# Book Reviews

**Theory and Practice of Error Control Codes,** R. E. Blahut (Reading, MA: Addison-Wesley, 1983, xi + 500 pp., $40.00).

JAMES L. MASSEY, FELLOW, IEEE

The 85 percent of this book that deals with block codes is always solid, and frequently creative enough to merit the description revolutionary. The 15 percent that deals with convolutional codes and with the connection between coding and modulation is, by contrast, shaky and sometimes inept.

The revolutionary core of this book is the spectral theory of cyclic codes that occupies Chapters 8–11 and part of Chapter 13—a full third of the book. Much of this material is entirely new and all of it must be read and understood by any serious future researcher in algebraic coding theory. It establishes the discrete Fourier transform (DFT) as the central tool in the study of cyclic codes. Although the relation of the DFT to cyclic codes was earlier recognized in varying degrees of explicitness by Reed and Solomon, Mattson and Solomon, Gore, Chien and Choy, and Lempel and Winograd, it is fair to say that Blahut was the first to appreciate the enormous untapped potential of the DFT in coding theory and he was certainly the pioneer in reconstructing (and enlarging) the theory of cyclic codes from the DFT standpoint [1]. In this view, a cyclic code is just the set of time-domain sequences whose spectra vanish over a specified set of frequencies. The coding engineer is forever liberated from the algebraic strait-jacket of ideals in polynomial rings, and algebraic coding theory is given a mighty shove toward its natural position among signal processing techniques.

These chapters should be read as avidly by researchers in other branches of signal processing as by coding theorists. Not only does the DFT free coding theory from much arcane algebra, but coding theory frees the DFT from the strictures of the complex field. Blahut makes this point repeatedly: take your transforms or perform your convolutions in the most convenient field!

There is much to admire in this part of the book. Helgert's alternant codes and the Goppa codes, both previously mysteries to this reviewer, are given eloquently simple formulations via the clever use of time-domain and frequency-domain "templates" combined with the convolution theorem for the DFT. Idempotents, too, arise to a new and simpler life in the frequency domain. And, of course, as is now generally well known from [1], the Reed–Solomon (RS) and BCH codes have beautiful frequency domain descriptions. All of this, and much more besides, can be found in Chapter 8.

Chapter 9 deals with decoding from the DFT viewpoint, and includes Blahut's own cunning simplification of the errors-and-erasures correction algorithm for RS and BCH codes. But the pinnacle of this chapter is its closing discussion on the computation of the DFT in finite fields. The Bluestein chirp algorithm, the Rader prime algorithm, and the Goertzel algorithm (all previously developed only for the complex field) are succinctly and masterfully developed.

Chapter 10 is a highly original treatment of multidimensional transform techniques for cyclic codes and their products. Much of this chapter is new, and so different from the past approaches in coding theory that it is difficult to summarize here; it must be read.

Chapter 11 treats fast algorithms both for transform evaluation and for convolution. It is hard to say who will find this of greater interest, the coding theorist or the signal processing specialist. The Winograd convolution algorithm, the Cooley–Tukey FFT, the Good–Thomas FFT, the Agarwal–Cooley convolution algorithm, and the Winograd FFT are all treated with elegance and ingenuity. Of perhaps understandably particular interest to this reviewer were two algorithms newly devised by Blahut, an "accelerated Berlekamp–Massey algorithm" and a "recursive Berlekamp–Massey algorithm"; the latter reduces the computational work from $0(n^2)$ to just about $0(n \log n)$ but is practical only for rather large $n$.

Our only regret about the coverage of the DFT was the omission of an explicit statement of what, since the appearance of [1], we have called "Blahut's theorem" in our lectures and writing. Blahut's theorem applies to DFT's over any fields and states that the Hamming weight of the sequence in one domain (time or frequency) equals the length of the shortest linear feedback shift register that can generate the periodic continuation of the sequence in the other domain. This result strikes us as an important addition to the list of useful DFT properties, and its absence from the book is mystifying.

Chapters 1–7 and parts of Chapters 13 and 14 contain the standard theory of linear block codes. This material is written with thoroughness and flair. We particularly admired the treatment of finite field algebra. It has the best selection of topics and proofs of any coding text. But we must say that we found distasteful the practice of writing, say, $GF(2^4)$ as GF(16), and even calling GF(16) the "hexadecimal field" and labelling its elements as $0, 1, 2, \cdots 9, A, B, \cdots F$; at the least, 2 ought to mean $1 + 1$ in any field.

The treatment of block codes is not entirely without blemishes. One such is the assertion on page 431 that "no binary code is a maximum-distance [-separable] code" which ignores the "simple parity-check codes" and "simple repetition codes" of Section 1.1. Gilbert bounds occasion many further blemishes. It is asserted on page 233 that a Gilbert-type inequality for alternant codes is in the "wrong direction" to permit use of Lemma 7.9.2. But in fact the inequality should have been written in the opposite direction after replacing $d - 1$ by $d$, just as was correctly done in the Gilbert bound for convolutional codes on page 455. The expression on page 455, which now begs for the application of Lemma 7.9.2, is, however, handled by a weaker and more awkward bound. The net result of all these machinations is that the very useful Gilbert relation, $d/n \geq H^{-1}(1 - R)$, which holds for all $n$, is never stated as other than an asymptotic bound. Perhaps more deplorably, the Gilbert bound is never shown to hold for linear block codes, although the rather elegant argument used to prove the bound for general codes (cf. pp. 446–447) could easily have been adapted to linear codes. In fact, the last sentence of page 453 could be read as suggesting that the Gilbert bound cannot be proved for linear block codes.

