $T$ , 使上式中后一项  $> 0$ , 即

$$F(p_2, p_1) < F(p_2, p_1)$$

而

$$F(p_1, p_1) = F(p_1, p_1) - D(p_1(x) - p_1(x)) \log \frac{dT^{-1}(x)}{dx} dx = F(p_1, p_1)$$

由半有界性可以知道

$$F(p_2, p_1) > F(p_1, p_1)$$

于是,  $F(p_2, p_1)$  有可能小于  $F(p_1, p_1)$ , 从而与半有界性矛盾。或者说, 若  $D > 0$ , 则总可以找到一种变换  $T$ , 使  $F(p_2, p_1) < F(p_1, p_1)$ , 即

$$F(p_2, p_1) < F(p_1, p_1)$$

所以,必有  $D=0$ 。因此,式(2.94)就变成

$$f(u, v) = u \frac{u}{v} \quad \text{证毕}$$

有了以上 4 个引理就可以证明唯一性定理。其思路为:首先利用可加性这一积分方程得到关于函数  $(u, v)$  的泛函方程,然后由  $(\cdot, \cdot)$  的泛函方程具体求得  $(\cdot, \cdot)$  函数,即可以证明该定理。

证明 (唯一性定理 2.3 的证明)

(1) 由函数  $(u, v)$  的泛函方程,求函数  $(u, v)$  的方程

设有概率密度函数  $g_2(x), g_1(x)$  以及  $h_2(y), h_1(y)$ , 并满足

$$F(g_2, g_1) < \infty, \quad F(h_2, h_1) < \infty$$

由可加性,有

$$\begin{aligned} & \int \int f(g_2(x)h_2(y), g_1(x)h_1(y)) dx dy \\ &= \int f(g_2(x), g_1(x)) dx + \int f(h_2(y), h_1(y)) dy \end{aligned} \quad (2.97)$$

将式(2.81)和式(2.82)代入式(2.97),可以得到

$$\frac{g_2(x)h_2(y)}{g_1(x)h_1(y)} - \frac{g_2(x)}{g_1(x)} - \frac{h_2(y)}{h_1(y)} - g_2(x)h_2(y) dx dy = 0 \quad (2.98)$$

对任意确定的  $g_2(x)$  和  $h_2(y)$ , 定义函数  $\phi(t)$  为

$$\phi(t) = \frac{tg_2(x)}{g_1(x)} - \frac{g_2(x)}{g_1(x)} - \phi(t)g_2(x) dx \quad (2.99)$$

于是式(2.98)可以改写为

$$\frac{h_2(y)}{h_1(y)} h_2(y) dy = 0 \quad (2.100)$$

由引理 2.3 可以知道

$$\phi(t) = D \frac{1}{t} - 1$$

故有

$$\phi(1) = 0 \quad (2.101)$$

将式(2.101)代入式(2.99)中,可以得到

$$\phi(1) = 0 \quad (2.102)$$

又

$$\frac{u \phi(u)}{1-u} = \frac{v \phi(v)}{1-v} = D, \quad \text{当 } u \rightarrow 1, v \rightarrow 1 \text{ 时} \quad (2.103)$$

将式(2.99)代入式(2.103)中,得

$$\begin{aligned} \frac{u}{1-u} &= \frac{u g_2(x)}{g_1(x)} - \frac{g_2(x)}{g_1(x)} - \phi(u) \\ &- \frac{v}{1-v} = \frac{v g_2(x)}{g_1(x)} - \frac{g_2(x)}{g_1(x)} - \phi(v) \quad g_2(x) dx = 0 \end{aligned} \quad (2.104)$$

定义函数  $\bar{\phi}(t)$  为

$$\bar{\phi}(t) = [\phi(tu) - \phi(t) - \phi(u)] \frac{u}{1-u} - [\phi(tv) - \phi(t) - \phi(v)] \frac{v}{1-v} \quad (2.105)$$

则式(2.104)可以改写为

$$-\frac{g_2(x)}{g_1(x)} g_2(x) dx = 0 \quad (2.106)$$

由引理 2.3 可以得到

$$\bar{\phi}(t) = D \frac{1}{t} - 1 \quad (2.107)$$

式中  $D$  为常数,但可能与  $u, v$  有关,故记作  $D(u, v)$ 。

将式(2.107)代入式(2.105)中,即得到函数  $\phi(\cdot)$  的方程

$$\begin{aligned} &[\phi(tu) - \phi(t) - \phi(u)] \frac{tu}{(1-t)(1-u)} - [\phi(tv) - \phi(t) - \phi(v)] \frac{tv}{(1-t)(1-v)} \\ &= D(u, v) \end{aligned} \quad (2.108)$$

上式对  $t > 0, u > 0, v > 0$ , 且  $t \neq 1, u \neq 1, v \neq 1$  均成立。显然

$$D(u, v) = -D(v, u) \quad (2.109)$$

(2) 求解方程(2.108)

定义函数  $d(u, v)$  为

$$d(u, v) = [\phi(uv) - \phi(u) - \phi(v)] \frac{uv}{(1-u)(1-v)} \quad (2.110)$$

则式(2.108)可以改写成

$$d(t, u) - d(t, v) = D(u, v) \quad (2.111)$$

当  $t = u$  时,有

$$d(u, u) - d(u, v) = D(u, v)$$

当  $t = v$  时,有



$$d(v, u) - d(v, v) = D(u, v)$$

故

$$d(u, u) - d(u, v) = d(v, u) - d(v, v) \quad (2.112)$$

又

$$d(u, v) = d(v, u)$$

所以有

$$2d(u, v) = d(u, u) + d(v, v) \quad (2.113)$$

定义函数  $a(u)$  为

$$a(u) = \frac{d(u, u)(1 - u)}{2} \quad (2.114)$$

则式(2.110)可以写成

$$\begin{aligned} uv[d(uv) - (u) - (v)] &= d(u, v)(1 - u)(1 - v) \\ &= \frac{1}{2}[d(u, u) + d(v, v)](1 - u)(1 - v) \\ &= a(u)(1 - v) + a(v)(1 - u) \end{aligned} \quad (2.115)$$

将式(2.115)中的  $u$  以  $t$  代换,  $v$  用  $uv$  代换, 可以得到

$$tuv[d(tuv) - (t) - (uv)] = a(t)(1 - uv) + a(uv)(1 - t) \quad (2.116)$$

对式(2.115)进行变换, 可以得到

$$uv(uv) = uv[d(u) + (v)] + a(u)(1 - v) + a(v)(1 - u)$$

代入式(2.116)中, 并整理得

$$\begin{aligned} tuv[d(tuv) - (t) - (u) - (v)] - a(t)(1 - uv) - a(u)(1 - tv) - a(v)(1 - tu) \\ = a(uv)(1 - t) - a(u)(1 - t) - a(v)(1 - t) \end{aligned} \quad (2.117)$$

同样, 若将式(2.115)中的  $u$  以  $tu$  代换,  $v$  不变, 可以简化得到

$$\begin{aligned} tuv[d(tuv) - (t) - (u) - (v)] - a(t)(1 - uv) - a(u)(1 - tv) - a(v)(1 - tu) \\ = a(tu)(1 - v) - a(t)(1 - v) - a(u)(1 - v) \end{aligned} \quad (2.118)$$

同理, 若将式(2.115)中的  $v$  以  $tv$  代换,  $u$  不变, 又可以得到

$$\begin{aligned} tuv[d(tuv) - (t) - (u) - (v)] - a(t)(1 - uv) - a(u)(1 - tv) - a(v)(1 - tu) \\ = a(tv)(1 - u) - a(t)(1 - u) - a(v)(1 - u) \end{aligned} \quad (2.119)$$

于是, (2.117), (2.118), (2.119)三式的右端连等, 均除以  $(1 - t)(1 - u)(1 - v)$  后, 得到

$$\frac{a(tu) - a(t) - a(u)}{(1 - t)(1 - u)} = \frac{a(uv) - a(u) - a(v)}{(1 - u)(1 - v)} = \frac{a(tv) - a(t) - a(v)}{(1 - t)(1 - v)} \quad (2.120)$$

其中  $\frac{a(uv) - a(u) - a(v)}{(1-u)(1-v)}$  与  $t$  无关,  $\frac{a(tv) - a(t) - a(v)}{(1-t)(1-v)}$  与  $u$  无关。由此可以知道, 等式最左端的值与  $t, u$  无关, 即应为某常数。设此常数为  $A/2$ , 即得

$$a(tu) - a(t) - a(u) = \frac{A}{2}[(1-t) + (1-u) - (1-tu)] \quad (2.121)$$

令

$$b(t) = -a(t) - \frac{A}{2}(1-t) \quad (2.122)$$

则式(2.121)可以写成

$$b(t) + b(u) = b(tu) \quad (2.123)$$

所以必有

$$b(t) = B \log t \quad (2.124)$$

其中  $B$  为常数。故

$$a(t) = -\frac{A}{2}(1-t) - B \log t \quad (2.125)$$

令

$$c(t) = (t) + A \frac{1}{t} - 1 + B \frac{\log t}{t} \quad (2.126)$$

可知

$$\begin{aligned} & uv[c(uv) - c(u) - c(v)] \\ &= uv[(uv) - (u) - (v)] \\ &\quad + Auv \left( \frac{1}{uv} - 1 - \frac{1}{u} - 1 - \frac{1}{v} - 1 \right) + Buv \left( \frac{\log uv}{uv} - \frac{\log u}{u} - \frac{\log v}{v} \right) \\ &= a(u)(1-v) + a(v)(1-u) + A(1-u)(1-v) \\ &\quad + B \log u(1-v) + B \log v(1-u) \\ &= 0 \end{aligned} \quad (2.127)$$

由式(2.127)可以知道

$$c(t) = C \log t \quad (2.128)$$

其中  $C$  为常数, 故

$$(t) = -A \frac{1}{t} - 1 - B \frac{\log t}{t} + C \log t \quad (2.129)$$

于是, 由式(2.81)和式(2.82)可以知道

$$f(u, v) = A(u-v) + Bv \log \frac{v}{u} + Cu \log \frac{u}{v} \quad (2.130)$$

所以最后可以得到

$$\begin{aligned}
 F(p_2, p_1) &= \int f(p_2(x), p_1(x)) dx \\
 &= \int A(p_2(x) - p_1(x)) dx + \int B p_1(x) \log \frac{p_1(x)}{p_2(x)} dx \\
 &\quad + \int C p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \\
 &= \int B p_1(x) \log \frac{p_1(x)}{p_2(x)} dx + \int C p_2(x) \log \frac{p_2(x)}{p_1(x)} dx \quad (2.131)
 \end{aligned}$$

由于改变  $p_2(x)$ ,  $p_1(x)$  可以使得上式右端中的两项的任一项任意大, 按照式(2.67)及半有界性假设,  $B, C$  应为非负常数, 且不同时为零。证毕

唯一性定理证明了散度函数的唯一性。由于  $B \geq 0, C \geq 0$  是任设的常数, 所以当取  $B=0$  或者  $C=0$  时, 就得到了鉴别信息(或方向散度)。因此, 该定理实际上也就证明了在上述 3 个条件下鉴别信息函数形式的唯一性。当然, 如果改变对函数性质的要求, 就会得到其他形式的函数。

## 2.5 对信息论基本概念的若干评注

本章我们介绍了信息论中的三个基本概念: 熵、互信息和鉴别信息。这三个概念的要点可以归纳如下:

(1) 信息论的三个基本概念分别给出了随机变量不确定性的量度以及在消除或减少这一不确定性时所获信息的量度。

随机变量不确定性的量度: 香农定义的熵是随机变量不确定性的最合理的量度。这可以从以下几个方面来理解:

尽管在不同的条件下可以得到不同形式的不确定性的量度, 但是, 直到目前为止, 从理论上以及函数形式的简洁上讲, 香农定义的熵函数仍然是最好的。

在连续分布下只存在微分熵这一问题并不是香农定义的致命缺陷。因为从概念上讲, 连续随机变量所取的值应该是无穷精度, 其不确定性为无穷是完全合理的。在实际应用中, 由于变量所取的数值只能是有限精度, 因此, 连续随机变量的熵为无穷这一点不会给实际应用带来困难。我们只需用一个相对尺度来衡量连续随机变量的不确定性即可。

减少或消除随机变量的不确定性的两条途径和信息的两种量度:

一条是对另一个与我们感兴趣的随机变量统计关联的随机变量进行观察、

试验,从而获得关于原随机变量的信息,减少或消除其不确定性。该信息量可以用互信息进行量度。

另一条是对我们感兴趣的随机变量本身进行观察、试验,从而获得信息,减少或消除其不确定性。该信息量可以用鉴别信息进行量度。

(2) 从统计数学的角度来看,信息论的三个基本概念给出了三个统计量,代表了三种量度,其中:

- 熵是一个系统无序性的量度;
- 鉴别信息是两种概率分布之间差异性的量度;
- 互信息是两个随机变量之间统计依存性的量度。

因此,熵、互信息和鉴别信息大大丰富了统计数学中对随机现象的描述方法,其意义超过了随机变量一般的数字特征。

(3) 三者的相互关系:

在信息论的三个基本概念中,熵是最基础的。鉴别信息则是最普遍的,由鉴别信息可以推出互信息,故互信息是鉴别信息的特例。由互信息又可以推出熵,故熵是互信息的特例。

三者的上述关系,使得它们的函数性质也存在相似之处,特别是三者均有凸性。凸性使得三者都特别适合作为优化问题中的目标函数,因为由此导出的极值总是全局极值。但三者的表达式中都含有对数函数,这给实际使用又带来一定的困难。

## 习 题

2.1 设  $X$  和  $Y$  是各有均值  $m_x, m_y$ , 方离差  $\sigma_x^2, \sigma_y^2$ , 且相互独立的高斯随机变量,已知  $U = X + Y$ ,  $V = X - Y$ 。试求  $I(U; V)$ 。

2.2 设有随机变量  $X, Y, Z$  均取值于  $\{0, 1\}$ , 已知  $I(X; Y) = 0$ ,  $I(X; Y|Z) = 1$ 。求证:  $H(Z) = 1$ ,  $H(XYZ) = 2$ 。(单位:比特/符号)

2.3 设随机变量  $X$  和  $Y$  的联合分布如下所示:

$X \backslash Y$	0	1
0	$1/3$	$1/3$
1	0	$1/3$

随机变量  $Z = X \oplus Y$ , 式中  $\oplus$  为模 2 和。试求:

- (1)  $H(X), H(Y)$ ;  
 (2)  $H(X|Y), H(Y|X), H(X|Z)$ ;  
 (3)  $I(X; Y), H(XYZ)$ 。

2.4 设随机变量  $X$  的值取自集合  $(a_1, a_2, \dots, a_{k-1}, a_k)$ , 已知  $p(X = a_k) =$ , 试证:

$$(1) H(X) = -\log p(X = a_k) - (1 - p(X = a_k)) \log(1 - p(X = a_k)) + (1 - p(X = a_k)) H(Y)$$

其中  $Y$  的值取自  $(a_1, a_2, \dots, a_{k-1})$ , 且有  $p(Y = a_i) = \frac{p(X = a_i)}{1 - p(X = a_k)}, i = 1, 2, \dots, k - 1$ ;

$$(2) H(X) = -\log p(X = a_k) - (1 - p(X = a_k)) \log(1 - p(X = a_k)) + (1 - p(X = a_k)) \log(k - 1)。$$

2.5 设随机变量  $X, Y, Z$  的值均取自集合  $\{0, 1\}$ , 试给出联合概率分布的实例, 使其满足:  $I(X; Y) = 0$  bit,  $I(X; Y|Z) = 1$  bit。

2.6 设  $X$  为连续随机变量, 试给出概率分布的实例, 使其满足微分熵  $h(X) < 0$ 。

2.7 设有信号  $X$  经处理器  $A$  后获输出  $Y$ ,  $Y$  再经处理器  $B$  后获输出  $Z$ 。已知处理器  $A$  和  $B$  分别独立处理  $X$  和  $Y$ 。试证:  $I(X; Z) = I(X; Y)$ 。

2.8 设有长  $N$  的二元序列, 其概率分布为

$$p(x_1 x_2 \dots x_N) = \begin{cases} 2^{-N+1}, & \text{当序列有偶数个 } 1 \\ 0, & \text{当序列有奇数个 } 1 \end{cases}$$

试求:  $I(X_1; X_2), I(X_2; X_3 | X_1), \dots, I(X_{N-1}; X_N | X_1 \dots X_{N-2})$ 。

2.9 设有随机变量  $X, Y, Z$ , 试给出联合分布的两个实例, 使其条件互信息能分别满足:

- (1)  $I(X; Y|Z) > I(X; Y)$ ;  
 (2)  $I(X; Y|Z) < I(X; Y)$ 。

2.10 已知随机变量  $X$  和  $Y$  的联合概率分布  $p(a_k, b_l)$  满足

$$p(a_1) = \frac{1}{2}, \quad p(a_2) = p(a_3) = \frac{1}{4}, \quad p(b_1) = \frac{2}{3}, \quad p(b_2) = p(b_3) = \frac{1}{6}$$

试求能使  $H(XY)$  取最大值的联合概率分布。

2.11 设随机变量  $X, Y, Z$  满足  $p(xyz) = p(x)p(y|x)p(z|y)$ 。求证:  $I(X; Y) = I(X; Y|Z)$ 。

2.12 求证:  $H(XYZ) = H(XZ) + H(Y|X) - I(Y; Z|X)$ 。

2.13 求证:  $I(X; Y; Z) = H(XYZ) - H(X) - H(Y) - H(Z) + I(X; Y) +$

$I(Y; Z) + I(Z; X)$ 。

2.14 令  $X$  为掷钱币直至其正面第一次向上所需的次数, 求  $H(X)$ 。

2.15 设  $p_i(x) \sim N(\mu_i, \sigma_i^2)$ , 试求  $I(p_2, p_1; X)$ 。

2.16 设随机序列  $\{X_n\}$  按某概率分布  $p(a_k)$  取值于  $\{a_1, a_2, \dots, a_k\}$ , 试证明其频率

$$P_N(a_k) = \frac{1}{N} \sum_{n=1}^N I(X_n = a_k)$$

其中  $I(X_n = a) = \begin{cases} 1, & X_n = a \\ 0, & \text{其他} \end{cases}$ , 且满足  $E\{I(P_N(a_k), p(a_k))\} = E\{I(P_N(a_k), p(a_k))\}$ 。

2.17 设  $p_1(x, y) = \frac{1}{2\pi\sigma_x\sigma_y} \exp\left[-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2} + \frac{y^2}{\sigma_y^2}\right)\right]$

$$p_2(x, y) = \frac{1}{2\pi\sigma_x\sigma_y\sqrt{1-\rho^2}} \exp\left[-\frac{1}{2(1-\rho^2)}\left(\frac{x^2}{\sigma_x^2} - 2\rho\frac{xy}{\sigma_x\sigma_y} + \frac{y^2}{\sigma_y^2}\right)\right]$$

试求:  $I(p_2, p_1; XY)$  及  $J(p_2, p_1; XY)$ ,  $I(X; Y)$ 。

2.18 试给出平均条件鉴别信息与无条件鉴别信息之间的不等式关系。

2.19 已知 12 个球中有一个球的重量与其它球不同, 其它球均等重。问如何用天平称 3 次找出此球。

## 第 3 章 信源的熵率、冗余度与冗余度压缩编码

对信息源或信源的研究一直是信息论研究中的主要组成部分。信息论对信源研究的内容包括以下 3 个方面：

### (1) 信源的建模

我们知道,信源输出信号的数学描述已有成熟的理论——随机过程,因此,可以说信源的建模在一定程度上也就是用恰当的随机过程来描述信号。然而,一般的随机过程理论并不涉及和讨论信号中所携带的信息,而信息论所关心的中心内容则是信号中携带的信息。

### (2) 信源输出信号中携带信息的效率的计算

在信息论中,信源输出信号所携带信息的效率是用熵率或冗余度来表示的,我们将在本章讨论各种信源的熵率的计算方法。

### (3) 信源输出信息的有效表示

一般地,信源输出信号中携带信息的效率并不很高,如何用适当的信号有效地表示信源输出的信息是人们感兴趣的问题,这就是信源编码的问题。在理论上信源编码与随机过程的同构问题紧密相关。在实际应用中,信源编码对信息的存储和传输都有极大的价值。我们将在本章中讨论无记忆信源和有记忆信源下的基本编码方法,包括等长分组编码、变长分组编码和变长树码,这些编码方法都已在实际中得到应用。限于篇幅,我们将只介绍其基本的原理。

## 3.1 信源、信源模型与信源编码

### 3.1.1 信源

信息论研究的对象是信息,显然,信息论首先需要研究信息的来源。在香农最早研究信息论的论文中,他把信息的来源称为信息源(information source),或简称信源。信源作为一般信息系统中信息的来源,其内容是很广泛的,如通信系统中传输的对象、信号处理系统中信号的来源、测量系统中被测物理量的来源、数据统计系统中原始数据的来源等等。

图 3.1 是香农给出的通信系统组成图。在图 3.1 中,信源的输出被称作消息(message),以突出说明消息一般是不能被直接送给信道传输的,消息通常需要经过发送器的变换才能转换成适于信道传输的信号(signal)。消息和信号的这种区别对通信系统来讲有一定的意义。

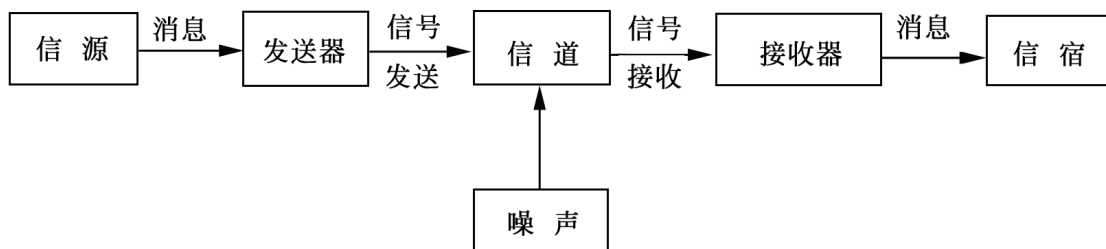


图 3.1 通信系统的组成图

在一般的情况下,消息和信号既是相互区别的,又是相互联系的。一方面,消息和信号的定义与含义不同。当信源的输出连同语义学上的意义一并加以理解时称为消息。例如,播音员播送的一段新闻,记者拍摄的一段录像,歌手演唱的一首歌曲等,都应该说是消息。而当信源的输出只被看作是随时间变化的某一物理量  $f(t)$  或随时间、空间位置变化的某一物理量  $f(x, y, t)$  时称为信号。另一方面,信源的输出在我们接到、看到、听到之前都是随机的、不确定的,属于随机现象。因此,从信息论的观点来看,信源的输出无论是看作消息,还是看作信号,均含有信息。

因此,消息、信号和信息都可以说是信源的输出,或者说它们是信源输出的三个方面。由于信息论关心的是信源输出的信息,所以可将信源称为信息源。

### 3.1.2 信源模型

对于信源输出的消息、信号和信息三个方面,统计信息论是不研究语义学上的意义的,所以只考虑信源输出的后两个方面,即信号和信息。应该说,信号是信息的载体和具体表达形式,信息必须借助信号才能得以表现,信息不能离开信号而单独存在。所以,研究信源就是要研究信号和信息的关系,特别是信号如何才能有效地携带信息。

为此,我们首先要对信源建立一个便于分析的数学模型。如何对实际信源,如语音信号、电视信号等,通过实验研究和数学处理建立数学模型是一个相当复杂的工作,不是信息论要研究的主要问题。在本章中,我们只给出并讨论几种比



较简单、但在理论上比较重要、在实用上比较普遍的几种信源模型。

首先, 信源可按不同的原则加以分类。

(1) 按信号取值的集合和信号取值时刻的集合是离散集合或连续集合进行分类, 可分为数字信源, 模拟信源和连续信源, 如表 3 .1 所示。

表 3.1 信源的分类

信号取值的集合	信号取值时刻的集合	信源的种类
离 散	离 散	数字信源 ( digital source ) (或离散信源 ( discrete source ) )
连 续	连 续	模拟信源 ( analog source ) (或波形信源 ( waveform source ) )
连 续	离 散	连续信源 ( continuous source )
离 散	连 续	

需要说明的是, 根据信号理论的分析, 对于频带有限信号的集合, 其信号在有限时间  $T$  内的值总可以足够精确地用  $2WT$  维空间中的一个矢量来表示, 其中  $W$  为信号带宽。特别地, 当这一  $2WT$  维空间的基底函数是采样函数时, 这  $2WT$  维矢量的每个标量值即为信号的采样值。本书今后在研究模拟信源 (或波形信源) 时, 只限于这种具有有限带宽特性的模拟信源。

(2) 按有穷维分布函数族的性质进行分类。

信源的深层特性在于信号在各时刻取值的概率分布函数, 这一族无限多个分布函数组成了信号的有穷维分布函数族, 它完整地描述了信源的统计规律性, 因此, 信源的完整的数学模型应包括以下几个方面:

- 信号取值的集合
- 信号取值时刻的集合
- 信号在各时刻取值的有穷维分布函数族

上述数学模型正好与随机过程完全对应, 这是很自然的, 因为信源输出的信号从数学角度来看就是一种随机过程。

根据信源输出信号所对应的不同的随机过程可以导出不同的信源模型。例如, 根据随机过程具有的随机变量前后独立与否可分为独立随机信源 (或称无记忆信源) 和不独立随机信源 (或称有记忆信源); 根据随机过程平稳与否可分为平稳 (稳恒) 信源和非平稳 (非稳恒) 信源。

此外, 与特殊的随机过程相对应又有特殊的信源模型。例如, 与高斯过程相对应的高斯信源, 与马尔可夫过程相对应的马尔可夫信源等, 其中, 马尔可夫信

源是有记忆信源中最简单且最具代表性的一种。

可以看出,信源的第一种分类法比较直观,有实际意义,但不够深刻。第二种分类法比较深刻,却不直观。

若把以上两种分类法合在一起,则可以组合成不同类型的信源。例如,取值离散的独立随机信源,又称为离散无记忆信源;取值时刻离散的高斯信源,又称为时离的高斯信源。

信息论最早和最多研究的是取值离散和取值时刻离散的信源,特别是对语言——这一人类交换信息的最主要工具——的研究,从而产生一系列与语言有关的信源专用术语。例如,将信源的输出信号看成是一个抽象符号的序列,这些符号被称为信源所用的字母,全体字母的集合被称为字母表。符号及字母和一般随机信号所取的数不同,符号与字母相互间是不能进行运算的,而数属于某种代数体系,可以进行一定的运算。但是,这一差别完全不会影响信源输出信号所携带信息这一最基本的性质,所以我们在今后的讨论中一般不再加以特别的区分,而且考虑到信息论中的习惯用法,仍沿袭使用字母、字母表等术语,尽管在很多情况下我们讨论的信源输出实际上是一个离散数列。

### 3.1.3 信源编码

#### 3.1.3.1 编码简介

编码最早的含义是将携带信息的一种字母序列或符号序列映射为另一种字母序列或符号序列。后来,由于数列和字母序列一样常被用来携带信息,所以编码的含义扩展到离散数列甚至连续数列之间的映射。上述映射及其映射前后的序列(或数列)一起构成码,如 Morse 码、ASCII 码等。实现上述映射的装置称为编码器,编码器的输入字母称为源字母,输出字母称为码字母。有关编码及其相关概念的示意图如图 3.2 所示。



图 3.2 编码及其相关概念示意图

从理论上讲,编码实现的是序列到序列的映射。在具体实现时,由于考虑到时延的限制和计算复杂度的限制,编码实现时只能将序列分组后按一定的映射关系序贯地逐步完成。根据不同的分组方式及其随后的映射关系可以构成不同结构的码,如分组码、树码等。

分组码是指将编码器的源字母序列和码字母序列均分成组,而且映射是在分组的基础上独立进行的,即一定的源字母组唯一地确定了一定的码字母组。源字母组又称源字,码字母组又称码字。根据源字和码字的长度固定与否,分组码可以分为定长到定长分组码、定长到变长分组码、变长到定长分组码和变长到变长分组码四种。

树码是指编码器输出的码字母不仅仅由当前输入的源字母决定,而且还可能与以前的源字母或码字母有关。树码的映射关系可以用树图清楚地加以表示。根据分组长度的情况,树码可分为定长到定长树码、定长到变长树码等。还可以按其他特点构成特殊的树码,如映射关系时不变的树码称为滑动分组码,具有线性特性的滑动分组码称为卷积码等。

### 3.1.3.2 信源编码简介

编码可以用来完成各种不同的功能,以达到各种不同的目的。信源编码是指从功能上针对信源的编码,以使信号能更加有效地传输信息。信源编码是信源研究中的一个核心问题,也是信息论所讨论的编码中最重要的一种编码。

为了使信号更有效地传输信息,经信源编码后,码字母表的大小与源字母的大小相比或码字母序列的长度与源字母序列的长度相比,应该得到减小,这样才能去除信源输出信号的冗余度。

信源编码主要有冗余度压缩编码和熵压缩编码两种,冗余度压缩编码可以保证码字母序列在译码后无失真地复原为源字母序列,熵压缩编码只能保证译码时能按一定的失真容许度恢复源字母序列,但同时又能保留尽可能多的信息量。在本章中我们只讨论冗余度压缩编码。

## 3.2 离散稳恒信源的熵率与冗余度

稳恒信源是信源研究中最主要的一种信源,因为很多实际信源在较短的一段时间内都可以用稳恒信源作为其数学模型,而且稳恒信源的研究又是非稳恒信源研究的基础。稳恒信源输出的信号是一个稳恒的随机过程。当信源字母表

是离散的,且信号取值时刻也是离散时,此时的稳恒信源就称为离散稳恒信源。

设离散稳恒信源的字母表为  $\{a_1, a_2, \dots, a_K\}$ , 信源的输出序列用  $\{\dots, u_{-2}, u_{-1}, u_0, u_1, u_2, \dots, u_i, \dots\}$  来表示。根据稳恒随机过程的定义, 信源输出序列的一切有限维概率分布与时间轴起点的选择无关, 即有

$$P(u_i u_{i+1} \dots u_{i+N} = \mathbf{A}) = P(u_j u_{j+1} \dots u_{j+N} = \mathbf{A}) \quad (3.1)$$

其中,  $\mathbf{A}$  为某一特定的字母序列。这一点为稳恒信源的研究带来很大的方便。下面我们就来计算离散稳恒信源输出的信息量。

先假设信源字母序列的长度有限, 设为  $N$ , 并用  $(u_1, u_2, \dots, u_N)$  来表示, 那么, 我们可以将该有限长度的序列看成一个随机矢量。该随机矢量的熵可以用联合熵  $H(U_1 U_2 \dots U_N)$  来表示, 于是, 平均每个字母的熵  $H_N(U)$  可以表示为

$$H_N(U) = \frac{1}{N} H(U_1 U_2 \dots U_N) \quad (3.2)$$

当  $N \rightarrow \infty$  时, 若  $H_N(U)$  趋于某一极限, 则定义该极限为信源的熵率, 记作  $H(U)$ , 即

$$H(U) = \lim_{N \rightarrow \infty} H_N(U) \quad (3.3)$$

对于独立稳恒信源, 即无记忆稳恒信源, 前后时刻信源的输出彼此独立, 则有

$$H(U_1 U_2 \dots U_N) = \sum_{i=1}^N H(U_i) = NH(U_i), \quad i = 1, 2, \dots, N \quad (3.4)$$

于是有

$$H(U) = H_N(U) = H(U_i) = H(U_1) = H_1(U) \quad (3.5)$$

对于一般的稳恒信源, 可以证明, 极限  $\lim_{N \rightarrow \infty} H_N(U)$  一定存在。

**定理 3.1** 对于离散稳恒信源, 若  $H_1(U) < \infty$ , 则  $H(U)$  存在, 且有

$$H(U) = \lim_{N \rightarrow \infty} H(U_N | U_1 U_2 \dots U_{N-1}) \quad (3.6)$$

证明 (1) 证明  $H(U)$  的存在性。

根据信源的稳恒性以及无条件熵不小于条件熵的性质, 可知

$$\begin{aligned} H(U_{N-1} | U_1 U_2 \dots U_{N-2}) &= H(U_N | U_2 U_3 \dots U_{N-1}) \\ &\geq H(U_N | U_1 U_2 U_3 \dots U_{N-1}) \end{aligned} \quad (3.7)$$

这说明条件熵  $H(U_N | U_1 U_2 U_3 \dots U_{N-1})$  是随着  $N$  的增大而减小的, 于是, 可以得到

$$\begin{aligned} NH_N(U) &= H(U_1) + H(U_2 | U_1) + \dots + H(U_N | U_1 U_2 \dots U_{N-1}) \\ &= H(U_N) + H(U_N | U_{N-1}) + \dots + H(U_N | U_1 U_2 \dots U_{N-1}) \\ &\geq NH(U_N | U_1 U_2 \dots U_{N-1}) \end{aligned} \quad (3.8)$$

另一方面,又有

$$\begin{aligned} NH_N(U) &= H(U_N | U_1 U_2 \dots U_{N-1}) + H(U_1 U_2 \dots U_{N-1}) \\ &= H(U_N | U_1 U_2 \dots U_{N-1}) + (N-1)H_{N-1}(U) \end{aligned} \quad (3.9)$$

将式(3.9)代入式(3.8)中,得到

$$NH_N(U) = H_N(U) + (N-1)H_{N-1}(U)$$

即

$$H_N(U) = H_{N-1}(U) \quad (3.10)$$

根据熵的非负性以及该定理中的条件  $H_1(U) < \infty$ , 可以推出

$$0 \leq H_N(U) = H_{N-1}(U) < H_1(U) < \infty \quad (3.11)$$

这说明此数列单调有界,故极限  $\lim_{N \rightarrow \infty} H_N(U)$  必存在,且为 0 和  $H_1(U)$  之间的某一有限值。

(2) 证明  $H(U) = \lim_{N \rightarrow \infty} H(U_N | U_1 U_2 \dots U_{N-1})$ 。

我们取

$$\begin{aligned} (N+M)H_{N+M}(U) &= H(U_1 U_2 \dots U_{N-1}) + H(U_N | U_1 U_2 \dots U_{N-1}) + \\ &\quad \dots + H(U_{N+M} | U_1 U_2 \dots U_{N-1} U_N \dots U_{N+M-1}) \end{aligned} \quad (3.12)$$

并反复利用式(3.7),就可以得到

$$(N+M)H_{N+M}(U) = (N-1)H_{N-1}(U) + (M+1)H(U_N | U_1 U_2 \dots U_{N-1})$$

或

$$H_{N+M}(U) = \frac{N-1}{N+M}H_{N-1}(U) + \frac{M+1}{N+M}H(U_N | U_1 U_2 \dots U_{N-1}) \quad (3.13)$$

固定  $N$ , 并令  $M \rightarrow \infty$ , 则得

$$H(U) = H(U_N | U_1 U_2 \dots U_{N-1}) = H_N(U) \quad (3.14)$$

现在令  $N \rightarrow \infty$ , 则有

$$H(U) = \lim_{N \rightarrow \infty} H(U_N | U_1 U_2 \dots U_{N-1}) = \lim_{N \rightarrow \infty} H_N(U)$$

即

$$H(U) = \lim_{N \rightarrow \infty} H(U_N | U_1 U_2 \dots U_{N-1}) = H(U) \quad (3.15)$$

因此,有

$$H(U) = \lim_{N \rightarrow \infty} H(U_N | U_1 U_2 \dots U_{N-1}) \quad \text{证毕}$$

定理 3.1 表明,离散有记忆稳恒信源的输出信号所携带的信息量小于信号可能携带的信息量,如式(3.11)所示。其原因可以从两个方面来解释:

(1) 从式(3.8)可以看到,在长为  $N$  的序列中,各源字母所携带的信息量为

$H(U_n | U_1 U_2 \dots U_{n-1})$  ( $n=1, 2, \dots, N$ )。随着  $n$  的增加, 各源字母所携带的信息量随之减少, 这是统计约束条件不断增加的结果。因此, 信源输出中前后字母之间的统计依存关系是使信号有效携带信息量减少的一个重要原因。

(2) 式(3.10)和式(3.11)告诉我们,  $H_N(U)$  随着  $N$  的减小而不断增大, 其最大值为  $H_1(U)$ 。由熵的极值性可知

$$H_1(U) = \log K$$

其中,  $K$  为源字母表的字母数。因此, 当信源的一维概率分布不均匀时, 即使信源输出信号的前后字母之间不存在统计依存关系(即此时的信源为独立稳恒信源, 其熵率为  $H(U) = H_1(U)$ ), 也不能最大限度地携带信息。

在信息论中, 常用冗余度及相对冗余度来衡量信源输出信号携带信息的有效程度。冗余度越低, 则信源输出信号携带信息的有效性越高, 反之则越低。冗余度及相对冗余度的定义如下:

$$\text{冗余度} = \log K - H(U) \quad (3.16)$$

$$\text{相对冗余度} = 1 - \frac{H(U)}{\log K} \quad (3.17)$$

很多实际的信源都具有相当大的相对冗余度。以语言为例, G. A. Barnard 曾经给出西方几种主要语言的熵率值, 如表 3.2 所示, 其中,  $\log_2 K$  是按照字母表大小为  $K=26$  的情况下计算所得的最大可能值;  $H_1(U)$  是根据各字母的实际概率计算所得的熵, 此时不考虑前后字母的统计依存关系;  $H(W)$  则是按照单词计算所得的平均每个字母的熵值。在英语中, 一个单词所含的平均字母数是 4.5, 而法语、德语、西班牙语的一个单词所含的平均字母数分别为 4.8、5.92 和 4.96。这些数字说明,  $H_N(U)$  的值在  $N=4 \sim 6$  时平均每个字母的熵已有很大的减小。香农曾经统计过, 当  $N=100$  时, 英语  $H_N(U)$  的值仅为 1bit 左右, 这表明英语的相对冗余度至少可达到 80%。一般情况下, 信源的相对冗余度大于 50%。

表 3.2 西方几种主要语言的熵值(单位: bit)

熵	英语	法语	德语	西班牙
$\log_2 K$	4.70	4.70	4.70	4.70
$H_1(U)$	4.124	3.984	4.095	4.015
$H(W)$	1.65	3.02	1.08	1.97

由于信源中存在的这种冗余度, 这就涉及到数据的有效表示——冗余度压

缩。冗余度压缩编码不但具有理论上的意义,而且具有极大的实际应用价值,如语音编码、图像编码等。

### 3.3 离散无记忆信源的渐近等同分割性与信源的定长编码定理

离散无记忆稳恒信源是最简单的一种信源模型,其输出信号是一个离散的独立随机序列。对这一信源其熵率  $H(U)$  即为  $H_1(U)$ , 这一点很容易证明。实际上,由序列中各字母之间的独立性及序列的稳恒性可知

$$\begin{aligned} H_N(U) &= \frac{1}{N} H(U_1 U_2 \dots U_N) \\ &= \frac{1}{N} (H(U_1) + H(U_2) + \dots + H(U_N)) \\ &= \frac{1}{N} N H(U_1) = H(U_1) \end{aligned}$$

所以

$$H(U) = \lim_N H_N(U) = H_1(U)$$

#### 3.3.1 渐近等同分割性

离散无记忆信源有一个重要的性质,这就是渐近等同分割性。这一性质是信源编码的基础,下述定理阐述了信源的这一性质。

**定理 3.2 (渐近等同分割定理)** 设  $\mathbf{u} = u_1 u_2 \dots u_N$  是离散无记忆信源输出的一个特定序列,则任给  $\epsilon > 0$  和  $\delta > 0$ , 总可以找到一个整数  $N_0$ , 使当  $N \geq N_0$  时, 有

$$P \left| \frac{\log P(\mathbf{u})}{N} + H(U) \right| < \epsilon \quad > 1 - \delta \quad (3.18)$$

**证明** 设序列  $\mathbf{u} = u_1 u_2 \dots u_N$  中取字母  $a_k$  值的次数为  $n_k$  ( $k = 1, 2, \dots, K$ ), 由独立随机序列的性质可知

$$P(\mathbf{u}) = \prod_{k=1}^K p(a_k)^{n_k}$$

故

$$\log P(\mathbf{u}) = \sum_{k=1}^K n_k \log p(a_k) \quad (3.19)$$

另一方面,由上已知

$$H(U) = H_1(U) = - \sum_{k=1}^K p(a_k) \log p(a_k) \quad (3.20)$$

所以

$$\frac{\log P(\mathbf{u})}{N} + H(U) = \sum_{k=1}^K \frac{n_k}{N} - p(a_k) \log p(a_k) \quad (3.21)$$

上式中,由于 $\frac{n_k}{N}$ 是序列中 $a_k$ 出现的频率,所以它可以表示成

$$\frac{n_k}{N} = p(a_k) + \epsilon_k \quad (3.22)$$

将式(3.22)代入到式(3.21)中,并令

$$\epsilon_{\max} = \max_k |\epsilon_k| \quad (3.23)$$

即可得到

$$\left| \frac{\log P(\mathbf{u})}{N} + H(U) \right| = \left| \sum_{k=1}^K \epsilon_k \log p(a_k) \right| \leq \sum_{k=1}^K |\epsilon_k| \log p(a_k) \leq \epsilon_{\max} \sum_{k=1}^K \log p(a_k) \quad (3.24)$$

这样,如果在所有可能序列中,有一部分序列其 $\epsilon_{\max}$ 满足

$$\epsilon_{\max} \leq \frac{1}{\sum_{k=1}^K \log p(a_k)}, \quad \epsilon_{\max} > 0 \quad (3.25)$$

则该序列 $\mathbf{u}$ 即能满足

$$\left| \frac{\log P(\mathbf{u})}{N} + H(U) \right| < \epsilon_{\max} \quad (3.26)$$

我们把满足条件(3.26)的序列称为典型序列,并将典型序列的集合记作 $G$ ,即

$$G = \{ \mathbf{u} : \left| \frac{\log P(\mathbf{u})}{N} + H(U) \right| < \epsilon_{\max} \}$$

不满足条件(3.25)的序列的集合记为 $G_c$ 。显然, $G$ 的补集 $G^c$ 是 $G_c$ 的子集, $G^c \subset G_c$ 。下面来估计序列落入两个集合 $G$ 和 $G_c$ 中的概率。

对于集合 $G$ ,其中的序列不满足式(3.25),即至少存在一个值 $l$ ,使



$$\left| \frac{n_l}{N} - p(a_l) \right| \leq \max_{l=1, \dots, K} \left| \frac{n_l}{N} - p(a_l) \right| \quad (3.27)$$

如果把发生式(3.27)的情况记作事件  $E_l$ , 则  $G$  中所有序列的概率之和为

$$P \left( \bigcup_{l=1}^K E_l \right) = \sum_{l=1}^K P(E_l) \leq K \max_{l=1, \dots, K} P(E_l) \quad (3.28)$$

但按照大数定律, 当  $N$  足够大时, 对于任何  $l$  值总可以有一个整数  $N_0$ , 使当  $N > N_0$  时, 有

$$P(E_l) = P \left( \left| \frac{n_l}{N} - p(a_l) \right| \geq \frac{\epsilon}{K} \right) < \frac{1}{K}, \quad \epsilon > 0 \quad (3.29)$$

即  $\frac{n_l}{N}$  依概率收敛到  $p(a_l)$ 。这样我们就得到  $G$  中序列的概率之和小于 1, 即

$$P \left( \bigcup_{l=1}^K E_l \right) < 1$$

所以  $G$  中序列的概率之和大于  $1 - \epsilon$ , 此结论即为式(3.18)。

在证明过程中,  $\epsilon$  和  $K$  都是任意给定的, 所以不难明白, 我们可以取  $\epsilon = \frac{1}{K}$ , 此时定理依然成立。证毕

在上述定理的基础上我们就可以来证明离散无记忆信源的定长编码定理。

### 3.3.2 定长编码定理

所谓定长编码我们在节 3.1 中已有大致介绍, 在这里定长编码是定长到定长分组编码的简称。设离散无记忆信源的源字母表为  $\{a_1, a_2, \dots, a_K\}$ , 字母总数为  $K$ ; 码字母表为  $\{b_1, b_2, \dots, b_J\}$ , 字母总数为  $J$ 。则定长编码就是将长为  $N$  的源字母组映射为长为  $M$  的码字母组, 或者说把长为  $N$  的源字映射为长为  $M$  的码字, 如图 3.3 所示。

定长编码的这一编码过程有时可以利用扩展信源的概念而有一种更简单的理解方法。所谓离散无记忆信源的  $N$  次扩展信源是这样一信源: 设原信源的字母表为  $\{a_k, k=1, 2, \dots, K\}$ , 相应的概率分布为  $\{p(a_k), k=1, 2, \dots, K\}$ , 则该离散无记忆信源的  $N$  次扩展信源也是一个无记忆信源, 其字母表有  $K^N$  个字母, 每个扩展源字母各对应  $N$  个原信源字母, 而扩展源字母的概率即为其对应的  $N$  个原信源字母的概率之积, 可以证明  $H(X^N) = NH(X)$ 。扩展信源的概念是 N. Abramson 首先引入的。

利用这一概念, 我们可以把前述定长一定长分组编码看成是用长为  $M$  的码

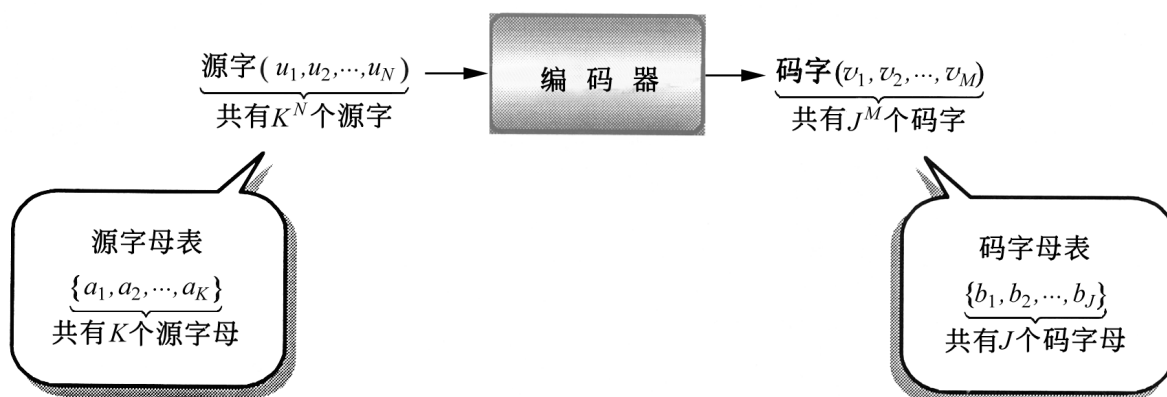


图 3.3 定长编码示意图

字对  $N$  次扩展信源的每个源字母进行编码, 就像在 ASCII 码中我们用长 8 位的二元数字对英文字母、阿拉伯数字和各种符号进行编码那样。利用这种定长编码, 我们可以对离散无记忆信源输出的冗余度进行压缩, 或者确切地说, 我们可以利用定长编码使信源输出的几乎所有序列都可以用新的与各序列对应的码字母序列来表示。这样, 编码输出的码字母序列就带有与信源字母序列相同的信息量而其冗余度则可以大大减少, 或在理想情况下得到零冗余度。下面的离散无记忆信源定长编码定理以定理形式给出了上述结论。

**定理 3.3** 设熵率为  $H(U)$  的离散无记忆信源被分成长  $N$  的源字母组, 并用长为  $M$  的码字母组进行编码, 码字母表的大小为  $J$ 。则对任给的数  $\epsilon > 0$  和  $\delta > 0$ , 只要  $N$  足够大, 且满足不等式

$$\frac{M}{N} \log J > H(U) + \epsilon \quad (3.30)$$

则源字母组没有自己特定码字的概率  $P_0$  可以小于  $\delta$ 。

**证明** 由渐近等同分割定理 3.2, 离散无记忆信源输出中典型序列的概率满足条件

$$2^{-N(H(U) + \epsilon)} > P(\mathbf{u}) > 2^{-N(H(U) - \epsilon)} \quad (3.31)$$

设典型序列集合  $G$  中的序列数目为  $N_G$ , 则有

$$\begin{aligned} 1 &= \sum_{\mathbf{u} \in G} P(\mathbf{u}) > N_G 2^{-N(H(U) + \epsilon)} \\ N_G 2^{-N(H(U) - \epsilon)} &> \sum_{\mathbf{u} \in G} P(\mathbf{u}) > 1 - \delta \end{aligned}$$

所以典型序列集合  $G$  中的序列数目  $N_G$  为

$$N_G < 1 / 2^{-N(H(U) + \epsilon)} = 2^{N(H(U) + \epsilon)}$$

根据该定理的条件(3.30), 我们可以选择  $\epsilon$ , 使其满足

$$M \log J = N(H(U) + \epsilon)$$

此即

$$J^M = 2^{N(H(U) + \epsilon)} \quad (3.32)$$

其中,  $J^M$  是可能码字的总数。此式说明对典型序列集合中的每一序列至少可以有一个对应的码字。留下来的只是集合  $G$  中序列, 它们有可能分不到码字。但是, 根据渐近等同分割定理 3.2, 当源字母序列长度  $N$  足够大时,  $G$  中序列的概率之和可以小于任给值  $\epsilon$ , 因此信源字母组没有自己特定码字的概率  $P_0$  可以小于  $\epsilon$ 。证毕

我们在前面给出的渐近等同分割定理和定长编码定理是在离散无记忆信源这种最简单信源的条件下证明的, 但在其他若干种信源的情况下也有类似的定理。证明各种情况下的这两条定理是信源研究中重要的理论问题, 由于本书的性质, 在本书中我们将不在更一般的信源下给出证明。但顺便指出, 渐近等同分割定理在信息论中又称熵定理或遍历性定理, 对稳恒遍历信源类似的结果则被称为 Shannon-McMillan 定理。基于这一定理, 还可以证明稳恒遍历信源下的定长编码定理。

定长编码在实际应用时有两个问题。一个是编译码的同步问题, 即如何使译码端知道每一个码字的起点; 另一个是如何有效处理分组长度与编译码复杂性、编译码延时等的关系。

对于第一个问题, 可以有两种办法加以解决。第一种方法是在每个码字前面加上一段很短的同步序列作为码字的前缀, 第二种方法是每隔若干个码字插入一个较长的同步序列。在正确选择同步序列和其他相关参数的情况下, 这两种方法所付出的代价都可以很小。

对于第二个问题, 为了使编码真正有效, 信源输出序列的分组长度必须很大, 这导致编译码的延时和编译码器复杂性的增加。人们曾经企图通过对分组长度和译码差错率之间关系的分析来为工程上的折衷设计方案提供依据, 但实际上却仍很难采用。由于该问题没有理想的解决办法, 所以定长编码在信源冗余度压缩编码中的理论意义远大于其实用价值。与此相反, 我们在下面要讨论的变长编码和树码在冗余度压缩编码中的理论意义虽不如定长编码, 但却具有很大的实用价值。

### 3.4 离散无记忆信源的变长编码

我们已经知道, 离散无记忆信源的冗余度是由于信源字母的概率分布不均

匀造成的。当用等概的码字母组对源字母组进行定长编码时,为了使编码有效,源字母组的长度必须很大才行。这在实际应用中很难实现。为了解决这一难题,可以采用可变长度的码字母组去适应不同概率的源字母组或源字母。

由定长的源字母组到变长的码字母组的分组编码简称变长编码。电报中的 Morse 码就是一种常见的变长编码。

码字长度可变带来的问题是如何使变长编码的译码器能对码字母序列进行正确的分组,以确保译码器能有唯一正确的译码输出。

我们知道,在与变长码类似的英文等语言文字中,正确的分组是靠空格和标点符号来完成的。但是,在编码器中却不能依靠这种特殊的符号,因为这样一来会引入附加的冗余度。不使用特殊符号却又能使译码器对码字母流进行正确分组的码是唯一可译码。

唯一可译码的定义是这样的:对任何一个有限长度的信源字母序列,如果编码得到的码字母序列不与其他任何信源字母序列所对应的码字母序列相同,则称这样的码为唯一可译码。

例如,对于源字母个数为 8 的信源,可以用二元数字 0 和 1 直接对源字母进行编码,构成唯一可译码,如表 3.3 所示。

表 3.3 一种唯一可译码

源字母	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$	$a_6$	$a_7$	$a_8$
码字	00	01	11	100	10100	10101	10110	10111

实现唯一可译码的一个重要方法是使码字本身含有标点符号的作用,能自动指示码字的结束。下面讨论的前缀码就是具有这种性质的一种码。

### 3.4.1 前缀码与 Kraft 定理

在一个变长码中,若没有任何一个码字是其他码字的前缀,则这一变长码称为前缀码。前缀码可以用树图清楚地表示出来,以上述例子为例,可以得到如图 3.4 所示的树图。

从图中可以看出,该码的码字全部对应于树的叶子,正好满足所有码字非其他码字的前缀这一约束条件,所以该码是一个前缀码。

怎样才能构造前缀码呢?前缀码存在的条件是什么?下面的 Kraft 定理可

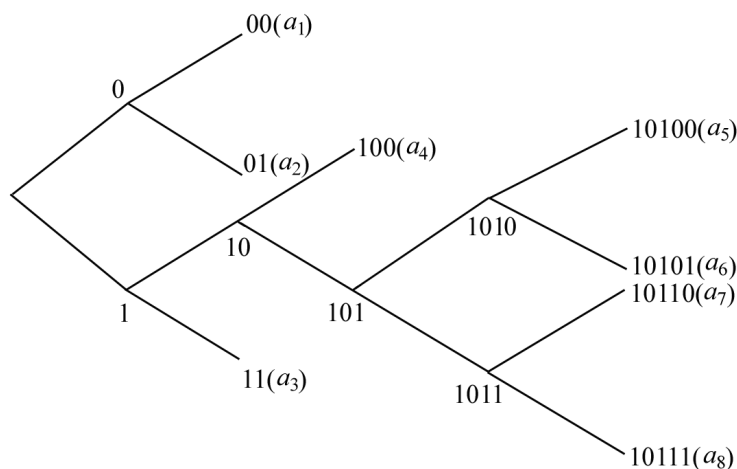


图 3.4 前缀码的树图

以回答该问题。

**定理 3.4 (Kraft 定理)** 设含有  $K$  个信源字母的信源要用  $J$  个字母的码字母表进行变长编码, 则当且仅当各码字的长度  $l_1, l_2, \dots, l_K$  满足 Kraft 不等式

$$\sum_{k=1}^K J^{-l_k} \leq 1 \quad (3.33)$$

时才存在前缀码。

**证明** (1) 必要性。由于前缀码总可以放在一棵树上, 所以可取一个有  $l$  层的  $J$  叉树, 且

$$l \geq \max_k l_k$$

树的第 0 层为根, 在第  $l$  层上共有  $J^l$  个结点。于是, 长为  $l_k$  的码字相当于砍去该  $J$  叉整树第  $l$  层上的  $J^{l-l_k}$  个结点, 所以  $K$  个码字总共砍去的第  $l$  层的结点数必小于  $J^l$ , 即

$$\sum_{k=1}^K J^{l-l_k} < J^l$$

也就是

$$\sum_{k=1}^K J^{-l_k} < 1$$

(2) 充分性。现假设码字长度满足  $l_1, l_2, \dots, l_K$ 。由于这只影响码字的标号, 所以总是可以的。我们可以从深度为  $l$  的  $J$  叉树的根出发, 在  $l_1$  层上取一个结点作为码字, 并随即去掉这一结点以后的树枝。由于在  $l_1$  层上共有  $J^{l_1}$  个结点, 所以这一步就砍掉了  $J^{l-l_1}$  个叶子, 而剩下  $J^l - J^{l-l_1}$  个叶子。如此下去, 到  $l_k$  层时, 取其上的一个结点作为码字, 并去掉该结点以后的树枝, 则又将砍掉

$J^{l-l_k}$  个叶子, 到此为止, 应该还剩下

$$J^l - J^{l-l_1} - J^{l-l_2} - \dots - J^{l-l_k}$$

个叶子。当到  $l_K$  层时, 应该还剩下

$$J^l - \sum_{k=1}^K J^{l-l_k}$$

个叶子。

由定理给出的条件

$$\sum_{k=1}^K J^{l_k} = 1$$

可以得到

$$J^l - \sum_{k=1}^K J^{l-l_k} = 0$$

所以, 可以按照上述方法构造得到前缀码。

证毕

由 Kraft 定理可知, 给定  $K, J$ , 只要允许码字长度可以足够长, 就总可以满足 Kraft 不等式, 从而得到前缀码。因此, Kraft 不等式只是对前缀码的码字长度的下界给出某种限制。

### 3.4.2 唯一可译码定理

Kraft 不等式给出的限制也是所有唯一可译码都必须满足的。

**定理 3.5** 任何唯一可译码均满足 Kraft 不等式, 即

$$\sum_{k=1}^K J^{l_k} = 1$$

其中,  $K, J$  分别是源字母和码字母的总数,  $l_k (k=1, 2, \dots, K)$  是唯一可译码的码字长度。

**证明** 设  $r$  是一个正整数, 并取

$$\begin{aligned} \sum_{k=1}^K J^{l_k} &= \sum_{k_1=1}^K J^{l_{k_1}} \sum_{k_2=1}^K J^{l_{k_2}} \dots \sum_{k_r=1}^K J^{l_{k_r}} \\ &= \sum_{k_1=1}^K \sum_{k_2=1}^K \dots \sum_{k_r=1}^K J^{(l_{k_1} + l_{k_2} + \dots + l_{k_r})} \end{aligned}$$

其中  $l_{k_1} + l_{k_2} + \dots + l_{k_r}$  可以看成是由  $r$  个码字组成的序列中的码字母总数。当  $k_1, k_2, \dots, k_r$  分别取  $1 \sim K$  之间的各种值时就产生了  $r$  个码字可能构成的全部

序列。

设这些序列中含有  $i$  个码字母的序列数为  $r_i$ , 则  $i$  的值必为  $i \in [1, r_{l_{\max}}]$ , 其中  $l_{\max} = \max_k l_k$ 。故有

$$\sum_{k=1}^K J^{-l_k} = \sum_{i=1}^{r_{l_{\max}}} r_i J^{-i} \quad (3.34)$$

根据定理条件, 该码是唯一可译码, 则这些码字母序列一定互不相同, 即长为  $i$  个码字母的序列的总数  $r_i$  不可能超过  $J^i$ , 于是有

$$\sum_{k=1}^K J^{-l_k} = \sum_{i=1}^{r_{l_{\max}}} J^i J^{-i} \leq \sum_{i=1}^{r_{l_{\max}}} J^{-i} = (J^{-1})^{r_{l_{\max}}} \quad (3.35)$$

令  $r = r_{l_{\max}}$ , 则上面的不等式的右端趋于 1, 即任何唯一可译码均满足 Kraft 不等式。证毕

该定理表明, 对任何唯一可译码均可在不改变码字长度的条件下得到相应的前缀码。也就是说, 为使唯一可译码具有前缀码的性质, 不会给码字长的下界增加限制。

## 3.5 变长编码的平均码长与最优编码

### 3.5.1 变长编码的平均码长

在上节中, 我们知道了任何唯一可译码均满足 Kraft 不等式(3.33)。由前缀码的树图表示, 我们发现, 如果信源字母的概率恰好取  $J^{-l_k}$  ( $k = 1, 2, \dots, K$ ), 即

$$\begin{matrix} a_1 & a_2 & \dots & a_K \\ J^{-l_1} & J^{-l_2} & \dots & J^{-l_K} \end{matrix}$$

则对该信源编码时只要选用有  $J$  个字母的码字母表, 并对概率为  $J^{-l_k}$  ( $k = 1, 2, \dots, K$ ) 的源字母给予长为  $l_k$  的码字, 即使可以使码字长度与源字母概率得到完全的适配, 从而使信源的冗余度得到理想的压缩。

一般情况下, 源字母概率分布不可能满足上述要求, 此时变长编码的性能就会有所下降, 且编码方法也因此而复杂起来。不过, 其基本原则仍然是高概率的源字母所对应的码字长度短, 低概率的源字母所对应的码字长度长。

前缀码的性能一般用平均码长来衡量, 平均码长越短, 前缀码的性能越好。

**定理 3.6** 当用  $J$  个字母的码字母表对熵率为  $H(U)$  的离散无记忆稳恒

信源进行变长编码时,若概率为  $p(a_k)$  的信源字母所对应的码字长为  $l_k$ , 则前缀

码的平均码长  $\bar{l} = \sum_{k=1}^K l_k p(a_k)$  必须满足

$$\bar{l} \geq \frac{H(U)}{\log J} \quad (3.36)$$

另一方面,必可以找到前缀码,使其平均码长满足

$$\bar{l} \leq \frac{H(U)}{\log J} + 1 \quad (3.37)$$

证明 由已知可得

$$\begin{aligned} H(U) - \bar{l} \log J &= H(U) - \sum_{k=1}^K l_k p(a_k) \log J \\ &= - \sum_{k=1}^K p(a_k) \log p(a_k) - \log J \sum_{k=1}^K l_k p(a_k) \\ &= \sum_{k=1}^K p(a_k) \log \frac{J^{-l_k}}{p(a_k)} \end{aligned}$$

考虑取自然对数的情形,则有  $\log x = x - 1$ , 代入上式, 可得

$$H(U) - \bar{l} \log J = \sum_{k=1}^K p(a_k) \left( \frac{J^{-l_k}}{p(a_k)} - 1 \right) = \sum_{k=1}^K J^{-l_k} - \sum_{k=1}^K p(a_k)$$

对上式应用 Kraft 不等式, 则有

$$H(U) - \bar{l} \log J \leq 1 - 1 = 0$$

即式(3.36)成立。

另一方面,若我们取码字长  $l_k$ , 使其满足

$$J^{-l_k} \geq p(a_k) \quad J^{-(l_k-1)}, \quad k = 1, 2, \dots, K \quad (3.38)$$

对上式的左边不等式求和, 则有

$$\sum_{k=1}^K J^{-l_k} \geq \sum_{k=1}^K p(a_k) = 1$$

也就是说, 这种编码方法满足 Kraft 不等式, 所以, 用其构造前缀码是可能的。

对式(3.38)的右边不等式求和, 则有

$$\sum_{k=1}^K p(a_k) \log p(a_k) < \sum_{k=1}^K p(a_k) \log J^{-(l_k-1)}$$

即

$$-H(U) < \sum_{k=1}^K p(a_k)(1 - l_k) \log J = (1 - \bar{l}) \log J$$

所以, 平均码长满足式(3.37)。

证毕



值得指出的一点是上述定理 3.6 是在对信源字母直接进行变长编码下获得的,这说明在  $H(U)$  较大和  $J$  的值较小(一般  $J$  取 2)时,变长编码与定长编码相比可以更快地获得较好的压缩效果,这对实际应用是很有价值的。

此外,在极限性能方面变长编码和定长编码有相同的效果。这一点不难证明。事实上,定长编码定理告诉我们,定长码长  $M$  应该满足

$$M > \frac{NH(U)}{\log J}$$

其中,  $M$  实际上是对  $N$  次扩展信源的源字母所对应的码字长度,那么,对于原信源字母所对应的码字长度应为

$$\frac{M}{N} > \frac{H(U)}{\log J} \quad (3.39)$$

对于变长编码,如果我们对原信源的  $N$  次扩展信源进行编码,则按照定理 3.6,有

$$\bar{l}_N \geq \frac{NH(U)}{\log J}, \quad \bar{l}_N < \frac{NH(U)}{\log J} + 1$$

其中,  $\bar{l}_N$  是  $N$  次扩展信源的源字母所对应的平均码长,  $NH(U)$  是  $N$  次扩展信源的熵率。这一平均码长折算到原信源时可得平均码长为

$$\bar{l} = \frac{\bar{l}_N}{N} \geq \frac{H(U)}{\log J}, \quad \bar{l} = \frac{\bar{l}_N}{N} < \frac{H(U)}{\log J} + \frac{1}{N} \quad (3.40)$$

这样,只要  $N$  足够大,我们就可以使  $\bar{l}$  与  $H(U)/\log J$  的值无限接近。因而,变长编码具有与定长码相同的极限性能。

### 3.5.2 最优编码

对于一般情况下系统地构造前缀码的问题香农曾经提出过一种方法,被称为香农码。1959 年, Gilbert 和 Moore 也提出过一种方法。但目前获得广泛应用的是 Huffman 早在 1952 年提出的方法,后来被称为 Huffman 码。Huffman 码建立在下面两个定理的基础上。对于这两个定理,我们将在码字母表为二元数字的情况下给出证明,但这一证明不难推广到码字母表具有任意多个码字母的情况。

**定理 3.7** 对每一给定的离散无记忆信源,存在一个最优的二元前缀码。这个码中最少发生的两个码字必具有相同的长度,且码中相同长度的码字有两个或两个以上时,其中必有两个码字的差别只在最后一位。

证明 设该离散无记忆信源的源字母有  $K$  个, 其字母表为  $\{a_1, a_2, \dots, a_K\}$ , 经适当排序后, 各源字母的发生概率为  $p(a_1), p(a_2), \dots, p(a_K)$ 。对此信源作二元变长编码, 则最优的前缀码的码字长必满足  $l_1, l_2, \dots, l_K$ , 其中, 字母  $a_k$  对应的码字长为  $l_k, k=1, 2, \dots, K$ 。因为, 如果存在着值  $m$  和  $n$ , 且  $1 \leq m < n \leq K$ , 使  $l_m > l_n$ , 而  $p(a_m) > p(a_n)$ , 则将两个信源字母对应的码字作一下对换, 就能得到平均码长更短的前缀码。这与我们假定前者为最优前缀码相矛盾, 是不可能的。

对于最少发生的两个码字, 其码字长度必定是最长的两个。如果这两个码字的长度不相等, 则按照前缀码中不存在码字为前缀的条件, 一定可以将这二者中较长码字的末位码字母去掉, 从而构成一个平均码长更短的前缀码。这与假设前者为最优前缀码相矛盾, 故最少发生的两个码字一定等长。

最后, 若在这些等长的码字中, 即使不考虑最后一位, 它们的组成也各不相同, 则可以去掉这些码字的最后一位, 而得到仍能互相区别、且不会与更短码字一致的码字, 这样一来得到的码将比原来的码更优。这又与假设矛盾。证毕

在定理 3.7 的证明过程中, 该定理并没有直接告诉我们编码的全过程, 只告诉我们对于最优的二元前缀码, 最小概率的两个码字等长, 且差别只在最后一位。实际上, 这已经告诉我们如何给出概率最小的两个码字的最后一位, 而这两个等长码字中相同部分的最后一位可以通过以下缩减信源的方法得到。

缩减信源是指由原信源缩减得到的信源, 其字母表为  $\{a_1, a_2, \dots, a_{K-1}\}$ , 且字母的发生概率为

$$\begin{aligned} p(a_k) &= p(a_k), \quad k = 1, 2, \dots, K-2 \\ p(a_{K-1}) &= p(a_{K-1}) + p(a_K) \end{aligned} \quad (3.41)$$

对此缩减信源应用定理 3.8, 就可以得到  $a_{K-1}$  所对应码字的最后一位, 此即  $a_{K-1}$  和  $a_K$  所对应码字的相同部分的最后一位。反复利用缩减信源的办法, 就可以得到所要的全部码字。该方法可用下述定理表述。

**定理 3.8** 设  $C$  是某信源经缩减后所得的缩减信源的最优前缀码, 将  $C$  中由原信源中的最小概率的两个字母缩减得到的字母所对应的码字后各加 0 和 1, 作为原信源的最小概率的两个码字, 而其余码字不变, 则这样得到的码  $C$  对原信源也是最优的。

证明 按照信源与缩减信源的关系,  $C$  和  $C$  应满足关系

$$\begin{aligned} l_k &= l_k, \quad k = 1, 2, \dots, K-2 \\ l_k &= l_{K-1} + 1, \quad k = K-1, K \end{aligned} \quad (3.42)$$

其中  $C$  码的平均码长为

$$\begin{aligned}\bar{l} &= \sum_{k=1}^{K-2} p(a_k) l_k + (l_{K-1} + 1)(p(a_{K-1}) + p(a_K)) \\ &= l + p(a_{K-1}) + p(a_K)\end{aligned}\tag{3.43}$$

而对缩减信源, 码  $C$  为最优码,  $\bar{l}$  为最短。另一方面, 由于  $p(a_{K-1}) + p(a_K)$  与码  $C$  无关, 所以码  $C$  的  $\bar{l}$  也应为最短。

反证: 假设该信源有最优码, 取平均码长为  $\bar{l}_{\min}$ , 且

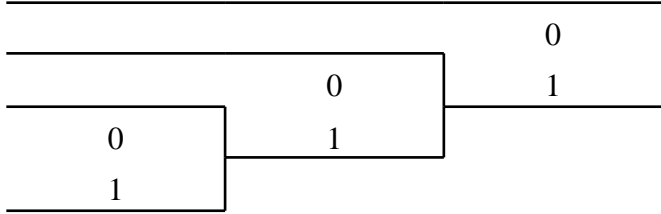
$$\bar{l}_{\min} < \bar{l}$$

则按照定理 3.7, 应有

$$\bar{l}_{\min} = \bar{l} + p(a_{K-1}) + p(a_K) < \bar{l} = \bar{l} + p(a_{K-1}) + p(a_K)$$

故  $\bar{l} < \bar{l}$ , 这与假设  $\bar{l}$  为码  $C$  的平均码长, 且  $\bar{l}$  为最短矛盾。因此,  $\bar{l}$  应为最短, 即码  $C$  为最优码。 证毕

**例 3.1** 对下列离散无记忆稳恒信源进行 Huffman 编码:

信源字母	概 率	码 字	编 码 过 程
$a_1$	1/2	0	
$a_2$	1/4	10	
$a_3$	1/8	110	
$a_4$	1/8	111	

解 该信源的熵率为

$$H(U) = H_1(U) = - \sum_{k=1}^K p(a_k) \log p(a_k) = 7/4 \text{ bit/字母}$$

按照定理 3.7 和定理 3.8 对该信源进行 Huffman 编码, 其编码过程如上所示。Huffman 编码后的平均码长为

$$\bar{l} = \sum_{k=1}^K p(a_k) l_k = 7/4$$

则可得编码后的相对冗余度, 即

$$\text{相对冗余度} = 1 - \frac{H(U)}{\log J} = 1 - \frac{7/4}{(7/4) \log 2} = 0$$

这相当于用 Huffman 变长编码后得到理想的冗余度压缩。

该信源之所以在用 Huffman 编码时取得理想的压缩效果, 是因为各信源字

母的概率刚好取  $J^{-l_k}$  的形式(这里  $J=2$ ), 从而使码的平均长度  $\sum_{k=1}^K p(a_k) l_k$  在数值上与信源的熵率  $-\sum_{k=1}^K p(a_k) \log p(a_k)$  一致。一般情况下,  $-\log p(a_k)$  并不取整数, 为了达到理想的压缩效果, 可以使用扩展信源, 如节 3.5.1 所讨论的那样, 在  $N$  时达到理想的压缩。

若对该信源字母进行定长编码, 则定长码长为 2, 大于变长编码的平均码长  $7/4$ 。可见变长编码比定长编码有效。但是, 由于变长编码器的输出速率不恒定, 为了在传统的恒速信道上使用, 必须增加缓存器, 从而导致一定的传输时延。

对最优编码需要说明以下几点:

(1) 最优编码并非唯一, 这是因为编码时 0 和 1 是任意给的, 同时在两个或两个以上的字母有相等概率时, 缩减的顺序不唯一。通常, 在平均码长  $\bar{l}$  相同的情况下, 应该选择码长方差较小的码。

(2) 最优编码是针对稳恒信源的, 且已知信源的统计特性。实际中, 信源一般非稳恒, 因此必须采取自适应措施, 跟踪信源的统计特性, 使最优编码的性能适应信源统计特性的变化。

## 3.6 离散无记忆信源的变长树码

前面我们提到, 当  $-\log p(a_k)$  不为  $\log J$  的整数倍时, 变长编码也要通过扩展信源的办法来改进压缩效果, 这自然会使编译码复杂化。解决这一问题的另一种途径就是采用树码。

在树码中, 编码器将输入的半无限长的信源字母序列映射为半无限长的码字母序列, 而从码字母序列中无法单独分出码字。对离散无记忆信源树码的一种具体编码方法是由 P. Elias 最早在一篇未发表的研究报告中提到的, 后经 F. Jelinek, J. Rissanen 等的改进和发展而进入实用, 现在人们一般称之为算术码(arithmetic coding)。

### 3.6.1 算术码

算术码的主要概念是把信源输出序列的概率和实数段  $[0, 1)$  中的一个数联系起来。在 Elias 最早提出的方法中, 这一联系过程如下所述。

设信源字母表为 $\{a_0, a_1\}$ , 其发生概率为  $p(a_0) = 0.6$ ,  $p(a_1) = 0.4$ 。按照这两个概率, 先将 $[0, 1)$ 分成两个与概率比例相应的区间, 即 $[0, 0.6)$ 和 $[0.6, 1)$ 。当信源输出的第一个字母  $u = a_0$  时, 数  $x$  的值处在区间 $[0, 0.6)$ 中; 若  $u = a_1$ , 则  $x$  的值处在区间 $[0.6, 1)$ 中。根据信源字母  $u_1$  的情况, 可以把  $x$  所在的段再次按概率比例分成两小段, 即:

$$[0, 0.36) \text{ 和 } [0.36, 0.6), \text{ 若 } u = a_0$$

或者

$$[0.6, 0.84) \text{ 和 } [0.84, 1), \text{ 若 } u = a_1$$

根据信源输出的第二个字母  $u_2$  的取值情况, 可以更精确地确定出数  $x$  所在的区间位置。在信源输出第  $n-1$  个符号后, 若  $x$  所在的位置为

$$[A_{n-1}, B_{n-1})$$

则当信源输出的第  $n$  个符号为  $u_n = a_0$  时, 有

$$\begin{aligned} A_n &= A_{n-1} \\ B_n &= A_{n-1} + 0.6(B_{n-1} - A_{n-1}) \end{aligned} \quad (3.44)$$

当  $u_n = a_1$  时, 有

$$\begin{aligned} A_n &= A_{n-1} + 0.6(B_{n-1} - A_{n-1}) \\ B_n &= B_{n-1} \end{aligned} \quad (3.45)$$

按照这一方法, 序列的概率刚好等于  $x$  所在区间的长度。随着序列的长度不断增加,  $x$  所在区间的长度就越短, 也就可以更加精确地确定  $x$  的位置。当信源字母序列长度趋于无限时,  $x$  所在区间成为一点。

显然, 上述  $x$  值可以用二进制数来表示, 即可以将信源字母序列表示成码字母表为 $\{0, 1\}$ 的二元树码。很明显, 这一编码是逐步前进的, 当信源输出第  $N$  个

源字母时, 信源字母序列的概率为  $p(u_1 u_2 \dots u_N) = \prod_{n=1}^N p(u_n)$ , 码字输出是此时  $A_N$  和  $B_N$  两点的二进制数表示中一致的部分。此时输出二进制数的位数, 亦即二元树码的长度  $m$  应为

$$\frac{1}{2^m} > \prod_{n=1}^N p(u_n) > \frac{1}{2^{m+1}}$$

在下一次信源字母输入时, 根据  $A_{N+1}$  和  $B_{N+1}$  两点的二进制数表示中一致的部分与上一次相比是否增加而确定编码器是否有新的码字母输出。

从上面的编码过程中可以看出, 对同样长度的信源字母序列输出的码字母序列长度不一定相等。因此, 这是一种变长树码。

上述编码方法可以推广到多个信源字母的情况。例如, 设信源字母表为

$\{a_0, a_1, a_2, a_3\}$ , 相应的概率为  $p(a_0) = 0.4$ ,  $p(a_1) = 0.3$ ,  $p(a_2) = 0.2$ ,  $p(a_3) = 0.1$ 。按照这一概率分布, 可先将  $[0, 1)$  分成四段, 即  $[0, 0.4)$ 、 $[0.4, 0.7)$ 、 $[0.7, 0.9)$  和  $[0.9, 1)$ , 每一段的长度分别对应一个字母的概率。当信源输出第一个字母时, 对应的值落在该字母所对应的区间中, 此后, 这一字母所对应的区间又按照概率值分成四个小区间, 而该位置在信源输出第二个字母时得到更精确的定位。仿照前面介绍的二元树码的编码方法, 可以得到该源字母序列的四元树码。

### 3.6.2 算术码的存在性

算术码的存在性可以用累积概率分布(cumulative distribution)加以说明。

设信源字母表为  $\{a_1, a_2, \dots, a_K\}$ , 字母  $a_k$  的概率为  $p(a_k)$  ( $k = 1, 2, \dots, K$ ), 将字母按其脚标排序, 并记作  $a_1 > a_2 > \dots > a_K$ 。于是, 可以定义字母  $a_k$  的累积概率为

$$F(a_k) = \sum_{a_i > a_k} p(a_i) \quad (3.46)$$

再定义修正的累积概率为

$$\bar{F}(a_k) = \sum_{a_i > a_k} p(a_i) + \frac{1}{2} p(a_k) \quad (3.47)$$

则  $F(a_k)$  和  $\bar{F}(a_k)$  的曲线如图 3.5 所示。

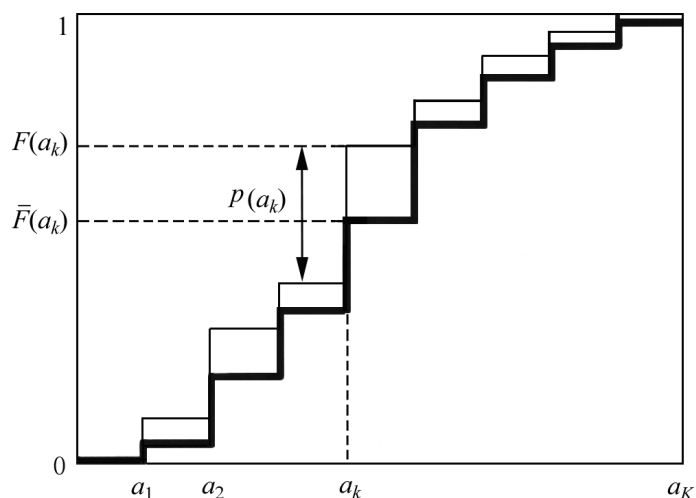


图 3.5 累积概率曲线

有了累积概率, 即可知道相应的源字母, 所以可以将源字母  $a_k$  的累积概率

$\bar{F}(a_k)$  作为其码字。一般情况下,  $\bar{F}(a_k)$  为实数, 若用二进制数精确表示, 则有可能需要无穷多位, 但作为码字只需有足够的位数, 使其能与  $a_k$  一一对应就够了, 所以只需用  $l_k$  位来表示  $\bar{F}(a_k)$ , 即取

$$\lfloor \bar{F}(a_k) \rfloor_{l_k} = 0 \dots\dots$$

则真实值  $\bar{F}(a_k)$  与近似值  $\lfloor \bar{F}(a_k) \rfloor_{l_k}$  之间的误差为

$$\bar{F}(a_k) - \lfloor \bar{F}(a_k) \rfloor_{l_k} < 2^{-l_k} \quad (3.48)$$

取  $l_k = \lceil \log_2 p(a_k)^{-1} \rceil + 1$  时, 有

$$F(a_k) - \bar{F}(a_k) = \frac{p(a_k)}{2} > 2^{-l_k}$$

所以

$$\bar{F}(a_k) - \lfloor \bar{F}(a_k) \rfloor_{l_k} < F(a_k) - \bar{F}(a_k) = p(a_k)/2 \quad (3.49)$$

这说明近似值  $\lfloor \bar{F}(a_k) \rfloor_{l_k}$  处于  $F(a_{k-1})$  与  $F(a_k)$  之间, 故用  $l_k = \lceil \log_2 p(a_k)^{-1} \rceil + 1$  位足以唯一地确定  $a_k$ 。此时, 平均码长为

$$\bar{l} = \sum_{k=1}^K p(a_k) l_k = \sum_{k=1}^K p(a_k) \left\lceil \log \frac{1}{p(a_k)} \right\rceil + 1 < H(X) + 2 \quad (3.50)$$

**例 3.2** 设离散无记忆信源字母表为  $\{a_1, a_2, a_3, a_4\}$ , 字母  $a_k$  的概率为  $p(a_k)$ ,  $k=1, 2, 3, 4$ , 且  $p(a_1) = 0.25$ ,  $p(a_2) = 0.50$ ,  $p(a_3) = 0.125$ ,  $p(a_4) = 0.125$ 。据此可以求出字母  $a_k$  的累积概率  $\bar{F}(a_k)$  和修正的累积概率  $F(a_k)$ , 以及  $\bar{F}(a_k)$  的二进制表示和相应的码字, 如表 3.4 所示。

表 3.4 累积概率及其二进制表示的一种举例

$a_k$	$p(a_k)$	$F(a_k)$	$\bar{F}(a_k)$	$\bar{F}(a_k)$ 二进制表示	$l_k$	码字	Huffman 编码
$a_1$	0.25	0.25	0.125	0.001	3	001	10
$a_2$	0.50	0.75	0.500	0.10	2	10	0
$a_3$	0.125	0.875	0.8125	0.1101	4	1101	110
$a_4$	0.125	1.00	0.9375	0.1111	4	1111	111

此时,  $\bar{F}(a_k)$  的二进制码字的平均码长  $\bar{l} = 2.75 \text{ bit}$ , 而 Huffman 编码的平均码长  $\bar{l}_{\text{Huf}} = 1.75 \text{ bit}$ , 且  $H(U) = H_1(U) = 1.75 \text{ bit}$ 。这说明, 该编码方法有冗余度, 虽然它得到的码字是一种前缀码, 但不是最优的。

**例 3.3** 设离散无记忆信源字母表为  $\{a_1, a_2, a_3, a_4, a_5\}$ , 字母  $a_k$  的概率为  $p(a_k)$ ,  $k=1, 2, 3, 4, 5$ , 且  $p(a_1) = 0.25$ ,  $p(a_2) = 0.25$ ,  $p(a_3) = 0.20$ ,  $p(a_4) =$

0.15,  $p(a_k) = 0.15$ 。据此可以求出字母  $a_k$  的累积概率  $F(a_k)$  和修正的累积概率  $\bar{F}(a_k)$ , 以及  $\bar{F}(a_k)$  的二进制表示和相应的码字, 如表 3.5 所示。

表 3.5 累积概率及其二进制表示的另一种举例

$a_k$	$p(a_k)$	$F(a_k)$	$\bar{F}(a_k)$	$\bar{F}(a_k)$ 二进制表示	$l_k$	码字	Huffman 编码
$a_1$	0.25	0.25	0.125	0.001	3	001	01
$a_2$	0.25	0.50	0.375	0.011	3	011	10
$a_3$	0.20	0.70	0.600	0.10011	4	1001	11
$a_4$	0.15	0.85	0.775	0.1100011	4	1100	000
$a_5$	0.15	1.00	0.925	0.1110110	4	1110	001

此时,  $\bar{F}(a_k)$  的二进制码字的平均码长  $\bar{l} = 3.5\text{bit}$ , 而 Huffman 编码的平均码长  $\bar{l}_{\text{Huf}} = 2.3\text{bit}$ , 且  $H(U) = H_1(U) = 2.285\text{bit}$ 。

在上面两个例子中, 算术编码的效果并不很好, 这是因为仅用算术编码方法对源字母进行编码。若对源字母序列进行编码, 则算术编码有独特的优点, 它可以随着序列长度  $N$  的增加而自然地改进压缩效果。

对于长  $N$  的信源字母序列, 同样可以加以排序。例如有  $v_N = u_1 u_2 \dots u_N$  和  $v_N = u_1 u_2 \dots u_N$ , 若有  $t \leq N$  存在, 使

$$\begin{aligned} u_n &= u_n, & \text{当 } n < t \text{ 时} \\ u_t &> u_t, & \text{当 } n = t \text{ 时} \end{aligned} \quad (3.51)$$

则记  $v_N > v_N$ 。据此排序后, 即可定义序列  $v_N$  的累积概率为

$$F(v_N) = \sum_{v_N > v_N} p(v_N) \quad (3.52)$$

现设序列  $v_N$  后链接  $u_{N+1}$ , 形成新序列  $v_{N+1} = v_N u_{N+1}$ , 则此序列的概率为

$$p(v_{N+1}) = p(v_N) p(u_{N+1}) \quad (3.53)$$

此序列的累积概率为

$$\begin{aligned} F(v_{N+1}) &= \sum_{v_{N+1} > v_{N+1}} p(v_{N+1}) \\ &= F(v_N) + p(v_N) \sum_{u_{N+1} > u_{N+1}} p(u_{N+1}) \\ &= F(v_N) + p(v_N) F(u_{N+1}) \end{aligned} \quad (3.54)$$

由于累积概率随着序列的序严格增加, 所以只要将区间

$$[F(v_N), F(v_N) + p(v_N) F(u_{N+1})]$$



用有限精度的二进制数加以表示,并将此二进制数与  $v_N$  加以对应,就可以实现无失真的编译码。

由于这种情况下码存在的充分条件仍然是 Kraft 不等式,所以在极限情况下,算术码可以实现对信源的理想压缩。

### 3.7 离散马尔可夫信源的熵率

前面我们讨论了离散无记忆信源的熵率,以及一般离散稳恒信源的熵率的极限式。对于一般离散稳恒信源,由于信源某一时刻输出的字母受其以前时刻发出字母的约束,从而使熵减小。这种约束可以追溯至很早以前,甚至无穷远,从而给熵率的计算和编码都带来复杂性。

本节我们将讨论一类相对简单的离散稳恒信源,在这类信源中,信源在某一时刻发出字母的概率除与该字母有关外,只与此前发出的有限个字母有关。若把这有限个字母记作一个状态,则信源发出某一字母的概率除与该字母有关外,只与该时刻信源所处的状态有关。在这种情况下,信源将来的状态及其送出的字母将只与信源现在的状态有关,而与信源过去的状态无关,因为将来的状态只取决于现在的状态及其后发出的字母。换句话说,将来只通过现在与过去发生联系,一旦现在的状态被确定,将来的状态就不会再与过去有联系。这种信源的一般数学模型就是马尔可夫过程,所以称这种信源为马尔可夫信源。

本节只研究时间离散、状态也离散的马尔可夫信源,简称离散马尔可夫信源。在数学中,这种时间离散、状态也离散的马尔可夫过程也称为马尔可夫链。

#### 3.7.1 马尔可夫链的基本概念

下面,我们先对马尔可夫链的性质作一个简单的回顾。

设信源字母表为  $\{a_1, a_2, \dots, a_K\}$ , 信源输出序列为  $u_1 u_2 \dots u_N$ 。若信源输出某一字母的概率与以前的  $m$  个字母有关,则此  $m$  个字母组成的各种可能的序列就对应于信源全部可能的状态  $\{1, 2, \dots, S\}$ , 这里  $S = K^m$ 。信源在各时刻的状态可以组成信源状态序列,记作  $s_1 s_2 \dots s_N$ 。信源在时刻  $n$  由状态  $i$  进入时刻  $n+1$  的状态为  $j$  的概率称为转移概率,记作  $q_{ij}(n)$ , 即

$$q_{ij}(n) = P(s_{n+1} = j | s_n = i)$$

若  $q_{ij}(n)$  与  $n$  的取值无关,则此类马尔可夫链称为时齐马尔可夫链。

马尔可夫链的  $m$  步转移概率  $q_{ij}^{(m)}(n)$  为

$$q_{ij}^{(m)}(n) = P(s_{n+m} = j | s_n = i)$$

对时齐马尔可夫链, 有

$$q_{ij}^{(m)}(n) = q_{ij}^{(m)}$$

$m$  步转移概率满足切普曼—柯尔莫哥洛夫 (Chapman-Kolmogorov) 方程, 即

$$q_{ij}^{(m+r)}(n) = \sum_k q_{ik}^{(m)}(n) q_{kj}^{(r)}(m+n)$$

对时齐马尔可夫链, 有

$$q_{ij}^{(m+r)} = \sum_k q_{ik}^{(m)} q_{kj}^{(r)}$$

时齐马尔可夫链可以用其状态转移图来表示, 图 3.6 是一个有着 6 个状态的时齐马尔可夫链。时齐马尔可夫链中的状态可以根据其性质进行分类。如果状态  $i$  经过若干步后总能到达状态  $j$ , 即存在  $n$ , 使  $q_{ij}^{(n)} > 0$ , 则称  $i$  可到达  $j$ ; 若两个状态相互可到达, 则称此二状态相通; 若一个状态经过若干步以后总能到达某一其他状态, 但不能从其他状态返回, 则称此状态为过渡态, 如图 3.6 中的状态 1; 一个只能从自身返回到自身而不能到达其他任何状态的状态称为吸收态, 如图 3.6 中的状态 6; 若经有限步后迟早要返回的状态称为常返态, 如图 3.6 中的状态 2, 3, 4 和 5; 在常返态中, 有些状态仅当  $n$  能被某整数  $d$  整除时才有  $q_{ii}^{(n)} > 0$ , 则称此状态为周期性的, 如图 3.6 中的状态 4 和 5, 其周期为 2; 对于  $q_{ii}^{(n)} > 0$  的所有  $n$  值, 其最大公约数为 1 的状态称为非周期性的; 非周期的、常返的状态称为遍历状态, 如图 3.6 中的状态 2 和 3。

