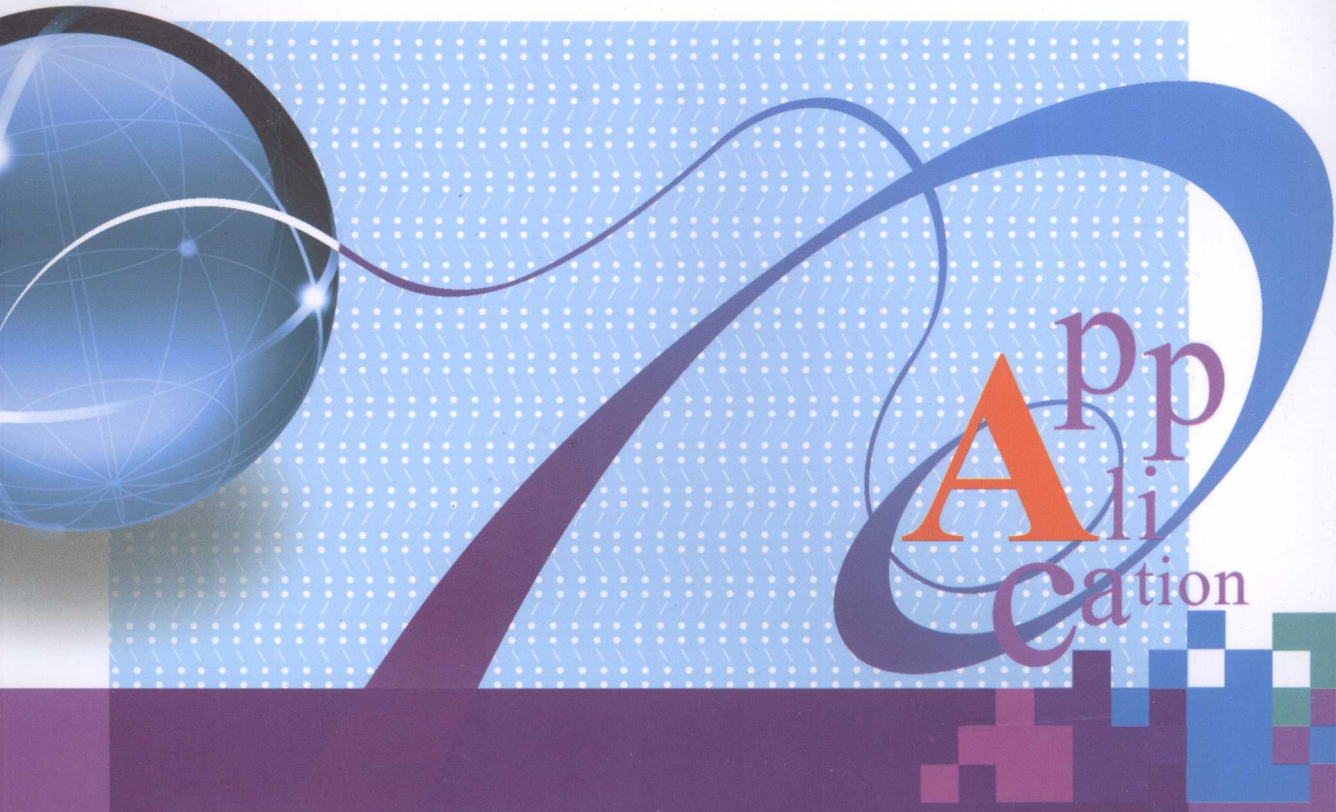
▶ 21世纪通信网络技术丛书



网络通信与工程应用系列

信道编码及其识别分析

张永光　楼才义　著　　杨小牛　审

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

21世纪通信网络技术丛书
——网络通信与工程应用系列

信道编码及其识别分析

张永光 楼才义 著
杨小牛 审

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书对信道编码（包括分组码、卷积码、Turbo 码、交织及扰码）的识别问题进行了系统完整的讨论，并将识别范围拓展到了 TPC 码、TCM 网格编码调制及空时编码，同时对数据的随机性分析也给予了相应介绍。全书条理清楚，取材新颖，内容上不仅包括适量而不累赘的相关编译码先验知识及编码识别基础理论，同时又紧扣编码识别主题，重点讨论具体的编码识别分析方法。

