From results for (N,K) codes with N' non idle positions the total number of nonzero symbols is

$$(q-1)\, q^{K-1} N'$$

so

$$W_{avg} = \frac{(q-1)\, N_A\, q^{N_A R - 1} - (q-1)(N_A - N_0)\, q^{(N_A - N_0)R - 1}}{q^{N_A R} - q^{(N_A - N_0)R}}$$

Q.E.D.

<u>Corollary</u>: $d_{min} \leq W_{avg}$

B. <u>Deterministic Decoding</u>

1. Feedback Decoding and Definite Decoding

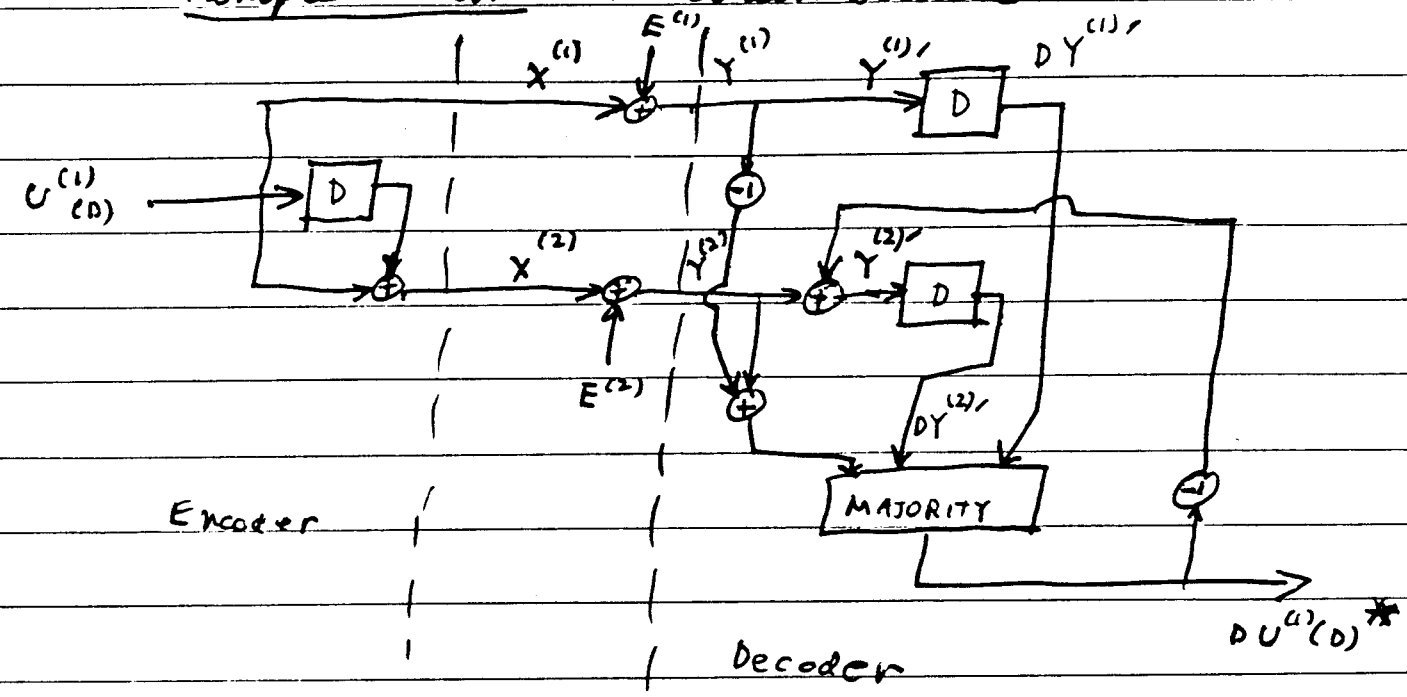
The theorem relating d_{min} and decoding with errors holds only for block 0. Two methods for decoding succeeding blocks have been proposed.

a. Feedback Decoding (FD)

It is assumed that all data up to time j is decoded correctly. Their effects on succeeding blocks $j+1, \cdots, j+m$ are removed. If blocks $j-m+1, \cdots, j$ have been decoded correctly and their effects removed, block $j+1$ <u>effectively becomes block 0</u> and the same decoding algorithm can be used to decode block $j+1$ from the modified blocks $j+1, \cdots, j+m+1$ with the same error correcting capability. If some previous decoding errors have been made, succeeding decoding will be adversely affected. Infact, <u>noisy error propagation</u> can occur, i.e., if a decoding error is made prior to block $j+1$, all blocks

from time $j+1$ on can be decoded incorrectly even with no channel errors!

Example (cont.) Feedback Decoder



Received symbols

$$y_j^{(1)} = x_j^{(1)} + e_j^{(1)} = u_j^{(1)} + e_j^{(1)} \qquad (1)$$

$$y_j^{(2)} = x_j^{(2)} + e_j^{(2)} = u_j^{(1)} + u_{j-1}^{(1)} + e_j^{(2)} \qquad (2)$$

The modified received symbols are

$$y_j^{(1)\prime} = y_j^{(1)} = u_j^{(1)} + e_j^{(1)} \qquad (1')$$

$$y_j^{(2)\prime} = y_j^{(2)} - u_{j-1}^{(1)*} = u_j^{(1)} + [u_{j-1}^{(1)} - u_{j-1}^{(1)*}] + e_j^{(2)} \qquad (2')$$

also

$$y_{j+1}^{(2)} - y_{j+1}^{(1)} = u_j^{(1)} + e_{j+1}^{(2)} - e_{j+1}^{(1)} \qquad (3')$$

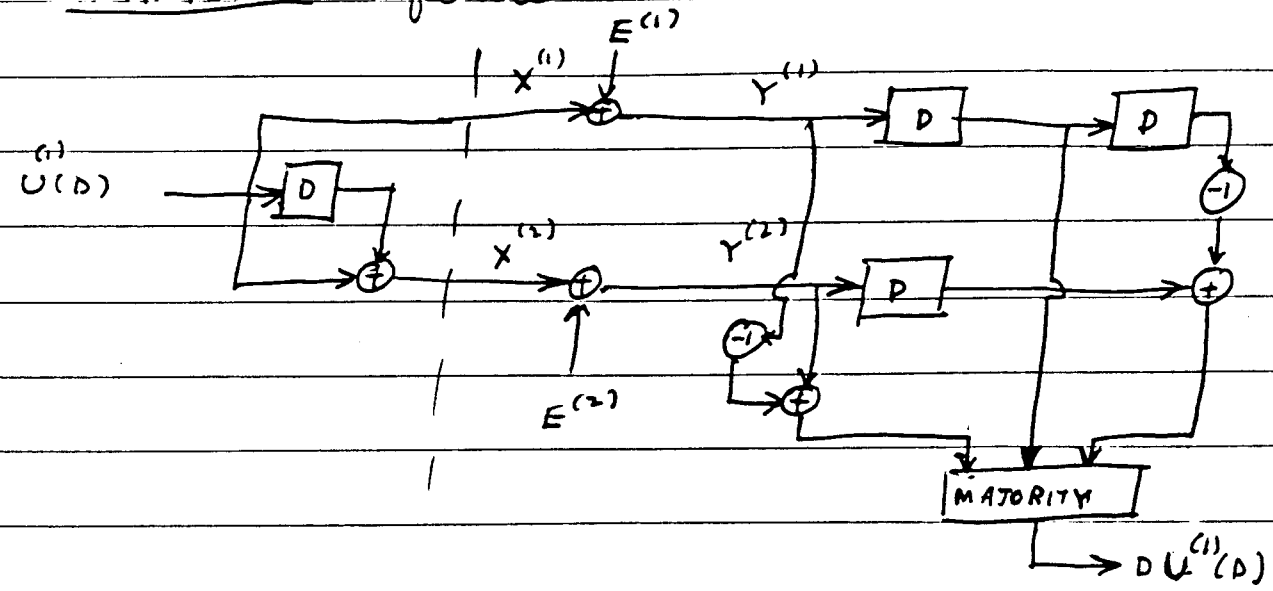
Notice that Eq 1', 2' and 3' all contain different error symbols. assuming $u_{j-1}^{(1)} = u_{j-1}^{(1)*}$ these equations give three independent estimates of $u_j^{(1)}$. If there are

no channel errors or a single channel error in the constraint length of four received symbols, $u_j^{(1)}$ can be decoded correctly by a majority vote of Eq's 1', 2', and 3' if $u_{j-1}^{(1)}$ has been decoded correctly. Notice that both $e_{j+1}^{(2)}$ and $e_{j+1}^{(1)}$ can be non zero and $u_j^{(1)}$ can be decoded correctly. However, $u_{j+1}^{(1)}$ will be decoded incorrectly. So the code can correct all single errors in a constraint length. This decoder has no noisy error propagation. Assume that $u_{j-1}^{(1)} \neq u_{j-1}^{(1)*}$ and that no channel errors occur in blocks j and $j+1$. Then Eq 1' and 3' give correct estimates of $u_j^{(1)}$ and this symbol is decoded correctly. Suppose we had chosen the decoding function $u_j^{(1)*} = y_j^{(2)'} = u_j^{(1)} + [u_{j-1}^{(1)} - u_{j-1}^{(1)*}] + e_j^{(2)}$. With no channel errors this decodes correctly when previous decoding is correct. However, once a decoding error is made all succeeding symbols are decoded incorrectly without any channel errors. This illustrates the important point that noisy error propagation depends on the code and the decoding scheme.

b. <u>Definite Decoding (DD)</u>

Definite decoding does not make use of past decoding estimates when decoding $\vec{u}_j$. The estimate $\vec{u}_j^*$ is calculated from the unmodified received sequence $[\vec{y}_{j-m}, \ldots, \vec{y}_{j-1}, \vec{y}_j, \vec{y}_{j+1}, \ldots \vec{y}_{j+m}]$.

EXAMPLE : Definite Decoder



at time $j+1$ the decoder can calculate

$$y_j^{(1)} = u_j^{(1)} + e_j^{(1)} \qquad (1'')$$

$$y_j^{(2)} - y_{j-1}^{(1)} = u_j^{(1)} + e_j^{(2)} - e_{j-1}^{(1)} \qquad (2'')$$

$$y_{j+1}^{(2)} - y_{j+1}^{(1)} = u_j^{(1)} + e_{j+1}^{(2)} - e_{j+1}^{(1)} \qquad (3'')$$

Once again these equations give three independent estimates of $u_j^{(1)}$ and all single errors in a constraint of 6 code symbols can be corrected. There can be no noisy error propagation since the decoding of $u_{j+1}^{(1)}$ is independent of the estimate $u_j^{(1)*}$. Notice that Equations 1' and 1'' are identical and so are equations 3' and 3''. Equations 2' and 2'' are the same except that the channel error $e_{j-1}^{(1)}$ appears in Eq 2'' instead of the <u>post decoding error</u> $u_{j-1}^{(1)*} - u_{j-1}^{(1)} \equiv e_{j-1}^{(1)\Delta}$

If the channel is good enough so that reliable decoding is expected, then intuitively one would expect that $P\{e_{j-1}^{(1)\Delta} \neq 0\} << P\{e_{j-1}^{(1)} \neq 0\}$, i.e, that a decoding error is much less probable than a channel error. This indicates that the probability of bit decoding errors should be less with feedback decoding than with definite decoding. This has not been proven analytically. However, simulation indicate that this is true when the best decoding functions are used.

