<<矩阵与编码>>

图书基本信息

书名：<<矩阵与编码>>

13位ISBN编号：9787030247018

10位ISBN编号：7030247019

出版时间：2009-6

出版时间：科学出版社

作者：郑宝东，张春蕊　编

页数：102

<<矩阵与编码>>

前言

长期以来，在认识和改造世界的过程中，人们对数学所起作用的认识是逐渐形成的，而且这种认识随着时代的进步在不断深化。
特别是近年来，随着数字信息技术的飞速发展，人们对数学在科学技术中所起作用的认识也越来越深刻。
在我们所处的数字信息时代，数学科学的迅猛发展，更加确立了它在整个科学技术中的基础地位。
数学已突破传统的应用范围，向几乎所有人类知识的领域渗透，并为人类的物质和精神文明作出了贡献。
甚至诸如人文、社会科学这样的领域，为了准确和定量地考虑问题，数学也已经成为了重要的工具。
近年来，随着高等教育事业的不断发展，以及数学在科学技术各领域不断凸显的重要作用，全国许多高等院校纷纷筹办数学和与数学有关的各专业，而且这些新专业的成立已经为我们国家培养了大量的数学和与数学有关的社会急需人才。
但是，毋庸讳言，与规模快速增长不相协调的是，目前招生培养的很多数学类专业毕业生的数学修养、能力等方面的综合素质，却出现了不同程度的下降。
针对这种局面，我们必须从实际出发，加快数学类专业的全方位改革步伐，提高数学类专业的办学质量，努力培养适合数字信息化时代需要的高素质的数学人才。
当前，我国正处于高等教育从精英教育到大众化教育的转型时期，高等教育的培养目标、培养模式、培养方案正处在调整之中。
针对当前压缩必修课教学课时、增开更多选修课的现实情况，如何确保培养学生的质量，已是我们必须面对和迫切需要解决的问题。
显然在夯实基础的前提下，选择适当的教材、精选教学内容、合理选取和配置讲授近现代理论体系是解决质量问题的关键之一。

<<矩阵与编码>>

内容概要

本书主要介绍纠错码、现代密码和认证码的基本理论及其实现方法。
作为预备知识，本书回顾性地介绍近世代数中的基本概念、基本理论，随后介绍在纠错码、现代密码和认证码的理论中起重要作用的交换环上的矩阵理论。
本书侧重于数学在纠错码、现代密码和认证码的理论中的应用，内容全面，文字简练，概念清楚，深入浅出，便于理解。

本书适合作为高等院校数学本科各专业特别是信息与计算科学专业高年级有关选修课程的简明教材，也可供对纠错码、现代密码和认证码有兴趣的技术人员及高等院校有关专业的教师参考。

<<矩阵与编码>>

书籍目录

章节摘录

插图：在公钥密码中，由于加密算法是确定性的，一般来说一个明文对应于一个密文．因而密码分析者可以对密文进行选择明文攻击，即可以选择任意明文，用公钥进行加密得到相应的密文，与原密文对照，即得所需明文．比如，若密码分析者对股票市场上的“买进”与“卖出”等感兴趣，则他可事先将这些信息加密后存储起来．一旦以后截获该密文，就可以直接在所存储的密文中进行查找，从而求得相应的明文．确定性加密算法的这个缺陷使人们想到，是否存在加密算法是非确定性的，即加密是概率的公钥密码体制，如果这样的公钥密码体制存在，则将其称为概率加密公钥密码体制，简称概率加密体制．科学发明、发现的历史说明，有时候提出想法比有了想法寻找实现的方法更重要．概率加密原理其实非常简单，用确定性加密算法也能轻易地实现概率加密算法．1 982年，美国加利福尼亚大学伯克利分校的Golwasser，Micali提出了一种概率加密方法（简称为GM方法），即同一明文被加密后可以得到不同的密文．这样，选择明文攻击就会失效．

<<矩阵与编码>>

编辑推荐

《矩阵与编码》：精炼素材，以利于短时间内了解掌握最基本理论和方法侧重于数学在纠错码、现代密码和认证码中的应用适当配备例题、习题，便于理解相关概念、理论和方法

版权说明