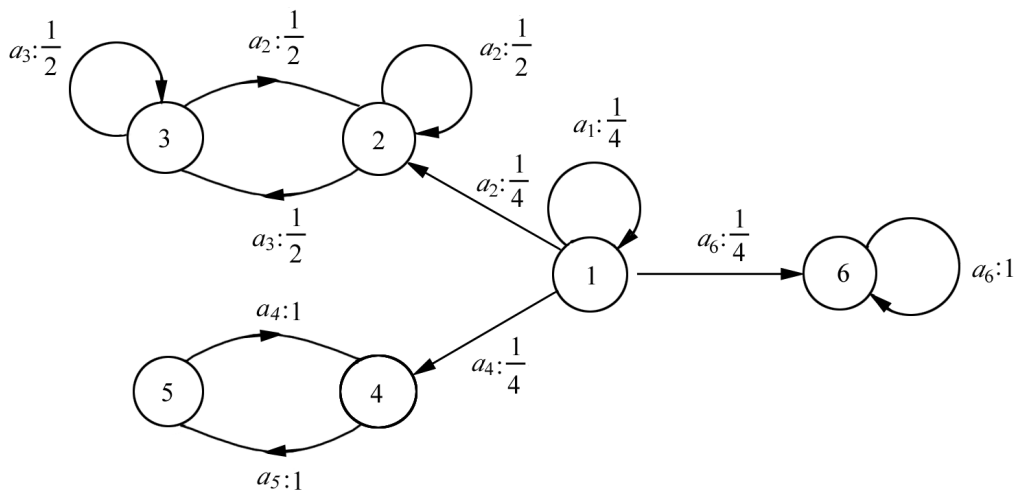


图 3.6 一个时齐马尔可夫链的状态转移图

根据状态空间中状态之间的可达性与相通性,可以对状态空间进行分解。若状态空间中的某一子集中的任何一状态都不能到达子集以外的任何状态,则称该子集为闭集,闭集中除自身全体外再没有其他闭集的闭集称为不可约的或既约的,如 $\{2, 3, 4, 5\}$ ,  $\{2, 3\}$ 和 $\{4, 5\}$ 均是闭集,但只有 $\{2, 3\}$ 和 $\{4, 5\}$ 才是不可约的。当然,任何有限的时齐马尔可夫链的状态集合总可以分解成既约闭集以及过渡态集合、吸收态集合。

一个不可约的、非周期的、状态有限的马尔可夫链,其  $n$  步转移概率  $q_{ij}^{(n)}$  在  $n$  时趋于一个和初始状态无关的极限概率  $p(j)$ , 它是满足方程组

$$p(j) = \sum_i p(i) q_{ij}, \quad \sum_j p(j) = 1$$

的唯一解;称  $p(j)$  为马尔可夫链的一个平稳分布,且  $p(j)$  就是系统此时处于状态  $j$  的概率。所以一个马尔可夫链从一个既约的、遍历的状态集合出发,经过足够长的时间以后,此马尔可夫链是稳恒和遍历的。在此之前,其概率有一段逐渐变化的过渡过程,在过渡过程阶段,需要用转移概率和初始时刻的概率分布来描述。

### 3.7.2 离散马尔可夫信源熵率的计算

离散马尔可夫信源的熵率可以分如下 3 步计算:

(1) 在给定过去某一时刻状态的前提下,计算信源在现时发出一个字母的熵

设过去某一时刻的状态为  $s_1 = i$ , 现在要求  $n$  时刻信源送出字母的熵  $H(U_n | U_1 U_2 \dots U_{n-1}, s_1 = i)$ 。根据条件熵的定义,有

$$\begin{aligned} H(U_n | U_1 U_2 \dots U_{n-1}, s_1 = i) \\ = - \sum_{u_1 u_2 \dots u_n} p(u_1 u_2 \dots u_n | s_1 = i) \log p(u_n | u_1 u_2 \dots u_{n-1}, s_1 = i) \end{aligned} \quad (3.55)$$

由马尔可夫链信源的性质可知,  $s_2$  由  $s_1$  和  $u_1$  确定,  $s_3$  由  $s_2$  和  $u_2$  确定, 等等, 故  $s_n$  可以由  $s_1$  和  $u_1 u_2 \dots u_{n-1}$  确定, 于是得

$$\begin{aligned} p(u_1 u_2 \dots u_n | s_1 = i) &= p(u_1 u_2 \dots u_n, s_n | s_1 = i) \\ &= p(u_1 u_2 \dots u_{n-1}, s_n | s_1 = i) p(u_n | s_n) \end{aligned} \quad (3.56)$$

$$p(u_n | u_1 u_2 \dots u_{n-1}, s_1 = i) = p(u_n | s_n) \quad (3.57)$$

将式(3.56)和式(3.57)代入式(3.55)中,得

$$\begin{aligned}
 H(U_n / U_1 U_2 \dots U_{n-1}, S_1 = i) &= - \sum_{\substack{u_1, \dots, u_n, s_n \\ s}} p(u_1 u_2 \dots u_{n-1}, s_n / S_1 = i) p(u_n / s_n) \log p(u_n / s_n) \\
 &= \sum_{j=1}^S p(s_n = j / S_1 = i) H(U_n / s_n = j) \quad (3.58)
 \end{aligned}$$

对任何给定的  $s_1$  的概率分布都可以得到相应的  $s_n$  的概率分布,所以对式(3.58)中的  $s_1$  取平均即可得

$$H(U_n / U_1 U_2 \dots U_{n-1}, S_1) = \sum_{j=1}^S p(s_n = j) H(U_n / s_n = j) \quad (3.59)$$

对于稳恒遍历过程,  $p(s_n = j)$  将与  $s_1$  的概率分布无关,为平稳分布  $p(j)$ 。同时条件熵  $H(U_n / s_n = j)$  与  $n$  无关,将其记作  $H(U / s = j)$ ,则得

$$H(U_n / U_1 U_2 \dots U_{n-1}, S_1) = \sum_{j=1}^S p(j) H(U / s = j) \quad (3.60)$$

(2) 在给定过去某一时刻状态的条件下,计算信源在其后发出的字母序列的熵率  $\frac{1}{N} H(U_1 U_2 \dots U_N / S_1)$

利用联合熵与条件熵的关系可有

$$\frac{1}{N} H(U_1 U_2 \dots U_N / S_1) = \frac{1}{N} \sum_{n=1}^N H(U_n / U_1 U_2 \dots U_{n-1}, S_1) \quad (3.61)$$

代入式(3.59),有

$$\frac{1}{N} H(U_1 U_2 \dots U_N / S_1) = \frac{1}{N} \sum_{j=1}^S \sum_{n=1}^N p(s_n = j) H(U_n / s_n = j) \quad (3.62)$$

当信源稳恒遍历时,有

$$\frac{1}{N} H(U_1 U_2 \dots U_N / S_1) = \sum_{j=1}^S p(j) H(U / s = j) \quad (3.63)$$

而对一般情况,可定义

$$P_{(1, N)}(j) = \frac{1}{N} \sum_{n=1}^N p(s_n = j) \quad (3.64)$$

则  $S_1$  条件下的信源的熵率为

$$\frac{1}{N} H(U_1 U_2 \dots U_N / S_1) = \sum_{j=1}^S P_{(1, N)}(j) H(U / s = j) \quad (3.65)$$

(3) 求信源的熵率  $H(U)$

因为

$$H(U_1 U_2 \dots U_N) = I(S_1; U_1 U_2 \dots U_N) + H(U_1 U_2 \dots U_N / S_1) \quad (3.66)$$

而又有

$$I(S_1; U_1 U_2 \dots U_N) = H(S_1) - H(S_1 / U_1 U_2 \dots U_N) \\ H(S_1) - \log S$$

故有

$$H(U) = \lim_N \frac{1}{N} H(U_1 U_2 \dots U_N) \\ = \lim_N \frac{1}{N} I(S_1; U_1 U_2 \dots U_N) + \lim_N \frac{1}{N} H(U_1 U_2 \dots U_N / S_1) \\ = \sum_{j=1}^S P_{(1)}(j) H(U / s = j) \quad (3.67)$$

式(3.67)成立是由于

$$\lim_N \frac{1}{N} I(S_1; U_1 U_2 \dots U_N) = 0$$

对稳恒的离散马尔可夫信源, 有  $P_{(1)}(j) = P(j)$ , 则

$$H(U) = \sum_{j=1}^S P(j) H(U / s = j) \quad (3.68)$$

至此, 我们已经计算出了离散马尔可夫信源的熵率。

从上面的计算过程中可以看出, 马尔可夫信源的熵率是由条件熵组成的。与离散无记忆信源相比, 由于马尔可夫信源字母分布不均匀以及信源字母序列前后间的约束关系, 使得马尔可夫信源的熵率更小。

若马尔可夫信源的输出字母概率只与前  $m$  个输出字母有关, 而与更早的输出字母无关, 则称之为  $m$  阶马尔可夫信源。若信源输出的字母总数为  $K$ , 则一般情况下,  $m$  阶马尔可夫信源的状态总数  $S = K^m$ 。显然,  $m$  越高, 对马尔可夫信源的描述会越复杂。

语言文字是马尔可夫信源的实例。以英文为例, 其字母的概率分布不均匀, 且每一字母的产生概率还受其前面字母的影响。那么, 每个字母发生概率到底与前面多少个字母有关呢? 这与精度有关。严格地讲, 这种约束关系可追溯到很远以前, 例如, 当在书籍的一章末尾发现印刷不清或错误之处, 有可能借助本章开头的内容来澄清或纠正。但事实上, 英文字母的发生概率在考虑前 5 个左右字母以后就变化不大了, 这说明用一个 5 阶马尔可夫信源来近似实际的英文信源已足够精确了。

如何选择恰当阶数的马尔可夫信源来近似实际信源是工程上要考虑的重要问题。

### 3.8 离散马尔可夫信源的编码定理与最优编码

在讨论离散无记忆信源的定长编码定理时, 我们已提到对一般的稳恒遍历信源存在类似的定长编码定理。一般情况下稳恒遍历信源的定长编码定理对于稳恒遍历的离散马尔可夫信源也是成立的, 因此利用定长编码定理, 从理论上讲可以实现对离散马尔可夫信源的理想压缩, 本节就不详细介绍了。

离散无记忆信源的变长编码可以很容易地推广到离散马尔可夫信源。

设马尔可夫信源是离散、稳恒、遍历的, 其初始状态为  $s_1 = i$ , 信源输出的序列为  $\mathbf{u} = u_1 u_2 \dots u_N$ 。对于给定的初始状态  $s_1$  下信源输出的每一序列可用变长编码的方法得到一个对应的码字, 其码字长  $L_i(\mathbf{u})$  满足

$$J^{-L_i(\mathbf{u})} P(u_1 u_2 \dots u_N / s_1 = i) < J^{-L_i(\mathbf{u})+1} \quad (3.69)$$

其中  $J$  是码字母总数。此时, 有

$$\sum_{\mathbf{u}} J^{-L_i(\mathbf{u})} P(u_1 u_2 \dots u_N / s_1 = i) = 1 \quad (3.70)$$

即全部序列所对应的所有码字长满足 Kraft 不等式 (这是变长码——唯一可译码存在的必要条件)。因此, 根据变长编码平均码长定理 3.6, 在该初始状态下所得的平均码长  $\bar{L}_i(\mathbf{u}) = N \bar{l}_i$  应该满足

$$\frac{H(U_1 U_2 \dots U_N / s_1 = i)}{\log J} \leq N \bar{l}_i \leq \frac{H(U_1 U_2 \dots U_N / s_1 = i)}{\log J} + 1 \quad (3.71)$$

令  $N \bar{l}_i$  在全部可能的初始状态下取平均, 即得

$$\frac{H(U_1 U_2 \dots U_N / S_1)}{N \log J} \leq \bar{l} \leq \frac{H(U_1 U_2 \dots U_N / S_1)}{N \log J} + \frac{1}{N} \quad (3.72)$$

对稳恒遍历的马尔可夫信源, 有

$$\lim_{N \rightarrow \infty} \frac{1}{N} H(U_1 U_2 \dots U_N / S_1) = \sum_{j=1}^S P(j) H(U / s = j)$$

即

$$H(U) = \sum_{j=1}^S P(j) H(U / s = j)$$

于是有

$$\frac{H(U)}{\log J} \leq \bar{l} \leq \frac{H(U)}{\log J} + \frac{1}{N} \quad (3.73)$$

上述结果可以归纳为马尔可夫信源的变长编码定理。

**定理 3.9** (马尔可夫信源的变长编码定理) 当用  $J$  个字母的码字母表对熵率为  $H(U)$  的离散马尔可夫信源进行变长编码时, 其平均码长  $\bar{l}$  满足

$$\frac{H(U)}{\log J} \leq \bar{l} \leq \frac{H(U)}{\log J} + \frac{1}{N} \quad (3.74)$$

其中  $N$  是信源字母分组的长度。

从马尔可夫信源的变长编码定理可以看出, 当  $N$  足够长时,  $\bar{l}$  可以无限接近  $\frac{H(U)}{\log J}$ , 从而达到理想压缩。

**例 3.4** 图 3.7 是一个离散稳恒遍历马尔可夫信源的状态转移图。此信源有三个字母  $a, b$  和  $c$ , 同时有三种状态 1, 2 和 3, 此信源的一步转移概率如下:

$$q_{11} = \frac{1}{3}, \quad q_{21} = \frac{1}{3}, \quad q_{31} = \frac{1}{3}$$

$$q_{12} = \frac{1}{4}, \quad q_{22} = \frac{1}{2}, \quad q_{32} = \frac{1}{4}$$

$$q_{13} = \frac{1}{4}, \quad q_{23} = \frac{1}{4}, \quad q_{33} = \frac{1}{2}$$

在各种状态下字母  $a, b$  和  $c$  的概率分别为

$$P(a|s=1) = P_1(a) = \frac{1}{3}, \quad P_1(b) = \frac{1}{3}, \quad P_1(c) = \frac{1}{3}$$

$$P(a|s=2) = P_2(a) = \frac{1}{4}, \quad P_2(b) = \frac{1}{2}, \quad P_2(c) = \frac{1}{4}$$

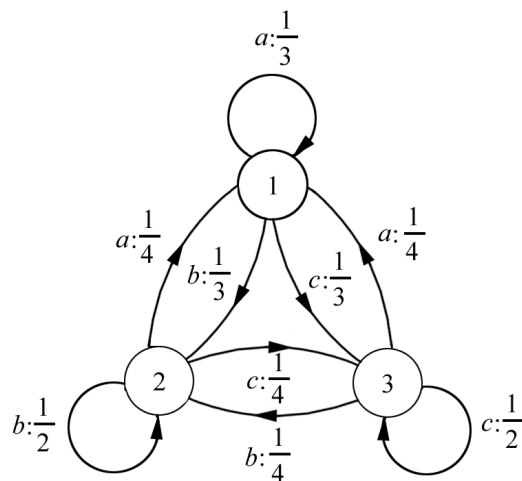
$$P(a|s=3) = P_3(a) = \frac{1}{4}, \quad P_3(b) = \frac{1}{4}, \quad P_3(c) = \frac{1}{2}$$

由该信源的平稳分布方程组

$$\begin{aligned} \sum_{i=1}^3 P(i) q_{ji} &= P(j) \\ \sum_{j=1}^3 P(j) &= 1 \end{aligned}$$

可以解得  $P(1) = \frac{3}{11}$ ,  $P(2) = \frac{4}{11}$ ,  $P(3) = \frac{4}{11}$ 。

稳恒后字母  $a, b, c$  的发生概率分别为



3.7 一个离散稳恒遍历马尔可夫信源的状态转移图示例

$$P(a) = \sum_{i=1}^3 P(i) P_i(a) = \frac{3}{11}$$

$$P(b) = \sum_{i=1}^3 P(i) P_i(b) = \frac{4}{11}$$

$$P(c) = 1 - P(a) - P(b) = \frac{4}{11}$$

则此马尔可夫信源的熵率为

$$\begin{aligned} H(U) &= \sum_{j=1}^3 P(j) H(U | s = j) \\ &= \frac{3}{11} \log 3 + \frac{4}{11} \log 2^{\frac{3}{2}} + \frac{4}{11} \log 2^{\frac{3}{2}} = \frac{16.755}{11} (\text{bit/字母}) \end{aligned}$$

(1) 若将此信源看成无记忆信源, 只对平稳时的字母按其概率进行变长的 Huffman 编码, 则可得

$$\begin{array}{ll} a & 01 \\ b & 00 \\ c & 1 \end{array}$$

此时平均码长为  $\bar{l} = \frac{18}{11}$ 。

(2) 若按马尔可夫信源进行变长编码, 则在不同状态时可得其码字和平均码长如下:

状态 1 时, 有  $a = 1, b = 00, c = 01, \bar{l}_1 = \frac{5}{3}$ ;

状态 2 时, 有  $a = 10, b = 0, c = 11, \bar{l}_2 = \frac{3}{2}$ ;

状态 3 时, 有  $a = 10, b = 11, c = 0, \bar{l}_3 = \frac{3}{2}$ 。

于是总的平均码长为

$$\bar{l} = P(1) \bar{l}_1 + P(2) \bar{l}_2 + P(3) \bar{l}_3 = \frac{17}{11}$$

这说明在考虑了马尔可夫信源的状态条件后, 变长编码的压缩效果得到改善, 且已相当接近理想的极限。

解毕

从原理上讲, 变长树码及其具体的一种实现算法——算术码可以推广到离散马尔可夫信源中。和离散马尔可夫信源下的变长编码一样, 在进行算术编码时必须考虑信源的状态, 即我们必须计算信源序列在各个状态下的条件累积概



率,并据此给出信源序列所相应的码字母序列。

对离散马尔可夫信源进行算术编码的第一个成功实例是由 G.G.Langdon 和 J.Rissanen 在 1981 年给出的,主要用于压缩传真图像。通过对传真的标准测试图像进行压缩的测试,表明其效果比当时最好的算法提高 20% ~ 30%。

从理论上讲,变长树码和定长、变长分组编码一样具有相同的极限性能。

## 习 题

3.1 设  $X_1, X_2, \dots$  为取自分布为  $\begin{matrix} a_1 & \dots & a_K \\ P_1 & \dots & P_K \end{matrix}$  的独立同分布离散随机序列,试求:  $\lim_N [P(X_1, X_2, \dots, X_N)]^{1/N}$ 。

3.2 设  $X_1, X_2, \dots, X_N$  为取自分布为  $\begin{matrix} 0 & 1 \\ 0.25 & 0.75 \end{matrix}$  的独立同分布离散随机序列,试求下列两种情况下序列取典型序列的概率:

(1) 定理 3.2 中的  $\epsilon = 0, N = 100$ 。

(2) 定理 3.2 中的  $\epsilon = 0.05$ 。

3.3 设有一独立增量过程,在整数时刻时发生数值为 +1 或 -1 的增量,增量取 +1 的概率为 0.9,取 -1 的概率为 0.1,其初值以等概取自集合  $\{-1, 0, +1, +2\}$ 。试求此随机过程的熵率。

3.4 设随机变量以等概取  $M$  种可能值。

(1) 试给出此信源的最优二元前缀码;

(2)  $M$  取何值时,平均码字长  $\bar{L} = \log_2 M$ 。

3.5 设有一阶马尔可夫信源,其输出序列  $(\dots, u_{-2}, u_{-1}, u_0, u_1, u_2, \dots)$  经冗余度压缩后为  $(\dots, v_{-2}, v_{-1}, v_0, v_1, v_2, \dots)$ 。试给出最佳压缩方法,并给出压缩前后序列的统计特性。

3.6 设有一个二阶马尔可夫信源  $X$ ,其信源符号集为  $\{0, 1\}$ ,条件概率分别为

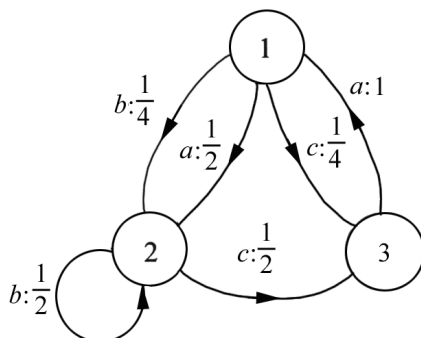
$$p(0/00) = p(1/11) = 0.8$$

$$p(1/00) = p(0/11) = 0.2$$

$$p(0/01) = p(0/10) = p(1/01) = p(1/10) = 0.5$$

试计算此信源的熵率。

3.7 设有马尔可夫信源如下图, 试求:



(1) 信源的熵率;

(2) 信源的有效编码及平均码字长。

3.8 一信源有  $K = x2^j$  ( $j$  为整数,  $1 \leq x \leq 2$ ) 个等概率可取的字母。用二元码字母对此信源字母进行 Huffman 编码, 试求此码的平均码字长 (用  $x, j$  表示)。

3.9 设有独立随机序列  $\{x_n\}$ ,  $p(x_n = 0) = p$ ,  $p(x_n = 1) = q$ , 随机序列  $\{y_n\}$  与  $\{x_n\}$  的关系为  $y_n = x_n \oplus y_{n-1}$ , 其中  $\oplus$  为模 2 和。试求:

(1)  $\{x_n\}$  和  $\{y_n\}$  的熵率  $H(X)$  和  $H(Y)$ ;

(2)  $H(Y) = 1$  bit/符号的条件。

3.10 设离散无记忆信源的字母表为  $\{a_i\}$ ,  $i = 1, 2, \dots, 7$ , 各字母的出现概率分别为 0.3, 0.25, 0.15, 0.1, 0.1, 0.05, 0.05, 试构造二元和三元 Huffman 码。

3.11 设有  $K$  个字母的离散无记忆信源, 熵率为  $H(U)$ , 用三元 (0, 1, 2) 码字母对信源进行 Huffman 编码, 设所得码字的平均长度为  $\bar{l} = \frac{H(U)}{\log_3 3}$ , 试证:

(1) 信源字母的概率均取  $\frac{1}{3^k}$  的形式, 其中  $k$  为整数;

(2)  $K$  为奇数。

3.12 有离散信源  $\begin{matrix} a_1 & a_2 & \dots & a_K \\ p(a_1) & p(a_2) & \dots & p(a_K) \end{matrix}$ , 用二元符号进行编码。

令  $l_k$  为  $a_k$  对应的码字长,  $C_k$  为相应的费用。现要求平均费用  $C = \sum_{k=1}^K p(a_k) C_k l_k$  最小。

(1) 试求最低平均费用  $C_{\min}$ ;

(2) 试证: 在最优编码下, 所得码的费用  $C$  满足不等式

$$C_{\min} \leq C \leq C_{\min} + \sum_{k=1}^K p(a_k) C_k$$

## 第4章 信道、信道容量与信道的有效利用

信息传输的通道(简称信道)是信息论中与信源并列的另一个主要研究对象。在这一章中,我们介绍这方面最成熟的并已获得实际应用的理论成果,这包括信道的建模、信道容量(信道通过信息的能力)以及在不同条件下充分利用信道容量的各种方法。

在对信道建模的讨论中我们只讨论基本的信道,即只有一个输入和一个输出的信道,以及基本信道的级联和并联。信道建模与信源建模一样是以随机过程的理论为基础的,所不同的是现在涉及输入和输出两个随机过程,因此在建模中条件概率或条件概率分布密度函数起着核心的作用。

信道容量是信道研究的核心。借助互信息的概念信息论成功地获得了信道容量的定量的量度。我们将分别讨论离散无记忆信道、连续信道和模拟信道的信道容量。一切不包括电气设备在内的传输信息的物理信道都是模拟信道,所以对模拟信道的信道容量的讨论具有最大的实际意义,因而是我们的最终目标。对离散无记忆信道和连续信道信道容量的研究,其理论价值超过实用价值,但在一定条件下都是有实用意义的。此外,对离散无记忆信道的讨论可以使我们比较容易地掌握信道容量的概念。

信息论对信道容量的分析为充分利用信道的信息传输能力提供了理论的依据,对实际通信系统的设计有巨大的指导意义。我们在本章后部分将比较详细地从各个角度介绍充分利用模拟信道信道容量的各种方法。

### 4.1 信道、信道模型与信道分类

#### 4.1.1 信道

在信息论中,信道是指信息传输的通道。我们在实际通信中所利用的各种物理通道是信道的最典型的例子,如电缆、光纤、电波传布的空间、载波线路等等。除了这些为在空间上将信息进行传输的信道以外,信息论中研究的信道还可包括那些为了在时间上将信息进行传输的信道,如磁带、光盘等。有时我们甚至可以把为了某种目的而使信息不得不经过的通道也看作信道,例如一个分类

器的输入到它的输出就可以看作是一个信道。这里最关键的是信道有一个输入以及一个与输入有关的输出。至于信道本身的物理组成可能是千差万别的,最简单的如一个放大器的输入到输出,而复杂的如一条国际通信的线路,其中可能包括终端设备、线路设备、电缆、微波等等。信息论研究的信道其输入点和输出点在一个实际物理通道中所处位置的选择完全取决于研究者的兴趣。例如,我们可以把通信中发送天线到接收天线之间的通道看成信道,也可以把通信中从话机到话机之间的通道看作信道。

### 4.1.2 信道模型与信道分类

在通信中,信道按其物理组成常被分成微波信道、光纤信道、电缆信道等。这种分类是因为信号在这些信道中传输的过程遵循不同的物理规律,而通信技术必须研究这些规律以获得信号在这些信道中传输时的特性。信息论不研究这些传输特性的获得问题,而假定传输特性是已经知道的,并在此基础上研究信息的传输问题。

由于信息论不研究信号在信道中传输的物理过程,并假定信道的传输特性已知,这样信息论就可以抽象地将信道用图 4.1 所示的模型来描述,并按其输入/输出信号的数学特点以及输入/输出信号之间关系的数学特点进行分类。

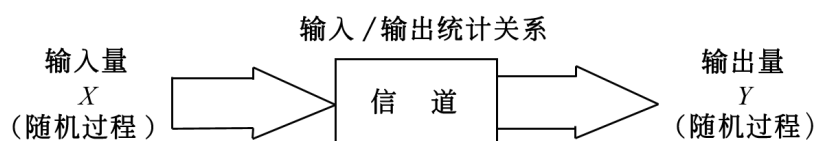


图 4.1 信道模型的示意图

具体来讲,信道的分类方法可以有以下几种:

(1) 信道按其输入/输出信号在幅度和时间上的取值是离散或连续来划分:这种划分方法可以将信道分成四类,如表 4.1 所示。

表 4.1 信道的分类

幅度	时间	信道名称
离散	离散	离散信道(discrete channel),也称数字信道(digital channel)
连续	离散	连续信道(continuous channel)
连续	连续	模拟信道(analog channel),也称波形信道(waveform channel)
离散	连续	(理论和实用价值均很小)

(2) 信道按其输入/输出之间关系的记忆性来划分:这种分类方法可以将信道分为有记忆信道和无记忆信道两类。如果信道的输出只与信道该时刻的输入有关而与其他时刻的输入无关,则称此信道是无记忆的;反之,如果信道的输出不但与信道现时的输入有关,而且还与以前时刻的输入有关,则称此信道为有记忆的。实际信道一般都是有记忆的。信道中的记忆现象来源于物理信道中的惯性,如电缆信道中的电感电容、无线信道中电波传布的衰落现象等。

(3) 信道按其输入/输出信号之间的关系是否是确定关系来划分:这种分类方法可以将信道分成有噪声信道和无噪声信道。一般来讲,信道输入/输出之间的关系是一种统计依存的关系,而不是确定的关系。这是因为信道中总存在某种程度的噪声。在某些情况下,信道中的噪声与有用信号相比很小因而可以忽略不计,则这时的信道可以理想化为具有确定关系的无噪声信道。无噪声信道曾经是信息论早期的一个研究内容,但它现在的实用价值很小,所以我们在本书中不再对它进行讨论。

有噪声信道是信息论研究的主要对象。在这种情况下,信道输入、输出在幅值和时间上的限制以及信道输入/输出之间的统计关系的描述就构成了信道的数学模型。输入/输出的统计关系在离散无记忆信道中只需用输出字母在输入字母条件下的条件概率矩阵来描述。对离散有记忆信道,信道现时的输出值与信道以前时刻的输入和输出有关,这时可以像有记忆信源中那样引入状态的概念。在把信道现时以前的输入和输出看成是一个状态后,信道输入/输出的统计关系就可以用信道以前时刻的状态及现时输入的条件下信道现时输出和状态的联合条件概率来描述。有记忆信道的分析比较复杂,目前得到的可用的研究成果很少,因此我们的讨论将重点放在无记忆信道或能转化成无记忆信道的信道上。

在对信道进行分类和建立数学模型以后,我们就可以开始研究信道传输信息的能力。我们将会看到这一能力可以用信道容量来表示,它代表了信道传输信息的最大能力。由于实际通信中所应用的物理信道本身如电缆、光纤、限定频带的电波传布空间等模型都属于模拟信道,因此模拟信道容量的研究具有最重要的价值。基于这一考虑,模拟信道容量及其充分利用问题的讨论是本章最重要的一个目标。

## 4.2 离散无记忆信道及其信道容量

让我们先从最简单、最基本的信道——离散无记忆信道入手,讨论信道容量

的概念。

设离散无记忆信道的输入  $X$  取自字母表  $A_X = \{a_1, a_2, \dots, a_K\}$ , 信道输出  $Y$  取自字母表  $A_Y = \{b_1, b_2, \dots, b_J\}$ 。由于信道无记忆, 所以输入/输出的统计关系可以用条件概率  $q(b_j | a_k)$  所组成的矩阵  $\mathbf{Q}$  来全面表示该信道输入/输出的统计关系, 即

$$\mathbf{Q} = [q(b_j | a_k)]_{K \times J} \quad (4.1)$$

其中,  $q(b_j | a_k)$  表示信道输入  $a_k$  下信道输出  $b_j$  的概率, 又称前向转移概率, 矩阵  $\mathbf{Q}_{K \times J}$  又称前向转移概率矩阵。

**例 4.1** 图 4.2 给出了离散无记忆信道的两个最简单的例子, 其中信道的输入字母表、输出字母表以及前向转移概率矩阵均标注在图中。

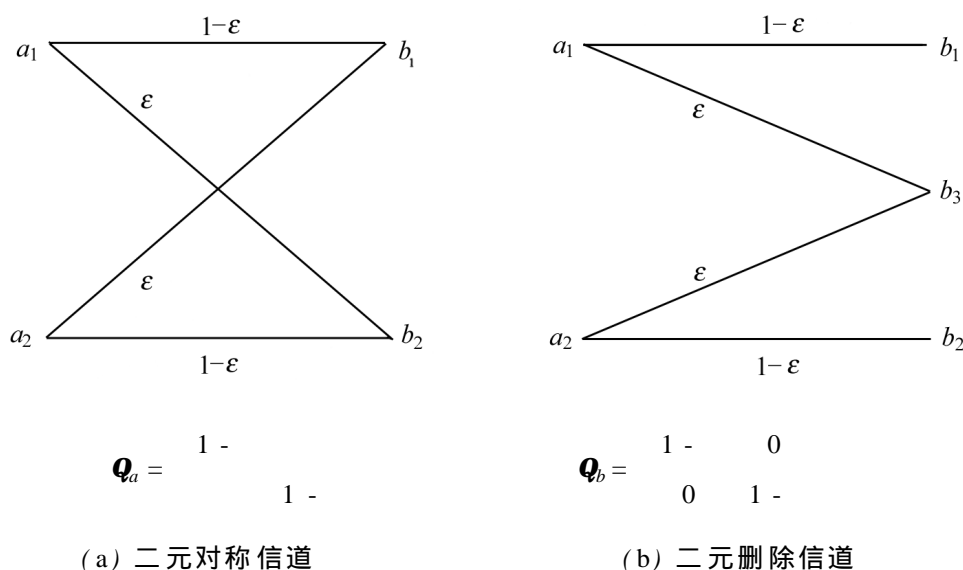


图 4.2 离散无记忆信道的两个实例

当信道输入端输入序列  $x_1 x_2 \dots x_N$  时, 信道输出端的输出设为  $y_1 y_2 \dots y_N$ , 则信道输入/输出之间的互信息为  $I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N)$ 。这一互信息是从信道输出端可以得到的关于输入端输入序列的信息量, 因此也就是我们通过信道可以传输的信息量。显然, 作为信息传输的通道, 我们希望此信息量尽量大, 所以在一般情况下, 我们定义信道的信道容量为

$$C = \lim_{N \rightarrow \infty} \frac{1}{N} \max_{p(\mathbf{x})} I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N) \quad (4.2)$$

信道容量表示通过信道可以传输的最大信息量。这一最大值是在输入序列的全部可能的概率分布下取的。这一定义对有记忆或无记忆的离散信道都适用, 但在无记忆时这一定义可以简化。

**定理 4.1** 设信道的输入、输出分别为  $\mathbf{x} = (x_1 x_2 \dots x_N)$  和  $\mathbf{y} = (y_1 y_2 \dots y_N)$ ,

$p(\mathbf{x})$  为输入字母的  $N$  维概率分布, 则对离散无记忆信道有

$$I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N) = \sum_{n=1}^N I(X_n; Y_n) \quad (4.3)$$

证明 对离散无记忆信道, 有

$$q(\mathbf{y} / \mathbf{x}) = q(y_1 y_2 \dots y_N / x_1 x_2 \dots x_N) = \prod_{n=1}^N q(y_n / x_n) \quad (4.4)$$

而

$$\begin{aligned} I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N) &= I(\mathbf{X}; \mathbf{Y}) \\ &= H(\mathbf{Y}) - H(\mathbf{Y} / \mathbf{X}) \end{aligned}$$

又

$$\begin{aligned} H(\mathbf{Y}) &= H(Y_1) + H(Y_2 / Y_1) + H(Y_3 / Y_1 Y_2) + \dots + \\ &\quad H(Y_N / Y_1 Y_2 \dots Y_{N-1}) = \sum_{n=1}^N H(Y_n) \\ H(\mathbf{Y} / \mathbf{X}) &= - \sum_{\mathbf{x}, \mathbf{y}} p(x_1 x_2 \dots x_N, y_1 y_2 \dots y_N) \log \prod_{n=1}^N q(y_n / x_n) \\ &= - \sum_{n=1}^N \sum_{\mathbf{x}, \mathbf{y}} p(\mathbf{x}, \mathbf{y}) \log q(y_n / x_n) \\ &= - \sum_{n=1}^N \sum_{x_n, y_n} p(x_n, y_n) \log q(y_n / x_n) \\ &= \sum_{n=1}^N H(Y_n / X_n) \end{aligned}$$

因此, 对离散无记忆信道, 有

$$I(\mathbf{X}; \mathbf{Y}) = \sum_{n=1}^N I(X_n; Y_n)$$

当且仅当输入序列为独立随机序列(即信源是离散无记忆的)时, 有

$$p(\mathbf{x}) = \prod_{n=1}^N p(x_n)$$

此时

$$\begin{aligned} p(\mathbf{y}) &= \sum_{\mathbf{x}} p(\mathbf{x}) q(\mathbf{y} / \mathbf{x}) \\ &= \sum_{\mathbf{x}} \prod_{n=1}^N p(x_n) \prod_{n=1}^N q(y_n / x_n) \end{aligned}$$

$$\begin{aligned}
 &= \sum_{n=1}^N p(x_n) q(y_n | x_n) \\
 &= \sum_{n=1}^N p(y_n)
 \end{aligned}$$

而且

$$H(\mathbf{Y}) = \sum_{n=1}^N H(Y_n)$$

从而有

$$I(\mathbf{X}; \mathbf{Y}) = \sum_{n=1}^N I(X_n; Y_n) \quad \text{证毕}$$

推论 离散无记忆信道的信道容量可以写成

$$C = \max_{\mathbf{p}} I(\mathbf{p}, \mathbf{Q}) \quad (4.5)$$

其中,  $\mathbf{p} = (p(a_1), p(a_2), \dots, p(a_K))$  为输入字母概率分布,  $\mathbf{Q}$  为前向转移概率矩阵。

证明 利用定理 4.1, 可知对离散无记忆信道有

$$I(\mathbf{X}; \mathbf{Y}) = \sum_{n=1}^N I(X_n; Y_n)$$

当信源稳恒时, 有

$$\begin{aligned}
 I(X_n; Y_n) &= I(X; Y) \\
 &= \sum_{k=1}^K \sum_{j=1}^J p(a_k) q(b_j | a_k) \log \frac{q(b_j | a_k)}{\sum_{i=1}^J p(a_i) q(b_j | a_i)}
 \end{aligned}$$

它是输入字母概率分布  $\mathbf{p} = (p(a_1), p(a_2), \dots, p(a_K))$  和前向转移概率矩阵  $\mathbf{Q}$  的函数, 可表示为  $I(\mathbf{p}, \mathbf{Q})$ 。这样离散无记忆信道输入/输出之间的互信息在一般情况下满足

$$I(\mathbf{X}; \mathbf{Y}) = NI(\mathbf{p}, \mathbf{Q}) \quad (4.6)$$

根据信道容量的定义式(4.2), 可知对离散无记忆信道, 其信道容量即为

$$C = \max_{\mathbf{p}} I(\mathbf{p}, \mathbf{Q})$$

这一数值代表了通过该离散无记忆信道传输信息的最大速率。

证毕

由定理 4.1 及其推论可知, 对离散无记忆信道而言, 要求其信道容量  $C$ , 只须求  $I(\mathbf{p}, \mathbf{Q})$  的最大值。由第 2 章的知识可知,  $I(\mathbf{p}, \mathbf{Q})$  是  $p(x)$  的上凸函数, 是  $q(y|x)$  的下凸函数, 故  $I(\mathbf{p}, \mathbf{Q})$  相对于  $\mathbf{p}$  必有一个唯一的极大值存在, 该极大值就是最大值。这一最大值只有在下面两个条件下才能达到:

(1) 信道输入的字母序列是一个独立的随机序列, 即要求信源是离散无记忆的。信源在经过冗余度压缩编码后输出的码序列一般满足此要求。



(2) 信道输入字母的概率分布是所有可能分布中能使互信息  $I(\mathbf{p}, \mathbf{Q})$  达到最大值的分布。

当然,这并不是说信道容量由输入字母的概率分布决定的。应该说,信道容量将只取决于信道的前向转移概率矩阵,它代表了信道作为信息传输通道的一个最重要的性能量度。信源发出的信源字母序列只有在满足一定条件时才能充分利用信道传输信息的最大速率,因此,计算各种信道的信道容量是一件具有理论意义和实用价值的工作。在下一节中我们将对此进行讨论。

### 4.3 离散无记忆信道容量的计算

根据上一节对离散无记忆信道容量的定义可知这一容量的计算在数学上是一个多元函数在有界闭区域上求解约束极值的问题,具体讲就是求函数  $I(\mathbf{p}, \mathbf{Q})$  在约束条件

$$\begin{aligned} \sum_{k=1}^K p(a_k) &= 1 \\ p(a_k) &\geq 0 \end{aligned} \quad (4.7)$$

下的最大值,该约束条件构成一个有界闭区域。

数学上求解有界闭区域上的最大值的一般方法如下:

(1) 求  $I(\mathbf{p}, \mathbf{Q})$  在该闭区域内部的极值点,并计算相应的函数值。

(2) 求  $I(\mathbf{p}, \mathbf{Q})$  在该闭区域边界上的极值点,并计算相应的函数值。当变量  $\mathbf{p}$  有  $K$  个分量  $(p(a_1), p(a_2), \dots, p(a_K))$  时,极值点有可能发生在其中若干个分量为零的边界上。这种若干个分量为零而其余分量之和为 1 的边界共有  $2^K - 2$  个,所以总共需求解  $2^K - 2$  个等式约束的极值。

(3) 从以上求出的极值中找出最大值作为信道容量。

#### 4.3.1 信道容量解的充要条件

可以看出,当  $K$  值较大时,上述计算量相当大。解决这一困难的一种办法是找出最大值的充要条件,该充要条件能够帮助我们排除一些不可能的边界,而且在某些情况下可以帮助我们很快找到最大值(或最小值)的位置。我们下面先介绍凸函数极值的下述定理。

**定理 4.2** 设  $f(\mathbf{x})$  是定义在所有分量均非负的半无限矢量空间上的可微

下凸函数,  $M = \min f(\mathbf{x})$  是  $f(\mathbf{x})$  在此空间上的最小值。则  $\mathbf{x} = \mathbf{x}^*$  时能达到此最小值  $M$  的充要条件是

$$\left. \frac{f(\mathbf{x})}{x_n} \right|_{\mathbf{x}=\mathbf{x}^*} = 0, \quad \text{当 } x_n > 0 \text{ 时} \quad (4.8)$$

$$\left. \frac{f(\mathbf{x})}{x_n} \right|_{\mathbf{x}=\mathbf{x}^*} \geq 0, \quad \text{当 } x_n = 0 \text{ 时} \quad (4.9)$$

证明 已知函数  $f(\mathbf{x})$  可微下凸, 若极值点不在边界上, 则其极值即为最小值。由微分学可知, 极值点的充要条件是

$$\left. \frac{f(\mathbf{x})}{x_n} \right|_{\mathbf{x}=\mathbf{x}^*} = 0, \quad \text{当 } x_n > 0 \text{ 时}$$

若极值点发生在边界处, 则其充要条件是  $f(\mathbf{x})$  沿此  $x_n = 0$  的分量向内时其值增加, 即

$$\left. \frac{f(\mathbf{x})}{x_n} \right|_{\mathbf{x}=\mathbf{x}^*} \geq 0, \quad \text{当 } x_n = 0 \text{ 时} \quad \text{证毕}$$

定理 4.2 可以理解为凸函数求极值的定理。不难理解, 若  $f(\mathbf{x})$  是可微上凸函数时, 只需将式 (4.9) 中的不等号反向即得该函数取最大值的充要条件。

由于  $I(\mathbf{p}, \mathbf{Q})$  是  $\mathbf{p}$  的上凸函数, 故可将定理 4.2 应用于离散无记忆信道的信道容量的求解上, 我们立即得到以下的信道容量定理。

定理 4.3 (离散无记忆信道的信道容量定理) 对前向转移概率矩阵为  $\mathbf{Q}$  的离散无记忆信道, 其输入字母的概率分布  $\mathbf{p}^*$  能使互信息  $I(\mathbf{p}, \mathbf{Q})$  取最大值的充要条件是

$$I(x = a_k; Y) / \mathbf{p} = \mathbf{p}^* = C, \quad \text{当 } p^*(a_k) > 0 \quad (4.10)$$

$$I(x = a_k; Y) / \mathbf{p} = \mathbf{p}^* \leq C, \quad \text{当 } p^*(a_k) = 0 \quad (4.11)$$

其中

$$I(x = a_k; Y) = \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p(b_j)}$$

是信源字母  $a_k$  传送的平均互信息,  $C$  就是这一信道的信道容量。

证明 已知信道容量是在约束条件

$$\sum_{k=1}^K p(a_k) = 1$$

下  $I(\mathbf{p}, \mathbf{Q})$  的最大值。按照拉格朗日乘数法, 此约束极值问题可转化为函数

$$g(\mathbf{p}) = I(\mathbf{p}, \mathbf{Q}) - \mu \sum_{k=1}^K p(a_k) - 1 \quad (4.12)$$

的无约束极值问题。由于  $g(\mathbf{p})$  是  $\mathbf{p}$  的上凸函数  $I(\mathbf{p}, \mathbf{Q})$  与  $\mathbf{p}$  的线性函数之和, 故  $g(\mathbf{p})$  仍为上凸函数。根据凸函数求极值的定理 4.2 可知,  $g(\mathbf{p})$  在  $\mathbf{p} = \mathbf{p}^*$  时取最大值的充要条件是

$$\left. \frac{g(\mathbf{p})}{p(a_k)} \right|_{\mathbf{p}=\mathbf{p}^*} = 0, \quad \text{当 } p(a_k) > 0 \text{ 时}$$

$$\left. \frac{g(\mathbf{p})}{p(a_k)} \right|_{\mathbf{p}=\mathbf{p}^*} \leq 0, \quad \text{当 } p(a_k) = 0 \text{ 时}$$

而

$$\begin{aligned} \frac{g(\mathbf{p})}{p(a_k)} &= \frac{1}{p(a_k)} \sum_{i=1}^K p(a_i) \sum_{j=1}^J q(b_j | a_i) \log \frac{q(b_j | a_i)}{p(b_j)} - \mu \\ &= \sum_{j=1}^J q(b_j | a_k) \log q(b_j | a_k) - \sum_{j=1}^J q(b_j | a_k) \log p(b_j) - \\ &\quad \sum_{j=1}^J p(b_j) \frac{q(b_j | a_k)}{p(b_j)} \log e - \mu \\ &= \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p(b_j)} - \log e - \mu \\ &= I(x = a_k; Y) - \log e - \mu \end{aligned}$$

因此

$$I(x = a_k; Y) = \mu + \log e, \quad \text{当 } p(a_k) > 0 \text{ 时} \quad (4.13)$$

$$I(x = a_k; Y) \leq \mu + \log e, \quad \text{当 } p(a_k) = 0 \text{ 时} \quad (4.14)$$

令  $C = \mu + \log e$ , 即得定理所述的结果。此时通过信道传输的平均互信息为

$$I(X; Y) = \sum_{k=1}^K p(a_k) I(x = a_k; Y) = C \quad (4.15)$$

证毕

定理 4.3 所得的结果可以有一个很简单的直观的理解。通过信道传输的互信息  $I(X; Y)$  是  $I(x = a_k; Y)$  的平均值, 所以, 若某一个  $a_k$  可传送的互信息  $I(x = a_k; Y)$  比其他字母可传送的互信息大, 我们就可以用提高  $p(a_k)$  的办法来使总的互信息增加。但当我们提高  $p(a_k)$  时,  $I(x = a_k; Y)$  必然减小, 这是因为

$$I(x = a_k; Y) = \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{\sum_{i=1}^K p(a_i) q(b_j | a_i)}$$

当  $p(a_k)$  增加时,  $q(b_j | a_k)$  就更加接近  $p(b_j)$ 。因此用这样的方法反复调整输入字母的概率分布, 最终必然使所有字母的  $I(x = a_k; Y)$  相等, 这时调整也随之终

止,互信息  $I(X; Y)$  达到最大。由于前向转移概率所取的某种特殊分布,某些输入字母条件下输出字母的条件熵可能很接近输出字母的无条件熵,致使  $I(x = a_k; Y)$  小于  $C$ , 说明这些可用的输入字母是不值得使用的,所以这些字母的  $p(a_k) = 0$ 。

### 4.3.2 某些简单情况下信道容量的解

离散无记忆信道的信道容量定理 4.3 没有给出互信息达到信道容量时输入字母的概率分布,因而未给出信道容量的解,但是它可以帮助我们求解简单情况下部分信道的信道容量。

**例 4.2** 求二元对称信道和二元删除信道的信道容量。

**解** 从图 4.2 中可以看到,这两种信道相对于输入字母有着非常明显的对称性,因此不难肯定,当输入字母等概分布时,即输入字母的概率分布为  $p(a_1) = p(a_2) = \frac{1}{2}$  时,才能使互信息达到信道容量。这一判断的正确性可以用定理 4.3 加以检验。对于二元对称信道,有

$$\begin{aligned} p(b) &= \sum_{k=1}^2 p(a_k) q(b/a_k) = \frac{1}{2} \\ p(b_1) &= p(b_2) = \frac{1}{2} \\ I(x = a_k; Y) &= \sum_{j=1}^2 q(b_j/a_k) \log \frac{q(b_j/a_k)}{p(b_j)} \\ &= (1 - \epsilon) \log \frac{1 - \epsilon}{1/2} + \epsilon \log \frac{\epsilon}{1/2} \\ &= 1 - H(\epsilon) \quad (k = 1, 2) \end{aligned}$$

其中  $H(\epsilon) = -\log \epsilon - (1 - \epsilon) \log(1 - \epsilon)$  为二元随机变量的熵函数。这满足定理 4.3 中要求的条件(4.10)和条件(4.11),所以在这一概率分布下的互信息值就是信道容量

$$C = 1 - H(\epsilon)$$

而对于二元删除信道,有

$$p(b) = \sum_{k=1}^2 p(a_k) q(b/a_k) = \frac{1}{2}(1 - \epsilon)$$

$$\begin{aligned}
 p(b_k) &= \sum_{k=1}^2 p(a_k) q(b_k / a_k) = \frac{1}{2} (1 - \epsilon) \\
 p(b_k) &= \\
 I(x = a_k; Y) &= \sum_{j=1}^3 q(b_j / a_k) \log \frac{q(b_j / a_k)}{p(b_j)} \\
 &= (1 - \epsilon) \log \frac{1 - \epsilon}{\frac{1}{2} (1 - \epsilon)} + \log \frac{\epsilon}{\frac{1}{2} (1 - \epsilon)} \quad (k = 1, 2) \\
 &= 1 - \epsilon
 \end{aligned}$$

因此这也是达到信道容量时的概率分布, 而该信道的信道容量为

$$C = 1 - \epsilon$$

这两个典型信道的信道容量随  $\epsilon$  的变化曲线如图 4.3 所示。图中曲线  $a$  为二元对称信道, 曲线  $b$  为二元删除信道。

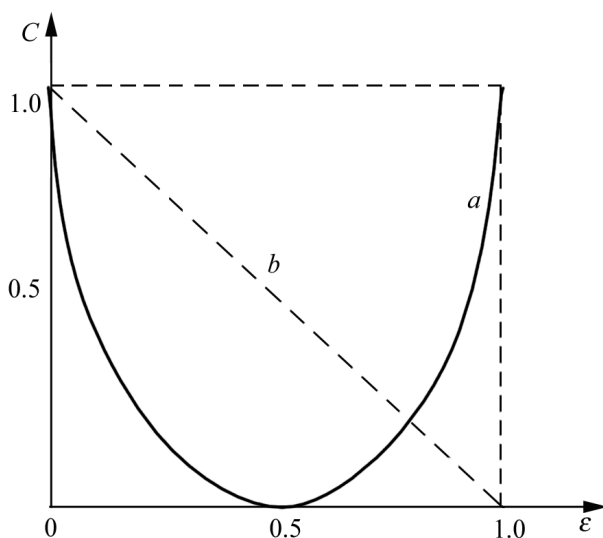


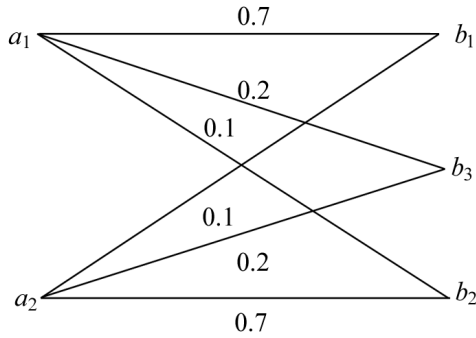
图 4.3 两种典型信道的信道容量曲线

以上例子说明, 当信道对称时, 输入字母的概率分布很容易被确定, 其正确性可以用离散无记忆信道的信道容量定理 4.3 验证。这就启示我们引入如下的对称信道的一般定义。

所谓对称的离散无记忆信道是这样的信道, 其输出字母的集合可以划分为若干子集, 对每个子集而言, 其前向转移概率矩阵中每一行都是其他行元素的一个排列, 每一列又都是其他列元素的一个排列。

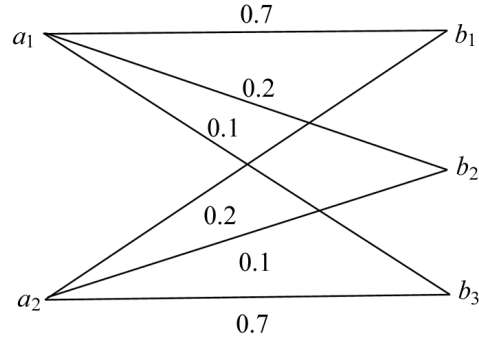
我们很容易验证, 图 4.2 的两种信道都符合这一定义。下面再举例说明一般的对称信道。

## 例 4.3



$$\mathbf{Q} = \begin{matrix} & \begin{matrix} b_1 & b_2 & b_3 \end{matrix} \\ \begin{matrix} a_1 \\ a_2 \end{matrix} & \begin{pmatrix} 0.7 & 0.1 & 0.2 \\ 0.1 & 0.7 & 0.2 \end{pmatrix} \end{matrix}$$

(a) 对称的离散无记忆信道



$$\mathbf{Q} = \begin{matrix} & \begin{matrix} b_1 & b_2 & b_3 \end{matrix} \\ \begin{matrix} a_1 \\ a_2 \end{matrix} & \begin{pmatrix} 0.7 & 0.1 & 0.2 \\ 0.2 & 0.7 & 0.1 \end{pmatrix} \end{matrix}$$

(b) 非对称的离散无记忆信道

对于对称信道在输入字母等概分布时达到信道容量这一直观的判断, 我们可以用下述定理的形式表述出来, 并根据对称信道的定义给出一般性的证明。

**定理 4.4** 对于对称的离散无记忆信道, 当输入字母等概时即达到信道容量。

**证明** 设信道的输入字母等概分布, 即

$$p(a_k) = \frac{1}{K}, \quad k = 1, 2, \dots, K$$

此时有

$$\begin{aligned} I(x = a_k; Y) &= \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p(b_j)} \\ &= \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{\frac{1}{K} \sum_{i=1}^K q(b_j | a_i)} \end{aligned}$$

根据对称的离散无记忆信道的定义, 可将输出字母分成若干子集  $J_1, J_2, \dots, J_n$ , 在同一个子集内其输出字母的概率  $p(b_j)$  是相同的, 这是因为

$$p(b_j) = \sum_{k=1}^K p(a_k) q(b_j | a_k) = \frac{1}{K} \sum_{k=1}^K q(b_j | a_k)$$

由于在同一子集内, 前向概率矩阵  $\mathbf{Q}$  的每一列都是其他列元素的一个排列, 于是

$$q(b_j | a_k) I(x = a_k; y = b_j) = q(b_j | a_k) \log \frac{q(b_j | a_k)}{p(b_j)}$$

所组成的矩阵具有和  $\mathbf{Q}$  矩阵相同的特性, 即在输出字母划分的相应子集内, 其各行(或各列)均为其他行(或列)元素的排列, 从而有

$$q(b_j | a_k) I(x = a_k; y = b_j), \quad i = 1, 2, \dots, n$$

对所有  $k$  相等 ( $k = 1, 2, \dots, K$ ), 于是

$$I(x = a_k; Y) = \sum_{i=1}^n \sum_{j=1}^J q(b_j | a_k) I(x = a_k; y = b_j)$$

将与  $k$  无关, 而是一个常数。因而符合离散无记忆信道的信道容量定理, 所以等概的输入字母分布确实可使互信息到达信道容量。证毕

### 4.3.3 一般情况下信道容量的解

在更加一般性的信道中, 我们现在来考虑输入/输出字母总数相等且前向转移概率矩阵  $\mathbf{Q}$  为非奇异矩阵的情况。对于这样的信道, 如果达到信道容量时的输入分布满足

$$p(a_k) = 0, \quad k = 1, 2, \dots, K$$

由离散无记忆信道的信道容量定理 4.3 可知, 当  $p(a_k) > 0$  时, 有

$$I(x = a_k; Y) = C, \quad k = 1, 2, \dots, K$$

此时的  $\mathbf{p}$  即为所求。将上式具体写为

$$\sum_{j=1}^J q(b_j | a_k) \log q(b_j | a_k) = C + \sum_{j=1}^J q(b_j | a_k) \log p(b_j), \quad k = 1, 2, \dots, K \quad (4.16)$$

另有

$$\sum_{j=1}^J p(b_j) = 1 \quad (4.17)$$

因此, 可以用式(4.16)和式(4.17)组成的  $K+1$  个方程求解  $p(b_j) (j = 1, 2, \dots, J)$ , 以及信道容量  $C$  这  $J+1$  个未知量, 再由  $\{p(b_j)\}$  可求解  $\{p(a_k)\}$ 。

实际上,  $p(b_j) (j = 1, 2, \dots, J)$  中只有  $J-1$  个是独立的。而

$$p(b_j) = \sum_{k=1}^K p(a_k) q(b_j | a_k), \quad j = 1, 2, \dots, J-1 \quad (4.18)$$

又有约束条件

$$\sum_{k=1}^K p(a_k) = 1 \quad (4.19)$$

因此, 可以用式(4.18)和式(4.19)组成的  $J$  个方程求  $K$  个未知量  $p(a_k) (k = 1, 2, \dots, K)$ 。

若将方程(4.16)进一步变形,可得

$$-H(Y/x=a_k) = C \sum_{j=1}^J q(b_j/a_k) + \sum_{j=1}^J q(b_j/a_k) \log p(b_j), \quad k=1,2,\dots,K$$

即

$$-H(Y/a_k) = \sum_{j=1}^J q(b_j/a_k) [C + \log p(b_j)], \quad k=1,2,\dots,K \quad (4.20)$$

令

$$c_j = C + \log p(b_j), \quad j=1,2,\dots,J \quad (4.21)$$

则有

$$\mathbf{Q} = \begin{pmatrix} -H(Y/a_1) \\ -H(Y/a_2) \\ \dots \\ -H(Y/a_K) \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_J \end{pmatrix} \quad (4.22)$$

这是含有  $J$  个未知数(信道容量  $C$  和  $J-1$  个  $p(b_j)$ )的  $K$  个方程的非齐次线性方程组。一般地,该方程组不一定可解,但当  $K=J$ ,且前向转移概率矩阵  $\mathbf{Q}$  为非奇异矩阵时,该方程组有解。

设

$$\mathbf{R} = \mathbf{Q}^{-1} = (r_{jk})$$

则得

$$\begin{pmatrix} -H(Y/a_1) \\ -H(Y/a_2) \\ \dots \\ -H(Y/a_K) \end{pmatrix} = \mathbf{R} \begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_J \end{pmatrix} \quad (4.23)$$

或

$$c_j = - \sum_{k=1}^K r_{jk} H(Y/a_k), \quad j=1,2,\dots,J \quad (4.24)$$

由式(4.21),可得

$$p(b_j) = 2^{j-C}, \quad j=1,2,\dots,J \quad (4.25)$$

利用条件(4.17),有

$$\sum_{j=1}^J 2^{j-C} = 1 \quad (4.26)$$

则得信道容量  $C$  为



$$C = \log_2 \prod_{j=1}^J 2^{j_j} \quad (4.27)$$

最后利用式(4.18)和式(4.19)即可求出输入字母的概率分布  $p(a_k)$  ( $k = 1, 2, \dots, K$ ), 此即达到信道容量时输入字母的概率分布。

应该强调的是, 上述求解结果的正确性仍然取决于所求得的  $p(a_k)$  是否满足在所有  $k = 1, 2, \dots, K$  下均满足  $p(a_k) > 0$ 。如果在某些  $k$  值下  $p(a_k) = 0$ , 说明  $I(X; Y)$  的最大值发生在边界上, 则仍然需要在所有可能边界上进行计算, 找出最大值所对应的输入概率分布。

### \* 4.3.4 信道容量的迭代解法

1972年, S. Arimoto 和 R. E. Blahut 分别为信道容量的求解问题给出了一种迭代算法, 该算法避免了我们在所有边界上计算的麻烦。这一迭代算法是在下述定理的基础上建立起来的。

**定理 4.5** 设信道的前向转移概率矩阵为  $\mathbf{Q} = [q(b_j | a_k)]_{K \times J}$ ,  $\mathbf{p}^0$  是任给的输入字母的一个初始概率分布, 其所有分量  $p^0(a_k)$  均不为零。按照下式不断对概率分布进行迭代、更新:

$$p^{r+1}(a_k) = p^r(a_k) \frac{\sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p^r(a_k) q(b_j | a_k)}}{\sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p^r(a_k) q(b_j | a_k)}} \quad (4.28)$$

其中

$$k(\mathbf{p}^r) = \exp[I(x = a_k; Y)] \Big|_{\mathbf{p} = \mathbf{p}^r} = \exp \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p^r(a_k) q(b_j | a_k)} \quad (4.29)$$

则由此所得的  $I(\mathbf{p}^r, \mathbf{Q})$  序列收敛于信道容量  $C$ 。

证明略。

在上述定理中, 输入字母概率分布的更新方法具有明显的意义, 即不断将具有较大互信息  $I(x = a_k; Y)$  的输入字母的概率加以提高, 将具有较小互信息  $I(x = a_k; Y)$  的输入字母的概率加以降低。这一原则和我们在对离散无记忆信道的信道容量定理 4.3 的解释时所说的道理是完全一致的。

Blahut 得到的信道容量的计算算法如图 4.4 所示。

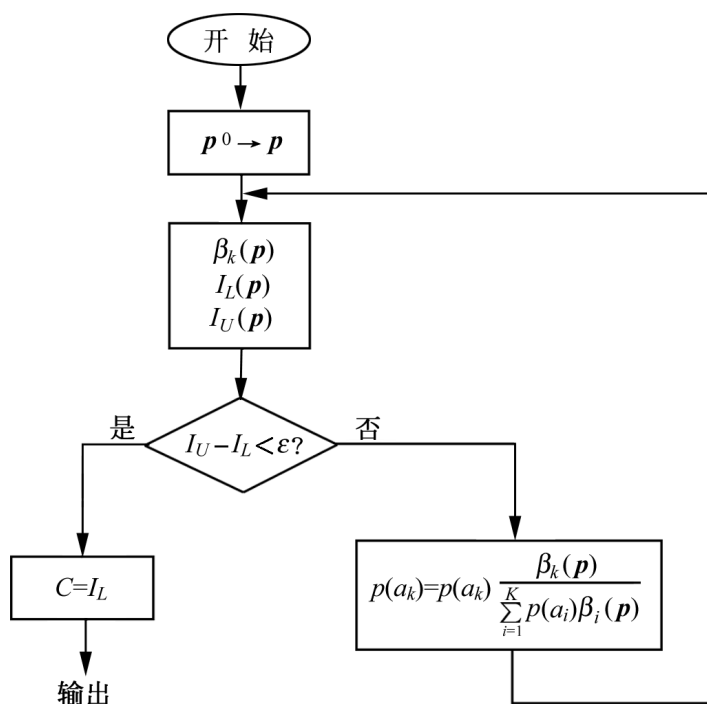


图 4.4 信道容量的迭代算法

迭代算法的迭代终止条件可以选用相邻的迭代结果的差值小于某给定值作为条件,但图中所用的 Blahut 建议的条件更加合理,即设

$$I_L = \log \prod_{k=1}^K p(a_k)^{I_k(\mathbf{p})} \quad (4.30)$$

$$I_U = \log \max_k I_k(\mathbf{p}) \quad (4.31)$$

当  $I_U - I_L < \epsilon$  时迭代结束。

显然,只有当所有非零概率的输入字母与输出的互信息相等时,  $I_L$  的值才等于信道容量,而  $I_U$  则是各输入字母与输出的互信息中最大的互信息,因此当  $I_U - I_L < \epsilon$  时,各字母的互信息已非常接近相等。

## 4.4 级联信道和并联信道的信道容量

这一节我们讨论信道在几种基本的组合下组合信道总容量与其组成信道容量之间的关系,由此可以加深我们对信道容量的理解。

### 4.4.1 级联信道

级联信道是信道最基本的组合形式,许多实际信道都可以看成是其组成信

道的级联。图 4.5 是由两个信道组成的最简单的级联信道。信道级联的主要条件是前一信道的输出字母表与后一信道的输入字母表一致。如图 4.5 所示, 信道 1 的输出  $Y$  恰好是信道 2 的输入,  $X$  和  $Z$  分别成为此级联信道的输入和输出。

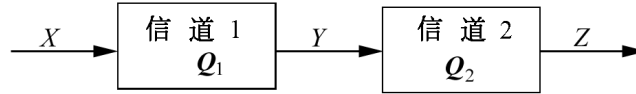


图 4.5 级联信道

我们先来分析一下级联信道中各输入、输出之间的关系。以图 4.5 为例, 信道 1 的输出  $Y$  与其输入  $X$  统计相关, 而信道 2 的输出  $Z$  又与其输入  $Y$  统计相关, 所以, 一般来讲,  $Z$  将与  $X$  统计相关。但另一方面, 级联的结构决定了  $Z$  的取值在给定  $Y$  以后将不再与  $X$  有关, 而只取决于信道 2 的前向转移概率矩阵  $\mathbf{Q}$ 。在概率论中, 我们称  $XYZ$  的这种关系为  $XYZ$  组成马尔可夫链。设  $X, Y, Z$  的字母表分别为  $A_X = \{a_1, a_2, \dots, a_k\}$ ,  $A_Y = \{b_1, b_2, \dots, b_l\}$  和  $A_Z = \{c_1, c_2, \dots, c_n\}$ , 则当  $X, Y, Z$  组成马尔可夫链时它们在概率上满足以下关系

$$p(xz / y = b_j) = p(x / y = b_j) p(z / y = b_j) \quad (4.32)$$

因此它们之间的互信息满足

$$- I(X; Z | Y) = H(XZ | Y) - H(X | Y) - H(Z | Y) = 0 \quad (4.33)$$

由此, 利用关系式

$$\begin{aligned} I(X; YZ) &= I(X; Y) + I(X; Z | Y) \\ &= I(X; Z) + I(X; Y | Z) \end{aligned} \quad (4.34)$$

可得

$$I(X; Y) = I(X; Z) + I(X; Y | Z) \quad (4.35)$$

由于互信息的非负性, 所以在马尔可夫链下有

$$I(X; Y) \geq I(X; Z) \quad (4.36)$$

根据  $I(XY; Z) = I(X; Z) + I(Y; Z | X) = I(Y; Z) + I(X; Z | Y)$ , 同理可得

$$I(Y; Z) \geq I(X; Z) \quad (4.37)$$

式(4.36)和式(4.37)表明, 级联信道的信道容量不可能大于其各组成信道的信道容量。实际上, 当信道不断级联时, 级联信道的信道容量一般将趋于零。

级联信道容量的计算并不困难。设有  $N$  个信道被级联在一起, 各信道的前向转移概率矩阵分别为  $\mathbf{Q}_1, \mathbf{Q}_2, \dots, \mathbf{Q}_N$ 。利用级联信道中各输入、输出组成马尔可夫链可以证明, 总的级联信道的前向转移概率矩阵为

$$\mathbf{Q} = \mathbf{Q} \mathbf{Q} \dots \mathbf{Q} = \prod_{n=1}^N \mathbf{Q}_n \quad (4.38)$$

利用求得的级联信道的  $\mathbf{Q}$  就可按上节介绍的办法计算级联信道容量。

**例 4.4** 求  $N$  个相同的二元对称信道组成的级联信道的信道容量。

**解** 设单个二元对称信道的前向转移概率矩阵为

$$\mathbf{Q} = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$$

所以  $N$  个二元对称信道级联后的信道前向转移概率矩阵为

$$\mathbf{Q} = \mathbf{Q}^N \quad (4.39)$$

由于  $\mathbf{Q}$  是对称矩阵, 所以不难用正交变换转化为对角矩阵, 即

$$\mathbf{T}^{-1} \mathbf{Q} \mathbf{T} = \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix} \quad (4.40)$$

其中

$$\mathbf{T} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbf{T}^{-1} \quad (4.41)$$

所以

$$\begin{aligned} \mathbf{Q} = \mathbf{Q}^N &= \mathbf{T}^{-N} \mathbf{T}^{-1} = \mathbf{T} \begin{bmatrix} 1 & 0 \\ 0 & (1/2)^N \end{bmatrix} \mathbf{T}^{-1} \\ &= \frac{1}{2} \begin{bmatrix} 1 + (1/2)^N & 1 - (1/2)^N \\ 1 - (1/2)^N & 1 + (1/2)^N \end{bmatrix} \end{aligned} \quad (4.42)$$

级联后的信道仍等效为一个二元对称信道, 其错误传递概率为

$$\frac{1}{2} [1 - (1/2)^N]$$

根据节 4.3.2 中的例子求出的二元对称信道的信道容量, 可知级联信道的信道容量为

$$C_N = 1 - H \frac{1 - (1/2)^N}{2} \quad (4.43)$$

不难看出, 当  $N \rightarrow \infty$  时, 级联信道的前向转移概率矩阵  $\mathbf{Q}$  变为

$$\lim_{N \rightarrow \infty} \mathbf{Q} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \quad (4.44)$$

此时级联信道的信道容量为

$$\lim_N C_N = 1 - H \frac{1}{2} = 0$$

这说明  $N$  时级联信道的输出将与输入无关。

我们在节 4.1 中曾经指出,信息论中的信道是一种广义理解的信道,特别是我们也可以把信号处理器看成是信道。在这种情况下,级联的信号处理器可看成级联信道。这样,从信息传输的观点来看,随着信号的不断处理,信号处理器的输出与最初输入信号之间的互信息将不断减小,直至完全独立。因此,关系式

$$\begin{aligned} I(X; Z) &= I(X; Y) \\ I(X; Z) &= I(Y; Z) \end{aligned}$$

在信息论中又称为数据处理定理。这一结论告诉我们,虽然数据处理可以满足我们的某种具体要求,但从信息量来看每一次处理都会损失一部分信息。

4.4.2 并联信道

并联信道是另外一种基本的信道组合形式。并联信道有三种并联方式,如图 4.6 所示。

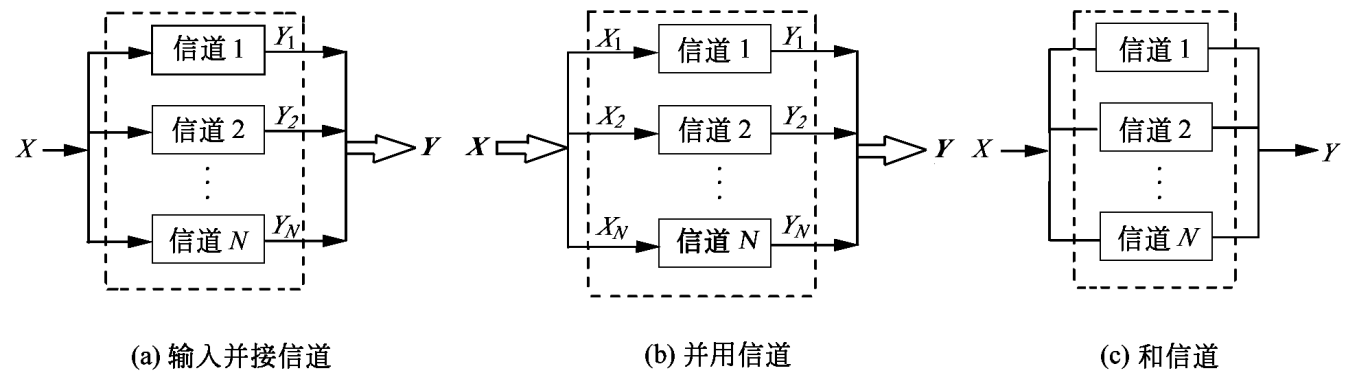


图 4.6 并联信道

我们把它们放在一起讨论是因为它们在结构上都有某种并联的形式,但这三种并联信道从其输入/输出字母表及其使用方式来看是很不一样的。图 4.6(a)被称为输入并接信道,因为它的  $N$  个组成信道具有相同的输入字母表,且输入被同时使用,而  $N$  个组成信道的输出是各自不同的,它们在一起组成输出字母组,我们用输出矢量  $\mathbf{Y} = (Y_1 Y_2 \dots Y_N)$  来表示。图 4.6(b)被称为并用信道,因为它的  $N$  个组成信道的输入、输出彼此独立、各不相同,分别对应着并联信道输入矢量和输出矢量的一个分量,因此,并用信道中的各个组成信道仅在使用上被并起来。图 4.6(c)有独立的  $N$  个组成信道,传输信息时每次只使用其中

一个信道,因此,这  $N$  个组成信道既没有在输入端被并接,也没有在使用上被同时使用,它们只是整个被当成一个信道任意选用其组成信道,所以我们称其为和信道。下面我们分别对它们的容量进行讨论。

#### 4.4.2.1 输入并接信道

输入并接信道可以看成是一个单输入多输出的信道,即其输入为  $X$ , 输出为  $\mathbf{Y} = (Y_1 Y_2 \dots Y_N)$ 。通过这一信道传输的信息为

$$\begin{aligned} I(X; Y_1 Y_2 \dots Y_N) &= I(X; Y_1) + I(X; Y_2 / Y_1) + \dots + I(X; Y_N / Y_1 Y_2 \dots Y_{N-1}) \\ &= I(X; Y_2) + I(X; Y_1 / Y_2) + I(X; Y_3 / Y_1 Y_2) + \dots + \\ &\quad I(X; Y_N / Y_1 Y_2 \dots Y_{N-1}) \\ &= \dots\dots\dots \\ &= I(X; Y_N) + I(X; Y_1 / Y_N) + \dots + I(X; Y_{N-1} / Y_1 \dots Y_{N-2} Y_N) \end{aligned} \quad (4.45)$$

由此可知,该信道的信道容量一定大于其中任意一个组成信道的信道容量。然而,输入并接信道的信道容量的具体求解比较困难,因为其前向转移概率矩阵非常庞大,即使在最简单的情况下,例如在由  $N$  个相同的二元对称信道并接而成的信道中,其输出矢量仍然有  $2^N$  种,具体计算将会很繁杂。但是,这一输入并接信道的信道容量有一个简单的上界。因为

$$\begin{aligned} I(X; Y_1 Y_2 \dots Y_N) &= H(X) - H(X | Y_1 Y_2 \dots Y_N) \\ &\leq H(X) \end{aligned}$$

所以

$$C \leq \max_{p(x)} H(X) \quad (4.46)$$

例如,在由  $N$  个相同的二元对称信道并接而成的信道下,其信道容量将不超过 1 bit/字母。

从信道利用的角度来看,输入并接信道的效率很低,但是,利用它可以提高信息传输的可靠性。例如,对一个物理量的若干次测量,或对同一个物理量采用若干不同的测量系统进行测量等。

#### 4.4.2.2 并用信道

并用信道的特点是其所有组成的信道被并联起来使用,但输入并未并接,各组成信道仍有各自的输入和输出,这一特点可表示为

$$p(y_1 y_2 \dots y_N / x_1 x_2 \dots x_N) = \prod_{n=1}^N p(y_n / x_n) \quad (4.47)$$

所以通过并用信道传输的互信息为

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}) &= H(\mathbf{Y}) - H(\mathbf{Y} / \mathbf{X}) \\ &= H(\mathbf{Y}) - \sum_{n=1}^N H(Y_n / X_n) \end{aligned} \quad (4.48)$$

由于

$$\begin{aligned} H(\mathbf{Y}) &= H(Y_1) + H(Y_2 / Y_1) + \dots + H(Y_N / Y_1 Y_2 \dots Y_{N-1}) \\ &= \sum_{n=1}^N H(Y_n) \end{aligned} \quad (4.49)$$

所以

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}) &= \sum_{n=1}^N [H(Y_n) - H(Y_n / X_n)] \\ &= \sum_{n=1}^N I(X_n; Y_n) \end{aligned} \quad (4.50)$$

当且仅当  $X_n (n=1, 2, \dots, N)$  相互独立时才有

$$H(\mathbf{Y}) = \sum_{n=1}^N H(Y_n) \quad (4.51)$$

$$\text{及} \quad I(\mathbf{X}; \mathbf{Y}) = \sum_{n=1}^N I(X_n; Y_n) \quad (4.52)$$

所以, 并用信道的信道容量为

$$C = \max_{p(\mathbf{x})} I(\mathbf{X}; \mathbf{Y}) = \max_{n=1}^N I(X_n; Y_n) = \sum_{n=1}^N C_n \quad (4.53)$$

即并用信道的信道容量为各组成信道的信道容量之和。

### 4.4.2.3 和信道

和信道的前向转移概率矩阵很容易由其组成信道求得。设和信道有  $N$  个组成信道, 各自的前向转移概率矩阵分别为  $\mathbf{Q}_1, \mathbf{Q}_2, \dots, \mathbf{Q}_N$ , 第  $n$  个组成信道的输入字母总数为  $K_n$ , 输出字母总数为  $J_n$ , 转移概率为  $q_n(b_{j_n} | a_{k_n}) (k_n = 1, 2, \dots, K_n, j_n = 1, 2, \dots, J_n)$ 。则和信道的前向转移概率矩阵是由  $\mathbf{Q}_1, \mathbf{Q}_2, \dots, \mathbf{Q}_N$  组成的分块对角矩阵, 即

$$Q = \frac{Q}{W} \quad (4.54)$$

设第  $n$  个信道的使用概率为  $p_n(C)$  时, 则第  $n$  个信道中输入字母  $a_{k_n}$  与输出的互信息为

$$I_n(a_{k_n}; Y) = \sum_{j_n=1}^{J_n} q_n(b_{j_n} / a_{k_n}) \log \frac{q_n(b_{j_n} / a_{k_n})}{p_n(C) \sum_{i=1}^{K_n} p_n(a_i) q_n(b_{j_n} / a_i)} \quad (4.55)$$

根据离散无记忆信道的信道容量定理 4.3, 应有

$$I_n(a_{k_n}; Y) = C_n + \log \frac{1}{p_n(C)} = C \quad (4.56)$$

又

$$\sum_{n=1}^N p_n(C) = 1 \quad (4.57)$$

于是, 和信道的信道容量为

$$C = \log_2 \sum_{n=1}^N 2^{C_n} \quad (4.58)$$

此时各组成信道的使用概率为

$$p_n(C) = 2^{(C_n - C)} \quad (4.59)$$

## 4.5 信道达到充分利用时输入输出字母概率分布的唯一性

前两节我们讨论了信道容量以及达到信道容量时所对应的输入分布的计算方法, 但值得指出的是这样计算得到的输入字母分布不一定是唯一的。对此我们只要看一下前面所举的二元对称信道的例子就可以了, 在这种信道中, 信道容量  $C$  为

$$C = 1 - H(p) = 1 + \log_2(1-p) + p \log_2 p + (1-p) \log_2 (1-p)$$

当  $p = \frac{1}{2}$  时, 有  $C = 0$ , 这时不管输入字母的概率分布如何, 均可达到信道容量。

当然, 这样的信道是没有意义的, 但它在理论上说明达到信道容量的输入字母概率分布不一定唯一。

对于一般的信道, 如果我们已经知道有两种概率分布可以使互信息达到信



道容量,则由此可以得到无限多种使互信息达到信道容量的概率分布,这一点不难证明。

设有  $\mathbf{p}$  和  $\mathbf{p}'$  均满足信道容量对输入分布的要求,即有

$$I(\mathbf{p}) = I(\mathbf{p}') = C$$

现设  $0 \leq \lambda \leq 1$ , 则由互信息函数的凸性可知

$$I(\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}') \geq \lambda I(\mathbf{p}) + (1 - \lambda) I(\mathbf{p}') = C$$

但左端不可能超过  $C$ , 因为  $C$  是互信息的最大值, 即

$$C = \max_{\mathbf{p}} I(\mathbf{p}, \mathbf{Q})$$

所以

$$I(\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}') = C, \quad 0 \leq \lambda \leq 1$$

由此可知,  $\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}'$  也是能使互信息达到信道容量的输入概率分布。

由上述证明可以看出, 信道得到充分利用时, 其输入概率分布可以不唯一。但此时信道的输出概率分布却是唯一的, 下述定理说明了这一点。

**定理 4.6** 使互信息达到信道容量的输出概率分布是唯一的。任何导致这一输出概率分布的输入概率分布都能使互信息达到信道容量。

**证明** (1) 当互信息达到信道容量时, 若其输入概率分布唯一, 则此时的输出概率分布也是唯一的。

(2) 当互信息达到信道容量时, 若其输入概率分布不唯一, 则可设  $\mathbf{p}$  和  $\mathbf{p}'$  是两个使互信息达到信道容量的输入概率分布。由前面的讨论可知,  $\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}'$  ( $0 \leq \lambda \leq 1$ ) 也能使互信息达到信道容量, 即

$$I(\mathbf{p}) = I(\mathbf{p}') = I(\lambda \mathbf{p} + (1 - \lambda) \mathbf{p}') = C$$

引入第三个随机变量  $Z$ , 其概率分布为

$$\begin{aligned} &P(Z = c_1) = \alpha \\ &P(Z = c_2) = 1 - \alpha \end{aligned}$$

并用  $Z$  来控制  $X$ , 如图 4.7 所示。这样, 我们把  $\mathbf{p}$  和  $\mathbf{p}'$  看成是  $Z$  在取  $c_1$  和  $c_2$  时的输入字母的条件概率分布, 即

$$\mathbf{p} = (p(a_1 | z = c_1), p(a_2 | z = c_1), \dots, p(a_K | z = c_1))$$

$$\mathbf{p}' = (p(a_1 | z = c_2), p(a_2 | z = c_2), \dots, p(a_K | z = c_2))$$

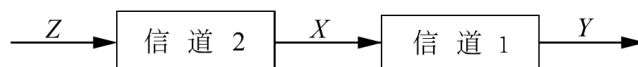


图 4.7 随机变量  $Z$  控制信道的输入  $X$

于是有

$$I(\mathbf{p}) = I(X; Y | z = a), \quad I(\mathbf{p}) = I(X; Y | z = a)$$

故有

$$I(\mathbf{p}) + (1 - \lambda) I(\mathbf{p}) = I(X; Y | Z)$$

而

$$I(\mathbf{p}) + (1 - \lambda) I(\mathbf{p}) = C$$

$$I(\mathbf{p} + (1 - \lambda)\mathbf{p}) = I(X; Y)$$

因此,有

$$I(X; Y) = I(X; Y | Z) \quad (4.60)$$

另一方面,因为  $ZXY$  构成马氏链,故应有

$$I(Z; Y | X) = 0 \quad (4.61)$$

而

$$\begin{aligned} I(Y; XZ) &= I(X; Y) + I(Z; Y | X) \\ &= I(Z; Y) + I(X; Y | Z) \end{aligned}$$

将其代入式(4.60)和式(4.61),可得

$$I(Z; Y) = 0 \quad (4.62)$$

这说明  $Y$  和  $Z$  统计独立,即

$$p(b_j | z = a) = p(b_j | z = a) = p(b_j), \quad j = 1, 2, \dots, J$$

这表明  $\mathbf{p}$  和  $\mathbf{p}$  给出相同的输出概率分布。所以输出概率分布唯一。

(3) 由离散无记忆信道的信道容量定理 4.3 可知,只要满足

$$I(x = a_k; Y) = C, \quad p(a_k) > 0$$

互信息即可达到信道容量。而

$$I(x = a_k; Y) = \sum_{j=1}^J q(b_j | a_k) \log \frac{q(b_j | a_k)}{p(b_j)}$$

只与信道的前向转移概率  $\mathbf{Q}$  及输出概率分布  $p(b_j) (j = 1, 2, \dots, J)$  有关,所以,任何使输出概率分布满足定理 4.3 要求的输入概率分布都能使互信息达到最大。证毕

下面这一定理说明在什么情况下互信息达到信道容量时的输入概率分布会唯一,它同时也说明了在一般情况下为什么达到信道容量时的输入概率分布不是唯一的。

**定理 4.7** 在达到信道容量时,如果输入概率分布中具有零概率的字母总数达到最大,则此时非零概率可被唯一地确定,且这些非零概率的输入字母总数不会

超过输出字母的总数。

证明 设  $M$  是使互信息达到信道容量的输入概率分布中具有非零概率的字母的最少数目, 这些具有非零概率的输入字母组成集合  $A$ 。再假设信道容量有解, 且达到信道容量时的输出概率分布为  $p_0(b_j)(j=1, 2, \dots, J)$ 。则有

$$\sum_{a_k \in A} p(a_k) q(b_j | a_k) = p_0(b_j), \quad j = 1, 2, \dots, J \quad (4.63)$$

这  $J$  个方程至少可以求出  $p(a_k)(k=1, 2, \dots, K)$  的一个解, 设为  $p_0(a_k)(k=1, 2, \dots, K)$ 。假若此解不唯一, 则与方程(4.63)对应的齐次方程组必有非零解, 设为  $h$  即有

$$\sum_{a_k \in A} h(a_k) q(b_j | a_k) = 0 \quad (4.64)$$

于是对  $\alpha \in [0, 1]$ , 有

$$\begin{aligned} & \sum_{a_k \in A} [\alpha p_0(a_k) + (1-\alpha) h(a_k)] q(b_j | a_k) \\ &= \sum_{a_k \in A} \alpha p_0(a_k) q(b_j | a_k) + \sum_{a_k \in A} (1-\alpha) h(a_k) q(b_j | a_k) = \alpha p_0(b_j) \end{aligned}$$

这说明  $\alpha p_0(a_k) + (1-\alpha) h(a_k)$  为式(4.63)的解。而

$$\sum_{a_k \in A} [\alpha p_0(a_k) + (1-\alpha) h(a_k)] = 1$$

即

$$\sum_{a_k \in A} \alpha p_0(a_k) + \sum_{a_k \in A} (1-\alpha) h(a_k) = 1$$

注意

$$\sum_{a_k \in A} p_0(a_k) = 1$$

故有

$$\sum_{a_k \in A} h(a_k) = 0$$

这说明  $h(a_k)(k=1, 2, \dots, K)$  中必有小于零的项, 因此, 改变  $\alpha$  的取值, 总可以找到  $\alpha_0$ , 使  $\alpha_0 p_0(a_k) + (1-\alpha_0) h(a_k)(k=1, 2, \dots, K)$  中某一项为零。这样就得到一个新的输入概率分布, 它只有  $M-1$  个字母具有非零概率。这与原假设  $M$  是使互信息达到信道容量的输入概率分布中具有非零概率的字母的最少数目相矛盾, 故方程(4.63)的解唯一。

又因方程(4.63)的解唯一, 故必有  $M=J$ 。

证毕

至此我们就结束对离散信道的讨论,下一节我们将转向连续信道。

## 4.6 连续信道的信道容量

在本章第一节对信道进行一般讨论时,我们曾提到一类重要的信道模型,即连续信道。连续信道是时间离散、幅度连续的信道的简称。一般地,连续信道的输入信号和输出信号可以在整个实数域或其某个子集上连续取值。连续信道输入/输出之间的多维条件概率密度构成了对这种信道的描述。

设信道的输入序列为  $\mathbf{x} = x_1 x_2 \dots x_N$ , 相应的输出序列为  $\mathbf{y} = y_1 y_2 \dots y_N$ , 则多维条件概率密度为

$$q(\mathbf{y} | \mathbf{x}) = q(y_1 y_2 \dots y_N | x_1 x_2 \dots x_N)$$

和离散信道时一样,连续信道同样可以分为有记忆和无记忆两类。对稳恒的无记忆连续信道而言,信道的输出只与其相应的输入有关,而且这一关系不随时间而变,即

$$q(\mathbf{y} | \mathbf{x}) = \prod_{n=1}^N q(y_n | x_n) \quad (4.65)$$

其中  $q(y_n | x_n) = q(y | x)$  不随时间而改变。因此,稳恒的无记忆连续信道只需要用  $q(y | x)$  就可以完整描述其信道的统计特性。

但是,与离散信道不同的是,连续信道的输入所取的值域不足以完全表示对信道输入的限制,因为不同的信号取值往往对应于信道在传输信号时所花费的不同的费用,如功率。这样,连续信道的信道容量与信道输入/输出的值域有关,而且还与信道传输信号时所允许的平均费用有关。为了能适当地反映这一关系,在连续信道中我们使用信道的容量费用函数来描述信道传输信息的能力。

假设我们用随机矢量  $\mathbf{X} = (X_1 X_2 \dots X_N)$  来表示连续信道的输入,其概率密度函数为  $p(\mathbf{x}) = p(x_1 x_2 \dots x_N)$ , 信道输入为  $\mathbf{x}$  时所对应的费用设为  $b(\mathbf{x})$ , 则在概率密度为  $p(\mathbf{x})$  的条件下的平均费用为

$$E\{b(\mathbf{X})\} = \int_{\mathbf{x}} p(\mathbf{x}) b(\mathbf{x}) d\mathbf{x} = \prod_{n=1}^N E\{b(X_n)\} \quad (4.66)$$

于是,我们定义连续信道的容量费用函数  $C(\cdot)$  为

$$C(\cdot) = \lim_{N \rightarrow \infty} \frac{1}{N} C_N(\cdot) \quad (4.67)$$

其中

$$C_N(\cdot) = \sup_{p(\mathbf{x})} \{ I(\mathbf{X}; \mathbf{Y}); E\{b(\mathbf{X})\} \leq N \} \quad (4.68)$$