本书可作为通信、计算机等领域中从事信道编码相关工作的研究人员，特别是广大通信侦察、通信对抗及智能通信领域的相关研究人员的参考书，也可作为相关专业高年级本科生和研究生的教材或参考书。

图书在版编目（CIP）数据

信道编码及其识别分析 / 张永光，楼才义著. —北京：电子工业出版社，2010. 9
ISBN 978-7-121-11690-2
（21 世纪通信网络技术丛书）

Ⅰ. ①信… Ⅱ. ①张… ②楼… Ⅲ. ①信道编码 Ⅳ. ①N911.22

中国版本图书馆 CIP 数据核字（2010）第 165788 号

责任编辑：竺南直　　特约编辑：郭　莉
印　　刷：
装　　订：北京中新伟业印刷有限公司
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
开　　本：787×1 092　1/16　印张：15.75　字数：402 千字
印　　次：2010 年 9 月第 1 次印刷
印　　数：3 500 册　　定价：36.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

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。

服务热线：（010）88258888。

柳梢青

老去春秋　壯心半盡　到底難休
一夢淩煙　覺來餘恨　繚亂無收
此身飄若飛鷗
有未遂　羞歸故丘
聊寄江湖　不商不仕　且做研究

出 版 说 明

通信网络技术是当今发展最快、应用最广和最前沿的通信领域之一。通信技术发展到今天，已经不是传统意义上的充满神秘色彩的深奥技术了，它已经与日常的应用密不可分。可以说，网络的出现，使通信技术有了广阔的用武之地。正是由于有了固定电话网、移动通信网和 Internet，使通信技术的应用在这些平台上有了用武之地，渗透到了我们日常生活的方方面面。

为了促进和推动我国通信产业的发展，电子工业出版社通信分社特策划了一套《21 世纪通信网络技术丛书》。这套丛书根据不同的层面，又细分为三个系列：《移动通信前沿技术系列》、《3GPP LTE 无线通信新技术系列》和《网络通信与工程应用系列》。

《移动通信前沿技术系列》是从移动通信技术（3G 技术）的应用现状与发展情况出发，全面介绍当今移动通信领域涉及的关键技术与热点技术，例如：软件无线电；移动 IP 技术；移动数据通信；WCDMA；TD—SCDMA；cdma2000；移动通信系统网络规划与优化；智能天线技术；认知无线电技术；WiMAX，WiFi，ZigBee 宽带无线接入技术；UWB 技术；UMTS 技术；Ad Hoc 技术等。

《3GPP LTE 无线通信新技术系列》是以 3GPP 中 LTE 标准的关键技术在无线、宽带、高速、资源中的有效管理和利用，以及在 B3G/4G 无线通信领域中的应用为主。LTE 作为 3G 技术的一个重要的长期演进计划，代表了国际无线通信领域的最新发展需求和解决方案，例如：基于 OFDM 的上、下行（HSxPA）的多址接入技术；随机接入技术；多天线 MIMO 技术；多链路自适应技术；多播技术；功率控制技术；宽带无线网络的安全性、可移动性、可管理性；高效信源与信道编码和调制 MQAM 技术等。

《网络通信与工程应用系列》是以技术为先导，以构建网络的体系结构、标准、协议为目标所开展的对现代无线、移动、宽带通信网络的规划与优化，以及结合工程应用的方向所提出来的。例如：无线网状网、WLAN、无线传感器网络、3G/B3G/4G 通信网工程设计与优化、卫星移动通信网、三网融合技术、网络新安全技术与策略、RFID 应用网络、下一代基于 SIP 的统一通信、光网络与光通信等。

本套丛书依托各高等院校在通信领域从事科研、教学、工程、管理的具有丰富的理论与实践经验的专家、教授；各研究院所的研究员；国内有一定规模和研发实力的科技公司的研发人员，以及国外知名研究实验室的专家、学者等组成编写和翻译队伍，力求实现内容的先进性、实用性和系统性；力求内容组织循序渐进、深入浅出；理论阐述概念清晰、层次分明、经典实例源于实践；力求很强的可读性和可操作性。

