Correction to "A Further Note on Backwards Markovian Models"

G. VERGHESE AND T. KAILATH, FELLOW, IEEE

We wish to thank a conference reviewer and Prof. M. B. Pursley for pointing out an error in the arguments of the Appendix of the above note.[1] We forgot that two uncorrelated random variables may not remain so after conditioning.

However, all the results in our note continue to be true, except that the arguments in the Appendix must be replaced by the more laborious, but correct, alternative proof outlined in the body of the paper. These proofs merely involve verifying that the appropriate orthogonality conditions are satisfied by the given expressions. More specifically, writing

$$\mathcal{X}_{i+1,T}=\begin{bmatrix} x_{i+1} \\ \cdot \\ \cdot \\ \cdot \\ x_T \end{bmatrix} \qquad \mathcal{U}_{i+1,T-1}=\begin{bmatrix} u_{i+1} \\ \cdot \\ \cdot \\ \cdot \\ u_{T-1} \end{bmatrix},$$

we have

$$\mathcal{X}_{i+1,T}=\mathcal{A}x_{i+1}+\mathcal{B}\,\mathcal{U}_{i+1,T-1}$$

for some $\mathcal{A},\mathcal{B}$, from which it is easy to show that

$$E\left[\left(u_i-G_i'\pi_{i+1}^{-1}x_{i+1}\right)\mathcal{X}_{i+1,T}'\right]=0,$$

so that (9) and (12) of the paper hold. It may similarly be shown that the $\{\tilde{u}_i\}$ are uncorrelated.

G. Verghese was with the Information Systems Laboratory, Stanford University, Stanford, CA. He is now with the Electric Power Systems Engineering Laboratory, MIT, Cambridge, MA 02139.

T. Kailath is with the Information Systems Laboratory, Stanford University, Stanford, CA 94305.

[1] G. Verghese and T. Kailath, *IEEE Trans. Inform. Theory*, vol. IT-25, no. 1, pp. 121–124, Jan. 1979.

Book Reviews

The Theory of Error-Correcting Codes—F. J. MacWilliams and N. J. A. Sloane (Amsterdam: North-Holland and New York: Elsevier/North-Holland, xx + 762 pp., $39.50).

JAMES L. MASSEY, FELLOW, IEEE

This is the first comprehensive book on error-correcting codes written by mathematicians, and it establishes a standard of masterful scholarship that will not soon be surpassed. The authors have gleaned a treasury of coding facts (including an extensive table of best codes) from the 1478 entries in the bibliography and packaged them with clear explanations, elegant proofs, and graceful writing, together with many new or improved results.

Despite its massiveness, this is a narrow book. It deals only with block codes, virtually only with independent errors and the Hamming metric, and principally with code structure as contrasted with methods for encoding and decoding. Have no doubt about it, this book presents error-correcting codes as seen by the eye of the combinatorial mathematician, not the communications engineer! It is a much closer relative to van Lint's slim monograph [1] than to the principal other books on algebraic coding [2]–[5]. Compared to these latter, this book probes much more deeply into such structural aspects of a code as its weight (or distance) distribution and its automorphism group (i.e., the group of permutations that take the code into itself). The authors are clearly excited by the rich variety of combinatorial configurations embodied in codes, and only an intransigent reader will avoid contagion.

As no codes are richer in structure than the two Golay perfect codes and their extensions, these remarkable codes pop up every few pages in this book until the penultimate Chapter 20 (pp. 634–650), which is entirely devoted to showing their essential uniqueness and deriving their automorphism groups. Perhaps next in structural richness are maximum distance separable codes, which include the Reed–Solomon codes, and their treatment is proportionally extensive. Finite geometry codes, which include the Reed–Muller codes, receive almost as much coverage. And so on in order of decreasing structural beauty. There is a pleasant abundance of material on highly structured nonlinear codes.

The timing of this book was propitious; it includes many important results too recent to be in [1]–[4]. Among these are the complete Tietäväinen–van Lint proof that there exist no undiscovered perfect codes; Justesen's constructive and asymptotically good codes; Goppa codes and alternant codes; anticodes; and, preemintly, Delsarte's linear programming approach to bounding minimum distance that culminates in the current champion of asymptotic upper bounds, the McEliece–Rodemich–Rumsey–Welch bound. Other topics extensively treated in this book but not to be found, or given only cursory treatment, in [1]–[5] are t-designs, Hadamard transforms, normal bases for finite fields, Krawtchouk polynomials, bent functions, symplectic forms, and association schemes—the reader will find excellent introductions to all of these rather esoteric mathematical concepts.