式中上确界在  $I(\mathbf{X}; \mathbf{Y})$  存在最大值时, 式(4.68)也可以直接用最大值记号代替, 即

$$C_N(\cdot) = \max_{p(\mathbf{x})} \{ I(\mathbf{X}; \mathbf{Y}); E\{b(\mathbf{X})\} \leq N \} \quad (4.69)$$

和离散无记忆信道一样, 对连续无记忆信道也存在关系

$$I(\mathbf{X}; \mathbf{Y}) = \lim_{N \rightarrow \infty} \frac{1}{N} I(X_N; Y_N) = NI(X; Y) = NI(\mathbf{p}, \mathbf{Q})$$

故连续无记忆信道的容量费用函数一般情况下为

$$C(\cdot) = \sup_{p(\mathbf{x})} \{ I(\mathbf{p}, \mathbf{Q}); E\{b(X)\} \leq \cdot \} \quad (4.70)$$

或

$$C(\cdot) = \max_{p(\mathbf{x})} \{ I(\mathbf{p}, \mathbf{Q}); E\{b(X)\} \leq \cdot \} \quad (4.71)$$

当  $I(\mathbf{p}, \mathbf{Q})$  存在最大值时。

与离散信道时类似, 在连续信道下求解信道容量费用函数也是比较困难的, 即使是在无记忆的一般连续信道下往往也只能给出数值解。但幸运的是, 实际信道中的大部分可以近似地看成是稳恒加性噪声信道, 这种信道的输入/输出条件概率密度(或前向转移概率密度)函数具有非常简单的形式, 能推导出一些简洁的信道容量费用函数的表达式, 而且其结果对实际工作有相当普遍的指导意义, 在理论上也极有价值, 因此我们本节的讨论将集中在这种信道上。

#### 4.6.1 无记忆加性噪声信道的信道容量费用函数

无记忆加性噪声信道是无记忆连续信道中最简单又最重要的一种信道。

设  $X$  和  $Y$  是无记忆连续信道的输入、输出。若  $X$  和  $Y$  之间满足

$$Y = X + Z \quad (4.72)$$

其中  $Z$  是独立无记忆噪声源的输出, 则称此信道为无记忆加性噪声信道。

无记忆加性噪声信道的前向转移概率密度函数可以这样求得: 设  $X = x$ ,  $Z = z$ , 则有

$$Y = y = x + z$$

所以, 无记忆加性噪声信道的前向转移概率密度函数为

$$q(y|x) = p_z(z = y - x) = p_z(y - x) \quad (4.73)$$

其中  $p_z(z)$  是噪声的概率密度函数。可以看出, 该信道的前向转移概率密度函

数是输入、输出之间差值的函数。由于这一原因,无记忆加性噪声信道也可以定义成前向转移概率密度是输入、输出之间差值函数的信道。这两个定义完全等效。差值转移概率密度函数使信道输入、输出之间的互信息有比较简单的关系。实际上,设输入的概率密度函数为  $p_X(x)$ , 则互信息  $I(X; Y)$  为

$$I(X; Y) = h(Y) - h(Y|X)$$

其中

$$\begin{aligned} h(Y|X) &= - \int p_X(x) q(y|x) \log q(y|x) dx dy \\ &= - \int p_X(x) p_Z(y-x) \log p_Z(y-x) dx dy \\ &= - \int p_X(x) p_Z(z) \log p_Z(z) dx dz \\ &= h(Z) \end{aligned} \quad (4.74)$$

于是有

$$I(X; Y) = h(Y) - h(Z) \quad (4.75)$$

如果我们取信道输入信号的平均功率  $E(X^2)$  作为信息传输的费用,则由式(4.70)可得无记忆加性噪声信道的信道容量费用函数为

$$\begin{aligned} C(P_s) &= \sup_{p_X(x)} \{ I(X; Y); E(X^2) \leq P_s \} \\ &= \sup_{p_X(x)} \{ h(Y) - h(Z); E(X^2) \leq P_s \} \end{aligned} \quad (4.76)$$

在上式中,由于  $h(Z)$  与  $p_X(x)$  无关,因此求最大值的运算只需对  $h(Y)$  进行。这一情况使求解信道容量费用函数的工作得到简化,并可得到一些非常有价值的结果。

## 4.6.2 无记忆加性高斯噪声信道的信道容量费用函数

在无记忆加性噪声信道中,如果噪声的概率密度是高斯分布的概率密度函数,则称此信道为无记忆加性高斯噪声信道。此类信道是深空通信、卫星通信等实际信道的非常理想的模型,而且因为高斯分布的热噪声是无法彻底避免的,因此它在理论上有很大的价值。

为求无记忆加性高斯噪声信道的信道容量费用函数,我们首先介绍下面的定理。

**定理 4.8** 若给定连续随机变量概率分布的均值和方差,则当随机变量的

概率密度函数取高斯分布时随机变量的微分熵取最大值。

证明 设  $p_{YG}(y)$  和  $p_Y(y)$  是具有相同的均值  $m$  和方差  $\sigma^2$  的两种分布, 其中  $p_{YG}(y)$  是高斯分布的概率密度函数,  $p_Y(y)$  是非高斯分布的概率密度函数。则

$$\begin{aligned}\log p_{YG}(y) &= \log \frac{1}{\sigma^2} \exp -\frac{(y-m)^2}{2\sigma^2} \\ &= -\frac{1}{2} \log(2\sigma^2) - \frac{(y-m)^2}{2\sigma^2}\end{aligned}\quad (4.77)$$

于是有

$$\begin{aligned}h_G(Y) &= -\int p_{YG}(y) \log p_{YG}(y) dy \\ &= -\frac{1}{2} \log(2\sigma^2) + \frac{1}{2} \\ &= -\frac{1}{2} \log(2e\sigma^2)\end{aligned}\quad (4.78)$$

另一方面, 有

$$\begin{aligned}-\int p_Y(y) \log p_{YG}(y) dy &= -\int p_Y(y) \left[ -\frac{1}{2} \log(2\sigma^2) - \frac{(y-m)^2}{2\sigma^2} \right] dy \\ &= \frac{1}{2} \log(2\sigma^2) + \frac{1}{2\sigma^2} \int p_Y(y) (y-m)^2 dy \\ &= \frac{1}{2} \log(2\sigma^2) + \frac{1}{2\sigma^2} \sigma^2 \\ &= \frac{1}{2} \log(2e\sigma^2)\end{aligned}\quad (4.79)$$

比较式(4.78)和式(4.79), 可以得到

$$-\int p_Y(y) \log p_{YG}(y) dy = -\int p_{YG}(y) \log p_{YG}(y) dy \quad (4.80)$$

于是高斯分布的微分熵与一般非高斯分布的微分熵之差为

$$\begin{aligned}h_G(Y) - h(Y) &= -\int p_{YG}(y) \log p_{YG}(y) dy + \int p_Y(y) \log p_Y(y) dy \\ &= \int p_Y(y) \log \frac{p_Y(y)}{p_{YG}(y)} dy \\ &= \int p_Y(y) \left[ 1 - \frac{p_{YG}(y)}{p_Y(y)} \right] dy = 0\end{aligned}\quad (4.81)$$

这就证明了在具有相同均值和方差的随机变量中, 高斯分布的随机变量具有最

大的微分熵。同时高斯分布的随机变量的熵只与方差有关,因此在功率一定下,均值为零的高斯分布具有最大的微分熵。证毕

由此,我们可按下述步骤求无记忆加性高斯噪声信道的信道容量费用函数:

(1) 设噪声  $Z$  的概率密度函数为  $p_Z(z)$ , 则

$$p_Z(z) = \frac{1}{\sqrt{2\pi} P_N} \exp \left( -\frac{z^2}{2P_N} \right) \quad (4.82)$$

其中,  $E(Z) = 0$ ,  $E(Z^2) = P_N$ 。则其微分熵为

$$h(Z) = \frac{1}{2} \log(2\pi e P_N) \quad (4.83)$$

(2) 根据式(4.76), 求  $h(Y)$  在  $E(X^2) = P_S$  约束条件下的最大值  
由于

$$E(Y) = E(X) + E(Z) = E(X)$$

且信号的非零均值不会带来微分熵的增加,在方差受限的情况下,微分熵的最大值只与方差有关,所以可以取  $E(Y) = E(X) = 0$ 。又

$$\begin{aligned} E(Y^2) &= E(X^2 + 2XZ + Z^2) = E(X^2) + E(Z^2) + 2E(XZ) \\ &= E(X^2) + E(Z^2) = P_S + P_N \end{aligned} \quad (4.84)$$

由定理 4.8 可知,在均值为零、方差为  $P_S + P_N$  的条件下,高斯分布具有最大的微分熵,即

$$\sup_{p_X(x)} h(Y) = \frac{1}{2} \log[2\pi e(P_S + P_N)] \quad (4.85)$$

因此,  $Y$  的分布是均值为零、方差为  $P_S + P_N$  的高斯分布。

得到  $Y$  的分布后,输入  $X$  的分布即可由  $X = Y - Z$  得到。由于现在  $Y$  和  $Z$  均为高斯分布,所以不难由特征函数得到  $X$  也为高斯分布,即

$$p_X(x) = \frac{1}{\sqrt{2\pi} P_S} \exp \left( -\frac{x^2}{2P_S} \right) \quad (4.86)$$

(3) 由式(4.76)即可得到无记忆加性高斯噪声信道的信道容量费用函数为

$$C(P_S) = \frac{1}{2} \log \left( 1 + \frac{P_S}{P_N} \right) \quad (4.87)$$

上述结果对实际工作具有重大的指导意义。它说明当利用具有高斯分布的信号作为信道的输入时,无记忆加性高斯噪声信道的信道容量可以得到充分的利用。也就是说在无记忆加性高斯噪声信道中传输信息时,高斯分布的信号是最有效的,所谓有效是指在同样的信号功率下信道可以传输最多的信息。与此同时,我们在这里要同时指出与此有密切关系的另一个结论,即在无记忆加性噪



声信道中高斯分布的噪声对高斯分布的输入信号具有最大的破坏力。下述定理说明了这一点。

**定理 4.9** 在无记忆加性噪声信道中, 设输入信号  $X$  具有高斯分布  $p_{XG}(x)$ , 加性噪声的功率为  $P_N$ , 则当噪声的概率密度函数取高斯分布  $p_{ZG}(z)$  时, 输入/输出的互信息达到最小。

**证明** 当噪声取高斯分布时, 信道输出  $Y$  的分布也为高斯分布, 且

$$\begin{aligned} p_{YG}(y) &= \int_x p(x, y) dx \\ &= \int_x p_{XG}(x) q(y/x) dx \\ &= \int_x p_{XG}(x) p_{ZG}(z = y - x) dx \end{aligned} \quad (4.88)$$

如果噪声的分布为非高斯分布, 则信道输出  $Y$  的分布也为非高斯分布, 且

$$p_Y(y) = \int_x p_{XG}(x) p_Z(z = y - x) dx \quad (4.89)$$

我们用  $I(X_G; Y_G)$  和  $I(X_G; Y)$  分别代表  $Y$  为高斯分布和非高斯分布时信道输入/输出之间的互信息, 则有

$$\begin{aligned} I(X_G; Y) - I(X_G; Y_G) &= h(Y) - h(Z) - h_G(Y) + h_G(Z) \\ &= - \int p_Y(y) \log p_Y(y) dy + \int p_Z(z) \log p_Z(z) dz + \\ &\quad \int p_{YG}(y) \log p_{YG}(y) dy - \int p_{ZG}(z) \log p_{ZG}(z) dz \end{aligned}$$

利用证明定理 4.8 时的中间结果式(4.80), 可以得到

$$\begin{aligned} I(X_G; Y) - I(X_G; Y_G) &= \int p_Y(y) [\log p_{YG}(y) - \log p_Y(y)] dy + \\ &\quad \int p_Z(z) [\log p_Z(z) - \log p_{ZG}(z)] dz \end{aligned}$$

将式(4.89)代入上式, 并作变量代换  $z = y - x$ , 即得

$$\begin{aligned} I(X_G; Y) - I(X_G; Y_G) &= \int p_{XG}(x) p_Z(y - x) \log \frac{p_{YG}(y)}{p_Y(y)} dy dx + \\ &\quad \int p_{XG}(x) p_Z(y - x) \log \frac{p_Z(y - x)}{p_{ZG}(y - x)} dy dx \\ &= \int p_{XG}(x) p_Z(y - x) \log \frac{p_{YG}(y) p_Z(y - x)}{p_Y(y) p_{ZG}(y - x)} dy dx \\ &\quad \int p_{XG}(x) p_Z(y - x) \left[ 1 - \frac{p_Y(y) p_{ZG}(y - x)}{p_{YG}(y) p_Z(y - x)} \right] dy dx \end{aligned}$$

$$\begin{aligned}
 &= 1 - \frac{p_Y(y)}{p_{YG}(y)} \int p_{XG}(x) p_{ZG}(y-x) dx dy \\
 &= 0
 \end{aligned}$$

其中  $\int p_{XG}(x) p_{ZG}(y-x) dx = p_{YG}(y)$ , 故有

$$I(X_G; Y) = I(X_G; Y_G) \quad (4.90)$$

证毕

高斯分布在作为输入信号概率分布时的有利于信息传输与作为加性噪声功率分布时的不利于信息传输这两个结果突出地说明了高斯分布的随机变量具有最大微分熵这一特性,它是同一特性在两种情况下的两种表现形式。

### 4.6.3 一般无记忆加性噪声信道的信道容量费用函数的界

对一般的无记忆加性噪声信道,由式(4.76)所表示的信道容量费用函数无法给出解析形式的解。然而,我们可以利用这一表达式对信道容量费用函数的值作出估计,并给出其上下界的表达式。

(1) 下界

根据式(4.76),我们有

$$\begin{aligned}
 C(P_s) &= \sup_{p_{X(x)}} [I(X; Y); E(X^2) = P_s] \\
 &= I(X_G; Y) \quad (4.91)
 \end{aligned}$$

其中,  $I(Y_G; Y)$  是输入信号取方差为  $P_s$  的高斯分布时信道输入/输出之间的互信息。又由上节的定理 4.9 可知

$$I(X_G; Y) = I(X_G; Y_G)$$

其中,  $Y_G$  为信道的噪声具有与一般噪声相同的方差且为高斯分布时的输出。

由式(4.87)可知

$$I(X_G; Y_G) = \frac{1}{2} \log \left( 1 + \frac{P_s}{P_N} \right)$$

于是有

$$C(P_s) = I(X_G; Y_G) = \frac{1}{2} \log \left( 1 + \frac{P_s}{P_N} \right) \quad (4.92)$$

此即一般无记忆加性噪声信道的信道容量费用函数的下界。

(2) 上界

当输入信号功率限制在  $P_s$  以下, 噪声功率已给定为  $P_N$  时, 由式(4.84)可知此时输出信号的功率将小于等于  $P_s + P_N$ 。由式(4.85)可知, 此时  $Y$  的微分熵  $h(Y)$  为

$$h(Y) = \frac{1}{2} \log[2 e (P_s + P_N)] \quad (4.93)$$

于是

$$C(P_s) = \frac{1}{2} \log[2 e (P_s + P_N)] - h(Z) \quad (4.94)$$

式中  $h(Z)$  的取值将取决于  $Z$  的概率分布。当给出  $Z$  的概率分布后就可得到  $h(Z)$  的表达式, 所以, 式(4.94)即为一般无记忆加性噪声信道的信道容量费用函数上界的表达式。

有时我们也利用熵功率的概念使上界得到另一种表示形式。我们知道, 在相同方差下高斯分布的随机变量具有最大的微分熵, 即

$$h(Z) = h_G(Z) = \frac{1}{2} \log(2 e P_N)$$

所以定义

$$P_e = \frac{1}{2 e} \exp(2 h(Z)) \quad (4.95)$$

为具有微分熵值  $h(Z)$  的随机变量  $Z$  的熵功率。从物理意义上讲, 熵功率是具有相同微分熵值的高斯随机变量的功率。

引进了熵功率后, 式(4.94)就可以写成

$$C(P_s) = \frac{1}{2} \log \frac{P_s + P_N}{P_e} \quad (4.96)$$

综合式(4.92)和式(4.96), 即得到一般无记忆加性噪声信道的信道容量费用函数的估计值为

$$\frac{1}{2} \log \left( 1 + \frac{P_s}{P_N} \right) = C(P_s) = \frac{1}{2} \log \frac{P_s + P_N}{P_e}$$

#### 4.6.4 无记忆加性高斯噪声信道的级联和并联

由多个无记忆加性高斯噪声信道进行级联或并联所组成的复合信道是一种有用的信道模型。在这一小节中我们要讨论这种复合信道的信道容量费用函数。

级联信道的情况比较简单, 因为对无记忆加性高斯噪声信道来讲级联的效果

仅仅是使各个组成信道的噪声得到累加,其和仍为高斯噪声,且噪声功率为各组成信道的噪声功率之和。于是级联信道的信道容量函数仍可以按照式(4.87)计算。

对于并联信道(这里指并用信道),设有  $N$  个无记忆加性高斯噪声信道被并联使用,各信道的输入、输出分别为  $X_n, Y_n (n = 1, 2, \dots, N)$ , 各信道的信号功率和噪声功率分别为  $P_{S_n}$  和  $P_{N_n} (n = 1, 2, \dots, N)$ , 且并联信道的总约束为信号总功率小于  $P_S$ , 即

$$\sum_{n=1}^N P_{S_n} = P_S, \quad P_{S_n} \geq 0 \quad (4.97)$$

于是此并联信道的信道容量函数为

$$\begin{aligned} C(P_S) &= \sup_{p(\mathbf{X})} I(\mathbf{X}; \mathbf{Y}); \quad \sum_{n=1}^N P_{S_n} = P_S \\ &= \sup_{p(\mathbf{X})} I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N); \quad \sum_{n=1}^N P_{S_n} = P_S \end{aligned} \quad (4.98)$$

其中,上确界是在输入信号的联合概率密度函数  $p(x_1 x_2 \dots x_N)$  在式(4.97)的约束条件下取的。根据节4.4.2中对并用信道的分析可知

$$I(\mathbf{X}; \mathbf{Y}) = \sum_{n=1}^N I(X_n; Y_n) \quad (4.99)$$

其中等号当且仅当各分量统计独立时才成立。所以,为求  $C(P_S)$ , 首先应使各组成信道的输入统计独立,并使各组成信道的输入/输出之间的互信息各自达到最大,然后在约束条件(4.97)下求

$$C(P_S) = \max_{\sum_{n=1}^N P_{S_n} = P_S} \sum_{n=1}^N \frac{1}{2} \log \left( 1 + \frac{P_{S_n}}{P_{N_n}} \right) \quad (4.100)$$

这又是凸函数在约束条件下求极值的问题,可以从以下两个方面去考虑:

(1) 若极值不发生在边缘上,即约束条件中  $P_{S_n} \geq 0$  自然满足,此时即可按照极值点的充要条件求解,即取

$$\frac{\partial}{\partial P_{S_n}} \sum_{i=1}^N \frac{1}{2} \log \left( 1 + \frac{P_{S_i}}{P_{N_i}} \right) - \lambda \sum_{i=1}^N P_{S_i} = 0 \quad (4.101)$$

化简得

$$P_{N_n} + P_{S_n} = \frac{1}{2\lambda} \quad (4.102)$$

考虑到  $\sum_{n=1}^N P_{S_n} = P_S$ , 并令  $\sum_{n=1}^N P_{N_n} = P_N$ , 则由式(4.102)可得

$$\sum_{n=1}^N (P_{N_n} + P_{S_n}) = P_S + P_N = \frac{N}{2}$$

即

$$\frac{1}{N} = \frac{2}{N} (P_S + P_N) \quad (4.103)$$

所以

$$P_{S_n} = \frac{P_S + P_N}{N} - P_{N_n} \quad (4.104)$$

(2) 若极值发生在边缘上,则需要反复试算各边缘上无极值。边缘上存在极值的充要条件为

$$\frac{1}{P_{S_n}} \sum_{i=1}^N \frac{1}{2} \log \left( 1 + \frac{P_{S_i}}{P_{N_i}} \right) - \sum_{i=1}^N P_{S_i} < 0 \quad (4.105)$$

化简得

$$P_{N_n} + P_{S_n} > \frac{1}{2}, \quad \text{当 } P_{S_n} = 0 \text{ 时} \quad (4.106)$$

由此可知  $P_{S_n} = 0$  一定首先发生在  $P_{N_n}$  较大的组成信道上,因此试算可以首先从具有最大噪声功率的信道开始,令其  $P_{S_n} = 0$ ,然后对剩余信道按式(4.101)求解。若式(4.101)仍无解,则使次大噪声功率的信道的  $P_{S_n} = 0$ ,再对剩余的  $N - 2$ 个信道按式(4.101)求解。如此继续下去,直至得到真正的解。

$N$  个无记忆加性高斯噪声信道的并用信道的解的一般情况如图 4.8 所示。

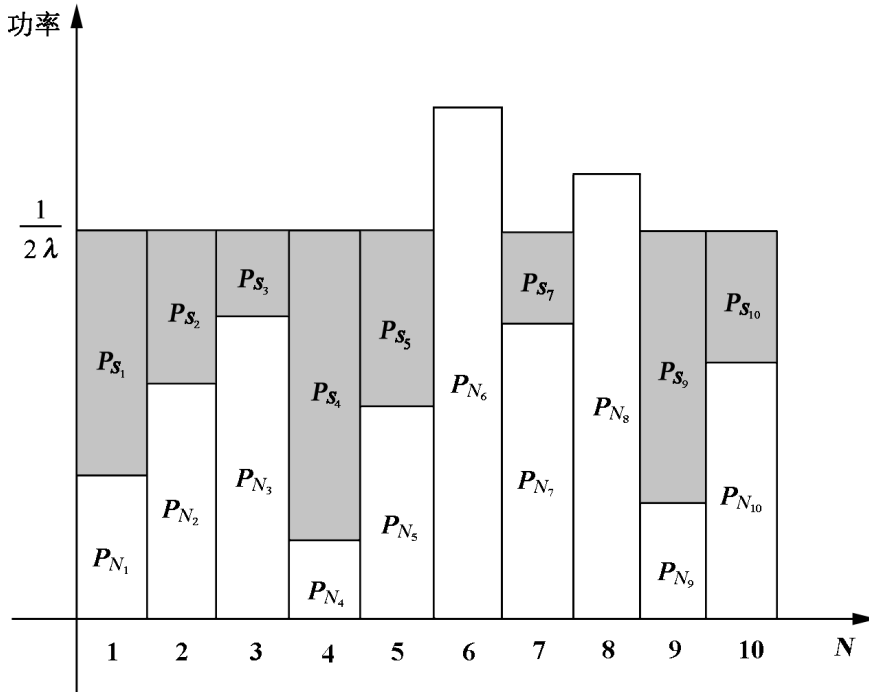


图 4.8 并联信道中的功率分配

图中阴影部分的总面积为  $P_s$ 。 $P_s$  在各组成信道中的功率分配就像水在一个底部不平的水池中漫溢一样,个别噪声功率特别大的信道,即使在水池中的总水量达到  $P_s$  时仍可能没有分配到任何信号功率。

## 4.7 模拟信道的信道容量

在连续信道的基础上我们现在进一步转向讨论模拟信道。如本章第一节所述,模拟信道是输入和输出信号在幅度和时间上都连续取值的信道。不难理解,模拟信道是供信息传输的物理媒体,如光纤、电缆、电磁波传布的大气层或宇宙空间等的最为恰当的信道模型,因此,对模拟信道的研究具有重大的实际意义和实用价值。但是对模拟信道的严格的理论研究会遇到数学上的某些困难或需要更深的数学工具,所以我们在下面的讨论采用在数学上可能不够严格但在工程上可被接受的方法。这样我们就可以在较小的篇幅内介绍一些工程上有用的结论。

### 4.7.1 模拟随机信号的正交展开

分析和处理模拟信号的一个有效方法就是在选择一组合适的归一化正交函数族  $\{e_n(t)\}$  的基础上,通过积分变换使模拟信号可以用一组离散的可数数列来表示。在数学上,为了使这样的表示真正可行,一般把模拟信号限定为平方可积的复函数,即模拟信号  $x(t)$  应满足条件

$$\int_T |x(t)|^2 dt < \infty \quad (4.107)$$

我们将满足上述条件的函数  $x(t)$  记作  $L^2$  函数,或  $L^2(T)$  函数以指明函数的定义域为  $T$ 。这样的限制并不是所有的函数都满足的,例如冲激函数和无限时间域上的三角函数等就不满足此限制,但是在工程上遇到的信号则总是可以看成是这样的时间函数。

我们知道,一个归一化的正交函数族  $\{e_n(t)\}$  是指该集中的每个函数都是归一化的,且每一对函数又都是正交的,即

$$\int_T e_i(t) e_j^*(t) dt = \begin{cases} 1, & \text{当 } i = j \\ 0, & \text{当 } i \neq j \end{cases} \quad (4.108)$$

利用这一归一化正交函数族,我们可以得到任一  $L^2$  函数  $x(t)$  对应的离散数列

$\{x_n\}$ , 其中  $x_n$  为

$$x_n = \int_T x(t) e_n^*(t) dt \quad (4.109)$$

若所选的归一化正交函数族  $\{e_n(t)\}$  能使任一  $L^2$  函数  $x(t)$  及其离散数列  $\{x_n\}$  满足

$$\lim_N \int_T \left| x(t) - \sum_{n=1}^N x_n e_n(t) \right|^2 dt = 0 \quad (4.110)$$

则称集合  $\{e_n(t)\}$  是一个完备的归一化正交函数族, 且式(4.110)称为 Parseval 等式。

下面回顾一下  $L^2$  函数的级数表达式。根据式(4.110),  $L^2$  函数  $x(t)$  可写成

$$x(t) = \sum_{n=1}^{\infty} x_n e_n(t) + x_r(t) \quad (4.111)$$

其中  $x_r(t)$  满足

$$\int_T x_r(t) e_n^*(t) dt = 0, \quad \text{对所有 } n \text{ 成立} \quad (4.112)$$

所以, 在这个意义下, 我们把式(4.111)经常写成

$$x(t) = \sum_{n=1}^{\infty} x_n e_n(t) \quad (4.113)$$

而工程上遇到的大部分信号的确可以使  $x_r(t) = 0$ 。

式(4.113)给出了  $L^2$  函数用归一化正交函数族进行展开的级数表达式, 它表明  $L^2$  函数可以用归一化正交函数的线性组合来逼近, 或者说式(4.113)也给出了  $L^2$  函数空间到无限维复矢量空间的映射关系, 从而使  $L^2$  函数空间中的函数  $x(t)$  可以用一个无限维矢量  $(x_1 \ x_2 \ \dots \ x_n \ \dots \ x)$  来表示。对模拟信号来说, 这是一个非常有力的分析手段, 它不但能给我们一个形象直观的理解方法, 而且使我们在分析模拟信号时可以应用矢量空间中的许多概念和分析方法。

作为归一化正交函数族的例子, 我们下面举出两个最常用的归一化正交函数族。

### (1) 复正弦函数

复正弦函数族  $\frac{1}{2} e^{jn\pi t}, n=0, \pm 1, \pm 2, \dots$  组成信号空间  $L^2(-1, +1)$  中的

完备的归一化正交函数族。  $L^2(-1, +1)$  中的任意函数都可在式(4.111)和式(4.112)的意义下展开成

$$x(t) = \sum_{n=-\infty}^{+\infty} \frac{1}{2} x_n e^{jn\pi t} \quad (4.114)$$

其中

$$x_n = \frac{1}{2} \int_{-1}^{+1} x(t) e^{-jn\pi t} dt \quad (4.115)$$

这就是傅里叶展开式。

## (2) 采样函数或 sinc 函数

在数字信号处理中广泛应用低通实信号或基带实信号的采样函数族

$$\frac{\sin 2W(t - \frac{n}{2W})}{2W(t - \frac{n}{2W})}, \quad n=0, \pm 1, \pm 2, \dots$$

是  $L^2(-\infty, +\infty)$  上的一个归一化正交函数族。对于频带限制在  $(-W, +W)$  的基带信号  $x(t)$  来讲, 都可以用这一函数族展开成

$$\begin{aligned} x(t) &= \sum_{n=-\infty}^{+\infty} x_n \frac{\sin 2W(t - \frac{n}{2W})}{2W(t - \frac{n}{2W})} \\ &= \sum_{n=-\infty}^{+\infty} x_n 2W \operatorname{sinc} 2W(t - \frac{n}{2W}) \end{aligned} \quad (4.116)$$

其中

$$x_n = \int_{-\infty}^{+\infty} x(t) 2W \operatorname{sinc} 2W(t - \frac{n}{2W}) dt = \frac{1}{2W} x(\frac{n}{2W}) \quad (4.117)$$

但是这一函数族不能用来展开频带超过  $W$  的基带信号, 所以它不是  $L^2(-\infty, +\infty)$  上的完备的归一化正交函数族。

对同一个  $L^2$  函数, 在不同的完备归一化正交函数族下会得到不同的展开表达式。虽然从函数逼近的角度看, 这种不同的展开在项数趋于无穷时都可使和式在均方意义上收敛于所逼近的函数, 但是在函数正交展开的实际应用中如何选择恰当的完备归一化正交函数族往往还有其他考虑。对随机信号而言, 下述的  $K$ - $L$  展开具有特别重要的意义。

设  $x(t)$  是零均值随机过程的一个实现或一个样本,  $\{\phi_n(t)\}$  是完备的归一化正交函数族, 因此,  $x(t)$  可以按式 (4.113) 展开, 其中系数  $x_n$  可按式 (4.109) 求得。这些系数的二阶矩为



$$\begin{aligned}
 E(x_i, x_j^*) &= \int_T \int_T e_i^*(t) e_j(t) E[x(t) x^*(t)] dt dt \\
 &= \int_T \int_T R_X(t, t) e_i^*(t) e_j(t) dt dt \quad (4.118)
 \end{aligned}$$

其中  $R_X(t, t)$  是随机信号的相关函数。如果我们选择  $\{e_n(t)\}$  为齐次方程

$$\int_T R_X(t, t) e_j(t) dt = \lambda_j e_j(t) \quad (4.119)$$

的解, 则将此式代入式(4.118)中得

$$E(x_i, x_j^*) = \int_T \lambda_j e_j(t) e_i^*(t) dt = \lambda_j \delta_{ij} \quad (4.120)$$

若  $x(t)$  不是零均值的信号, 我们可以取  $x(t) - E[x(t)]$  作为新的随机信号而获得与式(4.120)类似的关系。这一关系说明, 利用满足条件(4.119)的归一化正交函数族对  $L^2$  函数进行展开所得的系数彼此不相关或者说是线性独立的。满足式(4.119)的函数在数学上被称为积分方程核函数  $R_X(t, t)$  的特征函数。当  $x(t)$  是零均值的随机过程时, 该积分方程的核函数是随机信号的自相关函数; 当  $x(t)$  是非零均值的随机过程时, 该积分方程的核函数则是随机信号的自协方差函数。利用随机过程自协方差函数或自相关函数的特征函数所构成的归一化正交函数族对  $L^2$  函数进行的展开被称为随机信号的 Karhunen-Loeve 展开, 简称 K-L 展开。

在随机过程理论中, 我们知道所谓零均值的高斯随机过程  $x(t)$  是指这样的随机过程, 它与任何  $L^2$  函数(如  $e(t)$ )的内积  $\int_T x(t) e^*(t) dt$  是一个零均值、有限方差的高斯随机变量。这样, 当我们对稳恒高斯过程进行 K-L 展开时, 所得的展开系数不仅是线性独立的, 而且是统计独立的, 因为对高斯随机变量而言, 这二者是等价的。所以对稳恒高斯过程进行 K-L 展开所得系数的联合概率密度可以直接写成各一维概率密度的乘积, 即

$$p(x_1, x_2, \dots, x_N) = \prod_{n=1}^N p(x_n)$$

这一特性对高斯随机过程的分析显然具有极大的意义。对非高斯随机过程, 虽然 K-L 展开在理论上的意义不如在高斯随机过程中那样大, 但在实际应用中仍然有一定的价值。

## 4.7.2 模拟信道下的信道容量费用函数及其计算

在我们简要讨论了模拟信号的正交展开以后, 我们现在可以转向研究模拟

信道的容量费用函数问题。

设模拟信道的输入信号为  $x(t)$ , 相应的输出信号为  $y(t)$ 。我们自然可以假定  $x(t)$  和  $y(t)$  都是  $L^2$  函数, 因此都可以分别在某种归一化正交函数族的基础上进行展开。设  $x(t)$ ,  $y(t)$  展开后的系数分别为  $(x_1, x_2, \dots, x_n, \dots)$  和  $(y_1, y_2, \dots, y_n, \dots)$ , 则信道的统计特性可以用所有  $N$  值下的联合条件概率密度函数  $q(y_1 y_2 \dots y_N | x_1 x_2 \dots x_N)$  来描述。在只取有限维系数时信道输入/输出之间的互信息为

$$I(\mathbf{X}; \mathbf{Y}) = \int_{\mathbf{x}} \int_{\mathbf{y}} p(\mathbf{x}) q(\mathbf{y} | \mathbf{x}) \log \frac{q(\mathbf{y} | \mathbf{x})}{\int_{\mathbf{x}} p(\mathbf{x}) q(\mathbf{y} | \mathbf{x}) d\mathbf{x}} d\mathbf{x} d\mathbf{y} \quad (4.121)$$

其中,  $\mathbf{X} = (X_1 X_2 \dots X_N)$ ,  $\mathbf{Y} = (Y_1 Y_2 \dots Y_N)$ ,  $\mathbf{x} = (x_1 x_2 \dots x_N)$ ,  $\mathbf{y} = (y_1 y_2 \dots y_N)$ 。由于模拟信号在一般情况下为无限维信号, 所以当  $N \rightarrow \infty$  时, 若式(4.121)的极限存在, 则此极限就是  $X(t)$  和  $Y(t)$  之间的平均互信息, 即

$$I(X(t); Y(t)) = \lim_{N \rightarrow \infty} I(\mathbf{X}; \mathbf{Y}) \quad (4.122)$$

在式(4.121)和式(4.122)的基础上, 我们定义持续时间为  $T$  的信道的信道容量费用函数  $C_T(\cdot)$  为

$$C_T(\cdot) = \lim_{N \rightarrow \infty} \sup_{p(\mathbf{x})} \{ I(\mathbf{X}; \mathbf{Y}); E[b(\mathbf{X})] \leq T \} \quad (4.123)$$

并由此定义模拟信道的容量费用函数  $C(\cdot)$  为

$$C(\cdot) = \lim_{T \rightarrow \infty} \frac{1}{T} C_T(\cdot) \quad (4.124)$$

式(4.124)成立的条件是该极限确实存在。

对模拟信道容量费用函数的一般性研究在数学上相当困难, 因此下面我们将只讨论两种非常简单、但又具有很实用价值和理论意义的信道。

#### 4.7.2.1 限带、加性白色高斯噪声信道

这是一种最理想化的模拟信道。在这种信道中, 信号和噪声被限制在一定的频带中, 一般设此频带为  $[0, W]$ 。信道传输的费用就是信号的功率。又设信道的噪声是加性、高斯的, 且具有平坦的功率谱, 均值为零。

对这样的信道, 因为其输入、输出信号和噪声都是限带的, 所以我们可以按照采样定理, 利用式(4.116)和式(4.117)的采样函数对输入、输出信号和噪声进行正交展开, 得

$$x(t) = \sum_{n=-\infty}^{+\infty} x_n \sqrt{2W} \operatorname{sinc} \left( 2Wt - \frac{n}{2W} \right) \quad (4.125)$$

$$z(t) = \sum_{n=-\infty}^{+\infty} z_n \operatorname{sinc} 2W \left( t - \frac{n}{2W} \right) \quad (4.126)$$

$$y(t) = \sum_{n=-\infty}^{+\infty} y_n \operatorname{sinc} 2W \left( t - \frac{n}{2W} \right) \quad (4.127)$$

又因为

$$y(t) = x(t) + z(t)$$

所以有

$$y_n = x_n + z_n \quad (4.128)$$

由于噪声是零均值的高斯随机过程,按照随机过程中关于高斯过程的定义,零均值的高斯随机过程与任何  $L^2$  函数乘积的积分是一个零均值的有限方差的高斯随机变量,所以,  $z_n$  是零均值的高斯随机变量。又因噪声  $z(t)$  的功率谱是一个矩形函数,由傅里叶变换可求得其相关函数为

$$R_z(\tau) = N_0 W \frac{\sin(2W\tau)}{2W\tau} \quad (4.129)$$

其中  $N_0$  为噪声的单边功率谱密度。根据这一相关函数,由式(4.118), (4.116) 和(4.117)有

$$\begin{aligned} E(z_n, z_n) &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} R_z(t_1, t_2) e_n(t_1) e_n(t_2) dt_1 dt_2 \\ &= \frac{1}{2W} \int_{-\infty}^{+\infty} R_z\left(\frac{n}{2W}, t_2\right) e_n(t_2) dt_2 \\ &= \frac{1}{2W} \frac{1}{2W} R_z\left(\frac{n}{2W}, \frac{n}{2W}\right) \\ &= \frac{1}{2W} R_z\left(\frac{n-n}{2W}\right) \\ &= \begin{cases} 0, & \text{当 } n \neq n \\ N_0/2, & \text{当 } n = n \end{cases} \end{aligned} \quad (4.130)$$

即噪声的各样值之间互不相关,所以噪声各样值相互独立。

在信道频带受限及信号存在时间长度有限的情况下,按照采样定理,对信号和噪声都只需要  $2WT$  个采样点。这样,这一模拟信道就可以看成是由  $2WT$  个由式(4.128)所表示的独立的连续加性高斯噪声信道的并联,如图 4.9 所示,其中,  $Y_n = X_n + Z_n$ ,  $n=1, 2, \dots, N$ ,  $N=2WT$ 。

各组成信道的噪声功率可由 Parseval 关系式(4.110)及噪声的稳恒性质求得,于是有

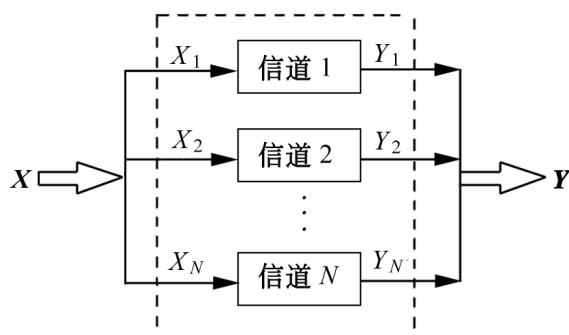


图 4.9 由  $2WT$  个独立的连续加性高斯噪声信道并联而表示的模拟信道

$$E \int_T z^2(t) dt = \sum_{n=1}^{2WT} E z_n^2 = 2WT \cdot E z_n^2 = N_0 WT$$

即

$$P_{N_n} = E z_n^2 = \frac{N_0}{2} \quad (4.131)$$

当然,直接由式(4.130)也可求得  $n=n$  时,正好该式为  $\frac{N_0}{2}$ 。根据节 4.6.2 中所求得的无记忆加性高斯噪声信道的信道容量式(4.87),可得各组成信道的输入/输出之间互信息为

$$I(X_n; Y_n) = \frac{1}{2} \log \left( 1 + \frac{2E(x_n^2)}{N_0} \right) \quad (4.132)$$

而对于并用的并联信道的输入/输出之间的互信息,由式(4.85)有

$$\begin{aligned} I(X_1 X_2 \dots X_{2WT}; Y_1 Y_2 \dots Y_{2WT}) &= \sum_{n=1}^{2WT} I(X_n; Y_n) \\ &= \sum_{n=1}^{2WT} \frac{1}{2} \log \left( 1 + \frac{2E(x_n^2)}{N_0} \right) \end{aligned} \quad (4.133)$$

由于上式中各输入信号样值的方差受到总功率的限制,即

$$P_{ST} = \sum_{n=1}^{2WT} E(x_n^2) = E \int_T x^2(t) dt = P_s T \quad (4.134)$$

根据 4.6.4 节对并用信道容量的讨论,当极值不发生在边缘时,有

$$P_{S_n} = \frac{P_{ST} + P_N}{N} - P_{N_n}$$

在这里,  $N = 2WT$ ,  $P_N = NP_{N_n} = 2WT \frac{N_0}{2} = WTN_0$ 。于是,当各样值功率相等

时, 即当

$$P_{s_n} = E(x_n^2) = \frac{P_s T}{2WT} = \frac{P_s}{2W} \quad (4.135)$$

时,  $I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N)$  取最大值, 即

$$\begin{aligned} \max I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N) \\ &= \frac{2WT}{2} \log \left( 1 + \frac{2 \frac{P_s}{2W}}{N_0} \right) \\ &= WT \log \left( 1 + \frac{P_s}{N_0 W} \right) \end{aligned} \quad (4.136)$$

将此结果代入定义式(4.123)和(4.124)中, 我们就得到限带、加性白色高斯噪声信道的容量费用函数为

$$C(P_s) = W \log \left( 1 + \frac{P_s}{N_0 W} \right) \quad (4.137)$$

这就是著名的关于信道容量的香农公式。

应顺便指出的是, 上述推导在数学上是粗糙的, 因为我们知道模拟信号不可能同时在时间和频带上受限。但是, 当  $WT$  的乘积值很大时, 我们可以越来越精确地认为信号在正交展开后只需要  $2WT$  个系数, 特别是当信号的持续时间趋于无穷时, 单位时间内的信号平均只有  $2W$  个采样值是自由的, 而在  $T$  时间段内平均只有  $2WT$  个自由的系数。因此, 这一近似是可以接受的, 我们将不再介绍数学上更严格的证明。

#### 4.7.2.2 一般高斯信道的容量费用函数

我们现在考虑较一般的高斯信道。假设模拟信道的传输函数  $H(f)$  不是理想的带通或低通, 信道的噪声也不是白色的高斯噪声, 假设其功率谱为  $N(f)$ 。这样的一般高斯限带信道如图 4.10 所示。对这样的信道严格计算其容量费用

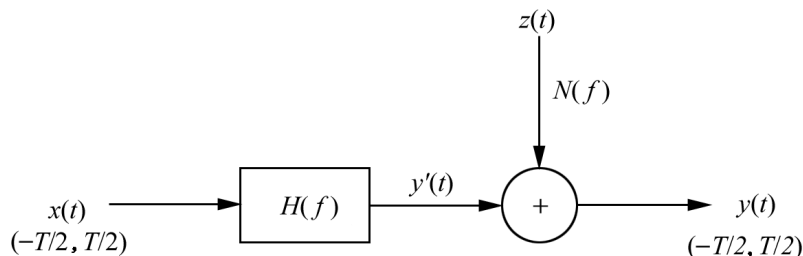


图 4.10 一般高斯信道

函数仍然是比较麻烦的,所以下面我们仍采用近似的、但工程上可接受的方法。

第一步,我们设法将此模拟信道等效为某种连续信道的并联。

设  $x(t)$  存在于有限的时间段  $-\frac{T}{2}, \frac{T}{2}$  内,将  $x(t)$  用如下归一化正交函数

族展开,即  $x(t) = \sum_{n=-\infty}^{+\infty} x_n \phi_n(t)$ , 其中

$$\begin{aligned} \phi_n(t) &= \begin{cases} \frac{2}{T} \cos n \frac{2\pi t}{T}, & n > 0, \quad |t| \leq \frac{T}{2} \\ \frac{1}{T}, & n = 0, \quad |t| \leq \frac{T}{2} \\ \frac{2}{T} \sin n \frac{2\pi t}{T}, & n < 0, \quad |t| \leq \frac{T}{2} \\ 0, & |t| > \frac{T}{2} \end{cases} \end{aligned} \quad (4.138)$$

各基函数通过信道滤波器后的输出为

$$y_n(t) = \int_{-T/2}^{T/2} x(\tau) h(t - \tau) d\tau \quad (4.139)$$

其中  $h(t)$  是与  $H(f)$  对应的冲激响应。可以想象,当  $T$  足够大时,式(4.139)将近似于时间段  $T$  内的三角函数,只是幅度差一个倍数  $|H(n/T)|$ ,且有一个相移。在  $h(t)$  是实函数的情况下,  $\phi_n(t)$  及其输出的相移与  $-\phi_n(t)$  及其输出的相移是相等的。这一情况使我们构造一个新的归一化正交函数族  $\{\phi_n(t)\}$ , 其中

$$\phi_n(t) = \frac{1}{H(n/T)} \int_{-T/2}^{T/2} x(\tau) h(t - \tau) d\tau \quad (4.140)$$

利用这一新的归一化正交函数族  $\{\phi_n(t)\}$  对  $y(t) = \int_{-T/2}^{T/2} x(\tau) h(t - \tau) d\tau$  进行展开,得到

$$\begin{aligned} y(t) &= \int_{-T/2}^{T/2} x(\tau) h(t - \tau) d\tau \\ &= \sum_{n=-\infty}^{+\infty} x_n \phi_n(t) \\ &= \sum_{n=-\infty}^{+\infty} x_n H(n/T) \phi_n(t) \\ &= \sum_{n=-\infty}^{+\infty} y_n \phi_n(t) \end{aligned} \quad (4.141)$$

其中

$$y_n = x_n H(n/T) \quad (4.142)$$

由于噪声  $z(t)$  不是白噪声, 我们可以将其看成是单边功率谱密度  $N_0$  的白噪声  $z(t)$  经过传输函数为  $N(f)$  的滤波器后所得到的输出, 即

$$z(t) = \int_{-\infty}^{+\infty} z(\tau) g(t - \tau) d\tau \quad (4.143)$$

其中

$$g(t) = \int_{-\infty}^{+\infty} N(f) e^{j2\pi ft} df \quad (4.144)$$

是  $N(f)$  的冲激响应。用  $\{z_n(t)\}$  对  $z(t)$  进行展开, 可得

$$z(t) = \sum_{n=-\infty}^{+\infty} z_n z_n(t) \quad (4.145)$$

其中

$$\begin{aligned} z_n &= \int_{-\infty}^{+\infty} z(t) z_n(t) dt \\ &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} z(\tau) g(t - \tau) d\tau z_n(t) dt \\ &= \int_{-\infty}^{+\infty} z(\tau) \int_{-\infty}^{+\infty} g(t - \tau) z_n(t) dt d\tau \end{aligned} \quad (4.146)$$

定义

$$z_n(\tau) = \int_{-\infty}^{+\infty} g(t - \tau) z_n(t) dt \quad (4.147)$$

则得

$$z_n = \int_{-\infty}^{+\infty} z(\tau) z_n(\tau) d\tau \quad (4.148)$$

根据前面对  $\{z_n(t)\}$  进行分析时所用的相同的道理可知  $z_n(t)$  也近似是时间段  $T$  内的三角函数, 故  $\{z_n(t)\}$  近似组成正交函数族, 且有

$$\int_{-T/2}^{T/2} z_n^2(\tau) d\tau = N_0 T \quad (4.149)$$

由于  $z(t)$  是白色高斯噪声, 按照随机过程理论中对白色高斯过程的定义,  $z(t)$  和任意  $L^2$  函数的乘积的积分值都是零均值的高斯随机变量, 所以  $z_n$  是零均值的高斯随机变量, 而且  $z_n$  的方差与  $z_n(\tau)$  具有下述关系式:

$$E z_n^2 = \frac{N_0}{2} \int_{-T/2}^{T/2} z_n^2(\tau) d\tau \quad (4.150)$$

类似的还可有

$$E z_m^2 = \frac{N_0}{2} \int_{-T/2}^{T/2} z_m^2(\tau) d\tau$$

及

$$E(z_n + z_m)^2 = \frac{N_0}{2} \int_{-T}^T \delta(t - t') dt$$

由此可知

$$E(z_n z_m) = 0, \quad \text{当 } n \neq m \text{ 时} \quad (4.151)$$

因此  $\{z_n\}$  是一组独立的高斯随机变量。

最后我们来看信道的输出  $y(t)$ , 已知

$$y(t) = x(t) + z(t) \quad (4.152)$$

用  $\{x_n(t)\}$  对  $y(t)$  进行展开, 得

$$y(t) = \sum_{n=-\infty}^{\infty} y_n x_n(t) \quad (4.153)$$

联合式(4.141), (4.142), (4.145)及式(4.152), (4.153), 即有

$$y_n = x_n H(nT) + z_n \quad (4.154)$$

或

$$\frac{y_n}{H(nT)} = x_n + \frac{z_n}{H(nT)} \quad (4.155)$$

这样, 整个模拟信道就可以看成是式(4.155)所表达的连续加性高斯噪声信道的并联, 其中, 各组成信道的输入为  $x_n$ , 输出为  $y_n/H(nT)$ , 噪声  $z_n/H(nT)$  的方差为  $N(nT)/|H(nT)|^2$ 。

第二步, 求等效的并联信道的容量费用函数。

这一并联信道所受的总约束是其平均功率不超过  $P_s T$ , 即

$$E \sum_{n=-\infty}^{\infty} x_n^2 \leq P_s T \quad (4.156)$$

根据节4.6.4对无记忆加性高斯噪声信道的并联的讨论, 特别是式(4.100), 不难得到持续时间为  $T$  的容量费用函数为

$$C_T(P_s T) = \max_{n \in I} \frac{1}{2} \log \frac{|H(nT)|^2}{2N(nT)} \quad (4.157)$$

其中,  $I$  是所有满足  $N(nT)/|H(nT)|^2 \leq 1/2$  的组成信道的集合, 而  $1/2$  是下式的解:

$$P_s T = \max_{n \in I} \frac{1}{2} - \frac{N(nT)}{|H(nT)|^2} \quad (4.158)$$

为达到此容量费用函数, 输入信号的总功率分配必须满足

$$E(x_n^2) = \frac{1}{2} - \frac{N(nT)}{|H(nT)|^2}, \quad n \in I$$

$$0, \quad n \notin I \quad (4.159)$$



这一结果的物理意义和节 4.6.4 中所述的完全一样。于是,由定义式(4.124)可知,此时信道的容量费用函数为

$$C(P_s) = \frac{1}{2T} \log \frac{|H(nT)|^2}{2N(nT)}$$

最后令  $T \rightarrow \infty$ , 则上式及式(4.158)和式(4.159)转为积分,即

$$C(P_s) = \int_F \frac{1}{2} \log \frac{|H(f)|^2}{2N(f)} df \quad (4.160)$$

其中,  $F$  是满足  $N(f) \leq |H(f)|^2$  的频率的集合,而  $F$  是下式的解:

$$P_s = \int_F \frac{1}{2} - \frac{N(f)}{|H(f)|^2} df \quad (4.161)$$

达到容量费用函数值时的功率分配为

$$P_s(f) = \begin{cases} \frac{1}{2} - \frac{N(f)}{|H(f)|^2}, & f \in F \\ 0, & f \notin F \end{cases} \quad (4.162)$$

完毕

上述高斯模拟信道的容量费用函数具有一个很有意思的特性,即只要  $|H(f)|^2$  的衰减比  $N(f)$  快,则在信号功率有限的情况下,一旦按照式(4.161)把功率分配完,则信道的容量费用函数就与  $F$  以外频率上的  $N(f)/|H(f)|^2$  无关。

## 4.8 限带加性白色高斯噪声信道的极限性能 及其与传输要求的匹配

在上节中我们已经强调指出模拟信道的重要实用意义,而在模拟信道中又重点对限带加性白色高斯噪声信道的信道容量费用函数作了分析和计算。这种信道不但在理论上便于分析,信道容量费用函数具有最简洁的数学形式,而且更重要的是在理论上和实用上都有重要的意义和价值。在理论上高斯噪声是对信息传输最有害而在信道中又最普遍存在,而且无法彻底消除的噪声,由此分析白色高斯噪声信道是对其他各种信道分析的基础。在实用上,很多实用的通信方式,如卫星通信和电缆通信等都可以相当理想地用加性白色高斯噪声信道作为这种通信的信道模型。因此对这一重要的信道模型的分析能为工程设计提供理论基础和实用的设计方法。考虑到这一信道模型的重要性,我们将在这一节对限带加性白色高斯噪声信道作进一步深入的讨论。

### 4.8.1 限带加性白色高斯噪声信道的性能及其极限

限带加性白色高斯噪声信道的信道容量费用函数如式(4.137)所示,若其中的对数以 2 为底,则信道容量的单位为 bit/s(比特/秒),即

$$C(P_s) = W \log_2 \left( 1 + \frac{P_s}{N_0 W} \right) \quad \text{bit/s} \quad (4.163)$$

下面我们分三个方面对这一重要关系式作一分析,并得到这一信道的各种性能极限。

#### 4.8.1.1 增大信道容量的各种极限

(1) 在增加信道通带的宽度  $W$  而不改变信号的平均功率  $P_s$  的情况下增大信道容量的极限。

这种方法对空间通信有着现实意义,那里功率受到能源的限制而频谱资源则相对富裕,但这一办法所得到的增长是有限的,因为按式(4.163)我们有

$$\begin{aligned} \lim_{W \rightarrow \infty} C(P_s) &= \lim_{W \rightarrow \infty} \frac{P_s}{N_0} \log_2 \left( 1 + \frac{P_s}{N_0 W} \right)^{\frac{N_0 W}{P_s}} \\ &= \frac{P_s}{N_0} \log_2 e \approx 1.44 \frac{P_s}{N_0} \end{aligned} \quad (4.164)$$

$C(P_s)$  随  $W$  变化的曲线如图 4.11 所示,其中曲线的下方是实际可实现区,而曲线上方是不可实现区。

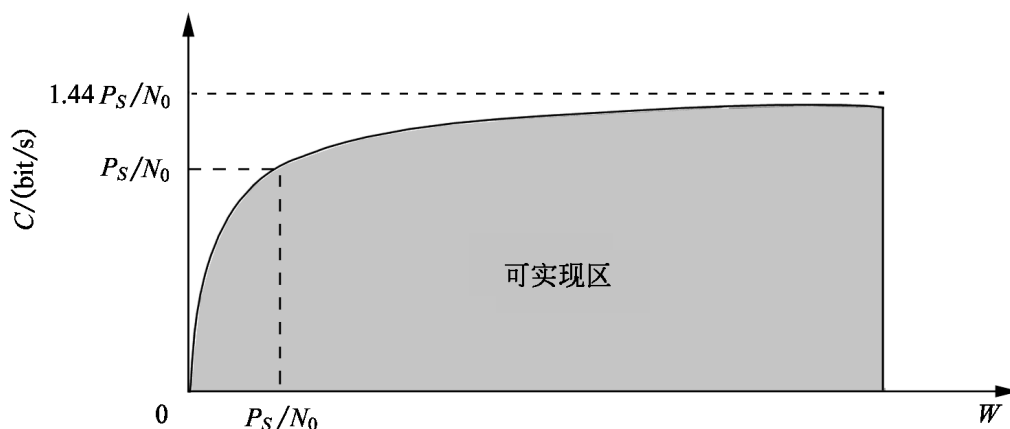


图 4.11 信道容量与带宽的关系图

(2) 在增加信号的平均功率  $P_s$  而不改变信道通带的宽度  $W$  的情况下增大信道容量的极限。

从理论上讲,这一增长没有限制,因为当  $P_s \gg N_0 W$  时,我们有

$$C(P_s) \approx W \ln \frac{P_s}{N_0 W} \quad \text{奈特/秒} \quad (4.165)$$

因为

$$\lim_{P_s \rightarrow \infty} \frac{dC(P_s)}{dP_s} = \lim_{P_s \rightarrow \infty} \frac{1}{N_0 + \frac{P_s}{W}} = 0 \quad (4.166)$$

故随着  $P_s$  的增长,  $C(P_s)$  的增长速度不断减小,直至趋于零。

$C(P_s)$  随  $P_s$  的变化曲线如图 4.12 所示,其中曲线下方为实际可实现区。

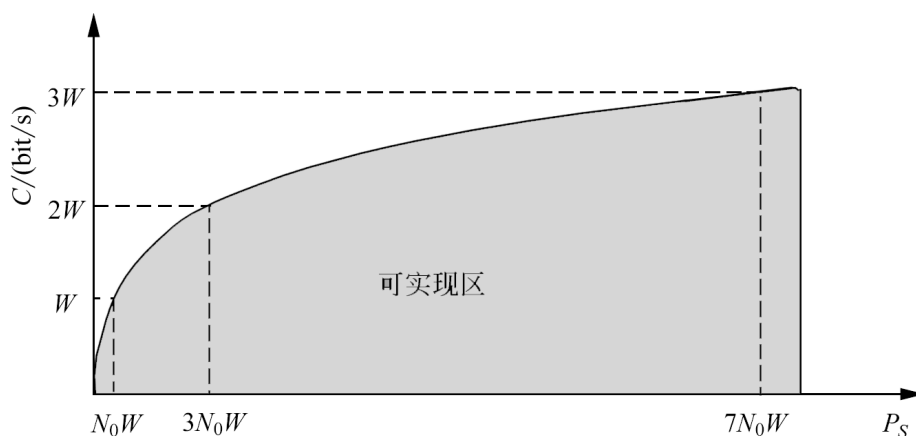


图 4.12 信道容量与信号功率的关系图

#### 4.8.1.2 有效利用信号功率的极限

如何有效地利用功率使同样功率下传输的信息量最大是人们感兴趣的一个问题。为此,我们可以取同样噪声强度下传送 1 bit 信息所需的最小能量为参数,并设为  $E_b$ ,于是,若要使信道的传输速率达到信道容量  $C$ ,则至少需要的平均功率为

$$P_s = E_b C$$

或

$$E_b = \frac{P_s}{C} \quad (4.167)$$

故

$$\frac{E_b}{N_0} = \frac{P_s}{N_0 C} = \frac{P_s}{N_0 W \log_2 \left( 1 + \frac{P_s}{N_0 W} \right)} \quad (4.168)$$

其中,  $P_s / N_0 W$  即为信号的信噪比,如记作  $\gamma$ ,则有

$$\frac{E_b}{N_0} = \frac{1}{\log_2(1 + \gamma)} \quad (4.169)$$

$E_b/N_0$  与  $\gamma$  的关系如图 4.13 所示。 $E_b/N_0$  的最小值发生在  $\gamma$  趋于零的时候, 此时

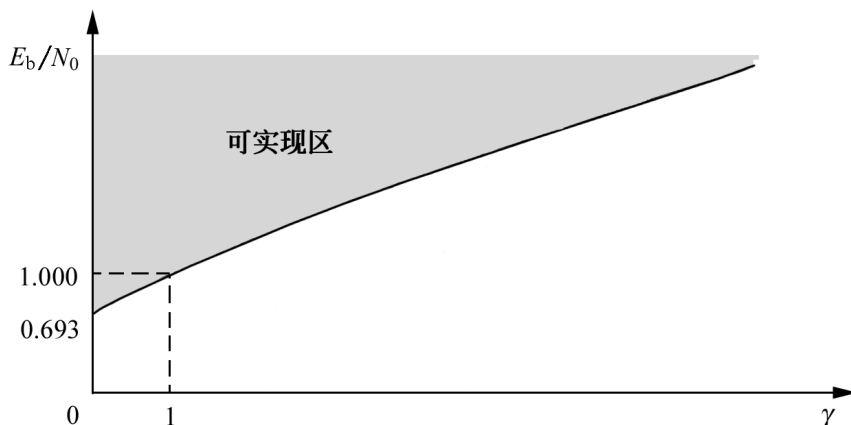


图 4.13  $E_b/N_0$  与信噪比的关系图

$$\begin{aligned} \min \frac{E_b}{N_0} &= \lim_{\gamma \rightarrow 0} \frac{1}{\log_2(1 + \gamma)} = \frac{1}{\log_2 e} \lim_{\gamma \rightarrow 0} \frac{1}{\ln(1 + \gamma)} \\ &= \frac{1}{\log_2 e} = 0.693 = -1.6 \text{ dB} \end{aligned} \quad (4.170)$$

实际上,  $E_b/N_0$  的最小值是在带宽趋于无限时达到的, 这一最小值称为香农限, 它表明传送 1 bit 信息所需的能量至少为  $0.693 N_0$ 。

物理学告诉我们热噪声是无处不在的。热噪声的功率谱密度  $N_0$  与温度有如下关系:

$$N_0 = kT \quad (4.171)$$

其中,  $k$  是玻耳兹曼常数,  $k = 1.38 \times 10^{-23}$  焦耳/开尔文,  $T$  是绝对温度, 所以, 从最根本的物理限制来讲, 传送 1 bit 信息所需的最小能量为

$$E_{b_{\min}} = 0.693 kT \quad (4.172)$$

### 4.8.1.3 功率受限下有效利用信道带宽的极限

对陆地通信来讲, 信号功率和频率资源都是有限的, 因此, 在一定的功率限制下有效利用信道带宽有很大的实际意义。为此我们可取单位带宽所传输的最大信息速率(即  $C/W$ )作为参数, 分析其与功率的关系。按照式(4.163)我们有

$$\frac{C}{W} = \log_2 \left( 1 + \frac{P_s}{N_0 W} \right) = \log_2 \left( 1 + \frac{E_b C}{N_0 W} \right) \quad (4.173)$$

或

$$\frac{E_b}{N_0} = 2^{\frac{C}{W}} - 1 \quad / \quad C W \quad (4.174)$$

$E_b/N_0$  与  $CW$  的关系如图 4.14 所示, 其中的一曲线全面衡量了信息传输中功率利用的有效性与带宽利用的有效性, 所以可以衡量各种调制、编码方式在理论上的优劣程度。对理想的通信系统, 其  $E_b/N_0$  与  $CW$  点应尽量靠近曲线。图 4.14 中同时画出了目前数字通信中常用的多电平正交调幅(MQAM)和多电平相移键控(MPSK)在理想情况下所达到的功率和带宽的利用率。

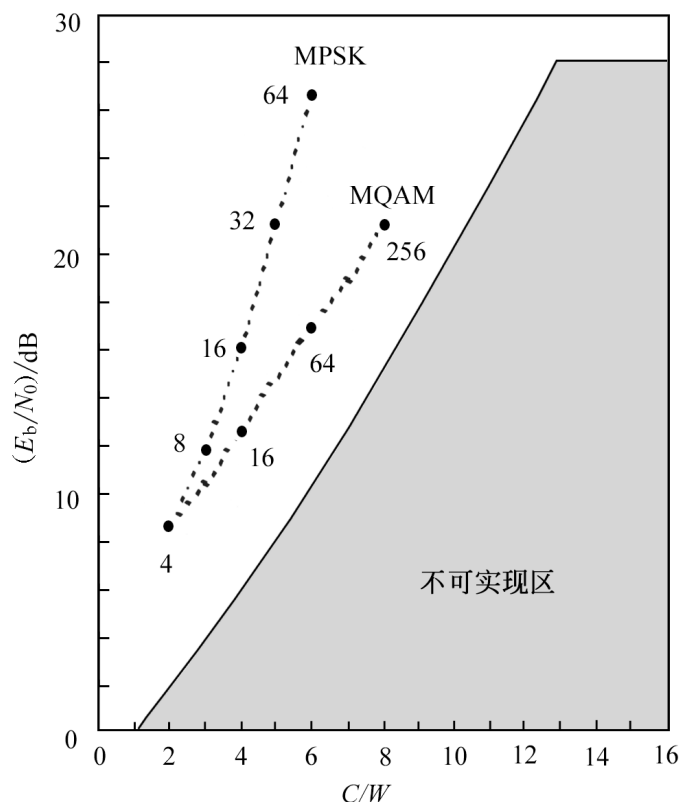


图 4.14 同时表示功率和带宽利用有效性的曲线

## 4.8.2 信道与信息传输要求的匹配

迄今为止, 我们对信道的讨论都是以信道为中心的, 即根据给定信道的特性, 为充分利用信道的信道容量而对输入信号提出一定的要求。但信道输入来源于信源的输出, 而信源往往有自己的特点以及对信息传输的要求, 即给定信源后, 要选择与之相匹配的信道, 使信道能充分传输信源所发出的信息。一般来讲, 这两方面不可能天然吻合, 为了解决这一矛盾, 信源的输出往往需要经过一

定的预处理后才能送入信道。在信道的输出端,输出信号又需要经过相应的后处理才能送至信息的最终接受者——信宿,如图4.15所示。

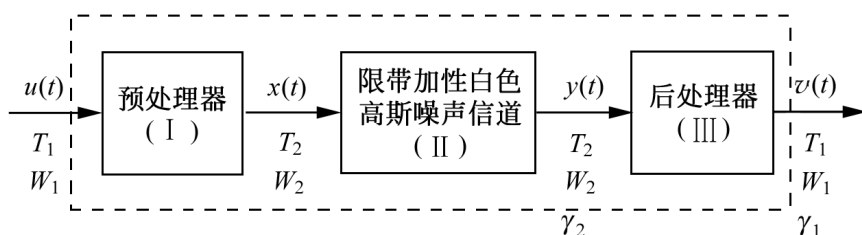


图 4.15 信源与信道的匹配

在理想情况下,应满足关系式

$$I(U(t); V(t)) = I(X(t); Y(t)) \quad (4.175)$$

若存在这样的理想处理器,则在理想情况下应有

$$W_1 T_1 \log(1 + \gamma_1) = W_2 T_2 \log(1 + \gamma_2) \quad (4.176)$$

根据这一基本关系式我们可以得到信道与信息传输要求的几种匹配方式,以及在理想情况下这些参数之间的关系。

#### 4.8.2.1 在相同频带下以时间换取信噪比

设信源信号的频带与信道的通带相同,即  $W_1 = W_2$ ,在平均功率受限的情况下,我们希望传输后的信号仍有很高的信噪比。根据式(4.176),有

$$T_1 \log(1 + \gamma_1) = T_2 \log(1 + \gamma_2)$$

即

$$\gamma_1 = (1 + \gamma_2)^{\frac{T_2}{T_1}} - 1 \quad (4.177)$$

这说明,只要  $T_2 > T_1$ ,就可以获得比  $\gamma_2$  更高的信噪比,也就是说,通过延长信道( )的传输时间(例如采用重复接收技术)可以提高信噪比。这一原理在很多弱信号接收技术中得到了应用,并被称为“时间积累法”。例如雷达信号的接收、从空间发回的图像信号的接收以及射电天文学中星体发射信号的接收等。

#### 4.8.2.2 在相同信噪比下以频带换取时间

若利用发送信号的功率来保证信号传输后的信噪比,即保证  $\gamma_1 = \gamma_2$ ,但我们希望能以比原始信号更短的时间内传送完毕信号。根据式(4.176),有

$$W_1 T_1 = W_2 T_2$$

或 
$$T_2 = \frac{W_1}{W_2} T_1 \quad (4.178)$$

这说明,利用频带的扩展可以使传输时间得以缩短。这一原理在通信电子对抗中有实际的应用,由于使信号传输时间缩短就有可能减少信号被侦察发现的可能性,例如潜艇通信。

### 4.8.2.3 在相同的持续时间下以带宽换取信噪比

在实时通信中,不允许使用我们在前面所述的用时间换取信噪比的方法,这时可以利用信号频带的扩展来换取信噪比。根据式(4.176),有

$$W_1 \log(1 + \gamma_1) = W_2 \log(1 + \gamma_2)$$

即

$$\gamma_1 = (1 + \gamma_2)^{\frac{W_2}{W_1}} - 1 \quad (4.179)$$

其中  $W_2/W_1$  称为扩频因子或扩频系数。当  $\gamma_2 \gg 1$  时,式(4.179)可以近似表示为

$$\gamma_1 \approx \gamma_2 \frac{W_2}{W_1} \quad (4.180)$$

这说明  $\gamma_2$  每增加 1 dB,扩频可给  $\gamma_1$  带来  $W_2/W_1$  dB 的增益,这一增益被称为扩频增益。

考虑到随着频谱的扩展,噪声的功率也在增加,则用  $P_s/N_0 W_1$  为标准,有

$$\gamma_2 = \frac{P_s}{N_0 W_2} = \frac{P_s}{N_0 W_1} \frac{W_1}{W_2}$$

代入式(4.179)中,有

$$\gamma_1 = 1 + \frac{P_s}{N_0 W_1} \frac{W_2}{W_1}^{\frac{W_2}{W_1}} - 1 \quad (4.181)$$

当  $W_2/W_1 \rightarrow \infty$  时,上式的极限为

$$\lim_{W_2/W_1 \rightarrow \infty} \gamma_1 = e^{\frac{P_s}{N_0 W_1}} - 1 \quad (4.182)$$

目前,在实际通信中所使用的各种调制方式中扩频方法所带来的增益都还远远小于式(4.182)所给出的极限。例如,在调幅中,即使用抑制载波调幅和相干解调,其扩频增益的关系为

$$\gamma_1 = 2 \gamma_2 = 2 \frac{W_2}{W_1} \quad (4.183)$$

在调频中,其扩频增益的关系式近似为

$$G_1 = G_2 \frac{3}{8} \frac{W_2}{W_1}^3 \quad (4.184)$$

显然,这两者都与理论极限尚有较大的差距。

## 4.9 限带模拟信道的数字化

模拟信道既可以用来传送模拟信号,又可以用来传送数字信号。模拟信道传送数字信号的理论基础是采样定理。根据这一定理,任何限带信号都可以用时间离散的采样值来表示,于是限带信道的输入和输出都可以等效为时间离散的连续信号。再进一步,如果我们选择一组离散的实数作为信道的输入,而在信道的输出端增加一个判决电路,将信道的输出信号判决后的离散数值输出,限带的模拟信道就可以完全作为一个数字信道来使用。

当限带信道中的噪声是加性白色高斯噪声时,经上述采样、量化、传输、判决组成的信道就可以看成是一个离散无记忆信道。当噪声是加性非白色高斯分布时,信道将是一个有记忆的离散信道。

不难理解,当信道输入被限制在有限个离散值以后,信道输入的幅度分布将不再满足充分利用信道所要求的输入幅度分布。此外,信道输出的量化也会带来信息的损失。所以,这二者均会使信道传输信息的速率低于信道容量所达到的值。

我们现在来看一下输入信号取值所受的限制会给信息的传输带来什么影响。设信道为限带低通加性白色高斯噪声信道,信道通带宽为  $W$ , 噪声的单边功率谱密为  $N_0$ , 信道输入为等间隔的实数值  $a_k$  ( $k = 1, 2, \dots, K$ ), 且各取值等概分布。在此条件下信道可以看成是输入离散、输出连续的无记忆信道, 其信息传输速率不难计算如下。

当输入信号取值为  $a_k$  时, 输出  $y$  的条件概率为

$$q(y / a_k) = \frac{1}{\sqrt{2\pi P_n}} \exp - \frac{(y - a_k)^2}{2 P_n} \quad (4.185)$$

其中  $P_n$  是噪声的功率, 为

$$P_n = N_0 W \quad (4.186)$$

于是, 根据无记忆信道的特点, 输入/输出的平均互信息为



$$I(X; Y) = \sum_{k=1}^K \frac{1}{K} - \frac{1}{2 P_n} \exp - \frac{(y - a_k)^2}{2 P_n} \log \frac{\exp - \frac{(y - a_k)^2}{2 P_n}}{\sum_{l=1}^K \frac{1}{K} \exp - \frac{(y - a_l)^2}{2 P_n}} dy \quad (4.187)$$

将  $y$  和  $a_k$  按噪声进行归一化, 即取

$$y = \frac{y}{P_n}, \quad a_k = \frac{a_k}{P_n} \quad (4.188)$$

将其代入式(4.187)中, 得

$$I(X; Y) = \sum_{k=1}^K \frac{1}{K} - \frac{1}{2} \exp - \frac{(y - a_k)^2}{2} \log \frac{\exp - \frac{(y - a_k)^2}{2}}{\sum_{l=1}^K \frac{1}{K} \exp - \frac{(y - a_l)^2}{2}} dy$$

令  $z = y - a_k$ , 则得

$$I(X; Y) = \log K - \sum_{k=1}^K \frac{1}{K} - \frac{1}{2} e^{-\frac{z^2}{2}} \log \sum_{l=1}^K \exp - \frac{(a_k - a_l)^2}{2} - z(a_k - a_l) dz \quad (4.189)$$

又设输入受平均功率的限制, 即

$$\sum_{k=1}^K \frac{1}{K} a_k^2 = P_s \quad (4.190)$$

由此可知,  $a_k$  应取离零点对称分布的位置以使直流分量为零。在这样的取值下对式(4.189)进行数值积分, 即可得  $I(X; Y)$  的数值曲线如图 4.16 所示。图中的曲线在不同  $K$  值下当  $P_s/P_n$  增大到一定程度后都趋于  $\log K$ , 这是因为噪声的影响在此时趋于零, 每采样值传递的信息量自然就接近于  $\log K$  bit。

图 4.16 给了我们两点重要的结论:

(1) 在高信噪比时, 为了充分利用信道容量必须采用多电平信号。这一结论说明了数字通信早期采用的两电平编码通信为什么后来无法得到发展, 同时也说明了为什么近代数字微波接力通信和数字卫星通信等都采用多电平调制。

(2) 在极低信噪比时采用两电平的数字通信方式就能相当有效地利用信道容量。这一结论可以说明在深空通信中为什么两电平的数字通信得到成功的应用。

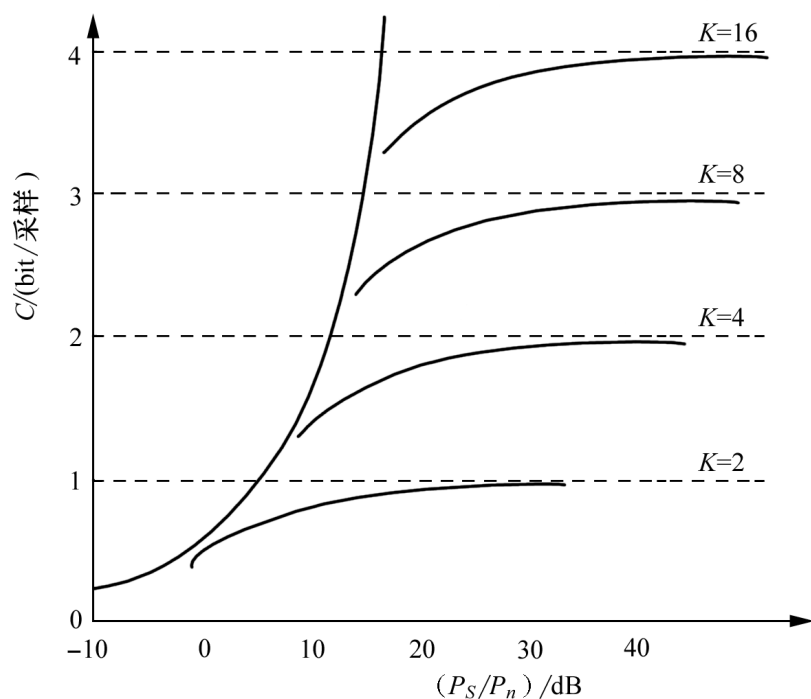


图 4.16 限带信道容量与数字化后的信息传输速率(示意图)

## \* 4.10 蜂窝移动通信条件下信道的有效利用

迄今为止,我们对信道的讨论都假定信道的噪声完全独立于信源,这种噪声最典型的代表就是电路中的热噪声。但在实际通信中,噪声还来源于自然界的各种电磁辐射以及各种电磁装置中的电磁泄漏。这种情况在现代蜂窝移动通信中表现得最为突出,在那里噪声主要来自系统中其他用户发射的信号。如何用信息论的方法来分析这种情况下系统的容量是这一节中我们要讨论的问题。

### 4.10.1 蜂窝移动通信与系统的频谱利用效率

蜂窝移动通信是 20 世纪 40 年代提出的,在 20 世纪 80 年代得到发展的移动通信系统,其核心概念是将地面分成蜂窝状的小区,小区形状的典型代表是六角形,如图 4.17 所示。 $N$  个小区组成一个小区群,小区群内各小区使用的频段互不相同,共同分享系统所用的频段;而各小区群使用的系统频段是相同的,此即频率资源在地域上的复用;小区的大小并不固定,当用户数增加时小区可以分裂。由于每个小区占用的频段在一定的小区群结构下是固定的,因此随着小区的分裂,小区的面积减小,从而使单位面积内可用的频段增加,用户数也就随之

增加。这样就解决了有限的频谱资源与不断增长的用户数的矛盾。

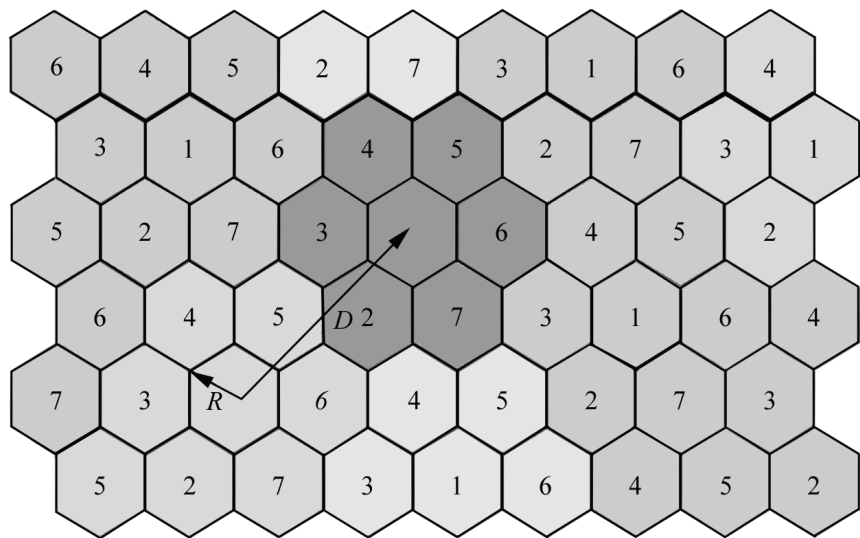


图 4.17 蜂窝移动通信中的小区、小区群与频率复用图形

在蜂窝通信系统中,各小区中心安装有基台,基台天线可以是无方向性的,也可以是有方向性的。若基台天线有方向性时,则天线将小区分成若干扇区。用户是移动的,各移动台与其所在小区或扇区的基台之间进行无线通信,各基台利用有线通信设备与移动交换中心相连,移动交换中心又与陆地固定通信网的交换中心相联。因此,用户的信号一旦进入基台,实际上就可与原有的陆地固定通信网相联。一切交换,无论是移动台用户与移动台用户,或移动台用户与固定通信网用户之间的交换,都是由移动交换中心与固定网交换设备共同协调完成的。

设小区的半径为  $R$ ,相隔  $D$  距离后是使用相同频段的小区,如图 4.17 所示。这样,在每个小区周围使用相同频段小区的信号都会对本小区的通信带来干扰,从而限制了信息传输的速率。由于移动通信中移动台的体积受到限制,所以系统中受干扰影响最大的是由移动台到基台的信号,即上行信号。

设某小区中有一移动台正处在本小区的边缘,即该移动台与基台的距离为  $R$ ,而邻近的某一同频小区的移动台又处在与本小区最近的距离,为  $D - R$ 。按照城市电波传播的规律,接收信号的强度与距离的 次方成反比,其中 的值在  $3 \sim 4$  之间,所以这两个移动台信号强度在本小区基台接收处的比例为

$$= \frac{D - R}{R} \tag{4.191}$$

显然,为了减小干扰的影响,  $D/R$  应尽量大。另一方面,  $D/R$  的取值与小区群的小区数  $M$  有关,即

$$M = \frac{1}{3} \left( \frac{D}{R} \right)^2 \quad (4.192)$$

因此要使信噪比增大,就必须增大  $M$ ,这样做又会减少每个小区可用的频段大小。

前面的分析表明,信道的信息传输能力与信道通带大小和信噪比相关,因此,对蜂窝移动通信系统的信息传输能力的一种衡量是按每小区、每单位频带的信息传输量,此即所谓的单位小区频谱利用效率。设小区的信息传输总速率为  $R_c$ ,系统占用的总带宽为  $W$ ,则定义单位小区频谱利用效率  $\eta_c$  为

$$\eta_c = \frac{R_c}{W} \quad (4.193)$$

## 4.10.2 不同接入方法下蜂窝移动通信系统的频谱利用效率及其比较

在点对点通信中,当很多用户共用一个信道时,可以采用频分复用、时分复用、码分复用等方法。从原理上讲,这几种复用方法均可以充分利用信道。在移动通信中,不同用户在地理上所处的位置不同,其共用信道的方法称为小区多址接入。常用的多址接入方法有频分多址接入、时分多址接入和码分多址接入三种。

在蜂窝移动通信系统中,不同的接入方法则会导致不同的频谱利用效率。下面将讨论频分多址接入和码分多址接入的频谱利用效率。

### 4.10.2.1 频分多址接入系统

由前面的讨论可知,信息传输所需功率与噪声功率之间的关系如式(4.174)所示,即

$$\frac{E_b}{N_0} = \frac{W}{C} 2^{\frac{C}{W}} - 1$$

对蜂窝移动通信系统而言,噪声主要来源于相邻的同频小区的信号,而不是电路的热噪声。作为近似,假设相邻的同频小区来的信号具有白噪声形式,则由式(4.191)可以得到频分多址接入系统基台处的信噪比为

$$= \frac{m}{6} \frac{D - R}{R} \quad (4.194)$$

将式(4.192)代入上式,即得

$$= \frac{m}{6} ((3M)^{V^2} - 1) \quad (4.195)$$

其中,6 是根据图 4.17 得到的。图中每一小区周围有六个同频小区,从而使信噪比降低六倍;而更远的同频小区来的信号很弱,可以忽略不计。 $m$  是由于天线方向性导致的扇区数,它使能接收到的同频段小区来的信号减少,从而增大信噪比。

在频分多址接入下,设每个用户占用的带宽为  $W_1$ ,信息传输速率为  $R$ ,则由式(4.195)可得

$$= \frac{E_b R_1}{N_0 W_1} = \frac{m}{6} ((3M)^{V^2} - 1) \quad (4.196)$$

其中  $N_0$  是等效的白色高斯噪声的单边功率谱密度。

又因小区的信息传输总速率  $R_c$  为

$$R_c = \frac{W_c}{W_1} R_1 \quad (4.197)$$

所以式(4.196)可写为

$$= \frac{E_b}{N_0} \frac{R_c}{W_c} = \frac{m}{6} ((3M)^{V^2} - 1) \quad (4.198)$$

将式(4.174) (此时式中的  $W$  为  $W_c$ ,  $C$  为  $R_c$ )代入上式,得

$$\frac{W_c}{R_c} (2^{R_c/W_c} - 1) = \frac{W_c}{R_c} \frac{m}{6} ((3M)^{V^2} - 1) \quad (4.199)$$

于是得

$$M = \frac{1}{3} \left[ \frac{6}{m} (2^{R_c/W_c} - 1)^{1/V^2} + 1 \right]^2 \quad (4.200)$$

故频分多址接入下的小区频谱利用效率为

$$\eta_c = \frac{R_c}{M W_c} = \frac{3 R_c}{W_c} \left[ \frac{6}{m} (2^{R_c/W_c} - 1)^{1/V^2} + 1 \right]^{-2} \quad (4.201)$$

## 4.10 2.2 码分多址接入系统

在码分多址接入系统下,不同的用户是靠地址码的不同来区分的,每个用户可以占用小区可用的频带;不同的小区也可用不同的码来区分。因此,从频带来看,这时的一个小区群就由一个小区组成。根据码分多址通信的理论,不同码的信号在接收处形成类似高斯白色噪声的干扰。

设一个小区中共有  $J+1$  个用户,基台收到的第 0 号用户的信号功率为

$P_{s_0}$ , 其他用户的信号均视为噪声, 其总功率为

$$P_n = \sum_{j=1}^J P_{s_j} \quad (4.202)$$

则在只考虑单个小区的情况下基台处的信噪比为

$$= \frac{P_{s_0}}{\sum_{j=1}^J P_{s_j}} \quad (4.203)$$

在实际通信系统中都使用功率控制的办法, 使接收处的功率近似相等, 即

$$P_{s_0} = P_{s_1} = \dots = P_{s_J} = P \quad (4.204)$$

此时式(4.203)化简为

$$= \frac{1}{J} \quad (4.205)$$

若考虑相邻小区来的干扰, 该信噪比将降低  $\mu$  倍, 其中根据理论分析和实验模拟, 当  $J=3$  时,  $\mu=2.2$ , 当  $J=4$  时,  $\mu=1.73$ 。则此时基台处的信噪比修正为

$$= \frac{1}{\mu J} \quad (4.206)$$

对于天线有方向性的情况, 信噪比将提高  $m$  倍。因此, 一般情况下码分多址接入系统的信噪比应为

$$= \frac{m}{\mu J} \quad (4.207)$$

或

$$\frac{E_b}{N_0} = \frac{W}{R_1} \frac{m}{\mu J} \quad (4.208)$$

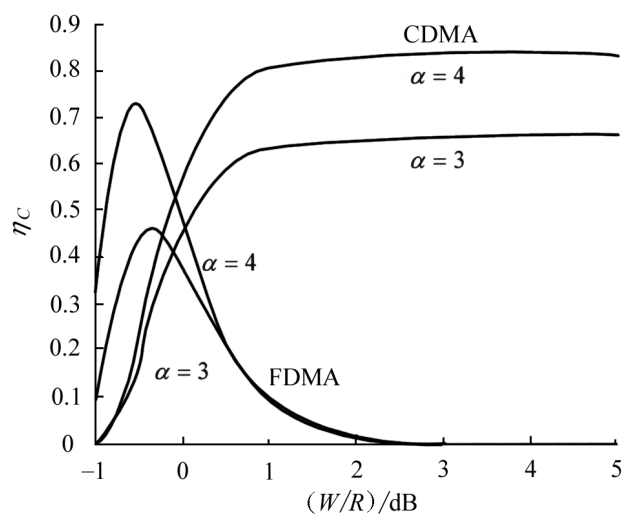
其中,  $N_0$  是最终的等效白色高斯噪声单边功率谱密度, 而  $E_b/N_0$  又满足式(4.174) (此时式中  $C=R$ ), 故有

$$J = \frac{m}{\mu(2^{R/W} - 1)} \quad (4.209)$$

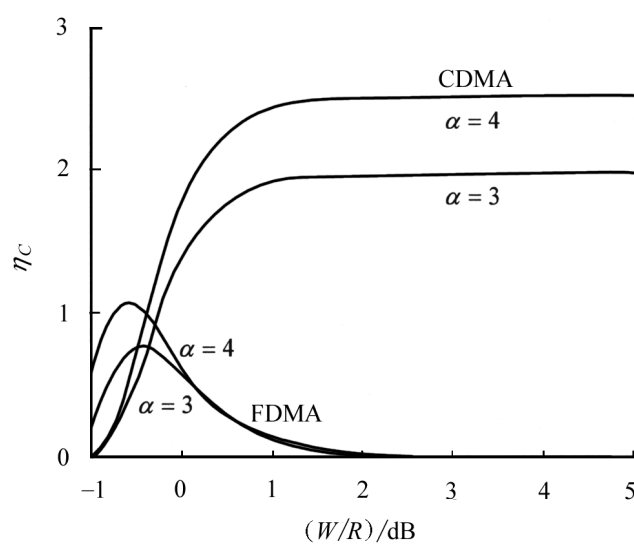
因此, 码分多址接入方式的小区频谱利用效率为

$$\eta_c = \frac{R_1(J+1)}{W} = \frac{m \frac{R_1}{W}}{\mu(2^{R/W} - 1)} = \frac{m}{\mu \ln 2} \quad (4.210)$$

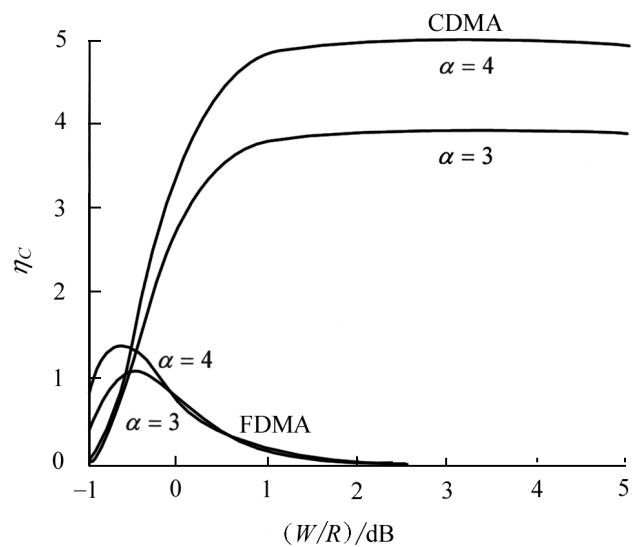
图4.18给出了不同扇区数下频分多址接入与码分多址接入两种情况的频



(a) 全向天线时



(b) 小区分成 3 个扇区时



(c) 小区分成 6 个扇区时

图 4.18 蜂窝移动通信系统的频谱利用效率

谱利用效率曲线。曲线的横坐标为单个用户所占的频带与其速率之比  $W/R$ , 该值在频分多址下为  $W_c/R_c$ , 在码分多址下为  $W/R_t$ 。图中, (a) 对应于全向天线, 即不分扇区的情况; (b) 对应于使用  $120^\circ$  方向天线, 将小区分成 3 个扇区的情况; (c) 对应于分成 6 个扇区的情况。

