Review of the book

"Applied Algebra - Codes, Ciphers, And Discrete Algorithms" by Darel W. Hardy, Fred Richman, and Carol L. Walker

CRC Press, Taylor & Francis Group, 2009

ISBN: 978-1-4200-7142-9

Julia Borghoff
DTU Mathematics, Technical University of Denmark

1 What the book is about

In Chapter 1 (Integers and Computer Algebra) the basics of integers and primes, binomial coefficients etc as well as the concept of induction for mathematical proofs are introduced.

Chapter 2 (Codes) gives several examples of basic codes such as binary or hexadecimal representation of numbers, the well known ASCII code, Braille code (which enables blind people to read), the Morse code, the Two-out-of-Five Code and the Hollerith Code. The latter was used to store for example FORTRAN code on punched cards. This cards are also known as IBM cards. For all codes in this chapter tables are given in which we find the encoding of the whole alphabet and/or of the digits 0 to 9.

The main topic of Chapter 3 (Euclidean Algorithm) is modular arithmetic. The mod function, the greatest common divisor (gcd) as well as the Euclidean and the extended Euclidean algorithm which calculate the gcd are introduced together with all necessary definitions and theorems (including proofs). Finally the Fundamental Theorem of Arithmetic is stated and inversion modulo n is explained. For all algorithms pseudo codes are given which are additionally illustrated by a couple of examples.

In Chapter 4 (Ciphers) the meaning of the word "cryptography" is explained followed by some very classical and simple examples of ciphers such as the *Caesar* cipher and the *Vigenere* Cipher. Afterwards the slightly more general concept of affine cipher and polyalphabetic cipher is explained. Here the order seems not to be optimal because Caesar and Vigenere are special examples of the latter. In the next subsection frequency analysis is used in order to break the simple cipher introduced in the previous section. However, the name of the section (Cryptanalysis) is misleading because only frequency analysis is mentioned and frequency analysis is not a threat to modern ciphers. The next section explains basic substitution and permutation ciphers. Unfortunately the book fails in making a connection between these simple ciphers and the more complex substitution-permutation networks which are often used in block cipher design. The section in the book about block ciphers is disappointing and does not have much to do with modern block ciphers.
The chapter concludes with three examples for ciphers which have been used. The *Playfair* cipher, the unbreakable cipher, which is better known as *one-time pad*, and the *Enigma*. The chapter does not cover more than an introductory lecture in basic cryptography.

Chapter 5 (Error-Control Codes) focuses, after defining the Hamming weight and distance, on different bar codes. Although these bar codes are very interesting I wish the authors would focus more on Hamming codes. Merely the (7,4) Hamming code is given as an example but the section lacks generalization.

Chapter 6 (Chinese Remainder Theorem) introduces the Chinese Remainder Theorem motivated by the problem of solving a system of linear equations modulo n. The Chinese Remainder Theorem is an important tool in public key cryptography. Some applications of the Chinese Remainder Theorem are given in this chapter such as extended precision arithmetic which makes large integer arithmetic easy, the greatest common divisor of polynomials and the inversion of the Hilbert matrix. For large n the determinant of the Hilbert matrix is close to zero which makes it often impossible to calculate its correct inverse using floating point arithmetic. This problem can be solved using the Chinese Remainder Theorem as illustrated in the book.

Chapter 7 (Theorems of Fermat and Euler) deals with number theoretical results which are important for cryptography. Starting with the fact that 1 only has the trivial square roots 1 and -1 modulo a prime, Wilson's Theorem is proven. Fermat's Little Theorem which says that $a^{p-1} \equiv 1 \mod p$ if a and p co-prime and p prime is stated and the Square-and-Multiply algorithm for efficient calculation of a power is explained. An application of Fermat's Little Theorem as primality test is given, furthermore the ideas of the more reliable Rabin's probabilistic primality test are developed. As an additional application of Fermat's Little Theorem exponential ciphers are introduced. In the last section a reduced residue system and the Euler totient function are defined. The chapter concludes with Euler's Theorem.

Chapter 8 (Public Key Ciphers) deals not only with Public Key Ciphers as RSA and the Knapsack cipher but also more general with public key cryptographic algorithms. RSA signatures are used as an example to explain the concept of electronic signatures. An example how you could use electronic signatures and public encryption in a message exchange system is given and the Digital Signature Algorithm is stated. Also the Secure Hash Algorithm (SHA) is mentioned but not explained in detail.

In Chapter 9 (Finite Fields) Galois Fields are introduced. After the general definition of a field, the simplest construction of a finite field is given, the integers modulo a prime p together with addition and multiplication. Followed by the definition of a ring and the polynomial ring over a finite field GF(p). Then the authors explain how to construct fields which number of elements is a prime power. The concrete constructions of the fields GF(4), GF(8) and GF(16) are shown before this is generalized to the construction of the field GF(p^n). Of special interested is the multiplicative group of a finite field. Properties of this group are discussed in Section 9.6. Finally it is discussed how to use powers of an element modulo a prime as a random number generator.

Chapter 10 (Error Correcting Codes) gives a small inside into the concept of error correcting codes by explaining encoding and decoding of BCH codes and Reed-Solomon codes which can be seen as a special case of BCH-codes. Remember that we have seen Hamming codes as another example for error correcting codes in Chapter 5.

In Chapter 11 (Advanced Encryption Standard) at first a short but incomplete description of the the Data Encryption Standard is given. This is followed by the construction of the Galois field GF(256) over which the AES mainly operates. Afterwards the basic steps of an AES-round are explained as well as the key expansion. Here we just find a plain description of the algorithm, a cryptanalysis or discussion of design properties is missing.

Chapter 12 (Polynomial Algorithms and Fast Fourier Transforms) deals mainly with polynomial interpolation. The Lagrange interpolation and Neville's iterated interpolation algorithm are explained as well as Kronecker algorithm for finding a divisor of a polynomial of certain degree. Polynomial interpolation is used in multiparty protocols.
The chapter closes with the Fast Fourier Transformation which transforms coefficients of a polynomial into function values and the reverse function, the Fast Fourier Interpolation, which goes from function values to coefficients.

The book supports learning by doing. In each section we can find many examples which clarify the mathematics introduced in the section and each section is followed by a series of exercises of which approximately half are solved in the end of the book. Additional the book comes with a CD-ROM containing an interactive version of the book powered by the computer algebra system *Scientific Notebook*.

2 What is this book about (summary)?

The book introduces algebraical concepts which are used in cryptography and coding and shows their applications in these fields as the title already says. First and foremost we have to say that the book deals with three large topics which are algebra, cryptography and coding. Therefore the book can only give a small insight into these fields. Algebraical basics such as finite fields, the Euclidean algorithm, the Chinese Remainder Theorem, Fermat's little Theorem and Euler Theorem are covered. Public and symmetric cryptography is discussed. Amongst others the two best known ciphers -RSA for the public key encryption and AES for the symmetric encryption- are explained. Unfortunately an analysis of those is outside the scope of the book. The Coding part of the book is subdivided into Error Control and Error Correcting codes. In the Error Control Codes part are mainly different kinds of bar codes discussed, while the Error Correcting Codes Chapter focuses on BCH-codes.

For me the most interesting sections of the book are the section about error control codes which are currently in use such as bar codes and the section about the Enigma machine.

It is important to mention that the mathematics in the book are developed as needed and the focus of the book lies clearly on learning by examples and exercises. Each section ends with a series of exercises and the solution of all odd exercises is given in the back of the book. Furthermore comes the book with an interactive version of it that is powered but the computer algebra system *Scientific Notebook*.

3 What is the book like (style)?

All mathematics in the book are developed when needed and clarified by a couple of examples. Although this makes it easy to read the book from the first to the last page, the book is quite useless as a handbook because sometimes generalizations and clear definitions are missing and some of the mathematics appears in later chapters instead of in the chapters where I would expect it.

The book is divided in short chapters and even shorter sections which are followed by a series of exercise. This shows that the book is an outcome of a course. The content of the book is basic algebra, cryptography and coding. As mentioned the chapters are rather short so in my opinion often just the surface of a topic is scratched. However, the book gives a good insight how algebra can be used in coding and cryptography but is of course far away from being complete.

4 Would you recommend this book?

This book might be interesting for computer science students with a not too strong algebraical background and no knowledge about cryptography and/or coding. As the authors mention the mathematics needed is developed along the way as needed starting at the very basics. The strength of the book is clearly the number of examples which on the other side in some case unfortunately leads to a lack of general definitions and theorems. Therefore this book is suitable for student who prefer learning by doing (the book provides many exercise) but have some difficulties with formal mathematical definitions and theorems.

I do not recommend the book for mathematics student or students which already have a good mathematical background or a strong background in cryptography or coding. For these student large parts of the content will be known already.

Because of the lack of generalizations and definition and the fact that some topic are not in the chapter I would expect them, the book is not suitable as a handbook.

Please consider while reading the recommendation that I am a mathematician with computer science as minor. Therefore my opinion might differ from the one of computer scientist or engineers especially concerning the mathematical content of the book.

The reviewer is a Ph.D. student in Symmetric Cryptology at the Department of Mathematics at the Technical University of Denmark