2. <u>Syndrome Decoding</u> (for canonic systematic codes)

<u>Def:</u> Syndrome Sequence

The syndrome sequence for canonic systematic codes is the difference between the parity check symbols recomputed from the received information symbols and the received parity check symbols, i.e.,

$$S^{(j)}(D) = \sum_{l=0}^{\infty} s_l^{(j)} D^l = \sum_{k=1}^{K_0} G_{(k)}^{(j)}(D) Y^{(k)}(D) - Y^{(j)}(D) \quad \text{for } j = K_0+1, \cdots, N_0$$

Note: for systematic code $X^{(k)}(D) = U^{(k)}(D)$ for $k = 1, \cdots, K_0$

Therefore

$$S^{(j)}(D) = \sum_{k=1}^{K_0} G_{(k)}^{(j)}(D)\left[U^{(k)}(D) + E^{(k)}(D)\right] - \left[\sum_{k=1}^{K_0} G_{(k)}^{(j)}(D) U^{(k)}(D) + E^{(j)}\right.$$

$$= \sum_{k=1}^{K_0} G_{(k)}^{(j)}(D) E^{(k)}(D) - E^{(j)}(D) \quad \text{for } j = K_0+1, \cdots, N_0$$

So $S^{(j)}(D)$ only depends on the error sequence and not on the information vector

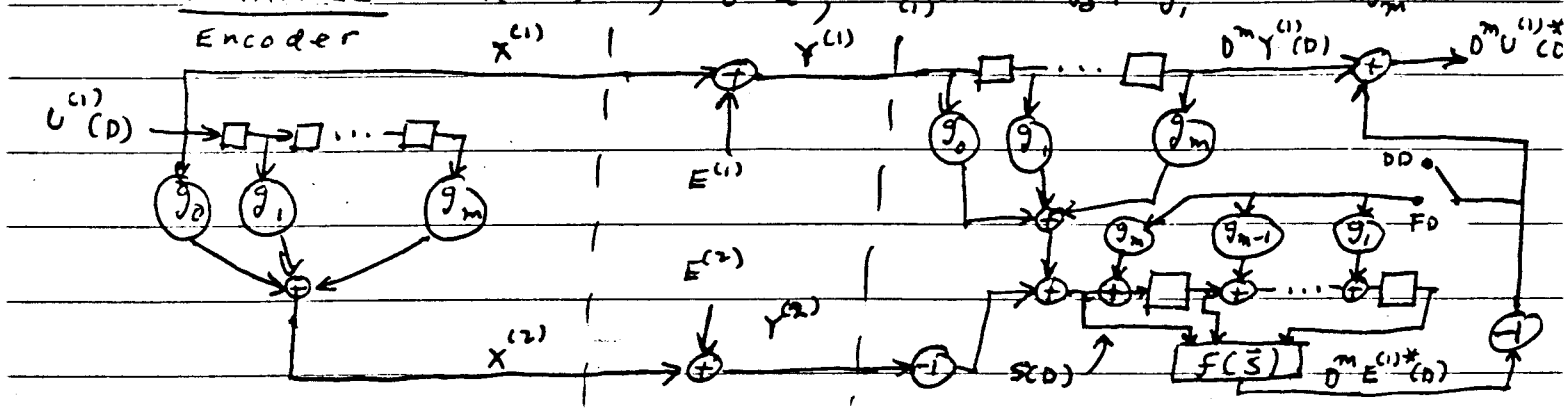
Define $\vec{s}_j = [s_j^{(K_0+1)}, \cdots, s_j^{(N_0)}]$

and $\vec{s} = [\vec{s}_0, \vec{s}_1, \cdots, \vec{s}_m]_{1 \times (m+1)(N_0 - K_0)}$

is the $1 \times N_A(1-R)$ syndrome vector used to decode block 0 since an error in block 0 can affect only the following m blocks. As in the case of block codes, $\vec{s}$ could have been caused by q^{RN_A} different error vectors since the actual error sequence + any one of the q^{RN_A} codewords results in the same syndrome. The optimum syndrome decoder would determine the most likely error pattern consistent with the syndrome.

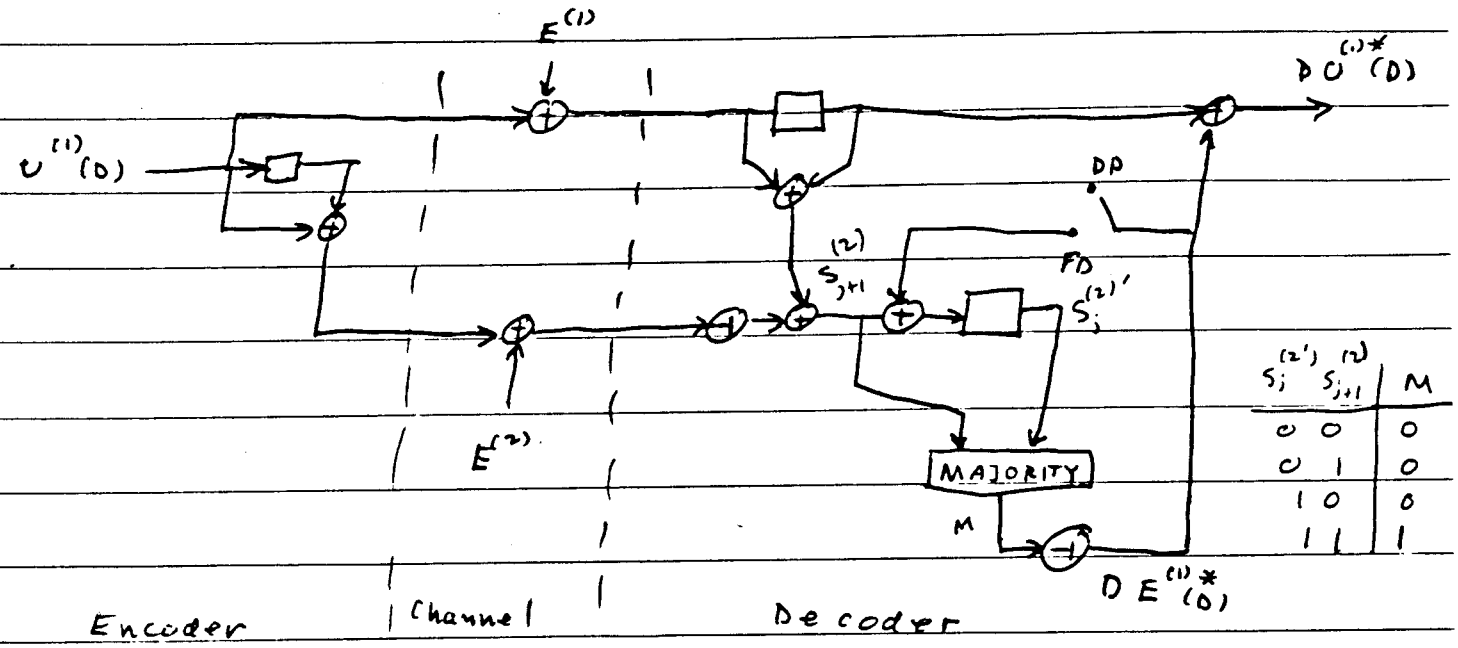
In a feedback syndrome decoder the errors in block 0, $\vec{e}_0$, are estimated from $\vec{s}$ and then used to remove their effect on $\vec{s}$. $\vec{e}_1$ is then estimated from $\{\vec{s}_1, \cdots, \vec{s}_{m+1}\}$ using the same algorithm. Notice that errors in the information symbols of block 0 affect $\{\vec{s}_0, \cdots, \vec{s}_m\}$ while errors in the check symbols of block 0 only affect $\vec{s}_0$. Therefore in decoding $\vec{e}_1$ only the estimated information symbol errors are needed to modify $[\vec{s}_1, \cdots, \vec{s}_m]$.

<u>EXAMPLE</u> $R = 1/2$, $N_0 = 2$, $G^{(2)}_{(1)}(D) = g_0 + g_1 D + \cdots + g_m D^m$



With the switch in the FD position the decoder is a feedback decoder. In the DD position it is a definite decoder. Notice that the decoder has a memory of $2m+1$.

Decoder for Simple Example



$s_j^{(2')}$	$s_{j+1}^{(2)}$	M
0	0	0
0	1	0
1	0	0
1	1	1

In DD mode

$$s_{j+1}^{(2)} = e_{j+1}^{(1)} + e_j^{(1)} - e_{j+1}^{(2)}$$

$$s_j^{(2)} = e_j^{(1)} + e_{j-1}^{(1)} - e_j^{(2)}$$

In FD mode the modified contents of the syndrome register for decoding $\psi_j^{(1)}$

$$s_{j+1}^{(2)\prime} = s_{j+1}^{(2)} = e_{j+1}^{(1)} + e_j^{(1)} - e_{j+1}^{(2)}$$

$$s_j^{(2)\prime} = s_j^{(2)} - e_{j-1}^{(1)*} = e_j^{(1)} + [e_{j-1}^{(1)} - e_{j-1}^{(1)*}] - e_j^{(2)}$$

This decoder is equivalent to the decoders on p. 62 and p. 64. Notice that in the feedback mode the channel error $e_{j-1}^{(1)}$ is replaced by the post decoding error $e_{j-1}^{(1)} - e_{j-1}^{(1)*}$.

3. Threshold Decoding [Ref: Massey-8, Gallager 3]

The decoding functions for the feedback and definite decoder examples and $f(\vec{s})$ for the syndrome decoder example appear to have been "pulled out of the air." One of the major elements of these decoders was a majority or threshold device. Threshold decoding was developed by Massey as a simple method for implementing the logical function $f(\vec{s})$. Threshold decoding is most efficient with binary codes. Massey [Ref 8, p. 91] shows that threshold decoders cannot take advantage of the improved distance structure of codes with symbols from higher order alphabets. Therefore the discussions here will be limited to binary codes. Threshold decoding is applicable to both block and convolutional codes so the theory will be formulated in a general framework.

Any syndrome digit is a known linear combination of the error symbols. Also any combination of syndrome symbols is once again a known function of error symbols. The syndrome vector calculated at the receiver has $N_A(1-R)$ components. Over GF(2) there are $2^{N_A(1-R)}$ possible linear combinations of syndrome symbols. Any such known sum will be called a <u>parity check</u> and will be denoted by the symbol A_i. A_i will be said to check error digit

e_j if e_j affects A_i.