从图 4.18 可以看出, 使用全向天线时两种多址接入方式的最大频谱利用效率大致相等。但在扇区数增加时, 码分多址接入的最大频谱利用效率随扇区数线性增长, 而频分多址接入的频谱利用效率却增长极微。因此, 可以粗略地认为, 码分多址接入的频谱利用效率与频分多址接入的频谱利用效率之比大致等于扇区数。

需要说明的是, 上述分析没有应用多用户信息理论, 所作的假设也是非常理想化的, 很多实际问题如电波传播中的多径衰落、天线的旁瓣辐射、接收信号的远近效应等等都未考虑。但是, 上述基本结论的正确性已得到工程实践的验证。

## 习 题

4.1 设有离散无记忆信道, 输入  $X$ :  $\begin{matrix} a_1 & a_2 & \dots & a_K \\ p(a_1) & p(a_2) & \dots & p(a_K) \end{matrix}$ , 输出

$Y$ :  $\begin{matrix} b_1 & b_2 & \dots & b_J \\ p(b_1) & p(b_2) & \dots & p(b_J) \end{matrix}$ , 输入/输出  $x$  和  $y$  的互信息  $I(x; y)$  也为一随机变量。试证: 当  $\text{Var}\{I(x; y)\} = 0$  时, 平均互信息  $I(X; Y)$  达到信道容量  $C$ 。

4.2 设某信道的输入  $X$  取值  $\{+1, -1\}$ , 又信道有加性噪声  $n$ , 其分布密度为  $p(n) = \begin{cases} \frac{1}{4}, & |n| \leq 2 \\ 0, & |n| > 2 \end{cases}$ , 求信道容量。

4.3 设在图 4.10 的一般高斯信道中  $N(f) = \frac{N_0}{2}$ ,  $H(f) = \frac{1}{1 + (f/f_0)^2}$ , 试求信道的容量费用函数  $C(P_s)$ 。

4.4 设  $X$  和  $Y$  为信道的输入和输出, 两者均取值于集合  $A = \{a_1, a_2, \dots, a_K\}$ 。已知  $p(x = a_k) = p_k$ ,  $p(y = a_j | x = a_k) = p_{kj}$ , 定义  $P_e = \sum_k p_k \sum_j p_{kj}$ , 求证:

$$H(X|Y) = P_e \log(K-1) + H(P_e)$$

其中  $H(P_e) = -P_e \log P_e - (1 - P_e) \log(1 - P_e)$ 。



4.5 已知信道转移概率矩阵如下, 求此信道的信道容量。

$x \backslash y$	0	1	2	3
0	1/3	1/3	1/6	1/6
1	1/6	1/3	1/6	1/3

4.6 设有信道, 输入  $X$  的字母表为  $\{0, 1, 2, \dots, K-1\}$ , 噪声为独立加性噪声  $Z$ ,  $Z$  的取值也在  $\{0, 1, 2, \dots, K-1\}$  集合中, 但两者相加为模  $K$  相加, 即输出  $Y = X + Z \pmod{K}$ , 试求此信道的信道容量。

4.7 设有二元对称信道  $Y_n = X_n + Z_n$ , 其中  $+$  为模 2 和,  $X_n, Y_n \in \{0, 1\}$ ,  $Z_n: \begin{matrix} 0 & 1 \\ 1-p & p \end{matrix}$ , 但  $Z_n$  不是独立随机序列, 试证:

$$\max I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N) = NC$$

其中  $C = 1 - H(P)$ 。

4.8 设有输入为  $X$ , 输出为  $\mathbf{Y} = (Y_1, Y_2)$  的高斯信道, 其中  $Y_1 = X + Z_1$ ,  $Y_2 = X + Z_2$ ,  $X$  的最大功率受限  $P$ ,  $(Z_1, Z_2) \sim N_2(0, K)$ , 其中  $K = \begin{pmatrix} \sigma_1^2 & \sigma_{12} \\ \sigma_{21} & \sigma_2^2 \end{pmatrix}$ 。

(1) 证明:  $I(X; Y_1 Y_2) = I(X; Y_1) + I(X; Y_2) - I(Y_1; Y_2) + I(Y_1; Y_2 | X)$

(2) 求  $\sigma_{12} = 1$  时的信道容量。

## 第5章 信道编码

在第4章中我们利用互信息的概念得到了信道容量,它表示通过信道可以传输的最大信息量。但是仅用互信息尚不能对信息传输的情况给出全面的描述。实际上在通信中人们不但要求传输的信息量大,而且还要求得到的信息是可靠的,即可以可靠地知道信道的输入是什么。互信息的值可以说明所得信息量的大小,却不能说明所得的信息能否可靠地确定信道的输入。这一点从互信息的定义中可以清楚地看出来。互信息的值仅与信道输入的不确定度在得知信道输入前和得知信道输入后所取值之差有关。即使互信息的值很大,信宿仍有可能无法可靠地确定信道的输入。这一问题在通信工程中称为通信可靠性。

我们知道在有噪声的离散信道中信道输入字母与相应输出字母之间仅有统计上的关系,仅凭信道的输出字母是不可能唯一地确定信道的输入字母的。在一定要作出唯一选择的情况下将无法避免差错,这时根据信道输出确定信道输入的可靠程度就反映为差错概率。对于有噪声的信道,这一差错概率完全取决于信道的特性,且不可能为零。但是香农的研究表明,如果我们把要传送的消息在传送前先进行编码,并在接收端采用适当的译码,则消息有可能得到无误的传输。也就是说,通过不可靠的信道可以实现可靠的信息传输。这一结论在用定理形式严格地表述以后被称为信道编码定理。

在下面的讨论中,我们将在离散无记忆信道的情况下首先介绍信道编码的基本概念,然后给出信道编码定理的证明,最后对编码的主要方法及码的性能指标作简要的讨论。

### 5.1 信道编码概述

信道编码与第3章中讨论的信源编码一样都是一种编码,但信源编码的作用是压缩冗余度以得到信息的有效表示,或在传输时提高信息的传输效率,而信道编码的作用是提高信息传输时的抗干扰能力以增加信息传输的可靠性。为区分这两种码,我们把信源编码所得的码称为信源码,信道编码所得的码称为信道码。在其他著作中,信道码也被称为数据传输码或差错控制码。信道编码与信

源编码在通信系统中的位置如图 5.1 所示。与图 3.1 比较,这里的信源码编码器与信道码编码器组成了图 3.1 中的发送器,而相应的两个译码器组成图 3.1 中的接收器。通信系统中有了这两种码就可以使信息在信道中得到高效而可靠的传输。当然,这两种码的编码也可以联合起来进行,这就是信源信道联合编码。但两者分别进行在一般情况下便于设计和实现,并有利于构成标准模块,增加系统的适应性。

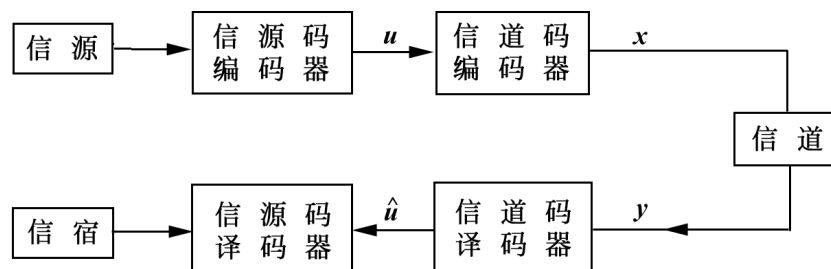


图 5.1 信道编码与通信系统组成模型

信道码的编码方法如 3.1.3 节介绍编码一般概念时所述,可分为两类,即分组码和树码。在分组码中,输入信道码编码器的输入序列  $\dots U_{-1}, U_0, U_1, \dots$  先被分组,例如  $L$  个输入字母一组,然后对每一组输入字母给以相应的码字。码字中的字母取自信道输入容许的字母表  $A_x$ 。如果编码器输入字母组共有  $M$  种可能的组合,我们分别用  $m, m=0, 1, 2, \dots, M-1$  表示,而相应的码字用  $\mathbf{c}_m (m=0, 1, 2, \dots, M-1)$  表示,则信道码编码器所完成的工作就是由  $\{0, 1, 2, \dots, M-1\}$  到  $\{\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{M-1}\}$  的一一映射。这一映射被称为编码函数。

码字通过信道传输后在接收端得到与发送码字长度相同的信道输出字母序列  $\mathbf{y}$ ,  $\mathbf{y}$  也被称为接收信号矢量或简称接收矢量。信道码的译码器就根据此接收矢量对发送的消息进行估计并输出  $\hat{m}$ 。由于信道中存在噪声,有可能  $\hat{m} \neq m$ , 这时译码发生差错。平均的译码差错概率或称误字率是数字信息传输质量的主要指标。

在分组码中,每一码字携带的最大可能信息量为  $\log M$ 。若码字长  $N$ , 码字母表的大小为  $|A_x|$ , 则信道码携带信息的效率可用其码率  $R$  来表示,即

$$R = \log M / N (\text{bit/字母}) \quad (5.1)$$

当  $|A_x| = 2, M = 2^K$  时,

$$R = K / N (\text{bit/字母}) \quad (5.2)$$

表 5.1 和表 5.2 是分组码的两个实例,它们的码率分别是  $1/3$  和  $4/7$ 。从原理上讲,信道码的码率必是小于 1 的数。这是因为发送信号矢量空间中的全

部矢量只能有一小部分可被取作码字,大部分矢量必须被禁用,这样才能为接收端发现和纠正传输中的差错提供可能。这是信道码为获得抗干扰能力所必须付出的代价。

表 5.1 重复码

<i>m</i>		码字	<i>m</i>		码字
十进制	二进制		十进制	二进制	
0	0	000	1	1	111

表 5.2 汉明码

<i>m</i>		码字	<i>m</i>		码字
十进制	二进制		十进制	二进制	
0	0000	0000000	8	1000	1000101
1	0001	0001011	9	1001	1001110
2	0010	0010110	10	1010	1010011
3	0011	0011101	11	1011	1011000
4	0100	0100111	12	1100	1100010
5	0101	0101100	13	1101	1101001
6	0110	0110001	14	1110	1110100
7	0111	0111010	15	1111	1111111

从分组码的编码函数可知,分组码的编码器是无记忆的,编码器的输出码字仅与此时刻编码器的输入有关,而树码的编码器是有记忆的。具体来说,若树码编码器的输入输出字母表都是二元字母表,编码器每次接收  $K$  个字母并输出  $N$  个字母,则在一般情况下,这  $N$  个输出字母不单取决于此时刻输入的  $K$  个输入字母,而且还与以前的  $V$  个输入字母有关。 $V + K$  被称为这一树码的约束长度,而  $K/N$  被称为该树码的码率。

信道码按码的结构的不同可分为线性码与非线性码。线性码的全体码字组成线性矢量空间,这时码中任二码字的和也是码中的码字。这一特点使码具有极其理想的对称性,从而给编码和译码带来很大的方便,也能使码性能的计算得到简化。迄今为止,获得实际应用的信道码绝大多数是线性码。线性的分组码又称群码,因为在数学结构上这一码的全体码字构成数学中的群。线性树码则又称卷积码,因为这种码的编码器相当于一个数字滤波器,编码运算相当于卷

积。从码性能的分析来讲,树码的分析较分组码的分析难,树码的构造理论也不如分组码的构造理论那样系统和成熟,但树码在相同的码率和同样的实现复杂度下一般有较好的性能。

信道码按其抗干扰模式的不同可分为抗随机差错码和抗突发差错码,但后者仅在差错模式比较稳定的信道中应用时才有意义。当突发差错的模式不稳定时将交织技术和抗随机差错码结合起来使用可以收到很好的效果。

信道码按其编译码理论所用数学工具的不同又可分成很多种码,如利用代数方法编码的代数码,用几何方法编码的几何码以及用组合数学方法编码的组合码等。

总的来讲,信道编码在理论上虽然还有一些基本问题没有解决,但已有的理论已相当丰富和系统,在本书中我们除配合信道编码定理的讨论对群码作简单的介绍外,对其他的编码方法将不再讨论。

## 5.2 信道译码准则

信道码与信源码在编码时都是完成一一对应的映射关系,但在译码时两者的情况就完全不同了。对信源码来说,译码是编码的简单逆运算,信源码的唯一可译性保证了译码输出的正确性,但在信道码时,码字经传输后有可能发生差错。实际上在离散无记忆信道下若发送的码字为  $\mathbf{c}_n = (c_{n1}, c_{n2}, \dots, c_{nN})$ , 则接收矢量为  $\mathbf{y} = (y_1, y_2, \dots, y_N)$  的概率是

$$P(\mathbf{Y} = \mathbf{y} / \mathbf{X} = \mathbf{c}_n) = \prod_{n=1}^N p(y_n / c_{nn}) \quad (5.3)$$

这就是说,同一个发送码字在接收端可能得到不同的接收矢量,因此译码函数不能是编码函数简单的逆函数,而是需将整个的接收矢量空间  $\{\mathbf{Y}\}$  划分成  $M$  个互不相交的子集  $\mathbf{Y}_m, m=0, 1, 2, \dots, M-1$ , 然后将子集  $\mathbf{Y}_m$  中的  $\mathbf{y}$  译码成  $m$ 。这一运算可用译码函数  $g(\cdot)$  表示成

$$g(\mathbf{y}) = m, \quad \text{当 } \mathbf{y} \in \mathbf{Y}_m \quad (5.4)$$

若码字  $\mathbf{c}_n$  经传输后在接收端所得的接收矢量不落在  $\mathbf{Y}_m$  子集中,则译码发生差错。在码和信道特性给定的条件下,译码的差错概率将取决于接收矢量空间按什么样的划分准则进行划分。划分接收矢量空间的准则也就是译码器的译码准则,按不同的要求可以有不同的译码准则。从理论上讲,理想的译码器应使平均的译码差错概率最小,这就是最小差错概率准则。在这一准则下,接收矢量空间

是这样划分的: 设  $p(\mathbf{y} | \mathbf{c}_n)$  是发送码字  $\mathbf{c}_n$  条件下接收矢量取  $\mathbf{y}$  的概率, 则按全概率公式可有

$$p(\mathbf{y} | \mathbf{c}_n) p(\mathbf{c}_n) = p(\mathbf{y}, \mathbf{c}_n) = p(\mathbf{c}_n | \mathbf{y}) p(\mathbf{y})$$

$$\text{或} \quad p(\mathbf{c}_n | \mathbf{y}) = \frac{p(\mathbf{y} | \mathbf{c}_n) p(\mathbf{c}_n)}{p(\mathbf{y})} \quad (5.5)$$

$$\text{其中} \quad p(\mathbf{y}) = \sum_{m=0}^{M-1} p(\mathbf{c}_m) p(\mathbf{y} | \mathbf{c}_m) \quad (5.6)$$

式(5.5)给出了接收矢量取  $\mathbf{y}$  的条件下发送码字取  $\mathbf{c}_m$  的概率, 所以在译码时如把这一  $\mathbf{y}$  译作  $m$ , 则译码正确的概率就等于  $p(\mathbf{c}_n | \mathbf{y})$ , 这时译码发生差错的概率是

$$P_{e|\mathbf{y}} = 1 - p(\mathbf{c}_n | \mathbf{y}) \quad (5.7)$$

译码器平均的译码差错概率是

$$\begin{aligned} P_e &= \sum_{\mathbf{y}} p(\mathbf{y}) P_{e|\mathbf{y}} = \sum_{\mathbf{y}} p(\mathbf{y}) (1 - p(\mathbf{c}_n | \mathbf{y})) \\ &= 1 - \sum_{\mathbf{y}} p(\mathbf{y}) p(\mathbf{c}_n | \mathbf{y}) \end{aligned} \quad (5.8)$$

为使平均的译码差错概率取最小, 译码器显然应对所有的  $\mathbf{y}$  都取能使  $p(\mathbf{c}_n | \mathbf{y})$  值最大的那个  $m$  值作为译码器的输出。用译码函数  $g(\cdot)$  表示时, 最小平均译码差错概率的译码准则是

$$p(g(\mathbf{y}) | \mathbf{y}) = \max_m p(\mathbf{c}_m | \mathbf{y}) \quad (5.9)$$

满足这一准则的译码器有时又称理想译码器, 但理想译码器也不是没有缺点的, 式(5.9)中  $p(\mathbf{c}_m | \mathbf{y})$  是信道的反向转移概率, 它依赖于输入的分布  $p(\mathbf{c}_m)$ , 因此当输入分布改变时, 理想译码器也就失去其理想性。为了减少译码性能对输入分布的依赖性, 可以取另一种实用的准则——最大似然译码准则。在这一准则下译码函数  $g(\cdot)$  满足

$$p(\mathbf{y} | g(\mathbf{y})) = \max_m p(\mathbf{y} | \mathbf{c}_m) \quad (5.10)$$

即取能使  $p(\mathbf{y} | \mathbf{c}_m)$  取最大值的那个  $m$  作为译码输出  $g(\mathbf{y})$ 。在这一准则下发送码字  $\mathbf{c}_n$  在收端被误译的概率为

$$P_{e|m} = \sum_{\mathbf{y} \in \mathbf{Y}_m^c} p(\mathbf{y} | \mathbf{c}_n) \quad (5.11)$$

其中  $\mathbf{Y}_m^c$  是  $\mathbf{Y}_m$  的补集。平均的译码差错概率是

$$P_e = \sum_m p(\mathbf{c}_n) P_{e|m} = \sum_m p(m) P_{e|m} \quad (5.12)$$

从式(5.12)可以看到,如果取

$$\max_m P_{e|m} = P_e^{\max} \quad (5.13)$$

则不管输入分布如何都可以保证

$$P_e < P_e^{\max} \quad (5.14)$$

当输入码字取均匀分布时,可以有

$$p(\mathbf{c}_m | \mathbf{y}) = \frac{1}{Mp(\mathbf{y})} p(\mathbf{y} | \mathbf{c}_m) \quad (5.15)$$

由此得

$$\begin{aligned} \max_m p(\mathbf{c}_m | \mathbf{y}) &= \max_m \frac{1}{Mp(\mathbf{y})} p(\mathbf{y} | \mathbf{c}_m) \\ &= \frac{1}{Mp(\mathbf{y})} \max_m p(\mathbf{y} | \mathbf{c}_m) \end{aligned} \quad (5.16)$$

这时取前向转移概率  $p(\mathbf{y} | \mathbf{c}_m)$  最大的  $m$  等价于取反向转移概率  $p(\mathbf{c}_m | \mathbf{y})$  最大的  $m$ , 两种准则等价。

现在来看表 5.1 和表 5.2 所示的两种码用于二元对称信道时其接收矢量空间该如何划分。我们假定输入消息的分布是均匀分布, 因此无论用哪一种准则结果都是一样的。

对于重复码, 这时的接收矢量空间共有 8 个矢量。发送码字经传输后有  $l$  个字母发生差错的概率是  $\binom{l}{l} (1 - \frac{1}{2})^{3-l}$ 。由于  $\frac{1}{2} < 1/2$ , 所以按最大似然准则译码器应将接收矢量译码成与其差别最小的码字, 即  $l=0$  和  $l=1$ , 这样就得

$$\mathbf{Y}_1 = \{(000), (001), (010), (100)\}$$

$$\mathbf{Y}_2 = \{(111), (110), (101), (011)\}$$

这时的误字率为

$$P_{e|1} = P_{e|2} = P_e = \sum_{l=2}^3 \binom{l}{l} (1 - \frac{1}{2})^{3-l} = 3 \cdot 2^{-2} - 2^{-3}$$

当  $\frac{1}{2} < 1/2$  时,  $3 \cdot 2^{-2} - 2^{-3} < \frac{1}{2}$ , 这说明传输的可靠性和不编码时相比提高了。

对于汉明码, 这时的接收矢量空间共有  $2^7 = 128$  个矢量。和上例中的情况一样, 在按最大似然译码准则译码时译码器应将接收矢量译码成与其差别最小的码字。如果把没有发生差错和只有一个字母发生差错的接收矢量放在一起作为一个子集, 则此子集中共有 8 个矢量。汉明码的 8 个码字都可按此方法得到一个以码字矢量为中心的子集。汉明码的特点是每一码字与任一其他码字至少有三处不同, 因此这 8 个子集互不相交。它们合在一起又刚好占满整个接收矢量空间。按照这一方法, 汉明码可以纠正一个差错, 但有两个或两个以上字母发

生差错时都将被译成其他码字,译码的误字率为

$$P_e = \sum_{l=2}^7 C_7^{l-1} (1-p)^{7-l}$$

在上述两例中,重复码的码率是  $1/3$ , 而汉明码的码率是  $4/7$ , 它们的抗干扰能力是一样的,都只能纠一个差错。这样人们自然会问:在保持同样的码率下能否有更好的码使译码的误字率更低呢?在下面两节中我们将证明,只要分组码的码率小于信道的信道容量,则存在误字率可以任意小的分组码。这个和人们直观想象大相径庭的结论是香农首先得到的。同时值得指出的是,香农在证明这一结论时所用的方法也是出人意料的。按照通常的想法想证明这一结论可能先要构造一个理想的好码,然后计算这一码用于传输时的误字率,但这两点都是很难实现的。首先,构造具有理想性能的好码是一个极其复杂的问题,在当时根本无望解决。其次,想在  $N$  值很大时计算这一理想好码在理想译码器或最大似然译码器下的误字率也是极其困难的。香农巧妙地躲开了这两个难题。首先,他不去寻找理想的好码而是用随机编码的方法得到所有可能生成的码的集合,然后在码集合中随机选择一个码作为信道码,最后再计算所造码的性能在集合上平均时所具有的性能。由于所求的是平均的性能,这就可以利用大数定律且不必考虑码的确切结构。其次,在译码时,他利用了联合典型序列的概念,即将接收矢量译码成与其联合典型的码字。这种译码方法不是最优的,但便于进行理论分析,在下一节中我们将详细介绍这一概念。

### 5.3 联合典型序列与联合渐近等同分割定理

关于信源输出随机序列中典型序列的概念是在讨论信源编码定理时首次提出的,正是这一概念为信源编码奠定了基础。联合典型序列的概念是典型序列的概念在涉及两个随机序列时的自然扩展,它是信道编码的基础,其定义如下:

设  $(\mathbf{X}, \mathbf{Y})$  是长  $N$  的随机序列对,  $p(\mathbf{x}, \mathbf{y}) = \prod_{n=1}^N p(x_n, y_n)$ , 则在这些随机序列对中满足下列条件的序列对被称为联合典型序列:

$$(1) \quad \left| \frac{1}{N} \log p(\mathbf{x}) + H(X) \right| < \epsilon \quad (5.17)$$

$$(2) \quad \left| \frac{1}{N} \log p(\mathbf{y}) + H(Y) \right| < \epsilon \quad (5.18)$$



$$(3) \quad \left| \frac{1}{N} \log p(\mathbf{x}\mathbf{y}) + H(XY) \right| < \quad (5.19)$$

式中  $\epsilon$  是任意小的数。联合典型序列的全体构成联合典型序列集, 记作  $G$ 。

按此定义不难得到随机序列对  $(\mathbf{X}, \mathbf{Y})$  取某联合典型序列  $(\mathbf{x}, \mathbf{y})$  的概率  $p(\mathbf{x}, \mathbf{y})$  满足

$$p(\mathbf{x}, \mathbf{y}) \leq 2^{-N[H(XY) + \epsilon]} \quad (5.20)$$

$$p(\mathbf{x}, \mathbf{y}) \geq 2^{-N[H(XY) - \epsilon]} \quad (5.21)$$

或将上两式合并简记为

$$p(\mathbf{x}, \mathbf{y}) \approx 2^{-NH(XY)}$$

按同样的道理, 有

$$p(\mathbf{x}) \approx 2^{-NH(X)}$$

$$p(\mathbf{y}) \approx 2^{-NH(Y)}$$

联合典型序列具有与典型序列类似的性质, 特别是同样具有渐近等同分割性。

**定理 5.1 (联合渐近等同分割定理)** 设随机序列对  $(\mathbf{X}, \mathbf{Y})$  的  $p(\mathbf{x}, \mathbf{y}) = \prod_{n=1}^N p(x_n, y_n)$ , 则对任意小的数  $\epsilon > 0$ , 我们总能找到足够大的  $N$  使全体序列对的集合能被分成满足下述条件的集合  $G$  及其补集  $G^c$ :

$$(1) \quad P\{(\mathbf{X}, \mathbf{Y}) \in G^c\} < \epsilon \quad (5.22)$$

$$P\{(\mathbf{X}, \mathbf{Y}) \in G\} > 1 - \epsilon \quad (5.23)$$

$$(2) \quad |G| \leq 2^{N(H(XY) + \epsilon)} \quad (5.24)$$

$$|G| \leq (1 - \epsilon) 2^{N(H(XY) - \epsilon)} \quad (5.25)$$

(3) 设  $(\mathbf{X}, \mathbf{Y})$  是相互独立的随机序列对, 但它与  $(\mathbf{X}, \mathbf{Y})$  有相同的边缘分布, 即

$$P\{(\mathbf{X}, \mathbf{Y}) = (\mathbf{x}, \mathbf{y})\} = p(\mathbf{x})p(\mathbf{y}) \quad (5.26)$$

$$\text{则} \quad P\{(\mathbf{X}, \mathbf{Y}) \in G\} \leq 2^{-N[I(X; Y) - 3\epsilon]} \quad (5.27)$$

$$P\{(\mathbf{X}, \mathbf{Y}) \in G\} \leq (1 - \epsilon) 2^{-N[I(X; Y) + 3\epsilon]} \quad (5.28)$$

**证明** (1) 把  $(\mathbf{X}, \mathbf{Y})$  看成单个的随机序列, 则按定理 3.2 (渐近等同分割定理) 即可得式 (5.22) 和式 (5.23)。

$$(2) \text{ 由 } 1 = \sum_{(\mathbf{x}, \mathbf{y}) \in G} p(\mathbf{x}, \mathbf{y}) + \sum_{(\mathbf{x}, \mathbf{y}) \in G^c} p(\mathbf{x}, \mathbf{y}) \quad |G| \leq 2^{N(H(XY) + \epsilon)}$$

可得  $|G| \leq 2^{N(H(XY) + \epsilon)}$

$$\text{又由 } 1 - \sum_{(\mathbf{x}, \mathbf{y}) \in G^c} p(\mathbf{x}, \mathbf{y}) = \sum_{(\mathbf{x}, \mathbf{y}) \in G} p(\mathbf{x}, \mathbf{y}) \quad |G| \leq (1 - \epsilon) 2^{N(H(XY) - \epsilon)}$$

可得  $|G| = (1 - \epsilon) 2^{N(H(XY) - \epsilon)}$

(3) 按假设有  $P\{(\mathbf{X}, \mathbf{Y}) \in G\} = \sum_{(\mathbf{x}, \mathbf{y}) \in G} p(\mathbf{x}) p(\mathbf{y})$ , 其中  $p(\mathbf{x}) = 2^{-NH(X)}$ ,  $p(\mathbf{y}) = 2^{-NH(Y)}$

将它们与式(5.24)和式(5.25)一起代入式(5.28)并注意到  $H(X) + H(Y) - H(XY) = I(X; Y)$  即得式(5.27)和式(5.28)。 证毕

在5.2节中我们曾提到在有干扰的信道中传输信息时,与一定的发送码字相对应的接收矢量有可能是接收矢量空间中的任意一个矢量。而上述定理指出虽然有这样的可能,但是随着  $N$  的增加,接收矢量几乎只能是与发送码字联合典型的序列,取其他序列的概率将趋于零。这一结果为在  $N$  很大时信道码的译码提出了一条新的思路,一种新的译码方法,即在译码时取与接收矢量联合典型的码字作为译码器的输出。由于联合典型序列的数目大致是  $2^{NH(XY)}$ ,它们在由  $\mathbf{X}$  的典型序列和  $\mathbf{Y}$  的典型序列随机独立组合产生的  $2^{N(H(X) + H(Y))}$  个序列对中只占很小的一部分,大致是  $1/2^{NI(X; Y)}$ ,因此当发送码字的数目少于  $2^{NI(X; Y)}$  时,这一译码方法可以保证得到很低的误码率。

## 5.4 信道编码定理

1948年,香农在他著名的论文中给出了下述有关信息传输的最基本的定理——信道编码定理:

**定理 5.2** 设  $R$  是信息传输的速率,  $C$  是离散无记忆信道的信道容量,  $\epsilon > 0$  是任意小的数,则只要  $R < C$  就总存在码字长为  $N$ , 码字数为  $M = 2^{NR}$  的分组码使译码的平均差错概率  $P_e < \epsilon$ 。

香农当时给出的这一定理的证明不很严格,但他在证明中所用的随机编码的方法则在后来的严格证明中一直被采用,所以在我们给出这一定理的证明以前有必要先介绍什么是随机编码。

按照分组码的编码方法,编码器要对每一消息  $m$ ,  $m = 0, 1, \dots, M - 1$  给以相应的长为  $N$  的码字  $\mathbf{c}_m = (c_{m1}, c_{m2}, \dots, c_{mN})$ 。所谓随机编码就是按照信道输入字母表的字母概率分布完全随机地从中选取字母作为码字的字母。从  $\mathbf{c}$  的第一个码字母  $c_1$  开始一直取到  $\mathbf{c}_{M-1}$  的最后一个码字母  $c_{M-1, N}$ , 从而得到全部  $M = 2^{NR}$  个码字,组成一个码  $\mathbf{C} = \{\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{M-1}\}$ , 这就是随机编码。随机编码产生某一特定码的概率  $P(\mathbf{C})$  是

$$P(\mathbf{C}) = \prod_{m=0}^{M-1} \prod_{n=1}^N p(c_{mn}) \quad (5.29)$$

所有可能产生的码的总数是  $|A_x|^{N2^{NR}}$ , 例如在  $|A_x| = 2, N = 16, M = 2^8$  这样最小的码字母表和不太长的码字下其总数为  $2^{4096} = 10^{1233}$ , 这是一个很大的数。当然, 在这些码中有一部分是无法用的, 例如码中有若干码字相同的码, 但由于码中码字数为  $2^{NR}$ , 只占全部可能序列数  $2^N$  的很小的一部分, 因此同一码中码字相同的概率很小, 大部分码中的码字各不相同。

在有了这样的码集以后, 香农不是去计算某一特定好码的性能而是设法计算这些码的平均的性能, 从而巧妙地回避了寻找好码这一难题。下面就是按照这一随机编码和联合典型译码方法所得到的定理的证明。

证明 设信道容量  $C$  所对应的信道输入字母的概率分布为  $p(x)$ , 按此概率分布用随机编码方法得到码集  $\{\mathbf{C}\}$ 。

令输入消息等概率分布, 则码  $\mathbf{C}$  的平均译码差错概率为

$$P_e(\mathbf{C}) = \frac{1}{2^{NR}} \sum_{m=0}^{M-1} P_{e|m}(\mathbf{C}) \quad (5.30)$$

在集合  $\{\mathbf{C}\}$  上对  $P_e(\mathbf{C})$  取平均得

$$\begin{aligned} \overline{P_e(\mathbf{C})} &\stackrel{\text{def}}{=} \overline{P_e} = \sum_{\mathbf{C}} P(\mathbf{C}) P_e(\mathbf{C}) \\ &= \frac{1}{2^{NR}} \sum_{m=0}^{M-1} \sum_{\mathbf{C}} P(\mathbf{C}) P_{e|m}(\mathbf{C}) \end{aligned} \quad (5.31)$$

在随机编码中, 不同  $m$  值产生对应码字的方法是完全一样的, 因此  $P_{e|m}(\mathbf{C})$  在对码集取平均后将得到一个与  $m$  无关的值, 即

$$\sum_{\mathbf{C}} P(\mathbf{C}) P_{e|m}(\mathbf{C})$$

的值与  $m$  无关, 故可取  $m=0$ , 这样就得

$$\overline{P_e} = \sum_{\mathbf{C}} P(\mathbf{C}) P_{e|0}(\mathbf{C}) \stackrel{\text{def}}{=} \overline{P_{e|0}} \quad (5.32)$$

设  $\mathbf{y}$  是发送码字  $\mathbf{c}$  时信道输出处得到的接收矢量, 定义  $\mathbf{y}$  与  $\mathbf{c}_m$  构成联合典型序列的事件为  $E_m$ , 即

$$E_m = \{(\mathbf{c}_m, \mathbf{y}) \in G\}, \quad m = 0, 1, \dots, M-1 \quad (5.33)$$

则按联合典型译码法, 译码差错将在  $\mathbf{y}$  不与  $\mathbf{c}_0$  联合典型或  $\mathbf{y}$  与  $\mathbf{c}_0$  以外其他码字联合典型时发生, 所以

$$\overline{P_e} = \overline{P_{e|0}} = P(E_0^c \cup E_1 \cup \dots \cup E_{M-1}) \quad (5.34)$$

按联合界公式  $P[\bigcup_k S_k] \leq \sum_k P(S_k)$ , 得

$$\overline{P_e} \leq P(E_0^c) + \sum_{m=1}^{M-1} P(E_m) \quad (5.35)$$

由于  $\mathbf{y}$  是对应于输入  $\mathbf{a}$  时的信道输出, 所以它与  $\mathbf{a}, \mathbf{e}, \dots, \mathbf{a}_{M-1}$  相互独立, 故按定理 5.1 中的式(5.22)及式(5.27)得

$$\begin{aligned} \overline{P_e} &\leq \sum_{m=1}^{M-1} 2^{-N[I(X;Y) - 3]} \\ &= \sum_{m=1}^{M-1} (2^{NR} - 1) 2^{-N(C-3)} \\ &\quad + 2^{-N(C-3-R)} \end{aligned} \quad (5.36)$$

若  $R < C - 3$ , 且令  $N$  足够大, 则可使

$$2^{-N(C-3-R)}$$

所以最后得

$$\overline{P_e} \leq 2 \quad (5.37)$$

到此已经证明, 在足够长的码字下, 随机编码码集中码的平均译码差错概率  $P_e$  对码的平均值小于 2, 所以在这些码中至少有一个码具有与平均性能相同的平均译码差错概率, 即其  $P_e$  满足

$$P_e < 2 \quad (5.38)$$

令  $\epsilon = 2$ , 就得到所要的最终结果。

证毕

自香农给出信道编码定理的证明以来, 引起了人们对信道编码的极大兴趣, 但是香农只是证明了满足这种特性的码的存在性, 还不能按其证明方法得到好码。由于随机编码所得的码集很大, 通过搜索得到好码的方法在实际上很难实现, 而且即使找到其中的好码, 这种码的码字也是毫无结构的, 这意味着译码时只能用查表的方法, 而在  $N$  很大时这一译码表所需的存储量也是很难被接受的, 因此真正实用的信道码还需通过各种数学工具来构造, 使码具有很好的结构性以便于译码。

## 5.5 信道编译码方法的最初范例——汉明码

大约在信息论创建的同时, 与香农同在贝尔实验室工作的汉明提出了信道码的第一个系统的编译码方法——汉明码。在这一方法中汉明提出用模 2 和对

二元分组码码元进行一致性检验,以此来发现并确定码字中差错码元的位置。所谓一致性检验就是对被检验码元位置上的码字母进行统计,如果要求这些二元字母中 1 的数目是偶数,则称偶检验,否则称奇检验。汉明指出,如果我们能找到  $M$  个独立的一致检验条件,则检验结果就可以用来表示  $2^M$  种差错情况。设码字长为  $N$ ,则为了表示没有差错及  $N$  种单个差错的情况, $M$  应满足

$$2^M \geq N + 1 \quad (5.39)$$

同时,码字中必须有  $M$  位码元是为使一致检验条件成立而附加的,这些码元被称为检验位或监督位,而代表原消息的码元被称为信息位。以  $N=7$  为例,此时  $M=3$ ,用  $\mathbf{c} = (c_0, c_1, c_2, \dots, c_6)$  表示任一码字,则三个独立的一致检验方程可用码元的模 2 和值表示如下:

$$c_0 + c_1 + c_2 + c_3 = 0 \quad (5.40a)$$

$$c_1 + c_2 + c_3 + c_4 = 0 \quad (5.40b)$$

$$c_0 + c_1 + c_3 + c_6 = 0 \quad (5.40c)$$

码字中的前四位码元是信息位,后三位是检验位。如用  $(u_0, u_1, u_2, u_3)$  表示消息,则有

$$(c_0, c_1, c_2, c_3) = (u_0, u_1, u_2, u_3) \quad (5.41)$$

及 
$$c_4 = u_0 + u_1 + u_2 \quad (5.42a)$$

$$c_5 = u_1 + u_2 + u_3 \quad (5.42b)$$

$$c_6 = u_0 + u_1 + u_3 \quad (5.42c)$$

应该指出的是,码字中码元的这种区分只是因为代表消息的字母在信息位处可以毫无改变地直接出现,而在检验位处的码元则与若干位消息码元有关,但从一致检验的条件来讲,处在同一检验条件中的各个码元相互间只存在一种约束关系,不存在检验者和被检验者的关系。

式(5.40)所建立的汉明码共有 16 个码字,如表 5.2 所示。这一码的码字长  $N=7$ ,约束条件数  $M=3$ ,满足式(5.39)的要求,能纠正一个差错。

汉明码的巧妙之处在于它的编译码算法都特别简单,其编码过程已如前述,而其译码过程只需先按一致检验方程确定有无差错以及差错发生的位置,然后在该差错发生的码元处加 1 并取其模 2 值。例如,若一致检验方程(5.40a)和(5.40b)均成立但式(5.40c)的检验结果为 1,则差错必发生在  $c_6$  处,所以对接收矢量的这一码元字母加 1 并取其模 2 值后即得发送码字的正确估计值。

汉明码的码率  $R = K/N$  在上例中为  $4/7$ ,但若取  $M=10$ ,则按式(5.39)其码率可达  $1013/1023$ 。可以证明在同样的纠错能力下汉明码的码率是最高的。

## 5.6 分组码之一:线性码

汉明码被提出时并没有像信息论那样一开始就有系统的理论,因此它并没有立刻引起理论界的兴趣和重视,但在随后的若干年中它渐渐引起代数学家的兴趣,并迅速发展成系统的理论即代数编码理论。在这一节中我们将极其简要地介绍代数编码理论在分组码方面最主要的成果——线性码。

### 5.6.1 线性码的定义、编码与生成矩阵

在汉明码中汉明实际上提出了一个极其重要的概念,这就是把码字母 0, 1 不仅仅看作是符号(在信源的冗余度压缩编码中正是这样看的)而且看作是可以运算的数。不但如此,他还引入了一种特殊的运算——模 2 算术。按代数学理论, 0, 1 两个数在模 2 下的算术运算恰好构成有限域中最简单的域,即由两个元素组成的域。关于有限域的一般理论是在 19 世纪由伽罗瓦(E. Galois)建立的。按定义有限域具有以下性质:

(1) 是有限个元素的集合,对集合中的元素定义有两种运算——加和乘。

(2) 对加法,域中存在零元素 0,对乘法,域中存在幺元素 1。

(3) 对域中的每一个元素  $a$  都存在加逆元素  $(-a)$ ,  $a + (-a) = 0$ ; 对域中的每一个非零元素  $a$  都存在乘逆元素  $a^{-1}$ ,  $aa^{-1} = 1$ 。加逆和乘逆的存在也可说成是域中存在减法和除法。

(4) 加法和乘法各符合结合律和交换律;加法和乘法一起符合分配律,即  $a \cdot (b + c) = a \cdot b + a \cdot c$ 。

有限域并不能在任意数量的元素集合下都存在。最基本的有限域是有素数个元素的素数域,它由素数个数  $\{0, 1, 2, \dots, p-1\}$  及模  $p$  算术运算构成,其中  $p$  为素数,素数域记作  $F_p$ 。

域  $F_p$  上的  $m$  维矢量空间  $V_m(F_p)$  有  $p^m$  个元素,对  $V_m(F_p)$  中的任意两个元素  $\mathbf{a} = (a_0, a_1, a_2, \dots, a_{m-1})$ ,  $\mathbf{b} = (b_0, b_1, b_2, \dots, b_{m-1})$  按下述方法定义加法和乘法后也构成域:

(1) 加法:  $(a_0, a_1, \dots, a_{m-1}) + (b_0, b_1, \dots, b_{m-1}) = (a_0 + b_0, a_1 + b_1, \dots, a_{m-1} + b_{m-1})$

(2) 乘法:  $\mathbf{a} \cdot \mathbf{b} = \mathbf{c}$  其中  $\mathbf{c}$  由下述方程确定:

$$a_0 + a_1 x + \dots + a_{m-1} x^{m-1}$$

$$(a_0 + a_1 x + \dots + a_{m-1} x^{m-1})(b_0 + b_1 x + \dots + b_{m-1} x^{m-1}) \bmod p(x)$$

式中  $p(x)$  是  $F_p$  上不可约的  $m$  次多项式, 这样得到的域被称为素数域的扩域, 记作  $F_{p^m}$  或  $GF(p^m)$ , 以纪念有限域理论的创始人。

在引入有限域的概念以后, 汉明码的编码过程式(5.41)和式(5.42)就可以看成是元素在二元域上的消息矢量  $\mathbf{u}$  与二元域上矩阵  $\mathbf{G}$  的乘积, 即

$$\mathbf{c} = \mathbf{uG} \quad (5.43)$$

式中

$$\mathbf{u} = (u_0, u_1, u_2, u_3) \quad (5.44)$$

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad (5.45)$$

而一致检验方程组(5.40)则可表示成

$$\mathbf{cH}^T = \mathbf{0} \quad (5.46)$$

式中

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad (5.47)$$

这样, 按式(5.43)生成的全部码字组成了二元域上 7 维向量空间的一个 4 维子空间, 矩阵  $\mathbf{G}$  的 4 个行矢量是这一子空间的 4 个基矢量。同时,  $\mathbf{H}$  矩阵的行矢量则在 7 维向量空间中张成一个 3 维子空间, 这两个子空间中的矢量互相垂直。

将上述编码中的二元域推广到一般的有限域  $F_q$ , 就得到代数编码理论中所谓的线性码。线性码的定义如下:

域  $F_q$  上的一个  $(N, K)$  线性码  $\mathbf{C}$  是域  $F_q$  上  $N$  维向量空间  $V_N(F_q)$  中的一个  $K$  维子空间,  $N$  是码字长,  $K$  是信息位数,  $K/N$  是码率。行空间与此  $K$  维子空间相同的矩阵  $\mathbf{G}$  是这一码的生成矩阵, 满足条件

$$\mathbf{Hx}^T = \mathbf{0}, \text{ 当且仅当 } \mathbf{x} \in \mathbf{C} \quad (5.48)$$

的矩阵  $\mathbf{H}$  是这一码的一致检验矩阵。

显然, 一致检验矩阵  $\mathbf{H}$  的行空间是一个  $N - K$  维子空间, 它也是一个线性码。 $\mathbf{H}$  是这一码的生成矩阵,  $\mathbf{G}$  则是这一码的一致检验矩阵。我们称这一码与  $\mathbf{G}$  生成的码互为对偶码。

由线性代数知识不难知道  $K$  维子空间中任意  $K$  个线性独立的矢量都可以

作为这一子空间的基矢量,而由这些基矢量组成的矩阵都可以看成是这一子空间或这一码的生成矩阵,这些矩阵相互间是行等价的,但在这些矩阵中有唯一的一个行缩减梯法式矩阵,同一码的所有可能的生成矩阵都等价于这一行缩减梯法式矩阵。矩阵的行缩减梯法式具有下述性质:

- (1) 每行最左的非零元素是 1。
- (2) 每行最左非零元素所在列的其他元素均为零。
- (3) 设第  $l$  行的最左非零元素发生在  $t_l$  列,则有  $t_1 < t_2 < t_3 < \dots$ 。

所以每一个线性码对应唯一的行缩减梯法式生成矩阵。

当缩减梯法式生成矩阵  $\mathbf{G}$  具有下述形式

$$\mathbf{G} = (\mathbf{I}_K \quad \mathbf{A}) \quad (5.49)$$

时(其中  $\mathbf{I}_K$  为  $K$  阶单位矩阵),我们称由此产生的码为系统码,因为这时码字的前  $K$  位码元与消息矢量的  $K$  位码元完全相同。不难明白系统码的一致检验矩阵  $\mathbf{H}$  应为

$$\mathbf{H} = (-\mathbf{A}^T \quad \mathbf{I}_{N-K}) \quad (5.50)$$

线性码中两个码字之间的汉明距是指两个码字中相应码元取不同数值的码元的数目,而在一个码字中非零码元的数目被称为这一码字的重量,简称码重。

线性码的最重要的性质是其线性特性以及在此基础上的对称性。所谓线性特性是指线性码中任二码字的和或差仍为一码字。由于这一特点如果我们在一个码的所有码字上减去任一特定的码字,其所得的结果将仍是这同一码的全部码字。这就是线性码的高度的对称性,这一对称性在码距与码重的关系上得到了很好的反映。例如为求码中码字间的距离分布我们只须求出码中任一码字与其他所有码字的距离分布就可以了,因为所有码字的这一距离分布都是相同的。同时又因为任两个码字的差仍为一码字,所以这一码距分布又与这一码的码重分布相同。这些性质在线性码纠正差错能力的分析中起着极其重要的作用。

## 5.6.2 线性码的伴随式与伴随式译码

信道码的编码是一个一一映射的过程,但是信道码的译码恰是一个多一映射的过程。这一特点决定了信道码的译码一般有很高的复杂度,代数编码理论所作的努力有很大一部分就是为了使译码能有较低的复杂度。在这方面,线性码的对称性是使译码复杂度得以降低的一个极其重要的性质。

设信道输入与输出字母表的元素都是  $F_q$  中的元素,码字长  $N$ ,若信道噪声



是加性的,则接收矢量  $\mathbf{y}$  为

$$\begin{aligned}\mathbf{y} &= (y_0, y_1, \dots, y_{N-1}) = \mathbf{c} + \mathbf{z} \\ &= (c_0, c_1, \dots, c_{N-1}) + (z_0, z_1, \dots, z_{N-1})\end{aligned}\quad (5.51)$$

式中  $\mathbf{z}$  是随机噪声矢量,具有概率分布

$$P(\mathbf{Z} = \mathbf{z}) = p(\mathbf{z}), \mathbf{z} \in V_N(F_q) \quad (5.52)$$

$\mathbf{z}$  的具体数值称为差错模式。在接收矢量有差错的情况下利用一致检验矩阵对接收矢量进行检验将得到

$$\mathbf{s} = \mathbf{H}\mathbf{y}^T = \mathbf{H}(\mathbf{c} + \mathbf{z})^T = \mathbf{H}\mathbf{z}^T = \mathbf{0} \quad (5.53)$$

所以  $\mathbf{s} = \mathbf{0}$  可以指示差错的存在。它就像疾病伴随的症状那样随差错模式的变化而变化,所以被称为伴随式。

利用伴随式  $\mathbf{s}$  确定  $\mathbf{z}$  可能取值的方法是基于代数学中群的陪集分解理论。群是一种代数系统,对群中的元素定义有一种运算(加或乘),此运算满足下述 4 种性质:

(1) 闭合性:集合中任二元素运算的结果仍是集合中的元素。

(2) 结合律:对集合中的任意三个元素  $a, b, c$ ,若运算为加,则有  $(a + b) + c = a + (b + c)$ ;若运算为乘,则有  $(ab)c = a(bc)$ 。

(3) 幺元素:群中存在幺元素,运算为加法时此幺元素为 0,运算为乘法时为 1。

(4) 逆元素:运算为加法时,群中元素均存在加逆元素;运算为乘法时群中非零元素均存在乘逆元素。

和线性空间中存在线性子空间一样,群中也存在子群。群中子群是群元素集合的一个子集,它同时满足群的所有性质。

由群和子群的上述定义可清楚地看出,从群的意义讲  $(N, K)$  线性码又可看成是  $N$  维矢量在加法运算下所成加群的一个子群,线性码又称为群码就由此而来。

群的一个重要性质是群中元素可以按某一子群进行陪集分解。设加群  $G$  有元素  $g^1, g^2, \dots$ , 其子群  $H$  有元素  $h_1, h_2, \dots, h_n$ 。将这些元素按下法排成阵列:在第 1 行中写下子群的所有元素,子群的零元素放在最左端,其他元素则在第 1 行中出现并仅出现一次;取群中任一尚未在第 1 行中出现过的元素作为第 2 行的第 1 个元素,然后用这个元素分别与第 1 行中各元素相加后的和作为第 2 行的元素;类似地得到第 3 行、第 4 行等直至群的所有元素都出现在阵列中为止,如图 5.2 所示。除第 1 行外,阵列中同一行的元素组成一个陪集,陪集左端

第一个元素称为此陪集的陪集首。在第 1 行元素为子群的条件下,这一分解具有以下两定理所述的重要性质。

$$\begin{array}{cccccc}
 h_1 = 0 & h_2 & h_3 & \dots & h_n \\
 g_1 + h_1 = g_1 & g_1 + h_2 & g_1 + h_3 & \dots & g_1 + h_n \\
 \dots & \dots & \dots & \dots & \dots \\
 g_m + h_1 = g_m & g_m + h_2 & g_m + h_3 & \dots & g_m + h_n
 \end{array}$$

图 5.2 群的陪集分解

**定理 5.3** 当且仅当群  $G$  中两个元素  $g_1$  和  $g_2$  的差  $g_1 - g_2$  是子群  $H$  的元素时,  $g_1$  和  $g_2$  在同一陪集中。

**证明** 首先设  $g_1$  和  $g_2$  均在陪集首为  $g_i$  的陪集中, 则  $g_1$  和  $g_2$  必可表示成

$$g_1 = g_i + h_j, \quad g_2 = g_i + h_k$$

所以

$$g_1 - g_2 = h_j - h_k$$

因  $h_j, h_k$  均为子群元素, 故  $g_1 - g_2$  是子群元素。

反之, 若  $g_1 - g_2 = h_l$  是子群元素, 设  $g_1 = g_i + h_m$ , 则  $g_2 = g_1 - h_l = g_i + h_m - h_l$  故  $g_1$  和  $g_2$  同在  $g_i$  为陪集首的陪集中。证毕

**定理 5.4** 群  $G$  中的任一元素必在且仅在子群  $H$  的一个陪集中。

**证明** 按阵列的构造方法可知群  $G$  中的元素必在阵列中出现, 故只须证其仅出现一次。

设有某一元素在同一陪集中出现两次, 即有

$$g_i + h_l = g_i + h_m$$

则得  $h_l = h_m$ , 但这是不可能的。

再设有某一元素在不同陪集中出现, 即有

$$g_i + h_m = g_j + h_n$$

设  $i > j$ , 则  $g_i = g_j + h_n - h_m$ 。这说明  $g_i$  已在  $g_j$  为首的陪集中出现过, 不应在以后的陪集中再作陪集首。证毕

域  $F_q$  上  $N$  维矢量空间的全部元素在加法下构成加群, 所以可将其按某一  $(N, K)$  线性码作陪集分解并得到以全部码字为第 1 行元素的阵列, 阵列中的其他陪集则由陪集首与码字相加得到。按式(5.53)可知同一陪集的元素有相同的伴随式, 所以接收矢量的伴随式可以告诉我们差错模式落在哪一个陪集中。如果我们再把陪集首作为差错模式, 则据此可得到发送码字的估计值, 译码即告完成。

很明显,在上述译码过程中陪集首的选择具有重要的作用,当且仅当陪集首确实与差错模式一致时译码结果才是正确的,但按陪集分解方法陪集首的选定有一定的随意性。由定理 5.3 可知同一陪集的任一元素均可选作陪集首而不会影 响陪集的组成,另一方面由伴随式也不能确定陪集首的选择。实际上陪集中的任一元素均有可能是真正的差错模式,所以只有在确定了译码准则以后才可以唯一地确定陪集首。

在 5.2 节中已经指出,信道译码一般有两种准则。在对输入码字的概率分布没有先验知识的情况下最大似然译码准则是比较实用的准则,这时只须知道信道的特性。例如对  $q$  元对称无记忆信道,有

$$P(\mathbf{Z} = \mathbf{z}) = \prod_{n=0}^{N-1} P(Z_n = z_n) \quad (5.54)$$

$$\text{设} \quad P(Z = 0) = 1 - (q - 1) \quad (5.55a)$$

$$P(Z = z) = \frac{1}{q-1}, \quad z \neq 0 \quad (5.55b)$$

$$\text{则} \quad P(\mathbf{Z} = \mathbf{z}) = [1 - (q - 1)]^{N - w(\mathbf{z})} \left(\frac{1}{q-1}\right)^{w(\mathbf{z})} \quad (5.56)$$

式中  $w(\mathbf{z})$  是差错模式的重。如果  $n \geq 1/q$ , 则式(5.56)右端是  $w(\mathbf{z})$  的减函数,这时最大可能的  $\mathbf{z}$  是重量最小的  $\mathbf{z}$ , 它应被选作陪集首。

以上所述的译码方法通常被称为伴随式译码,其一般步骤可归结如下:

- (1) 由接收矢量计算伴随式;
- (2) 按信道特性在陪集中找出最大可能的矢量作为陪集首;
- (3) 在接收矢量中减去陪集首后作为发送码字的最大似然估计值输出。

从原理上讲,伴随式译码可用于任何线性码,它的实现需要存储  $q^{N-K}$  个伴随式及其相应的陪集首,其译码速度是已知方法中最快的。

## \* 5.7 分组码之二:循环码

在这一节中我们将对循环码作极其简要的介绍,其目的不是要由此导出实际可用的循环码及其编译码方法,而是要说明代数编码理论在构造信道编码时所追求的目标及其在码的对称性方面已达到的完美程度,从而为理解实用的循环码打下基础。如前所述,码的对称性一方面可以保证码字在矢量空间中有均匀的分布,而这是在对称信道和最大似然译码时所希望的。另一方面,对称性可以为译码算法的简化提供条件,而这是码的实用性所需要的。

### 5.7.1 循环码的定义

1957 年 E. Prange 在线性码中找出了一种具有更多结构特性的线性码的子集, 它不但具有任二码字之和仍为码字的线性特性, 而且任一码字的循环移位 (左移或右移) 后所得的结果仍是码字。具有这一特性的子空间被称为循环子空间, 相应的线性码则被称为循环码。

循环码在线性码中占有重要的位置。现在已知的好的线性码, 从最简单的汉明码到线性码中性能最好的 BCH 码都是循环码。

为进一步说明循环码定义的含义, 可取表 5.2 所列的汉明码为例, 它的生成矩阵  $\mathbf{G}$  为

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad (5.57)$$

对此矩阵作简单的行处理, 在此矩阵的第 1 行处先后加上第 3 行和第 4 行并在第 2 行处加上第 4 行, 其余行不变, 即得此码生成矩阵的另一种表示形式  $\mathbf{G}$ , 于是有

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad (5.58)$$

$\mathbf{G}$  的特点是它的每一行都是第 1 行循环右移产生的矢量。按线性码性质, 线性码的任一码字都是生成矩阵行矢量的线性组合, 因此由矩阵  $\mathbf{G}$  的特点即可推论此矩阵所对应的线性码还具有循环码的性质。如果直接看表 5.2 中这一码的 16 个码字, 则这一性质更加明显, 在这 16 个码字中除全 0 码字和全 1 码字外, 其余为 1011000 和 1110100 两个码字及其各自循环移位后所得的 14 个码字, 因此任一码字的循环移位所得的仍是码字。

### 5.7.2 循环码的编码与生成多项式

离散数学告诉我们一个有序的数组既可以用矢量表示, 也可以用多项式表

示。在用多项式表示时码字矢量  $\mathbf{c} = (c_0, c_1, c_2, \dots, c_{N-1})$  可以表示成码字多项式  $c(D)$ , 即

$$c(D) = c_0 + c_1 D + c_2 D^2 + \dots + c_{N-1} D^{N-1} \quad (5.59)$$

类似地, 可以用多项式代替矩阵的行矢量。例如式(5.58)中的矩阵  $\mathbf{G}$  可以表示成多项式矩阵  $\mathbf{G}(D)$ , 即有

$$\mathbf{G}(D) = \begin{pmatrix} g(D) \\ Dg(D) \\ D^2 g(D) \\ D^3 g(D) \end{pmatrix} \quad (5.60)$$

其中  $g(D) = 1 + D^2 + D^3$ 。最后, 由生成矩阵行矢量的线性组合产生码字的过程则可由多项式生成矩阵中多项式的线性组合来表示, 所以与式(5.43)对应可有

$$c(D) = (u_0, u_1, u_2, u_3) \begin{pmatrix} g(D) \\ Dg(D) \\ D^2 g(D) \\ D^3 g(D) \end{pmatrix} = (u_0 + u_1 D + u_2 D^2 + u_3 D^3) g(D) \quad (5.61)$$

令 
$$u(D) = u_0 + u_1 D + u_2 D^2 + u_3 D^3$$

为消息多项式, 则由式(5.61)得

$$c(D) = u(D) g(D) \quad (5.62)$$

式(5.62)说明, 在用多项式表示法代替矢量表示法以后线性码的编码可以看成是消息多项式与  $g(D)$  多项式的相乘,  $g(D)$  在这里的作用相当于生成矩阵在式(5.43)中的作用, 所以  $g(D)$  被称为生成多项式。不同的生成多项式将决定不同的码, 而同一码的码字多项式则有相同的生成多项式为其因子。

到此为止我们还没有说明这样得到的码是否是循环码。按循环码的定义, 码字的循环移位应仍为码字。在用多项式表示码字的情况下码字的移位相当于用  $D$  乘以码字多项式, 而循环意味着要求  $D^N = 1$ , 所以码字多项式  $c(D)$  的循环移位可以表示成

$$Dc(D) \bmod (D^N - 1)$$

由于同一码有相同的生成多项式, 所以若要求循环移位所得仍是同一码的码字, 则必须有

$$\{ Dc(D) \bmod (D^N - 1) \} \bmod g(D) = 0 \quad (5.63)$$

已知 
$$c(D) \bmod g(D) = 0 \quad (5.64)$$

所以要使式(5.63)成立就必须有

$$(D^N - 1) \bmod g(D) = 0 \quad (5.65)$$

或 
$$D^N - 1 = g(D) h(D) \quad (5.66)$$

这就是线性码同时具有循环码特性的条件。不难理解,这一条件不但是必要的,而且也是充分的。所以可有结论:当且仅当线性码由整除  $D^N - 1$  的生成多项式  $g(D)$  生成时,这一线性码同时还是循环码。式(5.66)中的  $h(D)$  被称为这一循环码的一致检验多项式。

循环码的编码可以如上面所述由消息多项式  $u(D)$  与生成多项式  $g(D)$  相乘得到,但这样得到的码不是系统码。为得到系统码形式的循环码,只须按如下步骤进行编码:

- (1) 将  $u(D)$  乘以  $D^{N-K}$  得  $D^{N-K} u(D)$ ;
- (2) 用  $g(D)$  除  $D^{N-K} u(D)$  得商  $q(D)$  及余式  $D^{N-K} u(D) \bmod g(D)$ ;
- (3) 取  $c(D) = D^{N-K} u(D) - D^{N-K} u(D) \bmod g(D)$ 。

上述最后一步所得的  $c(D)$  即是以  $g(D)$  为生成多项式的循环码码字。这一点不难证明,因为由第2步有

$$D^{N-K} u(D) = g(D) q(D) + D^{N-K} u(D) \bmod g(D) \quad (5.67)$$

故 
$$\begin{aligned} c(D) &= D^{N-K} u(D) - D^{N-K} u(D) \bmod g(D) \\ &= g(D) q(D) + D^{N-K} u(D) \bmod g(D) - D^{N-K} u(D) \bmod g(D) \\ &= g(D) q(D) \end{aligned} \quad (5.68)$$

$c(D)$  以  $g(D)$  为因子,所以确是循环码的码字,而且由上述步骤所得的码与按式(5.62)直接相乘得到的码是同一个码。

代数学知识告诉我们,若  $M$  能被  $N$  整除,则  $D^M - 1$  也能被  $D^N - 1$  整除,因此能被  $g(D)$  整除的  $D^N - 1$  多项式将远不止一个。在这些能被  $g(D)$  整除的  $D^N - 1$  中最小的  $N$  值是循环码可用码字长的最大值,其原因很简单,如果所用的码字长大于这一值  $N_m$ ,则相隔  $N_m + 1$  位的两个消息码元将在式(5.67)中有相同的余式,从而得到一个最小码距只有2的码,很难在实际中有应用。此外不难证明,若生成多项式为  $m$  次,则  $N_m$  的最大值为  $2^m - 1$ 。

### 5.7.3 循环码的伴随式与译码原理

循环码的译码在原理上与一般线性码的译码极为相似。在一般线性码时,伴随式是译码的主要基础,而在循环码时与上述伴随式类似的伴随多项式是循

环码译码的主要基础。

设接收信号对应的多项式 (简称接收多项式) 为  $y(D)$ , 它是码字多项式  $c(D)$  与差错多项式  $z(D)$  之和, 即

$$y(D) = c(D) + z(D) \quad (5.69)$$

将  $y(D)$  除以生成多项式  $g(D)$  则可得商  $q(D)$  及余式  $s(D)$ , 即

$$y(D) = g(D)q(D) + s(D) \quad (5.70)$$

由于循环码的所有码字都以  $g(D)$  为因式, 所以余式  $s(D)$  与差错多项式  $z(D)$  有简单的关系

$$s(D) = y(D) \bmod g(D) = z(D) \bmod g(D) \quad (5.71)$$

此式表明  $s(D)$  可以指示接收多项式中是否有差错以及差错的模式, 所以  $s(D)$  被称为循环码的伴随多项式或简称伴随式。

在一般的线性码中同一陪集的元素对应相同的伴随式, 不同陪集的元素对应有不同的伴随式, 各伴随式之间是没有任何关系的, 但在循环码中由于循环码所特有的码字循环移位仍得码字的性质, 在任一特定差错多项式的伴随式及其  $N-1$  个循环移位所得差错多项式的伴随式之间亦存在类似的“循环移位”特性。这一特性可以定理形式表述如下。

**定理 5.5** 设  $s(D)$  是差错多项式  $z(D)$  对应的伴随式,  $s_1(D)$  是  $z(D)$  的循环移位, 即  $Dz(D) \bmod (D^N - 1)$  对应的伴随式, 则  $s_1(D) = Ds(D) \bmod g(D)$ 。

**证明** 设  $y(D) = c(D) + z(D) = g(D)q(D) + s(D)$

将  $c(D) = u(D)g(D)$  代入上式, 即得

$$z(D) = g(D)[q(D) - u(D)] + s(D) \quad (5.72)$$

另一方面, 按所给条件有

$$\begin{aligned} s_1(D) &= [Dy(D) \bmod (D^N - 1)] \bmod g(D) \\ &= [Dz(D) \bmod (D^N - 1)] \bmod g(D) \end{aligned} \quad (5.73)$$

将式(5.72)代入上式, 得

$$\begin{aligned} s_1(D) &= [D(g(D)[q(D) - u(D)] + s(D)) \bmod (D^N - 1)] \bmod g(D) \\ &= D[g(D)[q(D) - u(D)] + s(D) \bmod g(D) \\ &= Ds(D) \bmod g(D) \end{aligned}$$

证毕

循环码的这一性质, 说明任一特定的差错多项式与其  $N-1$  个循环移位所得差错多项式在伴随式方面有很强的关系, 这些关系在差错多项式的计算或存储中都可以加以利用。例如可以对差错多项式或差错模式进行分类, 把任一特定差错模式及其  $N-1$  个循环移位所得的差错模式作为一类, 每类用此特定差

错模式作为其代表,从而减少译码时需要区别的差错模式的数目。以 $(7, 4)$ 汉明码为例,当作为一般线性码时译码需要区别的差错模式有 7 种,但当作为循环码时只需识别 1 种就可以了,因为其余 6 种都是这一差错模式循环位移所得的结果。

在伴随式的基础上循环码的译码在原理上由以下 3 步组成:

- (1) 按码的生成多项式或一致检验多项式计算接收多项式的伴随式;
- (2) 按伴随式计算差错多项式;
- (3) 在接收多项式中减去差错多项式后作为对发送码字的估计值输出。

译码的主要运算量或存储量来自上述第 2 步运算,如何减少这一运算量或存储量是代数编码理论研究中的一个重要内容。

## 5.8 树码、网格码与卷积码

树码是信道编码的另一种重要编码方式。在这种编码中消息序列首先被分成长为  $K$  的组,我们称它为信息码元组。与分组码不同的是,这一信息码元组不是被直接映射成信道码字,而是以此前  $M - 1$  组信息码元为条件将当前时刻的信息码元组映射成长为  $N$  的信道码元组,因此每一信道码元组都与  $M$  个信息码元组的内容有关。

树码的一种正式定义是这样的:一个 $(N, K)$ 树码是从域  $GF(q)$  上的半无限序列集合到同一  $GF(q)$  上半无限序列集合的一个映射。在这一映射中对任给  $M$  值均存在如下性质:前  $MK$  个信息码元相同的两个半无限序列经映射得到的两个半无限序列其前  $MN$  个信道码元也必相同。 $M$  是这一码的约束长度,  $R = K/N$  是这一码的码率。

树码的编码规律可以用类似 3.4 节所述的树图加以清晰的描述。当  $M$  是有限值时,树上间隔  $M$  的分支就会呈现相同的映射,树图因此可以用简化的篱笆状图或称网格图来表示,相应地称有限约束长的树码为网格码。

网格码中的约束关系如果是时不变的,则所得的网格码被称为滑动分组网。如再进一步把约束关系限制在线性约束关系,则此时的编码所得就相当于将消息序列输入数字滤波器后所得的输出,所以这样的码被称为卷积码,它是树码中得到最多分析结果和最广泛应用的一种码。

卷积码与线性分组码有很多类似之处。每一特定的卷积码也有其对应的生成矩阵,其差别仅在于卷积码的生成矩阵的元素是系数在有限域上的多项式。



卷积码的编码可以表示成半无限的消息序列在分组后与生成矩阵相乘。一个最简单的系数在二元域上的 $(2, 1)$ 卷积码的生成矩阵  $\mathbf{G}(D)$  为

$$\mathbf{G}(D) = (D^2 + 1, D^2 + D + 1) \quad (5.74)$$

设输入的消息序列为  $u(D)$ , 即

$$u(D) = u_0 + u_1 D + u_2 D^2 + \dots \quad (5.75)$$

$$\mathbf{c}(D) = u(D) \mathbf{G}(D) = (c_1(D), c_2(D)) \quad (5.76)$$

其中

$$c_1(D) = (u_0 + u_1 D + u_2 D^2 + \dots)(1 + D^2)$$

$$c_2(D) = (u_0 + u_1 D + u_2 D^2 + \dots)(1 + D + D^2)$$

按数字信号处理中的  $Z$  变换理论, 上式中的  $D$  相当于  $Z$  变换中的  $Z^{-1}$ , 而式 (5.76) 的多项式相乘则相当于离散数字序列通过数字滤波器时的卷积, 其关系如图 5.3 所示。图中的两个数字滤波器均由三级移位寄存器组成, 在实际实现时, 它们可以共用寄存器。由于系数在  $GF(2)$  上, 所以寄存器各级输出至相加器的连线的有无就代表了系数取 1 或 0。编码开始时, 移位寄存器先被置 0。随着消息序列的输入, 寄存器中的内容不断改变, 编码器所处的状态也不断变化。对这一具体的编码器而言, 它有四种可能的状态, 它们分别对应于移位寄存器右端两级所存储的此前输入的两位信息码元的值, 所以编码器的输出不但与此时刻输入的信息码元有关, 而且还与此前输入的两位信息码元有关。

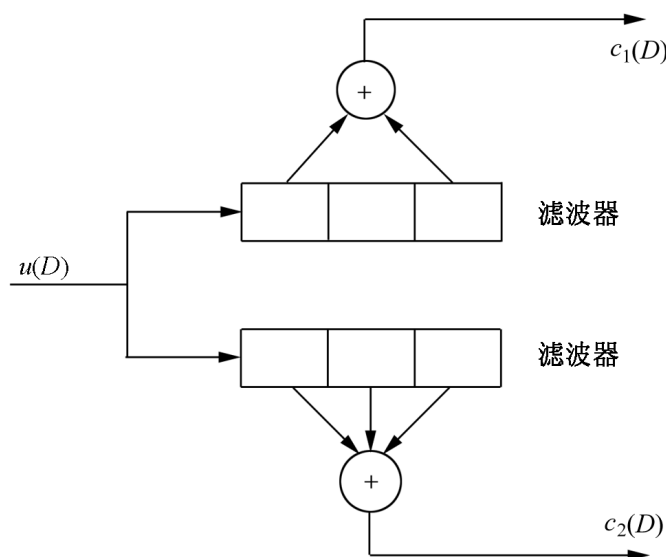


图 5.3 卷积码编码器实例

例如设

$$u(D) = 1 + D + D^3$$

则

$$c_1(D) = (1 + D + D^3)(1 + D^2) = 1 + D + D^2 + D^5$$

$$c(D) = (1 + D + D^3)(1 + D + D^2) = 1 + D^4 + D^5$$

上述编码过程可以用图 5.4 所示的状态图清晰地加以表示。图中 4 个长方框分别代表编码器的 4 个可能状态, 各状态之间的有向边表示在有信息码元输入时状态发生转移的方向, 实线代表输入为 1, 虚线代表输入为 0, 有向边旁边括号内的数字代表编码器的输出。根据状态图就可以方便地画出卷积码的网格图, 上述卷积码的网格图如图 5.5 所示。在初始时刻 ( $t=0$ ) 编码器处于 00 状态, 此时在 00 状态有虚线连向 00 状态, 有实线连向状态 10, 它们分别与输入为 0 和输入为 1 相对应。在  $t=1$  时刻这两种可能的状态, 根据输入消息的不同又分别与两种状态相连, 从而有可能停留在 4 种可能状态中的一种上。在  $t=2$  时这 4 种可能的状态根据输入消息码元的不同又各自转入下一个对应的状态。此后这一状态转移情况在网格图中就不断重复。不难看出, 网格图可以看成是状态图沿时间的展开, 它描绘出编码过程的全景。对应于任一确定的输入消息序列, 在网格图上将有一条由虚线(0)与实线(1)相连而成的路径与其对应, 沿路径边上标注的数字就是编码器的输出。

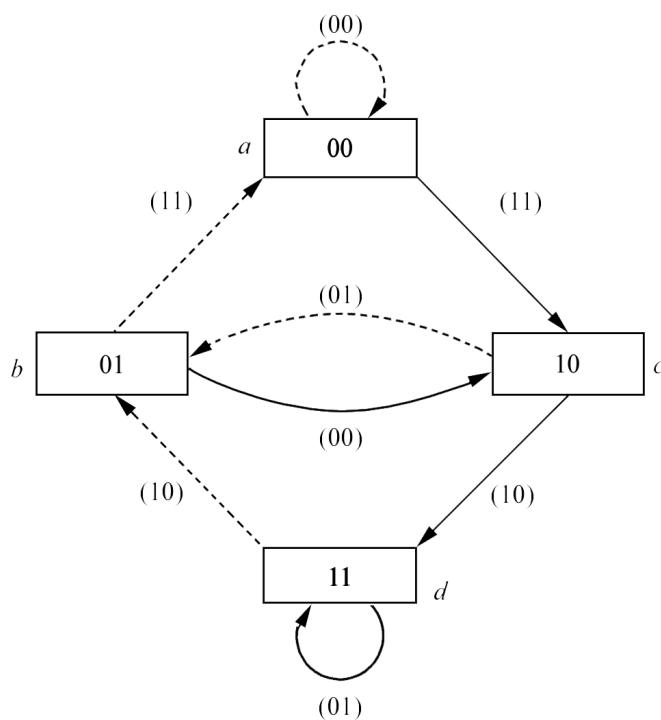


图 5.4 卷积码状态图

在一般情况下, 卷积码的生成矩阵是一个  $K$  行  $N$  列的多项式矩阵, 即

$$\mathbf{G}(D) = (g_{kn}(D))_{KN} \quad (5.77)$$

它由  $KN$  个多项式元素组成。在编码时输入的消息序列先经串并变换得到  $K$

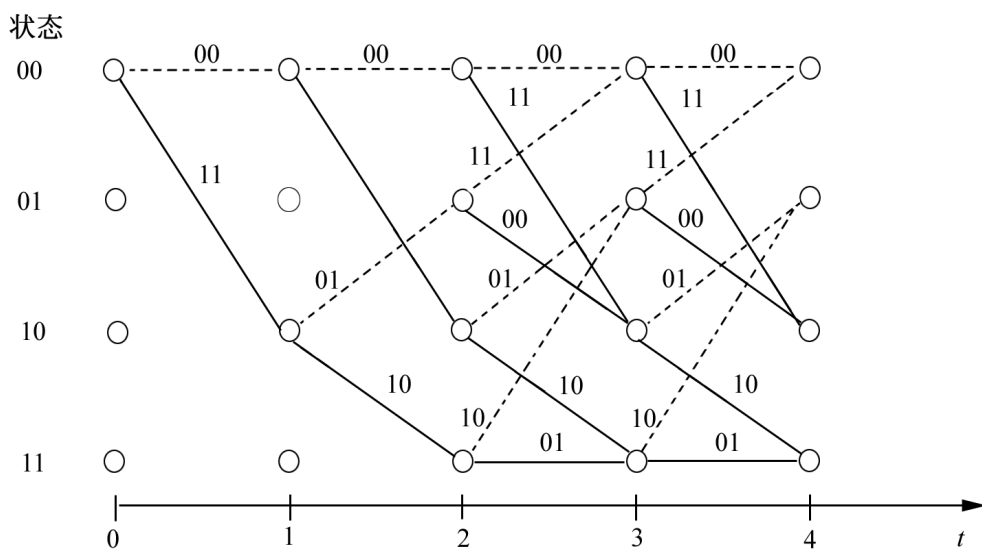


图 5.5 卷积码网格图实例

个并行的子序列  $u_k(D)$ ,  $k = 1, 2, \dots, K$ , 而编码器输出为

$$\mathbf{c}(D) = (c_1(D), c_2(D), \dots, c_N(D)) \quad (5.78)$$

其中

$$c_n(D) = \sum_{k=1}^K u_k(D) g_{kn}(D) \quad (5.79)$$

卷积码的约束长度按前述卷积码定义应为

$$M = \max_{k, n} [\deg(g_{kn}(D)) + 1] \quad (5.80)$$

其中  $\deg(g_{kn}(D))$  表示多项式  $g_{kn}(D)$  的幂次。但有些作者也把  $MK$  称为约束长度。

卷积码的性能取决于编码所得信道码元序列之间的距离, 但与分组码时情况不同的是卷积码的编码输出是一个半无限的码元序列族, 因此我们需要了解这些半无限码元序列之间的距离分布。这一问题初看似乎很复杂, 但实际上只须把注意力集中在第一个信道码元组的译码。如果它能被正确译出, 则由此所得的第一信息码元组对其后编码输出的影响就可以正确地计算出来, 这时随后第二个信道码元组的译码就面临和第一个信道码元组的译码完全相同的问题, 因此第一个信道码元组的译码是解决卷积码译码的突破口。为分析这一问题, 只需考察第一个信道码元组不相同的所有编码输出序列的前  $l$  个信道码元组。显然此集合中任二序列间的汉明距与第一个信道码元组的译码有直接的关系, 把此汉明距中的最小值记作  $d_l$ , 显然有

$$d_1 \quad d_2 \quad d_3 \quad \dots \quad (5.81)$$

$d_l$  中的最大值被定义为卷积码的自由距, 即

$$d_{\text{free}} = \max_i d_i \quad (5.82)$$

例如,在以上所举的卷积码例子中  $d_1 = 2$ ,  $d_2 = 3$  及  $d_{\text{free}} = 5$ 。卷积码的自由距正是卷积码半无限码元序列之间的最小距,它是衡量卷积码抗差错能力的一个最重要的参数。在对卷积码的研究中有大量的工作就是为了寻找有大的自由距的卷积码,可惜的是卷积码的理论研究和分组码的理论研究相比要困难得多,因此这方面的理论成果很少。但尽管在理论研究中遇到困难,现在已找到一些好的卷积码,这些码在宽带高斯信道中使用时的性能甚至优于最好的分组码。特别是 1993 年由 C. Berrou 等人提出的 Turbo 码在白色高斯噪声下的性能已非常接近香农给出的理论极限,这一码在误码率  $P_e$  为  $10^{-5}$  时所要求的信噪比  $E_b/N_0$  与理论极限仅差 0.7dB。

## 5.9 关于信道编码理论的若干评注

基于代数的信道编码构造方法目前已发展成相当系统的理论,在习惯上它常被简称为编码理论并被数学家们看成是近世代数的一个分支,但这一理论在给人以系统、完美的同时却尚未能给出从香农信道编码定理看来是理想的好码。所有已知的在  $N$  为有限值时有强纠错能力的码按其构造方法在  $N \rightarrow \infty$  时不是  $R = 0$ , 就是  $d_{\text{min}}/N \rightarrow 0$ 。唯一能使两者同时不趋于零的码是 1972 年时 J. Justensen 提出的码,但这一码的纠错能力并不理想。而香农编码定理证明存在有  $R$  接近  $C$  且能使传输误字率接近于零的好码,寻找这一意义上的好码的任务远没有完成。

代数编码理论的两个显著的特点是运算基于有限域,距离量度使用汉明距,正是这两个特点为代数编码的发展奠定了条件,但是这两点与物理信道的实际情况相距甚远,与香农编码定理关于模拟信道的理想信号要求相距甚远。对实际的物理信道而言,信号应当用时间的实函数或复函数表示。而在高斯信道中信号之间的距离量度应该是欧氏距离。为解决这一问题不断有人作各种努力,但是完全基于模拟信号(实函数或复函数)的构造方法都没有成功。直到 1977 年 G. Ungerboeck 终于找到了一条正确的解决途径。他的方法的要点是:

(1) 信道编码输出的有限域上的码字母序列分段后映射成多进数字调相信号或正交调幅信号。

(2) 用这些调制信号在复平面上表示时的欧氏距代替汉明距。

通过这一途径成功地把编码理论和调制理论结合起来,既利用了编码理论

已有的丰富的研究成果,又使这一理论能适应实际物理信道对理想信号的要求。Ungerboeck 提出的方法也因这种结合而被称为网格编码调制。现在,由于 G. Ungerboeck 及其后 G. D. Forney 等人的工作网格编码调制方法已形成系统的理论,而这一技术也已成为现代数字通信系统中标准的构成模块。一些具体的网格编码调制方法已在 ITU 制定的国际标准中被采用,对此感兴趣的读者可在近年出版的编码理论书籍或通信技术书籍中找到更详尽的介绍。

## 习 题

5.1 设有码  $\mathbf{C}$  在用此码传输时能使  $H(\mathbf{U}|\mathbf{Y}) = 0$  (式中  $\mathbf{U}$  表示码字矢量,  $\mathbf{Y}$  代表接收矢量), 试证此时的码率  $R$  必小于该信道的信道容量  $C$ 。(提示:  $H(\mathbf{U}) = H(\mathbf{U}|\mathbf{Y}) + I(\mathbf{U};\mathbf{Y})$ 。)

5.2 设用码字母表大小为  $J$  码长为  $N$  的分组码通过信道容量为  $C$  的信道传输信息, 试证: 收端译码的差错概率  $P_e$  满足

$$P_e \geq \frac{1}{\log J} (R - C) - \frac{1}{N}$$

式中  $R$  为输入信道的信息速率。

5.3 若最小码重为  $d$ , 码字母取自  $GF(q)$  的  $(N, K)$  码能纠正全部  $t$  个和  $t$  个以下的差错, 且  $t = \frac{d-1}{2}$ 。试证

$$[C_N^0 + (q-1)C_N^1 + \dots + (q-1)^t C_N^t] q^K = q^N$$

(能使上式取等号的码称为完备码。)

5.4 试证: 当且仅当监督矩阵  $\mathbf{H}$  的所有  $d-1$  列均线性独立时码的最小重才大于等于  $d$ 。

5.5 试证:  $(N, K)$  线性码的最小重  $d$  满足

$$N - K \leq d - 1$$

( $d = N - K + 1$  的码称为最大距离可分码。)

5.6  $(N, K)$  线性码  $\mathbf{C}$  的重量枚举式是指多项式

$$A(z) = \sum_{n=0}^N A_n z^n$$

式中  $A_n$  是指码中重  $n$  的码字数。若码  $\mathbf{C}$  的对偶码具有重量枚举式  $B(z) = \sum_{n=0}^N B_n z^n$ , 其中  $B_n$  是对偶码中重  $n$  的码字数, 则有

$$q^k B(k) = [1 + (q - 1)z]^n A \frac{1 - z}{1 + (q - 1)z}$$

上式称为 MacWilliams 等式。

(1) 用 (7, 4) 汉明码及其对偶码的码重分布检验上述关系式;

(2) 先求得 (15, 11) 汉明码对偶码的码重分布, 然后利用上式给出 (15, 11) 汉明码的码重分布。

5.7 设 (6, 3) 二元线性码的生成矩阵

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

(1) 找出  $\mathbf{G}$  的行缩减梯形法式表示;

(2) 求监督矩阵  $\mathbf{H}$ ;

(3) 找出最小重陪集首项;

(4) 在二元对称信道中对接收矢量 111010, 000011, 101010 进行译码;

(5) 计算码的重量枚举式。

5.8 设  $\mathbf{C}$  是  $GF(3) = (0 \ 1 \ 2)$  上的线性码, 而

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$$

(1) 试找出其对偶码;

(2) 在三元对称信道下对 2121, 2011, 2222 进行译码。

5.9 设有码如下所示:

信息	码字
00	00000
01	01101
10	10111
11	11010

(1) 找出生成矩阵  $\mathbf{G}$  与监督矩阵  $\mathbf{H}$ ;

(2) 在二元对称信道下给出最大似然译码的译码表;

(3) 求正确译码的概率。

5.10 试证:

(1) 二元线性码中码字重必全为偶数或奇偶各半;

(2)  $(N, K)$  码的平均码字重不超过  $N/2$ 。

5.11 设有两码如下:

码 **C**:  $x_1 = u_1$ ,  $x_2 = u_2$ ,  $x_3 = u_3$ ,  $x_4 = u_1 + u_2$

$x_5 = u_1 + u_3$ ,  $x_6 = u_2 + u_3$ ,  $x_7 = u_1 + u_2 + u_3$ ;

码 **G**:  $x_6 = u_2$ , 其它与 **C** 同;

其中  $u_i$  表信息码元,  $x_i$  表纠错码的码元。

- (1) 写出两码的 **G** 与 **H**;
- (2) 给出二元对称信道下的最大似然译码表;
- (3) 计算译码差错概率。

## 第 6 章 信源的信息速率失真函数 与熵压缩编码

信源的熵压缩编码是与信源的冗余度压缩编码并列的两类不同性质的编码,前者是有失真的,而后者是无失真的。对连续信源和模拟信源而言,实际上不可能也不必要进行无失真的编码,因此使用有失真的熵压缩编码对这两种信源来说是自然的和必然的选择。对离散信源来说,有失真的熵压缩编码理论也仍然有实用的价值。例如在通常被称为模式分类这样的问题中,有失真的熵压缩编码就是自然的选择。

信源的冗余度压缩编码	无失真	保熵
信源的熵压缩编码	有失真	熵压缩

在本章中我们将从以下两个方面讨论信源的熵压缩编码:

### (1) 信息速率失真函数(rate-distortion functions)

这是熵压缩编码的基础。这一函数成功地将信息与失真这两种不同的量度联系在一起,为信号处理中同时考虑这两个因素提供了可能。本章重点讨论离散信源、连续信源、模拟信源下信息速率失真函数的计算。对后两种信源一般情况下的计算是非常困难的,所以我们只给出了高斯连续信源与高斯模拟信源下的结果。

### (2) 熵压缩编码的具体方法

我们将重点介绍三种有代表性的方法,如下所示。虽然矢量量化时最通用的是熵压缩分组编码,但其基本概念和方法可以在标量量化中得到清楚的阐述,所以我们只重点介绍标量量化。变换编码是目前得到广泛应用的熵压缩分组编码,我们在这里重点讨论了如何得到最优的变换编码。最后作为熵压缩树码的实例我们对预测编码的过程进行了分析和讨论。



## 6.1 熵压缩编码和信源的信息速率失真函数

### 6.1.1 熵压缩编码

我们在第3章对信源的讨论中已经对离散信源作了比较仔细的分析,获得了主要几种离散信源的熵率和冗余度。从信息论的角度来看,离散信源的冗余度是对信号携带信息能力的一种浪费,解决的办法就是冗余度压缩编码。冗余度压缩编码可以对信源输出的信息进行有效的表示,它既可以保证信源输出信号在编译码前后不会有任何失真,同时从信号携带信息的角度来看可以保证编译码前后的信号具有相同的熵率,因此,冗余度压缩编码是无失真的保熵的编码。

但是,无失真的保熵的编码并非总是必需和可能的。在有些情况下,信息的接收者——信宿不需要或无力接收信源发出的全部信息。例如人眼对视觉信号的接收,人耳对听觉信号的接收等等就是这样,此时我们希望编译码后的信号在带有允许的失真下能使熵率尽量减小,以利于以后可能的传输或处理。在另一些情况下,则由于受到信息存储、处理或传输设备的限制而不得不对信源输出的信号作某种近似的表示以降低熵率。例如把连续信号送往数字计算机或数字信道时就是这样。诸如此类的问题导致了信源编码中另一类重要的编码——熵压缩编码,这种编码就是要在编译码前后的失真不超过一定数位的条件下把编码后的输出信号的熵率压缩到最小。

如果说无失真的冗余度压缩编码主要是针对离散信源的话,那么有失真的熵压缩编码就主要针对连续信源。连续信源在按照离散信源时类似的方法定义熵率时将会导致无穷大的熵率值,所以对连续信源的熵压缩编码是绝对必需的,但从理论上讲,熵压缩编码同样适用于离散信源。

### 6.1.2 离散无记忆信源的熵压缩分组编码及信源的信息速率失真函数

我们现在从离散无记忆信源开始来讨论熵压缩编码的理论。虽然从实用的观点来看讨论离散信源的熵压缩编码是没有多大意义的,因为熵压缩编码主要用于连续信源,但是从这里开始讨论可以使基本概念的阐述变得简单和易于理解。

设离散无记忆信源的字母表为  $A_U = \{ u_1, u_2, \dots, u_K \}$ , 熵压缩编码的码字母表为  $A_V = \{ v_1, v_2, \dots, v_J \}$ , 信源输出的字母序列记作  $\dots u_{-2} u_{-1} u_0 u_1 u_2 \dots$ , 编码后相应的码字母序列记作  $\dots v_{-2} v_{-1} v_0 v_1 v_2 \dots$ , 其中,  $u_n$  取字母  $u_k$  的概率为  $p(u_k)$ ,  $v_n$  取字母  $v_j$  的概率为  $p(v_j)$ 。熵压缩编码可以采用分组码的方式, 也可以采用树码的方式。当采用分组码时, 信源输出的源字母序列首先被分成由  $N$  个源字母组成的源字, 码字母序列也被相应分成由  $N$  个码字母组成的码字, 于是, 熵压缩分组编码实际上要完成由源字到码字的映射

源字      熵压缩分组编码      码字  
                    多对一映射

与冗余度压缩编码不同的一点是, 熵压缩编码在实际应用时一般只需要编码器。由于不存在与编码过程相反的逆过程, 因此一般意义下的译码器是不需要的, 所以我们可以认为熵压缩编码器的输出被直接送往信宿, 在这种情况下信源字母序列与码字母序列的差异就是熵压缩编码引入的失真。