This book will be indispensable to anyone doing research in algebraic coding theory. The Preface suggests (and specifies the appropriate sections for) its use as a text in any of the following four courses in coding theory: i) an elementary course for mathematicians, ii) an advanced course for mathematicians, iii) an elementary course for engineers, and iv) an advanced course for engineers. I would support its use for i) and ii), but definitely not for (iii) or (iv). My suggestion of a text for iii) would be Lin [4] or McEliece [5], and for iv) would be Peterson and Weldon [2] or Berlekamp [3]. The most glaring deficiency of this book as an engineering text is the complete lack of material on convolutional codes, and hence also on Viterbi and sequential decoding. Other serious deficiencies are the absences of treatments of soft-decision decoding (generalized minimum distance decoding and related schemes), burst-correcting techniques, and, inexplicably, Berlekamp's iterative algorithm for solving the key equation in the decoding of the Bose–Chaudhuri–Hocquenghem codes (only the Sugiyama *et al.* Euclidean algorithm approach to solving the key equation is included). As McEliece has pointed out, "A systems engineer...is still well advised to use Berlekamp's procedure [for solving the key equation]...with hindsight it is now possible to view Berlekamp's algorithm as an improved version of Euclid's!" [5, pp. 260–261].

This book is much more to be commended for its technical soundness than criticized for the few small lapses that I now describe. Although $p<\frac{1}{2}$ can be assumed without loss of generality for the error probability of a binary symmetric channel (BSC), the corresponding condition for the q-ary symmetric channel is $p<(q-1)/q$ (not $p<\frac{1}{2}$ as stated on p. 11) as this makes correct reception more likely than any particular error, although for $q>2$ it does entail loss of generality. It is not true, contrary to the claim on p. 36, that "only a slightly more complicated" scheme than bounded distance decoding suffices to achieve channel capacity on the BSC—if it were so, block codes would be much more popular in applications. The authors make the popular mistake (on p. 394) of assuming that the number of majority gates grows exponentially with L in L-step majority decoding of an $[n,k]$ code; in fact, that number need never exceeds k [6, p. 100].

Typographical and Freudian errors seem to be at a minimum. The only ones that I found worth pointing out here were the inclusion of $M^{(5)}(x)$ as a factor of $g(x)$ in the [23,12] Golay code on p. 205, the specification of the overall rate of a concatenated code as $(k/K)\cdot(n/N)$ rather than $(k/n)\cdot(K/N)$ on p. 307, and "projective" rather than "Euclidean" in the section title on p. 696. I would also note that only the lower bound on d is proved for Theorem 9 on p. 562, and that $\gtrsim$ can be strengthened to $>$ in Theorem 30 on p. 557.

The authors' style is much to my liking, with some annoying exceptions. It grates on me to see parts of speech replaced by mathematical symbols (e.g., "the sum is $>M(M-1)d$"), tables and summaries labeled as "figures," and a decimal point used to denote multiplication (e.g., "1101.1011"). I also consider the unexplained abbreviation "Garshamov" (p. v of Vol. I and p. 315) confusing and a bit too cute. We all have our hang-ups. More substantively, I see no reason for reversing the order of coefficients from that in [2] when representing binary polynomials by octal numbers—needless confusion will result—and I found the index to be rather inadequate.

This reviewer has upon occasion remarked that "block codes make for good papers but convolutional codes make for good communications;" I am now persuaded to generalize this conjecture to "*books and* papers."

References

[1] J. H. van Lint, *Coding Theory*, Lecture Notes in Mathematics, No. 201. Berlin: Springer-Verlag, 1971.

[2] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: M.I.T. Press, 1972.

[3] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[4] S. Lin, *An Introduction to Error-Correcting Codes*. Englewood Cliffs, NJ: Prentice-Hall, 1970.

[5] R. J. McEliece, *The Theory of Information and Coding*, Encyclopedia of Mathematics and Its Applications, Vol. 3. Reading, MA: Addison-Wesley, 1977.

[6] J. L. Massey, *Threshold Decoding*. Cambridge, MA: M.I.T. Press, 1963.

James L. Massey is a Professor of System Science at the University of California, Los Angeles. He served this TRANSACTIONS *as Editor from 1974 to 1977, and as Associate Editor for Algebraic Coding from 1972 to 1974. His reviews of references [2] and [4] above also appeared in this* TRANSACTIONS.