本套丛书的主要读者对象是广大从事通信网络技术工作的各科研院所和公司的广大工程技术人员；各高等院校的专业教师和研究生；刚走上工作岗位的大学毕业生；以及与此相关的其他学科的技术人员，供他们阅读和参考。

本套丛书从 2008 年上半年开始陆续推出，希望广大读者能关注它，多对本套丛书提出宝贵意见与建议，欢迎通过电子邮箱 wchn@phei.com.cn 进行探讨、交流和指正，以便今后为广大读者奉献更多、更好的优秀通信技术类图书。

电子工业出版社
通信出版分社

序

无线通信自从1897年马可尼（Marconi）在英格兰海峡首次成功进行两艘行驶船只之间的无线电通信以来，已经经历了一百多年的发展历程。特别是1948年著名Shannon定理的提出为无线通信奠定了坚实的理论基础，也为无线通信的技术发展指明了努力的方向。Shannon定理告诉我们，如果信源的信息速率 R 小于信道容量 C，只要输入符号数目 n 足够大，则采用适当的编码来达到在信道上的可靠传输在理论上是可能的，即可以实现差错概率 p 的任意小（$n\to\infty$，$p\to 0$）。在这一基本理论的指导下，人们对如何在有扰信道上通过高效率的纠错编码实现可靠通信表现出了极大的热情，提出了各种信道编码理论和算法，有力推动了无线通信的快速发展。

众所周知，无线通信的最大特点是传输信道的开放性，表现为信道干扰的无处不在、无时不在。这就要求无线通信必须采取纠错编码措施来应对各种形式的信道干扰，才能实现高可靠的通信。因此，纠错编码（也称为信道编码）是在有扰信道上实现可靠通信不可或缺的重要环节。经过半个多世纪的发展，人们提出了针对不同信道、不同用途的各种信道编码方法，估计不下百余种。最简单最古老的信道编码方法就是被大家所熟知，也是被广泛使用的奇偶校验算法。它是通过在一个编码字符（如7比特的标准ASCII码）后添加1比特的0或1，使其码组（7比特的标准ASCII码添加1比特后变为8比特的码组）中0或1的个数为奇数或偶数来实现的。接收方如果收到的码组中0或1的个数不为奇数或偶数，则认为接收的码组有错误，并要求发送方重发，直至接收正确为止。由此也可以看出，为确保可靠通信而采取的信道编码措施是以降低通信效率（单位时间内传输的信息量）为代价的。但在无线信道上进行通信时，以降低通信效率为代价的信道编码是无法回避的重要环节。

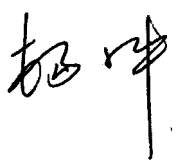
本书的书名叫《信道编码及其识别分析》，那为什么要进行信道编码的识别分析呢？很显然，作为合作通信双方是可以预先知道信道编码的方式及其编码参数的，接收方完全可以根据这些先验信息进行正确的信道解码，并正确恢复出发送方的信源信息。所以，信道编码识别分析首先想到的应用场合是在非合作的通信侦察领域。因为作为非合作的侦察方来说，被侦察方（通常为敌方）的通信参数（包括信道编码方式和编码参数）是很难预先获得的，通常需要通过对信道编码的识别分析来获取。所以，对于通信侦察如果需要获得信息层的内涵情报，信道编码识别分析是必不可少的，否则后续的信息解码或解译就无从谈起了。因此，信道编码识别分析在通信侦察领域是极其重要的一项工作，尤其是在数字通信几乎占据整个通信领域的当今社会，信道编码识别分析研究的重要性显得更为突出。当然，正确的信道编码识别分析对于实施灵巧通信干扰，特别是实施网络攻击也是非常有意义的。

信道编码识别分析的另一个应用方向是在目前蓬勃发展的智能通信（也叫认知通信）领域。所谓的智能通信就是通信的发送方可以根据所处的地理、电磁环境、频谱约束等情况以及业务需求，选择最佳的通信体制、通信方式和通信参数与接收方进行可靠通信。也就是说智能通信系统的通信体制、通信方式和通信参数是随时随地不断变化的，这就要求智能通信