如何对熵压缩编码引入的失真进行量度是一个比较复杂的问题, 它与实际的应用环境有关。在信息论中, 我们假定单个信源字母与单个码字母之间的失真是可以确定的, 把它记作  $d(u_k, v_j)$ , 或简记为  $d(k, j)$  后, 就得到一个  $K \times J$  个  $d(k, j)$  组成的字母失真矩阵

$$d(k, j) \quad K \times J$$

由于熵压缩编码是多对一映射, 所以一般来讲  $K > J$ 。类似地, 我们可以得到一个由信源字和码字之间的失真组成的  $K^N \times J^N$  字失真矩阵。字失真的量度在原则上讲应根据实际情况单独确定, 但我们一般采用的是所谓和失真量度。设  $\mathbf{u}$  和  $\mathbf{v}$  分别表示信源字和码字, 其中  $\mathbf{u} = (u_1 u_2 \dots u_N)$ ,  $\mathbf{v} = (v_1 v_2 \dots v_N)$ , 则在和失真量度下字失真的值为

$$d(\mathbf{u}, \mathbf{v}) = \frac{1}{N} \sum_{n=1}^N d(u_n, v_n) \quad (6.1)$$

字失真的统计平均  $E\{d(\mathbf{U}, \mathbf{V})\}$  就自然地成为码的失真量度, 称为码的平均失真。

如果我们把信源字的集合记作  $\{ \mathbf{u}_l^N, l = 1, 2, \dots, K^N \}$ , 把码字的集合记作  $\{ \mathbf{v}_m^N, m = 1, 2, \dots, J^N \}$ , 则熵压缩编码就可以用一个由条件概率  $q(\mathbf{v}_m^N | \mathbf{u}_l^N)$  组成的  $K^N \times J^N$  的字转移概率矩阵来表示。编码器按照这一概率矩阵在输入序列与输出序列之间建立起一种联系, 其互信息为

$$I(\mathbf{U}; \mathbf{V}) = I(U^N; V^N) = H(V^N) - H(V^N | U^N) \quad (6.2)$$

若把编码器看成是一个信道, 则  $I(U^N; V^N)$  就是信源通过编码器传输的信息速率, 故理想的熵压缩编码器的输出可能达到的最低熵率就是信源通过编码器所必须传输的最低的信息速率, 该最低的信息速率取决于信源的统计特性  $p(u)$ 、分组码的长度  $N$ 、字失真矩阵和允许的最大平均失真  $D$ 。当前三者给定后, 该最低的信息速率即为允许的最大平均失真  $D$  的函数, 该函数可表示为

$$R_N(D) = \min_{\{p(u, v) | E\{d(u, v)\} \leq D\}} I(U^N; V^N) \quad (6.3)$$

其中,  $\min$  是在平均失真满足

$$E\{d(u, v)\} = \sum_{u, v} p(u, v) d(u, v) \leq D \quad (6.4)$$

的所有字转移概率矩阵集合中取的。如果我们进一步对  $R_N(D)$  在所有可能的  $N$  值下取最小, 则可以得到一个只取决于信源统计特性和失真定义的函数  $R(D)$ , 其中

$$R(D) = \inf_N \frac{1}{N} R_N(D) \quad (6.5)$$

式(6.5)给出的  $R(D)$  函数被称为信源的信息速率失真函数, 简称率失真函数。

率失真函数  $R(D)$  给出了熵压缩编码可能达到的最小熵率与失真的关系, 其逆函数  $D(R)$  称为失真率函数, 它代表了一定信息速率下所可能达到的最小的平均失真。

## 6.2 信息速率失真函数的性质

在按式(6.5)具体计算离散无记忆信源的信息速率失真函数  $R(D)$  之前, 我们首先对这一函数的一般性质进行讨论, 下面是这一函数的主要性质。

**性质 6.1**  $R_N(D)$  的定义域为  $(D_{\min}, \infty)$ 。

**证明** 在和失真量度下, 码的平均失真为

$$\begin{aligned} E\{d(u, v)\} &= \sum_{u, v} p(u, v) d(u, v) \\ &= \sum_{u, v} p(u, v) \frac{1}{N} \sum_{n=1}^N d(u_n, v_n) \\ &= \sum_{n=1}^N \sum_{u_n, v_n} \frac{1}{N} p(u_n, v_n) d(u_n, v_n) \\ &= \sum_{n=1}^N \sum_{u_n, v_n} \frac{1}{N} p(u_n) q(v_n | u_n) d(u_n, v_n) \end{aligned}$$

$$\begin{aligned}
 &= \sum_{u_n} \sum_{v_n} p(u_n) q(v_n | u_n) d(u_n, v_n) \\
 &= \sum_u \sum_v p(u) q(v | u) d(u, v)
 \end{aligned} \quad (6.6)$$

若取

$$\begin{aligned}
 q(v_n | u_n) &= \begin{cases} 1, & \text{当 } v_n = v_n^* \text{ 时, 其中 } d(u_n, v_n^*) = \min_{v_n} d(u_n, v_n) \\ 0, & \text{其他} \end{cases}
 \end{aligned} \quad (6.7)$$

则得到可能的最小平均失真  $D_{\min}$  为

$$D_{\min} = \sum_u p(u) \min_v d(u, v) \quad (6.8)$$

另一方面, 定义

$$D_{\max} = \min_v \sum_u p(u) d(u, v) \quad (6.9)$$

并使编码器在任何输入的源字下都取使式(6.9)成立的码字  $\mathbf{v}$ , 则此时有

$$\begin{aligned}
 E\{d(\mathbf{U}, \mathbf{V})\} &= \sum_u \sum_v p(u) q(v | u) d(u, v) = \min_v \sum_u p(u) d(u, v) = D_{\max} \\
 I(U^N; V^N) &= H(V^N) = 0
 \end{aligned} \quad (6.10)$$

这说明当  $D = D_{\max}$  时,  $R_N(D) = 0$ 。

反之, 若  $R_N(D) = 0$ , 则达到此信息速率的熵压缩编码器的输入  $\mathbf{u}$  和输出  $\mathbf{v}$  之间必统计独立, 此时码的平均失真为

$$\begin{aligned}
 E\{d(\mathbf{U}, \mathbf{V})\} &= \sum_u \sum_v p(u) p(v) d(u, v) \\
 &= \sum_v p(v) \sum_u p(u) d(u, v) \\
 &= \sum_v p(v) D_{\max} = D_{\max}
 \end{aligned} \quad (6.11)$$

所以, 当  $R_N(D) = 0$  时, 必有  $D = D_{\max}$ 。

综上所述,  $R_N(D)$  的定义域为  $(D_{\min}, D_{\max})$ , 但在  $D = D_{\max}$  以后,  $R_N(D) = 0$ 。

证毕

**性质 6.2**  $R_N(D)$  是  $D$  的下凸函数, 也就是说, 若有  $\alpha_1, \alpha_2$  及  $D_1, D_2, D$ , 其中  $\alpha_1 + \alpha_2 = 1, D = \alpha_1 D_1 + \alpha_2 D_2$ , 则有

$$R_N(D) \geq \alpha_1 R_N(D_1) + \alpha_2 R_N(D_2) \quad (6.12)$$

**证明** 设  $q_1(\mathbf{v} | \mathbf{u})$  是达到  $R_N(D_1)$  的字转移概率,  $q_2(\mathbf{v} | \mathbf{u})$  是达到  $R_N(D_2)$  的字转移概率, 且这两种字转移概率下的互信息分别为  $I_1(U^N; V^N)$  和  $I_2(U^N; V^N)$ , 则

$$I(U^N; V^N) = R_N(D_1), \quad E\{d_1(\mathbf{U}, \mathbf{V})\} = D_1 \quad (6.13)$$

$$I(U^N; V^N) = R_N(D_2), \quad E\{d_2(\mathbf{U}, \mathbf{V})\} = D_2 \quad (6.14)$$

现定义字转移概率

$$q(\mathbf{v} | \mathbf{u}) = \alpha_1 q_1(\mathbf{v} | \mathbf{u}) + \alpha_2 q_2(\mathbf{v} | \mathbf{u}) \quad (6.15)$$

则在此转移概率下编码器的平均失真满足

$$\begin{aligned} E\{d(\mathbf{U}, \mathbf{V})\} &= \alpha_1 E\{d_1(\mathbf{U}, \mathbf{V})\} + \alpha_2 E\{d_2(\mathbf{U}, \mathbf{V})\} \\ \alpha_1 D_1 + \alpha_2 D_2 &= D \end{aligned} \quad (6.16)$$

设在上述字转移概率下编码器输入/输出的互信息为  $I(U^N; V^N)$ , 则由式(6.4)可得

$$R_N(D) = R_N(\alpha_1 D_1 + \alpha_2 D_2) = I(U^N; V^N) \quad (6.17)$$

由于互信息是转移概率的下凸函数, 则有

$$I(U^N; V^N) \leq \alpha_1 I(U^N; V^N) + \alpha_2 I(U^N; V^N) \quad (6.18)$$

综合式(6.13)、(6.14)、(6.17)和(6.18), 即得

$$R_N(D) \leq \alpha_1 R_N(D_1) + \alpha_2 R_N(D_2) \quad \text{证毕}$$

**性质 6.3** 对离散无记忆信源, 有  $R_N(D) = NR_1(D)$ 。

**证明** (1) 设  $q(\mathbf{v} | \mathbf{u})$  是达到  $R_N(D)$  的字转移概率, 即此时有

$$I(U^N; V^N) = R_N(D), \text{ 且 } E\{d(\mathbf{U}, \mathbf{V})\} = D$$

对离散无记忆信源, 有

$$p(\mathbf{u}) = \prod_{n=1}^N p(u_n) \quad (6.19)$$

故

$$\begin{aligned} I(U^N; V^N) &= H(U^N) - H(U^N | V^N) \\ &= \sum_{n=1}^N H(U_n) - H(U_1 | V^N) - H(U_2 | U_1 V^N) - \dots \\ &= \sum_{n=1}^N [H(U_n) - H(U_n | V_n)] = \sum_{n=1}^N I(U_n; V_n) \end{aligned} \quad (6.20)$$

若记  $D_n$  为信源字和码字各相应字母之间的平均失真, 则有

$$I(U_n; V_n) = R_1(D_n) \quad (6.21)$$

而

$$E\{d(\mathbf{U}, \mathbf{V})\} = D = \frac{1}{N} \sum_{n=1}^N D_n \quad (6.22)$$

于是有

$$I(U^N; V^N) = R_N(D) = \sum_{n=1}^N R_1(D_n) \quad (6.23)$$

又已知  $R_1(D)$  是  $D$  的下凸函数, 则应有

$$\frac{1}{N} \sum_{n=1}^N R_1(D_n) \geq R_1\left(\frac{1}{N} \sum_{n=1}^N D_n\right) = R_1(D) \quad (6.24)$$

综合式(6.23)和式(6.24), 则得

$$R_N(D) \geq NR_1(D) \quad (6.25)$$

(2) 设  $q(v|u)$  是达到  $R_1(D)$  的转移概率, 即

$$I(U; V) = R_1(D), \quad E\{d(U, V)\} = D$$

并取编码器的字转移概率为

$$q(\mathbf{v} | \mathbf{u}) = \prod_{n=1}^N q(v_n | u_n) \quad (6.26)$$

此时, 该编码器就相当于一个离散无记忆信道, 则有

$$I(U^N; V^N) = \sum_{n=1}^N I(U_n; V_n)$$

所以

$$I(U^N; V^N) \geq NR_1(D) \quad (6.27)$$

而此时的平均失真为

$$E\{d(\mathbf{U}, \mathbf{V})\} = \frac{1}{N} \sum_{n=1}^N D_n = D \quad (6.28)$$

故有

$$I(U^N; V^N) \geq R_N(D) \quad (6.29)$$

综合式(6.27)和式(6.29), 得

$$R_N(D) \geq NR_1(D) \quad (6.30)$$

因此, 综合式(6.25)和式(6.30), 即得

$$R_N(D) = NR_1(D) \quad (6.31)$$

证毕

从此性质可以得到离散无记忆信源的率失真函数  $R(D)$  的简单表达式为

$$R(D) = \inf_N \frac{1}{N} R_N(D) = R_1(D) \quad (6.32)$$

而  $R_1(D)$  为

$$R_1(D) = \min\{I(U; V), E\{d(U, V)\} = D\}$$

所以离散无记忆信源的率失真函数可表示为

$$R(D) = \min\{I(U; V), E\{d(U, V)\} \leq D\} \quad (6.33)$$

性质 6.4  $R(D)$  是定义域上的非增函数。

证明 设  $D_2 \leq D_1$ , 则有

$$\{q(\mathbf{v} | \mathbf{u}), E\{d(\mathbf{U}, \mathbf{V})\} \leq D_1\} \supseteq \{q(\mathbf{v} | \mathbf{u}), E\{d(\mathbf{U}, \mathbf{V})\} \leq D_2\}$$

故

$$\min\{I(U^N; V^N), E\{d(\mathbf{U}, \mathbf{V})\} \leq D_2\} \geq \min\{I(U^N; V^N), E\{d(\mathbf{U}, \mathbf{V})\} \leq D_1\}$$

从而即得

$$R_N(D_2) \geq R_N(D_1)$$

以及

$$R(D_2) \geq R(D_1) \quad \text{证毕}$$

根据率失真函数的以上 4 个性质, 我们不难得到  $R(D)$  曲线的一般形状如图 6.1 所示, 图中  $D_{\min}$  和  $D_{\max}$  的值取决于失真矩阵, 若对任一  $k$  都至少有一个  $j$  使  $d(k, j) = 0$ , 则有  $D_{\min} = 0$ ; 若失真矩阵中的元素有无穷大值, 则  $D_{\max}$  可能取无穷大,  $R(D_{\max})$  的值为零, 但  $R(D_{\min})$  一般需要通过较多的计算才能得到。如果失真矩阵的每行和每列有且仅有一个元素为零, 则此时  $D_{\min} = 0$ , 且有

$$R(0) = H(U) - H(U|V) = H(U)$$

当信源为连续信源时,  $H(U) = \infty$ , 此时  $R(0) = \infty$ 。

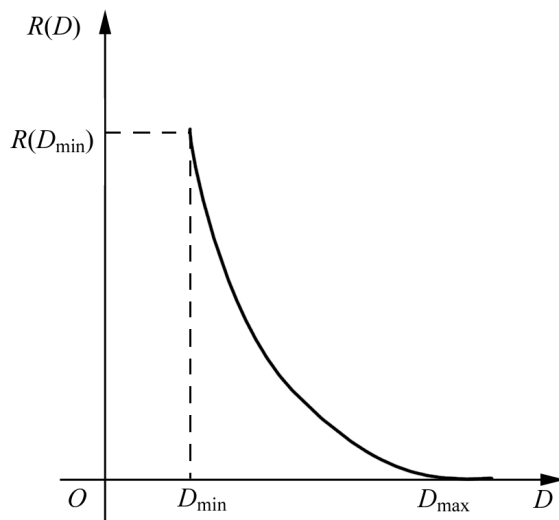


图 6.1  $R(D)$  曲线的一般形状

由  $R(D_{\max}) = 0$  及  $R(D)$  的下凸性可知,  $R(D)$  在  $(D_{\min}, D_{\max})$  上连续。又由  $R(D)$  的非负、下凸、非增及  $R(D_{\max}) = 0$  这几个条件可知,  $R(D)$  在  $[D_{\min}, D_{\max}]$  区间内必为严格递减函数, 所以  $R(D)$  曲线是由  $R(D_{\min})$  开始严格递减, 直至  $R(D_{\max}) = 0$  的连续下凸曲线。

最后, 我们由  $R(D)$  在  $[D_{\min}, D_{\max}]$  区间内的严格递减性可以得到一个重要

的推论:离散无记忆信源的信息速率失真函数定义中的不等式约束可以改为等式约束,即式(6.33)可以改写成

$$R(D) = \min\{I(U;V), E\{d(U,V)\} = D\} \quad (6.34)$$

### 6.3 离散无记忆信源下的信息速率失真函数的计算

现在我们来求离散无记忆信源下使互信息达到  $R(D)$  的编码器的转移概率。按照式(6.34),上述求解问题与第4章的信道容量求解时一样是一个有约束极值问题,即求

$$\min_{\substack{K \quad J \\ k=1 \quad j=1}} p(k)q(j|k) \log \frac{q(j|k)}{\sum_{l=1}^J p(k)q(j|l)} \quad (6.35)$$

其约束条件为

$$E\{d(U,V)\} = \sum_{k=1}^K \sum_{j=1}^J p(k)q(j|k)d(k,j) = D \quad (6.36)$$

$$\sum_{j=1}^J q(j|k) = 1, \quad k = 1, 2, \dots, K \quad (6.37)$$

$$q(j|k) \geq 0, \quad j = 1, 2, \dots, J, \quad k = 1, 2, \dots, K \quad (6.38)$$

#### 6.3.1 信息速率失真函数解的充要条件及参数方程

信息速率失真函数的求解和信道容量的求解一样,由于不等式的约束条件带来了许多麻烦。在没有不等式约束条件(6.38)时,由第2章的讨论知道  $I(\mathbf{P}, \mathbf{Q})$  是  $\mathbf{Q}$  的下凸函数,故必有唯一的极小值,亦即最小值,但是在不等式(6.38)的约束下,  $I(\mathbf{P}, \mathbf{Q})$  的最小值有可能发在某几个条件概率为零的边界上,从而可能涉及很多组等式约束的极值求解问题,所以一般没有解析形式的解。下面的定理给出了解所满足的充要条件及其参量方程。

**定理 6.1** 编码器输入/输出的互信息在转移概率  $\mathbf{Q}^*$  时达到  $R(D)$  的充要条件是

$$q^*(j|k) = p^*(j) e^{s d(k,j)} \quad (6.39)$$

$$\sum_{k=1}^K p^*(k) e^{s d(k,j)} = 1, \quad \text{当 } p^*(j) > 0 \text{ 时} \quad (6.40)$$



$$\prod_{k=1}^K p(k) e^{s d(k, j)} = 1, \quad \text{当 } p^*(j) = 0 \text{ 时} \quad (6.41)$$

其中,  $k$  满足

$$k = \arg \max_{j=1}^J p^*(j) e^{s d(k, j)} \quad (6.42)$$

此时有

$$D = \sum_{k=1}^K \sum_{j=1}^J p(k) p^*(j) e^{s d(k, j)} d(k, j) \quad (6.43)$$

$$R(D) = sD + \sum_{k=1}^K p(k) \log k \quad (6.44)$$

证明 利用拉格朗日乘数法将式(6.35)的求解化为下述函数

$$g(\mathbf{Q}) = I(\mathbf{P}, \mathbf{Q}) - \sum_{k=1}^K \mu(k) \sum_{j=1}^J q(j|k) - s \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) d(k, j) \quad (6.45)$$

在有界区域内的无约束极值问题。由于  $g(\mathbf{Q})$  是  $\mathbf{Q}$  的下凸函数  $I(\mathbf{P}, \mathbf{Q})$  和  $\mathbf{Q}$  的线性函数之和, 故仍为下凸函数。根据第 4 章中关于凸函数极值点的充要条件, 可知其最小值必须满足

$$\frac{\partial g(\mathbf{Q})}{\partial q(j|k)} = 0, \quad \text{当 } q^*(j|k) > 0 \quad (6.46)$$

$$\frac{\partial g(\mathbf{Q})}{\partial q(j|k)} \leq 0, \quad \text{当 } q^*(j|k) = 0 \quad (6.47)$$

令

$$k = e^{\mu(k) - p(k)} \quad (6.48)$$

则有

$$\begin{aligned} g(\mathbf{Q}) &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log \frac{q(j|k)}{\sum_{l=1}^K p(l) q(j|l)} - \\ &\quad \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log k - \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log e^{s d(k, j)} \\ &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log \frac{q(j|k)}{k p(k) e^{s d(k, j)}} \end{aligned}$$

取偏导数有

$$\begin{aligned}
\frac{g(\mathbf{Q})}{q(j|k)} &= \frac{1}{q(j|k)} \sum_{m=1}^K \sum_{n=1}^J p(m) q(n|m) \log \frac{q(n|m)}{p(l) q(n|l)} - \\
&\quad \frac{1}{q(j|k)} \sum_{m=1}^K \sum_{n=1}^J p(m) q(n|m) \log [p(m) e^{s d(m,n)}] \\
&= p(k) \log \frac{q(j|k)}{p(j)} - p(k) \log [p(k) e^{s d(k,j)}] \quad (6.49)
\end{aligned}$$

$$= p(k) \log \frac{q(k|j)}{p(k)} - p(k) \log [p(k) e^{s d(k,j)}] \quad (6.50)$$

当  $q^*(j|k) > 0$  时, 由式(6.46)及式(6.49)得解的充要条件为

$$q^*(j|k) = p^*(j) k e^{s d(k,j)} \quad (6.51)$$

根据约束条件(6.37)对式(6.51)取和, 则得拉格朗日乘数为

$$k = \sum_{j=1}^J p^*(j) e^{s d(k,j)} - 1 \quad (6.52)$$

又由式(6.46)及式(6.50)得

$$q(k|j) = p(k) k e^{s d(k,j)}$$

即得

$$\sum_{k=1}^K p(k) k e^{s d(k,j)} = 1 \quad (6.53)$$

若有  $q^*(j|k) = 0$ , 则按照式(6.47)及式(6.50), 可得

$$q(k|j) = p(k) k e^{s d(k,j)} \quad (6.54)$$

将式(6.54)对全部  $k$  值取和, 即得

$$\sum_{k=1}^K p(k) k e^{s d(k,j)} = 1 \quad (6.55)$$

可以看出, 式(6.51)、(6.52)、(6.53)和(6.55)在形式上已与定理中的充要条件中的式(6.39)、(6.40)、(6.41)和(6.42)一致, 只是这里是按照  $q^*(j|k)$  是否为零给出的, 而不是按照  $p^*(j)$  是否为零给出的。事实上, 除了  $s = -$  以外, 这两个条件是等价的。因为按照式(6.48)  $k$  是不为零的, 所以由式(6.51)可以看出, 当且仅当  $p^*(j)$  为零时  $q^*(j|k)$  才为零, 即若某个  $k$  值下  $q^*(l|k) = 0$ , 则必有  $q^*(l|k)$  对所有  $k$  均为零, 于是必有  $p^*(l) = 0$ 。

以上推理尚有不严格之处, 即式(6.51)中先假定了  $q^*(j|k) > 0$ 。为了使推理更严格, 可用  $q^*(l|k) = 0$  作为一个约束条件, 构造出新函数

$$J(\mathbf{Q}) = g(\mathbf{Q}) - q(l|k)$$

其中  $\lambda$  为拉格朗日乘数, 然后按无约束极值问题求解, 即得

$$q^*(j|k) = p^*(j) e^{s d(k,j)}, \quad \text{当 } j \neq l \text{ 时} \quad (6.56)$$

$$q^*(j|k) = p^*(j) e^{s d(k,j) + \overline{p(k)}}, \quad \text{当 } j = l \text{ 时} \quad (6.57)$$

对  $q^*(j|k)$  的  $j$  的所有值取和, 可知  $\lambda > 0$ , 故不管  $\lambda$  取多少, 只要  $q^*(l|k) = 0$ , 则必有  $p^*(l) = 0$ , 因此, 式(6.51)、(6.53)和(6.55)与式(6.39)、(6.40)和(6.41)完全等价。

另一方面, 当  $\mathbf{Q} = \mathbf{Q}^*$  时, 平均失真应等于  $D$ , 互信息应等于  $R(D)$ , 故有

$$\begin{aligned} E\{d(k, j)\} &= \sum_{k=1}^K \sum_{j=1}^J p(k) q^*(j|k) d(k, j) \\ &= \sum_{k=1}^K \sum_{j=1}^J p(k) p^*(j) e^{s d(k,j)} d(k, j) = D \\ I(\mathbf{P}, \mathbf{Q}^*) &= R(D) = \sum_{k=1}^K \sum_{j=1}^J p(k) q^*(j|k) \log [p(k) e^{s d(k,j)}] \\ &= sD + \sum_{k=1}^K p(k) \log p(k) \end{aligned}$$

此即定理要证的式(6.43)和式(6.44), 在这两式中,  $D$  和  $R(D)$  是通过参数  $s$  联系起来的,  $R(D)$  并没有显式解。为了明确表示这一关系, 可以将上面两式写成

$$D_s = \sum_{k=1}^K \sum_{j=1}^J p(k) p^*(j) e^{s d(k,j)} d(k, j) \quad (6.58)$$

$$R(D_s) = sD_s + \sum_{k=1}^K p(k) \log p(k) \quad (6.59)$$

证毕

下面我们来看看  $R(D_s)$  与参数  $s$  的关系

$$\begin{aligned} \frac{dR(D_s)}{dD_s} &= s + D_s \frac{ds}{dD_s} + \sum_{k=1}^K p(k) \frac{1}{p(k)} \frac{dp(k)}{ds} \\ &= s + \frac{ds}{dD_s} D_s + \sum_{k=1}^K p(k) \frac{1}{p(k)} \frac{dp(k)}{ds} \end{aligned} \quad (6.60)$$

其中

$$\begin{aligned} \sum_{k=1}^K p(k) \frac{1}{p(k)} \frac{dp(k)}{ds} &= \sum_{k=1}^K p(k) \frac{1}{p(k)} (-1) \sum_{j=1}^J p^*(j) e^{s d(k,j)} d(k, j) \\ &= - \sum_{k=1}^K \sum_{j=1}^J p(k) p^*(j) e^{s d(k,j)} d(k, j) = -D_s \end{aligned}$$

代入式(6.60)中,即得

$$\frac{dR(D_s)}{dD_s} = s \quad (6.61)$$

由此可以得出  $s$  等于  $R(D_s)$  在  $D_s$  处的斜率。

根据定理 6.1, 在一些简单情况下, 我们可以给出  $\mathbf{Q}^*$  及  $R(D)$  的解。设在  $j = 1, 2, \dots, J$  中  $p^*(j) > 0$  的个数为  $J_P$ , 其集合记作  $A_{VP}$ , 取矩阵  $\mathbf{A}$  为

$$\mathbf{A} = (a_{kj})_{K \times J_P} = (e^{s d(k, j)})_{K \times J_P}$$

并记

$$x_k = \sum_{j \in A_{VP}} p(j) a_{kj}, \quad k = 1, 2, \dots, K \quad (6.62)$$

$$y_k = \frac{1}{K} \quad (6.63)$$

$$\mathbf{P}(j) = (p(j_1), p(j_2), \dots, p(j_j), \dots, p(j_{J_P}))^T, \quad j \in A_{VP} \quad (6.64)$$

据此, 式(6.42)和式(6.40)可写成

$$\mathbf{A} \mathbf{P}(j) = \mathbf{y} \quad (6.65)$$

$$\mathbf{A}^T \mathbf{x} = \mathbf{1} \quad (6.66)$$

其中,  $\mathbf{y} = (y_1, y_2, \dots, y_K)^T$ ,  $\mathbf{x} = (x_1, x_2, \dots, x_K)^T$ ,  $\mathbf{1} = (1, 1, \dots, 1)_{J_P \times 1}^T$ 。

式(6.65)表示了  $K$  个方程, 式(6.66)表示了  $J_P$  个方程。如果  $K = J_P$ , 则  $\mathbf{A}$  为方阵, 假定其逆矩阵存在, 则得

$$\mathbf{x} = (\mathbf{A}^T)^{-1} \mathbf{1} \quad (6.67)$$

根据式(6.63)即可得  $\mathbf{y}$ 。将求得的  $\mathbf{y}$  代入式(6.65)中, 则得

$$\mathbf{P}(j) = \mathbf{A}^{-1} \mathbf{y} \quad (6.68)$$

由  $\mathbf{P}(j)$  及  $\mathbf{y}$  代入式(6.39)中即可求得  $\mathbf{Q}^*$ , 再利用式(6.43)和式(6.44)即可求出  $R(D)$  的参量表达式。在某些简单的情况下, 参数  $s$  有可能被消去而得到  $R(D)$  的解析表达式。

需要说明的是,  $R(D)$  的求解虽然在一定程度上和信道容量求解相似, 但从实际角度看却大不相同。在信道容量的求解问题中, 输入字母总数与输出字母总数相等这种最简单的情况代表了在实用中最有意义的情况, 而在信息速率失真函数的求解问题中,  $K = J_P$  这种最简单的情况是最没有实际意义的。有实际意义的是  $K > J_P$  的情况, 而此时求式(6.65)和式(6.66)的解析解是困难的。

下面给出信息速率失真函数的另一种表示形式, 该形式对于获得此函数的下界十分有用。

**定理 6.2** 信息速率失真函数可以表示成

$$R(D) = \max_{s \geq 0, s} sD + \sum_{k=1}^K p(k) \log_k \quad (6.69)$$

其中

$$\begin{aligned} s &= (s_1, s_2, \dots, s_K), \quad s_k \geq 0 \\ s &= \sum_{k=1}^K p(k) e^{s d(k, j)} = 1 \end{aligned} \quad (6.70)$$

则  $s$  和  $s$  能使上述最大值达到的充要条件是它们能满足式 (6.39)、(6.40)、(6.41) 和 (6.42)。

证明 设  $s \geq 0$ ,  $s \geq s$ , 且  $\mathbf{Q}$  满足  $E\{d(k, j)\} \leq D$ , 于是

$$sE\{d(k, j)\} \leq sD$$

则有

$$\begin{aligned} I(\mathbf{P}, \mathbf{Q}) - sD &= \sum_{k=1}^K p(k) \log_k \\ I(\mathbf{P}, \mathbf{Q}) - s \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) d(k, j) &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log_k \\ &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log \frac{q(j|k)}{p(j) e^{s d(k, j)}} \\ &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \left( 1 - \frac{p(j) e^{s d(k, j)}}{q(j|k)} \right) \\ &= 1 - \sum_{j=1}^J p(j) \sum_{k=1}^K p(k) e^{s d(k, j)} = 1 - \sum_{j=1}^J p(j) = 0 \end{aligned}$$

所以对所有满足  $E\{d(k, j)\} \leq D$  的  $\mathbf{Q}$  均有

$$I(\mathbf{P}, \mathbf{Q}) \leq sD + \sum_{k=1}^K p(k) \log_k$$

故

$$I(\mathbf{P}, \mathbf{Q}) \leq \max_{s \geq 0, s} sD + \sum_{k=1}^K p(k) \log_k$$

另一方面, 由定理 6.1 可知, 存在  $\mathbf{Q}^*$  满足

$$\sum_{k=1}^K \sum_{j=1}^J p(k) q^*(j|k) d(k, j) = D$$

且存在  $s \geq 0$  和  $s$ , 使当  $D = D_s$  时有

$$R(D_s) = I(\mathbf{P}, \mathbf{Q}^*) = sD_s + \sum_{k=1}^K p(k) \log_k$$

所以

$$R(D) = \max_{s \geq 0, \{p_k\}} sD + \sum_{k=1}^K p_k \log \frac{1}{p_k} \quad \text{证毕}$$

### \* 6.3.2 求解信息速率失真函数的迭代算法

尽管在理论分析中要找解析解始终是一个重要的目标,因为它可以帮助我们了解参数间的关系。但在实际工程中,数值解仍是可接受的。和计算信道容量的迭代算法相似,R. Blahut 于 1972 年提出了求解信息速率失真函数的迭代算法。下述定理则是该算法的基础。

**定理 6.3** 设  $s \geq 0$ , 令  $\mathbf{Q}$  表示  $q(j|k)$  组成的转移概率矩阵,  $p_0(j)$  是迭代的初始概率, 且  $p_0(j) > 0$ 。定义

$$p_{n+1}(j) = p_n(j) \frac{\sum_{k=1}^K p_k e^{s d(k,j)}}{\sum_{l=1}^J p_n(l) e^{s d(k,l)}} \quad (6.71)$$

$$q_{n+1}(j|k) = \frac{p_n(j) e^{s d(k,j)}}{\sum_{l=1}^J p_n(l) e^{s d(k,l)}} \quad (6.72)$$

则当  $n \rightarrow \infty$  时, 有

$$D(\mathbf{Q}_n) \rightarrow D_s \quad (6.73)$$

$$I(\mathbf{Q}_n) \rightarrow R(D_s) \quad (6.74)$$

**证明** 对任何给定的  $\mathbf{Q}$ , 可以得到互信息  $I(\mathbf{Q})$  和平均失真  $D(\mathbf{Q})$ 。定义

$$V(\mathbf{Q}) = I(\mathbf{Q}) - sD(\mathbf{Q}) \quad (6.75)$$

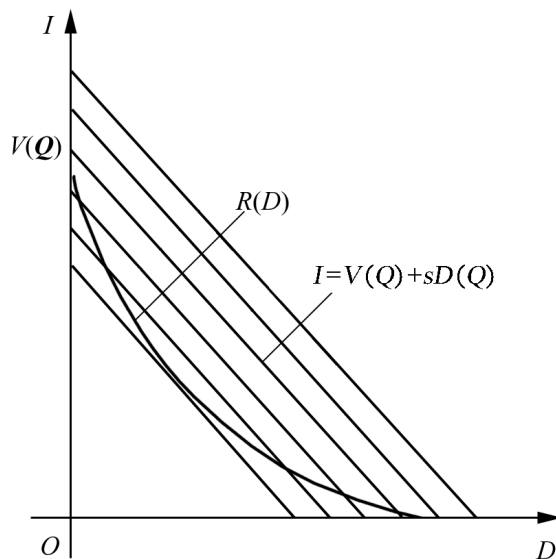
可以想象, 在同样的平均失真下, 上述  $\mathbf{Q}$  所对应的  $I(\mathbf{Q})$  不一定是最小的, 而我们要找的是最小的  $I(\mathbf{Q})$ 。如果我们以  $I$  和  $D$  为坐标, 将式 (6.75) 写成

$$I(\mathbf{Q}) = V(\mathbf{Q}) + sD(\mathbf{Q})$$

则此式对应于  $I$ - $D$  平面上斜率为  $s$  的直线, 如图 6.2 所示, 这时  $V(\mathbf{Q})$  刚好对应于该直线与  $I$  轴的交点。下面将证明在迭代中  $V(\mathbf{Q}_n)$  不断减小, 直至该直线与  $R(D)$  曲线相切, 此时  $I(\mathbf{Q})$ ,  $D(\mathbf{Q})$  成为  $R(D)$  曲线上斜率为  $s$  的点。

由于

$$\begin{aligned} V(\mathbf{Q}_{n+1}) &= I(\mathbf{Q}_{n+1}) - sD(\mathbf{Q}_{n+1}) \\ &= \sum_{k=1}^K p_k \sum_{j=1}^J q_{n+1}(j|k) \log \frac{q_{n+1}(j|k)}{p_{n+1}(j)} - s \sum_{k=1}^K p_k \sum_{j=1}^J q_{n+1}(j|k) d(k,j) \end{aligned}$$

图 6.2  $I$ - $D$  平面与  $R(D)$  曲线

将式(6.72)代入上式得

$$\begin{aligned}
 V(\mathbf{Q}_{t+1}) &= I(\mathbf{Q}_{t+1}) - sD(\mathbf{Q}_{t+1}) \\
 &= \sum_{k=1}^K \sum_{j=1}^J p(k) q_{n+1}(j|k) \log \frac{p_n(j) e^{s d(k,j)}}{p_{n+1}(j) \prod_{l=1}^J p_n(l) e^{s d(k,l)}} - \\
 &\quad \sum_{k=1}^K \sum_{j=1}^J p(k) q_{n+1}(j|k) \log e^{s d(k,j)} \\
 &= \sum_{j=1}^J p_{n+1}(j) \log \frac{p_n(j)}{p_{n+1}(j)} - \sum_{k=1}^K p(k) \log \prod_{l=1}^J p_n(l) e^{s d(k,l)}
 \end{aligned}$$

于是有

$$\begin{aligned}
 V(\mathbf{Q}_{t+1}) - V(\mathbf{Q}_t) &= \sum_{j=1}^J p_{n+1}(j) \log \frac{p_n(j)}{p_{n+1}(j)} - \sum_{k=1}^K \sum_{j=1}^J p(k) q_n(j|k) \\
 &\quad \cdot \log \frac{p_{n-1}(j) \prod_{l=1}^J p_n(l) e^{s d(k,l)}}{p_n(j) \prod_{l=1}^J p_{n-1}(l) e^{s d(k,l)}} \\
 &= \sum_{j=1}^J p_{n+1}(j) \log \frac{p_n(j)}{p_{n+1}(j)} + \sum_{k=1}^K \sum_{j=1}^J p(k) q_n(j|k)
 \end{aligned}$$

$$\begin{aligned}
& \cdot \log \frac{\frac{p_n(j)}{J} e^{s d(k, j)}}{q_n(j|k) \prod_{l=1}^J p_n(l) e^{s d(k, l)}} \\
& \prod_{j=1}^J p_{n+1}(j) \frac{p_n(j)}{p_{n+1}(j)} - 1 + \prod_{k=1}^K p(k) q_n(j|k) \\
& \cdot \frac{\frac{p_n(j)}{J} e^{s d(k, j)}}{q_n(j|k) \prod_{l=1}^J p_n(l) e^{s d(k, l)}} - 1 \\
& = 0 + \prod_{k=1}^K \frac{\frac{p(k)}{J} e^{s d(k, j)}}{\prod_{l=1}^J p_n(l) e^{s d(k, l)}} \prod_{j=1}^J p_n(j) e^{s d(k, j)} - 1 \\
& = 1 - 1 = 0
\end{aligned}$$

即

$$V(\mathbf{Q}_{n+1}) - V(\mathbf{Q}_n) = 0$$

等号只在满足条件

$$p_{n+1}(j) = p_n(j) \quad (6.76)$$

及

$$q_n(j|k) = \frac{\frac{p_n(j)}{J} e^{s d(k, j)}}{\prod_{l=1}^J p_n(l) e^{s d(k, l)}} \quad (6.77)$$

时才成立。而式(6.77)即定理 6.1 所述的式(6.39)。

由于  $V(\mathbf{Q}_n)$  随  $n$  非增, 且以  $R(D) - sD$  为界, 故  $n \rightarrow \infty$  时必有极限,  $q_n(j|k)$  和  $p_n(j)$  也必有极限, 分别设为  $q^*(j|k)$  和  $p^*(j)$ , 则此极限满足

$$q^*(j|k) = \frac{p^*(j) e^{s d(k, j)}}{\prod_{l=1}^J p^*(l) e^{s d(k, l)}} \quad (6.78)$$

$$p^*(j) = \prod_{k=1}^K p(k) q^*(j|k) = p^*(j) \prod_{k=1}^K \frac{p(k) e^{s d(k, j)}}{\prod_{l=1}^J p^*(l) e^{s d(k, l)}} \quad (6.79)$$

由于  $q^*(j|k)$  满足  $R(D)$  函数的充要条件, 故此时的  $D(\mathbf{Q}^*)$  即为  $D_s$ ,  $I(\mathbf{Q}^*)$  即为  $R(D_s)$ , 且有



$$V(\mathbf{Q}^*) = R(D_s) - sD_s \quad (6.80)$$

证毕

### 6.3.3 信息速率失真函数解的唯一性问题

在讨论离散无记忆信道的信道容量的解时我们已经指出, 达到信道容量的输入概率分布不是唯一的。类似地, 在求解信息速率失真函数时我们发现, 达到信息速率失真函数  $R(D)$  时的编码器转移概率及输出码字母的概率分布也不一定是唯一的。下述定理给出了该不唯一性的证明。

**定理 6.4** 设  $\mathbf{Q}$  和  $\mathbf{Q}^*$  均为信息速率失真函数  $R(D)$  的解, 则  $\mathbf{Q}$  也必为  $R(D)$  的解, 即

$$I(\mathbf{P}, \mathbf{Q}) = R(D)$$

其中  $0 < \alpha < 1$ , 且

$$q(j/k) = \alpha q_1(j/k) + (1 - \alpha) q_2(j/k) \quad (6.81)$$

并且此时对所有  $j, k$  均有下述关系式成立

$$\frac{q(j/k)}{p(j)} = \frac{\alpha q_1(j/k)}{p_1(j)} = \frac{q_2(j/k)}{p_2(j)} \quad (6.82)$$

**证明** 由于式(6.81)成立, 则有

$$\begin{aligned} D &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j/k) d(k, j) \\ &= \sum_{k=1}^K \sum_{j=1}^J p(k) \alpha q_1(j/k) d(k, j) + (1 - \alpha) \sum_{k=1}^K \sum_{j=1}^J p(k) q_2(j/k) d(k, j) \\ &= D_1 + (1 - \alpha) D_2 \end{aligned}$$

而  $D_1 = D_2 = D$ , 所以  $D = D$ , 于是有

$$I(\mathbf{P}, \mathbf{Q}) = R(D) \quad (6.83)$$

另一方面,  $I(\mathbf{P}, \mathbf{Q})$  是  $\mathbf{Q}$  的下凸函数, 则有

$$\begin{aligned} I(\mathbf{P}, \mathbf{Q}) &= \alpha I(\mathbf{P}, \mathbf{Q}_1) + (1 - \alpha) I(\mathbf{P}, \mathbf{Q}_2) \\ &= \alpha R(D) + (1 - \alpha) R(D) = R(D) \end{aligned} \quad (6.84)$$

综合式(6.83)和式(6.84), 即得

$$I(\mathbf{P}, \mathbf{Q}) = R(D)$$

对定理的第二部分, 有

$$\begin{aligned}
I(\mathbf{P}, \mathbf{Q}) &= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \log \frac{q(j|k)}{p(j)} \\
&= \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \cdot \log \frac{q(j|k)}{p_1(j)} \frac{q(j|k)}{p(j)} \frac{p_1(j)}{q(j|k)} + \\
&\quad (1 - \alpha) \sum_{k=1}^K \sum_{j=1}^J p(k) q(j|k) \cdot \log \frac{q(j|k)}{p_2(j)} \frac{q(j|k)}{p(j)} \frac{p_2(j)}{q(j|k)} \\
&= I(\mathbf{P}, \mathbf{Q}) - 1 + \sum_{j=1}^J \frac{p_1(j)}{p(j)} \sum_{k=1}^K p(k) q(j|k) + \\
&\quad (1 - \alpha) I(\mathbf{P}, \mathbf{Q}) - 1 + \sum_{j=1}^J \frac{p_2(j)}{p(j)} \sum_{k=1}^K p(k) q(j|k) \\
&= I(\mathbf{P}, \mathbf{Q}) + (1 - \alpha) I(\mathbf{P}, \mathbf{Q}) \quad (6.85)
\end{aligned}$$

其中, 等式仅当  $\ln x = x - 1$  中  $x = 1$  时才成立。而前面已证明等式是成立的, 故

$$\frac{q(j|k) p_1(j)}{p(j) q(j|k)} = \frac{q(j|k) p_2(j)}{p(j) q(j|k)} = 1$$

即式(6.82)成立。

证毕

由定理 6.4 可知, 若  $\mathbf{Q}$  时的输出分布为  $p_1(j)$ ,  $\mathbf{Q}$  时的输出分布为  $p_2(j)$ , 则  $\mathbf{Q}$  时的输出分布为

$$\begin{aligned}
p(j) &= \sum_{k=1}^K p(k) q(j|k) \\
&= \sum_{k=1}^K p(k) q(j|k) + (1 - \alpha) \sum_{k=1}^K p(k) q(j|k)
\end{aligned}$$

$$= p_1(j) + (1 - ) p_2(j) \quad (6.86)$$

这说明达到信息速率失真函数  $R(D)$  时的编码器转移概率及输出码字母的概率分布都可能不唯一。

### 6.3.4 乘积信源的信息速率失真函数

在实际信源中,有些信源每次发出的不是单个字母而是一个字母组。只要信源发出的各字母组之间是统计独立的,则该信源显然仍可以看成是离散无记忆信源,只是此时信源字母表中的字母现在实际上是一个字母组。但是,字母组中的各个字母之间的关系和取值有以下三种情况:

- 字母组中前后字母可能取自不同的字母表,且相互间统计不独立;
- 字母组中前后字母取自相同的字母表,且相互间统计独立;
- 字母组中前后字母取自不同的字母表,但相互间统计独立。

对于第一种情况,我们一般只能把字母组当作新的字母表来处理,然后计算  $R(D)$ 。第二种情况实际可以蜕化为单个字母生成的离散无记忆信源。而第三种情况我们称其为乘积信源。如果乘积信源的失真量度采用和失真量度,则该信源的信息速率失真函数  $R(D)$  有一种比较简单的计算方法。

我们以每次发出两个字母的乘积信源为例,说明乘积信源的信息速率失真函数的计算原理。设信源产生的字母组序列为  $\mathbf{u}, \mathbf{u}, \mathbf{u}, \dots, \mathbf{u}, \dots$ , 其中,  $\mathbf{u} = (u_{n_1}, u_{n_2}), (u_{n_1}, u_{n_2}) \in \{k_1, k_2\}, p(k_1, k_2) = p(k_1)p(k_2), k_1 = 1, 2, \dots, K_1, k_2 = 1, 2, \dots, K_2$ 。这样一个信源就可以看成是由字母  $\{k_1\}$ 、概率  $\{p(k_1)\}$  及字母  $\{k_2\}$ 、概率  $\{p(k_2)\}$  对应的两个离散无记忆信源的乘积信源。若此时乘积信源的失真量度是其组成信源的失真量度之和,即

$$d(k_1, k_2, j_1, j_2) = d_1(k_1, j_1) + d_2(k_2, j_2) \quad (6.87)$$

则此信源的信息速率失真函数  $R(D)$  与其组成信源的信息速率失真函数  $R_1(D_1)$ 、 $R_2(D_2)$  有下述定理所述的简单关系。

**定理 6.5** 设  $R_1(D_1(s))$  和  $R_2(D_2(s))$  是在相同  $s$  值下两个独立信源的信息速率失真函数值,则乘积信源的信息速率失真函数  $R(D(s))$  为

$$R(D(s)) = R_1(D_1(s)) + R_2(D_2(s)) \quad (6.88)$$

其中

$$D(s) = D_1(s) + D_2(s) \quad (6.89)$$

并且此时与  $R(D(s))$  对应的转移概率  $q^*(j_1, j_2 | k_1, k_2)$  即为分别与  $R_1(D_1(s))$

和  $R_2(D_2(s))$  对应的转移概率  $q_1^*(j_1 | k_1)$  和  $q_2^*(j_2 | k_2)$  的乘积, 即

$$\begin{aligned} q^*(j_1 j_2 | k_1 k_2) &= q_1^*(j_1 | k_1) q_2^*(j_2 | k_2) \\ k_1 &= 1, 2, \dots, K_1, \quad k_2 = 1, 2, \dots, K_2 \\ j_1 &= 1, 2, \dots, J_1, \quad j_2 = 1, 2, \dots, J_2 \end{aligned} \quad (6.90)$$

证明 由定理假设可以知道,  $q_1^*(j_1 | k_1)$  及  $q_2^*(j_2 | k_2)$  分别是  $R_1(D_1(s))$  和  $R_2(D_2(s))$  在斜率为  $s$  处的解, 所以只需证明满足式(6.90)的  $q^*(j_1 j_2 | k_1 k_2)$  满足  $R(D(s))$  解的充要条件即可。

为此, 将输出字母组的概率  $p(j_1 j_2)$  展开, 并代入式(6.90), 则有

$$\begin{aligned} p^*(j_1 j_2) &= \sum_{k_1=1}^{K_1} \sum_{k_2=1}^{K_2} p(k_1 k_2) q^*(j_1 j_2 | k_1 k_2) \\ &= \sum_{k_1=1}^{K_1} p(k_1) q_1^*(j_1 | k_1) \sum_{k_2=1}^{K_2} p(k_2) q_2^*(j_2 | k_2) \\ &= p^*(j_1) p^*(j_2) \end{aligned} \quad (6.91)$$

若  $q^*(j_1 j_2 | k_1 k_2)$  是  $R(D(s))$  的解, 则根据定理 6.1 所讲的信息速率失真函数解的充要条件及式(6.39)、(6.40)、(6.41)和(6.42), 应有

$$\begin{aligned} &\sum_{k_1=1}^{K_1} \sum_{k_2=1}^{K_2} p(k_1 k_2) \exp\{s[d_1(k_1, j_1) + d_2(k_2, j_2)]\} \\ &= 1, \quad \text{当 } p^*(j_1 j_2) > 0 \text{ 时} \\ &1, \quad \text{当 } p^*(j_1 j_2) = 0 \text{ 时} \end{aligned} \quad (6.92)$$

其中

$$p^*(j_1 j_2) = \sum_{k_1=1}^{K_1} \sum_{k_2=1}^{K_2} p(k_1 k_2) \exp\{s[d_1(k_1, j_1) + d_2(k_2, j_2)]\}^{-1} \quad (6.93)$$

由式(6.52)及式(6.91), 可得

$$p^*(j_1 j_2) = p^*(j_1) p^*(j_2) \quad (6.94)$$

因此, 式(6.92)变成

$$\begin{aligned} &\sum_{k_1=1}^{K_1} \sum_{k_2=1}^{K_2} p(k_1 k_2) \exp\{s[d_1(k_1, j_1) + d_2(k_2, j_2)]\} \\ &= \sum_{k_1=1}^{K_1} p(k_1) \exp[s d_1(k_1, j_1)] \sum_{k_2=1}^{K_2} p(k_2) \exp[s d_2(k_2, j_2)] \end{aligned} \quad (6.95)$$

而已知  $q_1^*(j_1 | k_1)$  和  $q_2^*(j_2 | k_2)$  分别是  $R_1(D_1(s))$  和  $R_2(D_2(s))$  的解, 故有

$$\prod_{k_1=1}^{K_1} p(k_1) \exp[s d_1(k_1, j_1)] = 1, \quad \text{当 } p^*(j_1) > 0 \text{ 时} \quad (6.96)$$

$$1, \quad \text{当 } p^*(j_1) = 0 \text{ 时}$$

$$\prod_{k_2=1}^{K_2} p(k_2) \exp[s d_2(k_2, j_2)] = 1, \quad \text{当 } p^*(j_2) > 0 \text{ 时} \quad (6.97)$$

$$1, \quad \text{当 } p^*(j_2) = 0 \text{ 时}$$

结合式(6.91), 即可以知道式(6.92)成立, 故由式(6.90)给出的  $q^*(j_1, j_2 | k_1, k_2)$  的确是  $R(D(s))$  的解, 所以式(6.88)和式(6.89)成立。证毕

上述定理不难推广到由  $N$  个相互统计独立的离散无记忆信源组成的乘积信源。但需指出的是上述推导中的失真按(6.87)式定义的, 即把字母组看成是乘积信源的新字母下定义得到的。所以定理中的信息速率和失真是指单位字母组的信息速率和失真。如仍以组成信源的字母为单位, 则上述信息速率和失真还需在  $N$  个组成信源的字母间平分, 即各乘以  $1/N$ 。

## 6.4 连续无记忆信源的信息速率失真函数

在讨论完离散无记忆信源以后, 我们现在转向连续无记忆信源的信息速率失真函数及其求解。

### 6.4.1 连续无记忆信源信息速率失真函数的定义及其解的充要条件

与离散无记忆信源相似, 连续无记忆信源  $U_t$  在  $t = 0, \pm 1, \pm 2, \dots$  等离散时刻所输出的信号  $\dots, u_{-2}, u_{-1}, u_0, u_1, u_2, \dots$  具有独立和相同的分布, 所不同的是  $u_n$  的取值是整个实数域, 此时, 熵压缩编码器的输出  $v_n$  也可以取实数域中的任意值。设我们用  $p(u)$  和  $p(v)$  分别表示编码器输入和输出的一维概率密度函数,  $q(v|u)$  表示一维转移概率密度函数。经过与离散无记忆信源相似的推理, 可以知道连续无记忆信源的信息速率失真函数可定义为

$$R(D) = \inf\{I(P, Q); E\{d(U, V)\} \leq D\} \quad (6.98)$$

其中

$$I(P, Q) = \int p(u) q(v|u) \log \frac{q(v|u)}{p(v)} du dv \quad (6.99)$$

$$E\{d(U, V)\} = \int p(u) q(v|u) d(u, v) du dv \quad (6.100)$$

此时的信息速率失真函数也是在  $D_{\min} < D < D_{\max}$  内的连续严格递减函数。与式

(6.9)和式(6.10)对应,  $D_{\min}$  和  $D_{\max}$  分别为

$$D_{\min} = \int_{-\infty}^{+\infty} p(u) \inf_v d(u, v) du \quad (6.101)$$

$$D_{\max} = \inf_v \int_{-\infty}^{+\infty} p(u) d(u, v) du \quad (6.102)$$

与离散无记忆信源时信息速率失真函数  $R(D)$  的严格递减性一样, 对连续无记忆信源而言, 定义式(6.98)中的小于等于号实际上可以用等号代替。

与离散无记忆信源不同的是, 连续无记忆信源的  $I(P, Q)$  是转移概率密度函数的泛函, 故式(6.98)要求对泛函式(6.99)取最小值, 约束条件为

$$q(v|u) \geq 0 \quad (6.103)$$

$$\int_{-\infty}^{+\infty} q(v|u) dv = 1 \quad (6.104)$$

$$\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} p(u) q(v|u) d(u, v) du dv = D \quad (6.105)$$

约束条件下的泛函求极值问题和约束条件下函数求极值问题类似, 即利用拉格朗日乘数将问题转化为无约束极值问题, 并用变分代替微分, 这样就可以得到连续无记忆信源下信息速率失真函数解的充要条件。

**定理 6.6** 在连续无记忆信源下, 编码器的转移概率密度函数能使互信息达到信息速率失真函数值  $R(D)$  的充要条件是

$$q(v|u) = \lambda(u) p(v) e^{s d(u, v)}, \quad (6.106)$$

$$\int_{-\infty}^{+\infty} \lambda(u) p(u) e^{s d(u, v)} du = 1, \quad \text{当 } p(v) > 0 \text{ 时} \quad (6.107a)$$

$$\int_{-\infty}^{+\infty} \lambda(u) p(u) e^{s d(u, v)} du < 1, \quad \text{当 } p(v) = 0 \text{ 时} \quad (6.107b)$$

其中

$$\lambda(u) = \left( \int_{-\infty}^{+\infty} p(v) e^{s d(u, v)} dv \right)^{-1} \quad (6.108)$$

同时, 对  $s \geq 0$ ,  $R(D)$  和  $D$  满足参量方程

$$D_s = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \lambda(u) p(v) p(u) e^{s d(u, v)} d(u, v) du dv \quad (6.109)$$

$$R(D_s) = s D_s + \int_{-\infty}^{+\infty} p(u) \log \lambda(u) du \quad (6.110)$$

证明略。

在定理 6.6 中, 参量  $s$  的物理意义也和离散无记忆信源一样, 有

$$R(D_s) = s \quad (6.111)$$

和离散无记忆信源时一样,连续无记忆信源的信息速率失真函数也有另一种表示形式,如定理 6.7 所述。

**定理 6.7** 连续无记忆信源的信息速率失真函数可以表示成

$$R(D) = \sup_{s \geq 0} \left[ sD + \int_{-\infty}^{+\infty} p(u) \log \left( \frac{1}{p(u)} \right) du \right] \quad (6.112)$$

其中

$$s = - \int_{-\infty}^{+\infty} (u) p(u) e^{s d(u, v)} du \quad 1 \quad (6.113)$$

$s$  和  $(u)$  能使上述上确界达到的充要条件是满足式(6.106)、(6.107)及(6.108)。

证明略。

需要说明的是,连续情况下的信息速率失真函数与离散情况下信息速率失真函数的一个主要差别在于  $D=0$  时,由于连续信源的  $H(U)=-\infty$  而使  $R(D)$  为  $-\infty$ 。从某种意义上讲,也正是由于此,连续信源的熵压缩编码是不可缺少的。

## 6.4.2 差值失真量度下连续无记忆信源信息速率失真函数的计算

和连续无记忆信源下信道容量的计算一样,连续无记忆信源下信息速率失真函数的计算一般也相当困难,在绝大多数情况下无解析解。但我们知道在加性噪声信道下信道容量的求解得到一定程度的简化,类似地在信息速率失真函数的求解中差值失真量度也可以使问题得到简化,且该失真量度具有很大的实用价值。

所谓差值失真量度是指失真的量度为编码器输入/输出之差的函数,即

$$d(u, v) = (u - v) \quad (6.114)$$

例如,  $d(u, v) = (u - v)^2$ ,  $d(u, v) = |u - v|$  等。

### 6.4.2.1 差值失真量度下信息速率失真函数的下界

由信息速率失真函数的表示式(6.112)和式(6.113),可以取

$$(u) = \frac{K}{p(u)} \quad (6.115)$$

则  $(u)$  的条件可以写成

$$K e^{s(u-v)} du = K e^{s(z)} dz \quad 1 \quad (6.116)$$

若  $(z)$  满足

$$e^{s(z)} dz < \infty \quad (6.117)$$

则可以取  $K$  满足

$$K = \frac{1}{\int e^{s(z)} dz} \quad (6.118)$$

即使式(6.116)成立, 此时由式(6.112), 可得

$$\begin{aligned} R(D) &= sD + \int p(u) \log(u) du \\ &= h(U) + sD - \int \log e^{s(z)} dz \end{aligned} \quad (6.119)$$

于是,  $R(D)$  的下界是  $D$  和  $s$  的函数, 记作

$$R_L(D, s) = h(U) + sD - \int \log e^{s(z)} dz \quad (6.120)$$

由于

$$\frac{R_L(D, s)}{s} = D - \int (u) g_s(u) du \quad (6.121)$$

$$\frac{\partial^2 R_L(D, s)}{\partial s^2} = - \int (u)^2 g_s(u) du + \left( \int (u) g_s(u) du \right)^2 \quad (6.122)$$

其中

$$g_s(u) = \frac{e^{s(z(u))}}{\int e^{s(z)} dz} \quad (6.123)$$

若把  $g_s(u)$  看成是一个概率密度函数, 则式(6.122)就相当于  $(u)$  相对于  $g_s(u)$  的方离差的负值, 可知该二次偏导数小于零, 故  $R_L(D, s)$  是  $s$  的上凸函数。因此,  $R_L(D, s)$  相对于变量  $s$  有唯一的最大值, 且在该极值点  $s$  处满足

$$\frac{\partial R_L(D, s)}{\partial s} = 0$$

即有

$$\int (u) g_s(u) du = D \quad (6.124)$$

所以在给定  $D$  时可以由该式解得  $s$ 。

另一方面, 有

$$-\frac{\partial}{\partial s} \int (u) g_s(u) du = - \frac{\partial^2 R_L(D, s)}{\partial s^2} > 0 \quad (6.125)$$

则  $\int (u) g_s(u) du$  随  $s$  单调非减, 故  $s$  与  $D$  值必一一对应, 此时的  $D$  即为式(6.109)中的  $D_s$ 。于是在极值点  $s$  时的下界为



$$\begin{aligned}
R_L(D_s, s) &= h(U) + sD_s - \int \log e^{s(z)} dz \\
&= h(U) + \int g_s(u) s(u) - \log e^{s(z)} dz du \\
&= h(U) + \int g_s(u) \log(g_s(u)) du \\
&= h(U) - h(g_s) \quad (6.126)
\end{aligned}$$

若不考虑  $R(D)$  的解  $\mathbf{Q}^*$  发生在边界处的情况, 则在上述  $s$  和  $D_s$  下, 只要  $(u)$  满足

$$\int (u) p(u) e^{s(u-v)} du = K e^{s(u-v)} du = 1 \quad (6.127)$$

及

$$(u) = \int p(v) e^{s(u-v)} dv^{-1} \quad (6.128)$$

时确有处处非负解  $p(v)$ , 即可以有

$$R_L(D_s, s) = R(D_s) \quad (6.129)$$

为求  $p(v)$  可将式 (6.128) 改写成

$$p(v) e^{s(u-v)} dv = \frac{1}{(u)} = \frac{p(u)}{K} \quad (6.130)$$

而由式 (6.127) 可以知道

$$K = \frac{1}{\int e^{s(u-v)} du} \quad (6.131)$$

则式 (6.130) 化为

$$p(u) = \frac{\int p(v) e^{s(u-v)} dv}{\int e^{s(u-v)} du} = \int p(v) g_s(u-v) dv \quad (6.132)$$

若由上式解得的  $p(v)$  处处非负, 则说明式 (6.127) 和式 (6.128) 成立, 此时的  $R_L(D_s, s)$  即为  $R(D_s)$ 。

求解式 (6.132) 比较容易。我们可以作 Fourier 变换, 得到

$$F_u(\omega) = F_g(\omega) \times F_v(\omega) \quad (6.133)$$

其中,  $F_u(\omega)$ ,  $F_g(\omega)$ ,  $F_v(\omega)$  分别为  $p(u)$ ,  $g_s(u)$ ,  $p(v)$  的 Fourier 变换。由此可以得到  $F_v(\omega)$ , 经过逆变换后即可以得到  $p(v)$ 。

#### 6.4.2.2 差方失真量度下的信息速率失真函数

所谓差方失真量度是指失真量度为差值的平方, 即有

$$d(u, v) = (u - v)^2 \quad (6.134)$$

于是有

$$g_s(u) = \frac{1}{2s} e^{-su^2} = -\frac{1}{2s} e^{-su^2} \quad (6.135)$$

$$D = \int_{-\infty}^{+\infty} (u) g_s(u) du = -\frac{1}{2s} \quad (6.136)$$

给定  $D$  时, 可以用  $D$  表示  $s$ , 则  $g_s(u)$  变为

$$g_s(u) = \frac{1}{2D} e^{-\frac{u^2}{2D}}$$

所以, 由式(6.126)差方失真量度下信息速率失真函数的下界为

$$\begin{aligned} R_L(D, s) &= h(U) - h(g_s) \\ &= h(U) - \frac{1}{2} \log(2\pi e D) \end{aligned} \quad (6.137)$$

若利用熵功率的概念, 设  $h(U)$  的熵功率为  $P_e$ , 则

$$h(U) = \frac{1}{2} \log(2\pi e P_e) \quad \text{或} \quad P_e = \frac{1}{2\pi e} e^{2h(U)} \quad (6.138)$$

故

$$R_L(D, s) = \frac{1}{2} \log \frac{P_e}{D} \quad (6.139)$$

若由式(6.132)或式(6.133)求得的  $p(v)$  处处非负, 则  $R_L(D, s)$  就等于  $R(D)$ 。

下面分两种情况讨论。

### (1) 高斯信源

设信源具有正态分布, 即

$$p(u) = \frac{1}{\sqrt{2\pi P_u}} \exp \left\{ -\frac{(u - m)^2}{2P_u} \right\} \quad (6.140)$$

对  $p(u)$  作 Fourier 变换, 可得

$$F_u(\omega) = \exp \left\{ -\frac{1}{2} P_u \omega^2 - jm\omega \right\} \quad (6.141)$$

而  $g_s(u)$  的 Fourier 变换为

$$F_{g_s}(\omega) = \int_{-\infty}^{+\infty} g_s(u) e^{-j\omega u} du = \exp \left\{ -\frac{1}{2} D \omega^2 \right\} \quad (6.142)$$

则有

$$F_v(\cdot) = \frac{F_u(\cdot)}{F_{g_s}(\cdot)} = \exp \left[ -\frac{1}{2} (P_u - D)^{-2} - jm \right] \quad (6.143)$$

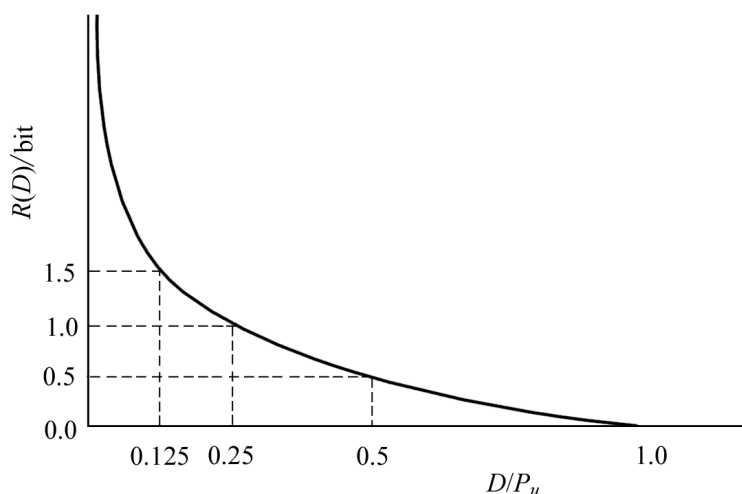
作 Fourier 逆变换, 即得

$$p(v) = \frac{1}{2(P_u - D)} \exp \left[ -\frac{(v - m)^2}{2(P_u - D)} \right] \quad (6.144)$$

显然,  $p(v)$  处处非负, 故有

$$R(D) = R_L(D, s) = \frac{1}{2} \log \frac{P_u}{D}, \quad 0 < D < P_u \quad (6.145)$$

无记忆高斯信源在差方失真量度下的信息速率失真函数的曲线如图 6.3 所示。



### 6.3 无记忆高斯信源在差方失真量度下的 $R(D)$

下面讨论一下此时编码器的转移概率密度函数  $q(v|u)$ 。

设  $m=0$ , 而  $u$  满足

$$\int_{-\infty}^{\infty} p(u) e^{s(u-v)^2} du = K \int_{-\infty}^{\infty} e^{s(u-v)^2} du = 1$$

则有

$$K = \frac{1}{\int_{-\infty}^{\infty} e^{s(u-v)^2} du} = \frac{1}{2\sqrt{D}} \quad (6.146)$$

故

$$q(v|u) = \frac{K}{p(u)} = \frac{1}{p(u) 2\sqrt{D}} \quad (6.147)$$

由充要条件定理 6.6 可以知道, 当  $p(v) > 0$  时有

$$\begin{aligned} q(v|u) &= \frac{1}{2\sqrt{D}} \frac{p(v)}{p(u)} e^{s(u-v)^2} = \frac{1}{2\sqrt{D}} \frac{p(v)}{p(u)} e^{s(u-v)^2} \\ &= \frac{1}{2\sqrt{D}} \frac{P_u}{P_u - D} \exp \left[ -\frac{v^2}{2(P_u - D)} + \frac{u^2}{2P_u} - \frac{(u-v)^2}{2D} \right] \quad (6.148) \end{aligned}$$

令  $\beta = 1 - D/P_u$ , 则有

$$q(v|u) = \frac{1}{2\beta D} \exp \left[ -\frac{(v-u)^2}{2\beta D} \right] \quad (6.149)$$

此即互信息达到  $R(D)$  时的编码器转移概率密度函数。

## (2) 一般信源

对一般信源, 若已知  $p(u)$  和  $g_s(u)$ , 原则上讲可以得到  $F_v(\cdot)$ , 从而求出  $p(v)$ ,  $q(v|u)$  和  $R(D)$ 。下述定理将给出一般的无记忆连续信源在差方失真量度下的信息速率失真函数的一个实用的上界。

**定理 6.8** 设无记忆连续信源的概率密度函数  $p(u)$  满足条件

$$u p(u) du = 0 \quad (6.150)$$

$$\int u^2 p(u) du = P_u \quad (6.151)$$

则在差方失真量度下, 此信源的信息速率失真函数  $R(D)$  满足条件

$$R(D) \leq \frac{1}{2} \log \frac{P_u}{D}, \quad 0 < D < P_u \quad (6.152)$$

当且仅当  $p(u) = \frac{1}{2\sqrt{P_u}} \exp \left[ -\frac{u^2}{2P_u} \right]$  时上式才取等号。

**证明** 在  $0 < D < P_u$  时, 令

$$q(v|u) = \frac{1}{2\beta D} \exp \left[ -\frac{(v-u)^2}{2\beta D} \right]$$

其中  $\beta = 1 - D/P_u$ , 则此时相应的平均失真为

$$\begin{aligned} D(Q) &= \int p(u) q(v|u) d(u, v) dv du \\ &= \int p(u) q(v|u) [v - u - (1 - \beta)u]^2 dv du \\ &= \int p(u) \left[ D + \frac{D}{P_u} u^2 \right] du = D + \frac{D}{P_u} P_u = D \end{aligned} \quad (6.153)$$

在此转移概率密度函数下的互信息  $I(P, Q)$  应满足

$$I(P, Q) = R(D) \quad (6.154)$$

另一方面

$$I(P, Q) = \int p(u) q(v|u) \log \frac{q(v|u)}{p(v)} du dv$$

$$\begin{aligned}
&= - \int p(v) \log p(v) dv + \int p(u) q(v/u) \log q(v/u) du dv \\
&= h(V) + \int p(u) q(v/u) \left[ -\frac{(v-u)^2}{2D} - \frac{1}{2} \log(2D) \right] du dv \\
&= h(V) - \frac{1}{2} - \frac{1}{2} \log(2D) \\
&= h(V) - \frac{1}{2} \log(2eD) \tag{6.155}
\end{aligned}$$

所以有

$$R(D) - I(P, Q) = h(V) - \frac{1}{2} \log(2eD) \tag{6.156}$$

现对  $h(V)$  作如下估计:

$$\begin{aligned}
\int v p(v) dv &= \int \int v p(u) q(v/u) du dv \\
&= \int p(u) \int v q(v/u) dv du \\
&= \int p(u) u du = 0 \tag{6.157}
\end{aligned}$$

$$\begin{aligned}
\int v^2 p(v) dv &= \int \int v^2 p(u) q(v/u) dv du \\
&= \int p(u) (D + u^2) du \\
&= D + P_u = P_u - D \tag{6.158}
\end{aligned}$$

由于等功率下高斯信源具有最大微分熵, 则有

$$h(V) = \frac{1}{2} \log[2e(P_u - D)] \tag{6.159}$$

代入式(6.156)中, 则得

$$R(D) - \frac{1}{2} \log \frac{P_u - D}{D} = \frac{1}{2} \log \frac{P_u}{D} \tag{6.160}$$

且当信源为高斯信源时上式取等号。又因式(6.159)仅在高斯信源时取等号, 故当且仅当高斯信源时上式才取等号。证毕

综合在差方失真量度下连续无记忆信源的信息速率失真函数的上、下界, 可知

$$\frac{1}{2} \log \frac{P_e}{D} \leq R(D) \leq \frac{1}{2} \log \frac{P_u}{D} \tag{6.161}$$

表 6.1 给出了几种主要分布的信源的信息速率失真函数的上下界之差。

表 6.1 四种主要分布的信源的信息速率失真函数上下界之差 (e=2. 7182, C=0. 5772)

分布	$p(u)$	$h(U)$	上下界之差(比特)
高斯分布	$\frac{1}{\sqrt{2\pi}P_u}\exp\left(-\frac{u^2}{2P_u}\right)$	$\frac{1}{2}\log_2(2\pi eP_u)$	0
均匀分布	$\frac{1}{2\sqrt{3}P_u},  u \leq\sqrt{3}P_u$ 0, 其他	$\frac{1}{2}\log_2(12P_u)$	0. 255
拉普拉斯分布	$\frac{1}{\sqrt{2}P_u}\exp\left(-\frac{\sqrt{2} u }{P_u}\right)$	$\frac{1}{2}\log_2(2e^2P_u)$	0. 104
伽玛分布	$\frac{4}{3\sqrt{\pi}P_u}\exp\left(-\frac{3 u }{2P_u}\right)$	$\frac{1}{2}\log_2\left(\frac{4}{3}e^{1-C}P_u\right)$	0. 709

实际的信息速率失真函数,在  $R \rightarrow 0$  时与上界接近,在  $D \rightarrow 0$  时与下界接近。图 6. 4 给出了伽玛分布下的  $R(D)$  曲线及其上、下界曲线。

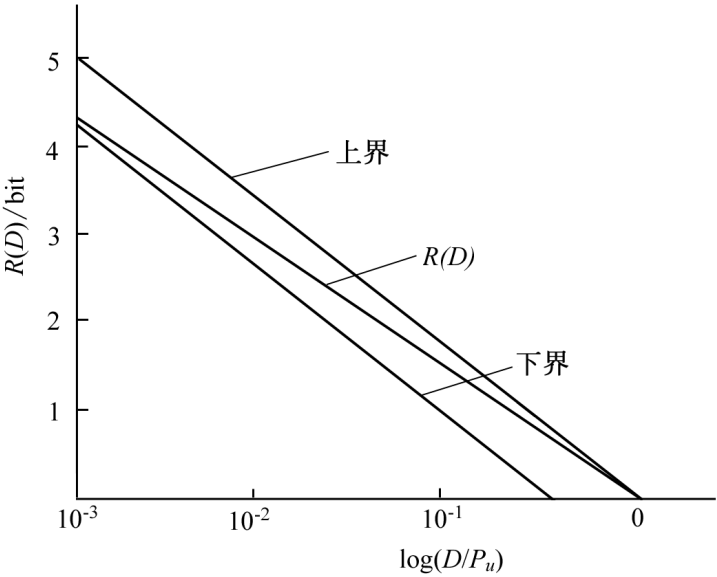


图 6.4 伽玛分布的  $R(D)$  及其上下界

6.5 标量量化

对连续无记忆信源进行熵压缩编码的常用方法是标量量化。设标量量化器有  $K$  个输出电平  $\{q_1, q_2, \dots, q_K\}$ , 它可以把取任意实数值的信源输出  $u$  逐个地

映射成  $K$  个可能离散值中的一个。该映射是借助  $K+1$  个门限电平  $- \infty = T_0 < T_1 < T_2 < \dots < T_{K-1} < T_K = +\infty$  (或者说  $K-1$  个门限电平), 按照下式完成的:

$$q(u) = \begin{cases} q_1, & u < T_1 \\ q_k, & T_{k-1} < u < T_k, k = 2, 3, \dots, K-1 \\ q_K, & u > T_{K-1} \end{cases} \quad (6.162)$$

当标量量化器的输入信号为  $(u_1, u_2, \dots, u_N)$ , 其中  $u_n \in (-\infty, +\infty)$  时, 量化器的输出就有  $K^N$  种可能, 记为  $(v_1, v_2, \dots, v_N)$ , 其中  $v_n \in \{q_1, q_2, \dots, q_K\}$ 。每一电平  $q_k$  的出现概率为

$$p(q_k) = \int_{T_{k-1}}^{T_k} p(u) du \quad (6.163)$$

由于此映射为多对一映射, 所以通过该量化器传输的信息速率  $R_K$  为

$$\begin{aligned} R_K &= \frac{1}{N} I(U^N; V^N) = I(U; V) \\ &= H(V) - H(V|U) \\ &= H(V) = - \sum_{k=1}^K p(q_k) \log p(q_k) \end{aligned} \quad (6.164)$$

而量化带来的平均失真为  $D_K$

$$\begin{aligned} D_K &= E \left[ \frac{1}{N} \sum_{n=1}^N d(U_n, V_n) \right] \\ &= \frac{1}{N} \sum_{n=1}^N E\{d(U_n, V_n)\} \\ &= E\{d(U, V)\} \\ &= \sum_{k=1}^K \int_{T_{k-1}}^{T_k} d(u, q_k) p(u) du \end{aligned} \quad (6.165)$$

一般来讲, 标量量化器输出电平的概率分布不一定是均匀分布的。量化器输出的可能最大比特速率为  $M_K$ , 即

$$M_K = \log_2 K \quad (6.166)$$

信息传输速率  $R_K$ 、平均失真  $D_K$  和二元符号速率  $M_K$  是标量量化器的三个主要性能指标, 选择不同的  $\{T_k\}$  和  $\{q_k\}$ , 量化器将有不同的  $R_K$ ,  $D_K$  和  $M_K$ 。

### 6.5.1 均匀量化

均匀量化是标量量化器中最简单的一种,此时量化间隔相等,  $q_k$  取量化间隔的中点。我们定义,若在给定量化电平数  $K$  的条件下,使平均失真  $D_K$  达到最小的均匀量化器称为最优均匀量化器。对高斯信源, T. J. Jr. Goblick 和 J. L. Holsinger 得到的最优均匀量化器的  $R_K$ ,  $D_K$  和  $M_K$  的关系大致为

$$R_K(D_K) = \frac{1}{4} + \frac{1}{2} \log \frac{P_u}{D_K} \quad \text{bit/字母} \quad (6.167)$$

$$M_K(D_K) = 0.125 + 0.6 \log \frac{P_u}{D_K} \quad \text{bit/字母} \quad (6.168)$$

需要指出的是,在给定输出电平数  $K$  的条件下,均匀量化所达到的平均失真并不是所有标量量化中最小的。

### 6.5.2 Lloyd-Max 算法

S. P. Lloyd 和 J. Max 曾经指出,为使标量量化器的平均失真  $D_K$  最小,  $\{T_k\}$  和  $\{q_k\}$  应分别满足以下两个条件

$$(T_{k-1} - q_{k-1})^2 = (q_k - T_{k-1})^2, \text{即 } T_{k-1} = \frac{1}{2}(q_{k-1} + q_k) \quad (6.169)$$

$$\frac{D_K}{q_k} = 0, \quad k = 1, 2, \dots, K \quad (6.170)$$

在差方失真量度下,有  $d(u, v) = (u - v)^2$ , 此时第二个条件式(6.170)可以化为

$$\frac{D_K}{q_k} = \frac{1}{q_k} \int_{T_{k-1}}^{T_k} p(u)(u - q_k)^2 du = 0$$

$$\int_{T_{k-1}}^{T_k} (u - q_k) p(u) du = 0 \quad (6.171)$$

按照这两个必要条件式(6.169)和式(6.171),反复对  $\{T_k\}$  和  $\{q_k\}$  进行迭代,就可以得到给定  $K$  下使  $D_K$  最小的  $\{T_k\}$  和  $\{q_k\}$ , 此即 Lloyd-Max 算法。

表 6.2 给出了高斯信源在不同电平数  $K$  值下的最优均匀量化和 Lloyd-Max 算法得到的平均失真。可以看出,随着电平数  $K$  的增加, Lloyd-Max 算法的改善表现得更加明显。



表 6.2 高斯信源在不同量化算法下的相对平均失真

输出电平数	1	4	8	16	24	32
最优均匀量化	1	0.1188	0.03744	0.01154	0.005747	0.003490
Lloyd-Max 算法	1	0.1175	0.03454	0.009497	0.004367	0.002499

从表 6.2 可以看出,标量量化对无记忆高斯连续信源而言是一种相当有效的熵压缩编码方法。在最优均匀量化中,此时的信息速率式(6.167)与理想值仅差  $1/4 \text{ bit/字母}$ ,已很接近极限值。当然,对其他分布不均的信源,如拉普拉斯信源、伽玛信源,这一差距会更大些。

## 6.6 有记忆连续信源与模拟信源的信息速率失真函数

迄今为止我们只讨论了无记忆连续信源的熵压缩编码,下面我们转到有更大实用价值的有记忆连续信源与模拟信源的熵压缩编码上来。有记忆连续信源与模拟信源的熵压缩编码与有记忆离散信源的冗余度压缩编码虽然都要利用记忆所带来的冗余度,但两者在有无失真量度这一点上是完全不一样的。与无记忆连续信源相比,有记忆连续信源与模拟信源的信息速率失真函数将更难计算,但是在某些特例下,我们仍可以得到一些有重大实用价值的结果。

### 6.6.1 有记忆连续信源的信息速率失真函数的定义

设  $U_t$  是有记忆连续信源,其输出  $(\dots, u_{-2}, u_{-1}, u_0, u_1, u_2, \dots)$  中各时刻的输出间存在统计依存关系,且  $u_n$  的值取自整个实数域。设信源输出序列被分组构成信源字  $\mathbf{u} = (u_1, u_2, \dots, u_N)$ , 编码器输出为码字  $\mathbf{v} = (v_1, v_2, \dots, v_N)$ , 则有记忆连续信源的信息速率失真函数  $R(D)$  可以定义为

$$R(D) = \lim_N \frac{1}{N} R_N(D) \quad (6.172)$$

其中

$$R_N(D) = \inf \{ I(U^N; V^N); E\{d(\mathbf{U}, \mathbf{V})\} \leq D \} \quad (6.173)$$

$$I(U^N; V^N) = - \int p(\mathbf{u}) q(\mathbf{v} | \mathbf{u}) \log \frac{q(\mathbf{v} | \mathbf{u})}{p(\mathbf{v})} d\mathbf{u} d\mathbf{v} \quad (6.174)$$

$$E\{d(\mathbf{U}, \mathbf{V})\} = \int p(\mathbf{u}) q(\mathbf{v} | \mathbf{u}) d(\mathbf{u}, \mathbf{v}) d\mathbf{u} d\mathbf{v} \quad (6.175)$$

$$d(\mathbf{u}, \mathbf{v}) = \frac{1}{N} \sum_{n=1}^N d(u_n, v_n) \quad (6.176)$$

可以证明,对于稳恒的有记忆连续信源,式(6.172)的极限一定存在。

### 6.6.2 模拟信源的信息速率失真函数的定义

对于模拟信源  $U(t)$ , 其输出  $u(t)$  是时间  $t$  的连续函数, 且函数也在实数域中连续取值。根据第4章的讨论, 若  $u(t)$  在  $0 < t \leq T$  内是  $L^2(T)$  函数, 则总可以在某种归一化正交函数族的基础上对  $u(t)$  进行展开, 并利用展开后的系数所组成的系数矢量来代替  $u(t)$ 。同样, 对编码器的输出信号  $v(t)$  ( $0 < t \leq T$ ) 也可以作相同的处理。

设  $\mathbf{x}$  和  $\mathbf{y}$  分别是  $0 < t \leq T$  期间  $u(t)$  和  $v(t)$  展开后的前  $N$  位系数所组成的系数矢量, 则模拟信源的信息速率失真函数  $R(D)$  可定义为

$$R(D) = \lim_T \frac{1}{T} R_T(D) \quad (6.177)$$

其中

$$R_T(D) = \inf \{ I_T(U(t); V(t)); E\{d_T(U(t), V(t))\} \leq D \} \quad (6.178)$$

$$I_T(U(t); V(t)) = \lim_N I(\mathbf{X}; \mathbf{Y}) \quad (6.179)$$

$$I(\mathbf{X}; \mathbf{Y}) = \sum_{\mathbf{x}} \sum_{\mathbf{y}} p(\mathbf{x}) q(\mathbf{y} | \mathbf{x}) \log \frac{q(\mathbf{y} | \mathbf{x})}{p(\mathbf{y})} d\mathbf{x} d\mathbf{y} \quad (6.180)$$

$$E\{d_T(U(t), V(t))\} = E \int_0^T d(u(t), v(t)) dt \quad (6.181)$$

可以证明,对于稳恒的模拟信源,式(6.177)的极限一定存在。

对模拟信源的信息速率失真函数的严格讨论将涉及很多数学问题, 其中大部分不是工程应用所感兴趣的, 所以我们不再作一般的讨论。

### 6.6.3 高斯有记忆连续信源的信息速率失真函数

高斯有记忆连续信源是指信源的输出序列中任意  $N$  个字母组成的矢量  $\mathbf{u}$  都满足高斯概率分布密度, 即

$$p(\mathbf{u}) = (2\pi)^{-N/2} / |\mathbf{N}|^{-1/2} \exp \left\{ -\frac{1}{2} (\mathbf{u} - \mathbf{m})^T \mathbf{N}^{-1} (\mathbf{u} - \mathbf{m}) \right\} \quad (6.182)$$

其中,  $\mathbf{m}^T = \{E\{U_1\}, E\{U_2\}, \dots, E\{U_N\}\}$ ,  $\mathbf{N} = (n_{kj})_{N \times N}$  为协方差矩阵, 而

$$k_{kj} = E\{U_k U_j\} - E\{U_k\}E\{U_j\}, \quad k, j = 1, 2, \dots, N \quad (6.183)$$

当  $\mathbf{m}^T = (0, 0, \dots, 0)$  时, 有

$$k_{kj} = E\{U_k U_j\}, \quad k, j = 1, 2, \dots, N \quad (6.184)$$

此时  $\mathbf{K}_N$  即为相关矩阵。相关矩阵具有 Toeplitz 矩阵的性质, 即它是对称的, 且沿着任一对角线的所有元素都相等。

下面将讨论差方失真量度下高斯有记忆连续信源的信息速率失真函数。

首先, 对信源字和编码器输出的码字作坐标变换, 取

$$\mathbf{X} = \mathbf{U} \quad (6.185)$$

$$\mathbf{Y} = \mathbf{V} \quad (6.186)$$

其中  $\mathbf{V}$  是由  $\mathbf{U}$  的归一化特征矢量组成的矩阵。由于  $\mathbf{K}_N$  为对称矩阵, 则满足

$$\mathbf{K}_N^{-1} = \mathbf{K}_N^T \quad (6.187)$$

$$\mathbf{K}_N^T = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_N) \quad (6.188)$$

其中主对角线上的元素  $\lambda_1, \lambda_2, \dots, \lambda_N$  是  $\mathbf{K}_N$  的特征值。

经过变换后, 信源字  $\mathbf{x}$  的协方差矩阵为

$$\begin{aligned} \mathbf{K}_N &= E\{\{\mathbf{X} - E\{\mathbf{X}\}\}\{\mathbf{X} - E\{\mathbf{X}\}\}^T\} \\ &= \mathbf{K}_N^T \\ &= \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_N) \end{aligned} \quad (6.189)$$

故有

$$p(\mathbf{x}) = \prod_{n=1}^N \frac{1}{\sqrt{2\pi\lambda_n}} \exp\left(-\frac{x_n^2}{2\lambda_n}\right) \quad (6.190)$$

这说明  $\mathbf{x}$  的各个分量统计独立。同时, 根据此变换的正交归一化性质, 可得

$$d(\mathbf{u}, \mathbf{v}) = d(\mathbf{x}, \mathbf{y}) = \frac{1}{N} \sum_{n=1}^N d(x_n, y_n) \quad (6.191)$$

又此变换是可逆的, 故有

$$I(U^N; V^N) = I(X^N; Y^N) \quad (6.192)$$

于是求解  $R_N(D)$  的问题就可以在新的坐标系中进行。

其次, 在新的坐标系中, 该信源相当于组成信源为高斯连续信源的乘积信源, 于是有记忆高斯连续信源的信息速率失真函数为

$$R_N(D(s)) = \frac{1}{N} \sum_{n=1}^N r_n(D_n(s)) \quad (6.193)$$

其中

$$D(s) = \frac{1}{N} \sum_{n=1}^N D_n(s) \quad (6.194)$$

而  $r_n(D_n(s))$  是各组成信源的信息速率失真函数,  $D_n(s)$  是此函数在斜率为  $s$  处所对应的平均失真。由节 6.4.2.2 的结果可以知道

$$r_n(D_n(s)) = \begin{cases} \frac{1}{2} \log \frac{n}{D_n(s)}, & D_n(s) \leq n \\ 0, & D_n(s) > n \end{cases} \quad (6.195)$$

$r_n(D_n(s))$  的斜率为

$$s = \begin{cases} -\frac{1}{2D_n(s)}, & 0 < D_n(s) \leq n \\ 0, & D_n(s) > n \end{cases} \quad (6.196)$$

则有

$$D_n(s) = \begin{cases} -\frac{1}{2s}, & -\frac{1}{2s} \leq n \\ n, & -\frac{1}{2s} > n \end{cases} \quad (6.197)$$

于是得到

$$R_N(D(s)) = \frac{1}{N} \sum_{n=1}^N \max \left( 0, \frac{1}{2} \log \left( -\frac{1}{2s} - n \right) \right) \quad (6.198)$$

$$D(s) = \frac{1}{N} \sum_{n=1}^N \min \left( -\frac{1}{2s}, n \right) \quad (6.199)$$

当  $-\frac{1}{2s} = \min_n n$  时, 有

$$D(s) = -\frac{1}{2s} \quad (6.200)$$

$$\begin{aligned} R_N(D(s)) &= \frac{1}{N} \sum_{n=1}^N \frac{1}{2} \log \frac{n}{D(s)} = \frac{1}{2N} \sum_{n=1}^N \log \frac{n}{D(s)} \\ &= \frac{1}{2N} \log \prod_{n=1}^N \frac{n}{D(s)} \\ &= \frac{1}{2} \log \frac{N!}{D(s)^N} \end{aligned} \quad (6.201)$$

当  $-\frac{1}{2s} = \max_n n$  时, 有

$$D(s) = \frac{1}{N} \sum_{n=1}^N n \quad (6.202)$$

$$R_N(D(s)) = 0 \quad (6.203)$$

最后, 利用下述关于 Toeplitz 矩阵的 Toeplitz 分布定理, 求  $N \rightarrow \infty$  时  $R_N(D)$  的极限  $R(D)$ 。

**定理 6.9** (Toeplitz 分布定理) 设  $T_N$  是一个无限 Toeplitz 矩阵,  $t_{nn}$  是其第  $n$  对角线上的元素, 且  $\{t_{nn}\}$  的谱  $\Phi(\omega)$  为

$$\Phi(\omega) = \sum_{n=-\infty}^{+\infty} t_{nn} e^{-jn\omega} \quad (6.204)$$

若  $\Phi(\omega)$  有界, 则对任意连续函数  $G(\cdot)$  均有

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N G\left(\frac{\lambda_n}{N}\right) = \frac{1}{2\pi} \int_{-\pi}^{+\pi} G(\Phi(\omega)) d\omega \quad (6.205)$$

其中  $\lambda_n$  是以  $T_N$  主对角线为中心的  $N$  阶矩阵  $T_N$  的特征值。

证明略。

利用上述定理, 由式(6.198)和式(6.199)可以得到谱密度函数为  $\Phi(\omega)$  的高斯有记忆连续信源的率失真函数为

$$R(D) = \frac{1}{4\pi} \int_{-\pi}^{+\pi} \max\{0, \log(\Phi(\omega) - 2s)\} d\omega \quad (6.206)$$

$$D(s) = \frac{1}{2\pi} \int_{-\pi}^{+\pi} \min\left\{\Phi(\omega), \frac{1}{2s}\right\} d\omega \quad (6.207)$$

白色高斯信号可以看成是高斯有记忆信源的特例, 此时谱密度为常数, 设

$\Phi(\omega) = \sigma^2$ , 则由式(6.207)可得  $D(s) = \frac{\sigma^2}{2s}$  当  $0 < \frac{\sigma^2}{2s} < \sigma^2$ , 由式(6.206)可得

