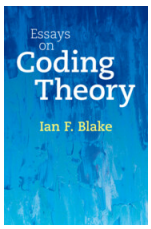
Review of [1,2]



Essays on Coding Theory
by **Ian F. Blake**

Cambridge University Press, 2024
Hardback $69.99, eBook $69.99, 474 pages

Review by **Rutuja Kshirsagar** and **Gretchen L. Matthews**

1 Overview

Coding theory, a branch of mathematics and theoretical computer science, focuses on the efficient sharing and storage of information. Since its inception in 1948, the field has made significant strides and now finds applications across various domains, including communications, data storage, cryptography, and security. The core challenges in coding theory can be broadly categorized into three main areas: 1. How to efficiently encode information or data; 2. How to transmit or share this encoded data; and 3. How to decode the received data to accurately retrieve the original information.

Ian F. Blake's book *Essays on Coding Theory* provides an in-depth review of various topics within the field. Aimed at graduate students and early-career researchers, the book is designed to help readers grasp the fundamentals of modern coding theory - topics that do not appear in more standard texts. Although it assumes a foundational understanding of algebraic coding and information theory, important definitions and terminologies are introduced either in the introductory chapter or at the start of each chapter as needed. The author has made a commendable effort to maintain consistent notation throughout the book, enhancing readability. The explanations are clear, and while some proofs are not presented in full detail, the author effectively guides readers through the proof strategies. The primary goal of the book is to acquaint readers with research in different areas of coding

[2]Another review of this text by the same authors appears in the American Mathematical Monthly, published online: 7 Oct 2024.

theory, rather than presenting the most current advancements. Nevertheless, the book includes references to more recent publications and resources for those interested in further exploration.

2 Book Summary

The book is organized in the following way:

- **Chapter 1 and 2** address fundamental concepts such as finite fields, error correction, and erasure recovery. These foundational topics are crucial for building a robust understanding of the more advanced ideas presented throughout the book. By thoroughly explaining these core principles, the author ensures that readers are well-prepared to grasp the subsequent, more complex theories and applications discussed in the later chapters.

- **Chapter 3** focuses extensively on low-density parity-check (LDPC) codes, a class of error-correcting codes first introduced by Gallager. LDPC codes are renowned for their remarkable error-correcting performance and efficiency, which make them invaluable across a range of applications, including the advancement of flash memory technologies. The chapter not only explores the foundational concepts established by Gallager but also covers subsequent developments and refinements in LDPC codes. These advancements include improvements in decoding algorithms, optimization techniques, and novel applications that have further enhanced the practicality and performance of LDPC codes in modern communication systems.

- **Chapter 4** explores polar codes, a class of error-correcting codes introduced by Arikan in 2008. These codes are particularly significant for their role in the development of 5G networks. Polar codes are distinguished by their advanced error-correcting capabilities, which play a crucial role in ensuring the efficient and reliable transmission of data in modern communication systems. The chapter provides the theoretical foundations of polar codes and their construction principles.

- **Chapter 5-10** details the concepts of locality and distributed storage, highlighting the importance of efficiently recovering and managing data. The chapters examine various families of codes that leverage the principle of accessing a small subset of code symbols to correct errors

or retrieve missing information. Key code families covered include locally recoverable codes, locally decodable codes, regenerating codes, network codes, and batch codes, among others.

Each of these code families employs innovative techniques to enhance data reliability and accessibility, which are crucial for modern distributed storage systems. Locally recoverable codes, for instance, allow for the recovery of lost or corrupted data by accessing only a small number of other code symbols. Locally decodable codes enable the retrieval of specific data bits without needing to decode the entire dataset, while regenerating codes focus on optimizing the repair of lost data. Network codes and batch codes further contribute to efficient data management and error correction across distributed systems.

