Review of the book

"Codes: An Introduction to Information, Communication and Cryptography"

by Norman L. Biggs

Springer, 2008

ISBN: 978-1-84800-273-9

M. Frederic Ezerman
CRRG Nanyang Technological University, Singapore

September 2011

1 Summary of the review

There are many introductory or first course coding theory textbooks available. A good number of these textbooks either concentrate on algebraic coding theory or putting coding theory in the context of information theory. Most first course textbooks in cryptology focus on algorithms and techniques in fulfilling the security conditions that cryptographic protocols need to satisfy.

Biggs tried to put information theory, coding theory and cryptology together in this introductory textbook. The positive side is that each subject is well-motivated and the transition from one to the other feels smooth. The book is self-contained and can be used flexibly. The trade-off is that the treatment covers only the very basic materials in those three interconnected subjects. Beginners with appetite for more coverage and depth in only one or two of the subjects would most likely be left wanting for more.

2 Summary of the book

Chapter 1 sets the author's agenda of showing how codes play important roles in processing information in economic, reliable, and secure ways. After that, the book can be divided into roughly three parts.

Chapters 2 to 4 highlight the economy aspects of coding. Concepts such as source, entropy, uncertainty, and information are introduced. Properties that good codes must satisfy to minimize resources needed such as unique decodability and optimality are then treated. Data compression and its algorithms are used to demonstrate the power of properly designed codes in keeping resource requirement low.

Chapters 5 to 9 discuss noisy communication channels, their information carrying capacity, and Shannon's theorem on error-correction over noisy channel. Naturally, some constructions of practical codes reaching some level of protections while keeping transmission rates reasonably high are presented. Due to the text's introductory nature, only linear codes of mostly cyclic constructions are detailed.

Chapters 10 to 15 discuss cryptography. Starting from the simplest substitution cipher and the frequency analysis attack on it, the treatment covers symmetric key encryption standards as well as the public key crypto system as illustrated mainly by the RSA system. Perhaps the most technical part of this book is the last chapter which discusses Elliptic Curves cryptography.

Overall, Biggs has given us an inviting first course textbook which hopefully whets the students' appetite to go deeper and wider into the wonderful world of codes.

3 What is the book like (style)?

This book introduces the recurring themes in coding, namely economy, reliability, and security in an integrated and even-paced way. The motivation and practical concerns behind the development of the theory under consideration are usually presented concisely and clearly, which is nice for a first course textbook. I find the exposition on the Kraft-McMillan number and its connection to uniquely decodable codes particularly nice.

In many places the language is quite informal and sometimes proofs are postponed until a later part of the (sub)chapter so as not to disrupt the flow of the argument. There are exercises after every subchapter which are helpful.

This text assumes close to nothing in terms of mathematical background. Necessary concepts from elementary abstract algebra and number theory are provided just before they are used in the discussion.

In general, the text is engaging and friendly.

4 Would you recommend this book?

I would recommend the book to the following audience:

① Beginning students intending to work mostly on the more applied part of coding theory in their future career.

② Future or present policy makers seeking more clarity on the significance of and possible contribution of codes in practical matters.

③ General audience interested in gaining better knowledge on the inner workings of codes.

5 Some Suggestions and Errata

First, some suggestions for possible future edition(s):

① It would be nice to have a short Chapter 0 or an appendix collecting elementary mathematical concepts from basic algebra (group, polynomial rings, finite fields, etc.) and number theory (modular arithmetic, fundamental theorem of arithmetic etc.) which are used in the text for easy reference rather than scattering them in an *just in time* fashion throughout the book.

② The concept of *erasure correction* can be an interesting addition to *error correction* in Ch. 6 since erasure is a significant problem in reliable communication.

③ In Ch. 6 Sect. 3 the alternative of *requesting rebroadcasting* can also be mentioned in addition to the options listed in the paragraph after the proof of Th. 6.13.

The errata list below is in no way exhaustive.

① Ch. 5 p. 73, the line after Figure 5.1 delete *by* after *we shall*.

② Example 8.4 p. 125, 3rd line of the solution delete *is* after *codewords are*.

③ Page 128, the equation after the line beginning with *The variables ...*, middle part should be $x_2 + x_3 + x_5 = 0$.

④ Exercise 9.3 on p. 144, first line, double *the*, remove one of them.

⑤ Section 9.2, first two lines, double *of the*, remove one of them.

⑥ Example 9.7 has a wrong solution. The correct one is $x^4 + x^5$.

⑦ Page 227, last paragraph, line 2, the pair should be (π_A, σ_A).

The reviewer recently completed a Ph.D. in Mathematics at Nanyang Technological University Singapore.