$R(D) = \frac{1}{2} \log \frac{\sigma^2}{D}$ , 此结果与式(6.145)完全一致。

#### 6.6.4 高斯模拟信源的信息速率失真函数

本节给出高斯模拟信源在差方失真量度下的信息速率失真函数  $R(D)$  的一个不严格的分析。设  $U(t)$  是一个零期望值的稳恒高斯模拟信源。若对该信源的输出  $u(t)$  在  $t = nh$  时刻进行采样, 并对采样值加权, 将得到一个时间离散、幅值连续的有记忆高斯序列  $x_n$  为

$$x_n = hu(nh), \quad n = 0, \pm 1, \pm 2, \dots \quad (6.208)$$

若记模拟信源的相关函数为  $\rho(\tau)$

$$\rho(\tau) = E\{U(t)U(t+\tau)\} \quad (6.209)$$

则新序列  $\{x_n\}$  的相关矩阵  $R_h$  的元素  $r_m$  为

$$\begin{aligned} r_m &= E\{X_n X_{n+m}\} \\ &= hE\{U(nh)U((n+m)h)\} \\ &= h r(mh) \end{aligned} \quad (6.210)$$

对编码器的输出  $v(t)$  作类似的处理, 可得

$$y_n = hv(nh), \quad n = 0, \pm 1, \pm 2, \dots \quad (6.211)$$

根据式 (6.206) 和式 (6.207), 可得采样后得到的有记忆高斯连续信源的  $R(D)$  和  $D(s)$  分别为

$$R(D) = \frac{1}{4} \max_{-1}^{+1} [0, \log(-2s - h)] \quad (6.212)$$

$$D(s) = \frac{1}{2} \min_{-1}^{+1} [-\frac{1}{2s}, h] \quad (6.213)$$

其中

$$h(\cdot) = \sum_{m=-\infty}^{+\infty} r_m e^{-jm} = \sum_{m=-\infty}^{+\infty} h(mh) e^{-jmh} \quad (6.214)$$

此时所得  $R(D)$  和  $D(s)$  的单位分别为每采样的互信息和每采样的失真。若改用每秒互信息和每秒平均失真来衡量, 则必须用

$$= \frac{1}{h}$$

代替变量  $s$ , 于是分别得到

$$R(D) = \frac{1}{4} \max_{-1/h}^{+1/h} [0, \log(-2s - h)] \quad (6.215)$$

$$D(s) = \frac{1}{2} \min_{-1/h}^{+1/h} [-\frac{1}{2s}, h] \quad (6.216)$$

令  $h \rightarrow 0$ , 得

$$\begin{aligned} \lim_{h \rightarrow 0} h(h) &= \lim_{h \rightarrow 0} \sum_{m=-\infty}^{+\infty} h(mh) e^{-jmh} \\ &= \sum_{-\infty}^{+\infty} ( ) e^{-j\omega} d = ( ) \end{aligned} \quad (6.217)$$

其中,  $( )$  是高斯信源  $U(t)$  的功率谱密度。利用此关系, 即可得到稳恒高斯信源的信息速率失真函数

$$R(D) = \frac{1}{4} \max_{-1}^{+1} [0, \log(-2s - ( ))] \quad (6.218)$$

$$D(s) = \frac{1}{2} \min \left( \frac{1}{s}, \frac{1}{2s} \right) \quad (6.219)$$

例 6.1 计算限带高斯信源的  $R(D)$ 。

设该信源的平均功率为  $P_u$ , 功率谱密度为常数, 即

$$S(f) = \begin{cases} \frac{P_u}{2B}, & |f| \leq B \\ 0, & |f| > B \end{cases} \quad (6.220)$$

代入式(6.218)和式(6.219)则分别得

$$D(s) = \frac{1}{2s} \quad (6.221)$$

$$R(D) = \frac{1}{2} \log \frac{P_u}{D} \quad (6.222)$$

消去  $s$ , 并令  $F_0 = \frac{1}{2}$ , 即得

$$R(D) = \frac{1}{2} \log \frac{P_u}{D} = F_0 \log \frac{P_u}{D}, \quad 0 < D \leq P_u \quad (6.223)$$

当然, 对一般的限带稳恒信源, 是无法得到  $R(D)$  的解析表示形式的。但是, 仿照无记忆连续信源, 可以得到一般限带稳恒模拟信源的信息速率失真函数的上下界为

$$F_0 \log \frac{P_e}{D} \leq R(D) \leq F_0 \log \frac{P_u}{D} \quad (6.224)$$

其中  $P_e$  是限带稳恒模拟信源的熵功率。注意, 此时  $P_e$ ,  $P_u$  和  $D$  的单位均是每秒下而非单位字母或单位采样下的功率或失真。

## 6.7 变换编码——实用的熵压缩分组编码

本节讨论一种实用的熵压缩分组编码——变换编码, 它在语音、图像等信源的压缩编码中都有相当重要的应用。变换编码的具体组成图如图 6.5 所示, 图中输入的信源字母序列首先被分成长为  $N$  的字母组, 构成信源字或矢量  $\mathbf{u}$ ;  $\mathbf{u}$  经变换(一般为线性变换)后生成矢量  $\mathbf{x} = \mathbf{A}\mathbf{u}$ , 其中,  $\mathbf{A}$  为非奇异的去相关矩阵; 于是  $\mathbf{x}$  的各个分量不相关, 并分别用相同的量化方法进行标量量化; 标量量化的输出组成码字或量化矢量  $\mathbf{v}$ ;  $\mathbf{v}$  在接收端一般经逆变换得到输出  $\mathbf{y} = \mathbf{B}\mathbf{v}$ , 其中,  $\mathbf{B}$  也是非奇异矩阵。

从变换编码的这一组成特点可以看出与理论上的熵压缩分组编码相比,变换编码多了两个附加限制:

- 变换限制为线性变换;
- 量化是对各分量独立进行。

这种限制自然会影响编码器的性能,但是从具体实现来讲是简单而又方便的。

在图 6.5 的组成图中我们并没有确定矩阵  $\mathbf{A}$ ,  $\mathbf{B}$  的性质以及量化方法和量化所用的总比特数,显然它们将决定变换编码的性能。为使具体的计算简化,让我们假定信源矢量序列在足够的分组长度下统计独立,具有零数学期望和相同的统计分布,但矢量中各分量之间有统计依存关系,于是变换编码导致的最后输出处的平均失真为

$$\begin{aligned}
 D &= E \sum_{n=1}^N d(U_n, Y_n) = E \sum_{n=1}^N (U_n - Y_n)^2 \\
 &= E\{(\mathbf{U} - \mathbf{Y})^T (\mathbf{U} - \mathbf{Y})\} \\
 &= E \operatorname{tr} (\mathbf{A}^{-1} \mathbf{X} - \mathbf{B}\mathbf{V})(\mathbf{A}^{-1} \mathbf{X} - \mathbf{B}\mathbf{V})^T \quad (6.225)
 \end{aligned}$$

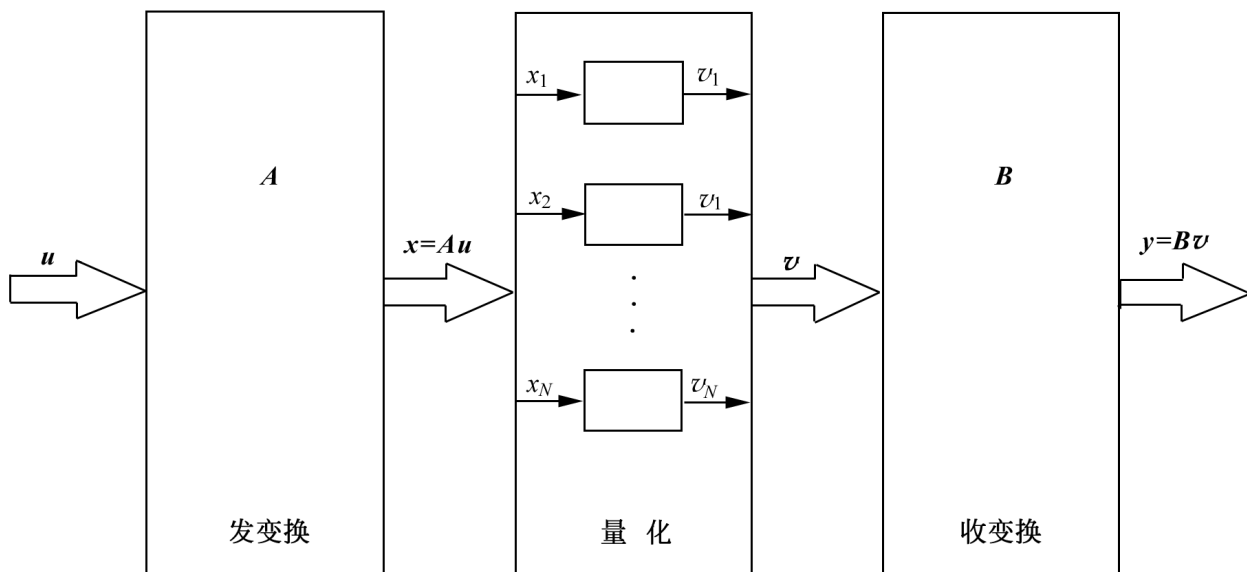


图 6.5 变换编码组成图

在给定总的量化比特数下能使上述平均失真  $D$  取最小的变换编码称为最优变换编码。最优变换编码下矩阵  $\mathbf{A}$ ,  $\mathbf{B}$  及量化器的特点是我们关心的问题,下面我们分别加以讨论。

**性质 6.5** 设发变换矩阵为  $\mathbf{A}$ , 则最优的收变换矩阵为

$$\mathbf{B} = \mathbf{A}^{-1} \quad (6.226)$$

其中



$$= \{E\{\mathbf{XV}^T\}\}\{E\{\mathbf{VV}^T\}\}^{-1} \quad (6.227)$$

证明 设  $D$  的表示式如式(6.225), 则展开后为

$$D = \text{tr}\{\mathbf{A}^{-1} E\{\mathbf{XX}^T\}(\mathbf{A}^{-1})^T\} + \text{tr}\{\mathbf{BE}\{\mathbf{VV}^T\}\mathbf{B}^T\} - 2\text{tr}\{\mathbf{BE}\{\mathbf{VX}^T\}(\mathbf{A}^{-1})^T\}$$

故有

$$\begin{aligned} -\frac{D}{\mathbf{B}} &= \mathbf{BE}\{\mathbf{VV}^T\} + \mathbf{BE}\{\mathbf{VV}^T\}^T - 2\{E\{\mathbf{VX}^T\}(\mathbf{A}^{-1})^T\}^T \\ &= \mathbf{BE}\{\mathbf{VV}^T\} + \mathbf{BE}\{\mathbf{VV}^T\} - 2\mathbf{A}^{-1} E\{\mathbf{XV}^T\} \end{aligned}$$

为得到  $D$  的最小值, 令

$$-\frac{D}{\mathbf{B}} = \mathbf{0}$$

即得

$$\mathbf{B} = \mathbf{A}^{-1} E\{\mathbf{XV}^T\}\{E\{\mathbf{VV}^T\}\}^{-1} = \mathbf{A}^{-1} \quad \text{证毕}$$

性质 6.6 变换编码的最优发变换去相关矩阵  $\mathbf{A}$  是以  $\mathbf{U}$  的协方差矩阵  $\mathbf{M}_u$  的正交归一化特征矢量作为行矢量组成的矩阵。

证明 对最优变换编码, 有  $\mathbf{B} = \mathbf{A}^{-1}$ , 代入  $D$  的表达式(6.225)中有

$$\begin{aligned} D &= E \text{tr} (\mathbf{A}^{-1} \mathbf{X} - \mathbf{A}^{-1} \mathbf{V})(\mathbf{A}^{-1} \mathbf{X} - \mathbf{A}^{-1} \mathbf{V})^T \\ &= \text{tr} \mathbf{A}^{-1} E\{(\mathbf{X} - \mathbf{V})(\mathbf{X} - \mathbf{V})^T\}(\mathbf{A}^{-1})^T \end{aligned} \quad (6.228)$$

由 的定义式(6.227)可知 在对角线上的元素为

$$_n = \frac{E\{X_n V_n\}}{E\{V_n^2\}} \quad (6.229)$$

当量化器中标量量化的方法一定时,  $V_n$  将与  $X_n$  成正比变化, 即在  $X_n$  变化某一倍数时,  $V_n$  也以相同倍数变化。所以在一定分布下,  $_n$  将只与量化方法有关, 而与  $x_n$  的方差无关。于是, 矩阵  $E\{(\mathbf{X} - \mathbf{V})(\mathbf{X} - \mathbf{V})^T\}$  对角线上的元素为

$$E\{(X_n - _n V_n)^2\} = _n^2 (l_n), \quad n = 1, 2, \dots, N \quad (6.230)$$

其中

$$_n^2 = E\{X_n^2\} \quad (6.231)$$

$$(l_n) = E\{X_n^2 - \frac{E\{X_n V_n\}}{E\{V_n^2\}} V_n^2\} \quad (6.232)$$

$l_n$  是第  $n$  个分量的量化比特数。

令

$$\mathbf{K} = \text{diag}\{(l_1), (l_2), \dots, (l_N)\} \quad (6.233)$$

则式(6.228)可进一步表示为

$$D = \text{tr}\{\mathbf{A}^{-1} \mathbf{K} \mathbf{M}_x (\mathbf{A}^{-1})^T\} \quad (6.234)$$

其中  $\mathbf{M}_x$  为  $\mathbf{X}$  的协方差矩阵。

由于  $\mathbf{X} = \mathbf{A}\mathbf{U}$ , 则有

$$\mathbf{M}_x = \mathbf{A}\mathbf{M}_u\mathbf{A}^T \quad (6.235)$$

代入式(6.234)中, 即有

$$\begin{aligned} D &= \text{tr}\{\mathbf{A}^{-1}\mathbf{K}\mathbf{A}\mathbf{M}_u\mathbf{A}^T(\mathbf{A}^{-1})^T\} \\ &= \text{tr}\{\mathbf{A}^{-1}\mathbf{K}\mathbf{A}\mathbf{M}_u\} \end{aligned} \quad (6.236)$$

其中,  $\mathbf{K}$  只取决于量化方法和总的量化比特在各分量间的分配, 而与各分量的统计特性无关, 所以  $\mathbf{K}$  和  $\mathbf{M}_u$  均独立于  $\mathbf{A}$  矩阵。

对式(6.236)取微分, 即得使  $D$  最小的发变换矩阵  $\mathbf{A}$  应满足

$$-\frac{D}{\mathbf{A}} = -(\mathbf{A}^{-1}\mathbf{K}\mathbf{A}\mathbf{M}_u\mathbf{A}^{-1})^T + (\mathbf{M}_u\mathbf{A}^{-1}\mathbf{K})^T = \mathbf{0}$$

或

$$\mathbf{A}^{-1}\mathbf{K}\mathbf{A}\mathbf{M}_u\mathbf{A}^{-1} = \mathbf{M}_u\mathbf{A}^{-1}\mathbf{K}$$

即

$$\mathbf{K}\mathbf{A}\mathbf{M}_u\mathbf{A}^{-1} = \mathbf{A}\mathbf{M}_u\mathbf{A}^{-1}\mathbf{K} \quad (6.237)$$

这说明  $\mathbf{A}\mathbf{M}_u\mathbf{A}^{-1}$  是对角矩阵  $\mathbf{K}$  的特征矢量作为列矢量所组成的矩阵, 所以  $\mathbf{A}\mathbf{M}_u\mathbf{A}^{-1}$  也是对角矩阵。而  $\mathbf{A}$  是去相关矩阵, 故  $\mathbf{M}_x$  也是对角矩阵。由式(6.235)可知, 此即  $\mathbf{A}\mathbf{M}_u\mathbf{A}^T$  是对角阵, 故

$$\mathbf{A}\mathbf{M}_u\mathbf{A}^T = \mathbf{A}\mathbf{M}_u\mathbf{A}^{-1} \quad (6.238)$$

式中  $\mathbf{A}\mathbf{M}_u\mathbf{A}^{-1}$  是对角阵。显然,  $\mathbf{A}\mathbf{M}_u$  非奇异, 故有

$$\mathbf{A}^T = \mathbf{A}^{-1}$$

或

$$\mathbf{A}\mathbf{A}^T = \mathbf{I} \quad (6.239)$$

这说明  $\mathbf{A}$  必有正交行矢量。  $\mathbf{A}$  的选取有一定任意性, 因为不同的  $\mathbf{A}$  导致的  $\mathbf{A}$  在理想情况下经收变换  $\mathbf{B} = \mathbf{A}^{-1}$  后有相同的平均失真。若取  $\mathbf{B} = \mathbf{I}$ , 则得最优变换编码的去相关矩阵是由  $\mathbf{M}_u$  的归一化特征矢量作为行矢量组成的矩阵, 该矩阵所作的变换称为 Karhunen-Loeve 变换, 简称 K-L 变换。在这一变换下, 有

$$\mathbf{M}_x = \mathbf{A}\mathbf{M}_u\mathbf{A}^T = \text{diag}\{\mu_1, \mu_2, \dots, \mu_N\} \quad (6.240)$$

其中  $\{\mu_n\}_{n=1}^N$  是  $\mathbf{M}_u$  的特征值。于是有

$$\mu_n^2 = \mu_n, \quad n = 1, 2, \dots, N \quad (6.241)$$

证毕

**性质 6.7** 最优变换编码的最优量化器对各个分量分配的量化比特数应该

满足

$$\begin{aligned} l_n &= l - \frac{1}{2^n}, \quad \text{当 } \frac{1}{2^n} < -\frac{1}{(0)} \text{ 时} \\ l_n &= 0, \quad \text{当 } \frac{1}{2^n} = -\frac{1}{(0)} \text{ 时} \end{aligned} \quad (6.242)$$

其中  $l(\cdot)$  是  $(l)$  的逆函数, 且 满足

$$\sum_{n=1}^N l - \frac{1}{2^n} = L \quad (6.243)$$

证明 由式(6.236)、(6.237)和(6.238)及  $\mathbf{I} = \mathbf{I}$  可知

$$\begin{aligned} D &= \text{tr}\{\mathbf{A}^{-1} \mathbf{K} \mathbf{A} \mathbf{M}_u\} = \text{tr}\{\mathbf{K} \mathbf{A} \mathbf{M}_u \mathbf{A}^{-1}\} \\ &= \text{tr}\{\mathbf{K} \mathbf{A} \mathbf{M}_u \mathbf{A}^T\} = \sum_{n=1}^N \mu_n(l_n) = \sum_{n=1}^N \frac{1}{2^n}(l_n) \end{aligned} \quad (6.244)$$

由于  $\mathbf{x}$  的各个分量是按相同的量化方法分别进行量化的, 则假定各分量具有相同的平均失真和量化电平数的函数  $(l_n)$ 。这样, 对量化器进行优化, 唯一可变的参数就是总的量化比特数在各分量之间的分配, 即求式(6.244)在约束条件

$$\sum_{n=1}^N l_n = L \quad (6.245)$$

$$l_n \geq 0, \quad n = 1, 2, \dots, N \quad (6.246)$$

下达到最小时的  $l_n, n = 1, 2, \dots, N$ , 这是函数在约束条件下求最小值的问题。

设  $(l)$  是  $l$  的严下凸的减函数, 且具有连续的一阶导数  $(l)$ , 则  $D$  对  $\{l_n\}$  严下凸。为求最小值只需利用拉格朗日乘数法构造新函数

$$F = \sum_{n=1}^N \frac{1}{2^n}(l_n) + \lambda \left( \sum_{n=1}^N l_n - L \right) \quad (6.247)$$

取

$$\frac{\partial F}{\partial l_n} = \frac{1}{2^n}(l_n) + \lambda = 0, \quad \text{当 } l_n > 0 \text{ 时}$$

$$\frac{\partial F}{\partial l_n} = \frac{1}{2^n}(l_n) + \lambda = 0, \quad \text{当 } l_n = 0 \text{ 时}$$

即可得解

$$\begin{aligned} l_n &= l - \frac{1}{2^n}, \quad \text{当 } \frac{1}{2^n} > -\frac{1}{(0)} \text{ 时} \\ l_n &= 0, \quad \text{当 } \frac{1}{2^n} = -\frac{1}{(0)} \text{ 时} \end{aligned}$$

其中,  $l(\cdot)$  是  $(l)$  的逆函数, 且 满足

$$\sum_{n=1}^N l_n - \frac{1}{2} \sum_{n=1}^N l_n = L$$

证毕

性质 6.8 标量量化算法应该使平均失真式(6.225)最小。

可以证明使式(6.225)最小的标量量化算法等价于使  $X_n$  标量量化均方误差最小的算法,因此,可以用 Lloyd-Max 算法,且此时有  $\mathbf{B} = \mathbf{I}$ ,  $\mathbf{B} = \mathbf{A}^{-1}$ 。

例 6.2 变换编码在语音压缩中的应用。

设语音信号经 5 kHz 低通滤波器后,以 10 kHz 采样,然后进行线性预测分析(LPC)。所用的 LPC 系数是对数面积比。又设每秒取 100 帧语音(即每帧语音的长度为 10 ms),每帧有 14 个系数值组成一个信源字或矢量。

对该信源进行三种方法的熵压缩编码,所得的归一化均方误差(单位: dB)与信息速率(单位: bit/ 矢量)的曲线如图 6.6 所示,其中,曲线  $a$  为对信源矢量直接作矢量量化(矢量量化算法为 K-近邻算法);曲线  $b$  为先对信源矢量作变换(变换矩阵为特征矢量矩阵),再进行比特分配和 Lloyd-Max 算法;曲线  $c$  为对信源矢量的各分量直接用 Lloyd-Max 算法进行标量量化,并对总的量化比特数进行优化分配。

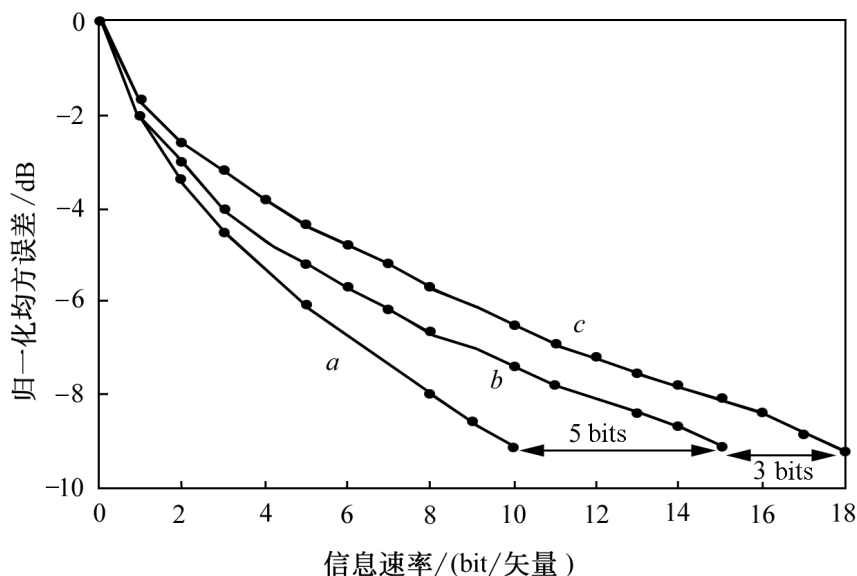


图 6.6 对语音信号进行三种熵压缩方法下的均方误差与信息速率

从图中可以看出,曲线  $b$  比  $c$  的信息速率大约下降 3 bits/ 矢量,这一改善主要依靠去相关获得的,而曲线  $a$  又比曲线  $b$  的信息速率有 5 bits/ 矢量的降低,这一改善是充分利用了 14 个对数面积比之间的非线性依存关系,因此,矢量量化是熵压缩分组编码的最有效方法。

### 6.8 预测编码——实用的熵压缩树码

预测编码的概念最早是由 Peter Elias 在 1955 年提出的,它是目前已得到广泛应用的一种实用的熵压缩树码。

预测编码是这样一种编码方法,在这种方法中编码器和译码器都存贮有过去的信号值,并以此来预测或估计未来信号的值;在编码端发出的不是信源信号本身,而是信源信号与预测值之差;在译码端,译码器将接收到的这一差值与译码器的预测值相加,从而恢复信源信号。预测编码的编译码过程如图 6.7 所示。

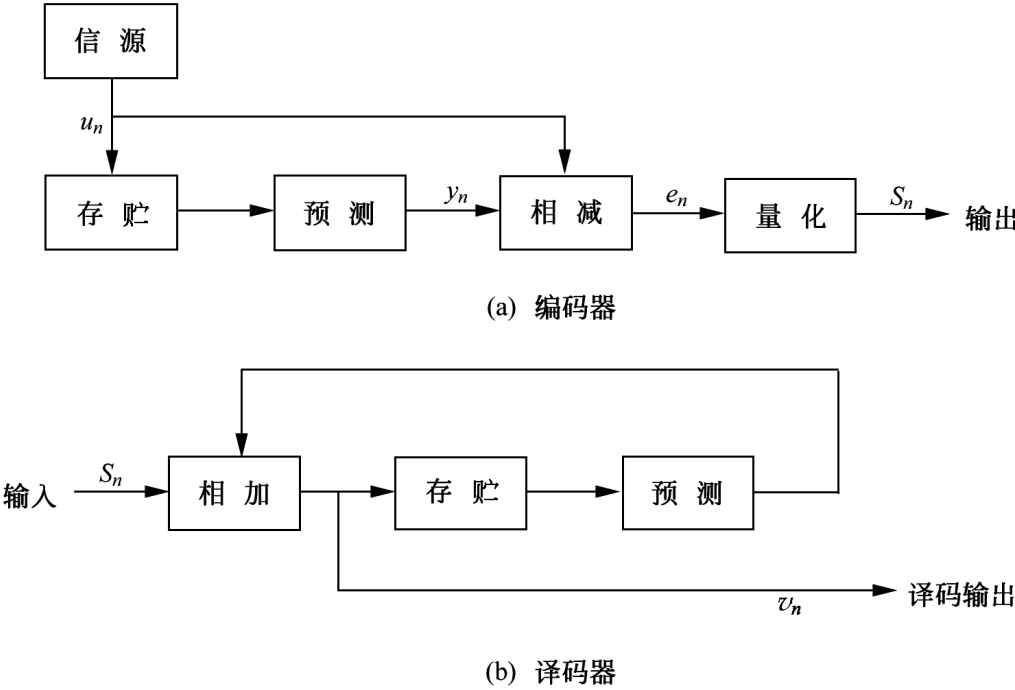


图 6.7 预测编码

根据预测器中预测值与信源信号过去时刻值之间的函数关系,预测器被分为线性预测器和非线性预测器,相应的预测编码被分为线性预测编码与非线性预测编码。

设信源输出信号序列为  $(\dots, u_{-2}, u_{-1}, u_0, u_1, u_2, \dots)$ , 预测器根据所存贮的信号过去值  $(\dots, u_{-1}, u_0, u_1, \dots, u_{n-1})$  对第  $n$  时刻的值进行预测, 得到预测值  $y_n$ 。该预测值  $y_n$  与信号实际值  $u_n$  之差即为预测误差  $e_n$ , 即

$$e_n = y_n - u_n \tag{6.248}$$

如何选取预测值  $y_n$ , 以使预测误差  $e_n$  满足某种意义上的最佳是预测编码设计中的核心问题。按照不同的最佳准则, 可以得到比较重要的三种最佳预测器。

### 6.8.1 最小均方误差预测器

最小均方误差预测器的最佳准则是使预测误差的均方值达到最小。

若对信号已有全面了解,即已知信号的所有条件概率分布密度  $q(u_n | u_{n-1} \cdot u_{n-2} \dots)$ , 则最佳预测器的预测值应是条件概率分布密度的均值,即

$$y_n = \bar{u}_n = \int_{-\infty}^{+\infty} u_n q(u_n | u_{n-1} \cdot u_{n-2} \dots) du_n \quad (6.249)$$

这是因为分布对均值点的二阶矩为最小,这正是预测误差的均方值为最小。

一般来讲,  $y_n$  是过去值的某一确定函数,可表示为  $y_n(u_{n-1}, u_{n-2}, \dots)$ 。仅当信号是独立随机序列时,才有

$$q(u_n | u_{n-1} u_{n-2} \dots) = p(u_n)$$

此时的  $\bar{u}_n$  为一个常数。

另一方面,  $y_n$  与过去值的函数关系可以是线性的,也可以是非线性的。1940年, N. Wiener 研究结果指出,最佳线性预测器可以由信号的自关函数完全确定。而最佳的非线性预测器目前尚无系统的确定方法。

### 6.8.2 最小平均绝对误差预测器

最小平均绝对误差预测器的最佳准则是使预测器的绝对误差的均值达到最小。

该意义上的最佳预测器的预测值应是条件概率分布密度的中值,这是因为分布相对于中值的一阶绝对矩最小,这正是预测的绝对误差的均值为最小。

同样,该中值(即预测值)是过去值的确定函数。对连续分布而言,中值是唯一的。

### 6.8.3 最大零误差概率预测器

最大零误差概率预测器(或最大零误差概率密度预测器)的最佳准则是预测值具有零误差的概率或概率密度为最大。

该意义上的最佳预测值应是条件分布的模式。无论离散或连续的情形,模式都可能不唯一,故只能从中作一选择。

总之,不同准则下的最佳预测给出不同的预测值,但是预测误差的分布与信源信号的一维分布具有相同的形状,其差别只是由于减去预测值而导致的分布的平移。当信源信号的一维分布具有单峰、且为对称分布时,三种准则给出的预测值相同。

**例 6.3** 设计高斯信源的最小均方误差预测器。

对一阶高斯马尔可夫信源,已知

$$p(u_{n-1}, u_n) = \frac{1}{2\pi(1-\rho^2)} \exp \left\{ -\frac{1}{2(1-\rho^2)} \left( \frac{u_n^2}{2} - 2\rho \frac{u_{n-1}u_n}{2} + \frac{u_{n-1}^2}{2} \right) \right\} \quad (6.250)$$

$$q(u_n / u_{n-1}) = \frac{1}{2\pi(1-\rho^2)} \exp \left\{ -\frac{(u_n - \rho u_{n-1})^2}{2(1-\rho^2)} \right\} \quad (6.251)$$

故有

$$\int_{-\infty}^{+\infty} u_n q(u_n / u_{n-1}) du_n = \rho u_{n-1}$$

所以一阶高斯马尔可夫信源的最小均方误差预测器的预测值为  $\rho u_{n-1}$ 。

对一般的高斯信源,已知

$$q(u_n / u_{n-1} u_{n-2} \dots) = \frac{1}{2\pi} \exp \left\{ -\frac{u_n^2 - \sum_{m=1}^{+\infty} \rho_m u_{n-m}^2}{2} \right\} \quad (6.252)$$

则有

$$\int_{-\infty}^{+\infty} u_n q(u_n / u_{n-1} u_{n-2} \dots) du_n = \sum_{m=1}^{+\infty} \rho_m u_{n-m} \quad (6.253)$$

所以一般高斯信源的最小均方误差预测器的预测值为  $\sum_{m=1}^{+\infty} \rho_m u_{n-m}$ 。

综上,对高斯信源而言,均方误差意义上的最佳预测就是线性预测,而且此时的预测误差具有高斯分布,并与信号的过去值无关。这说明预测编码后得到的预测误差信号是一个与信号的过去值无关的独立随机序列。

从信息论的观点来看,有记忆稳恒信源的熵率为

$$H(U) = \lim_{M \rightarrow \infty} H_M(U) \quad (6.254)$$

其中

$$H_M(U) = -\frac{1}{M} \sum_{u_n, u_{n-1}, \dots, u_{n-M+1}} \dots p(u_n u_{n-1} \dots u_{n-M+1}) \log p(u_n u_{n-1} \dots u_{n-M+1}) \quad (6.255)$$

或连续的有记忆稳恒信源的微分熵为

$$h(U) = \lim_M h_M(U) \quad (6.256)$$

其中

$$h_M(U) = - \frac{1}{M} \int \dots \int p(u_n, u_{n-1}, \dots, u_{n-M+1}) \cdot \log p(u_n, u_{n-1}, \dots, u_{n-M+1}) du_n du_{n-1} \dots du_{n-M+1} \quad (6.257)$$

若信源为  $L$  阶马尔可夫信源, 则有

$$p(u_n, u_{n-1}, \dots, u_{n-L}) = p(u_{n-1}, u_{n-2}, \dots, u_{n-L}) q(u_n | u_{n-1}, \dots, u_{n-L}) \quad (6.258)$$

于是  $L$  阶马尔可夫信源的微分熵为

$$h(U) = \int \dots \int p(u_{n-1}, u_{n-2}, \dots, u_{n-L+1}) du_{n-1} du_{n-2} \dots du_{n-L+1} \cdot \int q(u_n | u_{n-1}, \dots, u_{n-L}) \log q(u_n | u_{n-1}, \dots, u_{n-L}) du_n \quad (6.259)$$

这说明信源的熵等于其条件分布的熵的平均。所以有以下结论:

(1) 若对信源按其条件分布进行冗余度压缩, 可以实现理想的信源冗余度压缩。

(2) 对高斯信源, 均方误差意义下的最佳预测即是线性预测, 此时预测误差的分布就是信源信号的条件分布, 而最小均方误差等价于最小条件熵。

(3) 对一般信源, 均方误差意义下的最佳预测不是线性预测。尽管从性能上讲线性预测对非高斯信源不是最优的, 不能实现理想的冗余度压缩, 但是线性预测在实现上有着优越性, 即最佳线性预测只须求相关函数。相关函数是一个单变量函数, 它的求解比计算条件分布方便得多。

## 习 题

6.1 设已知离散无记忆信源在给定失真量度  $d(k, j)$ ,  $k=1, 2, \dots, K$ ,  $j=1, 2, \dots, J$  下的信息速率失真函数为  $R(D)$ , 现定义新的失真量度  $d(k, j) = d(k, j) - g_k$ 。试证: 在新的失真量度下信息速率失真函数  $R(D)$  为  $R(D) = R(D + G)$ , 其中  $G = \sum_k p(k) g_k$ 。

6.2 设有带宽为 4 kHz 的限带白色高斯信源, 欲通过信道容量为 16 kb/s 的信道传输, 试求在理想情况下信道输出端可能得到的最大信噪比。

6.3 设  $\{ \mathbf{u}^n \} (n=1, 2, \dots, N)$  是  $N$  个正交规范化的  $N$  维向量,  $\mathbf{A}$  是由  $(\mathbf{u}^1, \dots, \mathbf{u}^N)$



$^2, \dots, ^N$ )组成的正交矩阵,  $N$  维随机向量  $\mathbf{X}$  在正交变换下得到新的随机向量  $\mathbf{Z}$ ,  $\mathbf{Z} = \mathbf{A}^T \mathbf{X}$ , 其中  $\mathbf{X} = (x_1, x_2, \dots, x_N)^T$ ,  $\mathbf{Z} = (z_1, z_2, \dots, z_N)^T$ ,  $E\{\mathbf{X}\} = \mathbf{0}$ 。令

$$\sigma_n^2 = E\{(z_n - \bar{z}_n)^2\}, \quad \bar{z}_n = \frac{1}{N} \sum_{n=1}^N z_n$$

$$H(\mathbf{Z}) = - \sum_{n=1}^N \log \sigma_n$$

试证:所有正交变换中, K-L 变换所对应的  $\mathbf{Z}$  有最小的熵  $H(\mathbf{Z})$ 。

6.4 设无记忆信源  $X = \begin{matrix} -1, & 0, & 1 \\ p(x) & 1/3, & 1/3, & 1/3 \end{matrix}$ , 接收符号  $A_Y = \begin{matrix} 1 & 2 \\ 1 & 1 \\ 2 & 1 \end{matrix}$ , 失真矩阵  $\mathbf{D} = \begin{matrix} 1 & 2 \\ 1 & 1 \\ 2 & 1 \end{matrix}$ 。试求:  $D_{\max}$  和  $D_{\min}$  及达到  $D_{\max}$ ,  $D_{\min}$  时的转移概率矩阵。

6.5 已知二元信源  $\mathbf{X} = \begin{matrix} 0, & 1 \\ p, & 1-p \end{matrix}$  以及失真矩阵  $(d_{kj}) = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$ , 试求:

(1)  $D_{\min}$ ; (2)  $D_{\max}$ ; (3)  $R(D)$ 。

6.6 设有总功率为 10 mW 的限带 (0 ~ 5 kHz) 白色高斯信源通过加性白色高斯噪声信道传输, 后者的带宽为 0 ~ 10 kHz, 噪声的单边功率谱密度为  $1 \mu\text{W/Hz}$ , 容许最大输入功率为 20 mW。试求在理想情况下接收信号可以达到的最小均方误差。

6.7 设有平稳高斯信源  $X(t)$ , 其功率谱为

$$G(f) = \begin{cases} A, & |f| \leq F_1 \\ 0, & |f| > F_1 \end{cases}$$

失真度量取  $d(x, y) = (x - y)^2$ , 容许的样值失真为  $D$ 。试求:

(1) 信息速率失真函数  $R(D)$ ;

(2) 用一独立加性高斯信道 (带宽  $F_2$ , 限功率  $P$ , 噪声的双边功率谱密度  $\frac{N_0}{2}$ ) 来传送上述信源时, 最小可能方差与  $F_2$  的关系。

6.8 设有矢量信源, 其各分量  $X_k \sim N(0, \sigma_k^2)$ ,  $k = 1, 2, \dots, K$ , 是  $K$  个独立的随机变量, 失真  $d(x_1, x_2, \dots, x_K; \hat{x}_1, \hat{x}_2, \dots, \hat{x}_K) = \sum_{k=1}^K (x_k - \hat{x}_k)^2$ 。试证: 在此条件下

$$R(D) = \sum_{k=1}^K \frac{1}{2} \log \frac{2}{D_k}$$

其中,  $D_k = \frac{2}{k}$ , 当  $\frac{2}{k} < \frac{2}{k}$ , 满足  $\sum_{k=1}^K D_k = D$ 。

6.9 设有离散无记忆信源  $X$  经编码后输出  $Y$ , 失真矩阵的所有列是集合  $\{d_1, d_2, \dots, d_m\}$  的某一置换。定义函数

$$(D) = \max_{\mathbf{P}} \sum_{i=1}^m P_i d_i$$

- (1) 证明  $(D)$  是  $D$  的上凸函数;
- (2) 证明:  $I(X; Y) = H(X) - (D)$ 。

## 第7章 最大熵原理与最小鉴别信息原理

这一章我们要讨论在香农经典信息论中没有涉及的两个原理,即 E. T. Jaynes 提出的最大熵原理与 S. Kullback 提出的最小鉴别信息原理。虽然对这两个原理在学术界还存在不同的看法,但是它们在实际问题中的应用近年来一直在不断地发展。

本章将从以下几个方面讨论这两个原理:

(1) 陈述这两个原理的基本概念,并从下列三个方面讨论其价值和适用性:

- 从信息和组合论的意义上指出这两个原理的合理性;
- 给出这两个原理的公理化推导,从而说明在何种要求和假设下这两个原理是必然的结论和唯一可能的结果;
- 从非统计的意义(即从失真度的意义)上指出这两个原理的适用性,以说明这两个原理也可以从最小失真的意义上加以理解和利用。

(2) 在对原理本身进行上述讨论后,我们转而讨论这两个原理的应用。这一讨论不是全面的,我们只选择了两个基本的有代表性的应用作为例子进行介绍。然后对这两个原理下所得解的分布的特点作一讨论。

### 7.1 非适定问题与最大熵和最小鉴别信息原理

#### 7.1.1 非适定问题的提出

人类习惯于对客观世界或物理系统建立各种模型。利用模型,人们就可以根据物理系统所受的外界作用或激励来估计系统将会产生的反应,或者相反根据物理系统的外部表现来估计系统模型的参数及所受的激励,在数学上,前者称为正问题,后者称为逆问题。无论是正问题还是逆问题,问题的解总是与所给的条件联系在一起的,所给的条件过多称为过定;而条件不够则称为欠定。在逆问题中,我们常常会遇到条件不充分或欠定的情况。造成欠定的原因有以下两个:

- 对系统进行观察所得的数据不完全;
- 由于仪器误差或模型过于粗糙导致的数据不确定或不精确。

在数学家中, Hadamard 是较早研究欠定情况的人。他把由于欠定导致的解不唯一或不连续(即解不连续依赖于条件的变化)称为非适定问题。但他当时认为这类问题无物理意义可言。今天,人们已一致认识到这类问题的重要性,并把解不满足存在、连续且唯一这三个条件中任一条的问题均称为非适定问题。

非适定问题在科学研究和工程实践中经常可以遇到,例如地球物理学中利用地震勘探法确定地层构造,射电天文学中利用无线电干涉仪获取星空图像,计算机层析术中利用扫描投影数据构造断层图像,语音识别和语音编码中根据语音信号估计声道参数,图像处理中对散焦或目标位移造成的蜕化图像进行复原,雷达及声纳中根据接收信号进行功率谱估计,数字通信中对信道畸变带来的符号间串扰进行盲目均衡等都是这类问题的实例。

## 7.1.2 最大熵原理与最小鉴别信息原理

由于非适定问题的多样性,非适定问题的解决目前还没有统一的方法。但基于概率论的统计方法是其中最重要的一类方法,如最大似然解法等,基于最大熵原理的最大熵方法和基于最小鉴别信息原理的最小鉴别信息法也属于这一类。

设有随机变量  $X$  以某未知的概率  $q^*(a_k)$  取值  $a_k$ 。已知  $X$  的某若干种函数  $f_m(x)$  的数学期望为

$$\sum_{k=1}^K q^*(a_k) f_m(a_k) = C_m, \quad m = 1, 2, \dots, M$$

要求对  $X$  的分布作出估计,或者说求  $X$  分布的解。

在一般情况下,已知的约束条件对求解  $X$  的分布来讲总是不充分的,因此会有很多分布  $\{q(a_k)\}$  均满足这些约束条件,所以这是一个非适定问题,我们需要确定某种原则或原理才能在这种情况下从众多解中找出一个合理的解。从信息论的观点来看,最大熵原理及最小鉴别信息原理就是这时应该遵循的原理。

### 7.1.2.1 最大熵原理

E. T. Jaynes 在 1957 年提出了一种观点。他认为:在只掌握部分信息的情况下要对分布作出推断时,我们应该取符合约束条件但熵值取最大的概率分布,这是我们可以作出的唯一的不偏不倚的选择,任何其他的选择都意味着我们添加了其他的约束或假设,这些约束或假设根据我们所掌握的信息是无法作出的。

Jaynes 把这一观点称为最大熵原理, 并认为这是在这类问题中普遍适用的统计推断原理。

按最大熵原理, 为求在约束条件

$$\sum_{k=1}^K q(a_k) f_m(a_k) = C_m, \quad m = 1, 2, \dots, M \quad (7.1)$$

$$\sum_{k=1}^K q(a_k) = 1 \quad (7.2)$$

下能使熵

$$H(X) = - \sum_{k=1}^K q(a_k) \log q(a_k) \quad (7.3)$$

取最大的分布, 只需按拉格朗日乘数法, 令

$$F = H(X) - \sum_{k=1}^K q(a_k) - 1 - \sum_{m=1}^M \lambda_m \left( \sum_{k=1}^K q(a_k) f_m(a_k) - C_m \right) \quad (7.4)$$

取

$$\frac{\partial F}{\partial q(a_k)} = -1 - \log q(a_k) - \sum_{m=1}^M \lambda_m f_m(a_k) = 0$$

得

$$\log q(a_k) = -1 - \sum_{m=1}^M \lambda_m f_m(a_k)$$

或

$$\hat{q}(a_k) = \exp \left( -1 - \sum_{m=1}^M \lambda_m f_m(a_k) \right) \quad (7.5)$$

其中  $\lambda_0 = -1$ 。常数  $\lambda_0$  和  $\lambda_m (m=1, 2, \dots, M)$  原则上可由式(7.1)和式(7.2)共  $M+1$  个约束条件求得。式(7.5)就是满足约束条件的同时使熵有最大值的分布。

当随机变量  $X$  具有连续的分布时, 我们在第 2 章中已经说过此时熵不存在, 但此时有微分熵。所以在约束条件

$$\int q(x) f_m(x) dx = C_m, \quad m = 1, 2, \dots, M \quad (7.6)$$

$$\int q(x) dx = 1 \quad (7.7)$$

下可使微分熵

$$h(X) = - \int q(x) \log q(x) dx \quad (7.8)$$

最大。按拉格朗日乘数法,同理可解得

$$\hat{q}(x) = \exp \left\{ -\lambda_0 - \sum_{m=1}^M \lambda_m f_m(x) \right\} \quad (7.9)$$

虽然严格地讲此时应为最大微分熵原理,但是习惯上把离散和连续两种情况下的上述原理统称为最大熵原理。

统计物理中一些有名的分布已被证明都是在若干类似上述的约束条件下使熵或微分熵最大的分布。例如,统计力学中气体分子速度的分布是能量受约束下的最大熵分布,大气层空气密度随高度的分布是在平均势能受约束下的最大熵分布等。这些事实鼓舞了人们对最大熵原理的信心。自 1957 年 Jaynes 提出这一原理以来,这一原理先后在统计力学、统计学、运输工程、排队论、计算机系统建模、系统仿真、生产决策、股市分析等领域得到应用,特别是在信号处理领域,最大熵原理成为谱估计和图像复原中的主要方法。

### 7.1.2.2 最小鉴别信息原理

在 Jaynes 提出最大熵原理后不久, S. Kullback 在他的著作中第一次系统地提出了最小鉴别信息原理。他认为这一方法与香农率失真理论的方法相似,并指出在 1957 年 Jaynes 提出最大熵原理时, Fraser 还提出过“最少倾向性”分布的概念。但 Kullback 提出的这些观点和概念在初期并没有引起广泛注意,特别是在工程中没有很快得到应用,一直到 70 年代末,主要是由于 J. E. Shore 和 R. W. Johnson 的工作,这一原理开始得到广泛重视和应用。

最小鉴别信息原理是在下述情况下提出的,设随机变量  $X$  具有未知的概率分布密度函数  $q^*(x)$ ,在已知某若干函数  $f_m(x)$  的数学期望

$$\int q^*(x) f_m(x) dx = C_m, \quad m = 1, 2, \dots, M$$

及先验概率分布密度  $p(x)$  的条件下,如何对此未知的概率分布密度  $q^*(x)$  作出估计。最小鉴别信息原理认为,应该在所有满足下述条件

$$\int q(x) f_m(x) dx = C_m, \quad m = 1, 2, \dots, M \quad (7.10)$$

$$\int q(x) dx = 1 \quad (7.11)$$

的  $q(x)$  中选择能使鉴别信息

$$I(q(x), p(x)) = \int q(x) \log \frac{q(x)}{p(x)} dx \quad (7.12)$$

取最小值的解作为对  $q^*(x)$  的估计。这是因为在所有满足式(7.10)和式(7.11)的  $q(x)$  中,使式(7.12)最小的  $q(x)$  意味着由  $p(x)$  改变为  $q(x)$  所需的信息量最少,或者,按照 Kullback 的说法,使鉴别信息最小的分布是在满足约束条件下最接近于  $p(x)$  的概率分布。

最小鉴别信息  $I(q, p)$  是  $q(x)$  的泛函,因此按最小鉴别信息原理求  $q^*(x)$  的估计是一个条件变分问题。此问题的一般解法是引入拉格朗日乘子,并构造新泛函

$$F = \int q(x) \log \frac{q(x)}{p(x)} dx - \lambda_0 \int q(x) dx - \sum_{m=1}^M \lambda_m \int q(x) f_m(x) dx \quad (7.13)$$

取上述泛函对  $q(x)$  的变分,并使其等于零。而按欧拉方程,这相当于要求被积函数对  $q(x)$  的偏导数为零,即令

$$\log \frac{q(x)}{p(x)} + 1 - \lambda_0 - \sum_{m=1}^M \lambda_m f_m(x) = 0$$

解得

$$\hat{q}(x) = p(x) \exp \left[ -\lambda_0 - \sum_{m=1}^M \lambda_m f_m(x) \right] \quad (7.14)$$

其中  $\lambda_0 = -1$ 。 $\lambda_0$  和  $\lambda_m (m=1, 2, \dots, M)$  原则上可由式(7.10)和式(7.11)共  $M+1$  个约束条件求得。乘数的大小体现了约束条件对分布的影响程度,多余约束将对应零乘数。

对最大熵原理下的解(7.9)和最小鉴别信息原理下的解(7.14)进行比较,我们立刻可以看到,最小鉴别信息原理是最大熵原理的推广。显然,当随机变量具有离散分布且先验分布为等概分布时,这两个原理等价。

熵和鉴别信息是信息论中的两个基本概念。如果我们承认这两个概念的合理性,则利用最大熵原理或最小鉴别信息原理来解上述特定的非适定问题应该说是一个必然的推论或结果。因为在这两个原理下,我们得到的解中除了包含约束条件和先验概率分布所提供的信息外,没有有形或无形地增加其他我们实际上没有获得的信息,因此这样的结果是客观和合理的。当然,这样论证并没有排除最大熵原理和最小鉴别信息原理提出时人们对这两个原理的合理性所提出的全部疑问,所以,在下面几节中,我们将对这一问题作进一步分析和讨论。

## 7.2 最大熵原理的合理性

对最大熵原理提出的疑问主要有以下两个:

## (1) 关于最大熵原理所得解的客观性

引起这一疑问的原因要追溯到香农对熵的定义和解释。在那里, 香农是从通信的角度提出和讨论熵和信息的, 因此计算熵和信息时所用的概率分布带有一定的主观性。而最大熵原理是用于对客观物理系统的某种实际分布的估计, 那么这样得到的估计是否也带有主观性呢? 仔细分析最大熵原理所针对的问题, 就可以知道在这一问题中, 熵的确代表了人们对客观物理系统中某种物理量概率分布的无知程度, 它带有主观性。然而, 在最大熵原理下所给出的解却完全是一个客观的量, 因为这一解只与一组数学期望值有关, 而这组数学期望值是可以客观测量得到的, 所以最大熵原理给出的解完全是一个客观量, 没有主观的因素。

## (2) 如何理解被最大熵原理排除的其他满足约束条件的解

最大熵原理所给出的解是唯一的, 而非适定问题原来的解不唯一, 因此我们如何来理解适合约束条件的其他解, 它们在实际情况下会不会是真正的解呢? 对此, Jaynes 用熵集中定理对此作了解释, 这一解释是这样的。

设我们进行一个随机试验, 每次试验的结果有  $K$  种可能, 则在连续进行  $N$  次试验时所得到的将是随机序列的一个实现, 它总共有  $K^N$  种可能的序列。在这  $K^N$  种可能的序列中, 第  $k$  事件出现  $N_k = N f_k$  次 ( $k = 1, 2, \dots, K$ ) 的序列共有  $W(f_1, f_2, \dots, f_K)$  种

$$W(f_1, f_2, \dots, f_K) = \frac{N!}{(Nf_1)!(Nf_2)!\dots(Nf_K)!} \quad (7.15)$$

按 Stirling 阶乘公式, 当  $n$  充分大时, 则  $n! \approx 2n \frac{n^n}{e^n}$ , 故近似地有

$$\lim_N N^{-1} \log W = H(f_1, f_2, \dots, f_K) = - \sum_{k=1}^K f_k \log f_k \quad (7.16)$$

或

$$W(f_1, f_2, \dots, f_K) = \exp[NH(f_1, f_2, \dots, f_K)] \quad (7.17)$$

频率  $\{f_k, k = 1, 2, \dots, K\}$  可以看成是  $K$  维坐标中的一个点  $P$ , 所有可能的频率组合组成  $K$  维空间中的凸集  $S = \{P: f_k \geq 0, \sum_{k=1}^K f_k = 1\}$ 。在这个集合上, 熵  $H(f_1, f_2, \dots, f_K)$  连续地从零到  $\log K$  之间变化。当点  $P$  在凸集  $S$  的顶点时, 熵  $H(f_1, f_2, \dots, f_K) = 0$ ; 当点  $P$  在凸集  $S$  的中心时, 熵  $H(f_1, f_2, \dots, f_K)$  取最大。

在解非适定问题时, 我们对这些频率加了  $M+1$  个线性约束条件, 这些约束定义了一个  $K-M-1$  维的超平面  $S_M$ , 于是所有可能的解被限制在集合  $S =$



$S_M$  中, 且  $S$  的维数为  $K - M - 1$ 。由于熵是  $S$  上的凸函数, 而  $S$  是  $S$  中的一个凸子集, 故熵也是  $S$  上的凸函数, 因此熵在  $S$  中有唯一的最大值点。在集合  $S$  中我们定义新的坐标系  $(x_1, x_2, \dots, x_L)$ , 其中  $L = K - M - 1$ ,  $x_l$  ( $l = 1, 2, \dots, K - M - 1$ ) 是  $f_k$  的线性组合, 且在这个新坐标系中, 熵在 origin 取最大。这样, 我们就可以在 origin 附近对熵函数进行级数展开, 得

$$H(P) = H_{\max} - ar^2 + \dots, \quad a > 0 \quad (7.18)$$

其中  $r$  是  $P$  离开中心点的距离, 即

$$r = \sqrt{\sum_{k=1}^L x_k^2} \quad (7.19)$$

所以, 与  $H_{\max}$  相差  $H$  的点  $P$  将都限制在半径为  $R$  的  $L$  维球体内, 且  $R$  满足

$$aR^2 = H \quad (7.20)$$

根据式(7.17), 两组不同的频率所对应的  $W(f_1, f_2, \dots, f_K)$  值之比为

$$\frac{W(H)}{W(H_{\max})} \exp N(H - H_{\max}) = \exp(-NaR^2) \quad (7.21)$$

所以, 在半径为  $R$  的球中的点所对应的序列数目在  $K^N$  种可能序列所占的百分比  $F_R$  为

$$F_R = \frac{I(R)}{K^N} \quad (7.22)$$

其中

$$I(R) = \int_0^R e^{-Na r^2} r^{L-1} dr$$

这一积分结果正是自由度为  $L$  的  $\chi^2$  分布的分布函数, 因此有

$$2N(H - H_{\max}) = L(1 - F_R) \quad (7.23)$$

**例 7.1** 在掷色子的试验中, 若我们掷了 1000 次, 并知道点数的平均为 4.5, 即

$$\sum_{k=1}^6 kf_k = 4.5$$

则按最大熵原理, 所得的解为

$$(f_1, f_2, \dots, f_6) = (0.0543, 0.0788, 0.1142, 0.1654, 0.2398, 0.3475)$$

此时相应的熵值为

$$H_{\max} = 1.61358$$

而按  $\chi^2$  分布可以得到

(1) 95% 的符合约束条件的解, 其熵值满足

$$1.609 \quad H \quad 1.61358$$

(2) 99.99% 的符合约束条件的解, 其熵值满足

$$1.602 \quad H \quad 1.61358$$

这一结果说明, 从概率的观点来看, 熵值远离最大熵的可能解出现的机会非常小, 或者从组合的观点来看, 熵值远离最大熵的组合种类在所有可能的组合中所占的比例很小。因此, 最大熵解是在给定信息下可能作出的最可靠的解, 它在绝大多数情况下会接近于真实解, 因而最大熵原理是一种保险的策略。

最大熵原理合理性的这一解释也建立了这一原理与 Bayes 原理之间的关系, 实际上, 按式(7.17)我们可以得到使熵  $H(f_1, f_2, \dots, f_k)$  最大的解, 也就是使这一分布的概率最大的解, 因为后者的值是  $W(f_1, f_2, \dots, f_k)/K^N = \exp\{N[H(f_1, f_2, \dots, f_k) - \log K]\}$ , 所以最大熵解就是满足约束条件下的最大似然解。

## \* 7.3 最小鉴别信息原理与最大熵原理的公理化推导

### 7.3.1 最小鉴别信息原理的推导

我们在节 7.1 导出非适定问题的最小鉴别信息原理时用的是直观的、由鉴别信息概念出发的推断, 这种推断方法是 Kullback 在 1959 年时采用的。Shore 和 Johnson 在 1980 年证明这一原理也可用公理化的形式在数学上给出严格的推导。

设在上述非适定问题中, 我们用  $D$  表示  $X$  取值的集合, 用  $I$  表示已知的约束条件, 用  $Q$  表示所有可能的概率密度函数的集合,  $Q_I$  表示满足约束条件的密度函数的集合, 算子“ $\hat{q}$ ”表示泛函求最小值的运算, 即用

$$\hat{q}(\mathbf{x}) = p(\mathbf{x}) \quad I \quad (7.24)$$

来表示求解  $\hat{q}(\mathbf{x})$ , 使  $\hat{q}(\mathbf{x})$  满足

$$F(\hat{q}(\mathbf{x}), p(\mathbf{x})) = \min_{q(\mathbf{x}) \in Q_I} F(q(\mathbf{x}), p(\mathbf{x})) \quad (7.25)$$

的运算。泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  的形式在这里没有确定, 所有具有相同最小值解  $\hat{q}(\mathbf{x})$  的泛函被认为是等价的。

公理化推导的目的就是要对算子“ $\hat{q}$ ”提出某些公理性的假设, 然后以此来推导泛函应取的形式。Shore 和 Johnson 证明, 如果算子“ $\hat{q}$ ”满足以下 4 条公理, 则  $F(q(\mathbf{x}), p(\mathbf{x}))$  必取鉴别信息的形式。这 4 条公理分别是:

## (1) 唯一性公理

对于 "  $p(\mathbf{x}) \in Q$  和  $I = \{q^*(\mathbf{x}) \in Q\}$  , 其中  $Q_1 \subset Q$ , 算子 "  $T$  " 给出的  $\hat{q}(\mathbf{x}) = p(\mathbf{x}) \mid I$  是唯一的。

## (2) 不变性公理

令  $T$  是由  $\mathbf{x}$  到  $\mathbf{y}$  的坐标变换, 在此变换下, 密度函数为

$$(Tq)(\mathbf{y}) = |J|^{-1} q(\mathbf{x}) \quad (7.26)$$

其中  $J = \left| \frac{\partial \mathbf{y}}{\partial \mathbf{x}} \right|$  是雅可比行列式。我们用  $TQ$  表示对应于  $q(\mathbf{x}) \in Q$  的  $Tq(\mathbf{x})$  的集合, 用  $TQ_1 \subset TQ$  表示对应于  $Q_1 \subset Q$  的集合, 则对任意  $p(\mathbf{x}) \in Q$  和  $I = \{q^*(\mathbf{x}) \in Q_1\}$ , 应有

$$(Tp)(\mathbf{y}) = (TI)(\mathbf{y}) = T(p(\mathbf{x}) \mid I) \quad (7.27)$$

其中

$$TI = \{Tq^*(\mathbf{x}) \mid (TQ_1)\} \quad (7.28)$$

## (3) 系统独立性公理

设有随机变量  $X_1$  和  $X_2$ , 各自的取值集合为  $D_1$  和  $D_2$ 。令  $p_1(\mathbf{x}) \in Q_1$ ,  $p_2(\mathbf{x}) \in Q_2$  为先验概率密度函数,  $I_1 = \{q^*(\mathbf{x}) \in Q_1\}$  和  $I_2 = \{q^*(\mathbf{x}) \in Q_2\}$  是对这两个系统的已知的约束条件, 其中  $Q_1 \subset Q$ ,  $Q_2 \subset Q$ 。则应有

$$(p_1(\mathbf{x}) p_2(\mathbf{x})) \mid (I_1 \cap I_2) = (p_1(\mathbf{x}) \mid I_1)(p_2(\mathbf{x}) \mid I_2) \quad (7.29)$$

## (4) 子集独立性公理

设  $S_1, S_2, \dots, S_N$  是  $D$  的不相交子集, 它们满足

$$S_1 \cup S_2 \cup \dots \cup S_N = D$$

$$S_i \cap S_j = \emptyset, \quad i \neq j, \quad i, j = 1, 2, \dots, N$$

$p(\mathbf{x}) \in Q$  是已知的先验概率密度函数。  $X$  的真实密度函数  $q^*(\mathbf{x})$  在各子集上的条件概率密度函数记作  $q^*(\mathbf{x}) \mid S_n$ , 则

$$q^*(\mathbf{x}) \mid S_n = q^*(\mathbf{x} \mid \mathbf{x} \in S_n) = \frac{q^*(\mathbf{x})}{\int_{S_n} q^*(\mathbf{x}) d\mathbf{x}} \quad (7.30)$$

$I_n$  是对条件概率密度函数的约束, 即

$$I_n = \{q^*(\mathbf{x}) \mid S_n \mid Q_n\} \quad (7.31)$$

其中  $Q_n \subset Q$ ,  $Q_n$  是在  $S_n$  子集上的密度函数的集合。令  $M = \{q^*(\mathbf{x}) \mid \mu\}$  是关于  $q^*(\mathbf{x})$  在各子集的概率的信息,  $\mu$  是满足条件

$$\int_{S_n} q(\mathbf{x}) d\mathbf{x} = m_n, \quad n = 1, 2, \dots, N \quad (7.32)$$

及

$$m_n = 1$$

的概率密度函数的集合。则

$$(p(\mathbf{x}) \mid (I \cup M)) * S_n = (p(\mathbf{x}) * S_n) \mid I_n \quad (7.33)$$

其中  $I = I_1 \cup I_2 \cup I_3 \cup \dots \cup I_N$ 。

我们对上述公理分别作一些必要的解释。

唯一性公理是要求解是唯一的。不变性公理是指坐标变换下解的不变性,它要求先变换再求解与先求解再作变换所得的结果是相同的。系统独立性是针对由若干随机变量组成联合系统时求解过程中会发生的问题而提出的,此时先验概率密度和约束条件都有两种表示形式:

(1) 按联合系统的各组成系统进行表示,如先验概率为  $p_1(\mathbf{x})$  和  $p_2(\mathbf{x})$ , 约束条件为  $I_1 = (q^*(\mathbf{x}) \mid Q_{I_1})$  和  $I_2 = (q^*(\mathbf{x}) \mid Q_{I_2})$ 。

(2) 按联合系统进行表示,如先验概率密度为  $p(\mathbf{x}, \mathbf{y}) = p_1(\mathbf{x}) p_2(\mathbf{y})$ , 约束条件  $I_1$  和  $I_2$  可以在两维空间中表示,即用  $I = I_1 \cup I_2 = \{I_1 = (q^*(\mathbf{x}, \mathbf{y}) \mid Q_{I_1}), I_2 = (q^*(\mathbf{x}, \mathbf{y}) \mid Q_{I_2})\}$  来表示。

这样我们就可以用两种方法求解,由前法得到  $\hat{q}_1(\mathbf{x})$  和  $\hat{q}_2(\mathbf{x})$ , 由后法得到  $\hat{q}(\mathbf{x}, \mathbf{y})$ , 我们自然要求所得到的解相同, 即

$$\hat{q}(\mathbf{x}, \mathbf{y}) = \hat{q}_1(\mathbf{x}) \hat{q}_2(\mathbf{y}) \quad (7.34)$$

此即式(7.29)。

子集独立性是针对集合  $D$  被分成若干互不相交子集的情况而提出的,此时的约束条件可能是对各子集上的条件概率密度函数进行约束,这样我们就又有两种解法:

(1) 分别求解各子集上的条件概率密度函数, 即由  $\hat{q}_n(\mathbf{x}) = (p(\mathbf{x}) * S_n) \mid I_n$  求  $\hat{q}_n(\mathbf{x})$ 。

(2) 先求解总的概率密度函数, 然后获得各子集上的条件概率密度函数, 即先按  $p(\mathbf{x})$  和  $I = I_1 \cup I_2 \cup I_3 \cup \dots \cup I_N$  求得  $\hat{q}(\mathbf{x}) = p(\mathbf{x}) \mid I$ , 再求  $\hat{q}(\mathbf{x}) * S_n$ , 此时自然要求

$$\hat{q}_n(\mathbf{x}) = (p(\mathbf{x}) * S_n) \mid I_n = \hat{q}(\mathbf{x}) * S_n = (p(\mathbf{x}) \mid I) * S_n \quad (7.35)$$

至于进一步的附加信息  $M = (q^*(\mathbf{x}) \mid \mu)$  只是给出随机变量处在子集  $S_n$  的概率  $m_n$ , 这并不影响随机变量在子集  $S_n$  上的条件概率分布密度函数, 因此由式(7.35)有

$$(p(\mathbf{x}) \mid (I - M)) * S_n = (p(\mathbf{x}) * S_n) \mid I_n$$

下面我们来进行最小鉴别信息原理的公理化推导,即若算子“ $*$ ”满足上述 4 条公理,则必然导致最小鉴别信息原理。

证明 我们分 3 步来进行最小鉴别信息原理的公理化推导。

(1) 由子集独立性公理和不变性公理证明泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  只能取下述形式

$$F(q(\mathbf{x}), p(\mathbf{x})) = \int_D f(q(\mathbf{x}), p(\mathbf{x})) d\mathbf{x} \quad (7.36)$$

为了证明此结论,我们先引入引理。

引理 7.1 设  $S_1, S_2, \dots, S_N$  是互不相交子集,其并为  $D$ ,  $\hat{q}(\mathbf{x})$  是随机变量在  $D$  上的概率密度函数的解,即  $\hat{q}(\mathbf{x}) = p(\mathbf{x}) \mid (I - M)$ ,  $\hat{q}(\mathbf{x}) \mid Q$ , 且此解满足子集独立性公理,则概率密度函数  $\hat{q}(\mathbf{x})$  在子集  $S_n$  上的分布  $\hat{q}(\mathbf{x} \mid S_n)$  与  $q(\mathbf{x} \mid S_n)$ ,  $p(\mathbf{x} \mid S_n)$  以及  $N$  无关。

证明 设

$$\hat{q}_n(\mathbf{x}) = (p(\mathbf{x}) * S_n) \mid I_n \quad (7.37)$$

则  $\hat{q}_n(\mathbf{x})$  是在子集中求得的子集上的概率密度函数的解。

由于  $p(\mathbf{x}) * S_n$  只与  $p(\mathbf{x})$  在子集  $S_n$  上的值  $p(\mathbf{x} \mid S_n)$  有关,所以  $\hat{q}_n(\mathbf{x})$  也只与  $p(\mathbf{x} \mid S_n)$  有关。同时,  $\hat{q}_n(\mathbf{x})$  是子集  $S_n$  上的解,所以  $\hat{q}_n(\mathbf{x})$  不会与  $\hat{q}(\mathbf{x} \mid S_n)$  有关。

由子集独立性公理式(7.32)有

$$\hat{q}(\mathbf{x}) = m_n \hat{q}_n(\mathbf{x}), \text{ 当 } \mathbf{x} \in S_n \text{ 时} \quad (7.38)$$

证毕

所以  $\hat{q}(\mathbf{x} \mid S_n)$  与  $\hat{q}(\mathbf{x}) \mid S_n$  及  $p(\mathbf{x} \mid S_n)$  无关,当然也与  $N$  无关。

引理 7.2 设  $S_1, S_2, \dots, S_N$  为  $D$  中互不相交子集,其并为  $D$ 。已知先验概率分布密度  $p(\mathbf{x})$  及解  $\hat{q}(\mathbf{x}) = p(\mathbf{x}) \mid I$ , 且  $\hat{q}(\mathbf{x})$  满足不变性公理。令

$$p_n = \int_{S_n} p(\mathbf{x}) d\mathbf{x}, \quad \hat{q}_n = \int_{S_n} \hat{q}(\mathbf{x}) d\mathbf{x} \quad (7.39)$$

又设  $p(\mathbf{x})$  在各子集内保持不变,即  $p(\mathbf{x} \mid S_n)$  为常数,且约束条件

$$q(\mathbf{x}) f_m(\mathbf{x}) d\mathbf{x} = C_m \quad (7.40)$$

中的约束函数  $f_m(\mathbf{x})$  在各子集内也不变,则  $\hat{q}(\mathbf{x})$  在各子集内也保持不变,且泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  成为  $N$  对变量  $(q_n, p_n)$  的对称函数。

证明 由于  $f_m(\mathbf{x})$  在各子集内不变,所以由约束条件(7.40)可得

$$\sum_{n=1}^N \hat{q}_n f_{mn} = C_m \quad (7.41)$$

其中

$$\hat{q}_n = \int_{S_n} \hat{q}(\mathbf{x}) d\mathbf{x}, f_{mn} = f_m(\mathbf{x} \in S_n)$$

现设  $T$  是只将子集  $S_n$  内的点变换到子集  $S_n$  内且保持各子集测度不变的变换, 则在此变换下, 式(7.41)没有变化。另一方面, 由不变性公理式(7.27)可知解  $\hat{q}(\mathbf{x})$  也不变, 但这只有在  $\hat{q}(\mathbf{x} \in S_n)$  为常数时才有可能。因此,  $F(q(\mathbf{x}), p(\mathbf{x}))$  成为  $2N$  个变量  $q_1, q_2, \dots, q_N$  和  $p_1, p_2, \dots, p_N$  的函数, 即

$$F(q(\mathbf{x}), p(\mathbf{x})) = F(q_1, q_2, \dots, q_N, p_1, p_2, \dots, p_N)$$

为证明其对称性现对各子集进行置换排列, 得

$$F(q(\mathbf{x}), p(\mathbf{x})) = F(q_{(1)}, q_{(2)}, \dots, q_{(N)}, p_{(1)}, p_{(2)}, \dots, p_{(N)})$$

按不变性公理,  $F(q(\mathbf{x}), p(\mathbf{x}))$  的最小值解  $\hat{q}(\mathbf{x})$  应不变。由此推理, 若取所有可能的排列并取其平均作为泛函, 则此泛函必对称, 且其解仍相同, 所以,  $F(q(\mathbf{x}), p(\mathbf{x}))$  必等价于此  $N$  对变量  $(q_n, p_n)$  的对称函数。证毕

由引理 7.1 和 7.2, 我们可以得到下述定理 7.1。

**定理 7.1** 设  $S_1, S_2, \dots, S_N$  为互不相交子集, 其并为  $D$ , 先验概率密度函数  $p(\mathbf{x})$  在各子集内为常数, 约束条件中约束函数在各子集内也为常数, 且  $F(q(\mathbf{x}), p(\mathbf{x}))$  满足唯一性、不变性和子集独立性。则泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  与下述形式的函数等价:

$$F(q(\mathbf{x}), p(\mathbf{x})) = \sum_{n=1}^N f(q_n, p_n) \quad (7.42)$$

当  $D$  的不相交子集数不断增加, 各子集不断缩小时, 上述和式转化为积分

$$F(q(\mathbf{x}), p(\mathbf{x})) = \int_D f(q(\mathbf{x}), p(\mathbf{x})) d\mathbf{x} \quad (7.43)$$

在引理 7.1 和 7.2 中, 我们已经证明  $F(q(\mathbf{x}), p(\mathbf{x}))$  是  $\{(q_n, p_n)\}$  的对称函数, 式(7.43)则是这种对称函数的最简形式。但是, 对此定理的严格证明需要繁琐和冗长的推导, 在此略去。

(2) 在式(7.43)的基础上, 进一步求函数  $f(q(\mathbf{x}), p(\mathbf{x}))$  的形式, 从而求得泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  的形式, 这就是下述定理。

**定理 7.2** 设泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  满足唯一性、不变性和子集独立性, 则必有某函数  $h(\cdot)$ , 使  $F(q(\mathbf{x}), p(\mathbf{x}))$  等价于下述形式的泛函:

$$F(q(\mathbf{x}), p(\mathbf{x})) = \int_D q(\mathbf{x}) h(q(\mathbf{x}) / p(\mathbf{x})) d\mathbf{x} \quad (7.44)$$

**证明** 由定理 7.1 知道,  $F(q(\mathbf{x}), p(\mathbf{x}))$  可表示成

$$F(q(\mathbf{x}), p(\mathbf{x})) = \int_D f(q(\mathbf{x}), p(\mathbf{x})) d\mathbf{x}$$

现考虑新的约束条件

$$\int_D q(\mathbf{x}) a(\mathbf{x}) d\mathbf{x} = 0 \quad (7.45)$$

则由变分法可知满足上式的新的解应满足

$$+ a(\mathbf{x}) + g(q(\mathbf{x}), p(\mathbf{x})) = 0 \quad (7.46)$$

其中  $g(q(\mathbf{x}), p(\mathbf{x}))$  为  $f(q(\mathbf{x}), p(\mathbf{x}))$  对  $q(\mathbf{x})$  的微分, 即

$$g(q(\mathbf{x}), p(\mathbf{x})) = \frac{\partial}{\partial q(\mathbf{x})} f(q(\mathbf{x}), p(\mathbf{x})) \quad (7.47)$$

若令  $\mathbf{T}$  为由  $\mathbf{x}$  到  $\mathbf{y}$  的变换, 则经变换后的先验概率分布密度函数为

$$p(\mathbf{y}) = |\mathbf{J}|^{-1} p(\mathbf{x}) \quad (7.48)$$

而约束函数经变量变换后为

$$a(\mathbf{y}) = a(\mathbf{x}) \quad (7.49)$$

所以变换后的解  $\hat{q}(\mathbf{y}) = p(\mathbf{y}) \mathbf{T}$  应满足

$$+ a(\mathbf{y}) + g(\hat{q}(\mathbf{y}), p(\mathbf{y})) = 0 \quad (7.50)$$

此外, 按不变性公理可得

$$\hat{q}(\mathbf{y}) = |\mathbf{J}|^{-1} \hat{q}(\mathbf{x}) \quad (7.51)$$

将式(7.48)、(7.49)、(7.51)代入式(7.50), 得

$$+ a(\mathbf{x}) + g(|\mathbf{J}|^{-1} \hat{q}(\mathbf{x}), |\mathbf{J}|^{-1} p(\mathbf{x})) = 0 \quad (7.52)$$

结合式(7.52)和式(7.46), 即得

$$g(|\mathbf{J}|^{-1} \hat{q}(\mathbf{x}), |\mathbf{J}|^{-1} p(\mathbf{x})) = g(q(\mathbf{x}), p(\mathbf{x})) + (-1) a(\mathbf{x}) + (-1) \quad (7.53)$$

现在令  $S_1, S_2, \dots, S_N$  是  $D$  的互不相交子集, 且并为  $D$ , 先验概率密度函数  $p(\mathbf{x})$  及约束函数  $a(\mathbf{x})$  在各子集内为常数。则由引理 7.1 和 7.2 可知, 式(7.53)的右端在各子集内均为常数, 而在该式的左端, 雅可比行列式可随变换  $\mathbf{T}$  的变化而变化, 因此, 要使式(7.53)成立只有一个可能, 即函数  $g(q(\mathbf{x}), p(\mathbf{x}))$  取  $g(q(\mathbf{x}) | p(\mathbf{x}))$  的形式, 在这种情况下, 由式(7.47)可得

$$f(q(\mathbf{x}), p(\mathbf{x})) = q(\mathbf{x}) h(q(\mathbf{x}) | p(\mathbf{x})) + v(p(\mathbf{x})) \quad (7.54)$$

将此式代入式(7.43), 即得

$$F(q(\mathbf{x}), p(\mathbf{x})) = \int_D q(\mathbf{x}) h(q(\mathbf{x}) | p(\mathbf{x})) d\mathbf{x} + \int_D v(p(\mathbf{x})) d\mathbf{x} \quad (7.55)$$

由于上式右端的第二项是与  $q(\mathbf{x})$  无关的常数, 不会影响求  $F(q(\mathbf{x}), p(\mathbf{x}))$  的最

小值,因此可以略去,于是就得到我们所要的式(7.44)。

证毕

(3) 证明  $F(q(\mathbf{x}), p(\mathbf{x}))$  即为鉴别信息。

**定理 7.3** 设泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  满足唯一性、不变性、子集独立性和系统独立性,则此泛函与鉴别信息等价。

**证明** 在唯一性、不变性和子集独立性三条公理下,我们已经证明泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$  必与式(7.44)形式的泛函等价。

现设有两个随机变量  $X_1, X_2$  及相应的集合  $D_1, D_2$ , 未知的真实分布  $q_1(\mathbf{x}) \in Q, q_2(\mathbf{x}) \in Q$ , 先验概率分布密度函数  $p_1(\mathbf{x}), p_2(\mathbf{x})$  和已知的约束  $I_1, I_2$ , 其中  $I_1, I_2$  分别是

$$\int_{D_1} q_1(\mathbf{x}) a_1(\mathbf{x}) d\mathbf{x} = 0 \quad (7.56a)$$

$$\int_{D_2} q_2(\mathbf{x}) a_2(\mathbf{x}) d\mathbf{x} = 0 \quad (7.56b)$$

则按式(7.44)及变分法原理,其解应该满足

$$\lambda_n + \int_{D_n} a_n(\mathbf{x}) + u(r_n(\mathbf{x})) = 0, \quad n = 1, 2 \quad (7.57)$$

其中  $\lambda_n$  和  $\lambda_n$  分别是对应于约束条件

$$\int_{D_n} q_n(\mathbf{x}_n) d\mathbf{x}_n = 1, \quad n = 1, 2 \quad (7.58)$$

和式(7.56)的拉格朗日乘子,而

$$r_n(\mathbf{x}) = \frac{q_n(\mathbf{x})}{p_n(\mathbf{x})}, \quad n = 1, 2 \quad (7.59)$$

$$u(r) = h(r) + r \frac{d}{dr} h(r) \quad (7.60)$$

另一方面,这两个随机变量又可以用联合概率分布密度函数  $q(\mathbf{x}, \mathbf{x}) \in Q$  和  $p(\mathbf{x}, \mathbf{x})$  来描述。由于  $p_1(\mathbf{x})$  和  $p_2(\mathbf{x})$  没有提供任何关于  $X_1$  和  $X_2$  之间关系的知识,所以

$$p(\mathbf{x}, \mathbf{x}) = p_1(\mathbf{x}) p_2(\mathbf{x})$$

在联合概率系统中约束条件可写成

$$\int_{D_1} \int_{D_2} q(\mathbf{x}, \mathbf{x}) d\mathbf{x} d\mathbf{x} = 1 \quad (7.61a)$$

$$\int_{D_1} \int_{D_2} q(\mathbf{x}, \mathbf{x}) a_n(\mathbf{x}) d\mathbf{x} d\mathbf{x} = 0, \quad n = 1, 2 \quad (7.61b)$$

此时解应满足

$$\lambda_1 + \int_{D_1} a_1(\mathbf{x}) + \lambda_2 + \int_{D_2} a_2(\mathbf{x}) + u(r(\mathbf{x}, \mathbf{x})) = 0 \quad (7.62)$$



按系统独立性原理, 上述两个解应满足

$$q(\mathbf{x}, \mathbf{y}) = q(\mathbf{x})q(\mathbf{y})$$

于是有

$$r(\mathbf{x}, \mathbf{y}) = n(\mathbf{x})n(\mathbf{y}) \quad (7.63)$$

由此可得

$$\begin{aligned} u(n(\mathbf{x})n(\mathbf{y})) - u(n(\mathbf{x})) - u(n(\mathbf{y})) \\ = \alpha_1 + \alpha_2 - \alpha_1 + (\alpha_1 - \alpha_1)\alpha(\mathbf{x}) + (\alpha_2 - \alpha_2)\alpha(\mathbf{y}) \end{aligned}$$

先取此方程对  $\mathbf{x}$  的微分, 再取其结果对  $\mathbf{y}$  的微分, 即得

$$u(n(\mathbf{x})n(\mathbf{y}))n(\mathbf{x})n(\mathbf{y}) + u(n(\mathbf{x})n(\mathbf{y})) = 0 \quad (7.64)$$

在适当选择先验概率分布密度函数和约束条件下, 可使对  $s > 0$ , 有

$$n(\mathbf{x})n(\mathbf{y}) = s$$

这说明函数  $u(\cdot)$  满足

$$su(s) + u(s) = 0 \quad (7.65)$$

此方程的一般解是

$$u(s) = A \log s + B \quad (7.66)$$

其中  $A, B$  是任意常数。由式(7.60)和式(7.66)得

$$h(r) + r \frac{d}{dr} h(r) = A \log r + B \quad (7.67)$$

这是关于  $h(r)$  的微分方程, 其解为

$$h(r) = A \log r + \frac{C}{r} - A + B \quad (7.68)$$

将  $h(r)$  代入式(7.44), 就得

$$F(q(\mathbf{x}), p(\mathbf{x})) = A \int q(\mathbf{x}) \log \frac{q(\mathbf{x})}{p(\mathbf{x})} d\mathbf{x} + (C + B - A) \quad (7.69)$$

上式表明, 只要  $A > 0$ , 此泛函与鉴别信息将有相同的最小值点。至此, 我们证明了如果存在泛函  $F(q(\mathbf{x}), p(\mathbf{x}))$ , 其最小值点的解满足唯一性、不变性、子集独立性和系统独立性 4 条公理, 则此泛函必等价于鉴别信息。证毕

我们不难由鉴别信息的基本性质证明鉴别信息取最小所得的解确实满足上述 4 条公理, 因此, 综合此项和前述的证明, 我们知道鉴别信息(或其等价泛函)且只有鉴别信息取最小所得的解才能满足 4 条公理, 这意味着其他泛函取最小所得的解将不满足上述 4 条公理的一部分或全部。这 4 条公理有时统称一致性公理, 因为它要求不同计算途径下所得结果的一致性。

### 7.3.2 最大熵原理的推导

我们在节 7.1 中已经说过, 最大熵原理是最小鉴别信息原理的特例, 所以, 我们可以用类似于前面的方法以公理化的形式推导最大熵原理。二者的主要差别表现在如下两点:

(1) 由于最大熵原理主要用于离散分布和对先验分布完全无知的情况, 所以先验概率密度函数在运算中将不再出现。

(2) 变换下的不变性公理在此时蜕化为置换下的不变性公理。

在作了上述改动后, 我们可以证明能使 4 条公理满足的算子必然相当于使下述泛函取最小:

$$F(q) = A \sum_{k=1}^K q(a_k) \log q(a_k) - KA + B \quad (7.70)$$

其中,  $\{a_k\}$  是随机变量  $X$  取值的集合,  $A, B$  是常数。因此, 这相当于使熵

$$H(X) = - \sum_{k=1}^K q(a_k) \log q(a_k)$$

取最大。

最大熵解显然满足唯一性、置换不变性、子集独立性和系统独立性公理。因此这一证明也就意味着在离散分布和对先验分布无知的情况下, 只有最大熵原理才能提供满足这些公理的解。

## 7.4 最小失真意义下的最大熵原理与最小鉴别信息原理

前面三节对最大熵原理与最小鉴别信息原理的讨论都是建立在统计学的基础上的, 所要解决的问题是在给定先验概率密度函数及对概率密度函数的若干约束条件下, 对真实的分布给出一个最佳的估计或最优的解。但是, 这两个原理对于非概率密度函数、非统计问题也仍然有效, 这就是我们在这节中要讨论的最小失真意义下的最大熵原理与最小鉴别信息原理。为此我们讨论下述问题。

设有定义在  $n$  维欧氏空间  $\mathbf{R}^n$  中域  $D$  上的某未知函数  $R(\mathbf{x})$ ,  $R(\mathbf{x}) \in Q$ , 这里的  $Q$  是全部恒正、有界且可积的所有容许函数的集合。对此  $R(\mathbf{x})$  的先验估计为  $p(\mathbf{x})$ , 且已知  $R(\mathbf{x})$  的若干约束条件为

$$C_m = \int R(\mathbf{x}) g_m(\mathbf{x}) d\mathbf{x}, \quad m = 1, 2, \dots, M \quad (7.71)$$

但由于约束条件的数量有限,不足以唯一地确定  $R(\mathbf{x})$ 。

现在我们要在所有与约束条件一致的容许函数集合  $Q$  中找出一个函数  $\hat{q}(\mathbf{x})$ , 作为对  $R(\mathbf{x})$  的后验估计。我们希望  $\hat{q}(\mathbf{x})$  在某种意义上是最优的。在实际问题中,  $R(\mathbf{x})$  可能是系统的输入, 约束条件可能就是测量结果。

对这一问题的一般解决方法是先定义某种具体形式的失真  $D(q(\mathbf{x}), p(\mathbf{x}))$ 。  $D(\cdot, \cdot)$  的一般形式是

$$D(q(\mathbf{x}), p(\mathbf{x})) = \int f(q(\mathbf{x}), p(\mathbf{x})) w(\mathbf{x}) d\mathbf{x} \quad (7.72)$$

其中  $w(\mathbf{x})$  是恒正函数。然后根据先验的估计  $p(\mathbf{x})$  和约束条件, 在集合  $Q$  中选择这样的函数  $\hat{q}(\mathbf{x})$  作为对  $R(\mathbf{x})$  的后验估计。此函数  $\hat{q}(\mathbf{x})$  在所有与约束条件一致的容许函数中与  $p(\mathbf{x})$  有最小的失真, 即

$$D(\hat{q}(\mathbf{x}), p(\mathbf{x})) = \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) \quad (7.73a)$$

$$\hat{q}(\mathbf{x}) = \text{Arg} \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) \quad (7.73b)$$

这一准则从已知先验估计  $p(\mathbf{x})$  的角度来看是合理的, 但是尚不理想。不理想之处在于  $q(\mathbf{x})$  和被估计对象  $R(\mathbf{x})$  之间的失真在求解中没有任何反映。

### 7.4.1 方向正交与投影失真

为使上述问题中所谓的解不但与  $p(\mathbf{x})$  有最小的失真, 而且能反映它与  $R(\mathbf{x})$  之间的失真, 让我们对上述解决方法作进一步的分析。

设在上述问题中, 先验估计  $p(\mathbf{x})$ 、约束函数集  $\{g_m(\mathbf{x})\}$  以及失真的具体形式已经给定, 则对每一组约束数据  $\{C_m, m = 1, 2, \dots, M\}$  和  $p(\mathbf{x})$ , 在令  $D(q(\mathbf{x}), p(\mathbf{x}))$  最小时都可以有一个解, 这些解组成集合  $T$ 。集合  $T$  与  $p(\mathbf{x})$ ,  $D(\cdot, \cdot)$  以及  $\{g_m(\mathbf{x}), m = 1, 2, \dots, M\}$  有关, 但与  $\{C_m, m = 1, 2, \dots, M\}$  无关。该问题的解是  $Q_I$  中与  $p(\mathbf{x})$  有最小失真的函数, 即

$$\hat{q}(\mathbf{x}) = \text{Arg} \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) \quad (7.74)$$

但我们并不知道此函数  $\hat{q}(\mathbf{x})$  与  $R(\mathbf{x})$  之间的失真。按照上面的分析, 此解  $\hat{q}(\mathbf{x})$  也是集合  $T$  中的函数。既然这样, 我们有理由希望  $\hat{q}(\mathbf{x})$  也是  $T$  中与  $R(\mathbf{x})$  有最小失真的函数, 即我们希望

$$\text{Arg} \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) = \hat{q}(\mathbf{x}) = \hat{t}(\mathbf{x}) = \text{Arg} \min_{t(\mathbf{x}) \in T} D(R(\mathbf{x}), t(\mathbf{x})) \quad (7.75)$$

这一要求在一般情况下不一定能达到,为此,我们给出下面的定义。

设  $Q_I$  是满足约束条件(7.71)的容许函数集合,  $T$  是给定  $p(\mathbf{x})$ 、约束函数集合和距离  $D(\cdot, \cdot)$  的条件下所有最优解的集合。若此最优解满足

$$\text{Arg} \min_{t(\mathbf{x}) \in T} D(R(\mathbf{x}), t(\mathbf{x})) = \hat{t}(\mathbf{x}) = \hat{q}(\mathbf{x}) = \text{Arg} \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) \quad (7.76)$$

则称此失真  $D$  是满足方向正交原理的失真。

方向正交是 Hilbert 空间中一般正交概念的推广。若失真  $D$  取均方差的形式,则

$$D(q(\mathbf{x}), p(\mathbf{x})) = \frac{1}{2} \int (q(\mathbf{x}) - p(\mathbf{x}))^2 d\mathbf{x} \quad (7.77)$$

此时最优解满足变分法中的欧拉方程,即有

$$\hat{q}(\mathbf{x}) - p(\mathbf{x}) = \sum_{m=1}^M g_m(\mathbf{x}) \quad (7.78)$$

因此,所有最优解  $\hat{q}(\mathbf{x})$  的集合  $T$  是由线性子空间的平移组成的仿射集,在这种情况下,方向正交要求  $\hat{q}(\mathbf{x})$  满足

$$\begin{aligned} \hat{t}(\mathbf{x}) &= \text{Arg} \min_{t(\mathbf{x}) \in T} D(R(\mathbf{x}), t(\mathbf{x})) = \text{Arg} \min_{t(\mathbf{x}) \in T} \frac{1}{2} \int (R(\mathbf{x}) - t(\mathbf{x}))^2 d\mathbf{x} \\ &= \hat{q}(\mathbf{x}) = \text{Arg} \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) = \text{Arg} \min_{q(\mathbf{x}) \in Q_I} \frac{1}{2} \int (q(\mathbf{x}) - p(\mathbf{x}))^2 d\mathbf{x} \end{aligned} \quad (7.79)$$

这相当于要求  $R(\mathbf{x}) - \hat{q}(\mathbf{x})$  与  $T$  正交,  $\hat{q}(\mathbf{x}) - p(\mathbf{x})$  与  $Q_I$  正交。因而方向正交蜕化为 Hilbert 空间意义下的一般正交。而且我们看到,由于  $R(\mathbf{x}) - \hat{q}(\mathbf{x})$  与所有约束函数  $g_m(\mathbf{x})$  的内积为零,所以均方差形式的失真满足方向正交性。

如前所述,满足方向正交原理的失真有一个重要的性质:对给定的  $p(\mathbf{x})$  和约束数据集  $\{C_m, m=1, 2, \dots, M\}$ , 解  $\hat{q}(\mathbf{x})$  是  $T$  中与  $R(\mathbf{x})$  有最小失真的函数。如果我们把  $R(\mathbf{x})$  与  $\hat{q}(\mathbf{x})$  之间的失真看作一种距离,则意味着  $\hat{q}(\mathbf{x})$  是  $T$  中与  $R(\mathbf{x})$  有最短距离的函数。因此我们可以把  $\hat{q}(\mathbf{x})$  看成是  $R(\mathbf{x})$  在  $T$  上的投影;而  $R(\mathbf{x})$  与  $\hat{q}(\mathbf{x})$  之间的这种失真就被称为投影失真。

更确切一点说,对于取式(7.72)形式的失真,在给定先验估计  $p(\mathbf{x})$ 、约束函数  $\{g_m(\mathbf{x}), m=1, 2, \dots, M\}$ 、约束数据  $\{C_m, m=1, 2, \dots, M\}$  下,如果其解  $\hat{q}(\mathbf{x})$  满

足方向正交原理,则此失真被称为投影失真。

## 7.4.2 投影失真的一般形式

对于失真来说,投影失真显然是一种具有良好性质的失真。我们在上面也已经举例说明均方差形式的失真是一种投影失真。现在我们要问,投影失真一般应该具有什么形式,或者说在式(7.72)中被积函数  $f(y, z)$  应该具有什么形式?