<u>Def:</u> <u>Orthogonal Parity Checks</u>

a set $\{A_i\}$ of parity checks is said to be orthogonal on e_m if each A_i checks e_m but no other error bit is checked by more than one A_i.

<u>Ex:</u> $A_1 = e_1 + e_2 + e_3$

$A_2 = e_3 + e_4 + e_5$

$A_3 = e_3 + e_6 + e_7$

$\{A_i\}$ orthogonal on e_3

For a memoryless channel a set of J parity checks orthogonal on e_m provides J statistically independent estimates of e_m. This suggests decoding by majority vote. The following theorem characterizes the error correction and detection capabilities of majority decoding.

<u>Theorem:</u> Given a set of $J = 2t + s$ parity checks orthogonal on e_m and any pattern of t or fewer errors in the bits checked by $\{A_i\}$, then e_m will be decoded correctly and patterns of $t+1, \cdots, t+s$ errors will cause an error alarm if the following decoding rule is used:

$e_m^* = 1$ if more than $\frac{J+s}{2}$ of A_i are 1

$e_m^* = 0$ if $\frac{J-s}{2}$ or fewer have value 1

error alarm otherwise

Proof: assume $e_m = 0$ and no more than t errors have occured. In the worst possible case each error would

occur in a different check so that at most $t = \frac{J-s}{2}$ checks could be 1 and e_m is correctly decoded as 0. Similarly no more than $t+s = \frac{J-s}{2} + s = \frac{J+s}{2}$ errors will cause at most $\frac{J+s}{2}$ checks to be 1 and e_m is not incorrectly decoded to 1.

Assume that $e_m = 1$ and no more than t errors have occurred. Then at most $t-1$ of the other error bits checked can be 1. $e_m = 1$ is in each check so that $J - (t-1) = J - \left(\frac{J-s}{2}\right) + 1 = \frac{J+s}{2} + 1$ or more checks must be 1 and e_m is correctly decoded. With no more than $t+s$ errors, at least $J - (t+s-1) = \frac{J-s}{2} + 1$ checks will be 1 so that e_m is not incorrectly decoded to 0.

Q.E.D.

If K_0 sets of J parity checks orthogonal on each of the information noise symbols can be found, all patterns of $t = \frac{J}{2}$ or fewer errors in the bits checked can be corrected. Thus, if this is true, $d_{min} \geq 2t+1 = J+1$. If $J = d_{min} - 1$ orthogonal checks can be found for each information noise bit the code is said to be one step <u>completely orthogonalizable</u>. If a code can be completely orthogonalized, any error pattern guaranteed correctable by d_{min} can be corrected by majority decoding. In addition many error patterns of higher weight will generally be corrected also. For example, if $J = 10$ checks orthogonal on e_m are known, then $t = \frac{J}{2} = 5$ and six errors will cause a

decoding error only if each falls in a different parity check. This is unlikely if each A_i checks several error bits. See (Massey 8 pp 90-91) for an example of threshold decoding a maximal length code gives $P_e \sim 5\times10^{-7}$ while an algorithm a more sophisticated decoder makes use of probabilistic information. Given a set of parity checks $\{A_i\}$ a minimum probability of error decoder for e_m is

$$e_m^* = \begin{cases} 1 & \text{if } P(e_m=1/\{A_i\}) > P(e_m=0/\{A_i\}) \\ 0 & \text{otherwise} \end{cases}$$

using Bayes' rule the inequality becomes

$$P(e_m=1)\,P(\{A_i\}/e_m=1) > P(e_m=0)\,P(\{A_i\}/e_m=0)$$

with a memoryless channel the A_i with e_m fixed are statistically independent for an orthogonal set

so

$$P(e_m=1)\prod_{i=1}^{J} P(A_i/e_m=1) > P(e_m=0)\prod_{i=1}^{J} P(A_i/e_m=0)$$

Let $p_0 = 1-q_0 = P(e_m=1)$ and $p_i = 1-q_i = P(A_i \neq e_m)$.

$P(A_i \neq e_m) = P\{$odd number of errors in bits checked by A_i exclusive of $e_m\} = P\{A_i=0/e_m=1\} = P\{A_i=1/e_m=0\}$

So $P(A_i/e_m=1) = q_i^{A_i}\,p_i^{1-A_i}$ with A_i considered to be a real number. also $P(A_i/e_m=0) = q_i^{1-A_i}\,p_i^{A_i}$.

Thus the decoding rule is set $e_m^*=1$ if and only if

$$p_0\prod_{i=1}^{J} q_i^{A_i}\,p_i^{1-A_i} > q_0\prod_{i=1}^{J} q_i^{1-A_i}\,p_i^{A_i}$$

Taking logarithms and rearranging this becomes

$$\sum_{i=1}^{J} A_i \left(2 \log \frac{q_i}{p_i}\right) > \sum_{i=0}^{J} \log \frac{q_i}{p_i}$$

<u>Theorem</u>: The minimum probability of error decoder for e_m is

$$e_m^* = \begin{cases} 1 & \text{if } \sum_{i=1}^{J} A_i \left(2 \log \frac{q_i}{p_i}\right) > \sum_{i=0}^{J} \log \frac{q_i}{p_i} \\ 0 & \text{otherwise} \end{cases}$$

For an additive white Gaussian noise channel calculations show that an effective power gain of about 2 db over simple majority decoding is achieved with APP decoding.

<u>Error Probabilities</u>

Def: $P_1(e)$ = average probability of incorrectly decoding block 0 from the first N_A code bits.

It can be shown [Massey - Sect 2.6] that with maximum likelihood decoding $P_1(e)$ approaches 0 exponentially with N_A for convolutional codes by random coding arguments. However, with threshold decoding it appears that this is not true [- ch V]! For one class of codes Massey has shown that $P_1(e) > \frac{1}{2}\left(\frac{p_0}{q_0}\right)^{\frac{[2p_0 + N_0 - 1]}{2p_0}}$. For a variety of other codes he has calculated $P_1(e)$ exactly by machine calculation for both APP and majority,

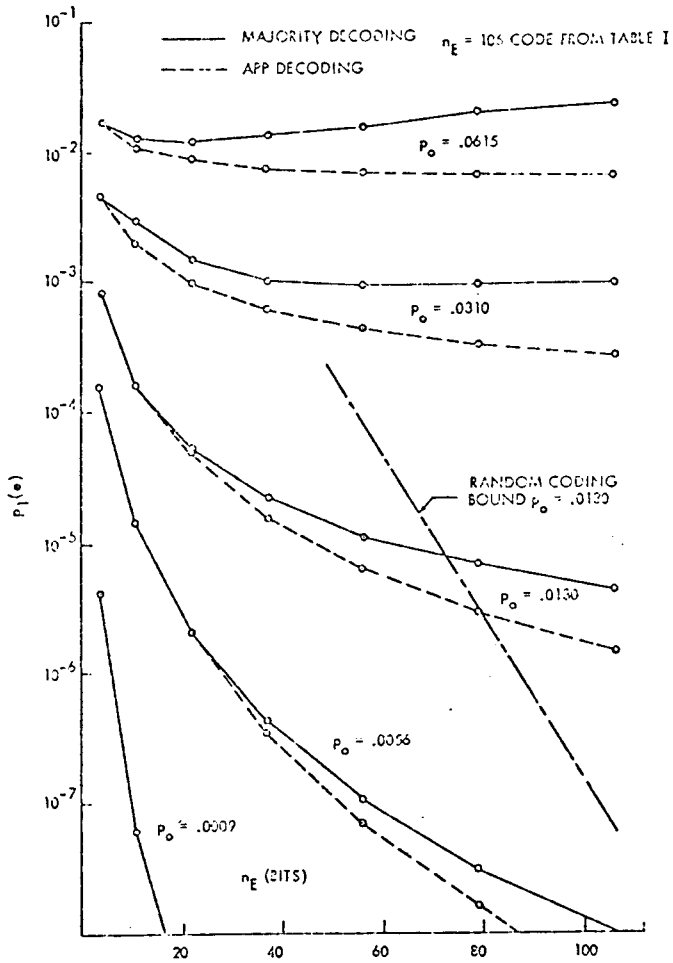


Fig. 16. Performance of R = 1/2 trial-and-error codes on the Binary Symmetric Channel.

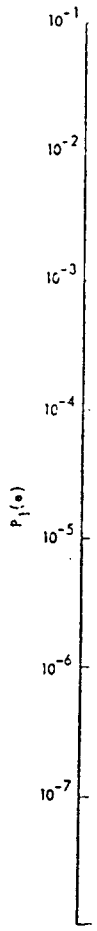


Fig. 17. Perfor
Channe

n_E = actual number of noise bits checked by $\{A_i\}$
= effective constraint length $\leq n_A$
P_o = transition probability for BSC

decoding. The accompanying figure shows typical results. n_E is the number of bits checked so that $n_E \le N_A$. With APP decoding $P_1(e)$ decreases monotonically with n_E but in majority decoding $P_1(e)$ reaches a minimum and eventually increases to 1/2. This indicates that threshold decoding is only useful at moderate constraint lengths.

4. Convolutional Codes for Threshold Decoding

a. Self Orthogonal Codes

a code is said to be self orthogonal if for each block zero information noise digit the set of syndrome digits checking that digit form an orthogonal set on that digit.

Consider the binary code with $R = 1/2$, $N_0 = 2$. Let

$$G_{(1)}^{(1)}(D) = 1, \quad G_{(1)}^{(2)}(D) = D^{d_0} + D^{d_1} + \cdots + D^{d_n}$$

with $0 \le d_0 < d_1 < \cdots < d_n$ and $\{d_i\}$ integers. Then

$$S^{(2)}(D) = G_{(1)}^{(2)}(D)\, E^{(1)}(D) + E^{(2)}(D)$$

$$= \left[D^{d_0} + D^{d_1} + \cdots + D^{d_n} \right] E^{(1)}(D) + E^{(2)}(D)$$

$$= \left[D^{d_0} + \cdots + D^{d_n} \right] \left[e_0^{(1)} + e_1^{(1)} D + \cdots \right] + \left[e_0^{(2)} + e_1^{(2)} D + \cdots \right]$$

The syndrome bits that check the block 0 information error digit $e_0^{(1)}$ are then

$$s_{d_0}^{(2)} = e_0^{(1)} + e_{d_0}^{(2)}$$

$$s_{d_1}^{(2)} = e_0^{(1)} + e_{d_1 - d_0}^{(1)} + e_{d_1}^{(2)}$$

$$\vdots$$

$$s^{(2)}_{d_n} = e^{(1)}_0 + e^{(1)}_{d_n - d_{n-1}} + \cdots + e^{(1)}_{d_n - d_0} + e^{(2)}_{d_n}$$

Each syndrome bit contains a different check noise bit $e^{(2)}_{d_j}$. The syndrome bit s_{d_j} contains the j information noise bits corresponding to the differences $\{ d_j - d_i ,\ i < j \}$ in addition to $e^{(1)}_0$. There are $1 + 2 + \cdots + n = \frac{1}{2} n(n+1)$ differences in these sets for $j = 1, \cdots, n$. The set of syndrome digits is orthogonal on $e^{(1)}_0$ if and only if ~~this set of~~ the differences are all distinct. If $d_0 \neq 0$ one would subtract d_0 from each d_i to produce a self-orthogonal code with the same set of differences but smaller memory.

