Notes On Hashing Mit

Data StructuresHashing in Computer ScienceMining of Massive DatasetsZahlungssysteme im Electronic CommerceApplied Cryptography and Network SecurityImage Understanding WorkshopMathematics for Computer ScienceAdvanced Data StructuresComplexity of Lattice ProblemsUnderstanding CryptographyOpen Data StructuresExplaining the Success of Nearest Neighbor Methods in PredictionInformation RetrievalAdaptation in Natural and Artificial SystemsAdvances in Cryptology - ASIACRYPT 2003CalculusIntroduction to Modern CryptographyAlgorithmsElements of Information TheoryInternational Mathematical NewsDesigning an InternetAdvances in Cryptology - CRYPTO 2002The Definitive Guide to DjangoLions' Commentary on UNIX 6th Edition with Source CodeRethinking Public Key Infrastructures and Digital CertificatesIntroduction to Computational Molecular BiologySoftware-optimized Universal Hashing and Message AuthenticationAdvances in Cryptology — CRYPTO '93Twenty Years Before the BlackboardExperimental and Efficient AlgorithmsThe Power of Habit: by Charles Duhigg | Summary & AnalysisSelected Areas in CryptographyAdvances in Cryptology — CRYPTO '96Principles of Computer System DesignMathematical WritingStructure and Interpretation of Computer Programs - 2nd EditionIntroduction To AlgorithmsIntroduction to Information RetrievalAlgorithm DesignPrinciples of Model Checking

Data Structures

An introduction to information retrieval, the foundation for modern search engines, that emphasizes implementation and experimentation.

Hashing in Computer Science

Basic concepts of molecular biology. Strings, graphs, and algorithms. Sequence comparasion and database search. Fragment assembly of DNA. Physical mapping of DNA. Phylogenetic trees. Genome rearrangements. Molecular structure prediction. epilogue: computing with DNA. Answers to selected exercises. References. index.

Mining of Massive Datasets

Structure and Interpretation of Computer Programs by Harold Abelson and Gerald Jay Sussman is licensed under a Creative Commons Attribution-NonCommercial 3.0 License.

Zahlungssysteme im Electronic Commerce

Class-tested and coherent, this textbook teaches classical and web information retrieval, including web search and the related areas of text classification and text clustering from basic concepts. It gives an up-to-date treatment of all aspects of the design and implementation of systems for gathering, indexing, and searching documents; methods for evaluating

systems; and an introduction to the use of machine learning methods on text collections. All the important ideas are explained using examples and figures, making it perfect for introductory courses in information retrieval for advanced undergraduates and graduate students in computer science. Based on feedback from extensive classroom experience, the book has been carefully structured in order to make teaching more natural and effective. Slides and additional exercises (with solutions for lecturers) are also available through the book's supporting website to help course instructors prepare their lectures.

Applied Cryptography and Network Security

Crypto '96, the Sixteenth Annual Crypto Conference, is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and P- vacy and the Computer Science Department of the University of California at Santa Barbara (UCSB). It takes place at UCSB from August 18 to 22, 1996. The General Chair, Richard Graveman, is responsible for local organization and registration. The scientific program was organized by the 16-member Program C- mittee. We considered 115 papers. (An additional 15 submissions had to be summarily rejected because of lateness or major noncompliance with the c- ditions in the Call for Papers.) Of these, 30 were accepted for presentation. In addition, there will be five invited talks by Ernest Brickell. Andrew Clark, Whitfield Diffie, Ronald Rivest,

and Cliff Stoll. A Rump Session will be chaired by Stuart Haber. These proceedings contain the revised versions of the 30 contributed talks. least three com- The submitted version of each paper was examined by at mittee members and/or outside experts, and their comments were taken into account in the revisions. However, the authors (and not the committee) bear full responsibility for the content of their papers.

Image Understanding Workshop

Mathematics for Computer Science

This book constitutes the refereed proceedings of the 12th International Conference on Applied Cryptography and Network Security, ACNS 2014, held in Lausanne, Switzerland, in June 2014. The 33 revised full papers included in this volume were carefully reviewed and selected from 147 submissions. They are organized in topical sections on key exchange; primitive construction; attacks (public-key cryptography); hashing; cryptanalysis and attacks (symmetric cryptography); network security; signatures; system security; and secure computation.