为了推导  $f(y, z)$  应取的形式,我们假定  $f(y, z)$  及其偏导数  $f_y$ 、 $f_z$ 、 $f_{yy}$ 、 $f_{zy}$  在第一象限存在且连续,同时为保证  $D(q(\mathbf{x}), p(\mathbf{x})) \geq D(p(\mathbf{x}), p(\mathbf{x}))$ , 对此函数及其偏导数附加以下必要的限制:

(1) 当  $z = y, y > 0$  时,  $f(y, z) = 0$ 。此条件保证  $D(p(\mathbf{x}), p(\mathbf{x})) = 0$ ;

(2) 当  $z = y, y > 0$  时,  $f_y(y, z) = 0$ 。按欧拉方程,此条件保证  $D(q(\mathbf{x}), p(\mathbf{x}))$  在  $(p(\mathbf{x}), p(\mathbf{x}))$  处有极值。

(3) 当  $y > 0, z > 0$  时,  $f_{yy}(y, z) > 0$ 。此条件保证  $D(q(\mathbf{x}), p(\mathbf{x}))$  是  $q(\mathbf{x})$  的严格下凸函数,从而保证解的唯一性。

在上述条件下,首先可有下列引理。

**引理 7.3** 设  $D$  是投影失真,则必有

$$f_{zyy}(y, z) = 0, \text{ 当 } y > 0, z > 0 \text{ 时} \quad (7.80)$$

此引理的证明此处略去。

**定理 7.4** 当且仅当  $f(y, z)$  具有形式

$$f(y, z) = J(y) - J(z) + (z - y)j(z) \quad (7.81)$$

其中  $j(u) = \frac{dJ}{du}$ 。且  $j(u) = \frac{dj}{du}$  存在、连续且恒正时,  $f(y, z)$  对应的失真量度  $D$  才是投影失真。

**证明** (1) 证明若  $D$  是投影失真,则可以得到  $f(y, z)$  的形式(7.81)。

设  $D$  是投影失真,则由引理 7.3 可知  $f_{zyy}(y, z) = 0$ , 故  $f_z$  是  $y$  的线性函数, 于是有

$$f(y, z) = - yj(z) + L(z) + M(y) \quad (7.82)$$

由条件(1),  $f(y, y) = 0$ , 则有

$$L(y) = yj(y) - M(y) \quad (7.83)$$

由条件(2),  $f_y(y, y) = 0$ , 则有

$$M(y) = j(y) \text{ 或 } M(y) = J(y) \quad (7.84)$$

于是有

$$\begin{aligned} f(y, z) &= -yj(z) + L(z) + M(y) \\ &= -yj(z) + zj(z) - J(z) + J(y) \\ &= J(y) - J(z) + (z - y)j(z) \end{aligned}$$

此即式(7.81)。

由假设, 偏导数  $f_{yy}$  存在且连续, 得  $j(u)$  存在且连续。再由条件(3), 得  $j(u)$  恒正。

(2) 证明若  $f(y, z) = J(y) - J(z) + (z - y)j(z)$ , 推导出  $D$  为投影失真。

设  $f(y, z)$  满足式(7.81)及相应的条件, 则  $D(R(\mathbf{x}), t(\mathbf{x}))$  可写成

$$D(R(\mathbf{x}), t(\mathbf{x})) = \int [J(R(\mathbf{x})) - J(t(\mathbf{x})) + (t(\mathbf{x}) - R(\mathbf{x}))j(t(\mathbf{x}))] d\mathbf{x} \quad (7.85)$$

另一方面, 先验估计为  $p(\mathbf{x})$  时满足约束条件式(7.71)的最佳估计  $\hat{q}(\mathbf{x})$  满足变分法中的欧拉方程, 故

$$f_y(\hat{q}(\mathbf{x}), p(\mathbf{x})) = \sum_{m=1}^M g_m(\mathbf{x}) \quad (7.86)$$

但  $f_y(q(\mathbf{x}), p(\mathbf{x})) = j(q(\mathbf{x})) - j(p(\mathbf{x}))$ , 所以

$$j(\hat{q}(\mathbf{x})) = j(p(\mathbf{x})) + \sum_{m=1}^M g_m(\mathbf{x}) \quad (7.87)$$

注意到式(7.85)中的  $t(\mathbf{x}) \in T$ ,  $T$  是所有满足式(7.87)的解的集合, 即

$$j(t(\mathbf{x})) = j(p(\mathbf{x})) + \sum_{m=1}^M g_m(\mathbf{x})$$

所以, 式(7.85)可写成

$$\begin{aligned} & D(R(\mathbf{x}), t(\mathbf{x})) \\ &= \int [J(R(\mathbf{x})) - J(t(\mathbf{x})) + (t(\mathbf{x}) - R(\mathbf{x}))j(t(\mathbf{x}))] d\mathbf{x} \\ &= \int [J(\hat{q}(\mathbf{x})) - J(t(\mathbf{x})) + (t(\mathbf{x}) - \hat{q}(\mathbf{x}))j(t(\mathbf{x}))] d\mathbf{x} + \\ & \quad J(R(\mathbf{x})) - J(\hat{q}(\mathbf{x})) + (\hat{q}(\mathbf{x}) - R(\mathbf{x}))j(p(\mathbf{x})) + \sum_{m=1}^M g_m(\mathbf{x}) d\mathbf{x} \\ &= D(\hat{q}(\mathbf{x}), t(\mathbf{x})) + D(R(\mathbf{x}), \hat{q}(\mathbf{x})) \end{aligned}$$

式中  $\alpha_m$  是与某  $t(\mathbf{x})$  对应的参数, 但由于

$$(\alpha_m - \alpha_m)(\hat{q}(\mathbf{x}) - R(\mathbf{x}))g_m(\mathbf{x})d\mathbf{x} = 0$$

所以,上式的最后一个等号成立。

根据  $f(y, z)$  满足的条件即可知道  $D(R(\mathbf{x}), t(\mathbf{x}))$  仅在  $t(\mathbf{x}) = \hat{q}(\mathbf{x})$  才取唯一的极小值,此时  $D(\hat{q}(\mathbf{x}), t(\mathbf{x})) = D(\hat{q}(\mathbf{x}), \hat{q}(\mathbf{x})) = 0$ , 即

$$\text{Arg} \min_{t(\mathbf{x})} D(R(\mathbf{x}), t(\mathbf{x})) = \hat{q}(\mathbf{x}) = \text{Arg} \min_{q(\mathbf{x}) \in Q_I} D(q(\mathbf{x}), p(\mathbf{x})) \quad \text{证毕}$$

所以  $D$  为投影失真。

这样我们就最终得到投影失真的一般形式为

$$D(q(\mathbf{x}), p(\mathbf{x})) = \int [J(q(\mathbf{x})) - J(p(\mathbf{x})) + (p(\mathbf{x}) - q(\mathbf{x}))j(p(\mathbf{x}))]d\mathbf{x} \quad (7.88)$$

其中  $j(u)$  是某一选定的函数。当我们要求解属于容许函数集合  $Q$  时,函数  $j(u)$  的选择应满足条件:  $j(u)$  对应于  $u > 0$  区间所取的值域是全部实数域。这时,由式(7.87)得

$$\hat{q}(\mathbf{x}) = j^{-1} [j(p(\mathbf{x})) + \sum_{m=0}^M g_m(\mathbf{x})] \quad (7.89)$$

即可保证  $\hat{q}(\mathbf{x}) \in Q$ 。

### 7.4.3 最小失真准则与熵准则

我们在前面已经得到投影失真的一般形式。在这个一般形式中,函数  $j(u)$  可以有不同的选择。在某些  $j(u)$  函数下,所得的投影失真将具有和熵或鉴别信息完全相同的形式,从而使最大熵准则或最小鉴别信息准则具有最小失真的意义。

(1) 当  $j(u) = \log u$  时,有

$$J(u) = u \log u - u$$

于是

$$\begin{aligned} D(q(\mathbf{x}), p(\mathbf{x})) &= \int [q(\mathbf{x}) \log q(\mathbf{x}) - q(\mathbf{x}) - p(\mathbf{x}) \log p(\mathbf{x}) + p(\mathbf{x}) + (p(\mathbf{x}) \\ &\quad - q(\mathbf{x})) \log p(\mathbf{x})] d\mathbf{x} \\ &= \int q(\mathbf{x}) \log \frac{q(\mathbf{x})}{p(\mathbf{x})} d\mathbf{x} + \int (p(\mathbf{x}) - q(\mathbf{x})) d\mathbf{x} \end{aligned}$$

当  $q(\mathbf{x}), p(\mathbf{x})$  为概率分布密度函数时,则得

$$D(q(\mathbf{x}), p(\mathbf{x})) = \int q(\mathbf{x}) \log \frac{q(\mathbf{x})}{p(\mathbf{x})} d\mathbf{x} \quad (7.90)$$

可以看到,这一失真量度具有和鉴别信息完全相同的泛函形式。在这一失真量度下的最小失真准则就相当于最小鉴别信息准则。

进一步分析,当上式中的  $p(\mathbf{x})$  为均匀分布时,最小失真准则就相当于使  $-\int q(\mathbf{x}) \log q(\mathbf{x}) d\mathbf{x}$  为最大,因而即为最大熵准则。

(2) 当  $j(u) = -\frac{1}{u}$  时,有

$$J(u) = -\log u$$

于是

$$D(q(\mathbf{x}), p(\mathbf{x})) = \int -\log \frac{q(\mathbf{x})}{p(\mathbf{x})} + \frac{q(\mathbf{x})}{p(\mathbf{x})} - 1 d\mathbf{x} \quad (7.91)$$

可以看到,这一失真与语音信号处理中常用的 Itakura-Saito 失真具有相同的形式。当  $p(\mathbf{x})$  取均匀分布时,上述失真的最小化相当于使  $-\int \log q(\mathbf{x}) d\mathbf{x}$  取最大。这时的最小失真准则又与 Burg 在谱估计中所提到的最大熵准则一致,因为 Burg 的最大熵准则是使信号熵率的频域表示式取最大,即

$$\max \frac{1}{2\pi} \int_{-\pi}^{\pi} \log S(e^{j\omega}) d\omega$$

其中  $S(e^{j\omega})$  是信号的功率谱。

(3) 当  $j(u) = u$  时,则有

$$J(u) = \frac{u^2}{2}$$

于是

$$D(q(\mathbf{x}), p(\mathbf{x})) = \int \frac{1}{2} (q(\mathbf{x}) - p(\mathbf{x}))^2 d\mathbf{x} \quad (7.92)$$

此即我们熟悉的均方失真。

均方失真是一种投影失真,但不能用于概率分布密度函数的估计问题中,这是因为  $j(u) = u$  这一函数对应于  $u > 0$  的值域不是整个实数域,因而不能保证最优解的恒正性。尽管如此,均方失真在投影失真中仍具有重要的地位,下面的定理证明了这一点。

**定理 7.5** 如果投影失真相对于  $q(\mathbf{x})$  和  $p(\mathbf{x})$  是对称的,则此失真量度  $D(q(\mathbf{x}), p(\mathbf{x}))$  必为均方失真的倍数。

**证明** 假定  $q(\mathbf{x})$  和  $p(\mathbf{x})$  在定义域  $D$  上为常数,这时  $D(q(\mathbf{x}), p(\mathbf{x}))$  的对称性意味着函数  $f(y, z)$  对  $y, z$  的对称性,即



$$D(q(\mathbf{x}), p(\mathbf{x})) = D(p(\mathbf{x}), q(\mathbf{x})) \quad f(y, z) = f(z, y)$$

由式(7.81)得

$$J(y) - J(z) + (z - y)j(z) = J(z) - J(y) + (y - z)j(y)$$

即

$$J(y) - J(z) = \frac{(y - z)(j(y) + j(z))}{2} \quad (7.93)$$

取上式在  $y = y_0$  处对  $y$  的导数, 得

$$j(y_0) = \frac{(j(y_0) + j(z))}{2} + \frac{(y_0 - z)j(y_0)}{2}$$

即

$$j(z) = j(y_0) - y_0 j(y_0) + j(y_0)z \quad (7.94)$$

所以,  $j(z)$  是  $z$  的线性函数。将此函数简记成

$$j(z) = az + b \quad (7.95)$$

则有

$$J(z) = \frac{a}{2} z^2 + bz \quad (7.96)$$

于是

$$\begin{aligned} f(q(\mathbf{x}), p(\mathbf{x})) &= J(q(\mathbf{x})) - J(p(\mathbf{x})) + (p(\mathbf{x}) - q(\mathbf{x}))j(p(\mathbf{x})) \\ &= \frac{a}{2} q^2(\mathbf{x}) + b q(\mathbf{x}) - \frac{a}{2} p^2(\mathbf{x}) - b p(\mathbf{x}) + (p(\mathbf{x}) \\ &\quad - q(\mathbf{x}))(ap(\mathbf{x}) + b) \\ &= \frac{a}{2} (p(\mathbf{x}) - q(\mathbf{x}))^2 \end{aligned} \quad (7.97)$$

所以

$$D(q(\mathbf{x}), p(\mathbf{x})) = \int f(q(\mathbf{x}), p(\mathbf{x})) d\mathbf{x} = \frac{a}{2} \int (q(\mathbf{x}) - p(\mathbf{x}))^2 d\mathbf{x} \quad (7.98)$$

证毕

## 7.5 最大熵与最小鉴别信息原理的应用及其解的分布

### 7.5.1 最大熵与最小鉴别信息原理的应用

由于熵和鉴别信息在信息技术中具有普遍意义, 所以最大熵和最小鉴别信息原理在理论上也有普遍的适用性, 但是利用这两个原理进行优化时, 熵和鉴

别信息的计算都是比较繁重的。尽管现在已有一些成熟的算法,如最大熵求解时的剑桥算法等,但其运算量比用二次函数作准则的最优化运算量仍然要大得多,因此在实际问题中应该根据这两个原理的特点正确地加以应用。下面我们通过两个实例分别说明这两个原理在什么情况下应用才是必要和适当的,并能取得其他准则达不到的效果。

### 7.5.1.1 谱估计

根据测量到的一段数据对原信号的功率谱作出估计是在科学研究和工程设计中经常遇到的问题。根据稳恒随机过程的理论,稳恒随机信号的功率谱是其相关函数的傅立叶变换,所以若设已知信号在 $(-T, T)$ 间隔内的值,则首先可取这一有限长度信号在时间上的下述平均值作为随机过程相关函数的近似估计值:

$$R_T(\tau) = \frac{1}{2T} \int_{-T+\tau/2}^{+T-\tau/2} X(t+\tau/2) X(t-\tau/2) dt, \quad \text{当 } |\tau| < 2T \quad (7.99)$$

$$0, \quad \text{当 } |\tau| \geq 2T$$

由此可得功率谱  $S(\omega)$  的估计值为

$$S_T(\omega) = \int_{-2T}^{2T} R_T(\tau) e^{-j\omega\tau} d\tau \quad (7.100)$$

$S_T(\omega)$  的期望和方差为

$$E\{S_T(\omega)\} = S(\omega) * \frac{\sin^2 T\omega}{T^2} \quad (7.101)$$

$$\text{Var}\{S_T(\omega)\} = E^2\{S_T(\omega)\} \quad (7.102)$$

作为一个统计意义上可靠的估计,估计应是无偏的,且估计的方差应该很小。由式(7.101)可以看到此估计值的期望在  $T \rightarrow \infty$  时趋于无偏。如果  $T$  可以足够大,则无偏的要求可以满足。但估计的方差不管  $T$  值取多大都不会减小,所以这一估值实际上很难使用。

造成这一情况的主要原因是  $R_T(\tau)$  在接近  $\pm 2T$  时的值极不可靠,为减小其影响,最直接的方法是用满足以下条件的窗函数  $w(\tau)$  对  $R_T(\tau)$  进行加权:

$$w(\tau) = 0, \quad \text{当 } |\tau| > D, D \ll 2T \quad (7.103)$$

然后用加权后的相关函数估计值求其谱

$$S_w(\omega) = \int_{-2T}^{2T} [R_T(\tau) w(\tau)] e^{-j\omega\tau} d\tau$$

$$= \frac{1}{2} S_T(\omega) * W(\omega)$$

$$= \frac{1}{2} S(\omega) * \frac{\sin^2 T}{T} * W(\omega) \quad (7.104)$$

其中  $W(\omega)$  是  $w(t)$  的傅立叶变换。

$S_w(\omega)$  的期望和方差在  $T$  值很大时有

$$E\{S_w(\omega)\} = \frac{1}{2} S(\omega) * W(\omega) \quad (7.105)$$

$$\text{Var}\{S_w(\omega)\} = \frac{E_w}{T} S^2(\omega), \quad \frac{E_w}{2T} S^2(\omega), \quad \frac{1}{D} \quad (7.106)$$

其中 
$$E_w = \int_{-2T}^{2T} w^2(t) dt = \frac{1}{2} \int_{-\infty}^{+\infty} W^2(\omega) d\omega \quad (7.107)$$

式(7.106)表明如果让  $E_w$  保持不变, 而令  $T \rightarrow \infty$ , 则功率谱估计的方差可趋于零。但式(7.105)表明功率谱估计值方差的减小必然伴随着功率谱估计值分辨率的降低, 这一矛盾使这种方法陷入一种两难的处境。

1967 年 J. P. Burg 根据最大熵原理对谱估计问题提出了理想的解决方法。他不是用窗函数简单地减少相关函数估计值  $R_T(\tau)$  两侧不可靠数据给功率谱的影响, 而是根据已知的比较可靠的部分数据对相关函数进行最大熵准则下的外推。具体说, 设已知随机信号的  $p+1$  个相关函数的值  $r_0, r_1, \dots, r_p$ , 则以此  $p+1$  个值为约束条件寻找满足此约束条件的具有最大熵率的随机过程, 这  $p+1$  个约束条件就是

$$E\{X_n X_{n+k}\} = r_k, \quad k=0, 1, \dots, p \quad (7.108)$$

可以证明满足此约束条件的最大熵率随机过程是  $p$  阶高斯马尔可夫过程, 它具有如下形式

$$X_n = \sum_{k=1}^p a_k X_{n-k} + GZ_n \quad (7.109)$$

其中  $Z_n$  是具有零均值及单位方差 ( $\sigma^2 = 1$ ) 的白色高斯噪声  $N(0, 1)$ ,  $G$  为其增益系数,  $a_k$  称自回归系数。  $G$  和  $a_k$  ( $k=1, 2, \dots, p$ ) 的值满足约束方程组(7.108)确定的下述  $p+1$  个方程:

$$r_0 = \sum_{k=1}^p a_k r_{-k} + G^2 \quad (7.110)$$

$$r_l = \sum_{k=1}^p a_k r_{l-k}, \quad l=1, 2, \dots, p \quad (7.111)$$

上述方程组称为 Yule-Walker 方程。现已有多种求解上述方程组的快速算

法,其中最著名的是 Levison 算法和 Durbin 算法。

Yule-Walker 方程的重要特点是它不但给出了  $p+1$  个相关函数值  $r_k$  和  $a_k$ ,  $G$  的关系,而且给出了如何由  $r_k (k=0, 1, 2, \dots, p)$  外推延迟值大于  $p$  时的相关函数值,这些值一般被称为相关函数的 Yule-Walker 外推,从而合理地扩大了对相关函数取值的了解。

在得知此最大熵率随机过程为高斯马尔可夫过程后就可以得知其功率谱的估计值为

$$(\quad) = \frac{G^2}{\left| 1 - \sum_{k=1}^p a_k e^{-jkT} \right|^2} \quad (7.112)$$

按最大熵方法的原理,上述估计是在不牺牲分辨率的条件下充分利用已有知识所可能得到的合理估计。这一估计的期望和方差没有一般的解析表达式,但可证明估计是渐近无偏和渐近正态的,当  $p$  值足够大时,其方差也趋于零。由于最大熵谱估计的这一特点,它在谱估计技术中已获得广泛的应用。

### 7.5.1.2 盲分离

盲分离又称独立分量分析,是一个适于用最小鉴别信息原理解决的问题,它在无线通信、声纳测量、医疗诊断和语音识别中都有应用。这一问题的一般模型如下:有  $M$  个信源各自独立地产生信号  $s_m(t)$ ,  $m=1, 2, \dots, M$ , 这些信号在接收点为阵列天线或阵列传感器所接收,并在阵列接收机输出处获得输出信号  $y_n(t)$ ,  $n=1, 2, \dots, N$ , 它是由  $s_m(t)$ ,  $m=1, 2, \dots, M$  经无记忆线性变换得到的,即

$$\mathbf{Y}(t) = \mathbf{A}\mathbf{S}(t) + \mathbf{Z}(t) \quad (7.113)$$

其中  $\mathbf{Y}(t) \in \mathbf{R}^N$ ,  $\mathbf{S}(t) \in \mathbf{R}^M$  是与  $y_n(t)$ ,  $s_m(t)$  相应的随机矢量,  $\mathbf{Z}(t) \in \mathbf{R}^N$  为噪声矢量,  $\mathbf{A} \in \mathbf{R}^{N \times M}$  为混合矩阵,其值取决于信号的传播途径。所谓盲分离是指在  $\mathbf{A}$  值未知的情况下从  $\mathbf{Y}(t)$  中分离恢复出  $\mathbf{S}(t)$ 。

如果  $\mathbf{Z}(t) = \mathbf{0}$ , 这时得到的是  $\mathbf{S}(t)$  的估值;如果  $\mathbf{Z}(t) \neq \mathbf{0}$ , 则可以准确地恢复  $\mathbf{S}(t)$ , 同时也就得到准确的  $\mathbf{A}$  值,这时的盲分离问题就可以看成是系统的盲辨识问题。再进一步,若  $\mathbf{S}(t)$  不是同一时刻若干信源信号组成的矢量,而是同一信源在时间上顺序采样所得数值组成的矢量,且  $\mathbf{A}$  是 Toeplitz 矩阵,则上述问题进一步退化为盲解卷或盲均衡问题。

下面我们以后以  $\mathbf{Z}(t) = \mathbf{0}$ ,  $\mathbf{A}$  为方阵的情况为例对盲分离问题的求解方法进行具体的分析和讨论。如前所述,这一问题中对信号的唯一已知条件是信号相互

间统计独立。显然,如果解存在则其解  $\mathbf{X}(t)$  必是  $\mathbf{Y}(t)$  的一个线性变换,即

$$\mathbf{X}(t) = \mathbf{F}\mathbf{Y}(t) \quad (7.114)$$

式中  $\mathbf{X}(t)$  的各个分量统计独立,但这样的解不唯一。因为若  $\mathbf{X}(t)$  的各分量统计独立,则由置换矩阵  $\mathbf{P}$  和对角矩阵组成的矩阵  $\mathbf{P}$  对  $\mathbf{X}(t)$  作变换后所得的矢量  $\mathbf{P}\mathbf{X}(t)$  也具有相互独立的分量,这就是说  $\mathbf{F}$  只须满足  $\mathbf{F}\mathbf{A} = \mathbf{P}$  而不必非满足  $\mathbf{F}\mathbf{A} = \mathbf{I}$  (单位矩阵)不可,因此在  $\mathbf{F}$  的  $N^2$  个未知数中实际上有  $N$  个是不可能根据各信源信号统计独立的条件加以确定的,这  $N$  个未知数可以用其他的约束条件加以确定。例如可以假设  $s_m(t)$  的方差值均为 1,或假定  $\mathbf{A}$  的对角线元素均为 1 并要求  $\mathbf{F}$  满足

$$\mathbf{F} = (\mathbf{I} + \mathbf{C})^{-1}, \text{ 其中 } \text{diag}(\mathbf{C}) = \mathbf{0}. \quad (7.115)$$

此时待求的矩阵  $\mathbf{C}$  有  $N(N-1)$  个未知数。

从矩阵  $\mathbf{C}$  的未知数数目可以看到利用二次函数作为准则进行最优化求解是不能得到解的。事实上,在有  $N$  个信源的情况下总共只有  $N(N-1)/2$  个二阶矩及相应的  $N(N-1)/2$  个约束方程。它只是待求未知数数量的一半。为求得全部未知数还需要  $N(N-1)/2$  个约束方程。

在盲分离问题求解的历史上,曾经通过对  $\mathbf{A}$  的结构加以进一步限制的办法来进行求解。如在 ESPRIT 算法中假定混合矩阵  $\mathbf{A}$  具有  $\begin{smallmatrix} \mathbf{B} \\ \mathbf{BD} \end{smallmatrix}$  的形式,其中  $\mathbf{B}$  是任意的,而  $\mathbf{D}$  是对角阵。C. Jutten 和 J. Herault 提出的 HJ 算法利用人工神经网络,对矩阵  $\mathbf{A}$  没有特别的限制但不能保证收敛于最优解,而理想的方法应对  $\mathbf{A}$  没有特殊的限制同时又能保证优化时收敛于全局最优处。

按概率论,矢量  $\mathbf{Y} = (y_1, y_2, \dots, y_N)$  中各分量统计独立时

$$p_{\mathbf{Y}}(y_1, y_2, \dots, y_N) = p_{\mathbf{Y}}(\mathbf{y}) = \prod_{n=1}^N p_{Y_n}(y_n) \quad (7.116)$$

所以  $\mathbf{Y}$  中各分量独立的程度可以用  $p_{\mathbf{Y}}(\mathbf{y})$  和  $\prod_{n=1}^N p_{Y_n}(y_n)$  差别的程度来衡量。而信息论已经指出在信息意义上鉴别信息是两种概率密度函数差别的一种理想量度,所以可取鉴别信息

$$I(p_{\mathbf{Y}}(\mathbf{y}), \prod_{n=1}^N p_{Y_n}(y_n)) = p_{\mathbf{Y}}(\mathbf{y}) \log \frac{p_{\mathbf{Y}}(\mathbf{y})}{\prod_{n=1}^N p_{Y_n}(y_n)} d\mathbf{y} \quad (7.117)$$

作为盲分离求解的优化准则。这样,盲分离的求解就成为最小鉴别信息准则下

的最优化问题。由于鉴别信息是凸函数,这就从原则上保证了其解必定是全局最优,所以最小鉴别信息准则下的优化计算是求解盲分离问题的理想的方法。

通过上述两个例子可以看到从理论上讲熵和鉴别信息是利用最优化方法求解问题时一个理想的准则函数,但应指出的是熵和鉴别信息的计算都是比较繁重的。虽然现在已有一些成熟的算法如最大熵优化时的剑桥算法等,但总的讲这两种准则下的优化都需要较大的计算量,这是这两种方法实用时的主要障碍。而在有些问题中虽然用二次函数已不足以解决问题,但使用有限阶的高阶矩已足以解决问题,这时也不必使用熵和鉴别信息作为准则。例如数字通信中的盲均衡问题可以用四阶矩解决就是一个很好的例子。所以,一般讲只有在那些比较复杂,或有特殊要求的问题中才能显示出最大熵原理和最小鉴别信息原理的优越性和应用它的必要性。

## 7.5.2 最大熵分布与最小鉴别信息分布

Jaynes 曾经指出,物理世界中一些重要的概率分布都是在一定约束条件下满足最大熵原理的概率分布,或简称最大熵分布。但也有不少概率分布不是最大熵分布。区别某一概率分布是不是最大熵分布的一个重要准则是看这一概率分布能否把均匀分布作为一个成员包含进来。所谓把均匀分布作为一个成员是指均匀分布可以是这一概率分布在其某一参数或某些参数取得特定值时的分布,或在其某一参数或某些参数趋于无穷时分布所取的极限。对于不是最大熵分布的概率分布可以引入先验概率分布的办法使其成为最小鉴别信息分布,其条件是保证先验概率分布是这一概率分布的一个成员。当随机变量是连续取值时几乎所有重要的概率分布都是最大熵分布。例如:

(1) 正态分布是定义域为 $(-\infty, +\infty)$ 时在给定  $E[X]$ 和  $E[X^2]$ 下的最大熵分布。

(2) 指数分布是定义域为 $(0, +\infty)$ 时在给定  $E[X]$ 条件下的最大熵分布。

(3) 第一类 Beta 分布是在给定  $E[\ln X]$ 和  $E[\ln(1 - X)]$ 条件下且变量定义域为 $[0, 1]$ 时的最大熵分布;第二类 Beta 分布则是在给定  $E[\ln X]$ 和  $E[\ln(1 + X)]$ 条件下且变量定义域为 $[0, \infty)$ 时的最大熵分布。

(4) 若定义域为 $[0, \infty)$ ,且给定  $E[X]$ 和  $E[\ln X]$ ,则最大熵分布为 Gamma 分布。

(5) Laplace 分布是定义域为 $(-\infty, +\infty)$ 时给定  $E[|X|]$ 条件下的最大熵

分布。

(6) Cauchy 分布则是定义域为  $(-\infty, +\infty)$  时  $E[\ln(1+x)^2]$  取特定值条件下的最大熵分布。

(7) 对数正态分布是定义域为  $[0, \infty)$  时给定  $E[\ln X]$  和  $E[\ln X]^2$  条件下的最大熵分布。

(8) Pareto 分布是定义域为  $x > 0$  时给定  $E[\ln X]$  条件下的最大熵分布。

这些连续概率分布都把均匀分布作为其一个成员,例如:

(1) 在正态分布中,均匀分布可以看成是正态分布在方差  $\rightarrow \infty$  时的极限。

(2) 对指数分布,均匀分布是其数学期望趋于无穷时所取的极限。

(3) 对 Gamma 分布,当其均值趋于无限时其极限分布也是均匀分布。

(4) 对第一类 Beta 分布,均匀分布是其两个参数均取 1 时的分布。对第二类 Beta 分布,当其一个参数趋于无限时分布所取的极限也是均匀分布。

在前述的最大熵原理与最小鉴别信息原理中,香农熵是作为概率系统不确定性的一种量度,而 Kullback 的鉴别信息则是作为两个概率分布之间差异的一种量度。正是这两种量度的特定形式给最大熵分布与最小鉴别信息分布带来了局限性。事实上在给定的概率分布和约束条件下,我们可以取其他的不确定性量度及这一量度下广义的最大熵原理使给定的概率分布成为给定约束条件下广义的最大熵分布。对最小鉴别信息分布也可以类似地求取概率分布之间差异性的其他量度及这一量度下广义的最小鉴别信息原理,使给定的概率分布成为给定约束条件下的最小鉴别信息分布。所以,对不确定性或概率分布之间差异性量度具体形式的改变和扩展可以使最大熵分布与最小鉴别信息分布的范围大大扩展。对这一问题的详细论述可以参见 J. N. Kapur 的有关著作。

## 习 题

7.1 在模式分类中为减小分类所需的计算量,一般选取其尽可能少的若干特征。试讨论:从信息理论的角度应按什么准则对特征进行排队和选取,并陈述其理由。

7.2 在模式分类问题中,设  $C$  代表被分类对象,  $\mathbf{X}$  表示其特征矢量。由于特征矢量空间维数受限而导致的分类最小差错率为  $P_e$ 。试讨论:用最大互信息  $I(C; \mathbf{X})$  准则进行分类能否使分类的差错率达到最小。

7.3 设  $p_1(x)$  是在给定约束条件下的最大熵分布,  $p_2(x)$  是满足相同约束条件的任一其他分布。试证: 两者熵的差为  $H(p_1) - H(p_2) = \int p_2(x) \cdot \log \frac{p_2(x)}{p_1(x)} dx$ 。

7.4 设有随机变量  $X$  取值于非负整数  $\{0, 1, 2, \dots\}$ , 已知其均值  $E\{X\} = K$ , 试给出  $X$  概率分布的最大熵估计。

7.5 设有一由无数粒子组成的物理系统, 每一粒子所处的状态均可有  $N$  种, 它们各相应于能量  $E_1, E_2, \dots, E_N$ 。令  $P_{nm}$  表示系统中有  $m$  颗粒子处于状态  $n$  的概率。现已知

$$(1) \sum_{n=1}^N \sum_{m=0}^{\infty} m P_{nm} = M$$

$$(2) \sum_{n=1}^N \sum_{m=0}^{\infty} E_n P_{nm} = E$$

求此系统的最大熵分布。

7.6 设随机变量  $X$  取值于非负整数集合, 已知  $X$  的概率分布为

$$p(n) = A^{n+1}, \quad 0 < A < 1, \quad n = 0, 1, 2, \dots$$

又经观察知  $X$  的数学期望为  $C$ , 试利用最小鉴别信息准则对  $X$  的概率分布作出估计。

7.7 试证: 在最大熵解中, 拉格朗日乘数  $\lambda_0$  满足

$$(1) \frac{\partial H}{\partial \lambda_m} = -E[f_m(x)], \quad \frac{\partial^2 H}{\partial \lambda_m^2} = \text{Var}[f_m(x)], \quad m = \{1, 2, \dots, M\}$$

$$(2) \frac{\partial^2 H}{\partial \lambda_r \partial \lambda_s} = \text{Cov}[f_r(x), f_s(x)], \quad r, s = \{1, 2, \dots, M\}$$

7.8 设已知离散随机变量的一阶与二阶原点矩, 试求此随机变量在

$K$  条件下  $\log p(x)$  取最大这一条件下的概率分布。

$k=1$

7.9 试证:  $I(q, p) = I(q, r) + I(r, p) = I(q, p-I) + I(p-I, p)$ 。



## 第 8 章 组合信息、算法信息与通用编码

在香农的信息理论中,信源信号的产生、传输、处理与接收等都被看作是一种随机现象,它们可以用一种统计的模型来描述,模型的参数被假定是已经知道的。正是在这样的前提下建立了熵、信息等概念的定义并讨论了信源编码的具体方法等,但在实际应用中,人们有时并不知道或难于得到这些统计模型的参数,有时并不关心这些现象的统计效果。在更深入和更严格的意义上讲,人们有时无法断定信号是确定的还是随机的,如果信号不是随机的,那么统计模型也就不存在了。在非随机的现象中,我们能定义信息的概念并对信源信号的冗余度进行压缩吗?对于这些问题前苏联学者 A. N. Kolmogorov 在他 1965 年的论文“关于信息量度定义的 3 种方法”中给出了肯定的回答。他指出除了在统计学意义上定义信息概念外,另外还有两种重要的定义方法,一种是从组合,即从计数和枚举等出发定义信息;另一种是从计算机算法理论出发定义信息。为区别于香农的信息概念,这两者可以分别称为组合信息与算法信息。Kolmogorov 的这一论文开辟了信息理论研究的新领域。随后不久, B. M. Fitingov, J. Ziv, A. Lempel 先后提出了基于组合的信源编码方法和基于有限自动机的信源编码方法。这些编码方法都不需要知道信源的统计特性,因而适用于不同统计特性的信源, Kolmogorov 把它们称为通用编码。

在这一章中我们将分别介绍组合信息、算法信息以及在此基础上的信源编码方法。为说明组合信息、算法信息提出的背景,我们从统计特性不确定时的信源编码问题开始讨论这些内容。

### 8.1 信源统计特性不确定时的信源编码问题

在第 3 章中我们曾对信源的冗余度压缩问题进行过讨论,并具体介绍了其中两种冗余度压缩编码的方法,即 Huffman 编码与算术编码。这类编码的主要特点是以信源的统计特性作为构造码书的依据,我们一般假定信源的统计特性已知,并在此特性的条件下构造码书,由于这一原因这类编码有时被统称为统计编码。

### 8.1.1 统计特性失配时统计编码的性能

统计编码在实际应用中的一个主要问题是信源统计特性的不确定,即在对信源进行编码时我们尚未得到信源确定的统计特性,或信源实际上并不稳恒因而根本没有确定的统计特性。无论是上述两种情况中的哪一种,其结果都是统计特性的失配,即构造最优编码时所基于的信源统计特性与信源实际的统计特性不相一致。统计特性的失配会使编码实际达到的压缩性能大大低于统计特性适配时的压缩性能,达不到压缩的效果。

为说明这一问题,我们以离散无记忆信源的 Huffman 编码为例,对统计失配时的压缩性能作一估计。按 3.5.2 节所述, Huffman 编码在理想情况下信源字母  $a_k$  对应的码字长  $l_k$  应与  $a_k$  的概率  $p(a_k)$  满足关系

$$l_k = -\log p(a_k)$$

此时编码后的平均码长是理论上可达到的最短平均码长  $\bar{l}_{\text{opt}}$ , 它等于信源的熵率  $H(U)$ , 即

$$\bar{l}_{\text{opt}} = \sum p(a_k) l_k = - \sum p(a_k) \log p(a_k) = H(U)$$

所以信源得到了理想的压缩。

如果在实际使用时实际信源字母的概率分布是  $\{q(a_k)\}$ , 则用上述码书对信源进行编码所得的平均码长将是  $\bar{l}$ , 且

$$\bar{l} = - \sum q(a_k) \log p(a_k) \quad (8.1)$$

它是  $\{q(a_k)\}$  的线性函数, 它与最短平均码长的差

$$\bar{l} - \bar{l}_{\text{opt}} = \sum q(a_k) \log \frac{q(a_k)}{p(a_k)} = I(q, p) \quad (8.2)$$

是  $\{q(a_k)\}$  的非负下凸函数, 且仅在

$$q(a_k) = p(a_k), \quad k = 1, 2, \dots, K$$

处才等于零, 所以  $\bar{l}$  是与  $\bar{l}_{\text{opt}}$  相切于该点的一个超平面。图 8.1 画出了  $K=2$  时统计失配导致的实际平均码长偏离最短平均码长的情况, 可以看到, 随着统计失配程度的增加, 这两者的差呈现单调的增长。

### 8.1.2 自适应统计编码

为解决统计编码在统计特性失配时性能的下降问题, 最直接的方法是使编

码所依据的统计特性能始终适应信源实际的统计特性,而不是使用固定的统计特性。现在一般把使用固定统计特性的统计编码称为静态统计编码,而对统计特性能随信源情况自动适应的统计编码称为自适应统计编码。

自适应统计编码中最早出现的一种现在被称为半自适应统计编码。它的原理极其简单:待发送的消息要经过编码器的两次扫描,在第一次扫描中编码器对消息进行统计以获取统计特性,然后构造码书;在第二次扫描时编码器根据所得的码书对消息进行编

码并随后输出。显然,半自适应统计编码在使用时除了要输出消息编码后的结果,同时还要附上构造码书时所用的信源统计特性或编码器所用的码书。这种方法的第一个缺点是两次扫描带来的编译码延时,这使它在实时通信中很难使用;第二个缺点是码书随着消息的更新而全部刷新。这种更新码书的方法不但效率低,而且要占用信道来传送码书从而降低了信道的利用率。

自适应统计编码技术综合了静态编码和半自适应编码的优点,它只需一次扫描并在一次扫描中同时完成统计特性适应和编码两项工作。在编码过程的每一步,新的一段消息是根据以往消息的统计特性进行编码。这一点是可以做到的,因为在收发两地都已有以往消息的数据,因此可以独立地构造码书用来对下一段消息进行编码。无论是 Huffman 编码还是算术编码,在设计有效的自适应技术中关键的问题是找到一种适当的数据结构,它可以方便地不断对码书进行逐步的更新。对 Huffman 码的这种逐步更新技术最早是 R . G . Gallager 在 1978 年首先提出的, D . E . Knuth 随后在 1985 年将这一技术发展成为一种有效的实用算法。至于算术编码, J . G . Cleary 和 I . H . Witten 在 1984 年时讨论了自适应算术编码,并将其与静态算术编码作了比较。自适应算术编码现在也有了有效的实用算法,但和自适应 Huffman 编码一样都需要比较复杂的数据结构以实现统计数据及其相应码书的逐步更新,我们在这里将不对此作更深入的讨论。

我们在这儿要指出的是,从信息论的观点不能认为自适应统计编码技术永远优于静态统计编码技术。其原因很简单:无论在半自适应或自适应统计编码

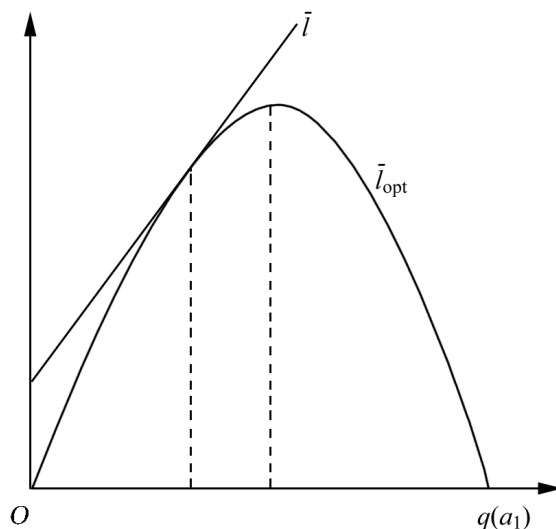


图 8.1 最短平均码长与实际平均码长

中除了要传送信源编码后的码字母流以外,还需要传送代表信源统计模型的数据,因此自适应或半自适应统计编码的最佳压缩性能不可能优于统计适配下静态统计编码的性能。但可以证明自适应编码可在任何情况下只略差于最佳的静态统计编码,而静态统计编码在统计失配时其性能将远劣于自适应统计编码。

对信源统计特性不确定给信源编码带来的困难还可以从另一种完全不同的途径加以解决,这就是根本不利用统计特性进行编码。这种方法是存在的,这就是通用编码,我们在下面将对此作详细的讨论。

## 8.2 基于组合的信息量度与通用编码

### 8.2.1 基于组合的信息量度

在第 1 章中我们曾经提到 R. V. L. Hartley 在 1928 年时提出的一种信息量度。Hartley 认为,按照 Nyquist 对脉冲传输速率与信道带宽关系的分析,接收机在收端只能分辨有限数目的脉冲幅度,设此数为  $M$ ,则  $N$  个脉冲可能组成的不同序列的数目是  $M^N$ ,因此定义信息量是此组合数的对数,即  $H = N \log M$ 。这一定义没有在随后得到广泛的重视和系统的研究,特别是香农的理论提出以后,人们的注意力大都被集中到基于统计的信息上,而把 Hartley 的定义看成是统计意义下的信息在等概情况下的特例。1965 年, A. N. Kolmogorov 的论文“关于信息量度定义的 3 种方法”改变了这种看法,他把基于组合的信息量度看成是信息量度的一种独立的方法。

按照 Kolmogorov 的观点,设变量  $X$  取自  $N$  个元素组成的集合,则此变量在组合意义下的熵为

$$H_c(X) = \log N \quad (8.3)$$

若此变量的值被确定,则我们得到信息

$$I_c = \log_2 N \quad (8.4)$$

当变量  $X_1, X_2, \dots, X_K$  分别取自由  $N_1, N_2, \dots, N_K$  个元素组成的  $K$  个集合时,其熵为

$$H_c(X_1 X_2 \dots X_K) = H_c(X_1) + H_c(X_2) + \dots + H_c(X_K) \quad (8.5)$$

当有多个变量时,基于组合的方法也可定义条件熵和互信息,即已知  $X = a$  条件下  $Y$  的熵为

$$H_c(Y|a) = \log_2 N(A_{Y|a}) \quad (8.6)$$

其中  $N(A_{Y|a})$  是  $X = a$  时  $Y$  所可能取的值构成的集合  $A_{Y|a}$  中的元数总数。而  $X$  提供的关于  $Y$  的信息是

$$I_c(X; Y) = H_c(Y) - H_c(Y|X) \tag{8.7}$$

例如, 若  $X$  和  $Y$  的取值及其可能的组合如表 8.1 所示, 其中 + 表示存在这种组合, - 表示不存在这种组合, 此时有

$$I_c(X = 1; Y) = 0$$

$$I_c(X = 2; Y) = 1$$

$$I_c(X = 3; Y) = 2$$

我们把这种基于组合意义上的熵和信息简称为组合熵和组合信息, 并在相应的符号下增加下标 C 以区别于统计意义下的熵和信息。

表 8.1 变量 X 和 Y 的取值及其组合

<div><div>Y</div><div>X</div></div>	1	2	3	4
1	+	+	+	+
2	+	-	+	-
3	-	+	-	-

8.2.2 通用编码

Kolmogorov 在组合信息领域的工作不仅在于明确组合信息的数学基础及其意义, 更重要的是他提出了基于组合概念的信源编码方法, 并把这种方法称为通用编码。他对这种编码方法的讨论是这样展开的: 设有信源其字母表的大小为  $K$ , 信源字母序列的长度为  $N$ , 其中第  $k$  字母在序列中出现  $N_k$  次, 出现的频率为  $f_k$ , 且

$$f_k = N_k / N, k = 1, 2, \dots, K$$

若  $f_k$  满足

$$-\sum_{k=1}^K f_k \log_2 f_k = h \tag{8.8}$$

则可证明当  $N$  足够大时, 长  $N$  的信源字母序列可有  $W$  种, 此  $W$  的渐近值为

$$\log_2 W \approx Nh \tag{8.9}$$

因此, 这样的信源字母序列可用  $Nh$  位二元码字母进行编码。

在 Kolmogorov 提出上述编码方法的基本概念后不久, B. M. Fitingof 完成

了对这一编码方法细节的研究,并提出了实现通用编码的一种具体方法。Fitingof 的编码方法是这样的:

(1) 输入的信源字母序列首先被分组,每组长  $N$ 。

(2) 对每组字母序列计算每个信源字母的出现频率  $f_k, k=1, 2, \dots, K$ , 由此得到频率矢量  $\mathbf{F} = (f_1, f_2, \dots, f_K)$ , 然后对频率矢量进行编码, 这一步编码需要  $\lceil \log_2 W(K, N) \rceil$  bit, 其中  $W(K, N)$  是不同频率矢量的总数。

(3) 在相同的频率矢量下信源字母序列仍有可能不同。设此时不同信源字母序列的总数为  $W(\mathbf{F})$ , 则为区分这  $W(\mathbf{F})$  种不同的序列需用  $\lceil \log_2 W(\mathbf{F}) \rceil$  bit 对给定的这组字母序列进行编码。

这样, 信源字母序列经编码后所得相应码字的长度  $L$  为

$$L = \lceil \log_2 W(\mathbf{F}) \rceil + \lceil \log_2 W(K, N) \rceil \quad (8.10)$$

利用组合数学的基本知识, 不难得出

$$W(\mathbf{F}) = N! / \prod_{k=1}^K N_k! \quad (8.11)$$

至于不同频率矢量的总数  $W(K, N)$  则可计算如下:

设有一队列, 长  $N + K - 1$ , 在此队列中放入  $N$  个小球, 则队列中尚有  $K - 1$  处没有小球。这  $K - 1$  个空位将整个队列分成  $K$  段, 这  $K$  段的总长恰为  $N$ , 所以我们可以依次把每一段的长度对应于信源字母在每一组中的出现次数  $N_k$ 。由于  $N$  个小球在  $N + K - 1$  个位置上的放法共有  $C_{N+K-1}^N$  种, 所以有

$$W(K, N) = C_{N+K-1}^N \quad (8.12)$$

这样, 上述通用编码方法所得的码字长  $L$  即为

$$L = \left\lceil \log_2 \frac{N!}{\prod_{k=1}^K N_k!} \right\rceil + \lceil \log_2 C_{N+K-1}^N \rceil \quad (8.13)$$

### 8.2.3 Fitingof 通用编码的性能

在上述 Fitingof 的通用编码中, 我们没有用到信源的统计特性。这样的编码方法对不同统计特性的随机信源字母序列是否都能达到理想的压缩呢? 下述定理回答了这一问题。

**定理 8.1** 设  $\{X_1, X_2, \dots, X_n\}$  为离散无记忆信源输出的信源字母序列, 其

熵率为  $H(p_1, p_2, \dots, p_N)$ ,  $L(X_1 X_2 \dots X_N)$  是  $X_1 X_2 \dots X_N$  经 Fitingof 通用编码后所得的码字长度。则对任给  $\epsilon > 0$ , 此长度的数学期望在  $N$  足够大时满足

$$E[L(X_1 X_2 \dots X_N)]/N < H(p_1, p_2, \dots, p_N) + \epsilon \quad (8.14)$$

证明 按式(8.13), 我们有

$$L(X_1 X_2 \dots X_N) < \log_2 C_{N+K-1}^N + \log_2 \frac{N!}{N_k!} + 2$$

$k=1$

所以

$$E[L(X_1 X_2 \dots X_N)] < E \log_2 C_{N+K-1}^N + \log_2 \frac{N!}{N_k!} + 2 \quad (8.15)$$

$k=1$

现分别对上式右端的前两项作出估计。

先对  $\log_2 C_{N+K-1}^N$  的上界进行估计。按

$$\log_2 C_{N+K-1}^N = \log_2 \frac{(N+K-1)!}{N!(K-1)!}$$

当  $N$  足够大时, 由 Stirling 公式

$$n! \approx 2^n n^n e^{-n}$$

得

$$\begin{aligned} \frac{(N+K-1)!}{N!(K-1)!} & \approx \frac{2^{N+K-1} (N+K-1)^{N+K-1} e^{-(N+K-1)}}{2^N N^N (K-1)^{K-1} e^{-(N+K-1)}} \\ & = \frac{2^{N+K-1} (N+K-1)^{N+K-1}}{2^N N^N (K-1)^{K-1}} \\ & = \frac{(N+K-1)^{N+K-1}}{N^N (K-1)^{K-1}} \end{aligned}$$

代入  $\log_2 C_{N+K-1}^N$  的表达式得

$$\begin{aligned} \log_2 C_{N+K-1}^N & \approx \log_2 \frac{(N+K-1)^{N+K-1}}{N^N (K-1)^{K-1}} \\ & = N \log_2 \frac{N+K-1}{N} + (K-1) \log_2 \frac{N+K-1}{K-1} \quad (8.16) \end{aligned}$$

其次, 对  $\log_2 \frac{N!}{N_k!}$  进行估计。同样, 按 Stirling 公式可得

$$\frac{N!}{N_k!} \approx \frac{2^N N^N e^{-N}}{2^{N_k} N_k^{N_k} e^{-N_k}}$$

$k=1$

$$\frac{N!}{\prod_{k=1}^K N_k!} = \frac{2^{NN^N/e^N}}{2^{\sum_{k=1}^K N_k \frac{N_k}{e}}} = 2^{1-K} \frac{N^K}{\prod_{k=1}^K N_k^{N_k}}$$

但  $2^{1-K} \frac{N^K}{\prod_{k=1}^K N_k^{N_k}} = \frac{2^K}{\left(\frac{N}{K}\right)^K} = 1$

所以

$$\begin{aligned} \log_2 \frac{N!}{\prod_{k=1}^K N_k!} - \log_2 \frac{N^K}{\prod_{k=1}^K N_k^{N_k}} &= -\log_2 \frac{N^K}{\prod_{k=1}^K N_k^{N_k}} \\ &= -\sum_{k=1}^K N_k \log_2 \frac{N_k}{N} \end{aligned}$$

对上式取统计平均, 即得

$$\begin{aligned} E \log_2 \frac{N!}{\prod_{k=1}^K N_k!} &= NE \sum_{k=1}^K \frac{N_k}{N} \log_2 \frac{N_k}{N} \\ &= -N \sum_{k=1}^K E \frac{N_k}{N} \log_2 E \frac{N_k}{N} \\ &= -N \sum_{k=1}^K p_k \log_2 p_k \\ &= NH(p_1, p_2, \dots, p_K) \end{aligned} \quad (8.17)$$

其中不等式是根据  $x \log x$  的凸函数性质及 Jensen 不等式得到的。

将式(8.16)和式(8.17)代入式(8.15)即得

$$\begin{aligned} E[L(X_1 X_2 \dots X_N)]/N &< \log_2 1 + \frac{K-1}{N} + \frac{K-1}{N} \log_2 1 + \frac{N}{K-1} \\ &\quad + H(p_1, p_2, \dots, p_K) \end{aligned} \quad (8.18)$$

现令  $N \rightarrow \infty$ , 则得我们所需要的式(8.14)。证毕

这样, 这一定理证明了 Fitingof 根据字母序列组合特性的编码方法在任何统计特性下都能使码字的平均长度无限地接近于信源的熵率, 因而是通用的编码方法。



在 Fitingof 之后, L . D . Davison, T . Cover 等都先后对通用编码的理论与实现方法进行了意义更广泛的研究, 但迄今为止, 基于组合的通用编码还没有一种具体的编码方法在工程中得到广泛应用。造成这种情况的原因之一可能是组合编码本身的缺陷, 这一点在式(8.18)中可以看到, 组合编码的平均码长与熵率的差值是随信源码字长  $N$  的增加按  $(\log N)/N$  的速率下降的, 而在统计编码中则是按  $1/N$  的速率下降的, 因此, 在有限码字长的情况下统计编码将有更好的性能。

## 8.3 算法信息量

### 8.3.1 单一事件或数值下的信息量度问题

在 8.1 节中我们已经指出统计编码在实际应用中的问题, 即我们在编码之前必须知道信源的统计特性, 这就使它的实际应用受到限制, 对统计信息的概念和定义也有类似的问题。统计信息的定义是针对随机变量的, 它需要有随机场作基础, 对于某一确定的数或事件就无法定义其信息量。随着计算机理论的发展, 这一矛盾就显得更为突出。例如下面的两个二元序列:

$$S_1 = 10110100101100010111$$

$$S_2 = 10101010101010101010$$

从直观上看应该具有不同的信息量。前者复杂、无规律, 有较多的信息量; 后者简单、有规律, 所提供的信息量应较少。对多元的字符序列有完全相同的问题。

对于非随机变量情况下如何定义信息量的问题数学家有很大的兴趣。实际上在 Kolmogorov 的公理化体系提出之前, 数学家对概率的概念及其规律的意义就一直有争论。在公理化体系建立之后, 数学家对什么是随机性、如何衡量随机的程度仍然是看法不一, 因此力图建立一个与随机变量概念无关的信息量度对数学界来说是很自然的。20 世纪 60 年代中期, 这一问题终于在 R . Solomonov, A . N . Kolmogorov 和 G . Chaitin 三人的努力下得到解决。他们三人的最初工作是完全独立进行的, 但 Kolmogorov 和 Solomonov 所得到的结论是完全相似的, 即建立起与概率论无关的信息量度, 而 Chaitin 的工作虽然是从计算的复杂性进行讨论, 所用的名称也不相同(Chaitin 称其为复杂度), 但三人得到的是本质上相同的结论。在以下的讨论中将主要沿袭 Kolmogorov 的方法, 对算法信息进行介绍。

### 8.3.2 Kolmogorov 算法熵

Kolmogorov 提出的基于算法意义下的熵是这样定义的。

设有计算机  $U$  和数值  $x, y$ , 而  $P$  是在  $y$  值给定的条件下能使计算机输出  $x$  值的程序,  $P$  用二元序列表示,  $l(P)$  是此程序的长度; 则在这些程序长度中, 最短的程序长度就被定义为  $x$  在条件  $y$  下的条件算法熵, 表示为

$$K(x|y) = \min_{U(P,y)=x} l(P) \quad (8.19)$$

一般来讲, 不同的计算机为输出相同的  $x$  所需程序的长度是不同的, 所以, 上述信息量度如果与计算机有关, 那么这一定义就将失去理论上的价值。但是计算机算法理论, 特别是可计算函数 (部分递归函数) 的理论为这一定义提供了坚实的理论基础。按照这一理论, 任一通用图灵 (Turing) 机  $U$  上执行的程序都可在另一通用图灵计算机  $U$  上执行并有相同的输出, 条件是在程序输入任一计算机  $U$  时在原程序上加以前缀程序  $uu$ , 告诉计算机  $U$  如何仿真计算机  $U$ , 因而此前缀程序只与计算机  $U$  和  $U$  有关, 而与程序  $P$  及  $x, y$  无关。这样, 按两台计算机定义得到的熵值将只差一个固定的值, 即程序  $uu$  的长度。这一差值在数学上一般没有意义, 因为随着程序长度的增加, 这一差值的影响将越来越小, 所以, 在上述定义中所用的计算机只需理解为某一通用的图灵机就可以了。

当上述概念用于考虑单个字符序列时, 信息量的大小决定于计算机为产生这一字符序列所用的最短程序的长度。显然, 越有规律的字符序列所用程序的长度将越短, 规律越复杂则所用程序的长度将越长, 所以 Kolmogorov 的算法熵有时被称为 Kolmogorov 算法复杂度 (complexity)。

算法信息量也可以用来考虑集合。设  $\mathbf{x} = (x_1 x_2 \dots x_N)$  是取自 Bernoulli  $(1/2)$  序列的一个长  $N$  的字符序列, 字符取自字母表  $A = \{0, 1\}$ ,  $A^N$  是这些长  $N$  的二元字符序列的集合。在这种情况下我们可以考虑各单个字符序列的算法熵, 并由此计算出集合  $A^N$  上平均的算法熵。但即使在这种情况下, 算法信息和统计信息的差别也是很明显的。在统计信息的概念下, 取自 Bernoulli  $(1/2)$  序列的每一个长  $N$  的字符序列具有相同的信息; 而在算法信息的概念下, 其中的有些字符序列由于毫无规律而要用长度很长的程序来产生, 而一些简单的, 如全 1 或全 0 字符序列则只需用很短的程序就可产生, 因而不同的字符序列将有各自特定的算法熵。

在定义了算法信息中的条件算法熵以后, 利用空集 或某特定的值就可得

到无条件算法熵  $K(x)$ , 即

$$K(x) = K(x / \quad) \quad (8.20)$$

而  $y$  给出的关于  $x$  的信息则可定义为

$$I(x|y) = K(x) - K(x|y) \quad (8.21)$$

显然

$$I(x|x) = K(x), \quad K(x|x) = 0$$

但是, Kolmogorov 指出, 统计信息论中的某些关系式在算法信息论中找不到相应的关系式。例如统计信息论中有

$$I(X; Y) = I(Y; X)$$

及

$$H(XY) = H(X) + H(Y|X)$$

但在算法信息论中没有相应的等式关系, 类似的关系式只能在渐近相等的意义下近似成立, 即

$$\begin{aligned} |I(x|y) - I(y|x)| &= O(\log I(x, y)) \\ K(x, y) &= K(x) + K(y|x) + O(\log I(x, y)) \end{aligned}$$

## 8.4 二元字符序列的算法熵

在算法熵的定义中程序  $P$  的长度被用来作为  $x$  的算法熵的量度, 程序  $P$  是用来产生  $x$  的。但从信源编码的角度来考虑, 如果把  $x$  看成是信源输出的序列, 则  $P$  可以看成是  $x$  的一种描述, 或一种表示, 是信源字母序列的一种压缩编码。可惜的是算法信息的这一定义对如何获得这一最短长度的程序没有提供任何启示, 它只是指出使  $x$  达到最大压缩的编码长度就是算法熵。尽管算法信息的定义有这一缺陷, 但算法熵代表了对单个字符串进行压缩编码的理论极限, 这在理论上是很有意义的, 所以在这一节中, 我们将在假定  $x$  是二元字符序列的前提下对这一理论极限的界、均值等进行估计。

**定理 8.2** 长  $N$  的二元字符序列的算法熵受限于如下上界:

$$K(\mathbf{x} / N) \leq NH_0 + \frac{1}{N} \sum_{n=1}^N x_n + \log N + C \quad (8.22)$$

式中  $C$  为常数,  $H_0(\cdot)$  表示二元熵函数  $H(p) = -p \log p - (1-p) \log(1-p)$ 。

**证明** 按条件,  $x$  为二元序列, 不同二元序列中的总数为  $2^N$ 。这些不同的序列可以先按序列中“1”的数目  $k$  进行排序,  $k = \{0, 1, \dots, N\}$ , 然后对相同  $k$  值下的序列按  $l$ ,  $l = \{1, 2, \dots, C_N^k\}$  进行排序, 程序  $P$  先令计算机生成所有这些序列

并按要求排序,然后再输出指定  $k, l$  值的序列,打印结束。这样的程序为用二元字符表示  $k$  值和  $l$  值共需

$$\log_2 k + \log_2 C_N^k = \log_2 (N+1) + NH_0(k) \quad (8.23)$$

位二元字符,上式中的不等式来自  $k \leq N$  及式(8.16)的结果。将

$$k = \frac{1}{N} \sum_{n=1}^N x_n$$

代入式(8.23)即得此程序的总长为

$$K(\mathbf{x}|N) \leq NH_0\left(\frac{1}{N} \sum_{n=1}^N x_n\right) + \log N + C$$

式中  $C$  为实现上述程序功能所需其他程序语言的二元字符表示长度,它与  $x$  及  $N$  无关。证毕

**定理 8.3** 设  $\mathbf{x} = (x_1, x_2, \dots, x_N)$  取自 Bernoulli 过程,  $A^N$  表示长  $N$  的这些二元字符序列的集合,则此集合中各序列的算法熵的数学期望满足

$$NH(X) \leq E[K(\mathbf{x}|N)] \leq NH(X) + \log N + C \quad (8.24)$$

式中  $H(X)$  为 Bernoulli 序列的香农熵率。

**证明** 其上界可由定理 8.2 直接得到。现证明其下界。按算法熵定义,计算机在执行任一程序  $P$  后若能输出所要的结果则即停机,所以所有这些能使计算机最终停机的程序的集合组成一个前缀码的码字集合,其长度  $l(P)$  满足 Kraft 不等式,即

$$\sum_{P: U(P) \text{ 停机}} 2^{-l(P)} \leq 1 \quad (8.25)$$

因此,按信源编码中的定理 3.6,此码字长的数学期望必大于信源的熵,此即下界。证毕

上述定理说明对随机序列的每一实现按算法信息的概念进行编码时,其码长的数学期望也能趋于随机序列的香农熵,因此从统计的意义上讲,也能实现理想的压缩。另一方面,如果我们将式(8.24)中的各项除以  $N$ ,则可知按算法信息所得编码的平均码长在  $N$  趋向无穷时,平均码长与香农熵率的差值将以  $(\log N)/N$  的速率趋于零,这一速率与信源的组合编码方法所得的速率相同。这一结果再次说明如果我们用统计平均的效果来衡量信源编码的优劣,则统计编码方法始终占有一定的优势。

上述两个定理可以在给定信源序列的情况下对可能的压缩作出估计,但它没有给出在各种可能的序列中能获得高压缩表示的序列在序列全体中所占的

比例。这一比例对信源编码理论是很有意义的,下面的两条定理回答了这个问题。

**定理 8.4** 具有算法熵  $K(\mathbf{x}) < M$  的序列的总数满足

$$|\{\mathbf{x} \in A^*; K(\mathbf{x}) < M\}| < 2^M \quad (8.26)$$

式中  $A = \{0, 1\}$ ,  $A^*$  表示由 0 和 1 所组成的全部序列。

**证明** 长度为  $m$  的二元序列的数目为  $2^m$ , 所以  $l(P) < M$  的程序总数为

$$\sum_{m=0}^{M-1} 2^m = 1 + 2 + 4 + \dots + 2^{M-1} = 2^M - 1 < 2^M$$

由于每一不同的程序只能对应一种输出,这样就得到所要的结果。 证毕

这一结果虽属意料之中,即复杂度越低的序列其数目将越少,但作为定理,它对信源编码的理论与实践仍具有十分深刻而重大的意义。

**定理 8.5** 设  $\mathbf{x} = (x_1, x_2, \dots, x_N)$  是 Bernoulli  $(1/2)$  过程中取得的一个序列, 则

$$P[K(\mathbf{x}|N) < M] < 2^{-(N-M)} \quad (8.27)$$

**证明**  $P[K(\mathbf{x}|N) < M] = \sum_{\mathbf{x}; K(\mathbf{x}|N) < M} P(\mathbf{x}) = \sum_{\mathbf{x}; K(\mathbf{x}|N) < M} 2^{-N}$   
 $= |\{\mathbf{x}; K(\mathbf{x}|N) < M\}| 2^{-N} < 2^M 2^{-N} = 2^{-(N-M)}$  证毕

上述两个定理说明算法熵小的序列不但数量少而且在 Bernoulli 过程中所占的比例也随算法熵的减小而指数下降,大部分长  $N$  的序列其算法熵接近  $N$ 。

对于算法熵满足式

$$\lim_N \frac{K(\mathbf{x}|N)}{N} = 1 \quad (8.28)$$

的序列程序  $P$  没有压缩的作用,所以这样的序列被称为不可压缩序列。算法信息的这一性质为随机这一概念找到了一种新的意义。我们可以认为不可压缩序列是真正的随机序列,因为在这样的序列中已没有任何形式的规律可以被利用来简化生成它所用的程序,所以序列的算法熵的大小可以作为序列随机程度的量度。由于这一原因,算法熵又被称为算法随机度(randomness)。

## 8.5 算法熵的不可计算性

算法熵的定义提出以后,如何计算算法熵的问题一直引起数学家的极大兴趣。虽然在上一节中我们已对二元字符序列算法熵的界及统计均值作出一些估计,但一般来讲序列的算法熵却是不可计算的。所谓不可计算在这里是指在数学上不可能找到一种一般的方法使我们能够给出任一特定字符序列的算法熵。

最早得到这一结论的是算法信息论的奠基者之一 G. Chaitin。Chaitin 后来在回忆这一发现过程时说:“最短程序这一问题的提出对于一个具有竞争精神和数学思维方法的程序员来讲是非常自然的。当我在大学学习程序课时, 学生们都试图在编程练习中写出最短的程序, 而且我们知道为使程序是否已经达到最短的结论真正可信, 我们还必须给出证明。但我们连这一证明的粗略思路都提不出来。最后我们发现这不是我们的无能, 而是我们遇到了数学上最基本的一个限制。”1970 年 Chaitin 利用数理逻辑的理论给出了算法熵不可计算的严格证明, 我们在这儿对这一结论作一概念上的说明。

算法熵的不可计算性与数理逻辑中哥德尔(Gödel)的不完全性定理有密切关系, 这一定理对数学中的很多悖论作出了解释。对序列的算法熵进行计算也涉及到悖论, 这就是说如果能证明“某一字符序列的算法熵是  $M$ ”, 那么这将是一个悖论。为说明这点, 我们先介绍与这一悖论最相近的著名悖论, 即罗素在 1906 年发表的“单词悖论”, 这一悖论是 G. Berry 告诉罗素的, 所以有时又称 Berry 悖论。它描述的是这样一个矛盾: 每一整数都可以用英文单词描述出来; 例如数字 5 可以用“five”也可以用“The next integer after four”表示; 考虑到英文有 27 个字符(包括空格), 所以如用长为 100 以下的字符序列应能描述  $27^{100}$  个有限整数; 这样就必定存在用少于 100 个字符就不能描述的最小的整数, 但是“ The smallest number not describe in 100 letters or fewer ”恰恰是用少于 100 个字符就把这整数描述出来了。现在再回到算法熵的计算上来。如果算法熵是可计算的, 则我们就可以用“给出算法熵  $10^{10}$  的第一个二元字符序列”这样短的程序来代替本应有  $10^{10}$  个二元字符的程序。这显然是矛盾的, 但我们在上述推理过程中并没有不合理的地方。按照合理的推理规则是不应推导出一个自相矛盾的结论的, 这就是悖论。产生这种悖论的原因是公理化系统的局限性。按照 Gödel 的不完全性定理, 任何公理化系统都有一些本系统内合理的命题, 其正确性不能在系统内得到证明。具体到算法熵的计算, Chaitin 得到 3 条主要的结论:

(1) 在一个具有  $n$  比特公理的形式系统中不可能证明某特定的二元序列具有大于  $n + C$  的算法熵, 其中  $C$  是某一常数。

(2) 对一个有  $n + C$  比特公理的形式系统, 它可以确定所有算法熵小于  $n$  的二元序列的算法熵, 它也可以知道哪些二元序列的算法熵大于等于  $n$ , 但不能知道这些序列的算法熵的确切值。

(3) 所有形式系统虽然总能确定算法熵小于  $n$  的那些序列, 但总有某方面

的缺陷,它们或是陈述公理的比特数很少但在证明中需要冗长的推理,或是证明过程很短但陈述公理的比特数不可置信地多。

概括上面的结论,对于算法熵小的序列我们总可以用这种或那种方法算得其算法熵,但对算法熵足够大的那些序列,则除了累试法以外我们不可能有其他有效的方法得到它们的算法熵的确切值。所谓有效的方法是指能对所有序列适用而不是仅对某一特定序列适用的方法,这就是算法熵的不可计算性。

算法熵的不可计算性对信源编码的研究是一个很大的打击。因为算法熵的计算有可能为信源编码提供一种有效的通用编码方法,而算法熵的不可计算性表明这样一种理想的通用编码方法是不可能得到的。

最后,我们简单提一下算法熵的概念与科学研究基本方法论的关系来结束对算法信息的讨论。

算法熵的概念可以描述成科学家在完成观察后希望对现象进行理解和预测时所面临的问题。科学观察的结果相当于算法熵定义中的字符序列  $x$ , 科学家企图搜索一个能与观察结果一致的理论, 这理论就相当于算法熵定义中的程序  $P$ 。按以前的分析,所有这些能使计算机停机的程序其长度  $l(P)$  满足 Kraft 不等式。在所有这些程序中产生同一特定字符序列  $x$  的程序不止一个,所以某一特定字符序列  $x$  的概率  $P_U(x)$  是

$$P_U(x) = \sum_{P: U(P)=x} 2^{-l(P)} \quad (8.29)$$

由于程序长度较短的  $P$  对应较大的概率,所以科学家总是认为最简单的理论就是最好的。如果理论的长度与观察结果的长度相同,理论就毫无意义;如果观察结果只能用相同长度的理论进行描述,则此观察结果只能被认为是完全随机(random)的,人们无法对它进行理解和预测。科学理论的价值就在于把观察结果压缩,归纳为很少的理论假设。

## 8.6 有限状态压缩编码器

对单个序列的压缩在理论上和实践上都有很大的意义。Chaitin 的研究得到了算法熵不可计算的结论,但这一结论并不意味着我们在这方面已无事可做。算法熵的定义和 Chaitin 的分析都是在通用图灵机作为计算模型的前提下得到的,如果对计算模型加以限制,就有可能得到局部情况下适用的且仍有价值的理论和编码方法。

1978 年, J. Ziv 和 A. Lempel 在有限状态自动机理论的基础上提出了有限状态压缩编码器的概念。在有限状态压缩编码器的条件下提出了序列的有限状态可压缩度和有限状态熵, 推导了编码定理, 使这两个概念对单个序列的作用就如同香农熵对概率空间的作用。Lempel-Ziv 编码就是他们提出的利用有限状态编码器进行信源编码的方法, 这一方法也可同时看成是具体实现序列有限状态可压缩度的一个构造性证明。

有限自动机是一个系统  $(A, S, B, \mu)$ , 其中  $A, S, B$  分别代表自动机输入、状态和输出的字母表,  $\mu$  是一个映射:  $S \times A \rightarrow S$ , 表示下一状态, 也是一个映射:  $S \times A \rightarrow B$ , 代表输出映射。图 8.2 为 Lempel-Ziv 编码所用的有限状态压缩编码器的一个例子, 它具有状态集  $\{s_1, s_2, s_3, s_4\}$ , 输入字母表  $\{a, b\}$  和输出字母表  $\{0, 1\}$ 。图中状态之间的有向线段及其旁的标注说明编码器在输入每一字母时状态的转移及相应的输出。图中的  $\emptyset$  (空集) 表示编码器没有输出。在第 3 章中我们提到一个有用的信源编码器, 其编码结果应是唯一可译的, 即信息上没有损失。按这一要求并非所有的自动机都可以成为信息无损的有限状态编码器。一个有限状态编码器如果是信息无损的, 则其输入字母序列可以由编码器在此输入时的初态  $s_i$ 、相应的输出字母序列及终止状态  $s_j$  三者组成的三重串  $(s_i, \text{输出序列}, s_j)$  所唯一地确定。例如, 图中的编码器是信息无损的,  $(s_3, 011, s_2)$  将唯一地把输入确定为  $aaba$ , 所以这一编码器是信息无损的。

利用有限状态编码器对序列进行压缩的一个重要机理是将输入字母序列进行分解, 分成很多字母序列段, 这些段被称为短语, 所有的短语都应该是互不相同的, 这样的分解有时被称为清晰的分解。将字母序列进行分解以得到压缩的想法可以上推到 1967 年, 这一年 H. E. White 提出了对英语文本采用字典编码的方法。众所周知, 英语单字的数量远少于英语字母进行组合可得到的数目。例如长度为

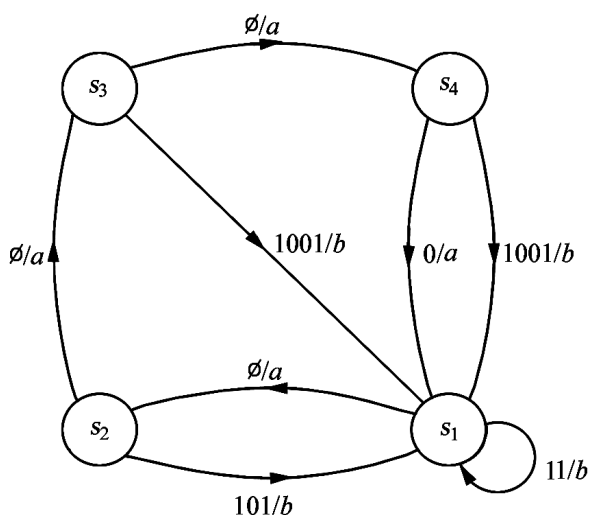


图 8.2 有限状态压缩编码器

4 的英文字母串可以有  $26^4 = 456976$  种不同组合, 已远超过常用英文单字的总数。所以利用字典进行编码可以得到压缩。但 White 的字典编码方法是静态的, 即利用固定的字典, 而且所用的分解也不是清晰的分解, 这些都是和有限状



态编码器不能相比的。

现设有字母序列  $x_1^N = (x_1 x_2 \dots x_N)$ , 输入到一个状态总数为  $A$  的有限状态编码器, 在编码后输入序列被分解成互不相同的一组短语, 它可表示成

$$x_1^N = w_1 w_2 \dots w_d, w_i \neq w_j$$

总共有  $d$  个短语, 每一短语都有其相应的编码器初态、编码器输出和编码器终态。例如, 将  $x_1^4 = abba$  输入图 8.2 的编码器, 序列可被分解成  $x_1^4 = ab, b, a$ , 其过程是编码器在开始时处于初态  $s_1$ , 经输入  $ab$  后输出  $(ab) = 101$  并停留在  $s_1$ ; 随后是  $b$  输入, 编码器输出  $(b) = 11$  并再次停在  $s_1$ ; 最后是  $a$  输入, 此时编码器无输出, 但状态由  $s_1$  过渡到  $s_2$ 。在一般情况下编码器对  $x_1^N$  的编码输出就是分解后所得  $d$  个短语对应输出的级联。设其总长为  $L(x_1^N)$ , 则编码所得的压缩比为

$$(x_1^N) = \frac{L(x_1^N)}{N \log A / 2} \quad (8.30)$$

显然  $(x_1^N)$  应是一个大于 0 但小于 1 的数, 且对不同的编码器将有不同的压缩比值。为使编码器获得最大的压缩效果(按上述定义, 压缩比为最小), 编码器应能在任意的单个序列输入下都能使所得清晰分解中各短语对应的输出取尽可能短的值, 但这些值的数量是有限的。设编码器有  $A$  个状态, 则无输出因而长度为 0 的短语最多可以有  $A$  个, 长度为 1 的短语最多可有  $A^2$  个; 一般的对应于输出长度为  $l$  的短语则最多可有  $A^{2^l}$  个, 由此分析下去, Ziv 和 Lempel 获得了有限状态压缩编码器可能得到的压缩比的下界。

**定理 8.6** 设有限状态压缩编码器是信息无损的, 且有  $A$  个状态, 信源输入字母表为  $A$ ,  $|A| = M$ , 输出字母表为  $B = \{0, 1\}$ ; 则对任一输入字母序列  $x_1^N$  编码器可以达到的最小压缩比的下界是

$$(x_1^N) \geq \frac{D(x_1^N) + \frac{A}{2}}{N \log M} \log \frac{D(x_1^N) + \frac{A}{2}}{A^{\frac{1}{2}}} + \frac{2}{N \log M} \quad (8.31)$$

其中  $D(x_1^N)$  是将  $x_1^N$  进行清晰分解所可能得到的最大的不同短语数。

**证明** 设输入字母序列  $x_1^N = (x_1 x_2 \dots x_N)$  经编码后被分解成  $D(x_1^N)$  个互不相同的短语, 如

$$x_1^N = w_1 w_2 \dots w_D$$

其编码输出序列为  $y^1 y^2 \dots y^L$ 。

令  $d_l$  为短语中相应输出字母序列长为  $l$  的短语的总数。已知所有短语均不同, 且编码器是信息无损的, 故这些短语的总数不可能超过其相应的三重串  $(s, s, s)$  的数目, 即

$$d_l \leq 2^l \quad (8.32)$$

另一方面,  $D$  是给定输入下最大可能的不同短语的数目。若  $D$  的值刚好等于如下的  $k$ :

$$D = \sum_{l=0}^k d_l = \sum_{l=0}^k 2^l, \quad k = 1, 2, \dots \quad (8.33)$$

则此分解刚好利用了长度小于等于  $k$  值的全部可能输出字母序列。在一般情况下, 有

$$2^{k+1} > D \geq 2^k$$

此时, 除全部长为小于等于  $k$  的输出字母序列外, 编码器应使用部分长  $k+1$  的字母序列, 所以  $D$  必可表示成

$$D = \sum_{l=0}^k 2^l + t = 2^{k+1} - 1 + t \quad (8.34)$$

其中

$$0 \leq t < 2^{k+1} \quad (8.35)$$

输出码字母序列长  $L(x_1^N)$  满足

$$\begin{aligned} L(x_1^N) &= \sum_{l=0}^k l 2^l + (k+1)t \\ &= [(k-1)2^{k+1} + 2] + (k+1)(t+1) \\ &= (k-1)(D+1) + 2(t+2) \end{aligned} \quad (8.36)$$

由式(8.34)可有

$$k-1 = \log \frac{D-1}{2} + \log \frac{D+1}{4} - \log \left( 1 + \frac{(t+1)}{D-1} \right)$$

代入式(8.36)得

$$L(x_1^N) = (D+1) \log \frac{D+1}{4} + \dots \quad (8.37)$$

其中

$$= \frac{2(t+2)}{D+1} - \log \left( 1 + \frac{(t+1)}{D-1} \right)$$

令

$$= \frac{(t+1)}{D-1} = \frac{D}{2^{k+1}}$$

则可写成

$$= \frac{2^2}{D+2} + \frac{2}{1+} - \log(1+)$$

不难知道  $0 < 1$ , 在此值域内有不等式

$$\frac{2}{1+} \log(1+)$$

所以

$$2^2 / (D+2) \quad (8.38)$$

由式(8.37)和式(8.38)得

$$(x_1^N) = \frac{L(x_1^N)}{N \log M} - \frac{D+2}{N \log M} \log \frac{D+2}{4^2} + \frac{2^2}{N \log M}$$

$D$  值与  $x_1^N$  有关, 所以一般情况下应记作  $D(x_1^N)$ , 此时即为所求的式(8.31)。

证毕

根据上述定理, 还可以得到这一编码方法的渐近结果。记  $\mathbf{x}$  为长度无限的单个序列, 并定义

$$(\mathbf{x}) \stackrel{\text{def}}{=} \limsup_N (x_1^N) \quad (8.39)$$

即可得具有  $k$  个状态的有限状态编码器可以达到的压缩比  $(\mathbf{x})$  具有下界, 亦即

$$(\mathbf{x}) \leq \limsup_N \frac{D(x_1^N) \log D(x_1^N)}{N \log M} \quad (8.40)$$

如定义任意有限状态编码器可达的压缩比为  $(\mathbf{x})$ , 即

$$(\mathbf{x}) \stackrel{\text{def}}{=} \lim (\mathbf{x})$$

则同样可得

$$(\mathbf{x}) \leq \limsup_N \frac{D(x_1^N) \log D(x_1^N)}{N \log M} \quad (8.41)$$

由此可知式(8.41)右端的量是有限状态压缩编码器的条件下单个序列可能得到的压缩的最大限度。除此以外, Ziv 和 Lewpel 还证明可以用有限状态编码器仿真其他定长到变长、变长到定长和变长到变长的编码, 因此式(8.41)的下界对这些编码方法也都是适用的。

## 8.7 Lewpel-Ziv 编码

Lewpel-Ziv 编码是 Ziv 和 Lewpel 根据上述有限状态压缩编码器的理论提出的一种具体算法。按照最早发表的论文, 此法应称为 Ziv-Lewpel 编码法, 但

目前习惯上均称其为 Lempel-Ziv 编码, 简称 LZ 编码。

在 LZ 编码中输入字母序列的分解是迭代进行的。在第  $i-1$  步, 编码器从  $w_{i-1}$  短语后的第一个字母开始向后搜索在此之前尚未出现过的最短短语  $w_i$ 。由于  $w_i$  是此时最短的新短语, 所以  $w_i$  在去掉最后一个字母后所得的前缀必定是在此之前已经出现过的。若设此前前缀是在第  $j < i$  步时出现的, 则对  $w_i$  的编码就可利用  $j$  和  $w_i$  最后一位所取的字母来表示。对前者最多需要  $\lceil \log i \rceil$  bit, 而对后者只需  $\lceil \log M \rceil$  bit。例如, 输入字母序列  $ababbbabababab...$  可迭代地被分解成  $a, b, ab, bb, aba, abab, \dots$ , 各短语被编码成  $(0, 0), (0, 1), (01, 1), (10, 1), (011, 0), (101, 1), \dots$ 。总的编码输出由这些短语对应的编码输出级联而成, 即为  $000101110101101011\dots$ 。

现设输入为  $x_1^N$ , 经此分解后得  $d(x_1^N)$  个短语。因为各短语均不相同, 所以编码输出的总长度为

$$L_{LZ}(x_1^N) = \sum_{i=1}^d [\log i] + [\log M] \quad (8.42)$$

LZ 编码所得的压缩比为

$$LZ(x_1^N) = \sum_{i=1}^d [\log i] + [\log M] / (N \log M) \quad (8.43)$$

在  $N \rightarrow \infty$  时可对这一压缩比的渐近值进行估计。

在式(8.43)中,  $i < d(x_1^N)$ , 所以令  $r = 2 + \log M$ , 可得

$$LZ(x_1^N) \leq [d(x_1^N) \log d(x_1^N) + r d(x_1^N)] / (N \log M)$$

$d(x_1^N)$  是 LZ 编码下对  $x_1^N$  分解所得的短语数。按照上节的讨论, 显然  $d(x_1^N) \leq D(x_1^N)$ 。代入上式得

$$\limsup_N LZ(x_1^N) \leq \limsup_N \frac{D(x_1^N) \log D(x_1^N)}{N \log M} + \frac{r D(x_1^N)}{N \log M} \quad (8.44)$$

为估计上式右端第二项的值, 我们先求  $D(x_1^N)$  与  $N$  的关系。

$D(x_1^N)$  是  $x_1^N$  分解成不同短语后短语总数可能的最大值。为达到这一点, 所有短语均应取可能的最短的值。当  $x_1^N$  中的短语恰好取尽所有长为  $k$  和小于  $k$  的短语时,  $N$  的值应为

$$N_k = \sum_{l=1}^k 2^l = (k-1)2^{k+1} + 2 \quad (8.45)$$

此时短语的总数为

$$D_k = \sum_{l=1}^k 2^l = 2^{k+1} - 1 \quad (8.46)$$

在一般情况下会有

$$N_k < K \quad N_{k+1} = k2^{k+2} + 2$$

在  $x_i^N$  中的短语取尽所有长为  $k$  和小于  $k$  的短语后, 其余则取长为  $k+1$  的短语, 所以有

$$D = D_k + \frac{N - N_k}{k+1} = 2^{k+1} - 1 + \frac{N - N_k}{k+1} < 2^{k+1} + \frac{N - N_k}{k+1} \quad \frac{N_k}{k-1} + \frac{N - N_k}{k-1} = \frac{N}{k-1} \quad (8.47)$$

另一方面, 由  $N > N_k$  可得

$$N > (k-1)2^{k+1} + 2 \quad 2^k$$

所以

$$k < \log N$$

由  $N < N_{k+1}$  可得

$$N < N_{k+1} = k2^{k+2} + 2 \quad (k+1)2^{k+2} < (\log N + 1)2^{k+2}$$

所以

$$k+2 > \log \frac{N}{\log N + 1}$$

即

$$\begin{aligned} k-1 &> \log N - \log(\log N + 1) - 3 \\ &= \log N - 1 - \frac{\log(\log N + 1) + 3}{\log N} \\ &> \log N - 1 - \frac{\log(2\log N) + 3}{\log N} \end{aligned} \quad (8.48)$$

将式(8.48)代入式(8.47)得

$$D(x_i^N) < \frac{N}{k-1} < \frac{N}{\log N - 1 - \frac{\log(2\log N) + 3}{\log N}}$$

由此可得(8.44)式右端第二项的值满足

$$\lim_N \frac{r d(x_i^N)}{N \log M} = \lim_N \frac{r D(x_i^N)}{N \log M} < \lim_N \frac{r}{\log N - 1 - \frac{\log(2\log N) + 3}{\log N} \cdot \log M} = 0$$

所以 LZ 编码的压缩比满足

$$\limsup_N \sup_{LZ} (x_i^N) = \limsup_N \frac{D(x_i^N) \log D(x_i^N)}{N \log M} \quad (8.49)$$

将这一结果和式(8.41)相比可以知道 LZ 编码的性能可以渐近地达到有限

状态压缩编码器性能的下界,因此这是一种性能优越的编码方法。由于它性能优越同时易于实现,它被 ITU 数据传输标准 V.42 所采用,并在很多计算机数据存储中得到应用。此外 LZ 编码不需知道信源的统计特性,在这一意义上它是一种通用编码。

## 8.8 LZ 编码压缩比与香农熵

LZ 编码具有有限状态压缩编码所可能达到的最优性能,因此将其与 Huffman 编码等统计编码方法作一比较是很有意义的。这一工作最早是由 Ziv 和 Lempel 完成的,他们证明当把 LZ 编码用于稳恒遍历信源时其压缩比以概率 1 收敛于该信源的香农熵。这一结果以定理形式可表示如下。

**定理 8.7** 设  $\{X_n\}$  是稳恒遍历信源,  $x_1^N$  是此信源输出的一个长为  $N$  的样本序列,信源的熵率为  $H(X)$ , 则  $x_1^N$  在经 LZ 编码后所得的压缩比可以以概率 1 满足关系式

$$\limsup_N \sup_{LZ} (x_1^N) = H(X) + \epsilon \quad (8.50)$$

其中  $\epsilon$  在  $N \rightarrow \infty$  时趋于零。

**证明** 按假设  $x_1^N$  是稳恒遍历信源输出的一个样本序列。现取能整除  $N$  的长度  $l$  将  $N$  分成  $N/l$  段。显然,长  $l$  的输入字母段可有  $|A|^l$  种组合。把每种组合作为一个字  $w$ , 则该字在  $x_1^N$  中出现的频率  $P(w, x_1^N)$  为

$$P(w, x_1^N) = \frac{l}{N} N(w, x_1^N)$$

其中  $N(w, x_1^N)$  为  $w$  在  $x_1^N$  中出现的次数。

现将此频率作为概率对  $x_1^N$  用 Huffman 编码方法进行编码,即可得一码书将所有长  $l$  的信源字母序列映射为相应的二码字母组。对足够长的  $N$  我们可以定义  $x_1^N$  的熵率  $H_l(x_1^N)$  为

$$H_l(x_1^N) = - \frac{1}{l} \sum_{w \in A^l} P(w, x_1^N) \log P(w, x_1^N) \quad (8.51)$$