A code was defined to be self orthogonal if the syndrome digits checking the <u>block 0</u> information noise digits formed orthogonal sets. However, for self orthogonal codes the set of syndrome digits which check <u>any</u> information error bit form an orthogonal set. Consider the $R = 1/2$, $N_1 = 2$ code. The syndrome digits checking $e^{(1)}_j$ are

$$s^{(2)}_{j+d_0} = e^{(1)}_j + \sum_{k=1}^{n} e_{j+d_0-d_k} + e^{(2)}_{j+d_0}$$

$$s^{(2)}_{j+d_1} = \sum_{k=0}^{n} e_{j+d_1-d_k} + e^{(2)}_{j+d_1}$$

$$\vdots$$

$$s^{(2)}_{j+d_n} = \sum_{k=0}^{n} e_{j+d_n-d_k} + e^{(2)}_{j+d_n}$$

where $e_j^{(1)} = 0$ if $j < 0$. If this set is not orthogonal, then for some $\alpha \neq \beta$ $(\alpha > \beta)$

$$\underbrace{j + d_\alpha - d_k}_{\text{in } S_{j+d_\alpha}} = \underbrace{j + d_\beta - d_\ell}_{\text{in } S_{j+d_\beta}}$$

or

$$d_\alpha - d_k = d_\beta - d_\ell$$

If $\alpha > k$ this is impossible since all positive differences distinct. If $\alpha < k$

$$d_\alpha - d_\beta = d_k - d_\ell > 0 \quad \text{since } \alpha > \beta$$

and also get contradiction. (for $\ell > k$ $d_k - d_\ell < 0$)

This implies that a majority decoder for a self orthogonal code can be used in either the feedback or definite mode with the same error correction radius.

A method for finding self-orthogonal codes described by Robinson is based on the concept of difference sets.

<u>Def: Difference Set</u>

A difference set of order $m+1$ and modulus N is a set $\{d_0, \dots, d_n\}$ of $n+1$ integers with $0 \leq d_0 < d_1 < \cdots < d_n < N$ such that $(d_j - d_i) \bmod N$ are all non-zero and distinct for $i \neq j$. There are $(n+1)n$ possible differences and the residues $(d_j - d_i) \bmod N$ are all between 0 and N for $i \neq j$. It is easy to show that $\alpha \bmod N \neq \beta \bmod N \Rightarrow \alpha \neq \beta$. If each residue is distinct then $N - 1 \geq (n+1)n$ or $N \geq n^2 + n + 1$. also each difference is distinct. A difference set of modulus $N = n^2+n+1$ is said to be perfect. It can be shown that perfect difference sets exist for every $n = p^r$ where p is prime and r is an integer and it is known that no other perfect

difference sets exist for $n < 1600$.

EX: The following two sets are perfect difference sets

$\{0, 1, 4, 6\}$ — $n = 3$, $N = 3^2+3+1 = 13$

$\{0, 3, 4, 9, 11\}$ — $n = 4$, $N = 21$

Thus every difference set describes an $R = 1/2$, $N_0 = 2$ binary code with $G^{(2)}_{(1)}(D) = \sum_{k=0}^{n} D^{d_k}$ that is self orthogonal. Perfect difference sets give self orthogonal codes with $J = n+1 = p^r$ with the shortest possible memory.

<u>Thm:</u> For self orthogonal codes with $R = 1/2$, $N_0 = 2$

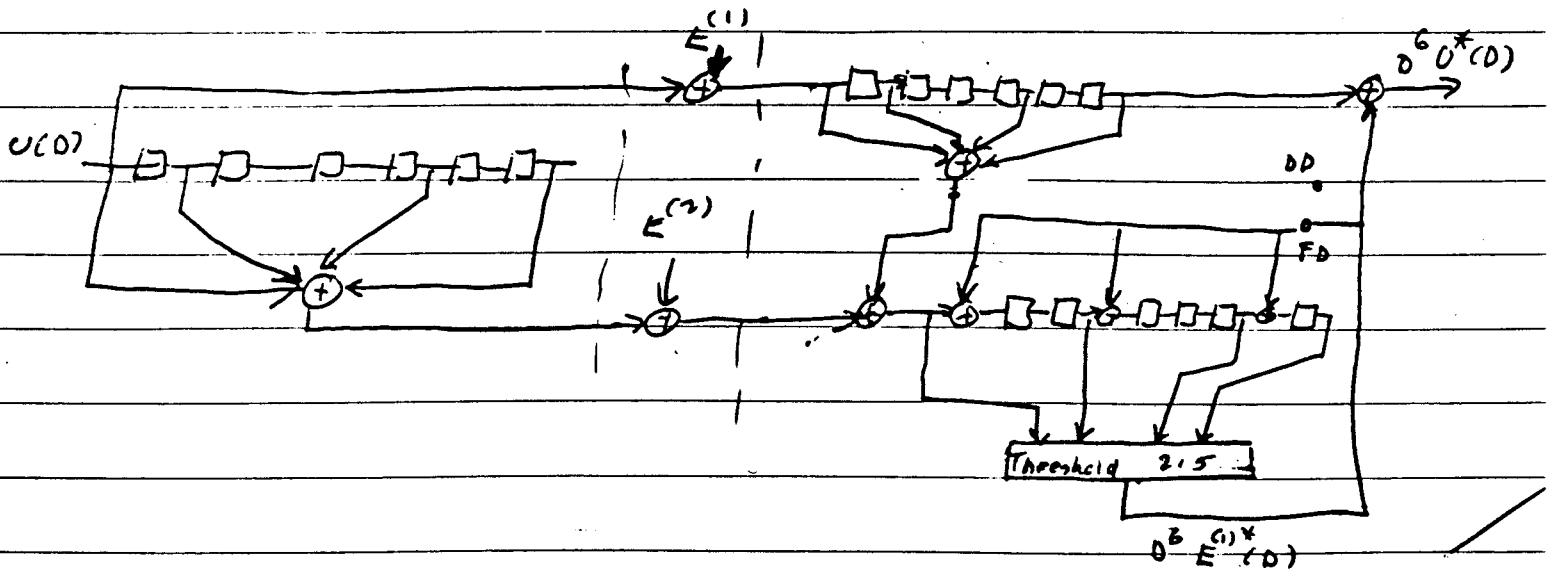
$d_{min} = J+1$

Proof: Always $d_{min} \geq J+1$. But $G^{(2)}_{(1)}(D)$ has only $J = n+1$ non-zero terms so that $U^{(1)}(D) = 1$ gives a code word with $J+1$ ones. Q.E.D.

Thus majority decoding is an efficient decoding scheme for self orthogonal codes.

EX: $R = 1/2$, $N_0 = 2$, perfect difference set $\{0, 1, 4, 6\}$

$G^{(2)}_{(1)}(D) = 1 + D + D^4 + D^6$



difference sets exist for $n < 1600$.

EX: The following two sets are perfect difference sets

$\{0, 1, 4, 6\}$ — $n = 3$, $N = 3^2+3+1 = 13$

$\{0, 3, 4, 9, 11\}$ — $n = 4$, $N = 21$

Thus every difference set describes an $R = 1/2$, $N_0 = 2$ binary code with $G^{(2)}_{(1)}(D) = \sum_{k=0}^{n} D^{\delta_k}$ that is self orthogonal. Perfect difference sets give self orthogonal codes with $J = n+1 = p^r$ with the shortest possible memory.

<u>Thm:</u> For self orthogonal codes with $R = 1/2$, $N_0 = 2$

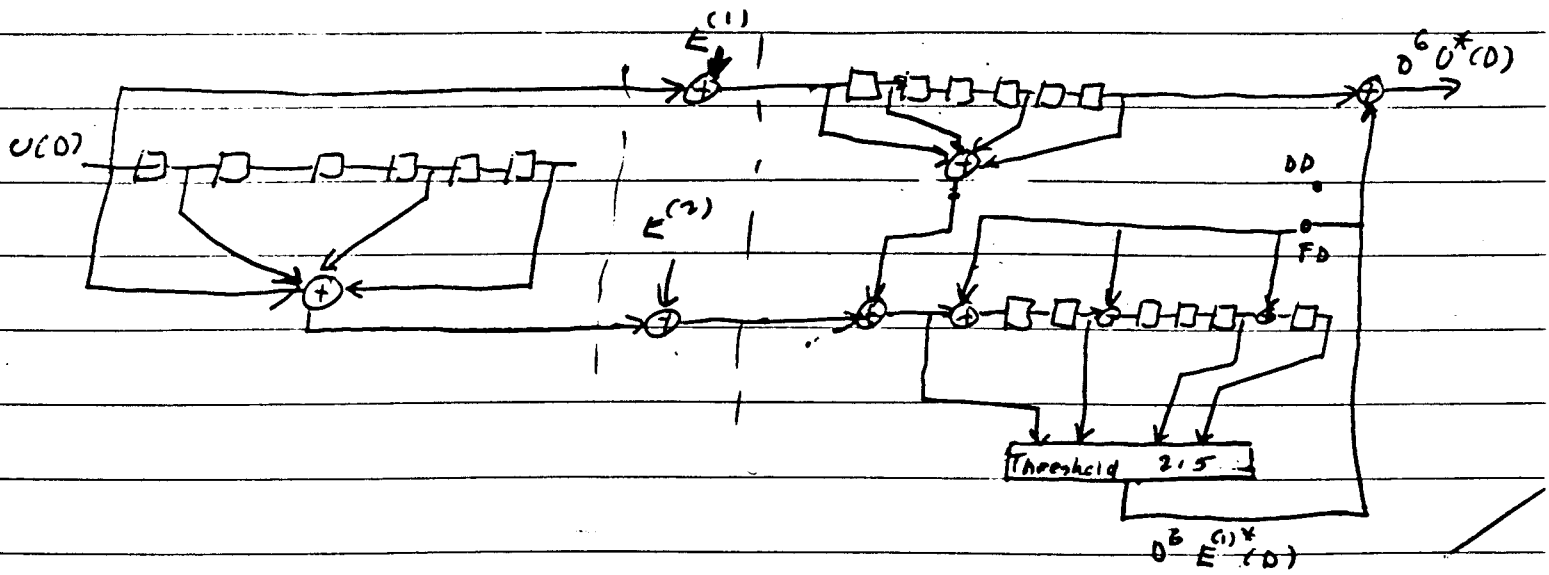
$d_{min} = J+1$

Proof: Always $d_{min} \geq J+1$. But $G^{(2)}_{(1)}(D)$ has only $J = n+1$ non-zero terms so that $U^{(1)}(D) = 1$ gives a code word with $J+1$ ones. Q.E.D.

