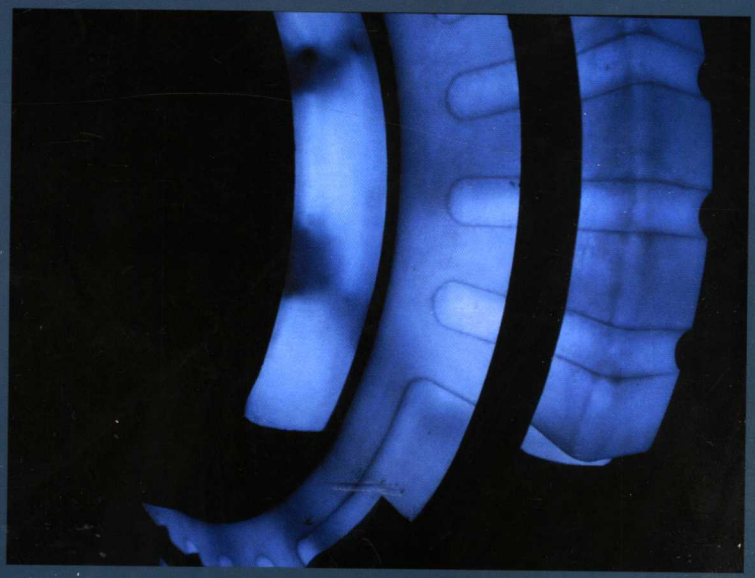
信息安全系列

密码学中的有关概率模型

北京中电电子出版社策划

李世取 黄晓英 刘文芬 张卫明 刘凤梅 著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国家科学技术学术著作出版基金
电子信息科技专著出版专项资金 资助出版
计算机网络与信息安全教育部重点实验室开放课题基金

密码学中的有关概率模型

北京中电电子出版社策划

李世取 黄晓英 刘文芬 张卫明 刘凤梅 著

電子工業出版社
Publishing House of Electronics Industry
北京中电电子出版社
北京·BEIJING

内 容 简 介

信息安全在当今社会的重要性是众所周知的，而概率论的思想和方法在密码设计和分析中一直占有重要的地位，这里建立合适的概率模型是解决问题的关键。

本书可作为信息安全、密码学与应用数学、计算机网络安全方面的理论工作者的参考书，也可作为相应专业研究生开展课题研究的指导书和参考用书。对从事密码设计、算法研究和密码分析及通信编码方面的工程技术人员也有使用价值和参考意义。

图书在版编目(CIP)数据

密码学中的有关概率模型/李世取等著. —北京：电子工业出版社，2005.11
ISBN 7-121-01808-X

Ⅰ.密… Ⅱ.李… Ⅲ.概率—数学模型—应用—密码 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2005)第 114253 号

责任编辑：赵 平
印 刷：北京大中印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：29 字数：742.4 千字
印 次：2005 年 11 月第 1 次印刷
印 数：2000 册 定价：68.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：(010) 68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

总　序

信息社会的兴起，进一步给全球带来了信息技术飞速发展的契机；信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动着人类社会的发展和人类文明的进步，把人类带入了崭新的时代；信息系统的建立已逐渐成为社会各个领域不可或缺的基础设施；信息已成为重要的战略资源，信息化的水平已成为衡量一个国家现代化和综合国力的重要标志，争夺控制信息权已成为国际竞争的重要内容。

胡锦涛主席指出，信息安全是个大问题，必须把安全问题放到至关重要的位置上，认真加以考虑和解决；温家宝总理在国家信息化领导小组第五次会议上指出，信息化是当今世界发展的大趋势，是推动经济社会发展和变革的重要力量。制定和实施国家信息化发展战略，是顺应世界信息化发展潮流的重要部署，要站在现代化建设全局的高度，大力推进国民经济信息化和社会信息化；会议审议并原则通过了《国家信息化发展战略（2006—2020 年）》。会议指出，坚持以信息化带动工业化、以工业化促进信息化；注重建设信息安全保障体系，实现信息化与信息安全协调发展；要夯实信息化基础，完善综合信息基础设施。中央领导多次强调，必须从经济发展、社会稳定、国家安全、公众利益的高度，充分认识信息安全的绝对重要性；各地各部门的领导干部，必须加紧学习网络化知识，高度重视网上斗争的问题并对加强我国信息安全保障工作提出了总体要求：坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。

然而，人们在享受信息网络所带来的巨大利益的同时，也面临着信息安全问题的严峻考验。现存的信息安全问题已经对我国的国家安全、经济安全、军事安全和社会安全构成了严重的影响和威胁，我们面临着信息安全的巨大挑战。因此，加速信息安全的研究和发展，加强信息安全保障能力已成为我国信息化发展的当务之急，成为国民经济各领域电子化成败的关键，成为提高中华民族生存能力的头等大事。为了构筑二十一世纪的国家信息安全保障体系，有效地保障国家安全、社会稳定和经济发展，需要尽快地并长期致力于增强广大公众的信息安全意识，提升信息系统研究、开发、生产、使用、维护、教育管理人员的素质和能力。