Advanced Data Structures

Explains the success of Nearest Neighbor Methods in Prediction, both in theory and in practice.

Complexity of Lattice Problems

Written by one of the developers of the technology, Hashing is both a historical document on the development of hashing and an analysis of the applications of hashing in a society increasingly concerned with security. The material in this book is based on courses taught by the author, and key points are reinforced in sample problems and an accompanying instructor s manual. Graduate students and researchers in mathematics, cryptography, and security will benefit from this overview of hashing and the complicated mathematics that it requires.

Understanding Cryptography

This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book. Algorithm Design introduces algorithms by looking at the real-world problems that motivate them. The book teaches students a range of design and analysis techniques for problems that arise in computing applications. The text encourages an understanding of the algorithm design process and an appreciation of the role of algorithms in the broader field of computer science. August 6, 2009 Author, Jon Kleinberg, was recently cited in the New York Times for his statistical analysis research in the Internet age.

Open Data Structures

"Published by OpenStax College, Calculus is designed for the typical two- or three-semester general calculus course, incorporating innovative features to enhance

student learning. The book guides students through the core concepts of calculus and helps them understand how those concepts apply to their lives and the world around them. Due to the comprehensive nature of the material, we are offering the book in three volumes for flexibility and efficiency. Volume 1 covers functions, limits, derivatives, and integration."--BC Campus website.

Explaining the Success of Nearest Neighbor Methods in Prediction

Information Retrieval

Django, the Python-based Web development framework, is one of the hottest topics in Web development today. Its creator (and co-author of this book) Adrian Holovaty has built a compelling array of Web applications using Django, including http://chicagocrime.org. Django creator Adrian Holovaty and lead developer Jacob Kaplan-Moss have created this book as the definitive guide to the technology. Beginning with fundamentals such as installation and configuration, the book tackles sophisticated features of Django, such as outputting non-HTML content such as RSS feeds and PDFs, caching, and user management. Also includes a detailed reference to Django's many configuration options and commands.

Adaptation in Natural and Artificial Systems

Inhaltsangabe:Einleitung: In den vergangenen Jahren beherrschten Diskussionen um die Globalisierung, die Entwicklung zur Dienstleistungsgesellschaft und virtuelle Unternehmen die Titelseiten der Manager Magazine. Seit kürzerem mußten diese Begriffe einem einzigen weichen, der sie alle zu vereinen scheint: Electronic Commerce. Der elektronischen Anbahnung und Abwicklung von Geschäften scheinen in der Zukunft kaum Grenzen gesetzt. Eine effizientere Gestaltung der Prozesse wird versprochen. Doch bevor dieses Versprechen eingelöst und Datenströme ersetzen können, was heute noch auf sichtbaren Wegen übertragen wird, müssen eine Vielzahl von Voraussetzungen erfüllt werden. Eine der wesentlichen Voraussetzungen ist die Abwicklung von Zahlungen über das Internet. Wie zu sehen sein wird, ist bereits eine Vielzahl von Zahlungssystemen speziell für den elektronischen Handel entwickelt worden. Diese eignen sich allerdings aufgrund ihrer Funktionen nicht für alle Transaktionsarten. Ziel dieser Arbeit ist es daher, heraus zu arbeiten welche Art Zahlungssysteme für welche Geschäftsbeziehungen oder Produktgruppen geeignet sind und welche Richtung die Entwicklung dieser Systeme in der Zukunft nehmen wird. Gang der Untersuchung: Eine umfassende Einführung in den Electronic Commerce liefert zu Beginn die wichtigsten Hintergründe. Angefangen mit der ökonomischen Betrachtung des Entstehen des neuen Marktes, werden elektronische Märkte in den historischen Kontext eingeordnet. Auch aus rechtlicher Sicht, sind im Zusammenhang mit dem neuen Geschäftsfeld verschiedene Rahmenbedingungen zu schaffen oder

