Concise Encyclopedia of Coding Theory

This book constitutes the thoroughly refereed post-proceedings of the International Workshop on Coding and Cryptography, WCC 2005, held in Bergen, Norway, in March 2005. The 33 revised full papers were carefully reviewed and selected during two rounds of review. The papers address all aspects of coding theory, cryptography and related areas, theoretical or applied.
Discover the first unified treatment of today's most essential information technologies—Compressing, Encrypting, and Encoding. With identity theft, cybercrime, and digital file sharing proliferating in today's wired world, providing safe and accurate information transfers has become a paramount concern. The issues and problems raised in this endeavor are encompassed within three disciplines: cryptography, information theory, and error-correction. As technology continues to develop, these fields have converged at a practical level, increasing the need for a unified treatment of these three cornerstones of the information age. Stressing the interconnections of the disciplines, Cryptography, Information Theory, and Error-Correction offers a complete, yet accessible account of the technologies shaping the 21st century. This book contains the most up-to-date, detailed, and balanced treatment available on these subjects. The authors draw on their experience both in the classroom and in industry, giving the book's material and presentation a unique real-world orientation. With its reader-friendly style and interdisciplinary emphasis, Cryptography, Information Theory, and Error-Correction serves as both an admirable teaching text and a tool for self-learning. The chapter structure allows for anyone with a high school mathematics education to gain a strong conceptual understanding, and provides higher-level students with more mathematically advanced topics. The authors clearly map out paths through the book for readers of all levels to maximize their learning. This book is suitable for courses in cryptography, information theory, or error-correction as well as courses discussing all three areas. Provides over 300 example problems with solutions. Presents new and exciting algorithms adopted by industry. Discusses potential applications in cell biology. Details a new characterization of perfect secrecy. Features in-depth coverage of linear feedback shift registers (LFSR), a staple of modern computing. Follows a layered approach to facilitate discussion, with summaries followed by more detailed explanations. Provides a new perspective on the RSA algorithm. Cryptography, Information Theory, and Error-Correction is an excellent in-depth text for both graduate and undergraduate students of mathematics, computer science, and engineering. It is also an authoritative overview for IT professionals, statisticians, mathematicians, computer scientists, electrical engineers, entrepreneurs, and the generally curious.

The latest edition of this classic is updated with new problem sets and material. The Second Edition of this
fundamental textbook maintains the book's tradition of clear, thought-provoking instruction. Readers are provided once again with an instructive mix of mathematics, physics, statistics, and information theory. All the essential topics in information theory are covered in detail, including entropy, data compression, channel capacity, rate distortion, network information theory, and hypothesis testing. The authors provide readers with a solid understanding of the underlying theory and applications. Problem sets and a telegraphic summary at the end of each chapter further assist readers. The historical notes that follow each chapter recap the main points. The Second Edition features: * Chapters reorganized to improve teaching * 200 new problems * New material on source coding, portfolio theory, and feedback capacity * Updated references Now current and enhanced, the Second Edition of Elements of Information Theory remains the ideal textbook for upper-level undergraduate and graduate courses in electrical engineering, statistics, and telecommunications.

**Information Theory**

Developing many of the major, exciting, pre- and post-millennium developments from the ground up, this book is an ideal entry point for graduate students into quantum information theory. Significant attention is given to quantum mechanics for quantum information theory, and careful studies of the important protocols of teleportation, superdense coding, and entanglement distribution are presented. In this new edition, readers can expect to find over 100 pages of new material, including detailed discussions of Bell's theorem, the CHSH game, Tsirelson's theorem, the axiomatic approach to quantum channels, the definition of the diamond norm and its interpretation, and a proof of the Choi–Kraus theorem. Discussion of the importance of the quantum dynamic capacity formula has been completely revised, and many new exercises and references have been added. This new edition will be welcomed by the upcoming generation of quantum information theorists and the already established community of classical information theorists.

**Coding and Cryptography**

Modern introduction to theory of coding and decoding with many exercises and examples.

**Information Theory and Coding by Example**
This book provides a practical introduction to the theory and practice of coding and information theory for application in the field of electronic communications. It is written at an introductory level and assumes no prior background in coding or information theory. While the mathematical level is detailed, it is still introductory. Through a discussion that balances theory and practical applications and abandons the traditional "theorem-proof" format, this valuable book presents an overview of digital communication systems and the concept of information. It is written in an easy-to-follow conversational style that integrates practical engineering issues through formal and conceptual discussions of mathematical issues. It also makes extensive use of explicit examples that illustrate methods and theory throughout the book. For the professional, it provides an essential hands-on head start for real-world projects and situations. An essential reference for professional engineers in the field of electronic communications.

