XI. PROCESSING AND TRANSMISSION OF INFORMATION*

Academic and Research Staff

Prof. P. Elias
Prof. R. M. Gallager
Prof. M. M. Goutmann
Prof. E. V. Hoversten
Prof. D. A. Huffman
Prof. R. S. Kennedy
Prof. J. L. Massey
Prof. E. Mortensen
Prof. C. E. Shannon
Prof. R. N. Spann

Graduate Students

D. S. Arnstein
E. A. Bucher
D. Chase
R. L. Greenspan
H. M. Heggestad
J. A. Heller
M. Khanna
Jane W-S. Liu
J. Max
J. C. Moldon
J. T. Pinkston III
E. M. Portner, Jr.
J. S. Richters
D. A. Wright

A. STUDIES IN CONVOLUTIONAL CODING

1. Plotkin Bound for Convolutional Codes

Massey, in unpublished work, has obtained an upper bound on the minimum distance of binary convolutional codes which is asymptotically the same as the Plotkin bound for block codes. This work has now been extended[1] to convolutional codes with symbols in an arbitrary finite field, GF(q). Letting d(N, K, m) denote the greatest minimum distance of convolutional codes with rate $R = K/N$ and memory m subblocks, that is, the constraint length $n_A = (m+1)N$ digits[2], one obtains the following theorem.

THEOREM: $d(N,K,m) \leq (b-1)N + qi + 1 + \left\lceil \frac{m+1-b}{b} \right\rceil (q-1)i$, where [x] denotes the least integer equal to or greater than x, and

$$b = \frac{\text{l.c.m.}(N-K, q)}{N - K}$$

$$i = \frac{\text{l.c.m.}(N-K, q)}{q}.$$

Convolutional codes may be considered as linear tree codes. It has also been shown[1] that the preceding theorem applies also to the class of nonlinear tree codes over GF(q), with $R = \frac{1}{N}$ and $N = qr + 1$ for some integer r, and such that the N encoded digits on each branch may be written

$$\underline{f}(i_o, i_1, \ldots, i_{j-1}) + \underline{B}i_j,$$

where $\underline{B}$ is a constant N-tuple, i_j is the information digit corresponding to the branch

*This work was supported principally by the National Aeronautics and Space Administration (Grant NsG-334).

in question, and $\underline{f}$ is an N-tuple function of the preceding information digits.

Some cases have been found[1] in which the bound of the preceding theorem is achieved with equality. For $q = 2$ and $K = 1$, equality can be obtained for any odd N when $m \leq 3$. For $N = 5$ and $N = 3$, equality can be obtained for $m \leq 4$ and $m \leq 6$, respectively.

2. Semidefinite Decoding

A decoding procedure called semidefinite decoding has been suggested by the author which allows the decoder to make some use of previous decoding decisions without the danger of infinite error propagation which can arise when feedback decoding is employed.

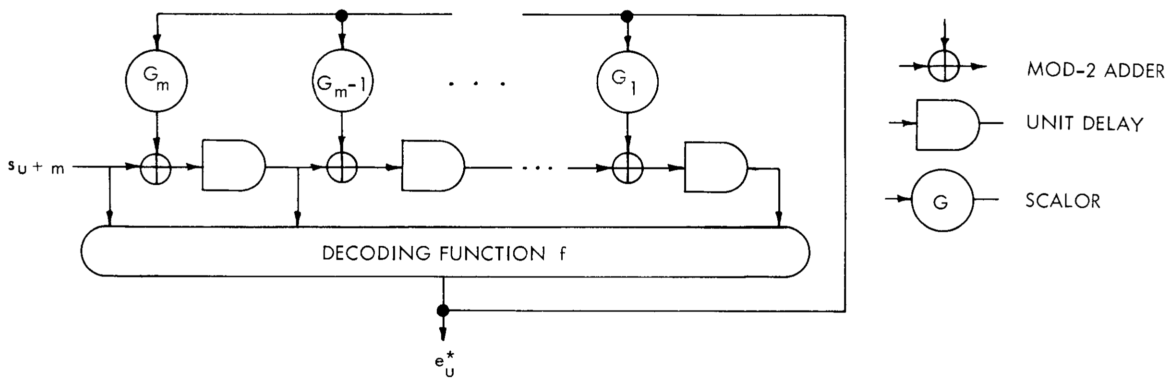

Fig. XI-1. Syndrome register for a feedback decoder.