bestehende Gesetze auf neue Sachlagen anzuwenden. Besonders hervorzuheben ist dabei die Anerkennung digital signierter Verträge, ohne die viele Marktteilnehmer blind auf die Erfüllung der lediglich elektronisch getroffenen Abmachungen durch einen unbekannten Geschäftspartner vertrauen müssen. Die Staaten spielen bei der Schaffung der Rahmenbedingungen natürlich eine wichtige Rolle. Sie handeln auch aus Eigeninteresse, da durch den Electronic Commerce sowohl Steuer- und Zolleinnahmen gefährdet scheinen, als auch die Souveränität des staatlichen Geldmonopols. Der elektronische Zahlungsverkehr, der im Mittelpunkt dieser Betrachtung steht, kann, wie in Kapitel 2 gezeigt wird, in vielerlei Sicht als eine Bedrohung für nationalstaatliche Währungen angesehen werden. Zur Abwicklung von Transaktionen im Internet sind Alternativen zu den klassischen Zahlungsmitteln allemal []

Advances in Cryptology - ASIACRYPT 2003

Cryptography plays a key role in ensuring the privacy and integrity of data and the security of computer networks. Introduction to Modern Cryptography provides a rigorous yet accessible treatment of modern cryptography, with a focus on formal definitions, precise assumptions, and rigorous proofs. The authors introduce the core principles of modern cryptography, including the modern, computational approach to security that overcomes the limitations of perfect secrecy. An extensive treatment of private-

key encryption and message authentication follows. The authors also illustrate design principles for block ciphers, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and present provably secure constructions of block ciphers from lower-level primitives. The second half of the book focuses on public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, El Gamal, and other cryptosystems. After exploring public-key encryption and digital signatures, the book concludes with a discussion of the random oracle model and its applications. Serving as a textbook, a reference, or for self-study, Introduction to Modern Cryptography presents the necessary tools to fully understand this fascinating subject.

Calculus

This book covers elementary discrete mathematics for computer science and engineering. It emphasizes mathematical definitions and proofs as well as applicable methods. Topics include formal logic notation, proof methods; induction, well-ordering; sets, relations; elementary graph theory; integer congruences; asymptotic notation and growth of functions; permutations and combinations, counting principles; discrete probability. Further selected topics may also be covered, such as recursive definition and structural induction; state machines and invariants; recurrences; generating functions.

Introduction to Modern Cryptography

A comprehensive introduction to the foundations of model checking, a fully automated technique for finding flaws in hardware and software; with extensive examples and both practical and theoretical exercises. Our growing dependence on increasingly complex computer and software systems necessitates the development of formalisms, techniques, and tools for assessing functional properties of these systems. One such technique that has emerged in the last twenty years is model checking, which systematically (and automatically) checks whether a model of a given system satisfies a desired property such as deadlock freedom, invariants, and request-response properties. This automated technique for verification and debugging has developed into a mature and widely used approach with many applications. Principles of Model Checking offers a comprehensive introduction to model checking that is not only a text suitable for classroom use but also a valuable reference for researchers and practitioners in the field. The book begins with the basic principles for modeling concurrent and communicating systems, introduces different classes of properties (including safety and liveness), presents the notion of fairness, and provides automata-based algorithms for these properties. It introduces the temporal logics LTL and CTL, compares them, and covers algorithms for verifying these logics, discussing real-time systems as well as systems subject to random phenomena. Separate chapters treat such efficiency-improving techniques as abstraction and symbolic manipulation. The book includes an extensive set of examples (most of which run through several chapters) and a

complete set of basic results accompanied by detailed proofs. Each chapter concludes with a summary, bibliographic notes, and an extensive list of exercises of both practical and theoretical nature.

