Review of the book

Protecting Information: From Classical Error Correction to Quantum Cryptography

by Susan Loepp and William Wootters

Cambridge University Press, 2006

ISBN: 978-0-52153-476-3

Fan Junjie, Bertrand
National University of Singapore

29 March 2012

1 Overview of Book

This book provides an elementary introduction to the basics of error correction and quantum cryptography. Suitable for upper-level undergraduates in mathematics, physics and computer science, this book is unusual amongst undergraduate texts on coding or cryptography in that it includes quantum physics and the emerging technology of quantum information. It is self-contained, providing students with a diverse exposure to the theory and applications of groups, finite fields as well as quantum physics. Numerous exercises are sprinkled throughout the text to aid the diligent student in better understanding concepts introduced in the text.

2 Book Summary

The first chapter is a quick but clear survey of elementary topics in cryptography. It begins with discussions of elementary ciphers as well as the Enigma cipher used during World War II. Then after a brief review of modular arithmetic, it introduces the Hill cipher and cryptanalytic techniques employed on the Hill Cipher. It then defines Feistel ciphers, and briefly covers the DES and AES algorithms. It ends with discussions on public key exchanges, using ideas from group and elliptic curve theory. This chapter is self-contained, allowing students without any knowledge in cryptosystems to quickly grasp the basics of cryptography.

Chapter 2 is an informal discussion on the basics of quantum mechanics, aimed at preparing the reader to understand the later chapters on quantum computation and basic quantum error correction. It starts with a clear discussion on photon polarization, including linear polarization, circular and elliptical polarization. This discussion is based on imagining simple photon polarization experiments. It then talks about general quantum variables and composite quantum variables. It ends with briefly discussing measuring subsystems and other incomplete measurements. This chapter succeeded in providing just enough background for the later chapters. The interested student wanting a more formal understanding in the basics of quantum mechanics may want to consult the references listed.

Chapter 3 discusses quantum cryptography using the basics developed in the previous chapter. It starts with an explanation of the Bennett-Brassard protocol, one of the most

widely studied quantum strategies for quantum key distribution. This discussion is followed by a survey of the no-cloning theorem and quantum teleportation. Here, the basic formalism of teleportation is briefly covered and the interested reader may want to consult the references listed in the footnotes to gain better understanding of recent teleportation experiments.

Chapter 4 takes a break from quantum mechanics and gives an introduction to classical error-correcting codes. This discussion is aimed at providing enough background to better understand the full protocol for quantum key distribution. This chapter is entirely self-contained, starting from a few mathematical preliminaries and examples. Using these preliminaries, it then launches into a discussion of hamming distance and linear codes. It continues with clear explanations of generator matrices, dual codes and syndrome decoding, and finally cumulates with a discussion of the hat problem. This chapter provides sufficient background on error-correcting codes for students to read more advanced texts, some of which are listed in the footnotes at the beginning of the chapter.

Chapter 5 returns to quantum cryptography. The first part uses the material of the previous chapter and discusses the application of error correction in quantum key distribution. It then provides an introduction to privacy amplification and explains how it can be used to improve the security of a quantum key distribution channel.

Chapter 6 provides an introduction to generalized Reed-Solomon or GRS codes. This chapter uses material on finite fields and modular arithmetic covered in chapter 1. It begins with a few definitions of concepts leading to the definition of the generalized Reed-Solomon codes. It then discusses briefly a particular finite field with 8 elements used in such codes. It then briefly covers a particular generator matrix for a GRS code, ending with introducing the concept of the dual of a GRS code.

The final chapter offers a compact introduction to quantum computing. It starts with a discussion of quantum gates and the Deutsch algorithm. It then provides some number theoretic background for Shor's factoring algorithm before explaining the algorithm in detail, including its probability of success and its efficiency. The book ends with a brief introduction to quantum error correction, touching on an X and a Z-correcting code, as well as the Shor code.

3 Reviewer's Comments

This book offers a good self-contained introduction to quantum cryptography and error correcting codes. This reviewers finds the writing is clear, engaging and of high quality. Although it is not comprehensive (it does not claim to be), in particular not covering the theory of information and entropy, the reader following this book would have no problems gaining a good overview of quantum information theory and would be ready to read more advanced texts on these topics, some of which are listed in footnotes in the relevant chapters.

Another plus point of this book is its abundance of exercises sprinkled throughout the text. This allows the diligent student to better understand the many concepts introduced.

A minor inconvenience is that some chapters, in particular chapter 2, are designed only to provide sufficient background for later chapters, and may lack in formalism and rigor needed for a full understanding of the subject matter. In these cases, the interested reader may have to consult the references listed to gain a better understanding of the material.

4 Reviewer's Recommendation

I recommend this book to advanced undergraduates in mathematics, physics and computer science interested in an introduction to quantum cryptography and error correction.

The reviewer is a math graduate student at the National University of Singapore