V. Burst Error Correcting Codes

A. as before codewords will be denoted $\bar{X}$, received words $\bar{y}$, and error sequences $\bar{E}$.

Def: a set of consecutive noise symbols $e_n, \ldots, e_{n+b-1}$ is a burst of errors relative to a guard space g if

(1) e_n and $e_{n+b-1} \neq 0$

(2) g consecutive digits on each side of the burst are 0

(3) There is no consecutive sequence of g 0's in the set $e_n, \ldots, e_{n+b-1}$

The length of the burst is b

Def: an encoder and decoder is said to have burst correcting capability b relative to guard space g if b is the largest integer for which every noise sequence $\bar{E}$ containing only bursts of length b or less relative to guard space g is correctly decoded.

Theorem 21 Gallager Bound

Let a sequence of source symbols be encoded into channel symbols by a code with R = source symbols/channel symbol. Then, in order for an encoder of bounded decoding delay and rate $R > 0$ to have a burst correcting capability b relative to a guard space g it is necessary

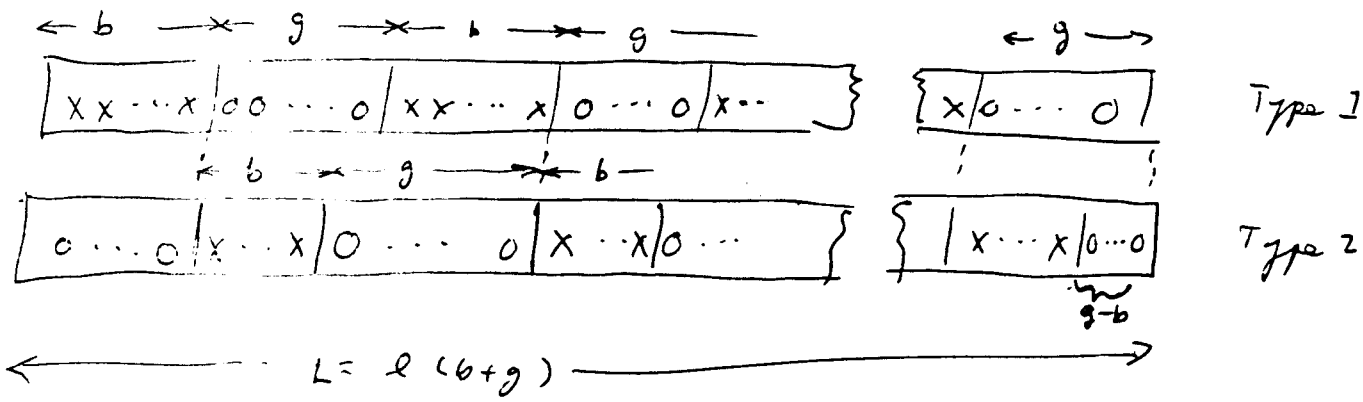
to have

$$\frac{g}{b} \geq \frac{\log_q(s) + R}{\log_q(s) - R} = \frac{1+\mathcal{R}}{1-\mathcal{R}}$$

where there are s letters in the code alphabet and q letters in the source alphabet, $\mathcal{R} = \frac{R}{\log_q s}$

Proof: Assume that there is a decoding delay of N source digits. Thus for $n > N$, by the time the nth source digit enters the encoder at least $n - N$ source digits must be decoded. If $R =$ source digits/channel digit, this is the same as requiring that by the time L channel digits have been received at least $RL - N$ source digits must be decoded. Suppose we are using a code that has burst correcting capability b relative to guard space g and let $L = \ell(b+g)$.

Consider the two types of noise sequences diagrammed below:



The errors must be 0 in the positions shown and arbitrary in the X positions. Let $\vec{X}_1$ and $\vec{X}_2$ be encoded sequences corresponding to different

choices of the first $RL-N$ source digits and $\vec{E}_1$ and $\vec{E}_2$ be errors of Type 1 and Type 2 respectively. By assumption these errors cannot cause incorrect decoding so that

$$\vec{X}_1 + \vec{E}_1 \neq \vec{X}_2 + \vec{E}_2$$

More generally if $\vec{E}_1$ and $\vec{E}_1'$ are errors of the first type and $\vec{E}_2$ and $\vec{E}_2'$ are errors of the second type, then

$$\vec{X}_1 + \vec{E}_1 + \vec{E}_2 \neq \vec{X}_2 + \vec{E}_1' + \vec{E}_2' \quad \text{because}$$

assume that this is true with equality, then

$$\vec{X}_1 + \vec{E}_1 - \vec{E}_1' = \vec{X}_2 + \vec{E}_2' - \vec{E}_2$$

but $\vec{E}_1 - \vec{E}_1'$ is a Type 1 error and $\vec{E}_2' - \vec{E}_2$ is a type 2 error so that there is a contradiction. Finally if $\vec{X}_1$ and $\vec{X}_2$ are equal and correspond to the same first $RL-N$ source digits but if either $\vec{E}_1 \neq \vec{E}_1'$ or $\vec{E}_2 \neq \vec{E}_2'$ then the inequality is also true.