系统的接收方必须能够正确地对接收信号进行识别分析，包括对信道载频、信号参数、信道编码方式、编码参数等进行识别分析。当然，智能通信毕竟也是合作通信，对某些通信体制或通信参数的识别分析是可以通过通信协议来实现的，以尽可能地降低系统的复杂性。

总之，信道编码识别分析不仅在智能通信领域有应用前景，尤其是在通信侦察或网络对抗领域有迫切的军事需求。信道编码识别分析技术难度很大，再加上总体上来看从事这方面研究的研究力量相对薄弱，可供引用或参考的理论成果不多（到目前为止，在国内外尚未看到公开出版的相关专著），但愿本书能起到抛砖引玉之作用，促使更多的有识之士能加入到这一研究队伍中来。

本书主要作者张永光先生从事这方面研究的时间虽然不算长，却能在这不长的时间内以他丰硕的研究成果（作者就信道编码识别分析所申请的专利多达 10 项）为基础撰写出这么一本专著实属不易，我们无不为他的这种敬业精神所感动。感谢他使我们能够一起共享他的研究成果，感谢他为这一技术领域所付出的辛勤工作和汗水。同时，考虑到信道编码识别分析技术新、理论深、难度大，本书作为国内外第一本公开出版的专著，肯定会存在这样或那样的问题，因此也真诚希望广大读者能对本书多提宝贵意见和建议。



二〇一〇年五月十二日

前　言

信息论、信道编码和密码学是现代数字通信系统中的三大核心支柱技术，目前信道编码已成为从事通信、计算机等领域中有关人员必须了解和掌握的一门技术。正如自然界的五行相生相克关系一样，信道编码中的独特结构在成就其优异性能的同时也留下了可以对其进行识别分析的特征。对信道编码进行识别分析，除了在智能通信、通信侦察领域具有基础性的意义外；在网络对抗领域同样具有重要意义，尤其当对方网络信源和通信协议被加密时，从信道编码结构上进行攻击是可供选择的有限手段之一。

经过半个多世纪的研究发展，国内外对信道编码进行讨论的相关专业书籍已经非常丰富，但是却尚未见到专门讨论信道编码识别方面的书籍。有鉴于此，考虑到初入此门时的窘迫和茫然，2009 年年底作者开始考虑规划一本关于信道编码识别分析方面的专业书籍。有幸的是，在作者单位领导和同事们的关心支持下，今天这本书终于面世了。在总结前人研究成果的基础上，本书第一次系统完整地对信道编码（包括纠错码、交织、扰码）识别提出了一揽子解决方案，同时对数据的随机性也进行了相应讨论，其中不少内容属于作者研究的独得之秘，并已申请了多项发明专利。敝帚虽微亦自珍，现在作者不揣自陋将之小心翼翼地拿出来，希望对相关领域的研究人员能够起到一定的参考作用，假使本书能为推动我国通信技术向深入发展献绵薄之力的话，作者将感到非常荣幸，功不唐捐。

本书适用于对信道编码识别感兴趣，并有一定信道编码基础的专业研究人员。本着“辨逻辑，晰条理，贵浅近，多举例，重实用”的原则，全书尽量不涉及较为晦涩的编译码理论知识，力图用较为明白易懂的语言来表达内涵丰富的信道编码识别技术。对于教材文献中的一般性结论，书中一般直接加以引用不予证明。

全书共分八章，除第 1 章概述和第 8 章总结部分外，其余各章均首先介绍与识别分析相关的编码知识，然后讨论具体的编码识别分析方法，最后为全章小结。各章内容如下：

第 1 章为概述，对信道编码（包括纠错码、交织、扰码）及数据随机性进行了简要介绍，在总结信道编码识别分析技术研究现状后讨论了一些简单实用的信道编码识别及验证方法。

第 2 章讨论分组码的识别分析技术，介绍了多种二进制线性分组码（包括 Hamming 码、Golay 码、CRC 码、BCH 码及部分 LDPC 系统码）的识别分析方法和 RS 码的识别分析方法。