Thus majority decoding is an efficient decoding scheme for self orthogonal codes.

EX: $R = 1/2$, $N_0 = 2$, Perfect difference set $\{0, 1, 4, 6\}$

$G^{(2)}_{(1)}(D) = 1 + D + D^4 + D^6$



(N_0, N_0-1) Self Orthogonal Codes

Let $G^{(N_0)}_{(1)}(D) = 1 + D^{d_{11}} + \cdots D^{d_{r1}}$

$$G^{(N_0)}_{(j)}(D) = 1 + D^{d_{1j}} + \cdots + D^{d_{rj}}$$

$$\vdots$$

$$G^{(N_0)}_{(N_0-1)}(D) = 1 + D^{d_{1(N_0-1)}} + \cdots + D^{d_{r(N_0-1)}}$$

and $d_{01} = d_{02} \cdots = d_{0(N_0-1)} = 0$

The syndrome digits that check $e_0^{(1)}$ are

$$s_0^{(N_0)} = e_0^{(1)} + e_0^{(2)} + \cdots + e_0^{(N_0-1)} + e_0^{(N_0)}$$

$$s_{d_{11}}^{(N_0)} = e_0^{(1)} + e_{d_{11}}^{(1)} + \sum_{\substack{i=0 \\ d_{i2} \le d_{11}}} e_{d_{11}-d_{i2}}^{(2)} + \cdots + \sum_{\substack{i=0 \\ d_{i(N_0-1)} \le d_{11}}} e_{d_{11}-d_{i(N_0-1)}}^{(N_0-1)} + e_{d_{11}}^{(N_0)}$$

$$s_{d_{21}}^{(N_0)} = e_0^{(1)} + e_{d_{21}-d_{11}}^{(1)} + e_{d_{21}}^{(1)} + \sum_{\substack{i=0 \\ d_{i2} \ge d_{21}}} e_{d_{21}-d_{i2}}^{(2)}$$

$$+ \cdots + \sum_{i=0} e_{d_{21}-d_{i(N_0-1)}}^{(N_0-1)} + e_{d_{21}}^{(N_0)}$$

$$\vdots$$

$$s_{d_{r1}} = \cdots + e_{d_{r1}}^{(N_0)}$$

as in the $(2,1)$ case, the $r(r+1)/2$ difference

$d_{j1} - d_{i1}$ for $0 \le i < j$ and $j = 1, \ldots, r$ (row)

must be distinct. In addition positive difference of the form $d_{j1} - d_{ik}$ (info. stream k) for $k \ne 1$ must be distinct (row j). Therefore

from j^{th} row $\rightarrow$ $d_{j1} - d_{ik} \ne d_{j'1} - d_{i'k}$ (from j'^{th} row) for $j' \ne j$, $k \ne 1$

or $d_{j1} - d_{j'1} \neq d_{ik} - d_{i'k}$

Therefore the differences in powers of D in the polynomials other than $G_{(1)}^{(N_0)}$ can not equal the $r(r+1)/2$ differences from $\{d_{01}, \cdots d_{r1}\}$. If a set of $(N_0-1)r$ numbers can be found such that this is true, then

$$\{ s_0^{(N_0)}, \cdots, s_{d_{r1}}^{(N_0)} \}$$

are a set of $J = r+1$ checks orthogonal on $e_0^{(1)}$.

Using the same reasoning, it follows that if the sets of $r(r+1)/2$ differences for

$$\{ d_{01}, d_{11}, \cdots, d_{r1} \}$$
$$\{ d_{02}, \cdots, d_{r2} \}$$
$$\vdots$$
$$\{ d_{0(N_0-1)} \cdots, d_{r(N_0-1)} \}$$

are all distinct and each set of differences contains different numbers, then

$$\{ s_0^{(N_0)}, s_{d_{1j}}^{(N_0)}, \cdots, s_{d_{rj}}^{(N_0)} \} \quad \text{for } 1 \leq j \leq N_0 - 1$$

form a set of $J = r+1$ checks orthogonal on $e_0^{(j)}$

Sets of integers with these properties are given by Weldon in:

R. Lucky, J. Salz, E. J. Weldon, <u>Principles of Data Communication</u>, McGraw-Hill, 1968 pp 407-408

for $R = 1/2, 2/3, 3/4, 4/5$

using threshold decoding $t = J/2$ so that $d_{min} \geq J+1 = r+2$. Let $U^{(1)}(D) = 1$, $U^{(2)}(D) = \cdots = U^{(N_0-1)}(D) = 0$. Then the corresponding code word has $x_0^{(1)} = 1$, $x_0^{(N_0)} = 1$, $x_{d_{11}}^{(N_0)} = 1$, $\ldots$, $x_{d_{r1}}^{(N_0)} = 1$ and all other x's $= 0$. Therefore

$d_{min} = J+1 = r+2$ and these codes are completely orthogonalizable.

Each set of differences has $r(r+1)/2$ numbers so that the largest number in the total set must be at least $(N_0-1)r(r+1)/2$ since there are (N_0-1) sets of differences. Thus

$$m \geq (N_0-1)\, r(r+1)/2 \quad \text{and}$$

$$N_A \geq N_0(m+1) \geq N_0\left[\frac{(N_0-1)r(r+1)}{2} + 1\right]$$

<u>Error Propagation in FB mode</u>

a threshold element will output a 1 if $T > J/2$ one's appear at its input. With no future channel errors, future syndromes are 0. The feedback connections complement the T one's and adds $r+1-T$ additional ones. Thus the weight of the syndrome vector changes (decreases) by $T-(r+1-T) = 2T-(r+1)$ $= 2T-J > 0$ for each 1 output. Therefore, the syndrome register will eventually clear to 0 with no future channel errors.

$(N_0, 1)$ Self Orthogonal Codes

Consider the code with generator polynomials

$$\bar{G}^{(1)}_{(1)}(D) = 1$$

$$\bar{G}^{(2)}_{(1)}(D) = G^{(N_0)}_{(1)}(D)$$

$$\vdots$$

$$\bar{G}^{(N_0)}_{(1)}(D) = G^{(N_0)}_{(N_0-1)}(D)$$

where $G^{(N_0)}_{(j)}$ $j = 1, \cdots, N_0-1$ are the generator polynomials for the (N_0, N_0-1) codes discussed previously. The resulting code has $J = (N_0-1)(r+1)$ checks orthogonal on $e_0^{(1)}$. Thus $d_{min} \geq J+1$. Let $C^{(1)}(D) = 1$. Then first constraint length of code word has $W(\xi) = 1 + (N_0-1)(r+1)$: so $d_{min} = J+1$ and code completely orthogonalizable

EX:

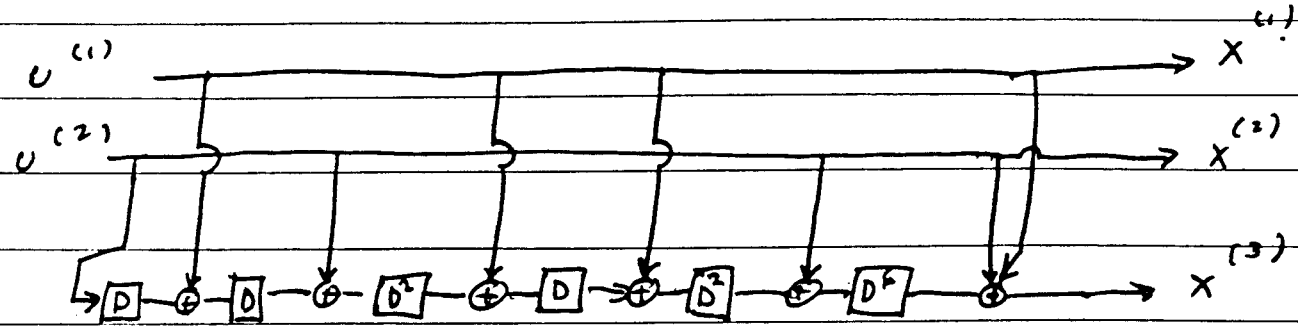
(a) $(3,2)$ code, $d = 5 \Rightarrow J = d-1 = 4$