**Quantum Information, Computation and Cryptography**

This book is an evolution from my book *A First Course in Information Theory* published in 2002 when network coding was still at its infancy. The last few years have witnessed the rapid development of network coding into a research field of its own in information science. With its root in information theory, network coding has not only brought about a paradigm shift in network communications at large, but also had significant influence on such specific research fields as coding theory, networking, switching, wireless communications, distributed data storage, cryptography, and optimization theory. While new applications of network coding keep emerging, the fundamental results that lay the foundation of the subject are more or less mature. One of the main goals of this book therefore is to present these results in a unifying and coherent manner. While the previous book focused only on information theory for discrete random variables, the current book contains two new chapters on information theory for continuous random variables, namely the chapter on differential entropy and the chapter on continuous-valued channels. With these topics included, the book becomes more comprehensive and is more suitable to be used as a textbook for a course in an electrical engineering department.

**Codes and Cryptography**

This book aims at presenting the field of Quantum Information Theory in an intuitive, didactic and self-contained
way, taking into account several multidisciplinary aspects. Therefore, this book is particularly suited to students and researchers willing to grasp fundamental concepts in Quantum Computation and Quantum Information areas. The field of Quantum Information Theory has increased significantly over the last three decades. Many results from classical information theory were translated and extended to a scenario where quantum effects become important. Most of the results in this area allows for an asymptotically small probability of error to represent and transmit information efficiently. Claude E. Shannon was the first scientist to realize that error-free classical information transmission can be accomplished under certain conditions. More recently, the concept of error-free classical communication was translated to the quantum context. The so-called Quantum Zero-Error Information Theory completes and extends the Shannon Zero-Error Information Theory.

**Information Theory, Coding and Cryptography**

Information Theory, Coding & Cryptography has been designed as a comprehensive book for the students of engineering discussing Source Encoding, Error Control Codes & Cryptography. The book contains the recent developments of coded modulation, trellises for codes, turbo coding for reliable data and interleaving. The text balances the mathematical rigor with exhaustive amount of solved, unsolved questions along with a database of MCQs.

**Boolean Functions for Cryptography and Coding Theory**

This fundamental monograph introduces both the probabilistic and algebraic aspects of information theory and coding. It has evolved from the authors' years of experience teaching at the undergraduate level, including several Cambridge Maths Tripos courses. The book provides relevant background material, a wide range of worked examples and clear solutions to problems from real exam papers. It is a valuable teaching aid for undergraduate and graduate students, or for researchers and engineers who want to grasp the basic principles.

**Quantum Computation and Quantum Information**

Most coding theory experts date the origin of the subject with the 1948 publication of A Mathematical Theory of
Communication by Claude Shannon. Since then, coding theory has grown into a discipline with many practical applications (antennas, networks, memories), requiring various mathematical techniques, from commutative algebra, to semi-definite programming, to algebraic geometry. Most topics covered in the Concise Encyclopedia of Coding Theory are presented in short sections at an introductory level and progress from basic to advanced level, with definitions, examples, and many references. The book is divided into three parts: Part I fundamentals: cyclic codes, skew cyclic codes, quasi-cyclic codes, self-dual codes, codes and designs, codes over rings, convolutional codes, performance bounds Part II families: AG codes, group algebra codes, few-weight codes, Boolean function codes, codes over graphs Part III applications: alternative metrics, algorithmic techniques, interpolation decoding, pseudo-random sequences, lattices, quantum coding, space-time codes, network coding, distributed storage, secret-sharing, and code-based-cryptography. Features Suitable for students and researchers in a wide range of mathematical disciplines Contains many examples and references Most topics take the reader to the frontiers of research

**Quantum Zero-Error Information Theory**

It has long been recognized that there are fascinating connections between coding theory, cryptology, and combinatorics. Therefore it seemed desirable to us to organize a conference that brings together experts from these three areas for a fruitful exchange of ideas. We decided on a venue in the Huang Shan (Yellow Mountain) region, one of the most scenic areas of China, so as to provide the additional inducement of an attractive location. The conference was planned for June 2003 with the official title Workshop on Coding, Cryptography and Combinatorics (CCC 2003). Those who are familiar with events in East Asia in the first half of 2003 can guess what happened in the end, namely the conference had to be cancelled in the interest of the health of the participants. The SARS epidemic posed too serious a threat. At the time of the cancellation, the organization of the conference was at an advanced stage: all invited speakers had been selected and all abstracts of contributed talks had been screened by the program committee. Thus, it was decided to call on all invited speakers and presenters of accepted contributed talks to submit their manuscripts for publication in the present volume. Altogether, 39 submissions were received and subjected to another round of refereeing. After careful scrutiny, 28 papers were accepted for publication.
Information Theory, Coding and Cryptography