第 3 章讨论卷积码的识别分析技术，这是目前信道编码识别分析领域中研究最多的一种码型，本章在介绍多种卷积码识别分析方法的基础上，深入讨论了 $(n-1)/n$ 型删余卷积码的识别分析方法。

第 4 章在前面纠错码识别分析技术讨论的基础上，主要讨论了分组交织和卷积交织的识别分析问题，其中分组交织分“线性分组码＋分组交织”和“卷积码＋分组交织”两种模式。

第 5 章在纠错码和交织识别分析技术的基础上，对非归零和归零两种形式的 Turbo 码（包括删余 Turbo 码）的识别分析方法分别给予了讨论。

第 6 章主要从流密码分析的角度，基于信源非平衡的特点，通过引入指示平衡性的指标讨论了自同步扰码和同步扰码的识别分析技术。

第 7 章主要介绍了一些对数据序列进行随机性检测的方法，用于对通信数据的加密情况

和统计特性进行进一步的分析。

第 8 章为全书的总结讨论部分，在对信道编码识别的应用予以介绍后，讨论了一些信道编码识别分析领域有待继续深入研究的内容。

各章中用于说明信道编码识别分析方法的实例均经作者仿真验证通过。

本书主要由张永光同志负责撰写，楼才义同志负责全书的统筹并作了重要补充，杨小牛同志对全书进行了仔细的审阅和定稿，并作序。

在这里，对研究过程中给予作者支持和帮助的单位同事（特别是陆辉同志）深表感谢，同时也要特别感谢撰写过程中身怀六甲的拙荆洪瑶女士对作者工作的大力支持，因此这本书也可说是和我们呼呼共同成长的。最后对百忙之中为本书提出宝贵修改意见的空军某部的陈国杰老师致以深深谢意。

由于信道编码识别分析技术本身处于通信技术的前沿领域，并且随着通信技术的快速发展，各种好的信道编码方案层出不穷，这就决定了信道编码的识别分析技术也必须不断发展完善，与时俱进，因此本书只能说是探索性质的，诚挚希望相关领域研究人员能够多多给予批评和提点。

张永光

2010 年早春

目　录

第1章 概　　述

天地茫茫昧本元，璇玑各演理难言。
欲识大道非常道，惟有精诚致眼前。

信道编码主要应用于数字通信，一个典型数字通信系统的模型如图 1.1 所示。

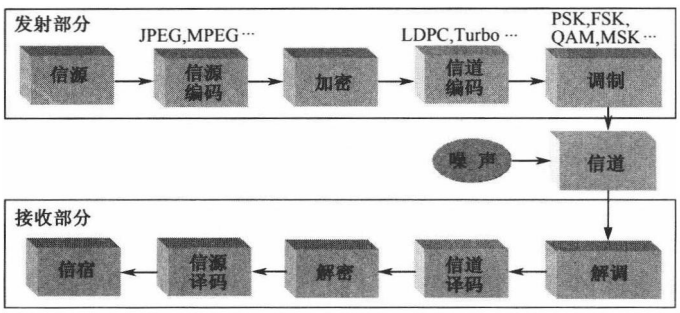


图 1.1　数字通信系统模型

其中信源编码的作用是把信源发出的消息转换成二进制形式的信息序列。为了增加通信的保密性，需要对信源编码器的输出数据进行加密；为了提高数据传输的可靠性，则需要对加密后的数据进行所谓的信道编码，信道编码就是为了减少传输过程中的各种干扰，通过人为增加冗余数据（比特），使系统具有自动检错或纠错的能力而进行的编码处理，又称之为抗干扰编码，一般意义上的信道编码主要指纠错码和交织。经过信道编码后的数据最后通过调制将其承载到无线电载波上，并通过无线信道到达接收端。接收端的处理过程正好与发射端相反。

1.1　信道编码介绍

数字信号在信道传输过程中，总会因遇到各种干扰而使信号失真，图 1.2 为信道编码使用效果示意图。

数字信号经有扰信道传输到接收端解调器进行解调时，由于信道干扰的影响，解调后的信息序列可能已有误码（一个典型噪声信道的比特错误概率可以达到 10^{-2}），对相当部分应用来说，这样的通信误码率是不能接受的。但是对于采用了信道编码的通信系统来说，经过信道译码器，可以对其中的误码进行纠正，恢复成原来的信息发送给用户终端。