consider sets $\{0, 8, 9, 12\}$, $\{0, 6, 11, 13\}$

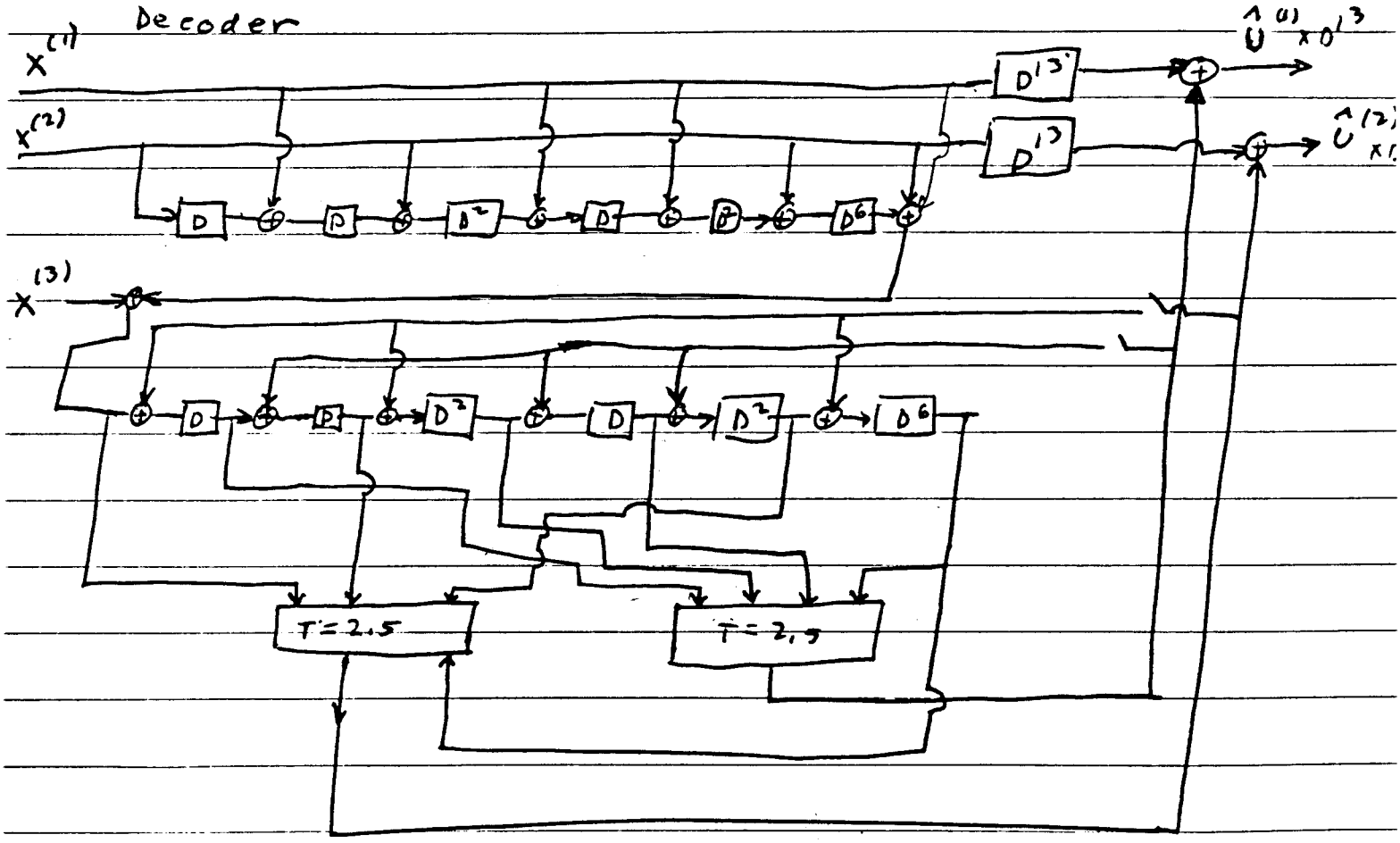
differences $r(r+1)/2 = 3(4)/2 = 6$

	0	8	9	12	0	6	11	13
$j=1$		8				6		
2		9	1			11	5	
3		12	4	3		13	7	2

encoder

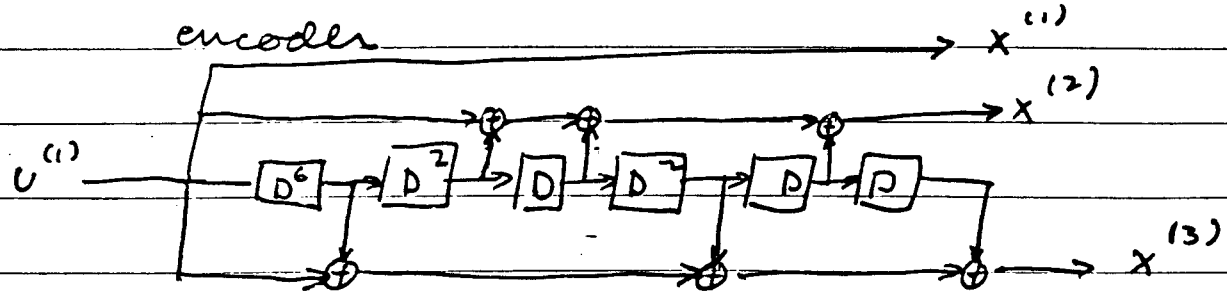


Decoder

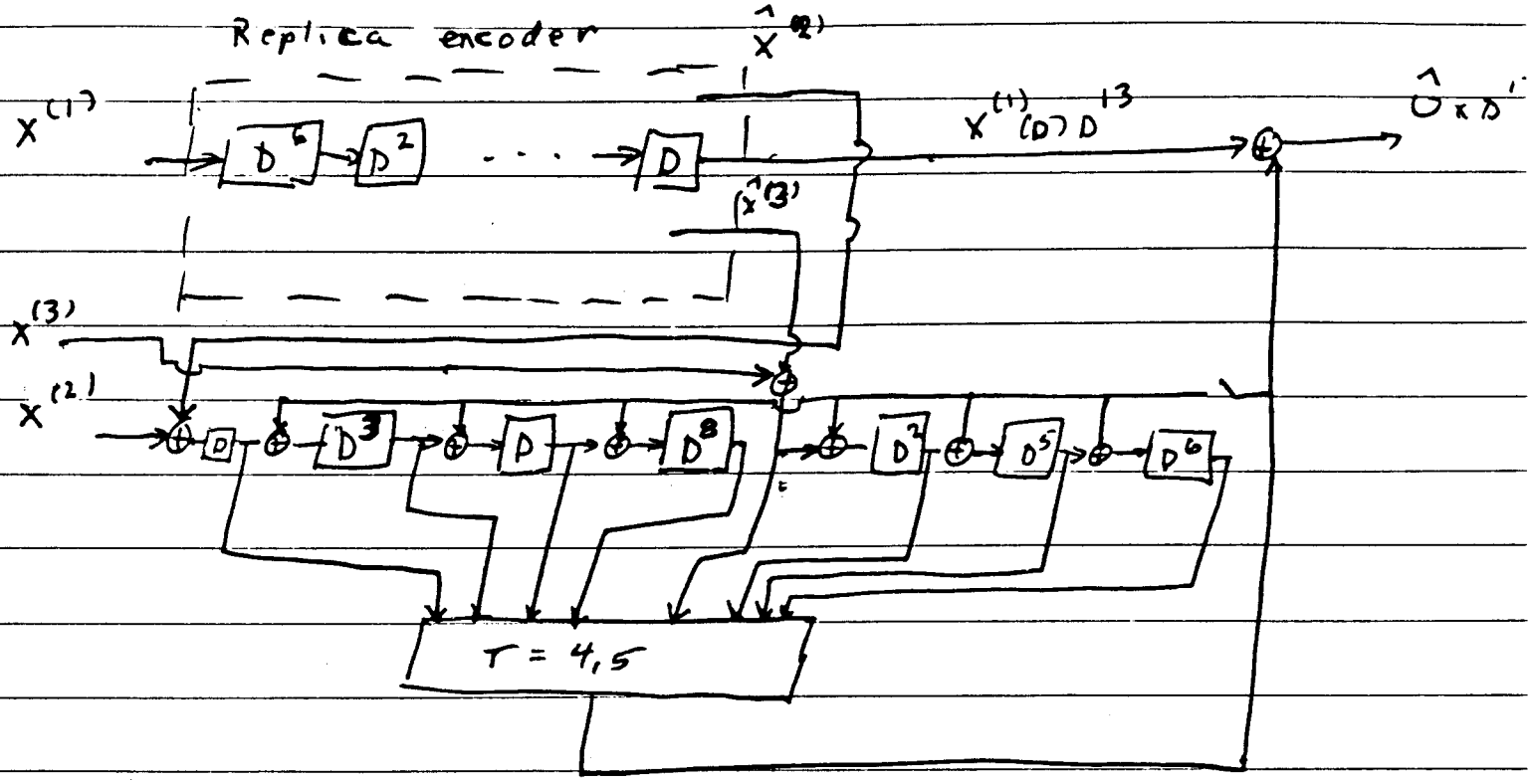


(b) (3, 1) Code, $J = 2 \times 4 = 8$

encoder



Decoder


Replica encoder
$\hat{x}^{(2)}$
$x^{(1)}$
D^6
D^2
D
$x^{(1)}(D)D^{13}$
$\hat{U}(D)$
$\hat{x}^{(3)}$
$x^{(3)}$
$x^{(2)}$
D
D^3
D
D^8
D^2
D^5
D^6
$T = 4,5$

In the FD mode whenever the threshold element emits a 1, the number of 1's stored in the syndrome register is reduced by at least two and this is true in general for self orthogonal codes. This ensures that this decoder has no noisy error propagation since if there are no channel errors after time j, then at time $j+m$ only 0's enter the syndrome register from the left. No matter what the contents of the register at time $j+m$, it will clear to all 0's soon since this occurs when the threshold element has no 1 outputs for m consecutive decisions. There can be only a finite number of 1 outputs because the number of 1's is reduced by at least 2 for each 1 output.

b. Uniform Codes

On page 60 it was shown that for convolutional codes $W_{avg} = \left(\frac{q-1}{q}\right)\left[N_A + \frac{N_0}{q^{K_0}-1}\right]$.

A class of convolutional codes will be presented here with $K_0 = 1$, $N_0 = q^m$ and $R = 1/q^m$ and $d_{min} = W_{avg} = \frac{(q-1)}{q}\left[(m+1) + \frac{1}{q-1}\right]q^m = \left[(q-1)(m+1)+1\right]q^m$

Let $G^{(1)}_{(1)}(D) = 1$ and $G^{(j)}_{(1)}(D) = 1 + g^{(j)}_{1(1)}D + g^{(j)}_{2(1)}D^2 + \cdots + g^{(j)}_{m(1)}D^m$

for $j = 1, \cdots, N_0 = q^m$ such that $[g^{(j)}_{1(1)}, \cdots, g^{(j)}_{m(1)}]$ for $j = 1, \cdots, N_0$ are all the distinct q^m m-tuples. Since $G^{(1)}_{(1)}(D) = 1$, the codes are systematic. With this convention, the $K_0 \times N_0$ matrices G_i on p. 33

are $1 \times (N_0 = q^m)$ row vectors

$$G_i = [\, g^{(1)}_{i(1)}, g^{(2)}_{i(1)}, \cdots, g^{N_0}_{i(1)} \,] \qquad i = 0, \cdots, m \,.$$

Since $G^{(j)}_{(1)}(D)$ has constant term 1 for all j

$$G_0 = [1, 1, \cdots, 1]$$

and $\quad g^{(1)}_{j(1)} = 0 \quad$ for $m \geq j \geq 1$

Consider code block m, then

$$\vec{x}_m = [\, u_0, u_1, \cdots, u_m \,] \begin{bmatrix} G_m \\ G_{m-1} \\ \vdots \\ G_0 \end{bmatrix}$$

and with the specified constraints on the G's

$$\vec{x}_m = [\, u_0, \cdots, u_m \,] \begin{bmatrix} 0 & \\ 0 & \\ \vdots & A_m \\ 0 & \\ \hline 1 & 1 \;\cdots\; 1 \end{bmatrix} \begin{matrix} \uparrow \\ m+1 \\ \downarrow \end{matrix}$$

$$\longleftarrow q^m \longrightarrow$$

where the columns of A_m are all the $q^m - 1$ distinct non-zero m-tuples over $GF(q)$. If $u_0 \neq 0$ and $u_m = 0$, then $[\, x^{(2)}_m, \cdots x^{(q^m)}_m \,]$ is a nonzero code word in a maximal length code and $x^{(1)}_m = 0$. Therefore $W(\vec{x}_m) = (q-1)q^{m-1}$. If $u_0 \neq 0$ and $u_m \neq 0$ then $[\, u_m, \cdots, u_m \,]$ is added to the maximal length code word. This changes to 0 only

those q^{m-1} positions that contain $-u_m$ but makes the q^{m-1} positions with zeros, non-zero so that $W(\vec{x}_m) = (q-1)q^{m-1}$ whenever $u_0 \neq 0$. Notice that $W(\vec{x}_0) = W(u_0, \ldots u_0) = q^m$ for $u_0 \neq 0$.

