Preface

Error correcting codes represent a widely applied technique for assuring reliable electronic communications and data recording. Although often some codes are introduced without the need for a polynomial approach, the attempt to provide a description where polynomial theory is however present could be of some interest. The intent of this book is to develop such theory, in a unitary way, trying to find several conceptual bridges between different classes of codes (block, convolutional, concatenated,…). This goal requires the introduction of some rather unusual mathematical tools (like interleaved polynomial multiplication or interleaved polynomial division), able to support it. Also some structural transformations, like modified code lengthening or modified H-extension, are needed in order to construct a coherent model, able to support noticeable new interpretations.

The introduction of quasi-cyclic codes as a true generalization of the concept of cyclic codes is only an example of the fruitful use of such mathematical tools and geometrical transformations. They are also important for giving an intuitive justification for the encoder circuits to be adopted. State diagrams, constructed on these encoder circuits, contribute to give a better understanding of the properties characterizing the codes under study, besides the measure of the decoding computational complexity.

The distinction between well-designed and not well-designed convolutional codes represents another innovative concept. The latter family of codes is equivalent to catastrophic convolutional codes, but since they are systematic, the catastrophic behavior is no longer a problem. On the other hand, a more than linear increase in the number of low-weight code frames with the number of frame periods remains a drawback for not well-designed convolutional codes, together with some difficulties in their parity check matrix determination and tail-biting arrangement organization. Direct product codes between a pair of block codes are demonstrated to be a subset of not well-designed convolutional codes. Some further conceptual (and rather surprising) bridges between block codes and convolutional codes are constructed.

The treatment is organized maintaining distinct the approaches based on the generator matrix and on the parity check matrix. The reader is gradually guided to the interpretation of such viewpoints. Some concepts, deriving from dual properties, will appear in all their strong efficacy only at this moment. Modified lengthening of cyclic codes and modified H-extension of cyclic codes are dual opportunities leading to a new comprehension of the intrinsic nature of convolutional codes. The former is obtained by acting on the generator matrix, and the latter on the parity check matrix. The same can be made for quasi-cyclic codes. Proper transformation of control symbols into information symbols and vice versa supports the above modifications.

Modern coding (mainly regarding turbo codes and LDPC codes) is a topic, which is faced after a wide application of the above innovative concepts, so allowing a comprehensive understanding of the structures characterizing such codes. For instance, modified H-extension of quasi-cyclic codes offers the possibility of setting up a sort of doubly convolutional LDPC code, in turn interpreted in relation to proper turbo product schemes. The introduction of BPG codes (Binomial Product Generator codes) allows to treat array LDPC codes and some forms of concatenated LDPC codes, together with their convolutional versions, not only by means of the parity check matrix.

The continuous search for ultimate extremely good performance, present in the recent literature, has the consequence of reducing attention to the above theoretic aspects. The dominant use of computer simulations and optimization procedures often entails a nonexhaustive investigation of the true geometrical nature of the code under study. Many code families, apparently very different, on more careful analysis, would appear instead strictly related. All these considerations may produce interesting future theoretical developments. To this purpose, the present comprehensive approach would give a possible contribution.

About 250 Definitions, 300 propositions (Theorems, Corollaries, Lemmas), nearly 500 examples, highly interconnected, can give an idea of the amount of contents treated. In four Appendices some useful concepts, not strictly related to the topics under development, are collected. They are devoted to nonskilled readers, who need auxiliary assistance for framing such theory in a proper context.

Acknowledgments

I wish to thank Marco Baldi for fruitful discussions and continuous help in obtaining most part of the numerical computations, Franco Chiaraluce for his hints and theoretical support, Andrea Carassai for some intuitive views, my students at the Polytechnic University of Marche for their contribution in the organization of some material, and finally Laura Fonti for typewriting help and figure assembling. A particular acknowledgment is devoted to Marco Chiani for having reviewed part of the content, when it was under development. I am also indebted to Rossano Marchesani, Roberto Garello, Torleiv Klove, for our collaboration during the long research activity at the basis of the present work.

http://www.springer.com/978-3-319-01726-6

Polynomial Theory of Error Correcting Codes
Cancellieri, G.
2015, XVIII, 732 p. 320 illus., Hardcover
ISBN: 978-3-319-01726-6