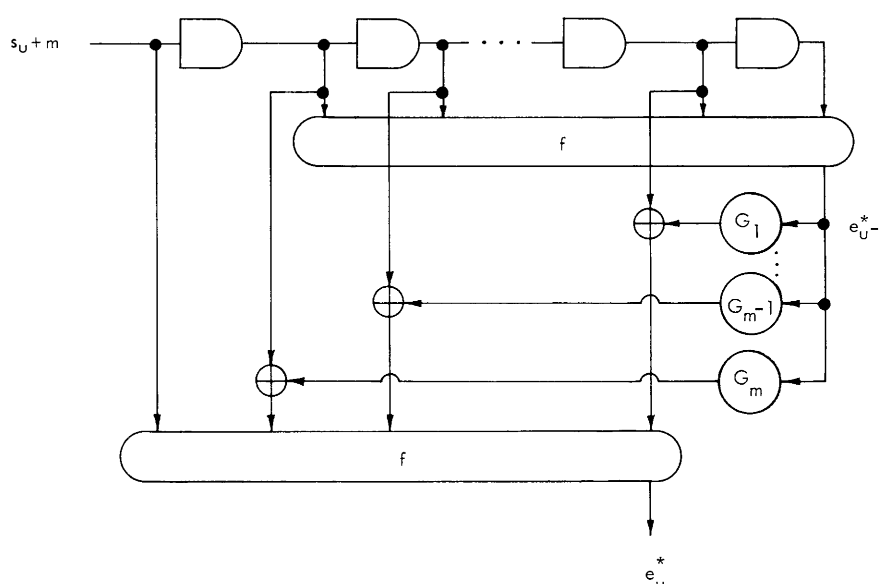

Fig. XI-2. Syndrome register for a (K=2)-stage semidefinite decoder.

This type of decoding is conveniently described in terms of the syndrome register[3] employed in the decoder. Figure XI-1 shows the syndrome register portion of a feedback decoder for an $R = \frac{1}{2}$ systematic binary convolutional code. s_{u+m} is the syndrome digit at time u + m, and e_u^* is the decoding estimate of the error in the information digit at time u. A definite decoder differs from that in Fig. XI-1 in that there is no feedback from the decoding decision into the syndrome register. A K = 2 stage semidefinite decoder is shown in Fig. XI-2. For such a decoder a definite decoding decision is made on e_{u-K+1}. This decision is then utilized in the circuit which estimates e_{u-K+2}.