Algorithms

Cryptography is now ubiquitous – moving beyond the traditional environments, such as government communications and banking systems, we see cryptographic techniques realized in Web browsers, e-mail programs, cell phones, manufacturing systems, embedded software, smart buildings, cars, and even medical implants. Today's designers need a comprehensive understanding of applied cryptography. After an introduction to cryptography and data security, the authors explain the main techniques in modern cryptography, with chapters addressing stream ciphers, the Data Encryption Standard (DES) and 3DES, the Advanced Encryption Standard (AES), block ciphers, the RSA cryptosystem, public-key cryptosystems based on the discrete logarithm problem, elliptic-curve cryptography (ECC), digital signatures, hash functions, Message Authentication Codes (MACs), and methods for key establishment, including certificates and public-key infrastructure (PKI). Throughout the book, the authors focus on communicating the essentials and keeping the mathematics to a minimum, and they move quickly from explaining the foundations to describing practical implementations, including recent topics such as lightweight ciphers for RFIDs and mobile devices, and current key-length recommendations.

The authors have considerable experience teaching applied cryptography to engineering and computer science students and to professionals, and they make extensive use of examples, problems, and chapter reviews, while the book's website offers slides, projects and links to further resources. This is a suitable textbook for graduate and advanced undergraduate courses and also for self-study by engineers.

Elements of Information Theory

List of figures. Preface to the 1992 edition. Preface. The general setting. A formal framework. lustrations. Schemata. The optimal allocation of trials. Reproductive plans and genetic operators. The robustness of genetic plans. Adaptation of codings and representations. An overview. Interim and prospectus. Glossary of important symbols.

International Mathematical News

This book constitutes the refereed proceedings of the 22nd International Cryptology Conference, CRYPTO 2002, held in Santa Barbara, CA, in August 2002. The 39 revised full papers presented were carefully reviewed and selected from a total of 175 submissions. The papers are organized in topical sections on block ciphers, multi-user oriented cryptosystems, foundations and methodology, security and practical protocols, secure multiparty computation, public key encryption, information theory and secret sharing, cipher design and analysis,

elliptic curves and Abelian varieties, authentication, distributed cryptosystems, pseudorandomness, stream ciphers and Boolean functions, commitment schemes, and signature schemes.

Designing an Internet

Why the Internet was designed to be the way it is, and how it could be different, now and in the future. How do you design an internet? The architecture of the current Internet is the product of basic design decisions made early in its history. What would an internet look like if it were designed, today, from the ground up? In this book, MIT computer scientist David Clark explains how the Internet is actually put together, what requirements it was designed to meet, and why different design decisions would create different internets. He does not take today's Internet as a given but tries to learn from it, and from alternative proposals for what an internet might be, in order to draw some general conclusions about network architecture. Clark discusses the history of the Internet, and how a range of potentially conflicting requirements—including longevity, security, availability, economic viability, management, and meeting the needs of society—shaped its character. He addresses both the technical aspects of the Internet and its broader social and economic contexts. He describes basic design approaches and explains, in terms accessible to nonspecialists, how networks are designed to carry out their functions. (An appendix offers a more technical discussion of network functions for readers

who want the details.) He considers a range of alternative proposals for how to design an internet, examines in detail the key requirements a successful design must meet, and then imagines how to design a future internet from scratch. It's not that we should expect anyone to do this; but, perhaps, by conceiving a better future, we can push toward it.

Advances in Cryptology - CRYPTO 2002

Principles of Computer System Design is the first textbook to take a principles-based approach to the computer system design. It identifies, examines, and illustrates fundamental concepts in computer system design that are common across operating systems, networks, database systems, distributed systems, programming languages, software engineering, security, fault tolerance, and architecture. Through carefully analyzed case studies from each of these disciplines, it demonstrates how to apply these concepts to tackle practical system design problems. To support the focus on design, the text identifies and explains abstractions that have proven successful in practice such as remote procedure call, client/service organization, file systems, data integrity, consistency, and authenticated messages. Most computer systems are built using a handful of such abstractions. The text describes how these abstractions are implemented, demonstrates how they are used in different systems, and prepares the reader to apply them in future designs. The book is recommended for junior and senior undergraduate students in Operating Systems, Distributed Systems, Distributed

Operating Systems and/or Computer Systems Design courses; and professional computer systems designers. Features: Concepts of computer system design guided by fundamental principles. Cross-cutting approach that identifies abstractions common to networking, operating systems, transaction systems, distributed systems, architecture, and software engineering. Case studies that make the abstractions real: naming (DNS and the URL); file systems (the UNIX file system); clients and services (NFS); virtualization (virtual machines); scheduling (disk arms); security (TLS). Numerous pseudocode fragments that provide concrete examples of abstract concepts. Extensive support. The authors and MIT OpenCourseWare provide on-line, free of charge, open educational resources, including additional chapters, course syllabi, board layouts and slides, lecture videos, and an archive of lecture schedules, class assignments, and design projects.