当今，信息安全的概念正在与时俱进：它从早期的信息保密发展到关注信息的保密、完整、可用、可控和不可否认的信息安全，并进一步发展到现今的信息保障和信息保证体系。单纯的保密和静态的保护已都不能适应今天的需要。信息保障体系是一个社会系统工程，它不仅涉及到信息技术体系本身还包括有信息安全的法律法规和组织管理体系。因此，现阶段以及未来的有效信息安全整体解决方案依赖于人利用技术进行操作这三个层面。而实施完整的信息保障战略还必须依赖于人才的培养和经费的支持。

中电电子出版社为适应上述形势的需要会同电子工业出版社，并经与国家信息安全领导机关和管理部门、信息安全的学术团队和研究机构、信息安全主要使用单位和行业、国内外知名专家进行了请示、商榷和研究，决定成立《信息安全系列》丛书编委会。《信息安全系列》丛书编委会由上述有关专家和部门主管领导组成，编委会在国家信息化领导小组的宏观政策指导

下，通过长期的努力，组织出版和发行这套丛书。丛书的指导思想是求新、求精、求快、求用，要围绕国内外信息安全的新技术、新发展、新知识和我国市场需求的原则进行考虑；丛书的选题范围是根据读者群定位为通俗、教育培训、领导和专业等四个层面；丛书的内容涉及信息安全技术、信息安全法律法规和信息安全管理等三个类型六个方面。为普及、提高、推广和发展信息安全理论和技术做出我们应有的贡献。

编委会设主任1人；副主任2人；编委会下设秘书处、编辑部、写作室。考虑到在运作推出《信息安全系列》丛书过程中的复杂性、艰巨性、长期性，因此，必须花大力气依靠编委会全体成员，用若干年时间，完成这项宏大工程。

沈昌祥

2005年10月18日

《信息安全系列》丛书编委会

前　言

信息安全在当今社会的重要性是众所周知的。而概率论的思想和方法在密码设计和分析中一直占有重要地位，这由流密码安全的标准之一是具有良好的“伪随机性”和对各种密码体制总能提出种种“相关攻击”方法的事实可见一斑。

为了弥补已有流密码生成器的一些不足，近些年来人们新设计了这样或那样的流密码生成器，如一般的“非线性组合生成器”。“钟控生成器”和“带记忆的组合生成器”及各类具有某种“信息压缩、扩展”功能的生成器，对这些新型流密码生成器的功能做更深层次的分析考察，以确定其可行性，是设计者们的首要任务；而从多角度、多侧面对这些新型流密码生成器做综合分析，力求发现其不足和弱点以对其实施某种有效的攻击，则是密码分析者们面临的挑战。

面对新问题，如何将概率方法更好地应用于以上两条战线的工作中，是值得有关学者考虑的课题。

正因为如此，1983 年以来，国内外人们对“组合”多条“线性移位寄存器”输出序列的“非线性组合生成器”进行了多方面的研究，特别对其抗“相关攻击”和“差分攻击”的问题进行了超乎寻常的研究，以寻求能抵抗“最佳仿射逼近攻击”和“差分攻击”的“组合器”并分析它们可能仍然存在的某些固有的、不可克服的弱点，攻击者们则力图由其输出序列去更多地发掘有关密钥的信息，这里自然涉及到了概率问题。

针对“线性移位寄存器”的不足，1984 年在欧洲密码学会议上由 T·贝思和 F·C·皮佩又首次提出了一种以移位寄存器为基础，通过对移位寄存器的时钟脉冲进行控制来产生伪随机序列的一种钟控生成器——“停走生成器(stop-and-go generator)”，随后人们又以“停走生成器”为基本构件构造了各类“钟控生成器”(其中有的已经得到实用)，并主要是用代数学的方法对这些生成器的功能、基本性质做了较为详尽的分析、探讨，国内著名密码学者肖国镇教授和旅欧密码学者丁存生博士在他们 1994 年的专著《流密码学及其应用》中“基于将钟控方法与非线性组合方法相结合的思想”，提出了“钟控非线性组合生成器”，并预言：“我们认为这种生成器可能成为最有发展前途的两种密钥流生成器之一”，但又强调指出：“要严格地对这种生成器的应用价值做定论，还必须对这种生成器进行进一步的分析”，同时提出了两个公开研究问题，其中之一即是分析输出序列和输入的“原序列”之间的符合率问题。而相较于人们对“非线性组合生成器”的研究而言，我们所见到的直接用概率论的思想方法来研究“钟控生成器”的还很少。

在研究非线性组合生成器抵抗相关攻击时，国外学者 Siegenthaler 于 1983 年提出了布尔函数相关免疫——其实就是有关布尔随机变量间的相互独立性——的概念，为了抵抗所谓的“相关攻击”——利用布尔随机变量间的相关性所实施的“攻击”，要求非线性布尔函数有高的相关免疫阶数，但是非线性布尔函数的相关免疫阶数与其非线性度、代数次数之间存在一种固有的制约关系：高的相关免疫阶数会导致低的非线性度和代数次数。为克服这种制约关系，1984 年 Rueppel 又提出了“带记忆的非线性组合生成器”，推广了无记忆组合函数相关免疫的概念，随后有若干学者对“带记忆的非线性组合生成器”相关免疫性和相关攻击等问题进行了