The inaugural research program of the Institute for Mathematical Sciences at the National University of Singapore took place from July to December 2001 and was devoted to coding theory and cryptology. As part of the program, tutorials for graduate students and junior researchers were given by world-renowned scholars. These tutorials covered fundamental aspects of coding theory and cryptology and were designed to prepare for original research in these areas. The present volume collects the expanded lecture notes of these tutorials. The topics range from mathematical areas such as computational number theory, exponential sums and algebraic function fields through coding-theory subjects such as extremal problems, quantum error-correcting codes and algebraic-geometry codes to cryptologic subjects such as stream ciphers, public-key infrastructures, key management, authentication schemes and distributed system security. Contents: Extremal Problems of Coding Theory (A Barg) Analysis and Design Issues for Synchronous Stream Ciphers (E Dawson & L Simpson) Quantum Error-Correcting Codes (K Feng) Public Key Infrastructures (D Gollmann) Computational Methods in Public Key Cryptology (A K Lenstra) Detecting and Revoking Compromised Keys (T Matsumoto) Algebraic Function Fields Over Finite Fields (H Niederreiter) Authentication Schemes (D Y Pei) Exponential Sums in Coding Theory, Cryptology and Algorithms (I E Shparlinski) Distributed Authorization: Principles and Practice (V Varadharajan) Introduction to Algebraic Geometry Codes (C P Xing)

Readership: Graduate students and researchers in number theory, discrete mathematics, coding theory, cryptology and IT security. Keywords: Coding Theory; Cryptology; Number Theory; Algebraic-Geometry Codes; Public-Key Infrastructures; Error-Correcting Codes

Coding Theory

This textbook equips graduate students and advanced undergraduates with the necessary theoretical tools for applying algebraic geometry to information theory, and it covers primary applications in coding theory and cryptography. Harald Niederreiter and Chaoping Xing provide the first detailed discussion of the interplay between nonsingular projective curves and algebraic function fields over finite fields. This interplay is fundamental to research in the field today, yet until now no other textbook has featured complete proofs of it. Niederreiter and Xing cover classical applications like algebraic-geometry codes and elliptic-curve cryptosystems as well as material not treated by other books, including function-field codes, digital nets, code-based public-key
cryptosystems, and frameproof codes. Combining a systematic development of theory with a broad selection of real-world applications, this is the most comprehensive yet accessible introduction to the field available. Introduces graduate students and advanced undergraduates to the foundations of algebraic geometry for applications to information theory. Provides the first detailed discussion of the interplay between projective curves and algebraic function fields over finite fields. Includes applications to coding theory and cryptography. Covers the latest advances in algebraic-geometry codes. Features applications to cryptography not treated in other books.

**Introduction to Cryptography With Coding Theory**

Containing data on number theory, encryption schemes, and cyclic codes, this highly successful textbook, proven by the authors in a popular two-quarter course, presents coding theory, construction, encoding, and decoding of specific code families in an "easy-to-use" manner appropriate for students with only a basic background in mathematics offerin

**Fundamentals of Information Theory and Coding Design**

**Algebraic Geometry in Coding Theory and Cryptography**

Algorithmic Information Theory treats the mathematics of many important areas in digital information processing. It has been written as a read-and-learn book on concrete mathematics, for teachers, students and practitioners in electronic engineering, computer science and mathematics. The presentation is dense, and the examples and exercises are numerous. It is based on lectures on information technology (Data Compaction, Cryptography, Polynomial Coding) for engineers.

**Coding Theory and Cryptology**

Covering topics in algebraic geometry, coding theory, and cryptography, this volume presents interdisciplinary
group research completed for the February 2016 conference at the Institute for Pure and Applied Mathematics (IPAM) in cooperation with the Association for Women in Mathematics (AWM). The conference gathered research communities across disciplines to share ideas and problems in their fields and formed small research groups made up of graduate students, postdoctoral researchers, junior faculty, and group leaders who designed and led the projects. Peer reviewed and revised, each of this volume's five papers achieves the conference’s goal of using algebraic geometry to address a problem in either coding theory or cryptography. Proposed variants of the McEliece cryptosystem based on different constructions of codes, constructions of locally recoverable codes from algebraic curves and surfaces, and algebraic approaches to the multicast network coding problem are only some of the topics covered in this volume. Researchers and graduate-level students interested in the interactions between algebraic geometry and both coding theory and cryptography will find this volume valuable.