For $1 \leq j < m$

$$\vec{x}_j = [u_0, \ldots, u_j] \begin{bmatrix} 0 & 1 & & \\ \vdots & 1 & A_m(j) & \\ 0 & 1 & & \\ \hline 1 & 1 & \cdots & 1 \end{bmatrix}$$

where $A_m(j)$ is the last j rows of A_m. For $u_0 \neq 0$ this is equivalent to the case for $\vec{x}_m$ where $u_0 = u_1 = \ldots = u_{m-j-1} = 0$, $u_{m-j} \neq 0$, and $u_{m-j+1}, \ldots, u_m$ are arbitrary. Thus the analysis for $\vec{x}_m$ is directly applicable so that $W(\vec{x}_j) = (q-1)q^{m-1}$ for $u_0 \neq 0$. Combining these results

$$\underset{u_0 \neq 0}{W(\vec{x})} = q^m + m(q-1)q^{m-1} = q^{m-1}[(q-1)(m+1)+1]$$

<u>Decoding Binary Uniform Codes</u>

For $q = 2$, $W(\vec{x}) = 2^{m-1}(m+2) = d_{min}$

The decoding procedure will be illustrated by the following example. Consider the $R = 1/4$ binary uniform code with

$$G^{(1)}_{(1)}(D) = 1$$

$$G^{(2)}_{(1)}(D) = 1 + D$$

$$G^{(3)}_{(1)}(D) = 1 + D^2$$

$$G^{(4)}_{(1)}(D) = 1 + D + D^2$$

For this code $m=2$, $N_A = (m+1)N_0 = 12$, $d_{min} = 8$

The syndrome transforms are

$$S^{(j)}(D) = G^{(j)}_{(1)}(D)\,E^{(1)}(D) + E^{(j)}(D) \qquad j = 2, 3, 4$$

and at time k

$$s^{(j)}_k = \sum_{i=0}^{2} g^{(j)}_{i(1)}\, e^{(1)}_{k-i} + e^{(j)}_k$$

For feedback decoding the equations for the ~~modified~~ contents of the syndrome register used ~~syndromes at times $k, k+1, k+2 \equiv k+m$~~ for estimating $e^{(1)}_k$ can be written as

$$\begin{bmatrix} s'^{(2)}_k \\ s'^{(2)}_{k+1} \\ s'^{(2)}_{k+2} \\ \hline s'^{(3)}_k \\ s'^{(3)}_{k+1} \\ s'^{(3)}_{k+2} \\ \hline s'^{(4)}_k \\ s'^{(4)}_{k+1} \\ s'^{(4)}_{k+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} e^{(1)\Delta}_{k-2} \\ e^{(1)\Delta}_{k-1} \\ e^{(1)}_k \\ e^{(1)}_{k+1} \\ e^{(1)}_{k+2} \end{bmatrix} + \begin{bmatrix} e^{(2)}_k \\ e^{(2)}_{k+1} \\ e^{(2)}_{k+2} \\ e^{(3)}_k \\ e^{(3)}_{k+1} \\ e^{(3)}_{k+2} \\ e^{(4)}_k \\ e^{(4)}_{k+1} \\ e^{(4)}_{k+2} \end{bmatrix}$$

where $e^{(n)\Delta}_{\ell} = e^{(n)}_{\ell} - e^{(n)*}_{\ell}$

The three $(m+1) \times (2m+1)$ sub matrices in the first matrix after the equality sign on the right are known as "parity parallelograms". Assuming that all past decoding decisions have been correct, i.e., $e^{(n)\Delta}_j = 0$ for $j < k$, a set of checks orthogonal on

$e_k^{(1)}$ can be formed by the following rules:

(1) use first row in each "parity parallelogram

(2) use any other row which checks only one digit in $E^{(1)}(D)$ other than $e_k^{(1)}$

(3) add to any other row that checks $e_k^{(1)}$ and at least two other digits in $E^{(1)}(D)$ that <u>unique</u> row which checks the same other digits in $E^{(1)}(D)$ but not $e_k^{(1)}$.

For the example above this results in the following set of parity checks:

$$
(1)\begin{cases}
s_k'^{(2)} = e_{k-1}^{(1)\Delta} + e_k^{(1)} + e_k^{(2)} \\
s_k'^{(3)} = e_{k-2}^{(1)\Delta} + e_k^{(1)} + e_k^{(3)} \\
s_k'^{(4)} = e_{k-2}^{(1)\Delta} + e_{k-1}^{(1)\Delta} + e_k^{(1)} + e_k^{(4)}
\end{cases}
$$

$$
(2)\begin{cases}
s_{k+1}'^{(2)} = e_k^{(1)} + e_{k+1}^{(1)} + e_{k+1}^{(2)} \\
s_{k+2}'^{(3)} = e_k^{(1)} + e_{k+2}^{(1)} + e_{k+2}^{(3)}
\end{cases}
$$

$$
(3)\begin{cases}
s_{k+1}'^{(3)} + s_{k+1}'^{(4)} = e_k^{(1)} + e_{k+1}^{(3)} + e_{k+1}^{(4)} \\
s_{k+2}'^{(4)} + s_{k+2}'^{(2)} = e_k^{(1)} + e_{k+2}^{(4)} + e_{k+2}^{(2)}
\end{cases}
$$

This gives $J = 7 = d_{min} - 1$ checks orthogonal on $e_k^{(1)}$ so that the code is completely orthogonalizable.

For any uniform code the procedure outlined above always results in $d_{min} - 1$ checks orthogonal on $e_k^{(1)}$.

<u>Proof</u>: Consider the last row of each parity parallelogram. Each row ends in a 1. Since $G_{(i)}^{(j)}(D) = 1 + g_{1(i)}^{(j)} D + \cdots + g_{m(i)}^{(j)} D^m$

for $j = 2, \cdots, 2^m$ correspond to all 2^m possible polynomials except $G_{(1)}^{(1)}(0) = 1$, 2^{m-1} of the rows have a 1 in the position corresponding to $e_k^{(1)}$. Except for the row $[0, \cdots, 0, 1, 0, \cdots 0 1]$, there is a row identical to one with a 1 in the position corresponding $e_k^{(1)}$ except for a 0 in the position corresponding to $e_k^{(1)}$. If these rows are added pairwise, they form a set of $2^{m-1}-1$ orthogonal checks on $e_k^{(1)}$. Each checks only $e_k^{(1)}$ and two corresponding check noise bits. The row $[0, \cdots, 0, 1, 0, \cdots 0, 1]$ must be taken alone since $[0, \cdots 0, 1]$ is not an allowable row. This results in a check on $e_k^{(1)}$, $e_{k+m}^{(1)}$ and the corresponding check noise bit. All these together form a set of 2^{m-1} checks orthogonal on $e_k^{(1)}$. The same analysis can be applied to the set of $m-1$ st rows. Only $[0, \cdots 0, 1, 0, \cdots 0, 1, 0]$ is taken alone and this checks $e_k^{(1)}$, $e_{k+m-1}^{(1)}$ and a check noise bit. The others only check $e_k^{(1)}$ and a check noise bit. This set together with the set for the mth rows form a set of $2 \times 2^{m-1}$ checks orthogonal on $e_k^{(1)}$. The same reasoning holds for all but the 1st rows. Each first row only checks $e_k^{(1)}$ and a check noise bit. Therefore the total number of resulting checks is

$$J = m(2^{m-1}) + \underbrace{(2^m - 1)}_{N_0 - 1 \ 1^{st} \text{ rows}} = 2^{m-1}(m+2) - 1 = d_{min} - 1$$

Q.E.D.

Notice that by this construction every information and check noise bit is checked by the resulting set.

Def: Effective constraint length N_E

The effective constraint length, N_E, is the total number of distinct bits checked by the orthogonal parity checks.

Therefore, for uniform codes $N_E = N_A$.

Error Propagation

Previous decoding errors only affect the $N_0 - 1$ checks corresponding to the first rows of the parity parallelograms due to the method of constructing the set of J checks. For the example we have been considering

$$[s_k'^{(2)}, s_k'^{(3)}, s_k'^{(4)}] = [e_{k-2}^{(1)\Delta} \quad e_{k-1}^{(1)\Delta}] \underbrace{\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}}_{A_2} + \text{other term}$$

Notice that A_2 generates a maximal length block code with the weight of all non-zero words equal to 2. Therefore a previous decoding error causes exactly two of the 7 orthogonal checks to be complemented. This is equivalent to receiving two channel errors that affect different checks. Since $d_{min} = 8$, one real channel error in $[\vec{y}_k, \ldots \vec{y}_{k+m}]$ can be corrected in addition. Thus in addition to no noisy error

propagation, some channel errors can still be corrected when previous decoding errors have been made. In general past decoding errors among $[e^{(1)\Delta}_{k-m}, \ldots, e^{(1)\Delta}_{k-1}]$ act as exactly 2^{m-1} channel errors, each in a different check. Since $d_{min} = (m+2)2^{m-1}$, $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = m2^{m-2} + 2^{m-1} - 1$ errors can be corrected with no previous decoding errors. With previous decoding errors only $m2^{m-2} - 1$ channel errors or less are guaranteed to be corrected.

References for Deterministic Decoders

1. J.L. Massey, Threshold Decoding, --
2. J.P. Robinson, "Error Propagation and Definite Decoding of Recurrent Codes," Digital Systems Lab Report 47, Princeton Univ., Dept. of EE., 1965.
3. J.P. Robinson, "Self Orthogonal Codes," Digital Systems Lab Report 43, Princeton, 1965.
4. Massey, "Uniform Codes," IEEE Trans. of Info. Th., IT-12, pp. 132-134, April 1966
5. D.D. Sullivan, "Control of Error Propagation in Convolutional Codes," Ph D Thesis, U. of Notre Dame, Dept of E.E., June 1966.
6. Massey, "Advances in Threshold Decoding," in Advances in Communication Systems, (Editor Balakrishnan), Academic Press, vol. 3.