一系列理论分析研究。且因具有良好的密码学性质，带记忆的非线性组合生成器在实践中也受到重视，已被应用于“蓝牙技术”中：1999 年“蓝牙特别兴趣组”公布的“蓝牙技术标准 1.0”中保障蓝牙器件之间通信安全的加密算法 E_0 就是一个带 4 bit 记忆的组合生成器，即所谓的“蓝牙组合生成器”，而“蓝牙组合生成器”实际上是对 Rueppel 提出的“基本加法生成器”的一种改进。

由以上所述可见，如何依据“非线性组合生成器”、“钟控生成器”和“带记忆的非线性组合生成器”的原型建立合适的概率模型，以更好和更自如地应用概率论的思想和方法对它们的功能做全面、系统、深入的研究，是既有理论意义也有实用价值的。

与国内外主要是以代数方面的数学工具研究“非线性组合生成器”、“钟控生成器”和“带记忆的非线性组合生成器”的论文、论著相比较，本书的主要特点是依据以上生成器的原型先建立起合适的概率模型，然后在严格概率模型的框架下充分应用概率的思想和方法展开相关问题的研究，而不仅仅局限在对有关问题的研究用到概率工具时才作一般性概率“描述”，力求学术思想严谨。我们认为可以针对“非线性组合生成器”、“钟控生成器”和“带记忆的非线性组合生成器”建立起合适的概率模型，其基本出发点是：为确保安全，现实的许多密码体制都力求密钥的选取应是“随机的”，且有实用价值的流密码都应具有良好的“伪随机性”，以确保人们难以通过直接的观察和简单的统计分析由“截获序列”获取“原序列”的信息，那么，在“真随机”的意义下，这时由“截获序列”难以获取“原序列”的信息在理论上将得到确证，等价的是若在“真随机”的意义下，“输出序列”中都确证存在“信息泄露”，那在“伪随机”的意义下这种“信息泄露”一般也会存在，因而这样的流密码生成器的实用性就应该受到质疑。正因为如此，我们才坚信针对某些密码生成器建立合适的概率模型，准确把握“真随机”意义下这些生成器的性态，对其设计者和分析者都是有意义的。

本书通过建立起上述“非线性组合生成器”、“钟控生成器”和“带记忆的非线性组合生成器”的严格的概率模型，并在适当的假设条件下对相关输出序列的分布特性和“大数性质”进行了系统、深入的研究、探讨，且得到了令人较为满意的回报。例如，人们在对“停走生成器”的输出序列做实际观察分析后发现，这类生成器的不足是其输出序列的 0 或 1 的“长游程过长”，因而又提出了“衮特生成器”，说“衮特生成器”可以弥补“停走生成器”输出序列“长游程过长”的不足，我们的概率模型对此就提供了很好的理论解释；又如通过对多种“钟控生成器”概率模型的输出序列与输入的“原序列”的符合率及相应性质的研究，除在概率意义下回答了肖国镇教授和丁存生博士提出的公开问题外，我们还发现它们的输出序列和“原序列”的某个子序列的符合率有着一种“不变性”，我们认为这有可能成为以停走生成器为基本构件的各类钟控生成器设计中的一个“瓶颈”，而这一现象直接从“钟控生成器”的原型做分析是难于发现的。所以，我们认为，尽管本书中建立的一些“概率模型”和“原型”存在着差距，但我们在概率意义下所得到的结论确实能为有关生成器的设计者和分析者提供重要参考。

为保证体系的完整性并为读者阅读方便，本书第 1 章、第 2 章专门综述了我们模型分析中要用到的概率论基础知识和古典概率极限的经典结论——独立随机变量序列的“大数性质”与近代概率极限的相关结论——齐次马氏链、严平稳序列、α - 混合序列的“大数性质”等，为有关方向的研究生读者提供了更好的理解和思想方法，对有的结论我们还给出了严格证明。

本书第 3 章、第 4 章、第 5 章、第 6 章的主要内容都是我们自己的研究结果，对所有主要结论都给出了严格详细的证明。

值得一提的是，在第3章中我们将自己在布尔随机变量方面的研究成果——布尔随机变量联合分布的分解式应用于“非线性组合生成器”概率模型输出序列和相应仿射序列符合率的计算，为这里“多条序列的综合分析”提供了新的思想方法。

在第4章中我们首次通过建立概率模型研究了“停走生成器”和已经公开的以停走生成器为基本构件的各类钟控生成器输出序列的性质，考察了序列的分布特性和有关大数性质，特别考察了各输出序列和“原序列”的某子序列的符合率问题，发现了相应“符合率”的不变性。还对肖国镇教授和丁存生博士提出并预言有“可能成为最有发展前途的密钥流生成器之一”的“钟控非线性组合生成器”概率模型输出序列的性质做了基本探讨，发现它一般已不再是单个停走生成器所输出的马氏链，而是严平稳的 α - 混合序列，这为用概率思想方法对此类生成器的性能做进一步的分析奠定了基础。