**Two-Dimensional Information Theory and Coding**

Table of contents

**Coding, Cryptography and Combinatorics**

First-ever comprehensive introduction to the major new subject of quantum computing and quantum information.

**Algorithmic Information Theory**

Algebraic & geometry methods have constituted a basic background and tool for people working on classic block coding theory and cryptography. Nowadays, new paradigms on coding theory and cryptography have arisen such as: Network coding, S-Boxes, APN Functions, Steganography and decoding by linear programming. Again understanding the underlying procedure and symmetry of these topics needs a whole bunch of non trivial knowledge of algebra and geometry that will be used to both, evaluate those methods and search for new codes and cryptographic applications. This book shows those methods in a self-contained form.
The theory of algebraic function fields over finite fields has its origins in number theory. However, after Goppa’s discovery of algebraic geometry codes around 1980, many applications of function fields were found in different areas of mathematics and information theory. This book presents survey articles on some of these new developments. The topics focus on material which has not yet been presented in other books or survey articles.

Algebraic Geometry for Coding Theory and Cryptography

Selected Topics in Information and Coding Theory

Coding Theory and Cryptography

These are the proceedings of the Conference on Coding Theory, Cryptography, and Number Theory held at the U. S. Naval Academy during October 25-26, 1998. This book concerns elementary and advanced aspects of coding theory and cryptography. The coding theory contributions deal mostly with algebraic coding theory. Some of these papers are expository, whereas others are the result of original research. The emphasis is on geometric Goppa codes (Shokrollahi, Shokranian-Joyner), but there is also a paper on codes arising from combinatorial constructions (Michael). There are both, historical and mathematical papers on cryptography. Several of the contributions on cryptography describe the work done by the British and their allies during World War II to crack the German and Japanese ciphers (Hamer, Hilton, Tutte, Weierud, Urling). Some mathematical aspects of the Enigma rotor machine (Sherman) and more recent research on quantum cryptography (Lomonoco) are described. There are two papers concerned with the RSA cryptosystem and related number-theoretic issues (Wardlaw, Cosgrave).
From the Rosetta Stone to public-key cryptography, the art and science of cryptology has been used to unlock the vivid history of ancient cultures, to turn the tide of warfare, and to thwart potential hackers from attacking computer systems. Codes: The Guide to Secrecy from Ancient to Modern Times explores the depth and breadth of the field, remain

**A Student's Guide to Coding and Information Theory**

The work introduces the fundamentals concerning the measure of discrete information, the modeling of discrete sources without and with a memory, as well as of channels and coding. The understanding of the theoretical matter is supported by many examples. One particular emphasis is put on the explanation of Genomic Coding. Many examples throughout the book are chosen from this particular area and several parts of the book are devoted to this exciting implication of coding.

**The Theory of Information and Coding**

Student edition of the classic text in information and coding theory

**Quantum Information Theory**

A concise, easy-to-read guide, introducing beginners to the engineering background of modern communication systems, from mobile phones to data storage. Assuming only basic knowledge of high-school mathematics and including many practical examples and exercises to aid understanding, this is ideal for anyone who needs a quick introduction to the subject.

**Coding Theory and Cryptography**

A complete introduction to the subject, providing the key techniques for modeling two-dimensional data and estimating their information content.
Foundations of Coding

Although devoted to constructions of good codes for error control, secrecy or data compression, the emphasis is on the first direction. Introduces a number of important classes of error-detecting and error-correcting codes as well as their decoding methods. Background material on modern algebra is presented where required. The role of error-correcting codes in modern cryptography is treated as are data compression and other topics related to information theory. The definition-theorem proof style used in mathematics texts is employed through the book but formalism is avoided wherever possible.

Codes

Information and Coding Theory

This multi-authored textbook addresses graduate students with a background in physics, mathematics or computer science. No research experience is necessary. Consequently, rather than comprehensively reviewing the vast body of knowledge and literature gathered in the past twenty years, this book concentrates on a number of carefully selected aspects of quantum information theory and technology. Given the highly interdisciplinary nature of the subject, the multi-authored approach brings together different points of view from various renowned experts, providing a coherent picture of the subject matter. The book consists of ten chapters and includes examples, problems, and exercises. The first five present the mathematical tools required for a full comprehension of various aspects of quantum mechanics, classical information, and coding theory. Chapter 6 deals with the manipulation and transmission of information in the quantum realm. Chapters 7 and 8 discuss experimental implementations of quantum information ideas using photons and atoms. Finally, chapters 9 and 10 address ground-breaking applications in cryptography and computation.