The Definitive Guide to Django

An extensively revised edition of a mathematically rigorous yet accessible introduction to algorithms.

Lions' Commentary on UNIX 6th Edition with Source Code

This book constitutes the refereed proceedings of the 4th International Workshop on Experimental and Efficient Algorithms, WEA 2005, held in Santorini Island, Greece in May 2005. The 47 revised full papers and 7 revised short papers presented together with

extended abstracts of 3 invited talks were carefully reviewed and selected from 176 submissions. The book is devoted to the design, analysis, implementation, experimental evaluation, and engineering of efficient algorithms. Among the application areas addressed are most fields applying advanced algorithmic techniques, such as combinatorial optimization, approximation, graph theory, discrete mathematics, scheduling, searching, sorting, string matching, coding, networking, data mining, data analysis, etc.

Rethinking Public Key Infrastructures and Digital Certificates

Stefan Brands proposes cryptographic building blocks for the design of digital certificates that preserve privacy without sacrificing security. As paper-based communication and transaction mechanisms are replaced by automated ones, traditional forms of security such as photographs and handwritten signatures are becoming outdated. Most security experts believe that digital certificates offer the best technology for safeguarding electronic communications. They are already widely used for authenticating and encrypting email and software, and eventually will be built into any device or piece of software that must be able to communicate securely. There is a serious problem, however, with this unavoidable trend: unless drastic measures are taken, everyone will be forced to communicate via what will be the most pervasive electronic surveillance tool ever built. There will also be abundant opportunity for

misuse of digital certificates by hackers, unscrupulous employees, government agencies, financial institutions, insurance companies, and so on.In this book Stefan Brands proposes cryptographic building blocks for the design of digital certificates that preserve privacy without sacrificing security. Such certificates function in much the same way as cinema tickets or subway tokens: anyone can establish their validity and the data they specify, but no more than that. Furthermore, different actions by the same person cannot be linked. Certificate holders have control over what information is disclosed, and to whom. Subsets of the proposed cryptographic building blocks can be used in combination, allowing a cookbook approach to the design of public key infrastructures. Potential applications include electronic cash, electronic postage, digital rights management, pseudonyms for online chat rooms, health care information storage, electronic voting, and even electronic gambling.

Introduction to Computational Molecular Biology

Lattices are geometric objects that can be pictorially described as the set of intersection points of an infinite, regular n-dimensional grid. De spite their apparent simplicity, lattices hide a rich combinatorial struc ture, which has attracted the attention of great mathematicians over the last two centuries. Not surprisingly, lattices have found numerous ap plications in mathematics and computer science, ranging from number theory and Diophantine

approximation, to combinatorial optimization and cryptography. The study of lattices, specifically from a computational point of view, was marked by two major breakthroughs: the development of the LLL lattice reduction algorithm by Lenstra, Lenstra and Lovasz in the early 80's, and Ajtai's discovery of a connection between the worst-case and average-case hardness of certain lattice problems in the late 90's. The LLL algorithm, despite the relatively poor quality of the solution it gives in the worst case, allowed to devise polynomial time solutions to many classical problems in computer science. These include, solving integer programs in a fixed number of variables, factoring polynomials over the rationals, breaking knapsack based cryptosystems, and finding solutions to many other Diophantine and cryptanalysis problems.

Software-optimized Universal Hashing and Message Authentication

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.

Advances in Cryptology — CRYPTO '93

Issues for Dec. 1952- include section: Nachrichten der Österreichischen Mathematischen Gesellschaft.

