(Reprinted from 1970 IEEE International Convention Digest, March 1970.)

SESSION 7D: NEW DIRECTIONS FOR INFORMATION
THEORY IN THE 70'S
PAPER 7D.2

CAN CODING BEAT THE SYSTEM?

James L. Massey
Dept. of Elec. Engr.
Univ. of Notre Dame
Notre Dame, Ind. 46556

INTRODUCTION

The thesis of this presentation is that the methods of information theory, in particular the techniques employed in connection with error-correcting codes, will play an increasingly important role in advancing mathematical systems theory. Systems theory is here understood to embrace the studies of time-continuous differential systems, time-discrete amplitude-continuous systems, and fully discrete systems or automata. We will attempt to justify this thesis by citing instances where systems theory has already been influenced by each of the following aspects of coding theory: (1) The central importance of finite structures in information theory and in coding, (2) The fundamentally algebraic nature of parity-check coding, (3) The fertility of coding theory as a spawning ground for new systems problems, and (4) The availability of coding techniques applicable to a broad class of problems in systems theory.

FINITE SYSTEMS

This author is indebted to L. Zadeh for calling to his attention the fact that the so-called "Mealy machine" of automata theory was in fact precisely defined by C. Shannon in the latter's foundation paper [1] for information theory some several years prior to Mealy's contributions. This bit of technical history is vivid evidence of the fact that finite alphabets and finite transducers lie at the very core of information theory and coding. Thus, it is hardly surprising that the minimization problem for finite-state machines was first formulated and solved by D. Huffman, [2] one of the first workers in coding theory.

LINEAR CODES AND LINEAR SYSTEMS

The pioneering work of R. Hamming [3], later generalized by D. Slepian and others, established the importance to information theory of linear codes (also known as parity-check codes and as group codes.) The basic mathematical structure for linear codes is the vector space over a finite (or Galois) field. The importance of this fact for systems theory is that such coding systems provided an application for linear algebra freed from the narrowing dependence on the real and complex number fields characteristic of former systems problems. When such normed fields are exorcised, only the purely algebraic aspects of the systems remain. Thus it was again the same D. Huffman--motivated by studies of such linear codes--who was led to introduce the linear finite-state machine and who began the development of the now elegant theory of these useful and intriguing devices [4]. The development of linear sample-data systems, influenced by its outgrowth from the study of differential systems, had previously been grounded more on analysis than on algebra. The impact of the successes in linear automata has been felt in the construction of unified algebraic theories which include the sample-data systems.

NEW SYSTEMS PROBLEMS

The fundamental decoding problem is that of recovering the input to the encoder from a noisy or corrupted version of its output. The least condition which one could impose on a useful encoder is that the input be recoverable when this corruption is nil, i. e. that the encoder be an invertible system. D. Huffman formulated this condition as a new systems property which he termed "information losslessness." [5] This author and M. Sain [6] noted the practical further necessity in coding that the inverse system be feedback-free and solved the problem as to when a feedback-free linear system has a feedback-free inverse. G. Forney [7] has recently given an elegant formulation of these results, and has shown how to handle such algebraically similar questions as when does a stable linear system have a stable inverse. These coding studies led M. Sain and the author to pose the general problem of invertibility of linear differential systems and to find that the discrete systems results carried through in toto. [8] Invertibility is a striking example of a new and fundamental systems problem whose origin lies in coding theory.

NEW SYSTEMS TOOLS

In their attempts to design simple decoders, coding theorists have developed techniques with great promise for wide applicability in systems theory. E. Berlekamp's ingenious "iterative algorithm" for decoding the Bose-Chaudhuri-Hocquenghem codes was shown by the author to be an efficient method to find the shortest linear feedback shift-register (i. e. the linear recursion of minimum order) which generates a prescribed finite sequence of digits in any field. [9] Although this is a common problem in systems synthesis and in systems identification, its efficient solution awaited coding theory and Berlekamp's technique should find many applications.

Sequential decoding [10], originated by J. Wozencraft, is recognized in coding theory as the natural and minimal-computational method for the search of a branch-weighted tree to find, with near certainty, the path of highest (or lowest) weight for the trees associated with convolutional error-correcting codes. A. Viterbi later formulated the optimum search procedure for such trees which J. Omura [11] has recognized to be equivalent to dynamic programming. The point could be made that coding theorists would be well-advised to look more closely at the methods available in systems theory. Another viewpoint follows from the observation that Viterbi's algorithm is practical only for short constraint length codes whereas the computational complexity of sequential decoding is independent of the code constraint length. Systems theorists would be well-advised to investigate the conditions under which sequential decoding would be a desirable practical alternative to dynamic programming.

REFERENCES

[1] C. Shannon and W. Weaver, The Mathematical Theory of Communication, Univ. of Illinois Press 1949, p. 26.

[2] D. Huffman, "The Synthesis of Sequential Switching Circuits," The Journal of the Franklin Institute, v. 257, 1954, pp. 161-190, 275-303.

[3] R. Hamming, "Error Detecting and Error Correcting Codes," Bell Sys. Tech. Journal, v. 29, 1950, pp. 147-160.

[4] D. Huffman, "The Synthesis of Linear Sequential Coding Networks," in Information Theory (Ed. C. Cherry), 1955 London Symp. on Info. Th., pp. 77-95.

[5] D. Huffman, "Information Conservation and Sequence Transducers," Proc. Symp. on Info. Networks, Poly. Inst. of Brooklyn, April 12-14, 1954, pp. 291-307.

[6] J. Massey and M. Sain, "Inverses of Linear Sequential Circuits," IEEE Trans. Computers, v. C-17, April 1968, pp. 330-337.

[7] G. Forney, "Convolutional Codes I: Algebraic Structure," to appear in IEEE Trans. Info. Th.

[8] M. Sain and J. Massey, "Invertibility of Linear Time-Invariant Dynamical Systems," IEEE Trans. Auto. Cont., v. AC-14, April 1969, pp. 141-149.

[9] J. Massey, "Shift-Register Synthesis and BCH Decoding," IEEE Trans. Info. Th., v. IT-15, January 1969, pp. 122-127.

[10] J. Wozencraft and I. Jacobs, Principles of Communication Engineering, John Wiley, New York, 1965, pp. 425-475.

[11] J. Omura, "On the Viterbi Decoding Algorithm," IEEE Trans. Info. Th., v. IT-15, January 1969, pp. 177-179.

This work was supported in part by the National Science Foundation under Grant GK-13618 to Univ. of Notre Dame.