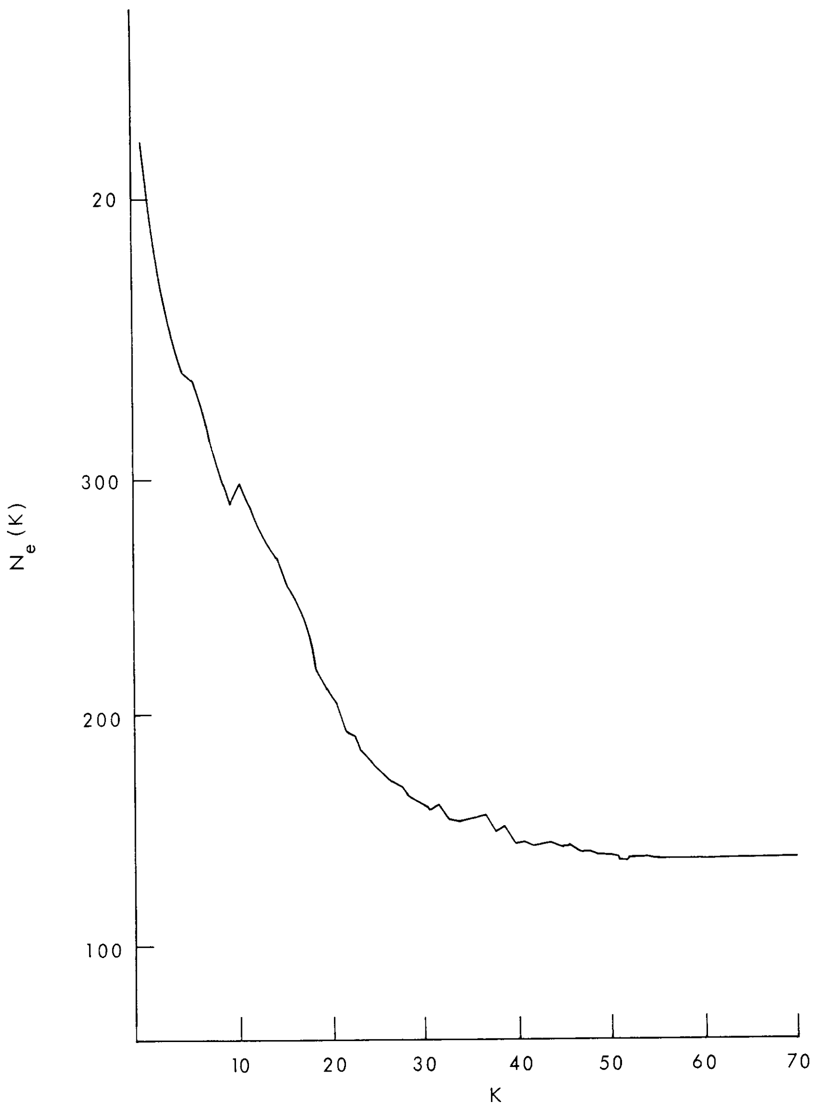

Fig. XI-3. Number of decoding errors, $N_e(K)$, per 100,000 information bits vs number of semidefinite decoding stages K, for R = 1/2. Self-orthogonal code (n_A=46, J=6).

In general, the decision on e_{u-K+j} will make use of the decisions on $e_{u-K+1}, \ldots, e_{u-K+j-1}$ for a K-stage semidefinite decoder. The case K = 1 coincides with definite decoding and $K = \infty$ coincides with feedback decoding.

The performance of semidefinite decoding has been analyzed by simulation[4] of decoders on the IBM 360/65 computer in the M.I.T. Computation Center. Figure XI-3 shows the result of semidefinite decoding employing a threshold decoding function f on the $n_A = 36$ self-orthogonal code for which 6 orthogonal parity checks can be formed. For this case, the decoding error probability is (approximately) a monotonically decreasing function of K which obtains its asymptotic or feedback-decoding value when K is almost equal to Rn_A. This result is typical of those obtained by simulation of semidefinite threshold decoders for the classes of self-orthogonal codes, uniform codes, and Massey's trial-and-error codes.

3. Gilbert Bound on Definite Decoding Distance

The customary minimum distance measure[2] employed with convolutional codes is that appropriate for feedback decoding. For definite decoding, an alternative measure is required. Consider an $R = \frac{1}{2}$ binary systematic convolutional code in which $i_o, i_1, i_2, \ldots$ is the sequence of information digits and $p_o, p_1, p_2, \ldots$ is the sequence of parity digits. The definite decoding minimum distance, d_{DD}, is defined to be the fewest number of positions in which there are disagreements in the vector

$$[i_o, i_1, \ldots, i_m, i_{m+1}, \ldots, i_{2m}, p_m, p_{m+1}, \ldots, p_{2m}]$$

for information sequences with different values of i_m. It is easily shown that d_{DD} is also the minimum Hamming weight of such a vector with i = 1.

It has been shown[5] that there exist convolutional codes such that

$$\lim_{m \to \infty} \frac{d_{DD}}{m} \geqslant .0262.$$

This is the first asymptotic result on definite decoding of a fixed convolutional code. The proof[5] of this result utilized a number of interesting new facts concerning the structure of sequences produced by linear feedback shift registers and the properties of parasymmetric matrices.

J. L. Massey

References

1. W. C. Wilder, "Extensions of the Plotkin Bound," S.M. Thesis, M.I.T., August 1967.

2. J. L. Massey, *Threshold Decoding* (The M.I.T. Press, Cambridge, Mass., 1963), pp. 11-19.

3. *Ibid.*, pp. 54-59.

4. L. A. Frasco, "Analysis and Simulation of Semi-Definite Decoding," S. M. Thesis, M. I. T., May 1967.

5. R. W. Kolor, "A Gilbert Bound for Convolutional Codes," S. M. Thesis, M. I. T., August 1967.