Twenty Years Before the Blackboard

Now in its second edition, this book focuses on practical algorithms for mining data from even the largest datasets.

Experimental and Efficient Algorithms

Advanced Data Structures presents a comprehensive look at the ideas, analysis, and implementation details of data structures as a specialized topic in applied algorithms. This text examines efficient ways to realize query and update operations on sets of numbers, intervals, or strings by various data structures, including search trees, structures for sets

of intervals or piece-wise constant functions, orthogonal range search structures, heaps, union-find structures, dynamization and persistence of structures, structures for strings, and hash tables. Instead of relegating data structures to trivial material used to illustrate object-oriented programming methodology, this is the first volume to show data structures as a crucial algorithmic topic. Numerous code examples in C and more than 500 references make Advanced Data Structures an indispensable text.

The Power of Habit: by Charles Duhigg | Summary & Analysis

This book constitutes the refereed proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2003, held in Taipei, Taiwan in November/December 2003.The 32 revised full papers presented together with one invited paper were carefully reviewed and selected from 188 submissions. The papers are organized in topical sections on public key cryptography, number theory, efficient implementations, key management and protocols, hash functions, group signatures, block cyphers, broadcast and multicast, foundations and complexity theory, and digital signatures.

Selected Areas in Cryptography

This textbook teaches introductory data structures.

Advances in Cryptology — CRYPTO '96

Detailed summary and analysis of The Power of Habit.

Principles of Computer System Design

For the past 20 years, UNIX insiders have cherished and zealously guarded pirated photocopies of this manuscript, a "hacker trophy" of sorts. Now legal (and legible) copies are available. An international "who's who" of UNIX wizards, including Dennis Ritchie, have contributed essays extolling the merits and importance of this underground classic.

Mathematical Writing

Essential Information about Algorithms and Data Structures A Classic Reference The latest version of Sedgewick, s best-selling series, reflecting an indispensable body of knowledge developed over the past several decades. Broad Coverage Full treatment of data structures and algorithms for sorting, searching, graph processing, and string processing, including fifty algorithms every programmer should know. See

Structure and Interpretation of Computer Programs - 2nd Edition

This book will help those wishing to teach a course in technical writing, or who wish to write themselves.

Introduction To Algorithms

Introduction to Information Retrieval

This book constitutes the thoroughly refereed postproceedings of the 10th Annual International Workshop on Selected Areas in Cryptography, SAC 2003, held in Ottawa, Canada, in August 2003. The 25 revised full papers presented were carefully selected from 85 submissions during two rounds of reviewing and improvement. The papers are organized in topical sections on elliptic and hyperelliptic curves, side channel attacks, security protocols and applications, cryptanalysis, cryptographic primitives, stream ciphers, and efficient implementations.

Algorithm Design

The CRYPTO ’93 conference was sponsored by the International Association for Cryptologic Research (IACR) and Bell-Northern Research (a subsidiary of Northern Telecom), in co-operation with the IEEE Computer Society Technical Committee. It took place at the University of California, Santa Barbara, from August 22-26, 1993. This was the thirteenth annual CRYPTO conference, all of which have been held at UCSB. The conference was very enjoyable and ran very of the General Chair, Paul Van Oorschot. smoothly, largely due to the efforts It was a pleasure working with Paul throughout the months leading up to the conference. There were 136 submitted papers which were considered by the Program Committee. Of these, 38 were selected for presentation at the conference. There was also one invited talk at the

conference, presented by Miles Smid, the title of which was “A Status Report On the Federal Government Key Escrow System.” The conference also included the customary Rump Session, which was presided over by Whit Diffie in his usual inimitable fashion. Thanks again to Whit for organizing and running the Rump session. This year, the Rump Session included an interesting and lively panel discussion on issues pertaining to key escrowing. Those taking part were W. Diffie, J. Gilmore, S. Goldwasser, M. Hellman, A. Herzberg, S. Micali, R. Rueppel, G. Simmons and D. Weitzner.

Principles of Model Checking

This book is the legacy of twenty years of mathematics teaching: part philosophy, part humour, and completely fascinating.

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION