ERROR DETECTING CODES

General Theory And Their Application In Feedback Communication Systems

Torleiv KLØVE
Department of Informatics, University of Bergen
Bergen, Norway

Valery I. KORZHIK
St. Petersburg University of Telecommunications
St. Petersburg, Russia

KLUWER ACADEMIC PUBLISHERS
Boston/London/Dordrecht

CONTENTS

PREFACE

There are two basic methods of error control for communication, both involve coding of the messages. The differences lay in the way the codes are utilized. The codes used are block codes, which are the ones treated in this book, or convolutional codes. In most cases the block codes used are linear codes. With forward error correction, the codes are used to detect and correct errors. In a repeat request system, the codes are used to detect errors, and, if there are errors, request a retransmission.

Usually it is a much more complex task to correct errors than merely detect them. To detect errors has the same complexity as encoding, which is usually linear in the length of the codewords. Optimal error correcting decoding is in general an NP-hard problem, and efficient decoding algorithms are known only for some classes of codes. This has generated much research into finding new classes of codes with efficient decoding as well as new decoding algorithms for known classes of codes.

There are a number of books on error control, some are listed at the beginning of the bibliography at the end of this book. The main theme of these books is error correcting codes. Error detection tends to be looked upon as trivial and is covered in a few pages at most. What is then the reason behind the following book which is totally devoted to error detecting codes? The reason is, on the one hand, that error detection combined with repeat requests is the most widely used method of error control, and on the other hand, that the analysis of the reliability of the information transmission system with error detection is usually quite complex. Moreover, the methods of analysis are often not sufficiently known and simple rules of the thump are used instead.

Integrity of data is very important in modern communication systems. A significant property of error detecting codes is that they can, in contrast to forward error correcting codes, guarantee a required reliability of message transmission over any channel.

There are many papers devoted to the problem of the error detecting capability of a linear code, as well as for the binary symmetric channel as for other channels, with or without memory. They are spread over many journals and conference proceedings. The goal of this book has been to collect all these results and present them in a unified and clear form. We have also included a number of new results of our own, which have not been published before.

The book starts in Chapter 1 with a survey of the main channels models and in Chapter 2 we give a short introduction to the theory of block codes, with emphasis on the parts important for error detection. The weight distribution is particularly important for this application, and is treated in more detail than in most books on error correction.

In Chapter 3 we give a detailed account of the known results on the probability of undetected error on the important binary symmetric channel. Combined detection and correcting is also briefly mentioned, from the error detection point of view; decoding algorithms are not given. For the benefit of a reader who is mainly interested in how the various results may be utilized in search for an error detecting code for a particular application, we give a short guide, in Section 3.11, to help in such a search.

In Chapter 4 we discuss briefly error detection on some other channels, in particular the Z-channel and channels with memory. Further we give a description of the method of channel transforms which allow us to obtain high reliability even for trivial codes. This method can be used also on the BSC as a substitute, it will (at a cost) remove the need of "good" error detecting codes.

Error detecting codes are used in so-called automatic repeat request (ARQ) systems. In Chapter 5 we give an overview over the main ARQ protocols. To describe all such protocols would be beyond the scope of this book. We have concentrated on the main protocols in use and those which in our view are most promising for use in future systems. We have given a short description of a number of protocols in the comments at the end of the chapter. In Chapter 6 we discuss the optimal choice of codes for the various ARQ protocols.

Finally, we give a bibliography of papers on error detection and related subjects. When we have had a choice, we have given references to books and papers in English, but also a number of significant papers in Russian containing results, not found in English translation, are included.

Each chapter includes a list of comments and references.

The required background for the reader of this book is some basic knowledge of coding theory (typically an introductory university course on "coding theory" or "statistical communication theory") and some basic mathematical knowledge: algebra (matrices, groups, finite fields, vector spaces, polynomials) and probability theory (random events and variables, distribution functions, Markov chains).

Parts of material in the book has been tested in graduate courses in Norway and Russia.

The various parts of the book are of course written by the two authors based on their expertize. Chapters 1, 4.2, 4.3, 5, and 6 are mainly due to Korzhik, and chapters 2,3 and 4.1 to Kløve. The reader will also recognize this in each authors individual style.

We hope that this book will be useful, both for coding theorists and mathematicians interested in error detection and for engineers employed with design of telecommunication systems, in particular with ARQ protocols. The probability of undetected error of linear codes has also found useful applications in frame synchronization, in the wire-tap channel, and in signature analysis for circuit testing. The book can also be used as a text book for a graduate course on error detection.

We thank Dr. V. Nikitin and Dr. P. Malev for doing the computations for some of the example and tables in Chapters 5 and 6, and also Dr. B. Kudryashov for useful discussion of his results on the FPMC model. Further, we thank a number of colleagues and students who have read and commented on parts of the manuscript for this book.

Bergen/St. Petersburg