信道编码的基本思想是：通过对发送端信息序列作某种变换，使原来彼此独立，相关性极小的信息码元产生某种相关性，在接收端利用这种相关性来检查并纠正信息码元在信道传输中所发生的差错。

图 1.2　有无信道编码通信的效果对比

在数字通信系统中，广义的信道编码一般包括加扰、纠错及交织三种类型的编码，从数学运算上来看，这三种编码分别采用的是混乱、加冗及置换的数学处理。目前这三种编码技术在通信领域都获得了广泛应用，其编码和解码技术已经较为成熟。

1.1.1　信道编码基础

1948 年，Shannon 在其经典论文“A Mathematical Theory of Communications”中指出：如果系统的传信率小于信道容量，则选择适当的编码技术可以实现可靠通信。

Shannon 采用信源和信道的概率模型，将信息可靠传输的基本问题归结为以下公式

$$C = W\log_2(1+S/N) \tag{1-1}$$

式中，C 代表信道容量，是指单位时间内信道上所能传输的最大信息量；W 代表带宽；S/N 代表信噪比（信号与噪声功率之比）。这就是著名的 Shannon 公式。由此，Shannon 建立了对信息通信的基本限制，引出了信道编码定理。

信道编码理论可以简单地描述为：如果信源的信息速率 R 小于 $C(R<C)$，只要输入符号数目 n 足够大，则采用适当的编码来达到在信道上的可靠传输在理论上是可能的，即可以实现差错概率任意小，如果 $n\to\infty$，差错概率将接近于 0。反之，如果 $R>C$，则不管在发送端和接收端采用了多少信号处理措施，都不可能达到可靠传输。

由式（1-1）可以得到如下结论：

1）提高信噪比 S/N 可以增加信道容量 C；

2）当噪声功率 $N\to 0$ 的时候，信道容量 $C\to\infty$，这表明在无干扰时的信道容量为 ∞；

3）增加信道带宽 W 并不能使信道容量 C 无限制地增加。当噪声为高斯白噪声时，随着 C 增大，噪声功率 $N=Wn_0$ 也随之增大（其中 n_0 为噪声的单边功率谱密度）：

$$\begin{aligned}\lim_{W\to\infty} C &= \lim_{W\to\infty} W\log_2(1+S/N)\\ &= \frac{S}{n_0}\lim_{W\to\infty}\frac{n_0W}{S}\log_2\left(1+\frac{S}{n_0W}\right)\\ &= \frac{S}{n_0}\log_2 e\\ &\approx 1.44\frac{S}{n_0}\end{aligned}$$

4）即使信道带宽W无限增大，信道容量C仍然是有限的$(C \leqslant 1.44S/n_0)$；

5）信道容量C一定的时候，信道带宽W与信噪比S/N之间可以彼此互换。

信道编码定理证明了最佳编码方法的存在性，指明了纠错码研究的方向，纠错码理论正是为寻找最佳编码方法而发展起来的。从此之后，寻找能够实际应用的逼近 Shannon 极限的编码方案就成了纠错编码理论的最终目标。

如果一个元素集合G，在其中定义一种运算“$*$”，并满足条件：

1）自闭性：$c=a*b$

2）结合律：$(a*b)*c=a*(b*c)$

3）单位元：$a*e=e*a=a$

4）逆元：$a*a^{-1}=a^{-1}*a=e$

则称这个元素集合为一个“群”$(a,b,c,e,a^{-1}\in G)$。如果这个集合中的元素还满足交换律：$a*b=b*a$，则称此集合为“交换群”。群中元素个数称为元素的“阶”，元素个数有限的“群”称为“有限群”，群中的“单位元”是唯一的，群中任一元素的“逆元”是唯一的。

如果一个元素集合F，在其中定义加法和乘法两种运算，而使得F满足如下条件：

1）在加法运算下为一个交换群，即其元素满足自闭性、交换律和结合律；

2）在乘法运算下F也是一个交换群，单位元满足非零元素的自闭性，交换律、结合律和逆元唯一性；

3）在加法、乘法下满足分配律。

则称此元素集合为一个“域”，域中的元素个数称为域的“阶”。

有限域在编码理论中具有重要的地位。包括有限个元素的域称为有限域或 Galois 域，通常把具有q个元素的有限域记为GF(q)。每个域中必须包含一个零元素 0 和一个单位元素e，最简单的有限域是二元域GF(2)。