Lucky, Saltz + Weldon

degree i produces another
plementation of the inter-
that of the basic code, ex-
t registers are roughly i

blem of correcting errors
ese codes are not as well
any of the basic properties
ery simply; (2) decoding is
ral classes of codes have
ding equipment required is
which are capable of cor-
oth. As with block codes,
codes are less well under-
an burst-correcting codes.
ock codes in that, because
ent, it is much more diffi-
for the probability of de-
ast decoding error tends to
roneous as well. That is,
ly, for most of the prac-
quite brief and consequently

ional codes was mentioned,
neral and powerful technique
ncy and low error rate must

gh not as well developed and
des, are competitive with the

the important parameters of
onvolutional codes. The fol-
ables:

sets of integers which specify

cting ability of the code

Table 12.2. Self-orthogonal Codes.[a]

$n_0 = 2$

$R = 1/2$ d	n	Sets of integers that specify code
3	4	(0, 1)
5	14	(0, 2, 5, 6)
7	36	(0, 2, 7, 13, 16, 17)
9	72	(0, 7, 10, 16, 18, 30, 31, 35)
11	112	(0, 2, 14, 21, 29, 32, 45, 49, 54, 55)
13	172	(0, 2, 6, 24, 29, 40, 43, 55, 68, 75, 76, 85)
15	256	(0, 5, 28, 38, 41, 49, 50, 68, 75, 92, 107, 121, 123, 127)
17	360	(0, 6, 19, 40, 58, 67, 78, 83, 109, 132, 133, 162, 165, 169, 177, 179)
19	434	(0, 2, 10, 22, 53, 56, 82, 83, 89, 98, 130, 148, 153, 167, 188, 192, 205, 216)
21	568	(0, 24, 30, 43, 55, 71, 75, 89, 104, 125, 127, 162, 167, 189, 206, 215, 272, 275, 282, 283)

$n_0 = 3$

$R = 1/3$ d	$R = 2/3$ d	n	Sets of integers that specify code
5	3	9	(0, 1)
			(0, 2)
9	5	42	(0, 8, 9, 12)
			(0, 6, 11, 13)
13	7	123	(0, 2, 6, 24, 29, 40)
			(0, 3, 15, 28, 35, 36)
17	9	261	(0, 1, 27, 30, 61, 73, 81, 83)
			(0, 18, 23, 37, 58, 62, 75, 86)
21	11	393	(0, 1, 6, 25, 32, 72, 100, 108, 120, 130)
			(0, 23, 39, 57, 60, 74, 101, 103, 112, 116)

$n_0 = 4$

$R = 1/4$ d	$R = 3/4$ d	n	Sets of integers that specify code
7	3	16	(0, 1)
			(0, 2)
			(0, 3)
13	5	80	(0, 3, 15, 19)
			(0, 8, 17, 18)
			(0, 6, 11, 13)
19	7	272	(0, 5, 15, 34, 35, 42)
			(0, 31, 33, 44, 47, 56)
			(0, 17, 21, 43, 49, 67)

Table 12.2 Self-orthogonal Codes.[a] (Continued)

$R = 1/4$ d	$R = 3/4$ d	n	Sets of integers that specify code
			$n_0 = 4$ (continued)
25	9	520	(0, 9, 33, 37, 38, 97, 122, 129)
			(0, 11, 13, 23, 62, 76, 79, 123)
			(0, 19, 35, 50, 71, 77, 117, 125)
			$n_0 = 5$
$R = 1/5$ d	$R = 4/5$ d	n	Sets of integers that specify code
9	3	25	(0, 1)
			(0, 2)
			(0, 3)
			(0, 4)
17	5	145	(0, 1, 26, 28)
			(0, 3, 13, 24)
			(0, 7, 19, 23)
			(0, 8, 17, 22)
25	7	490	(0, 22, 41, 57, 72, 93)
			(0, 14, 17, 61, 87, 95)
			(0, 39, 49, 51, 62, 69)
			(0, 9, 33, 37, 38, 97)

[a]This table is taken from the more complete version given in Robinson and Bernstein.[8] For a discussion of the codes tabulated here, see Sec. 12.2.2.

Table 12.3 lists orthogonalizable codes of efficiency 1/2 and 1/3 for various values of minimum distance. It is taken from Table II of Ref. [2]* where codes of efficiency 1/5 and 1/10 are also listed. For a discussion of these codes see Sec. 12.2.3.

Along with the usual parameters of d and n, the basic parity-check matrix $\mathbf{h}$ of each code is given. To save space it is given in the following form. Each row of the $(n_0 - 1)$-row matrix is given on a set of integers corresponding to the blocks in which a nonzero term appears in that row. The $n_0 - 1$ sets are distinguished by an exponent corresponding to the row number. Thus the matrix

$$\mathbf{h} = \begin{bmatrix} 000 & 000 & 000 & 100 & 110 \\ 100 & 100 & 100 & 000 & 101 \end{bmatrix}$$

* By permission of J. L. Massey.[9]

d	n	S
3	4	(0, 1
5	12	(0, 3
7	24	(0, 6
9	44	(0, 1
11	72	(0, 18
13	104	(0, 26

d	n	Set
3	3	(0)(0)[1]
5	9	(0, 1)[1]
7	15	(0, 1)[1]
9	24	(0, 1, 7
11	33	(0, 1, 9
13	54	(0, 1, 2, (0, 4, 5, (0, 1, 14

is represente
ways 1 and is
The inform
codes, that is,
check sums (f
table. Each s
parity-check r
of the orthog
number (base)
tion rules for
$(2^1, 4^2)$. Its pari

TABLE I
IMPROVEMENTS ON AND ADDITIONS TO TABLE OF DIFFERENCE TRIANGLES*

r	J	Number of Elements	Maximum Element	First Rows of Triangles
3	5	30	36	(3, 10, 11, 12)(15, 14, 2, 4)(7, 18, 1, 8)
4	5	40	50	(14, 20, 13, 3)(30, 5, 6, 4)(18, 7, 19, 2)(8, 9, 22, 1)
5	2	5	5	(1)(2)(3)(4)(5)
	3	15	15	(1, 7)(6, 5)(10, 4)(3, 9)(2, 13)
	4	30	32	(1, 14, 16)(4, 8, 13)(7, 2, 18)(5, 6, 17)(10, 19, 3)
	5	50	63	(1, 21, 6, 33)(5, 9, 10, 30)(11, 4, 31, 17)(2, 23, 20, 12)(8, 26, 3, 13)
	6	75	104	(38, 2, 22, 9, 30)(10, 4, 7, 67, 15)(6, 41, 17, 1, 35)(5, 23, 20, 12, 41)(46, 8, 26, 3, 13)
6	2	6	6	(1)((2)3)(4)(5)(6)
	3	18	19	(3, 16,)(4, 13)(1, 14)(2, 7)(10, 8)(5, 6)
	4	36	40	(3, 16, 12)(20, 10, 8)(22, 4, 13)(1, 14, 21)(29, 5, 6)(23, 2, 7)
	5	60	76	(27, 29, 5, 6)(24, 22, 4, 13)(20, 10, 8, 33)(1, 14, 21, 37)(13, 23, 2, 7)(45, 3, 16, 12)
	6	90	125	(42, 45, 3, 16, 12)(49, 43, 23, 2, 7)(1, 14, 21, 37, 47)(20, 10, 8, 33, 52)(55, 27, 29, 5, 6) (62, 24, 22, 4, 13)
7	2	7	7	(1)(2)(3)(4)(5)(6)(7)
	3	21	22	(3, 16)(4, 14)(15, 5)(7, 10)(13, 9)(11, 1)(6, 2)
	4	42	47	(3, 16, 23)(21, 13, 9)(29, 4, 14)(25, 11, 1)(15, 5, 26)(2, 6, 24)(7, 10, 28)
	5	70	89	(38, 10, 7, 28)(2, 6, 24, 56)(36, 31, 9, 13)(5, 15, 27, 37)(21, 4, 14, 43)(3, 16, 33, 26) (11, 1, 50, 23)
	6	105	146	(2, 6, 24, 56, 54)(3, 16, 33, 26, 68)(11, 1, 50, 23, 46)(21, 4, 14, 43, 44)(5, 15, 27, 37, 60) (58, 38, 10, 7, 28)(41, 36, 31, 9, 13)

* Only the first row of each triangle is given. use of tables let row of triangle $(\alpha_1, \alpha_2, \alpha_k)$

Then $\alpha_1 = d_1 - d_0$, $\alpha_2 = d_2 - d_1$ $\alpha_j = d_j - d_{j-1}$ ...

so choose $d_0 = 0$, $d_1 = \alpha_1$, $d_2 = \alpha_2 + \alpha_1$, $d_j = \alpha_j + d_{j-1}$, ...

first column of each triangle is the largest number in the triangle) of a set of triangles be as low as possible so that the decoder for the code derived from the triangles will have minimum constraint length. Hence, the construction of difference triangles is a problem that involves the construction of good self-orthogonal codes.

The method employed in constructing the difference triangles presented here was to begin with a set of "poor" triangles generated by computer and work the greatest number down by the following method. Remove the triangle containing the greatest number and construct by hand a new triangle with a lower greatest number with the numbers of the first triangle and the other unused numbers. In addition, a certain amount of borrowing from complete triangles before they are dissolved may be necessary. In other words, instead of relying on numbers not already contained in existing triangles, numbers from existing triangles must be borrowed with the idea that the triangles borrowed from will be reconstructed without the use of the borrowed numbers. It is this necessity that renders this method unwieldy for constructing very large triangles; for when working with more than about 250 numbers at once, there are too many possibilities to explore by hand and too many opportunities to run up against dead ends for this method to be productive. However, it has served well in obtaining the results presented here.

The tables of Robinson and Bernstein can be found in their paper together with instructions for the construction of self-orthogonal codes from difference triangles. Two of their results are improved: those for $r = 3$, $J = 5$, a decrease of 5 in the maximum element from 41 to 36; and for $r = 4$, $J = 5$, a decrease from 53 to 50. New triangles are given for $r = 5$, 6 and 7, and for $J = 2$ to 6.

E. J. KLIEBER[2]
Bell Telephone Laboratories, Inc.,
Holmdel, N. J. 07733

[2] Now a sophomore at the University of Chicago, Chicago, Ill.

Further Results on the Synchronization of Binary Cyclic Codes

and $g(D) = 1 + D^{d_1} + \cdots + D^{d_j} + \cdots + D^{d_r}$

Abstract—It is shown that certain coset codes derived from binary cyclic codes can determine the magnitude of a synchronization error, as well as its direction by examining only the syndrome of the received n tuple. For such coset codes, therefore, the need for a search procedure to recover synchronism is eliminated. In addition, the range of slip that can be detected and corrected for noisy channels is extended.

INTRODUCTION

The problem of loss of synchronization, or slip, for binary cyclic codes has recently attracted interest [1]–[6], [8]–[10]. One of the known techniques for obtaining codes capable of detecting and correcting synchronization error is to form a coset code [1]–[4] from a given (n, k) binary cyclic code by adding a fixed polynomial to each code word before transmission. In a previous paper [4], the ability of such coset codes to detect and correct synchronization error was examined by using the vector–matrix representation of cyclic codes. This correspondence derives some new results on the same problem by using the polynomial representation of cyclic codes as used in [3]. In particular, it is shown that there exist (n, k) coset codes that can determine both the magnitude and direction of the slip by examining only the syndrome of the received n tuple. Hence, unlike previous procedures for coset codes [3], [4], the present method does not require any search procedure. In passing, it may be mentioned that some other techniques also possess this feature [5], [6].

Except for some changes in notation, the formulation of the polynomial approach to slip will follow Tong [3]. Fig. 1 illustrates a left slip of s digits, where $A(x)$, $B(x)$, and $D(x)$ are any three consecutive coset code words. If there were no slip, the receiver

Manuscript received August 1, 1968; revised August 20, 1969. This work was supported in part by the National Research Council of Canada under Grant A-2735. Much of this correspondence was presented at the 2nd Annual Princeton Conference on Information Sciences and Systems, March 1968.