同时,设  $l$  足够大,则  $x_1^N$  分段后所得的各字母段可以近似看成是相互独立的。这样,按第 3 章中对 Huffman 码平均码长的讨论可知现时的平均码长  $\bar{L}_l$  满足

$$\bar{L}_l < H_l(x_1^N) + \frac{1}{l} \quad (8.52)$$

另一方面,我们在前面已经指出有限状态压缩编码器可以仿真任意的变长

编码。实际上在现时用一个具有  $|A|^l$  状态的有限状态编码器就可以仿真上述的 Huffman 编码。如果把这一有限状态编码器记作  $F(l, x_1^N)$ , 则上述 Huffman 编码的平均码长就又可以看成是这一  $F(l, x_1^N)$  的压缩比, 因此可得

$$F(l, x_1^N) (x_1^N) = l(x_1^N) + \frac{1}{l} \quad (8.53)$$

上式在任意  $N$  值下成立, 所以可有

$$\limsup_N F(l, x_1^N) (x_1^N) = \lim_N l(x_1^N) + \frac{1}{l}$$

或写作

$$F(l) (x) = l(x) + \frac{1}{l} \quad (8.54)$$

现令  $l \rightarrow \infty$ , 即得

$$\lim_l F(l) (x) = \lim_l l(x) + 0 = l(x)$$

按定理给定的条件  $x_1^N$  是稳恒遍历信源输出的一个样本序列, 因此  $l(x) = H(X)$  的概率为 1, 这样就可以有

$$\lim_l F(l) (x) = H(X)$$

最后, 利用 LZ 编码具有有限状态压缩编码器最优性能, 即压缩比可以渐近趋于下界这一特点, 即得

$$\limsup_N LZ(x_1^N) = \lim_l F(l) (x) = H(X) \quad \text{证毕}$$

LZ 编码压缩比可以达到信源熵率这一结论一方面说明 LZ 编码的有效性, 但也说明有限状态压缩编码器不能做得比 Huffman 编码更好。从这一点看可能令人失望, 但 LZ 编码仍有其独特的优点, 这就是它不需要在编码时知道信源的统计特性。在这一意义上它是一种通用编码, 而且是目前获得广泛实际应用的一种通用编码。

## 习 题

本章提及的内容对深入理解信息理论是必要的, 但书中所作的介绍是极其初步的, 以下问题既可作为本章的习题, 也可作为进一步了解和研究的参考材料。

8.1 要实现统计编码对信源统计特性的自适应, 难点不在于使编译器能

获知统计特性的变化,同步地进行跟踪。关键的问题是找到一种适当的数据结构使码书能方便地实现渐进的、编译码两端能取得一致的更新。考虑这一问题并在参看以下经典文献后对 Huffman 编码和算术码中的自适应方法作出总结。

[1] Knuth D E .Dynamic Huffman Coding . Journals of Algorithms, 1985,6:163 ~ 180

[2] Langdon G G, Rissanen L J . A Simple General Binary Source Code . IEEE Trans on Inform Theory, 1982, Vol IT-28, No 5, Sept

[3] Pennebaker W B, etc . An Overview of the Basic Principles of the Q-coder Adaptive Binary Arithmetic Coder . IBM J Res & Develop, 1988, 32(6): 717 ~ 726

8.2 按照 Kolmogorov 对信息理论的看法,在定义信息量时组合方法应先于概率方法,因此,信息理论的发展可独立于概率理论。参阅下述经典文献后写出报告和你的看法。

[1] Kolmogorov A N . Logical Basics for Information Theory and Probability Theory . IEEE Trans on Inform Theory, 1968, Vol IT-14, No 5, Sept

[2] Kolmogorov A N . Three Approaches for Defining the Concept of Information Quantity . In Russian, Information Transmission, 1965, Vol 1

[3] Kolmogorov A N . Combinatorial Foundations of Information Theory and the Calculus of Probabilities . Russian Math Surveys, 1983, 38(4): 29 ~ 40

8.3 Kolmogorov 提出的算法熵或算法复杂度是多种复杂度定义中最深刻的一种,可惜这一量度是不可计算的,参阅下述经典文献后写出报告。

[1] Chaitin G J . On the Difficulty of Computation . IEEE Trans on Inform Theory, 1970, Vol IT-16, Jan

[2] Chaitin G J . Information Theoretic Computational Complexity . IEEE Trans on Inform Theory, 1974, Vol IT-20, Jan

8.4 对于 Kolmogorov 算法复杂度的不可计算性, Lempel 和 Ziv 认为不存在绝对的复杂度量度,所以他们提出了具体的基于有限状态机的序列复杂度量度——“归一化有限状态复杂度”。这一定义与 Kolmogorov 的定义不同,有时按有限状态复杂度定义衡量是复杂的序列而按 Kolmogorov 的定义衡量却是不复杂的。而最主要的是 Lempel-Ziv 编码算法给出了计算这一定义下序列复杂



度的一个构造性方法。参看下述经典文献后写出你对两种复杂度定义的比较和看法。

- [1] Lempel A, Ziv J . On the Complexity of Finite Sequences . IEEE Trans on Inform Theory, 1976, Vol IT-22, Jan
- [2] Ziv J . Coding Theorems for Individual Sequences . IEEE Trans on Inform Theory, 1978, Vol IT-24, July

## 第9章 通信网中的信源编码与信道容量

当信息在通信网中流通时信息的有效表示与信道的充分利用等问题与单信源、单信道时的情况有很多不同,如何考虑这种情况下的信源编码与信道容量是本章讨论的主要内容。由于通信网组成与结构的千变万化,对通信网中信源编码与信道容量问题的一般性研究有很大的困难,因此这方面的研究一开始就是从特殊的、典型的、有代表性的容量问题或编码问题着手,先求得各种典型情况下的解,然后加以推广和拓展。但即使这样,在目前已提出的问题中也只有小部分得到满意的解决,相当一部分问题不是尚未得到解决就是尚未引起通信工程师的广泛兴趣。在本章中我们选择若干已得到较好解决且有较大工程指导意义的问题加以介绍,其中主要是反馈信道、多源接入信道的信道容量问题和分布信源的冗余度压缩编码问题。在所有的介绍中我们都将尽可能地同时给出其物理意义并对其在实际应用中的价值作适当的评述。

### 9.1 概 述

一般认为用信息论方法研究通信网中的信息传输问题是从香农 1961 年的论文“双向通信信道”开始的。这一论文首次研究处于地理上不同位置的两个信源、两个信宿所组成的最小通信网中的信息传输。论文在理论上引入不少新的概念,但在当时并未引起广泛的重视。

70 年代卫星通信与计算机通信的发展使通信网的拓扑结构趋于多样化,通信方式趋于多样化。基于单信源、单信道的信源编码与信道容量理论已无法回答此类通信网中信息的有效表示与信道的充分利用问题,这才使更多的信息论工作者把目光转向这一领域。1971 年 R. Ahlswede 提出了多径 (multi-way) 通信信道,1972 年 H. H. J. Liao 提出多源

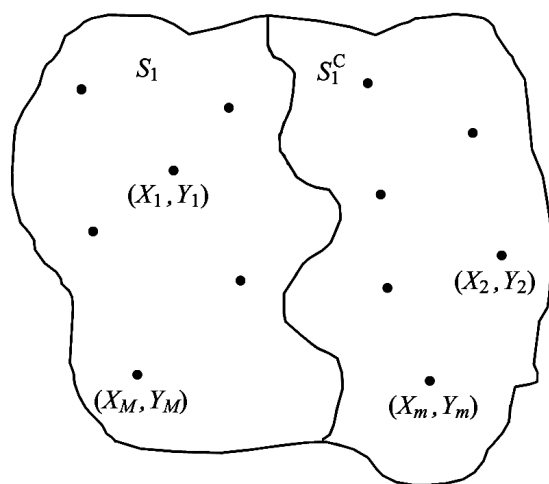


图 9.1 通信网的一般模型

接入(multiple-access)信道, T.M. Cover 提出广播(broadcast)信道, 1973 年 D. Slepian 和 J.K. Wolf 提出相关信源(correlated information sources)编码, 1975 年 A. Carleial 提出多端(multi-terminal)通信网络, 同年 J.K. Wolf 提出多用户(multi-user)通信信道。1977 年 IEEE Transactions on IT 出版了有关多端信道编码的专集, 同年 T. Berger 提出多端信源编码。至此, 用信息论方法研究通信网的问题终于全面展开。为表明这一研究领域与信息论早先研究领域的差异, 人们把早先研究的领域称为点点(point-to-point)信息理论, 而把新领域称为多端(multi-terminal)信息理论或多用户信息理论或网络(network)信息理论, 但迄今尚没有统一的名称。

用信息论方法研究通信网中的信息流通问题时, 通信网可用图 9.1 所示的一般模型来表示。图中共有  $M$  个收发点, 或  $M$  个用户, 点  $m$  发出信号  $X_m$  并收到信号  $Y_m$ , 各收发点都可能有信源和/或信宿; 各信源发出的信息可能是统计上不独立的, 各收发点有可能收到来自其他各点的信号, 同时也可能向其他各点发出信号; 网络中信道的整体特性可用所有收发点的输入输出字母表和输入输出信号集合的多维转移概率或转移概率密度函数来表示, 例如在离散无记忆情况下可用  $P(y_1 y_2 \dots y_M | x_1 x_2 \dots x_M)$  来表示。

通信网的一般问题是在给定网络中信道整体特性的情况下求解网络的最大信息流量, 以及在给定网络中信源特性的情况下求解信源信息的有效表示方法。这些问题从概念上说显然是单信道下信道容量问题或单信源下信源编码问题的扩展, 但是由于通信网形式的多样性, 想从网络的一般模型入手求其一般解是非常困难的。在过去几十年中人们从特殊问题入手提出了一系列在理论上或是应用上有较大意义的典型网络模型。这些典型网络也可以看成是复杂通信网分解后所得的各类基本组成单元, 因此对于一般通信网问题的解决也是很有意义的。

目前, 在网络信息流量方面提出的典型问题主要是如何求解以下几种典型网络模型的最大信息流量, 在文献中这些简单的典型网络模型仍被称作信道。

### (1) 双向(two-way)信道

双向信道如图 9.2 所示有两发两收, 通过信道按相反方向互送信息。在通信工程中的双向信道是将一个物理信道用时分或频分方法分成两个独立的信道来实现的, 但从信息论的观点来看用这种方法实现双向通信不一定是最好的, 因此要寻找最好的双向通信方法并求解双向信道的容量域。

### (2) 反馈信道

反馈信道可以看作是双向信道的一个特例, 如图 9.3 所示。在反馈信道中

正向信道传送信息,而反向信道只用来将接收信号反馈给发送端。

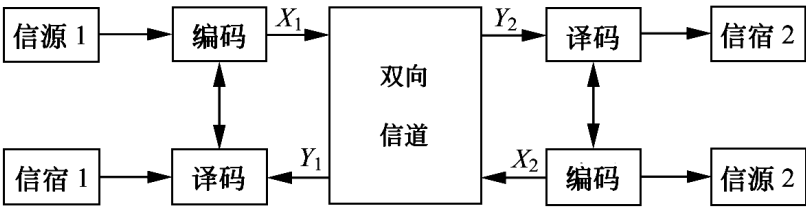


图 9.2 双向信道

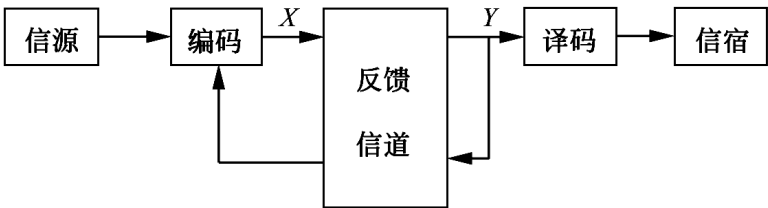


图 9.3 反馈信道

(3) 多源接入信道

多源接入或称多址接入信道是有多个信道输入信号,但只有一个信道输出信号的信道。信道的多个输入端口可供多个信源同时接入,故称多源接入信道,如图 9.4 所示。需要指出的是,接入信道的各个信源在地理上是分散的,所以无论是信源编码或是信道编码都必须分散进行。多源接入信道的这一特点使其有别于第 4 章所述的各种并联信道。和双向信道中 到的问题类似,在通信工程中多源或多址接入是用时分、频分或码分等方法将一个物理信道分成若干独立的子信道来实现的,因此各输入信号被局限在某种互不相交的子空间内。而在用信息论观点分析多源接入信道时就没有这样的限制。

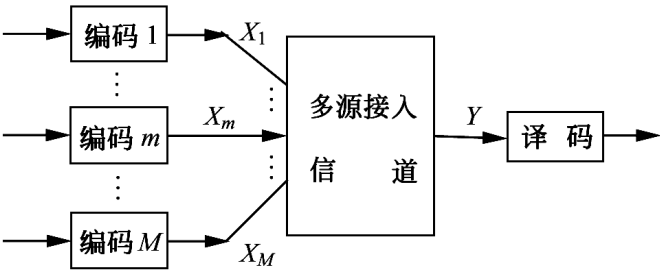


图 9.4 多源接入信道

(4) 广播信道

将多源接入信道中的信息流向全部反过来就得到广播信道。它有一个输入端口,多个输出端口,如图 9.5 所示。对这一信道需要强调的是各输出端口在地理上是分散的,各输出端口处信号受干扰的情况也不相同,因此译码只能分散独

立进行。与一般的广播概念不同的是各信宿要接收的信息并不一定相同, 图 中所画的  $M$  个信源明确地指明了这一点。在工程上  $M$  个信源以广播形式向  $M$  个信宿传送信息一般可采用时分方式, 但时分方式不一定是最佳的, 用信息论方法研究这一信道就是要搞清什么方式最好以及信道的容量域。当广播信道向所有信宿传送相同的信息且各输出端口的干扰情况相同时, 广播信道的问题就蜕化为单信道问题。

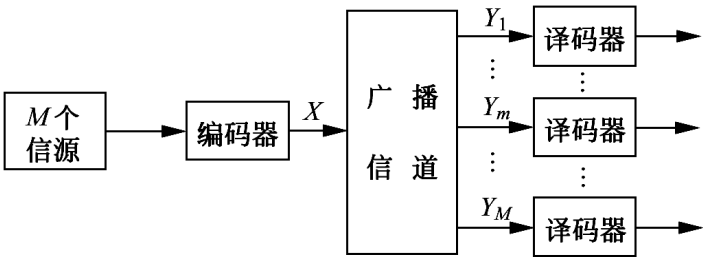


图 9.5 广播信道

(5) 中继信道

中继信道可以看成是广播信道与多源接入信道的组合, 如图 9.6 所示。它只有一个输入信号  $X$  和一个输出信号  $Y$ , 输入信号以广播形式同时送往中继点和终点, 中继点的输入信号是  $Y_1$ , 输出信号是  $X_1$ ,  $X_1$  和  $X$  再以多源接入方式送往终点, 最后得到信道输出  $Y$ 。信道的特性用  $p(y, y_1/x, x_1)$  描述。上述特点使其与通信工程师理解的中继通信不完全相同, 这是需要注意的。

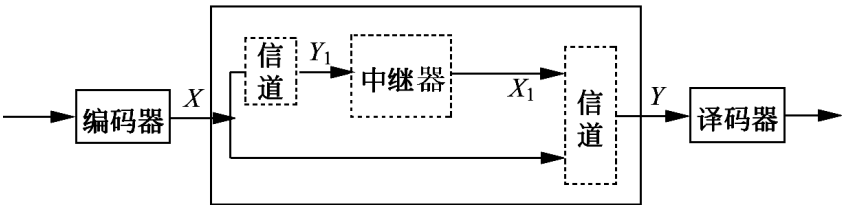


图 9.6 中继信道

在以上 5 种典型信道中, 多源接入信道是得到较好解决的信道, 对离散无记忆的反馈信道也已有明确的答案, 但双向信道、广播信道和中继信道的问题都尚未完全解决, 只得到部分的结果。

在信源编码方面, 通信网中的信源编码主要涉及地理上分散的若干信源的信息有效表示问题。这些在地理上分散的信源如果相互间是统计独立的, 则整个问题可被分解, 通信网中的信源编码也就蜕化为单信源的编码, 所以通信网中的信源编码主要讨论相关信源的编码。其次, 在通信网的信源编码中可能存在反馈, 这将使问题更趋复杂化。对通信网中信源编码问题的研究同样是从特殊

问题入手,提出一些典型问题,这些典型问题有时被称为模型。迄今为止已提出很多种模型,下面是几种有代表性的、且得到较好解决的模型。

(1) Berger 多端信源编码模型

这一模型是由 T . Berger 提出的。如图 9 .7 所示,编码器 1 和和编码器 2 是在不同地理位置的两个编码器,编码器向编码器或编码器向译码器传送信息的速率如图中  $R, R_{11}, R_{12}, R_{21}, R_{22}$  所示。这一模型可推广到多个信源及多个信宿的情况。T S . Han 等也提出过类似的多端信源编码模型,但在他们的模型中编码器与编码器之间没有联系,因而问题要简单些。

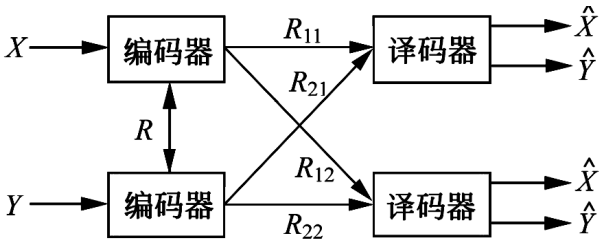


图 9 .7 Berger 多端信源编码

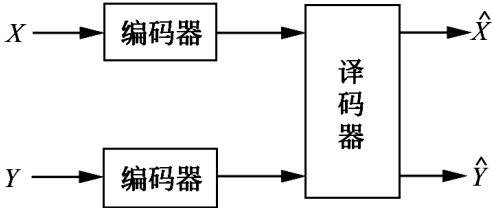


图 9 .8 Slepian-Wolf-Cover 模型

(2) Slepian- Wolf-Cover 模型

图 9 .8 所示的模型是现有几十种模型中最有实际意义且得到最好解决的模型,它是由 D . Slepian 和 J . K .Wolf 在 1973 年提出并解决的。我们在以后的讨论中将会作详细的介绍。

(3) 带边信息的信源编码

如图 9 .9 所示,带边信息的信源编码在组成上与 Slepian-Wolf-Cover 模型相似,其不同之处在于译码器只须译出  $X$  不需译出  $Y$ ,  $Y$  是作为一种辅助信息使用的,所以称为边信息。J . K rner, A . Wyner 等都研究过这一问题并给出其解。

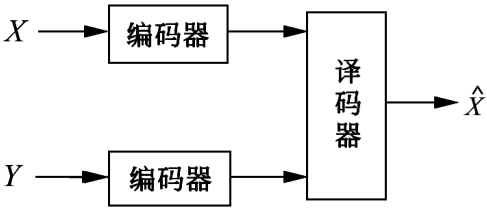


图 9 .9 带边信息的信源模型

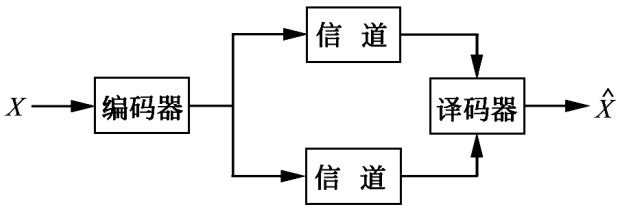


图 9 .10 带分集系统的信源模型

(4) 带分集系统的信源编码

如图 9 .10 所示,在这一模型中信源的编码输出经两个不同的信道传输后送入一个译码器,译码器得到的两个输入信号互相起辅助作用,达到分集的效果。

除上述有代表性的模型外还研究过很多其他的模型。在所有这些研究中首先研究的是冗余度压缩编码,部分扩展到熵压缩编码,后者有时被称为多端率失真理论。应该指出的是通信网中的信源编码虽然有工程应用的背景,但部分模型的提出更多考虑理论上的意义而与实际应用不一定有很强的联系,因此如何将这些理论成果应用于实际尚是今后要解决的问题。

不论是信道容量问题还是信源编码问题,在通信网的情况下要实现信息论所指出的最佳性能一般都会导致复杂的信号与信息处理。这种代价在多大程度上可接受完全是一个工程设计问题,这是工程师们在应用理论成果时需要注意和解决的。在目前技术条件下已有成果中的一部分虽然有很大的实际价值,如多源接入信道的容量定理为码分多址通信的多用户接收技术奠定了理论基础,但其实现时的代价仍然是其实用化的最大障碍。

## 9 2 反 馈 信 道

反馈信道的一般模型图已如图 9.3 所示,本节讨论反馈信道的一种最简单的情况。如图 9.11 所示,图中正向信道是一离散无记忆单用户信道,而反向信道是一个不发生差错的理想信道。信道输出  $Y$  通过反向信道被无误地反馈回发端。

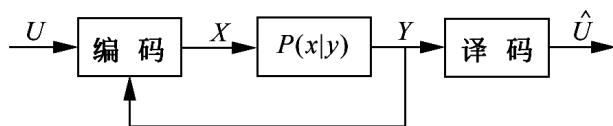


图 9.11 带有理想反馈的离散无记忆有反馈信道

设信道编码采用长为  $N$  的分组编码。由于有反馈的存在,发送码字的每一位码字母将可以不仅取决于信源的输入,而且还和此前反馈回来的接收码元有关。更确切地说,发送码字的第  $n$  位码元将不仅与信源输入有关,而且还取决于反馈回来的接收码字的前  $n-1$  位码元。反馈信道的利用显然使编码器获得了额外的有关正向信道传输差错情况的信息,从而改善信息的传输,但出乎一般意料的是这些信息并不能增加正向信道的信道容量。下述定理说明了这一点。

**定理 9.1** 带有理想反馈的离散无记忆信道的信道容量与无反馈时的信道容量相等。

**证明** 由于有反馈信息下的编码器仍然可以不使用反馈信息,因此为证明两者的信道容量相等只须证明有反馈时的信道容量没有增大。

在分组编码下, 设发送码字为  $\mathbf{x} = (x_1 x_2 \dots x_N)$ , 接收码字为  $\mathbf{y} = (y_1 y_2 \dots y_N)$ , 则收发码字间的互信息为

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}) &= I(X_1 X_2 \dots X_N; Y_1 Y_2 \dots Y_N) \\ &= H(Y_1 Y_2 \dots Y_N) - H(Y_1 Y_2 \dots Y_N / X_1 X_2 \dots X_N) \\ &= \sum_{n=1}^N H(Y_n) - \sum_{n=1}^N H(Y_n / X_1 X_2 \dots X_n, Y_1 Y_2 \dots Y_{n-1}) \end{aligned} \quad (9.1)$$

按无记忆信道的定义, 我们有

$$P(y_n | x_1 \dots x_n, y_1 \dots y_{n-1}) = P(y_n | x_n)$$

所以

$$\begin{aligned} I(\mathbf{X}; \mathbf{Y}) &= \sum_{n=1}^N H(Y_n) - \sum_{n=1}^N H(Y_n / X_n) \\ &= \sum_{n=1}^N I(X_n; Y_n) = NC \end{aligned} \quad (9.2)$$

证毕

下述定理是定理 9.1 的逆定理。

**定理 9.2** 若带有理想反馈的离散无记忆信道中的信息传输速率  $R$  大于正向信道的信道容量  $C$ , 则译码的码字差错概率将大于 0。

**证明** 设信道输入码字为  $\mathbf{x}$ , 输出码字为  $\mathbf{y}$ 。信道译码器根据接收码字  $\mathbf{y}$  给出发送码字的估值  $\hat{\mathbf{x}}$ , 当  $\hat{\mathbf{x}} \neq \mathbf{x}$  时译码发生错误。现引入随机变量  $E$ , 其值由下式确定:

$$E = \begin{cases} 1, & \text{当 } \hat{\mathbf{x}} = \mathbf{x} \\ 0, & \text{当 } \hat{\mathbf{x}} \neq \mathbf{x} \end{cases} \quad (9.3)$$

则有

$$\begin{aligned} H(E, \mathbf{X} / \mathbf{Y}) &= H(\mathbf{X} / \mathbf{Y}) + H(E / \mathbf{X}, \mathbf{Y}) \\ &= H(E / \mathbf{Y}) + H(\mathbf{X} / E, \mathbf{Y}) \end{aligned} \quad (9.4)$$

在得到  $\mathbf{Y}$  后译码器即可给出  $\hat{\mathbf{x}}$ , 故

$$H(E | \mathbf{X}, \mathbf{Y}) = 0 \quad (9.5)$$

此外,  $E$  只取两个可能的值, 故

$$H(E) = 1 \quad (9.6)$$

式(9.4)中另一项  $H(\mathbf{X} | E, \mathbf{Y})$  的值涉及发送码字集合的大小。当信息速率为  $R$  (比特/码字母) 时发送码字的集合最少应有  $2^{NR}$  个码字, 所以

$$\begin{aligned} H(\mathbf{X} / E, \mathbf{Y}) &= P(E = 0) H(\mathbf{X} / \mathbf{Y}, E = 0) + P(E = 1) H(\mathbf{X} / \mathbf{Y}, E = 1) \\ &= (1 - P_e) \times 0 + P_e \log(2^{NR} - 1) \end{aligned}$$



$$P_e NR \quad (9.7)$$

式中  $P_e$  即为译码的差错概率。

将式(9.5)至式(9.7)的结果代入式(9.4)即得

$$H(\mathbf{X}/\mathbf{Y}) = 1 + P_e NR \quad (9.8)$$

式(9.8)是著名的 Fano 不等式, 它是由 R. M. Fano 首先得到的。

现设信源等概地使用这  $2^{NR}$  个发送码字, 则

$$\begin{aligned} NR = H(\mathbf{X}) &= H(\mathbf{X}/\mathbf{Y}) + I(\mathbf{X};\mathbf{Y}) \\ &= 1 + P_e NR + I(\mathbf{X};\mathbf{Y}) \\ &= 1 + P_e NR + NC \end{aligned} \quad (9.9)$$

上式可改写为

$$P_e = 1 - \frac{C}{R} - \frac{1}{NR} \quad (9.10)$$

令  $N \rightarrow \infty$ , 得

$$P_e = 1 - \frac{C}{R} \quad (9.11)$$

所以

$$P_e > 0, \text{ 当 } R > C \quad (9.12)$$

证毕

对于反馈不能使信道容量增加这一现象可以直观地作这样的解释, 反馈是肯定能提供额外的信息的, 这是因为根据反馈回来的接收码元编码器可以确切知道信道干扰的情况, 但这些情况都是信道过去的情况, 由于信道的无记忆性这些信息对于了解信道现在和未来的干扰值毫无帮助, 所以编码器不可能利用这些信息去改善现时刻以及未来时刻的信息传输, 这就说明信道容量不可能增加。另一方面, 反馈使编码器知道过去发出的信息在传输中是否已发生差错, 从而可以采取有效的补救措施, 如重发。因此反馈在实际通信系统中的作用仍然是很大的, 它可以使无差错或接近无差错通信的实现变得容易起来。

如果正向信道是有记忆的, 则根据上述解释可以推知有反馈信道的容量将大于无反馈信道的容量, 所以定理 9.1 和定理 9.2 只在无记忆信道的条件下成立。

### 9.3 多个随机变量下的联合典型序列

我们在讨论信源编码时曾经指出离散无记忆信源的输出序列在长度足够长

时都是典型序列。典型序列的数量在所有可能序列的总数中虽然只占小部分,但是典型序列集合的概率却接近于 1,这一性质为信源编码奠定了基础。

在信道容量问题上,离散无记忆信道的输入序列与输出序列在序列足够长时是联合典型的,这一性质是信道编码定理的基础。

与上述情况一样,在用信息论观点分析通信网时联合典型序列的概念起着非常重要的作用。在这一节中我们将介绍分析下节讨论中需要的有关任意有限多个随机变量下联合典型序列的概念及其重要性质。

设  $\{X_1 X_2 \dots X_M\}$  为离散随机变量的有限集,其联合分布为  $p(x_1 x_2 \dots x_M)$ , 其中  $(x_1 x_2 \dots x_M) \in A_1 \times A_2 \times \dots \times A_M$ ,  $A_1 = \{a_{11}, a_{12}, \dots, a_{1K}\}$ ,  $A_m = \{a_{m1}, a_{m2}, \dots, a_{mK}\}$ 。令  $S$  是这些随机变量的某一有序子集,  $\mathbf{S}$  是  $N$  个独立  $S$  组成的长为  $N$  的序列,  $\mathbf{s}$  是  $\mathbf{S}$  的一个样本。例如,若  $S = (X_i, X_j)$ , 则

$$P(\mathbf{S} = \mathbf{s}) = P[(\mathbf{X}, \mathbf{X}_j) = (\mathbf{x}, \mathbf{x}_j)] = \prod_{n=1}^N p(x_{in}, x_{jn}) \quad (9.13)$$

按照大数定律,我们可以得到

$$-\frac{1}{N} \log p(s_1 s_2 \dots s_N) = -\frac{1}{N} \sum_{n=1}^N \log p(s_n) \rightarrow H(S) \quad (9.14)$$

即上式左端以概率 1 收敛于  $S$  的熵,  $S$  是上述随机变量集合  $\{X_1 X_2 \dots X_M\}$  中的任一个子集。这样的子集总共可有  $2^M$  个。

和第 3 章中定义典型序列集合  $G$  时的情况类似,我们定义  $M$  个随机变量集合时的联合典型序列集合  $G^N$  为

$$G^N(X_1 X_2 \dots X_M) = G^N(\mathbf{x} \mathbf{x} \dots \mathbf{x}_M); \left| \frac{1}{N} \log p(\mathbf{s}) + H(S) \right| < \epsilon, \quad \mathbf{S} \in \{X_1 X_2 \dots X_M\} \quad (9.15)$$

在上式中,  $S$  是  $(X_1 X_2 \dots X_M)$  的任一子集,所以联合典型序列实际需要满足  $2^M - 1$  个不等式约束。

联合典型序列可以是只对  $M$  个随机变量集合中的某一子集的,设子集的大小为  $L$ ,则此时只需要满足  $2^L - 1$  个不等式约束。

如果联合典型是相对于某一特定序列而言的,则得条件联合典型序列。例如,我们可用  $G^N(S_1 | \mathbf{s})$  表示  $S_1$  集合下相对于特定序列  $\mathbf{s}$  而言是联合典型的那些序列的集合。

下面三个定理给出了联合典型序列的概率、联合典型序列集合的概率、基数与随机变量集合的熵之间的关系。

**定理 9.3** 对任给  $\epsilon > 0$ , 总有足够大的  $N$  使下列不等式成立:

$$P(G^N(S)) = 1 - \epsilon, \quad S \in \{X_1, X_2, \dots, X_M\} \quad (9.16)$$

$$(1 - \epsilon)2^{N(H(S) - \epsilon)} < |G^N(S)| < 2^{N(H(S) + \epsilon)} \quad (9.17)$$

**证明** 对定理第一部分, 由  $G^N$  的定义可知这相当于要求证明

$$P\left|\frac{1}{N}\log p(\mathbf{s}) + H(S)\right| < \epsilon \quad (1 - \epsilon) \quad (9.18)$$

回忆第 3 章中定理 3.2 的证明方法, 利用大数定律即可证明式(9.18)成立。

对  $|G^N(S)|$ , 一方面我们有

$$1 > \sum_{\mathbf{s} \in G^N(S)} p(\mathbf{s}) \quad 2^{-N(H(S) + \epsilon)} = |G^N(S)| / 2^{-N(H(S) + \epsilon)} \quad (9.19)$$

另一方面有

$$1 - \epsilon = \sum_{\mathbf{s} \in G^N(S)} p(\mathbf{s}) \quad 2^{-N(H(S) - \epsilon)} = |G^N(S)| / 2^{-N(H(S) - \epsilon)} \quad (9.20)$$

由式(9.19)和式(9.20)即得式(9.17)。

**定理 9.4** 设  $S_1, S_2 \in \{X_1, X_2, \dots, X_M\}$ ,  $(\mathbf{s}, \mathbf{s}_2) \in G^N(S_1, S_2)$ , 定义  $G^N(S_1 | \mathbf{s})$  是  $\mathbf{s}$  序列中与特定  $\mathbf{s}$  序列联合典型的序列的集合。若  $\mathbf{s}_2 \in G^N(S_2)$ , 则对  $\epsilon > 0$  总可有足够大的  $N$  使下述不等式成立:

$$2^{-N(H(S_1/S_2) + 2\epsilon)} < p(\mathbf{s} | \mathbf{s}_2) < 2^{-N(H(S_1/S_2) - 2\epsilon)} \quad (9.21)$$

$$|G^N(S_1 | \mathbf{s}_2)| / 2^{N(H(S_1/S_2) + 2\epsilon)} \quad (9.22)$$

$$p(\mathbf{s}_2) / G^N(S_1 | \mathbf{s}_2) / (1 - \epsilon) 2^{N(H(S_1/S_2) - 2\epsilon)} \quad (9.23)$$

**证明** (1) 对  $(\mathbf{s}, \mathbf{s}_2) \in G^N(S_1, S_2)$ , 由定义可有

$$2^{-N(H(S_1) + \epsilon)} < p(\mathbf{s}) < 2^{-N(H(S_1) - \epsilon)} \quad (9.24)$$

$$2^{-N(H(S_1/S_2) + \epsilon)} < p(\mathbf{s} | \mathbf{s}_2) < 2^{-N(H(S_1/S_2) - \epsilon)} \quad (9.25)$$

将式(9.24)和式(9.25)代入  $p(\mathbf{s} | \mathbf{s}_2) = p(\mathbf{s}, \mathbf{s}_2) / p(\mathbf{s}_2)$ , 即可得式(9.21)。

(2) 由式(9.21)可得

$$1 \geq \sum_{\mathbf{s}_1 \in G^N(S_1 | \mathbf{s}_2)} p(\mathbf{s} | \mathbf{s}_2) \quad 2^{-N(H(S_1/S_2) + 2\epsilon)} = |G^N(S_1 | \mathbf{s}_2)| / 2^{-N(H(S_1/S_2) + 2\epsilon)}$$

此式即式(9.22)。

(3) 由式(9.21)还可有

$$1 - \epsilon = \sum_{\mathbf{s}_2 \in G^N(S_2)} p(\mathbf{s}) \quad P(\mathbf{s} | \mathbf{s}_2)$$

$$\begin{aligned}
 & \frac{p(\mathbf{s})}{G^N(S_2)} = \frac{2^{-N(H(S_1/S_2)-2)}}{G^N(S_1/S_2)} \\
 & = \frac{p(\mathbf{s}) / G^N(S_1/S_2)}{G^N(S_2)} \quad \text{证毕}
 \end{aligned}$$

此即式(9.23)。

**定理 9.5** 设  $S_1, S_2, S_3 \in \{X_1, X_2, \dots, X_M\}$ ,  $S_1, S_2, S_3$  是与  $S_1, S_2, S_3$  有相同成对边缘分布的随机变量集合, 但  $S_1$  与  $S_2$  在  $S_3$  条件下统计独立,  $G^N(S_1, S_2, S_3)$  是在  $p(\mathbf{s}, \mathbf{s}, \mathbf{s})$  分布下的联合典型序列集合, 则

$$2^{-N(I(S_1; S_2/S_3)+6)} < P[(S_1, S_2, S_3) \in G^N(S_1, S_2, S_3)] < 2^{-N(I(S_1; S_2/S_3)-6)} \quad (9.26)$$

**证明** 由条件  $S_1$  与  $S_2$  在  $S_3$  条件下统计独立, 即

$$P(S_1 = \mathbf{s}, S_2 = \mathbf{s}, S_3 = \mathbf{s}) = \prod_{n=1}^N p(s_{1n} / s_{3n}) p(s_{2n} / s_{3n}) p(s_{3n}) \quad (9.27)$$

故得

$$P[(S_1, S_2, S_3) \in G^N(S_1, S_2, S_3)] = \frac{p(\mathbf{s} / \mathbf{s}) p(\mathbf{s} / \mathbf{s}) p(\mathbf{s})}{G^N(S_1, S_2, S_3)} \quad (9.28)$$

由典型序列定义, 知

$$2^{-N(H(S_3)+1)} < p(\mathbf{s}) < 2^{-N(H(S_3)-1)} \quad (9.29)$$

将关系式(9.29)及式(9.21)代入式(9.28), 即得

$$\begin{aligned}
 P[(S_1, S_2, S_3) \in G^N(S_1, S_2, S_3)] & \geq \frac{G^N(S_1, S_2, S_3)}{G^N(S_1, S_2, S_3)} \cdot 2^{-N[H(S_3)-1+H(S_1/S_3)-2+H(S_2/S_3)-2]} \\
 & = 2^{-N[H(S_1, S_2, S_3)+1]} \cdot 2^{-N[H(S_3)+H(S_1/S_3)+H(S_2/S_3)-5]} \\
 & = 2^{-N[I(S_1; S_2/S_3)-6]}
 \end{aligned}$$

以及

$$P[(S_1, S_2, S_3) \in G^N(S_1, S_2, S_3)] \leq 2^{-N[I(S_1; S_2/S_3)+6]} \quad \text{证毕}$$

定理 9.5 在计算译码差错概率时要用到。在这里我们仅强调指出  $(\mathbf{s}, \mathbf{s}, \mathbf{s})$  序列是满足上述条件统计独立要求的, 而  $(\mathbf{s}, \mathbf{s}, \mathbf{s}) \in G^N(S_1, S_2, S_3)$  并不满足上述条件统计独立要求, 所以这一定理所计算的是  $G^N(S_1, S_2, S_3)$  中满足上述条件统计独立的  $(\mathbf{s}, \mathbf{s}, \mathbf{s})$  产生的那一部分序列的概率。

## 9.4 多源接入信道

### 9.4.1 多源接入信道的容量

多源接入信道是通信网模型中得到最多了解的一种模型,模型的一般表示已如图 9.4 所示。这一节的内容将以二源接入信道为例,深入细致地分析其容量。其结果将不难推广到多源接入的情况。

对离散无记忆二源接入信道,设输入信号  $X_1$  和  $X_2$  分别取值于字母表  $A_1$  和  $A_2$ ,输出信号  $Y$  取值于字母表  $B$ ,信道特性由转移概率  $p(y|x_1 x_2)$  表示。

信源 1 和信源 2 各利用信道输入  $X_1$  和  $X_2$  传送信息。设信道编码采用长为  $N$  的复合分组码  $(2^{NR_1}, 2^{NR_2}, N)$ , 其中  $2^{NR_1}$  和  $2^{NR_2}$  分别是与长  $N$  的码字对应的这两个信源中的消息数,即信源 1 的消息集为  $M_1 = (1, 2, \dots, 2^{NR_1})$ , 信源 2 的消息集为  $M_2 = (1, 2, \dots, 2^{NR_2})$ 。在发送时,信道编码器  $g_1$  和  $g_2$  分别将这两个信源的消息  $m_1$  和  $m_2$  映射成  $A_1^N$  和  $A_2^N$  中对应的码字;而在接收端,译码器根据接收信号恢复信源发生的消息,这些函数关系可表示成

$$\begin{aligned} g_1: M_1 &\rightarrow A_1^N \\ g_2: M_2 &\rightarrow A_2^N \\ h: B^N &\rightarrow (M_1, M_2) \end{aligned}$$

由于信道噪声的作用,译码器的输出并不总能和发送的消息一致,其平均的差错概率为

$$P_e = \sum_{(m_1, m_2) \in (M_1, M_2)} P(m_1, m_2) P(h(B^N) \neq (m_1, m_2) | \text{发}(m_1, m_2)) \quad (9.30)$$

如果假定  $m_1$  和  $m_2$  分别等概地取自  $(1, 2, \dots, 2^{NR_1})$  和  $(1, 2, \dots, 2^{NR_2})$ , 则

$$P_e = \frac{1}{2^{N(R_1 + R_2)}} \sum_{(m_1, m_2) \in (M_1, M_2)} P(h(B^N) \neq (m_1, m_2) | \text{发}(m_1, m_2)) \quad (9.31)$$

此时信源 1 和信源 2 的信息速率即为  $R_1$  和  $R_2$ 。信源的信息速率还不是信道传输信息的速率,但如果信道编码能使  $P_e \rightarrow 0$ , 则  $R_1$  和  $R_2$  即为信源通过信道传输信息的速率。我们把存在信道编码使  $P_e \rightarrow 0$  的速率对  $(R_1, R_2)$  称为可达速率对,而所有可达速率对的集合就称为此信道的信道容量域。

多源接入信道容量域的上述定义与第 4 章中通过互信息定义单用户信道容

量在本质上是一致的。实际上,在单用户信道中我们也可以通过信道编码的概念定义信道容量,并得到相同的容量值。信道容量域的这种定义方法把信道编码和信道容量域联系在一起,对工程实现来讲是特别有吸引力的。但在下面的讨论中我们将会看到这种定义方法并不能给实际信道中信道容量的计算带来任何简捷的途径,这是因为寻找最佳信道编码的工作对多元接入信道来讲也是一个困难的问题。迄今为止,香农提出的随机编码的概念仍然是这一定义下计算信道容量的唯一办法。下述定理就是利用随机编码的概念给出二源接入信道的信道容量域的。

**定理 9.6** 二源接入信道  $(A_1, A_2, B, p(y|x_1 x_2))$  的信道容量域是下述可达速率对  $(R_1, R_2)$  集合的凸包(集合元素一切可能凸组合的全体),即

$$R_1 < I(X_1; Y / X_2) \quad (9.32)$$

$$R_2 < I(X_2; Y / X_1) \quad (9.33)$$

$$R_1 + R_2 < I(X_1, X_2; Y) \quad (9.34)$$

式中互信息是在相应输入信号概率分布  $p_1(x_1)p_2(x_2)$  下取的值。

**证明** 下面分两步给出证明,首先证明符合定理条件的速率对是可达的,然后证明容量域是上述速率对集合的凸包。

(1) 证明符合式(9.32)、(9.33)和式(9.34)的速率对是可达速率对。

在这一证明中核心的问题是如何找到能够使  $P_e \rightarrow 0$  的信道编码方法,即函数  $g_1$  和  $g_2$ 。但这是一个很困难的问题,解决的办法是采用香农提出的随机编码方法。按照这一方法,设信道输入的概率分布为  $p(x_1 x_2) = p_1(x_1)p_2(x_2)$ ,则相应于信源 1 的第  $m_1$  个码字是按  $p_1(x_1)$  分布独立产生的,即码字  $\mathbf{X}(m_1)$  取  $x_{11} x_{12} \dots x_{1N}$  的概率为  $\prod_{n=1}^N p_1(x_{1n})$ 。而且,对应信源 1 的  $2^{NR_1}$  个码字都是按这种方法独立产生的。按照这一方法产生  $2^{NR_1}$  个码字后,一本码书就算完成了;对于信源 2 可用同样的办法产生一本包含有  $2^{NR_2}$  个码字的码书。显然,在这样生成的码书中两个码字完全相同的情况是有可能发生的。

信道译码的原则比较简单,当接收端收到  $Y^N$  时译码器选择这样的  $(m_1, m_2)$  值,使

$$(\mathbf{X}(m_1), \mathbf{X}(m_2), \mathbf{Y}) \in G^N \quad (9.35)$$

其中,  $m_1 = (1, 2, \dots, 2^{NR_1})$ ,  $m_2 = (1, 2, \dots, 2^{NR_2})$ 。如果满足联合典型的  $(m_1, m_2)$  值存在且唯一,则译码无误,否则就有差错发生。

在上述编码方法中,如果我们把所生成的码书看成是一本固定的码书,则平

均译码差错概率的计算仍然是相当困难的。而香农随机编码的方法并不是仅仅指用随机方法产生一本码书,而是用随机方法产生所有可能的码书。对信源 1 而言某一特定码书的生成概率将是

$$\frac{1}{2^{NR_1}} \prod_{m_1=1}^N p_1(x_{1n}(m_1))$$

式中  $x_{1n}(m_1)$  是指信源 1 的第  $m_1$  个码字中第  $n$  个码元所取的值;对信源 2 的码书,情况完全相似。在这样的编码方法下,所得的码是完全对称的,这就是说信源的每一个消息将以相同的概率分布映射为某一码字。因此,平均的译码差错概率将等于发送任一消息对下的条件译码差错概率。基于这一原因,为计算平均差错概率,我们可以假设  $(m_1, m_2)$  取任一可能的值,例如可以取  $(m_1, m_2) = (1, 1)$ 。

在这样的假设下,如果接收信号与消息对  $(1, 1)$  对应的码字构成唯一的一组联合典型序列,则译码正确。我们把这样的事件记作  $E_{11}$ , 即

$$E_{11} = \{(\mathbf{X}(1), \mathbf{X}(1), \mathbf{Y}) \in G^N\} \quad (9.36)$$

则由差错概率的联合界即得

$$P_e = P(E_{11}^c) + \sum_{(i,j) \neq (1,1)} P(E_{ij}) \quad (9.37)$$

式中  $E_{ij}$  为

$$E_{ij} = \{(\mathbf{X}(i), \mathbf{X}(j), \mathbf{Y}) \in G^N\} \quad (9.38)$$

式(9.37)中各项的值如下。

首先,由式(9.16)可知,当  $N \rightarrow \infty$ ,  $P(E_{11}^c) \rightarrow 0$ 。其次,对  $E_{i1} (i \neq 1)$ , 因  $\mathbf{X}(i)$  与  $(\mathbf{X}(1), \mathbf{Y})$  独立无关, 故

$$P(E_{i1}) = P((\mathbf{X}(i), \mathbf{X}(1), \mathbf{Y}) \in G^N) = \sum_{(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}) \in G^N} p(\mathbf{x}) p(\mathbf{x}, \mathbf{y}) / G^N = 2^{-N(H(X_1) + H(X_2|Y))}$$

由定理 9.3 得

$$P(E_{i1}) = 2^{-N[H(X_1) + H(X_2|Y) - H(X_1 X_2 Y) - 3J]} = 2^{-N[I(X_1; X_2 Y) - 3J]}$$

由于  $X_1$  与  $X_2$  独立, 故

$$I(X_1; X_2 Y) = I(X_1; X_2) + I(X_1; Y | X_2) = I(X_1; Y | X_2)$$

这样就得

$$P(E_{ii}) = 2^{-N(I(X_1; Y|X_2) - 3)} \quad (9.39)$$

利用同样的推理,可得

$$P(E_{jj}) = 2^{-N(I(X_2; Y|X_1) - 3)}, j = 1 \quad (9.40)$$

最后,对  $E_{ij}$ , 由于  $\mathbf{Y}$  是  $(\mathbf{X}(1), \mathbf{X}(1))$  产生的信道输出, 与  $(\mathbf{X}(i), \mathbf{X}(j))$  独立无关, 故

$$P(E_{ij}) = P((\mathbf{X}(i), \mathbf{X}(j), \mathbf{Y}) \in G^N) = \sum_{(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}) \in G^N} p(\mathbf{x}, \mathbf{x}) p(\mathbf{y}) \quad (9.41)$$

$$2^{-N[H(X_1 X_2) + H(Y) - H(X_1 X_2 Y) - 3]} = 2^{-N[I(X_1 X_2; Y) - 3]}$$

将式(9.39)、(9.40)和式(9.41)代入式(9.37)得

$$P_e = P(E_{11}) + 2^{-N[I(X_1; Y|X_2) - R_1 - 3]} + 2^{-N[I(X_2; Y|X_1) - R_2 - 3]} + 2^{-N[I(X_1 X_2; Y) - (R_1 + R_2) - 3]} \quad (9.42)$$

由定理所给条件式(9.32)、(9.33)和式(9.34)可知, 当  $N \rightarrow \infty$  时, 式(9.42)右端趋于零, 故定理所给的速率对是可达速率对。

(2) 证明信道容量域是上述可达速率对的凸包。

集合的凸包是指集合中所有元素的一切可能的凸组合的全体, 所以只须证明若  $(R_1, R_2)$  和  $(R_1, R_2)$  都是可达速率对, 则  $(\alpha R_1 + (1 - \alpha) R_1, \alpha R_2 + (1 - \alpha) R_2)$  也是可达速率对, 其中  $0 \leq \alpha \leq 1$ 。

这一证明只须利用时分的概念, 将整个时间分为  $\alpha$  和  $1 - \alpha$  两部分, 在  $\alpha$  部分时间中使用  $(R_1, R_2)$  对应的编码, 而在  $1 - \alpha$  部分时间中采用  $(R_1, R_2)$  对应的编码。这样, 信源 1 的速率将是  $\alpha R_1 + (1 - \alpha) R_1$ , 信源 2 的信息速率为  $\alpha R_2 + (1 - \alpha) R_2$ , 此时, 平均译码差错概率显然小于这两部分时间中的平均译码差错概率之和。所以在  $N \rightarrow \infty$  时也趋于零, 上述凸组合速率对可达。证毕

上述二源接入信道下的信道容量域定理可以直接推广到多源接入信道, 并得到下述定理。

**定理 9.7** 多源接入信道的容量域是满足下述不等式约束的速率矢量集的凸包

$$R(S) \leq I(X(S); Y | X(S^c)), S \in \{X_1, X_2, \dots, X_M\} \quad (9.43)$$

式中互信息是在相应概率分布  $p_1(x_1), p_2(x_2), \dots, p_M(x_M)$  下的值。

此外, 可以证明定理 9.6 的逆定理也成立, 即若条件(9.32)、(9.33)和(9.34)不满足, 则不存在能使译码差错率趋于零的码。所以这些条件既是充分的, 也是必要的。这一结果同样可推广到二源以上的多源接入信道。这些定理的证明此处从略。



## 9.4.2 相关信源输入下的多源接入信道

在多源接入信道中如果令  $M = 1$ , 则多源接入信道蜕化为单输入单输出的单用户信道, 这时我们在多源接入信道下所给出的关于信息传输可达速率的定义以及关于容量域的定理也将蜕化为单用户信道的信息传输可达速率与信道容量。不难理解由此所得的单用户信道容量域的上界即为第 4 章中按最大互信息定义的信道容量。但是, 在这里需要强调指出的是上述多源接入信道容量域的上界一般来讲不是多源接入信道输入输出之间的最大互信息。这是因为在多源接入信道可达速率的定义中已经假定各输入信号是统计独立的, 所以最大互信息是在改变  $\prod_{m=1}^M p(x_m)$ , 而不是改变  $p(x_1 x_2 \dots x_M)$  的条件下取得的。显然, 如果容许的输入概率分布是在所有可能的  $p(x_1 x_2 \dots x_M)$  集合中选取, 则输入信号集合的联合概率分布就可与信道转移概率达到更好的匹配, 从而使多源接入信道的可达速率增大。

## 9.5 高斯多源接入信道

### 9.5.1 高斯多源接入信道的容量域

高斯多源接入信道是多源接入信道的一个重要实例。在这个信道中各信源来的信号在接收端相加, 并受加性高斯噪声的干扰。图 9.12 所示是离散无记忆高斯二源接入信道示意图。按图 9.12, 信道输出  $Y$  为

$$Y = X_1 + X_2 + Z \quad (9.44)$$

式中噪声  $Z$  是独立同分布零均值的高斯随机变量, 方差为  $P_N$ , 信道输入  $X_1$  和  $X_2$  受平均功率限制, 即

$$E(X_m^2) \leq P_{sm}, m = 1, 2, \dots \quad (9.45)$$

显然, 这一信道的可达速率对应该满足定理 9.6 给出的一般条件, 所以现在只需将式(9.32)至式(9.34)中的互信息在高斯多源接入信道下的值计算出来。

首先, 由  $X_1, X_2, Z$  的相互独立性可得

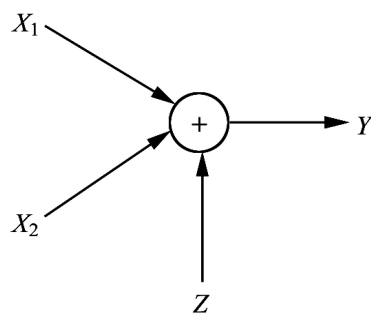


图 9.12 高斯二源接入信道

$$\begin{aligned}
I( X_1 ; Y \mid X_2 ) &= h( Y \mid X_2 ) - h( Y \mid X_1 X_2 ) \\
&= h( ( X_1 + X_2 + Z ) \mid X_2 ) - h( ( X_1 + X_2 + Z ) \mid X_1 X_2 ) \\
&= h( X_1 + Z \mid X_2 ) - h( Z \mid X_1 X_2 ) = h( X_1 + Z ) - h( Z ) \\
&= h( X_1 + Z ) - \frac{1}{2} \log(2 \text{ e } P_N)
\end{aligned}$$

$$\frac{1}{2} \log(2 - e^{-(P_{S_1} + P_N)}) - \frac{1}{2} \log(2 - e^{-P_N}) = \frac{1}{2} \log \left( 1 + \frac{P_{S_1}}{P_N} \right) \quad (9.46)$$

代入式(9-32),就有

$$R_1 < \frac{1}{2} \log \left( 1 + \frac{P_{s_1}}{P_N} \right) = G \quad (9.47)$$

同理可得

$$R_2 < \frac{1}{2} \log \left( 1 + \frac{P_{s_2}}{P_N} \right) = C \quad (9.48)$$

$$R_1 + R_2 < \frac{1}{2} \log 1 + \frac{P_{s_1} + P_{s_2}}{P_N} = C_{+2} \quad (9.49)$$

按条件(9.47)、(9.48)和(9.49)所得高斯二源接入信道的容量域如图 9.13 所示, 这个由所有可达速率对组成的凸包是一个凸五边形, 图中  $C_1 = \frac{1}{2} \log \left( 1 + \frac{P_{S_1}}{P_{S_2} + P_N} \right)$ ,  $C_2 = \frac{1}{2} \log \left( 1 + \frac{P_{S_2}}{P_{S_1} + P_N} \right)$ 。

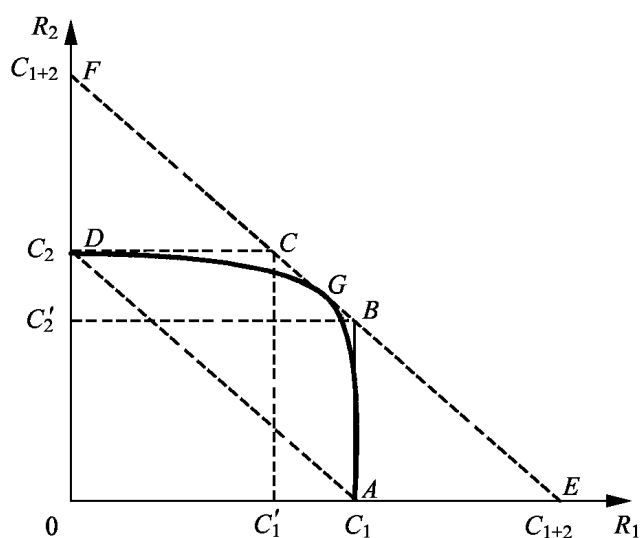


图 9.13 高斯二源接入信道的容量域

上述对高斯二源接入信道的分析和结论不难推广到高斯多源接入信道的情

况。设信道共有  $M$  个输入 ( $X_1 X_2 \dots X_M$ ), 各自的功率限制为 ( $P_{s_1}, P_{s_2}, \dots, P_{s_M}$ ),  $S$  是这一输入信号集合的任一子集, 则其信道容量域的表示式为

$$R_m = \frac{1}{2} \log \left( 1 + \frac{P_{s_m}}{P_N} \right) \quad (9.50)$$

显然, 这一容量域是  $M$  维空间中的一个凸多面体。随着  $M$  的加大, 总速率  $R_m$  。

## 9.5.2 对高斯多源接入信道容量域的讨论

下面从两个方面对高斯多源接入信道的容量作一讨论。首先讨论这一容量域的物理意义, 然后讨论这一容量域与通信工程中多址方法的关系。

### (1) 高斯多源接入信道容量域的物理意义

我们以高斯二源接入信道的容量域为例来具体解释容量域的构成机理, 如图 9.13 所示, 这一容量域以  $ABCD$  边为界。在  $A$  点  $R_2 = 0$ , 这时  $X_2$  取常数  $C$  或等于零, 所以

$$\max R_1 = \max_{X_2=C} I(X_1; Y | X_2) = \max I(X_1; Y) = \frac{1}{2} \log \left( 1 + \frac{P_{s_1}}{P_N} \right) = G$$

此后  $R_2$  开始增大, 这意味着  $X_2$  的平均功率增加, 由于  $X_1$  的平均功率在  $A$  点已经达到  $P_{s_1}$ , 所以在  $R_1$  增大时,  $R_1$  的速率已无法增加; 另一方面,  $X_2$  信号对  $X_1$  来讲是一种加性干扰, 但由于接收处信号的总功率也已增加, 所以仍可保证  $R_1$  有最大的信息传输速率而不会降低, 这样, 容量域的边界就由  $A$  点垂直向上直到  $B$  点。在  $B$  点处,  $X_2$  的平均功率增大到最大容许值  $P_{s_2}$ , 此后,  $R_2$  已无法在保持  $R_1$  不变的条件下继续上升, 这样就进入  $BC$  段。在  $BC$  段,  $X_1$  和  $X_2$  的平均功率都达到各自的最大容许值  $P_{s_1}$  和  $P_{s_2}$ , 所以总功率为常数, 总的信息传输速率  $R_1 + R_2$  也为常数, 此后  $R_2$  的继续增大是以降低  $R_1$  为代价来达到的, 具体的实现则是依靠编码方法的改变, 这一过程在  $C$  点结束。在  $C$  点以后  $X_2$  的平均功率保持不变, 但  $X_1$  的平均功率下降, 导致  $X_1$  的信息传输速率下降, 此过程以  $D$  为终点, 此时  $R_1 = 0, R_2 = G$ 。

高斯多源接入信道容量域中最重要的一个结论是: 当地理上分散的各个信源共用一个信道时, 尽管它们相互间没有联系且各自独立受平均功率的限制, 但其总容量的最大值却与单个信源受相同总平均功率限制下可以达到的

容量相同。关于如何在这样的情况下实现无误的传输,信息论提供的解释是这样的。当  $X_1$  和  $X_2$  各以  $P_{s_1}$  和  $P_{s_2}$  的平均功率传送信息时,如果  $R_1 < \frac{1}{2} \log 1 + \frac{P_{s_1}}{P_{s_2} + P_N}$ , 则  $X_1$  携带的信息可被完全正确地恢复。在这基础上,就可从接收的总信号中减去  $X_1$  并随后正确地获得  $X_2$  携带的信息。由于  $X_1$  这时已不对  $X_2$  构成干扰,所以  $X_2$  信号传送信息的速率为  $\frac{1}{2} \log 1 + \frac{P_{s_2}}{P_N}$ , 这一工作状态对应于图 9.13 中的点  $C$ 。相反,如把  $X_1$  信号看作是对  $X_2$  的干扰,则  $R_2 < \frac{1}{2} \log 1 + \frac{P_{s_2}}{P_{s_1} + P_N}$ , 此时得到正确恢复的  $X_2$  信号就可以从接收信号中减去,因此  $R_1 < \frac{1}{2} \log 1 + \frac{P_{s_1}}{P_N}$ , 这一工作状态恰好对应于图 9.13 中的点  $B$ 。不难证明,对  $B, C$  两点我们有

$$C_1 + C_2 = \frac{1}{2} \log 1 + \frac{P_{s_1}}{P_N} + \frac{1}{2} \log 1 + \frac{P_{s_2}}{P_{s_1} + P_N} = \frac{1}{2} \log 1 + \frac{P_{s_1} + P_{s_2}}{P_N} \quad (9.51)$$

$$C_2 + C_1 = \frac{1}{2} \log 1 + \frac{P_{s_2}}{P_N} + \frac{1}{2} \log 1 + \frac{P_{s_1}}{P_{s_2} + P_N} = \frac{1}{2} \log 1 + \frac{P_{s_1} + P_{s_2}}{P_N} \quad (9.52)$$

所以总的容量都达到了  $\frac{1}{2} \log 1 + \frac{P_{s_1} + P_{s_2}}{P_N}$ 。

### 9.5.3 多源接入信道容量域与多址方法的关系

前已指出,多源接入信道是以各种实用多址通信系统为背景建立的一种通信系统模型。因此信息论对这种信道容量域的分析结果自然应对实用多址通信系统中多址方法的比较选择有指导作用。在实用的多址通信系统中,常用的多址方法有频分多址、时分多址和码分多址三种。从信号理论上讲,这三种多址方法都是基于信号空间的正交分解,将整个信道划分为若干个独立的互不干扰的子信道。每个信源可使用一个子信道传送信息,其差别仅在于所取正交函数族的不同。但是在这三种多址方法下信道实际可达的信道容量是不完全一样的。下面以二源接入信道为例,对这三种多址方法作一比较。

首先来看时分多址。我们已经知道信号  $X_1$  的最大信息传输速率为  $C_1 = \frac{1}{2} \log 1 + \frac{P_{s_1}}{P_N}$ , 信号  $X_2$  的最大信息传输速率为  $C_2 = \frac{1}{2} \log 1 + \frac{P_{s_2}}{P_N}$ 。现在假设  $X_1$  和  $X_2$  以时分多址方法共用这一信道, 占用时间的百分比各为  $\alpha$  和  $1 - \alpha$ , 则  $R_1$  和  $R_2$  将沿  $AD$  线变化, 其可达速率域显然小于  $ABCD$  所示的理论容量域。但在这里需要指出的是对平均功率的理解。在上述讨论中, 平均功率实际上已被理解为“短时”平均功率, 即在时分多址所给定时隙中的平均功率而非全部时间平均的平均功率。如果我们把  $X_1$  和  $X_2$  在全部时间平均的平均功率限制在  $P_{s_1}$  和  $P_{s_2}$ , 则在它们以时分多址方法共用信道时其可达速率对将是

$$R_1 + R_2 = \frac{1}{2} \log 1 + \frac{P_{s_1}}{P_N} + \frac{1}{2} (1 - \alpha) \log 1 + \frac{P_{s_2}}{(1 - \alpha) P_N} \quad (9.53)$$

其边界将如图 9.13 中的曲线所示。当  $\alpha$  满足关系式

$$\alpha = \frac{P_{s_1}}{P_{s_1} + P_{s_2}} \quad (9.54)$$

时, 曲线与理论容量域的边界  $BC$  相切于  $G$ , 这时时分多址实现的容量达到了理论容许的最大值。在  $\alpha$  取其他数值时, 时分多址可达到的速率均小于理论容量域所给出的最大速率。

时分多址在什么条件下可实现  $BC$  线所示的最大容量呢? 答案很简单。如果把  $X_1$  和  $X_2$  的短时平均功率都限制在  $P_{s_1} + P_{s_2}$  以下, 则在  $X_1$  和  $X_2$  以时分多址共用信道时其速率将按  $EF$  直线变化, 其中就包括了  $BC$  直线段, 所以这是以加大短时平均功率为代价才达到的。

其次来看频分多址方法。这时需要利用限带加性白色高斯噪声信道容量的公式

$$C = W \log 1 + \frac{P_s}{N_0 W} \text{ bit/s} \quad (9.55)$$

设信道的总频带被分成  $W_1$  和  $W_2$  两部分, 则按前面的分析不难得出

$$R_1 = W_1 \log 1 + \frac{P_{s_1}}{N_0 W_1}, \quad R_2 = W_2 \log 1 + \frac{P_{s_2}}{N_0 W_2} \quad (9.56)$$

当  $W = W_1$  或  $W = W_2$  时,  $R_1$  或  $R_2$  分别达到其最大值, 这相当于  $A, D$  两点。随着  $W_1, W_2$  的变化,  $R_1 + R_2$  也将沿曲线变化。当  $W_1, W_2$  的值满足关系式

$$\frac{W_1}{W} = \frac{P_{s_1}}{P_{s_1} + P_{s_2}}, \quad \frac{W_2}{W} = \frac{P_{s_2}}{P_{s_1} + P_{s_2}} \quad (9.57)$$

时

$$\begin{aligned}
 R_1 + R_2 &= W_1 \log \left( 1 + \frac{P_{s_1} + P_{s_2}}{N_0 W} \right) + W_2 \log \left( 1 + \frac{P_{s_1} + P_{s_2}}{N_0 W} \right) \\
 &= W \log \left( 1 + \frac{P_{s_1} + P_{s_2}}{N_0 W} \right) \quad (9.58)
 \end{aligned}$$

此曲线与  $BC$  线相切, 此时频分多址的速率也达到理论容量域的最大值。这一情况与时分多址极其相似。

所以, 在相同的平均功率约束下, 时分多址与频分多址可达到的信息传输速率域均小于理论给出的容量域。但适当设计时隙分配或带宽分配的比例, 时分多址与频分多址都可使速率达到理论容量域所给的最大值。

码分多址技术中所有信道输入信号都占用信道的全部带宽和时间, 各信号间不存在时隙分配或带宽分配问题, 因此码分多址的可达速率域与理论容量域一致。在这一意义且仅在这一意义上我们可以认为码分多址方法是比较理想的方法。

## 9.6 分布信源编码

分布信源编码是通信网对信源编码提出的诸多问题中较为典型和重要的一个, 也是目前已得到较好解决的一个通信网信源编码问题。

离散无记忆分布信源编码的一般模型如图 9.14 所示。图中  $U_1, \dots, U_M$  是  $M$  个在地理上分散的信源, 各自的信源字母表为  $A_m (m = 1, 2, \dots, M)$ 。分布信源的联合概率分布为  $p(u_1 u_2 \dots u_M)$ , 具有联合熵  $H(U_1 U_2 \dots U_M)$ 。分布信源的输出是一个独立同分布随机矢量序列  $(u_{11}, u_{12}, \dots, u_{m1}, \dots, u_{M1}), (u_{12}, u_{13}, \dots, u_{m2}, \dots, u_{M2}), \dots, (u_{1n}, u_{1n+1}, \dots, u_{mn}, \dots, u_{Mn}), \dots$ 。分布信源编码的问题是如何对这一输出进行编码以达到冗余度的压缩。由于信源在地理上是分散的, 所以编码也是分散进行的。如图 9.14 所示, 有  $M$  个子编码器与各自的信源相连并对各自的输入进行编码, 但译码器只有一个,  $M$  个子编码器的输出将一并输入这一译码器, 由译码器恢复  $M$  个信源的输出。

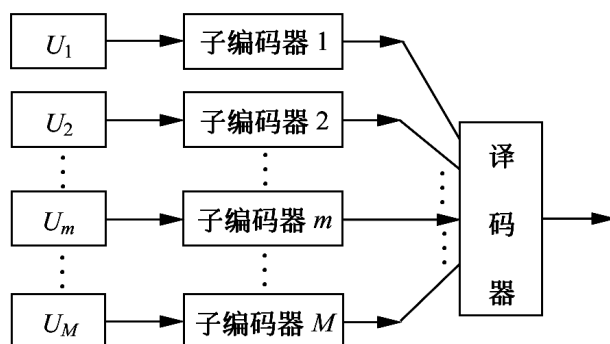


图 9.14 分布信源编码

现设  $M=2$ , 并采用等长的分组编码, 则一个涉及两个信源的分布信源编码可以按如下方法构造。

首先, 将两个信源输出的信源字母序列等分成长为  $N$  的信源字。两个子编码器的码字母表  $B_m (m=1, 2)$  采用相同的字母集  $Z = \{0, 1\}$ 。对两信源来的信源字, 子编码器将其分别映射为长  $NR_1$  和  $NR_2$  位码字母的码字, 这一映射用  $F_1$  和  $F_2$  表示为

$$F_1: A_1^N \rightarrow Z_2^{NR_1} \quad (9.59)$$

$$F_2: A_2^N \rightarrow Z_2^{NR_2} \quad (9.60)$$

这两个子编码器的输出一并输入译码器, 在译码器中恢复信源输出的信源字。这一映射可用  $D$  表示

$$D: Z_2^{NR_1} \times Z_2^{NR_2} \rightarrow A_1^N \times A_2^N \quad (9.61)$$

上述编码和译码就组成一个  $((2^{NR_1}, 2^{NR_2}), N)$  分布信源码。  $(R_1, R_2)$  是这一分布信源码的速率对, 因为当信源每秒送出一个信源字母时, 子编码器输出的二元字母数正是  $R_1$  和  $R_2$ 。

显然, 分布信源码的速率对  $(R_1, R_2)$  必须足够大以保证每个信源字对能映射为特定的码字对, 否则译码将发生错误, 译码的差错率  $P_e$  为

$$P_e = P[D(F_1(A_1^N), F_2(A_2^N)) \neq (A_1^N, A_2^N)] \quad (9.62)$$

对于某一给定的分布信源对  $U_1, U_2$ , 如果存在分布信源码  $((2^{NR_1}, 2^{NR_2}), N)$  能使  $N \rightarrow \infty$  时  $P_e \rightarrow 0$ , 则我们称速率对  $(R_1, R_2)$  是可达的。

按照第 3 章所述信源编码的理论, 如果信源不是分散的, 则可把信源  $U_1$  和  $U_2$  看作是联合熵为  $H(U_1 U_2)$  的联合信源, 这时取  $R_1 + R_2 > H(U_1 U_2)$  就可保证有能使译码的差错概率在  $N \rightarrow \infty$  时趋于零的分组码存在。但在联合信源时, 对  $U_1, U_2$  的编码是在单个编码器中统一进行的, 而在分布信源时这只能分别进行。D. Slepian 和 J. K. Wolf 在 1973 年时研究了这一问题并取得下述结果。

**定理 9.8** 对联合分布为  $p(u_1 u_2)$  的独立同分布离散无记忆分布信源  $(U_1, U_2)$ , 分布信源编码的可达速率对  $(R_1, R_2)$  满足不等式

$$R_1 \geq H(U_1 | U_2), \quad R_2 \geq H(U_2 | U_1) \quad (9.63)$$

$$R_1 + R_2 \geq H(U_1 U_2) \quad (9.64)$$

**证明** 前已说明, 分布信源的编码是在各子编码器中分布进行的。信源的分散使编码器不能直接对分布信源的联合典型序列进行编码, 因此不能用单一信源定长编码定理的证明方法来证明分布信源下的定长编码定理。下面是利用随机编码方法给出的定理证明。

分布信源编码的随机编码在概念上与信道容量定理证明中的随机编码非常相似。首先编码映射是随机生成的,其次我们求解随机编码的平均性能而不是求某一个码的性能。具体来说,随机编码的编码映射是这样确定的:分布信源编码器的两个子编码器各可提供  $2^{NR_1}$  和  $2^{NR_2}$  个码字母序列,对信源 1 送来的信源字  $\mathbf{u} \in A^N$  我们从  $2^{NR_1}$  个码字母序列中随机等概地选一码字母序列作为此信源字映射得到的码字,这一操作对信源 1 的所有信源字实行,这样就得到子编码器 1 的编码映射  $F_1$ ;子编码器 2 的编码映射  $F_2$  则从  $2^{NR_2}$  个码字母序列中用同样的随机映射的方法生成。值得强调的是,这两个编码映射的生成过程是对所有信源字进行的,同时有可能发生若干信源字映射为同一码字的情况。随机编码下译码映射的生成采用如下的办法:在译码器中存有随机编码生成的编码映射表,所以当收到某一码字对时就在这编码映射表中查找其对应的信源字对  $(\mathbf{u}, \mathbf{u})$ ,如果这样的信源字对唯一且  $(\mathbf{u}, \mathbf{u}) \in G^N(U_1 U_2)$ ,即  $(\mathbf{u}, \mathbf{u})$  是联合典型序列,则  $(\hat{\mathbf{u}}, \hat{\mathbf{u}}) = (\mathbf{u}, \mathbf{u})$ ,否则就认为译码有错。显然,在这样的编译码方法下译码有下面几种不同形式的差错:

(1) 码字对对应的信源字对不属于联合典型序列,这种差错记作

$$E_0 = \{(\mathbf{u}, \mathbf{u}) \mid \notin G^N\} \quad (9.65)$$

(2) 码字对对应的信源字对属联合典型序列,但不唯一,这有三种情况:

$$E_1 = \{(\mathbf{u}_1, \mathbf{u}_2) \mid F_1(\mathbf{u}_1) = F_1(\mathbf{u}_2), \text{且} (\mathbf{u}_1, \mathbf{u}_2) \in G^N\} \quad (9.66)$$

$$E_2 = \{(\mathbf{u}_1, \mathbf{u}_2) \mid F_2(\mathbf{u}_1) = F_2(\mathbf{u}_2), \text{且} (\mathbf{u}_1, \mathbf{u}_2) \in G^N\} \quad (9.67)$$

$$\begin{aligned} E_{12} &= \{(\mathbf{u}_1, \mathbf{u}_2) \mid F_1(\mathbf{u}_1) = F_2(\mathbf{u}_2), \text{且} (\mathbf{u}_1, \mathbf{u}_2) \in G^N\} \\ &= \{(\mathbf{u}_1, \mathbf{u}_2) \mid F_1(\mathbf{u}_1) = F_2(\mathbf{u}_2), \text{且} (\mathbf{u}_1, \mathbf{u}_2) \in G^N\} \end{aligned} \quad (9.68)$$

因此,译码的平均差错概率为

$$\begin{aligned} P_e &= P(E_0 \cup E_1 \cup E_2 \cup E_{12}) \\ &= P(E_0) + P(E_1) + P(E_2) + P(E_{12}) \end{aligned} \quad (9.69)$$

上式中各项的值可计算如下。

首先,由式(9.16)可知,当  $N \rightarrow \infty$  时,  $P(E_0) \rightarrow 0$ 。

其次

$$\begin{aligned} P(E_1) &= \sum_{(\mathbf{u}_1, \mathbf{u}_2)} P(\mathbf{u}_1, \mathbf{u}_2) P\{F_1(\mathbf{u}_1) = F_1(\mathbf{u}_2), (\mathbf{u}_1, \mathbf{u}_2) \in G^N\} \\ &= \sum_{(\mathbf{u}_1, \mathbf{u}_2)} P(\mathbf{u}_1, \mathbf{u}_2) P(F_1(\mathbf{u}_1) = F_1(\mathbf{u}_2)) \\ &\quad \sum_{\mathbf{u}_1 \neq \mathbf{u}_2} P(\mathbf{u}_1, \mathbf{u}_2) \cdot 2^{-NR_1} \end{aligned}$$



$$P(\mathbf{u}, \mathbf{u}) 2^{-NR_1} / G^N(U_1 | \mathbf{u}) /$$

$$(\mathbf{u}_1, \mathbf{u}_2)$$

由式(9.22)可得

$$|G^N(U_1 | \mathbf{u})| = 2^{N[H(U_1 | U_2) + 2]}$$

所以

$$P(E_1) = 2^{-N[R_1 - H(U_1 | U_2) - 2]} \quad (9.70)$$

由定理所给条件  $R_1 = H(U_1 | U_2)$  可得, 当  $N \rightarrow \infty$  时,  $P(E_1) = 0$ 。利用类似的推导不难得出条件(9.63)和(9.64)满足时  $P(E_2)$  和  $P(E_{12})$  均随  $N \rightarrow \infty$  而趋于零。这说明用随机编码方法所得的分布信源码其平均的译码差错概率趋于零。因而当条件(9.63)和(9.64)满足时能使译码差错概率趋于零的分布信源定长分组码一定存在, 或者说满足式(9.63)和式(9.64)的速率对都是可以达到的。证毕

这一定理说明分布信源编码虽然是分散进行的, 但仍然有可能利用信源之间的统计依存性达到最大的压缩。图 9.15 是这一定理所给的分布信源编码速率域图。在这张图中可以清楚地看出分布信源编码实行压缩的物理意义。在 B 点由于  $R_1 = H(U_1)$ , 所以信源 1 可以实现无差错的编译码, 从而使接收端获得正确的  $U_1$  值。在有正确  $U_1$  的条件下, 信源 2 的不确定性由  $H(U_2)$  减小为  $H(U_2 | U_1)$ , 这样, 对信源 2 的编码只需  $R_2 = H(U_2 | U_1)$  就可以了, 显然, 此时  $R_1$  和  $R_2$  的和满足式(9.64)。此后, 如果把  $R_1$  的速率进一步提高, 子编码器 1 的编码虽然可能会变得容易些, 但  $U_1$  的译码正确率已无法再提高, 所以  $R_2$  的速率不能再降低, 半无限直线 BD 就代表这种编译码状态。上述解释同样适用于 A 点和半无限直线 AC。图中 G 点是 AB 线上处于 A 和 B 之间的点, 与这一点

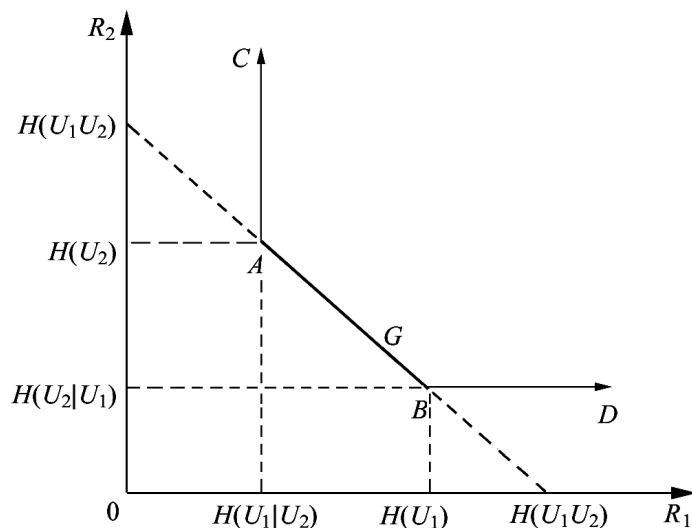


图 9.15 分布信源编码速率域

对应的速率  $R_1$  和  $R_2$  都没有达到各自信源所对应的熵, 即  $R_1 < H(U_1)$ ,  $R_2 < H(U_2)$ , 因此在译码时无法单独译出正确的  $U_1$  值或  $U_2$  值。但在  $R_1 + R_2 > H(U_1 U_2)$  条件下译码器根据输入的码字对仍可正确地复原出信源字。实现这一过程的一种途径是将  $A, B$  两点对应的编译码方法按时分方法交替使用。最后需要强调指出的是  $R_1 + R_2 > H(U_1 U_2)$  这一条件必须满足, 这对  $AB$  线上的点也是如此, 不能认为只要  $R_1 > H(U_1 | U_2)$  和  $R_2 > H(U_2 | U_1)$  就可实现无差错的编译码。

上述在两个信源下得到的分布信源定长编码定理可以很容易地推广到  $M$  个信源的一般情况, 此时的分布信源定长编码定理可表述如下。

**定理 9.9** 设  $(U_1 U_2 \dots U_M)$  是联合分布为  $p(u_1 u_2 \dots u_M)$  的独立同分布离散无记忆分布信源, 则分布信源码的可达速率矢量满足不等式

$$R(S) \leq H(S|S^c) \tag{9.71}$$

式中

$$S = \{U_1, U_2, \dots, U_M\}$$
$$R(S) = \begin{matrix} R_m \\ m, U_m \in S \end{matrix} \tag{9.72}$$

以上两个分布信源编码定理虽然都是针对无记忆信源的, 但对联合有记忆的遍历信源可以有类似的定长编码定理, 此时编码的可达速率受相应记忆信源熵率的约束。

### 习 题

9.1 设有二源接入信道, 信源  $X_1$  取值于  $A_1 = \{0, 1\}$ , 信源  $X_2$  取值于  $A_1 = \{0, 1\}$ , 信道输出为  $Y$ 。试求下述两种情况下的信道容量域并解释容量域边界上的最大信息传输速率是如何达到的。

- (1)  $Y = X_1 + X_2$  为简单的算术和, 无干扰。
- (2)  $Y$  取值仍在集合  $\{0, 1, 2\}$  中, 但在不同信源输入时  $Y$  取值的概率分布如下表所示:

输入 \ 输出	00	01	10	11
0	1 -	/ 2	/ 2	/ 2
1	/ 2	1 -	1 -	/ 2
2	/ 2	/ 2	/ 2	1 -

(3)  $Y = X_1 X_2$  为简单的算术积。

9.2 信息理论对信息传输有一个重要的结论:信道容量的充分利用可以在信源编码和信道编码分别独立进行的情况下实现。但在多源接入信道下这一结论不成立。试说明其原因,并举一实例。

9.3 在单用户的离散无记忆信道中已经证明反馈不能增加信道容量,但在有记忆的单用户离散信道以及多信源接入的无记忆信道中都能用反馈来增大容量域。试参阅定理 9.1 的证明及下述经典文献具体说明其原因。

[1] Gaarder N T., Wolf J K. The Capacity Region of A Multiple-Access Discrete Memoryless Channel Can Increase with Feedback. IEEE Trans on Inform Theory, 1975, Vol IT-21, Jan

9.4 本章关于通信网中的信源编码和信道编码问题的讨论在传统上被称为多用户信息理论。多用户信息理论不考虑众多信源共用通信网时必然存在的信源发送消息的突发性和网上传输延迟时间的变动。因而这一理论对现代分组交换网的发展较少有直接指导作用。试参阅下述文献后对此问题进行讨论并提出你的看法。

[1] Gallager R G. Basic Limits on Protocol Information in Data Communication Networks. IEEE Trans on Inform Theory, 1976, Vol IT-22, July

[2] Anantharam V. Bits Through Queues. IEEE Trans on Inform Theory, 1976, Vol IT-22, Jan

[3] Ephremidis A. Information Theory and Communication Networks: An Unconsummated Union. IEEE Trans on Inform Theory, 1998, Vol IT-44, Oct

## 参 考 文 献

- 1 . over Thomas M, Thomas Joy A . Elements of Information Theory . New York: Wiley, 1991
- 2 . Roman Steven . Coding and Information Theory . New York: Springer-Verlag, 1992
- 3 . McEliece Robert J . The Theory of Information and Coding: A Mathematical Framework for Communication . Reading, Mass .: Addison-Wesley Pub . Co ., Advanced Book Program, 1977
- 4 . Wells Richard B . Applied Coding and Information Theory for Engineers . Upper Saddle River, N J .: Prentice Hall, 1999
- 5 . Jones Duglas Samual . Elementary Information Theory . Oxford: Clarendon, 1979
- 6 . Lubbe J C A van der translated by Hoeve Hendrik Jan and Gee Steve . Information Theory . Cambridge[England]; New York: Cambridge University Press, 1997
- 7 . Anderson John B, Mohan Seshadri . Source and Channel Coding: An Algorithmic Approach . Boston: Kluwer Academic Publishers, 1991
- 8 . Kapur J N, Kesavan H K . Entropy Optimization Principles with Applications . Boston: Academic Press, 1992
- 9 . Ash Robert B . Information Theory . New York: Dover Publications, 1990
- 10 . dited by Verdu Sergio, McLaughlin Steven W . Information Theory: 50 Years of Discovery, Piscataway . NJ: IEEE Press, 2000
- 11 . Usher M J . Information Theory for Information Technologists . London: Macmillan, 1984
- 12 . Guiasu Silviu . Information Theory with Applications . New York: McGraw-Hill, 1977
- 13 . Gallager R G . Information Theory and Reliable Communication . New York, Willey, 1968
- 14 . Li Ming, Vitanyi Paul . An Introduction to Kolmogorov Complexity and Its Applications . New York: Springer-Verlag, 1993
- 15 . Blahut R E . Principles and Practice of Information Theory . Reading, MA: Addison-Wesley, 1987
- 16 . Berger T . Rate Distortion Theory . Englewood Cliffs, N J: Prentice-Hall, 1971
- 17 . Kullback S . Information Theory and Statistics . New York, Willey, 1959
- 18 . 孟庆生 . 信息论 . 西安: 西安交通大学出版社, 1986
- 19 . 仇佩亮 . 信息论及其应用 . 杭州: 浙江大学出版社
- 20 . 贾世楼 . 信息论理论基础 . 哈尔滨: 哈尔滨工业大学出版社, 1986
- 21 . 章照止, 林须端 . 信息论与最优编码 . 上海: 上海科学技术出版社, 1993
- 22 . 方军, 俞槐铨 . 信息论与编码 . 北京: 电子工业出版社, 1995
- 23 . 周炯 . 信息理论基础 . 北京: 人民邮电出版社, 1983
- 24 . 常迺 . 信息理论基础 . 北京: 清华大学出版社, 1993
- 25 . 周荫清 . 信息理论基础 . 北京: 北京航空航天大学出版社, 1993
- 26 . 姜丹, 钱玉美 . 信息理论与编码 . 合肥: 中国科学技术大学出版社, 1992
- 27 . 钟义信 . 信息科学原理 . 北京: 北京邮电大学出版社, 1996

# 索引

比特(bit)	23	编码定理	84
编码	77, 174	定长编码定理	84
信源编码	77	离散马尔可夫信源编码定理	105
熵压缩编码	78, 205	信道编码定理	182
冗余度压缩编码	78, 81		
静态统计编码	287	伴随式	189
自适应统计编码	287	伴随多项式	195
通用编码	289	频谱利用效率	166
变换编码	243	采样函数	148
预测编码	249	多用户信息理论	311
有限状态压缩编码	299	典型序列	83
唯一可译码	87	联合典型序列	180, 318
Lempel-Ziv 编码	300, 303	对数似然比	50
Huffmann 码	92	互信息	29, 31, 42
算术码	95	联合互信息	31
前缀码	87	条件互信息	31
Fitingof 通用编码	290	复杂度	294
分布信源编码	330	行缩减梯法式	188
信道编码	174	哈特利 (Hartley)	23
群码	176, 189	渐近等同分割	82
循环码	191		
线性码	186	鉴别信息	44, 45
代数码	177	条件鉴别信息	47
对偶码	187	联合鉴别信息	46
完备码	201	Jensen 不等式	21
最大距离可分码	201	K-L 展开	148
系统码	188	Kolmogorov 算法熵	294
网格码	196	Kolmogorov 算法复杂度	294
卷积码	176, 196		
随机编码	182		
汉明码	184		

Kraft 不等式	88	码率	175,196
Kraft 定理	88	分组码	78,175
可达速率对	321	定长分组码	78,84
		变长分组码	78,90
扩频因子	163	树码	78,95,175,196
扩频增益	163	网格码	196
拉格朗日乘数法	118,213,247	卷积码	176,196
量化	234	群	189
标量量化	234	子群	189
矢量量化	248	冗余度	81
均匀量化	236	相对冗余度	81
Lloyd-Max 算法	236	失真	204
马尔可夫链	100	字母失真矩阵	206
时齐马尔可夫链	100	字失真矩阵	206
一步转移概率	100	率失真函数	207
过渡态	101	平均失真	206
吸收态	101	生成矩阵	187
遍历状态	101	生成多项式	193
周期性/ 非周期性	101	熵	14,16
奈特(nat)	23	熵函数	19
逆问题	255	熵功率	143
陪集	189	Toeplitz 矩阵	239
陪集首	190	Toeplitz 分布定理	241
平稳分布	102	凸域	19
谱估计	278	凸函数	20
闭集	102	严格凸函数	20
不可约的	102	凸包	324
既约的	102	特征函数	149
码	77	稳恒信源	76
码字母	77	离散稳恒信源	79
字母表	78,84	唯一性	23
码字	478,175	熵函数形式的唯一性	23

鉴别信息函数形式的唯一性	57	二元对称信道	114
唯一性问题	132	二元删除信道	114
信道输入输出字母概率分布	132	信道容量	113, 114
信息速率失真函数解	221	信道容量域	321
误字率	175	信道容量费用函数	136
完备的归一化正交函数族	147	前向转移概率矩阵	114
网络信息理论	311	前向转移概率	114
信源	74	和信道	131
离散信源	76	输入并接信道	130
数字信源	76	无记忆加性噪声信道	137
模拟信源	76	无记忆加性高斯噪声信道	138
连续信源	76	并联信道	129
有记忆信源	76	并用信道	130
无记忆信源	76	无记忆信道	113
离散稳恒信源	79	有记忆信道	113
扩展信源	84	一致检验矩阵	187
高斯信源	77, 230	一致检验多项式	194
马尔可夫信源	76, 100	译码	175
信道	111	信源译码	175
离散信道	112	信道译码	175
数字信道	112	信道译码准则	177
模拟信道	112	理想译码器	178
双向信道	311	最大似然译码	178
反馈信道	311	译码差错概率	178
广播信道	312	伴随式译码	188
中继信道	313	域	186
多源接入信道	312	有限域	186
时分多址	328	扩域	187
频分多址	328	素数域	186
码分多址	328	约束长度	196
对称信道	121		
限带信道	150		

预测器	249	正问题	255
线性预测器	249	组合信息	288
非线性预测器	249	组合熵	288
最小均方误差预测器	250	最大熵原理	256
最小平均绝对误差预测器	250	最小鉴别信息原理	258
最大零误差概率预测器	250		