进一步，如果q为一个素数，则正整数集合$\{0,1,2,\cdots, q-1\}$在模q加法和乘法下为一个阶数为q的域GF(q)，称为素域，$GF(2)$即为一个素域。对于任何一个正整数m，可以将素域GF(q)扩展成有q^m个元素的域，称为域GF(q)的扩展域，记为GF(q^m)。任何有限域都是一个素域的扩展域。

为便于后文叙述，在此介绍几个概念。

◆ 本原元素：若在域GF(q)中，某一元素α的n次幂为$q-1$，则称α为本原元素。本原元素的各次幂构成域GF(q)的所有元素，每个有限域都有其本原元素。

◆ 本原多项式：系数取自域GF(q)上，以GF(q^m)中的本原元素为根的最小多项式$p(x)$，称为本原多项式。

◆ 域上多项式：系数取自域GF(q)上的多项式$f(x)$。在编码理论中，域上多项式的概念是比较有用的。

◆ 既约多项式：设$f(x)$是次数大于零的多项式，若除了常数和常数与本身的乘积以外再不能被域GF(q)上的其他多项式除尽，则称$f(x)$为域GF(q)上的既约多项式。

◆ 最小多项式：系数取自域GF(q)上，且以α为根的所有首一多项式（即最高次数的系数为 1 的多项式）中，必有一个次数最低的，称之为α的最小多项式。

1.1.2 纠错码

自 Shannon 的经典论文发表以来，纠错码就开始了迅速的发展，其主要发展历程如表 1.1 所示。

表 1.1 纠错码发展历程

纠 错 码	提 出 时 间	提 出 者
Hamming 码	1950	H.W.Hamming
Golay 码	1954	M.J.Golay
RM 码	1954	I.S.Reed、D.E.Muller
卷积码	1955	P.Elias
循环码	1957	E.Prange
RS 码	1960	I.S.Reed、G.Solomon
BCH 码	1960	R.C.Bose、D.K.Ray-Chaudhuri、A.Hocquenghem
LDPC 码	1961	R.G.Gallager
级联码	1966	G.D.Forney
Goppa 码	1970	V.D.Goppa
TCM 网格编码调制	1976	G.Ungerboeck
代数几何码	1982	M.A.Tsfasman、S.G.Vladut、T.Zink
Turbo 码	1993	C.Berrou、A.Glavieux、P.Thitimajshima

其实 Hamming 码的发现时间早于 Shannon 论文的发表时间，只是由于技术专利的原因导致其直到 1950 年才发表。

纠错码的实现方法是：信息位+监督位。由于监督位本身并不携带信息，因此，它们的加入必然要降低信息的传输速率。可见，纠错编码原则上以降低信息传输速率为代价来换取传输可靠性的提高。

纠错码有不同的分类方法，按照纠错码的不同功能，可以将其分为检错码、纠错码和纠删码；按照信息码元和附加监督码元之间的关系可分为线性码和非线性码；按照信息码元在编码后是否保持原来的形式不变，可分为系统码和非系统码；按照纠正错误类型的不同，可分为纠随机差错码和纠突发差错码，也有介于中间的纠随机/突发差错码；按照信息码元和监督码元之间的约束方式不同可划分为分组码和卷积码；按构码理论的不同，有代数码、几何码、算术码及组合码等。

除上述分类外，依看问题角度的不同，还有更多的分类方法。如按每个码元的取值情况，可以分为二进制码和多进制码；按码字之间的关系，有循环码和非循环码之分。不同的分类方法只是从不同的角度关注码的某一特性而加以归类，不代表该码的全部性质，如某线性码可能同时又是分组码，循环码，纠突发差错码，代数码和二进制编码。

线性分组码中信息码元和监督码元可以用线性方程联系起来，线性分组码满足：

1）封闭性，即任意两个许用码组之和仍然是一个许用码组；