Coding Theory and Cryptography

Page 12/15
Many people do not realise that mathematics provides the foundation for the devices we use to handle information in the modern world. Most of those who do know probably think that the parts of mathematics involved are quite "cl- sical", such as Fourier analysis and differential equations. In fact, a great deal of the mathematical background is part of what used to be called "pure" ma- ematics, indicating that it was created in order to deal with problems that originated within mathematics itself. It has taken many years for mathema- cians to come to terms with this situation, and some of them are still not entirely happy about it. This book is an integrated introduction to Coding. By this I mean replacing symbolic information, such as a sequence of bits or a message written in a natural language, by another message using (possibly) different symbols. There are three main reasons for doing this: Economy (data compression), Reliability (correction of errors), and Security (cryptography). I have tried to cover each of these three areas in sufficient depth so that the reader can grasp the basic problems and go on to more advanced study. The mathematical theory is introduced in a way that enables the basic problems to be stated carefully, but without unnecessary abstraction. The prerequisites (sets and functions, matrices, finite probability) should be familiar to anyone who has taken a standard course in mathematical methods or discrete mathematics. A course in elementary abstract algebra and/or number theory would be helpful, but the book contains the essential facts, and readers without this background should be able to understand what is going on.

**Cryptography, Information Theory, and Error-Correction**

This textbook forms an introduction to codes, cryptography and information theory as it has developed since Shannon's original papers.

**Fundamentals in Information Theory and Coding**

Boolean functions are essential to systems for secure and reliable communication. This comprehensive survey of Boolean functions for cryptography and coding covers the whole domain and all important results, building on the author's influential articles with additional topics and recent results. A useful resource for researchers and graduate students, the book balances detailed discussions of properties and parameters with examples of various types of cryptographic attacks that motivate the consideration of these parameters. It provides all the necessary
background on mathematics, cryptography, and coding, and an overview on recent applications, such as side channel attacks on smart cards, cloud computing through fully homomorphic encryption, and local pseudo-random generators. The result is a complete and accessible text on the state of the art in single and multiple output Boolean functions that illustrates the interaction between mathematics, computer science, and telecommunications.

**Elements of Information Theory**

Books on information theory and coding have proliferated over the last few years, but few succeed in covering the fundamentals without losing students in mathematical abstraction. Even fewer build the essential theoretical framework when presenting algorithms and implementation details of modern coding systems. Without abandoning the theoretical

**Algebraic Geometry Modeling in Information Theory**

This text is an elementary introduction to information and coding theory. The first part focuses on information theory, covering uniquely decodable and instantaneous codes, Huffman coding, entropy, information channels, and Shannon’s Fundamental Theorem. In the second part, linear algebra is used to construct examples of such codes, such as the Hamming, Hadamard, Golay and Reed-Muller codes. Contains proofs, worked examples, and exercises.

**Topics in Geometry, Coding Theory and Cryptography**

The National Security Agency funded a conference on Coding theory, Cryptography, and Number Theory (nicknamed Cryptoday) at the United States Naval Academy, on October 25-27, 1998. We were very fortunate to have been able to attract talented mathematicians and cryptographers to the meeting. Unfortunately, some people couldn't make it for either scheduling or funding reasons. Some of these have been invited to contribute a paper anyway. In addition, Prof. William Tutte and Frode Weierud have been kind enough to allow the inclusion of some very interesting unpublished papers of theirs. The papers basically fall into three categories. Historical papers on
cryptography done during World War II (Hatch, Hilton, Tutte, Ulfving, and Weierud), mathematical papers on more recent methods in cryptography (Cosgrave, Lomonoco, Wardlaw), and mathematical papers in coding theory (Gao, Joyner, Michael, Shokranian, Shokrollahi). A brief biography of the authors follows. - Peter Hilton is a Distinguished Professor of Mathematics Emeritus at the State University of New York at Binghamton. He worked from 1941 to 1945 in the British cryptanalytic headquarters at Bletchley Park. Professor Hilton has done extensive research in algebraic topology and group theory. - William Tutte is a Distinguished Professor Emeritus and an Adjunct Professor in the Combinatorics and Optimization Department at the University of Waterloo. He worked from 1941 to 1945 in the British cryptanalytic headquarters at Bletchley Park. Professor Tutte has done extensive research in the field of combinatorics.

Information Theory and Network Coding

Copyright code: 8359f1f2ed5e015cd76e0d643a32f808