It seems to us a shame that a standard algebraic proof of the MacWilliams' identities was used in Section 14.1 rather than the recent proof of Chang and Wolf [2], which is based on two ways of calculating the probability of undetected error when a linear block code is used only for error detection. This latter proof contains much engineering insight, something that the author is elsewhere careful to cultivate.

This reviewer has never understood why most coding textbooks are written as if nothing less than a surgeon's scalpel would suffice to dissect block codes, while nothing more than a woodman's axe is needed for convolutional codes. This book is a paradigm of this double standard. Chapter 12 and parts of Chapters 13–15 treat convolutional codes with impatience and imprecision; definitions are often bungled and logical reasoning abused.

As with other coding books, this one makes no distinction between the convolutional code itself, i.e., the set of all possible encoded sequences, and the particular encoder that might be chosen for that code. One of the most interesting contrasts between linear block codes and convolutional codes is that the choice of a linear encoder for the former is of minor importance, but for the latter it is of crucial importance. For instance, every convolutional code has "catastrophic encoders" whose use would be disastrous in practice, as well as non-catastrophic encoders. In any case, this book simply equates a linear encoder and the resulting convolutional code (cf. pp. 349–350). That having been done, the subsequent discussions of "catastrophic convolutional codes" and "equivalent codes" could not be logically consistent.

Forney's seminal work on the complexity of convolutional encoders [3] is mostly ignored. An unfortunate exception is the footnote on page 355,

which incorrectly asserts that the constraint length as defined in Definition 12.2.1 is the minimum number of storage cells needed in the encoder. (The (12, 9) Wyner–Ash code has constraint length 5, but in fact 2 storage cells suffice in the encoder if these are used to store the parity bits, rather than to store the information bits as is done in the encoder of Fig. 12.12). This is a serious misunderstanding because the minimum number of storage cells determines the number of states in the trellis of the code, and hence the complexity of the corresponding Viterbi decoder.

A positive feature of Chapter 12 is the attention (cf. page 357) given to systematic convolutional encoders with feedback in the encoding circuit, the first such attention in a coding textbook. This type of encoder has already proved to be of considerable practical importance.

The parity-check-polynomial matrix of a convolutional code is so carelessly defined on page 356 that the all-zero matrix qualifies. "Distance notions" fare no better. Definition 12.3.1 of the various "minimum distances" (usually called "column distances" in the literature) tacitly assumes that $G_0$ has rank $k_0$ so that the "initial information frames" differ for the input sequences. The meaning of these distances is not pursued. Because $d_5^* = 4$ and $d_6^* = 5$ for the (6, 3) encoder of Fig. 12.3, one sees that this code is not double-error-correcting over a decoding constraint span of five frames—six frames are needed. But Fig. 12.16 purports to give a double-error-correcting decoder over a span of five frames (and the accompanying text even says that the code is double-error-correcting over a span of three frames!). The reader can easily check that this decoder will incorrectly decode a double error pattern with an error in the first bit of the first and fourth frames. The problem is that the author has not bothered to distinguish between the encoding and decoding constraint length, another distinction that is crucial for convolutional codes but of minor import in block coding.

The discussions of Viterbi decoding and the Fano sequential decoding algorithm that conclude Chapter 12 are superficial and often misleading. For instance, one does not need to rely on "computer simulation" to choose the decoding delay for a Viterbi decoder or to choose the metric for a sequential decoder, as is asserted.

The climactic gaffe about convolutional codes occurs when the author asserts in his "proof" of Theorem 14.6.1 that "any upper bound on the minimum distance of the block code [obtained by truncating the convolutional code after $m$ frames]" is also an upper bound on the minimum distance of the convolutional code." This assertion blithely ignores the fact that distance "counts" only between encoded sequences that differ in the first information frame.

On page 3, the author states that the book will deal only with coder and decoder design and not with that of the modulator and demodulator. Unfortunately, he breaks his promise. The result is Chapter 15, the final chapter, which was obviously written in haste. The last paragraph on page 482 gives the appropriate credits for some bounds and examples that in fact appear nowhere in the chapter. Except for the standard treatment of Forney's generalized minimum distance decoding, this chapter is a weakly reasoned and imprecise discussion of the interplay between coding and modulation. For instance, Ungerboeck's coded octal-phase-modulation schemes are erroneously described on page 473 as "convolutional codes over the complex field." They are not such by the author's own definition, because the "encoder" is not linear over the complex field. Ungerboeck's schemes actually use a conventional binary convolutional encoder followed by a modulation mapping from triplets of binary digits to the eight phases.

It would be unjust to end this review on a sour note. In our view, this book has a Queen Anne front and a Mary Ann back. But Queen Anne reigns much the longer, and makes this an outstanding and revolutionary book on coding.

## References

[1] R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Dev.*, vol. 23, pp. 299–315, May 1979.

[2] S. C. Chang and J. K. Wolf, "A simple derivation of the MacWilliams identity for linear codes," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 476–477, July 1980.

[3] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 720–738, Nov. 1970.