Chapter 9 addresses private information retrieval (PIR) and PIR storage. The central concept remains the efficient access to localized information, but with an added dimension of privacy. In PIR, the retrieval of information is conducted in such a way that the server from which the data is downloaded remains unaware of the specific information being accessed. This ensures that the retrieval process is not only efficient but also preserves user privacy by concealing the nature of the data request from the server.

Overall, these chapters provide a comprehensive overview of how these advanced coding techniques are applied to improve data recovery and storage in distributed systems, showcasing their significant role in advancing modern information technology.

- **Chapter 11** introduces graph-based codes, including Tanner codes developed by Tanner and expander codes created by Sipser and Spielman. Expander graphs, particularly Ramanujan graphs, are notable for their strong connectivity and sparsity. These properties enable the development of codes with efficient encoding and decoding algorithms.

- **Chapter 12** explores coding methods that extend beyond traditional codes defined over finite fields with distance measured by the Hamming metric. It examines rank-metric codes, initially introduced by Delsarte, where the distance between codewords is defined by the rank of a matrix rather than by Hamming weight. Additionally, the chapter covers subspace codes, where codewords are subspaces of a vector space, and the distance is defined by a relevant metric on these subspaces. The chapter primarily focuses on developing and analyzing these advanced coding concepts.

- **Chapter 13** describes list decoding algorithms developed by Sudan and Guruswami. In contrast to traditional decoding methods that produce a single decoded result, list decoding algorithms provide a list of possible solutions. The chapter covers a range of list decoding techniques and their practical applications, highlighting how they enhance error correction. Furthermore, it explores the influence of list decoding on the design of capacity-approaching codes, demonstrating how these techniques contribute to developing codes that approach the theoretical limits of channel capacity.

- **Chapter 14** focuses on methods for generating sequences with specific desirable properties. These specialized sequences are instrumental in the development of codes used in various applications, including communication systems, mobile phones, and space technologies. The chapter reviews techniques for constructing these sequences and examines their significance in enhancing the performance and reliability of coding schemes across different fields.

- **Chapter 15 and 16** represent a gradual shift from coding theory to the realm of cryptography and quantum computing. They introduce key concepts in cryptography, with a particular focus on various schemes from post-quantum cryptography, highlighting their relevance in the context of emerging quantum computing technologies.

  These chapters provide an overview of the fundamental principles of quantum computation, explaining why quantum computing poses challenges for traditional cryptographic methods. They also cover essential concepts in quantum error correction (QEC), outlining the fundamental principles and the role of QEC codes in correcting errors in quantum systems.

  While the chapters introduce some small QEC codes to illustrate these concepts, they do not delve deeply into a broad range of QEC codes. Instead, they offer a foundational understanding of quantum error correction, setting the stage for readers to appreciate the interplay between quantum computing and cryptographic security without overwhelming them with excessive technical details.

- **Chapter 17** explores additional types of codes, including balanced codes and permutation codes, among others. This diverse coverage ensures a comprehensive conclusion to the book, rounding out the discussion with a broad overview of various coding techniques. By

including these additional code families, the chapter effectively wraps up the book, providing readers with a well-rounded understanding of the field.

- **Appendices** provide essential background on algebraic concepts that are crucial for understanding the material presented in the book. They cover finite geometries, linearized polynomials, Gaussian coefficients, Hasse derivatives, and the zeros of multivariate polynomials. These topics are fundamental for grasping the more advanced concepts discussed throughout the text.

3 Opinion and Conclusions

Blake's book is truly commendable and deserves high praise. We highly recommend it to anyone interested in modern coding theory, as it covers a broad range of current topics with reasonable depth and clarity. This book would be particularly valuable for professors teaching graduate or specialized courses on coding theory, providing a solid foundation and extensive resources for both teaching and further study. The book remains an excellent resource and a highly engaging read. Its comprehensive coverage and clear explanations make it a significant contribution to the field, and it will undoubtedly be a valuable asset for both students and educators alike. In summary, Blake's work stands out as a pivotal text that not only enhances understanding but also fosters a deeper appreciation for the complexities and innovations in coding theory.