在第5章我们对“带记忆的非线性组合生成器”建立了合理的概率模型，发现了一般条件下“带记忆组合生成器”输出序列的严平稳性和“记忆 - 状态序列”的齐次马氏性，研究了状态序列的极限性质，给出了条件相关性与无条件相关性相同的充分必要条件。我们对“相关免疫”的概念做了进一步推广，引入了 l 级 k 阶相关免疫的新概念，并利用弹性函数给出了满足任意级 K 阶相关免疫的带记忆组合生成器的构造方法，还部分地解决了带多比特记忆组合生成器的广义能量守恒(极限意义下的能量守恒)问题。另外需要指出的是，长期以来对带多比特记忆组合生成器的研究进展相对缓慢，一个主要的原因是其相关性的表示很复杂，而我们利用自己的“联合分布分解式”得到了一个一般性的相关系数计算公式，此公式易于实现快速计算，例如目前在对“蓝牙组合生成器”的相关攻击的研究中，J. Dj. Golic 和 K. Nyberg 等学者主要通过穷举或特殊的递推关系仅得到了长度不超过6的序列的相关系数，而利用我们的计算公式可得到11长以内的序列的所有相关系数。所以，我们认为这部分研究结果对于带记忆组合生成器的设计和攻击的研究都是很有参考价值的。

“m 值随机变量的极限理论”等是用概率思想方法研究多值(剩余类环上)非线性组合器概率模型的基础，在第6章中我们专门介绍了刘凤梅博士等所做的工作，全面、系统地介绍了作者在研究 m 值随机变量序列“部分和”的极限性质方面的成果。

近年来人们在密码学的有关研究中还讨论过一些典型的概率问题，为此在第7章中我们又介绍了自己所了解和研究过的其他概率模型。

书中第1章、第2章、第3章和第7章由李世取教授和刘文芬博士撰写，张卫明博士提供了第3章第3节的内容、滕吉红博士参与了第3章部分内容的研究，第4章内容基本取自黄晓英博士的学位论文，第5章内容基本取自张卫明博士的硕士学位论文，第6章内容基本取自刘凤梅博士的硕士学位论文。全书由李世取统稿，黄晓英、张卫明和刘凤梅对各自提供的内容做了校对。

虽说我们从事概率思想方法在密码学中的应用研究已有多年，但由于自身水平所限，加之对有关应用“背景”缺乏进一步的了解，因而对有些问题的研究结果还是显得不深、不透，这本拙著有若干不足甚至错误也许就在所难免，遵照“询问者智之本”的道理将它出版，唯愿能够起到“抛砖引玉”的作用。

恳请同行和读者们不吝赐教。

我要借此机会感谢我的导师严士健教授、刘秀芳教授等，是他们引导我走上了概率论的研究之路！同时感谢王隽骧教授、李占炳教授、廖昭茂老师等，他们和我的导师一起兢兢业业地

“传道、授业、解惑”，令我终生难忘。

我要感谢我的“师兄”陈木法院士，他在研究中对我的帮助曾使我受益匪浅！

感谢肖国镇教授和冯登国教授（博士），感谢他们提供的支持和帮助！

感谢吕述望教授的关心、支持和帮助！

感谢曾本胜教授和廉玉忠教授（博士）！

感谢王隽博士、范修斌博士、金晨辉博士、赵亚群博士、滕吉红博士、张文英博士和陈孟英博士、李书庆博士、祁建清博士、万朝阳博士等，他们参加了本书初稿大部分章节的研讨，特别要感谢范修斌博士！

感谢周锦君教授和她的弟子们！特别要感谢戚文峰教授（博士）和陈卫红教授（博士）！

感谢赵仁杰教授！

感谢韩文报教授（博士），感谢他的支持和有益的建议！

感谢楚泽甫教授！——没有他为系主任时当初的决策，至少现在不可能有这本书！

本书初稿的部分内容曾在多届硕士生和博士生研讨班上讲授，他们在听课过程中提出过若干宝贵意见，在此一并表示衷心感谢！特别要感谢斯雪明、何开成、赵耀东、李娜、李晓聪等博士生！

我还要感谢我的家人们，感谢女儿李信然（代静）在本书中提供了她研究“多值钟控生成器”的概率模型时所得到的主要结果，并参与了全书的校对等。特别要感谢我的儿子李未然（代远），在本书稿输入微机的过程中他主动提供了所有技术保障，本书能够顺利完稿有他一份辛劳！

感谢教研室同仁和其他以各种形式帮助了我们的所有人！

李世取

2005 年 6 月于郑州

目　录

第 1 章　概率论基础 …… (1)
1.1　概率空间及概率测度 …… (1)
1.2　随机变量及其分布函数 …… (3)
1.3　随机变量的特征函数及其与分布函数的关系 …… (8)
参考文献 …… (9)
第 2 章　概率极限理论 …… (10)
2.1　大数定律 …… (10)
2.2　分布函数列的弱收敛 …… (32)
2.3　特征函数列的正极限定理和逆极限定理 …… (41)
2.4　中心极限定理和重对数律 …… (45)
2.5　随机变量序列的 r 阶矩收敛 …… (60)
2.6　平稳随机变量序列及其遍历性 …… (66)
2.7　离散参数的马尔科夫链及其遍历性 …… (72)
2.8　取值为 -1 和 $+1$ 的独立同分布随机变量序列的性质 …… (102)
2.9　混合相依随机变量序列的极限定理 …… (108)
参考文献 …… (115)
第 3 章　密码学中非线性组合生成器的概率模型及其输出序列的极限性质 …… (116)
3.1　非线性组合生成器概率模型输出序列的极限性质 …… (116)
3.2　非线性组合生成器概率模型输出序列的有关精确分布 …… (126)
3.3　非线性组合生成器概率模型输出序列与多条仿射序列的综合分析 …… (130)
参考文献 …… (136)
第 4 章　钟控生成器的概率模型 …… (138)
4.1　“停走生成器”的一种概率模型 …… (138)
4.2　“停走生成器”输出序列与输入序列间的符合率问题 …… (145)
4.3　“停走生成器”输出序列的 α-混合性验证 …… (157)
4.4　“停走生成器”中的另一类符合率问题 …… (160)
4.5　“停走生成器”输出序列的大数性质 …… (169)
4.6　“加法型”组合器的一种概率模型 …… (174)
4.7　“乘法型”组合器的一种概率模型 …… (179)
4.8　多个“停走生成器”构成的组合器的概率模型 …… (190)
4.9　“另类钟控生成器”的一种概率模型 …… (201)
4.10　“衮特(Gunther)生成器”和“变形的衮特生成器”的概率模型 …… (223)
4.11　“停走生成器”概率模型输出序列的子序列和原序列的符合率问题 …… (232)
4.12　多值钟控生成器的概率模型 …… (243)

参考文献 …… (271)
第 5 章　带“记忆的”组合器的概率模型 …… (273)
5.1　带 1bit 记忆的组合器的概率模型 …… (274)
5.2　带多 bit 记忆的组合器的概率模型 …… (286)
5.3　带 1bit 记忆组合器的概率模型输出序列的性质分析 …… (300)
5.4　带多 bit 记忆组合器的概率模型输出序列的相关性分析 …… (314)
结束语 …… (326)
参考文献 …… (327)
第 6 章　*m* 值随机变量的极限理论 …… (329)
6.1　马氏链与剩余类环或有限域上的独立随机变量和的极限分布定理 …… (330)
6.2　特征函数与剩余类环或有限域上独立同分布随机变量和的极限分布定理 …… (338)
6.3　特征函数与剩余类环上独立同分布随机变量和的极限分布定理 …… (355)
6.4　收敛速度 …… (361)
6.5　在逻辑函数的密码学性质分析中的应用 …… (364)
参考文献 …… (371)
第 7 章　其他模型 …… (373)
7.1　序列的线性复杂度和定长二元随机序列的线性复杂度的数学期望 …… (373)
7.2　关于密码学中的周期随机序列 …… (381)
7.3　周期随机序列的线性复杂度的数学期望 …… (394)
7.4　“秘密共享方案”中的一个概率模型 …… (400)
7.5　RSA 的非完全映射特征分析中的概率模型 …… (405)
7.6　关于“缩减生成器”的概率模型 …… (419)
7.7　关于广义“缩减生成器”的概率模型 …… (427)
7.8　一般有限时态“钟控生成器”的概率模型 …… (442)
参考文献 …… (448)

第 1 章　概率论基础

用数学思想和方法解决社会生产、生活中的实际问题的前提常常是建立合适的数学模型。为更好地理解密码学中的有关问题时建立的概率模型，了解和掌握本章的概率论基础知识是很有必要的。

1.1　概率空间及概率测度

一、可测空间

1. 可测空间的定义及性质

定义 1.1　设 Ω 是任一非空集合，$\mathcal{P}(\Omega)$ 是 Ω 的全体子集构成的集族，$\boldsymbol{F}\subset\mathcal{P}(\Omega)$，称 $\boldsymbol{F}$ 为 Ω 上的 σ－代数[1]，如果

(1) $\Omega\in\boldsymbol{F}$；

(2) 若 $A\in\boldsymbol{F}$，则 $A^c=\Omega\setminus A\in\boldsymbol{F}$（集合 A 的余集——补集 A^c 也记作 $\bar{A}$）；

(3) 若 $A_n\in\boldsymbol{F}$，$n=1,2,\cdots$，则 $\bigcup\limits_{n=1}^{\infty}A_n\in\boldsymbol{F}$。

称二元总体 $(\Omega,\boldsymbol{F})$ 为一可测空间[1]。

易知，Ω 上的 σ－代数 $\boldsymbol{F}$ 具有以下基本性质：

(1) $\phi\in\boldsymbol{F}$；

(2) 若 $A_k\in\boldsymbol{F}$，$k=1,2,\cdots,n$，则 $\bigcup\limits_{k=1}^{n}A_k\in\boldsymbol{F}$ 且 $\bigcap\limits_{k=1}^{n}A_k\in\boldsymbol{F}$；

(3) 若 $A、B\in\boldsymbol{F}$，则 $B\setminus A\in\boldsymbol{F}$；

(4) 若 $A_n\in\boldsymbol{F}$，$n=1,2,\cdots$，则 $\bigcap\limits_{n=1}^{\infty}A_n\in\boldsymbol{F}$；

(5) 若 $A_n\in\boldsymbol{F}$，$n=1,2,\cdots$，且 $A_n\uparrow$，即 $A_1\subset A_2\subset\cdots$，则 $\lim\limits_{n\to\infty}A_n=\bigcup\limits_{k=1}^{\infty}A_k\in\boldsymbol{F}$，若 $A_n\in\boldsymbol{F}$，$n=1,2,\cdots$，且 $A_n\downarrow$，即 $A_1\supset A_2\supset\cdots$，则 $\lim\limits_{n\to\infty}A_n=\bigcap\limits_{k=1}^{\infty}A_k\in\boldsymbol{F}$。

二、概率测度及概率空间

1. 概率测度及概率空间的定义与性质

定义 1.2　设 $(\Omega,\boldsymbol{F})$ 为一可测空间，P 为 $\boldsymbol{F}\to[0,1]$ 的映射，称 P 为 $(\Omega,\boldsymbol{F})$ 上的概率（测度），如果 P 满足

(1) $P(\Omega)=1$；

(2) 若 $A_n\in\boldsymbol{F}$，$n=1,2,\cdots$，且 $A_i\cap A_j=\phi(i\neq j)$，则

$$P\left(\bigcup_{n=1}^{\infty}A_n\right)=\sum_{n=1}^{\infty}P(A_n)。$$

易知可测空间$(\Omega,\boldsymbol{F})$上的概率P具有下述性质：

(1) 正规性：$P(\phi)=0$；

(2) 单调性：$A、B\in\boldsymbol{F}$，$A\subset B$时，$P(A)\leqslant P(B)$且$P(B\setminus A)=P(B)-P(A)$；

(3) 有限可加性：若$A_k\in\boldsymbol{F}$，$k=1,2,\cdots,n$且$A_i\cap A_j=\phi(i\neq j)$，则

$$P\left(\bigcup_{k=1}^{n}A_k\right)=\sum_{k=1}^{n}P(A_k),$$

具体应用如$A、B\in\boldsymbol{F}$时，就有$P(B)=P(A\cap B)+P(A^c\cap B)$及

$$P\left(\bigcup_{k=1}^{n}B_k\right)=P(B_1)+P(B_2\cap B_1^c)+\cdots+P(B_n\cap B_1^c\cap\cdots\cap B_{n-1}^c)；$$

(4) 下、上连续性：若$A_n\in\boldsymbol{F}$，$n=1,2\cdots$，且$A_n\uparrow$即$A_1\subset A_2\subset\cdots$，则

$$P\left(\lim_{n\to\infty}A_n\right)=P\left(\bigcup_{k=1}^{\infty}A_k\right)=\lim_{n\to\infty}P(A_n)\text{——下连续性，}$$

若$A_n\in\boldsymbol{F}$，$n=1,2,\cdots$，且$A_n\downarrow$，即$A_1\supset A_2\supset\cdots$，则

$$P\left(\lim_{n\to\infty}A_n\right)=P\left(\bigcap_{k=1}^{\infty}A_k\right)=\lim_{n\to\infty}P(A_n)\text{——上连续性。}$$

三元总体$(\Omega,\boldsymbol{F},P)$称为一个概率空间[1]。此时，任一$A\in\boldsymbol{F}$都称为事件。

2．概率空间的例

(1) 古典概型中的概率空间　设$\Omega=\{\omega_1,\omega_2,\cdots,\omega_N\}$仅含有限个($N$个)元，取$\boldsymbol{F}$为

$$\boldsymbol{F}=\{A:A\subset\Omega\},$$

显然$\boldsymbol{F}$为是Ω上的一个σ－代数，即$(\Omega,\boldsymbol{F})$是一个可测空间，对任一$A\subset\Omega$，记

$$P(A)=\frac{|A|}{N}\text{，其中}|A|\text{表示}A\text{所含元素的个数，}$$

容易验证，这样得到的$P(\cdot)$是可测空间$(\Omega,\boldsymbol{F})$上的一个概率(测度)。如取

$$\Omega=GF^n(2)=\{(a_1,a_2,\cdots,a_n):a_i=0\text{或}1,1\leqslant i\leqslant n\},$$

$$\boldsymbol{F}=\{A:A\subset\Omega\},$$

而定义

$$P(A)=\frac{|A|}{2^n},\quad A\subset\Omega,\tag{1.1}$$

这样得到的概率空间$(GF^n(2),\boldsymbol{F},P)$在研究密码学中布尔函数的随机性质时是有用的。

(2) 初等概率论中常用到的概率空间　设$\Omega=R$(全体实数所构成的集合)，取

$$\boldsymbol{F}=\boldsymbol{B}\text{(全体实 Borel 集合所构成的集族)，}$$

对任一$B\in\boldsymbol{B}$，记

$$P(B)=\frac{1}{\sqrt{2\pi}}\int_B e^{-\frac{x^2}{2}}dx,$$

则由 Borel 集族和 Lebergue 积分的性质易知如上$(R,\boldsymbol{B},P)$是一个概率空间。若对任意取定的$a、b\in R$，$a<b$，定义在R上的函数$f(x)$满足：$a\leqslant x\leqslant b$时，$f(x)=\frac{1}{b-a}$，否则，$f(x)=0$，而对任一$B\in\boldsymbol{B}$，记

$$P(B)=\int_B f(x)dx,$$

易知，这样得到的$(R,\boldsymbol{B},P)$也是一个概率空间。

(3) 给定一个可测空间$(\Omega,\boldsymbol{F})$,总能定义其上的概率测度(Dirac 测度):取定 $\omega_0\in\Omega$,定义

$$P(A)=\begin{cases}1, & \omega_0\in A;\\ 0, & \omega_0\notin A,\end{cases}\quad A\in\boldsymbol{F},$$

容易验证如上定义的 $P(\cdot)$是可测空间$(\Omega,\boldsymbol{F})$上的概率测度。

1.2 随机变量及其分布函数

一、随机变量与随机元及其概率分布

1. 实值随机变量及其概率分布

定义 2.1 设$(\Omega,\boldsymbol{F},P)$是一概率空间,$\xi$ 是 $\Omega\to R$ 的映射,若对任一 $x\in R$,都有

$$\{\omega:\xi(\omega)<x\}\in\boldsymbol{F},$$

则称 ξ 为$(\Omega,\boldsymbol{F},P)$上的(实值)随机变量,且称

$$F_\xi(x)=P\{\omega:\xi(\omega)<x\},x\in R$$

为随机变量 ξ 的分布函数。设 $\xi_1,\xi_2,\cdots,\xi_n$ 是概率空间$(\Omega,\boldsymbol{F},P)$上的随机变量,称

$$F(x_1,x_2,\cdots,x_n)=P\{\xi_1<x_1,\xi_2<x_2,\cdots,\xi_n<x_n\},x_i\in R,1\leqslant i\leqslant n,$$

为随机变量 $\xi_1,\xi_2,\cdots,\xi_n$ 的联合分布函数。

注 1:对概率空间$(\Omega,\boldsymbol{F},P)$上的(实值)随机变量 ξ,也有称

$$F_\xi(x)=P\{\omega:\xi(\omega)\leqslant x\},x\in R$$

为 ξ 的分布函数的。就刻画随机变量取值的概率规律而言,随机变量的分布函数的上述两种定义方式没有质的区别,只是就其分析性质而言按第一种方式定义出的分布函数是左连续的,而按第二种方式定义出的分布函数却是右连续的。

随机变量中存在有两种基本类型:连续型的和离散型的。

(1) 离散型随机变量:若随机变量 ξ 可能取值的集合是一有限集或可列无穷集,即存在有限集或可列无穷集 $\boldsymbol{Q}^*\subset R$,使得 $\sum\limits_{a\in\boldsymbol{Q}^*}P\{\omega:\xi(\omega)=a\}=1$,则称 ξ 是离散型随机变量;

(2) 连续型的随机变量:若存在非负 Lebesgue 可测实函数 $f(x)$,使得

$$P\{\omega:\xi(\omega)\in B\}=\int_B f(x)\mathrm{d}x,B\in\boldsymbol{B}(\text{全体实 Bórel 集合所构成的集族}),$$

则称 ξ 是连续型随机变量。

2. 取值于抽象空间的随机元及其概率分布

定义 2.2 设$(\Omega,\boldsymbol{F},P)$是一概率空间,$(\Theta,\boldsymbol{S})$是任一可测空间,$X$ 是 $\Omega\to\Theta$ 的映射,若对任一 $E\in\boldsymbol{S}$,都有$\{\omega:X(\omega)\in E\}\in\boldsymbol{F}$,则称 X 为定义在概率空间$(\Omega,\boldsymbol{F},P)$上、取值于 Θ 的随机元,而称

$$P\{\omega:X(\omega)\in E\},E\in\boldsymbol{S}$$

为随机元 X 的概率分布。

例如,取可测空间$(\Theta,\boldsymbol{S})$中的 $\Theta=GF(2)=\{0,1\}$,$\boldsymbol{S}=\{\phi,\{0\},\{1\},\{0,1\}\}$,若 X 是 $\Omega\to\Theta$ 的映射,满足

$$\{\omega: X(\omega)=0\}\in \boldsymbol{F},$$

则称 X 为定义在概率空间$(\Omega,\boldsymbol{F},P)$上的布尔随机变量,称

$$P\{\omega: X(\omega)=0\}, P\{\omega: X(\omega)=1\}$$

为布尔随机变量 X 的分布律。取概率空间为前面的$(GF^n(2),\boldsymbol{F},P)$,定义

$$X_i(x_1,x_2,\cdots,x_n)=x_i,(x_1,x_2,\cdots,x_n)\in GF^n(2),\quad 1\leqslant i\leqslant n, \tag{1.2}$$

则得到该概率空间上的 n 个布尔随机变量$X_1,X_2,\cdots,X_n$。且容易知道,它们的分布律是

$$P\{X_i=0\}=P\{X_i=1\}=\frac{1}{2},1\leqslant i\leqslant n$$

此时,称布尔随机变量具有"均匀分布"或"对称分布"。

二、实值随机变量的数字特征

众所周知,实值随机变量可以由其分布定义各种数字特征(当然,除个别情况,随机变量的数字特征不能确定其分布),而对定义在概率空间$(\Omega,\boldsymbol{F},P)$上、取值于 Θ 的随机元,一般却不能定义其通常意义下的数字特征。

1. 实值随机变量的数学期望和 r 阶矩

定义 2.3 设 ξ 为概率空间$(\Omega,\boldsymbol{F},P)$上的(实值)随机变量,$F_\xi(x),x\in R$ 为其分布函数,若

$$\int|\xi|\mathrm{d}P=\int_{-\infty}^{+\infty}|x|\mathrm{d}F_\xi(x)<+\infty,$$

则称

$$E\xi=\int\xi\mathrm{d}P=\int_{-\infty}^{+\infty}x\mathrm{d}F_\xi(x)$$

为 ξ 的数学期望;对实数 $r>0$,若$\int|\xi|^r\mathrm{d}P=\int_{-\infty}^{+\infty}|x|^r\mathrm{d}F_\xi(x)<+\infty$,则称

$$E|\xi|^r=\int|\xi|^r\mathrm{d}P=\int_{-\infty}^{+\infty}|x|^r\mathrm{d}F_\xi(x)$$

为 ξ 的 r 阶绝对原点矩,特别,当 $r=k$ 是正整数,ξ 的 k 阶绝对原点矩存在时,称

$$E\xi^k=\int\xi^k\mathrm{d}P=\int_{-\infty}^{+\infty}x^k\mathrm{d}F_\xi(x)$$

为 ξ 的 k 阶原点矩。

注 2:由于实数 $0<r_1<r_2$ 时,有

$$\begin{aligned}0\leqslant\int|\xi|^{r_1}\mathrm{d}P&=\int_{|\xi|\leqslant1}|\xi|^{r_1}\mathrm{d}P+\int_{|\xi|>1}|\xi|^{r_1}\mathrm{d}P\\&\leqslant\int_{|\xi|\leqslant1}1\mathrm{d}P+\int_{|\xi|>1}|\xi|^{r_2}\mathrm{d}P=P\{|\xi|\leqslant1\}+\int_{|\xi|>1}|\xi|^{r_2}\mathrm{d}P\\&\leqslant1+\int|\xi|^{r_2}\mathrm{d}P,\end{aligned}$$

因而,对实数 $0<r_1<r_2$ 若随机变量的 r_2 阶绝对原点矩存在,则其 r_1 阶绝对原点矩一定存在。

2. 实值随机变量的方差和相关系数

由此可以如下定义随机变量的方差和两个随机变量的相关系数。

定义 2.4 若随机变量 ξ 的二阶矩存在，即 $E\xi^2=\int \xi^2 \mathrm{d}P=\int_{-\infty}^{+\infty} x^2 \mathrm{d}F_\xi(x)<+\infty$，则称

$$D\xi=\int (\xi-E\xi)^2 \mathrm{d}P=\int_{-\infty}^{+\infty}(x-E\xi)^2 \mathrm{d}F_\xi(x)$$

$$=\int \xi^2 \mathrm{d}P-(E\xi)^2=\int_{-\infty}^{+\infty} x^2 \mathrm{d}F_\xi(x)-(E\xi)^2$$

为随机变量 ξ 的方差(二阶中心矩)。

定义 2.5 设 ξ,η 都是概率空间$(\Omega,\boldsymbol{F},P)$上的(实值)随机变量，$F_{\xi,\eta}(x,y)$，$x、y\in R$ 为其联合分布函数，在 $E(\xi-E\xi)(\eta-E\eta)$存在时，称

$$\begin{aligned}\mathrm{Cov}(\xi,\eta)&=E(\xi-E\xi)(\eta-E\eta)\\&=\int(\xi-E\xi)(\eta-E\eta)\mathrm{d}P=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}(x-E\xi)(y-E\eta)\mathrm{d}F_{\xi,\eta}(x,y)\\&=\int\xi\eta\mathrm{d}P-(E\xi)(E\eta)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}xy\mathrm{d}F_{\xi,\eta}(x,y)-(E\xi)(E\eta)\\&=E(\xi\eta)-(E\xi)(E\eta)\end{aligned}$$

为 ξ 和 η 的协方差。

当 $\mathrm{Cov}(\xi,\eta)=0$ 时，称随机变量 ξ 和 η 不相关。又若有 $D\xi>0$ 和 $D\eta>0$，则称

$$\rho_{\xi,\eta}=\frac{\mathrm{Cov}(\xi,\eta)}{\sqrt{D\xi\cdot D\eta}}$$

为 ξ 和 η 的相关系数。

三、事件和随机变量的相互独立性

1. 事件的相互独立性

定义 2.6 设$(\Omega,\boldsymbol{F},P)$是一概率空间，$A、B\in\boldsymbol{F}$是两个事件，若

$$P(A\cap B)=P(A)P(B),$$

则称 A 与 B 相互独立。设 $A_i\in\boldsymbol{F}$，$1\leqslant i\leqslant n$ 都是事件，且

$$P(A_i\cap A_j)=P(A_i)P(A_j),1\leqslant i<j\leqslant n$$

$$P(A_i\cap A_j\cap A_l)=P(A_i)P(A_j)P(A_l),1\leqslant i<j<l\leqslant n,$$

$$\cdots$$

$$P(A_1\cap A_2\cap\cdots\cap A_{n-1}\cap A_n)=P(A_1)P(A_2)\cdots P(A_{n-1})P(A_n),$$

则称事件 $A_1,A_2,\cdots,A_{n-1},A_n$ 是相互独立的。

2. 相互独立的随机事件的基本性质[1]

设$(\Omega,\boldsymbol{F},P)$是一概率空间，$\{A_1,A_2,\cdots,A_n,B_1,B_2,\cdots,B_m\}\subset\boldsymbol{F}$，且事件

$$A_1,A_2,\cdots,A_n,B_1,B_2,\cdots,B_m$$

相互独立，若