Let the source have an alphabet of q letters. Therefore there are $q^{RL-N} = q^{Rl(g+b)-N}$ ways of choosing $\vec{X}_1$, one for each choice of the first $RL-N$ source digits. Similarly there are $q^{lb} = q^{lb \log_q s}$ ways of choosing $\vec{E}_1$ and $q^{lb} = q^{lb \log_q s}$ ways of choosing $\vec{E}_2$. Thus each choice of $(\vec{X}_1, \vec{E}_1, \vec{E}_2)$ leads to a different sequence $\vec{X}_1 + \vec{E}_1 + \vec{E}_2$. There are $s^{l(b+g)}$ sequences of length $l(b+g)$ so ~~that~~

$$q^{R\ell(b+g)-N}\, q^{\ell b}\, q^{\ell b} \le q^{\ell(b+g)}$$

$$q^{R\ell(b+g)-N}\, q^{\ell b \log_q s} \le q^{\ell g \log_q s}$$

$$R\cdot(b+g) - \frac{N}{\ell} + b\log_q s \le g \log_q s$$

or $\cancel{R(b+g) - \frac{N}{\ell} + 2b \le b+g}$

This is true for all $\ell \ge 1$ so that in limit as $\ell \to \infty$ $R(b+g) + b\log_q s \le g \log_q s$

$\cancel{R(b+g) + 2b \le b+g}$

or

$$\frac{g}{b} \ge \frac{\log_q(s) + R}{\log_q(s) - R}$$

Q.E.D.

<u>Remarks</u>: This bound is valid for block, convolutional, or any other type of coding scheme. The bound can be reached by convolutional codes.

EX. Consider $R = 1/2$ binary codes. Then

$$g \ge \frac{1+1/2}{1-\frac{1}{2}}\, b = 3b$$

B. <u>Cyclic Burst Error Correcting Codes</u>

For cyclic codes it is convenient to define a burst in a slightly different way to account for the cyclic code properties. For an error sequence $\vec{E} = [e_0, e_1, \ldots, e_{N-1}]$ we find the longest cyclically consecutive run of 0's and consider the rest of the block to be a burst. If a burst does not contain both e_0 and e_{N-1} it is called an <u>ordinary</u> burst. Otherwise it

will be called an end around burst.

EX

[1 0 ... 0 1] is an end around burst of length $b=2$. [0 ... 0 1 1 0] is an ordinary burst of length 2.

For cyclic codes, if an ordinary burst can be corrected by the code, an end-around burst of the same length can also be corrected since the received word can be cyclically shifted to result in a new codeword and an ordinary burst.

Theorem 22

A necessary but not sufficient condition for a cyclic code to correct all bursts of length b or less is that $2b \leq \deg g(D)$, i.e., the number of check symbols must be at least twice the burst length.

Proof:

Let $\deg g(D) = r$. If $r < 2b$ it will be shown that two burst of length b or less have the same syndrome and therefore cannot be uniquely corrected.

Let $g(D) = g_0 + g_1 D + \cdots + g_{b-1} D^{b-1} + g_b D^b + \cdots + D^r$

Define $E_1(D) = g_0 + \cdots + g_{b-1} D^{b-1}$ and

$E_2(D) = -D^b (g_b + \cdots + D^{r-b})$

Then $E_1(D) - E_2(D) = g(D)$ and

$$E_1(D) = g(D) + E_2(D)$$

so that $E_1(D) \bmod g(D) = E_2(D) \bmod g(D)$

and the bursts E_1 and E_2 have the same syndromes.

→ <u>Theorem 23</u>

A cyclic code can detect any burst of length r or less if $\deg g(D) = r$.

Proof:

Let $E(D) = \{ D^k [b_0 + b_1 D + \cdots b_{r-1} D^{r-1}] \} \bmod (D^N - 1)$

i.e., $E(D)$ is some cyclic permutation of $b_0 + b_1 D + \cdots + b_{r-1} D^{r-1}$. Then

$$E(D) \bmod g(D) = [D^k (b_0 + \cdots + b_{r-1} D^{r-1}) - f(D)(D^N - 1)] \bmod g(D)$$

$$= \{ D^k (b_0 + \cdots + b_{r-1} D^{r-1}) \} \bmod g(D)$$

but $g(D)$ does not divide D^k or $b_0 + \cdots + b_{r-1} D^{r-1}$

QED.

<u>Theorem 24</u>

A necessary but not sufficient condition for a cyclic code to correct all burst of length b or less is that

$$\deg g(D) \geq \log_q [1 + N q^{b-1} (q-1)]$$

<u>Proof:</u>

Each correctable error must correspond to a distinct syndrome so that

$$q^r \geq \text{no. correctable error patterns}$$

or $r \geq \log_q (\text{no. correctable error patterns})$

The number of correctable error patterns is determined as follows: There is 1 no error pattern. For any correctable pattern the first error can occur in any of N positions and can take on $q-1$ values. The remaining $b-1$ positions can take on any of q values. Thus there are $N q^{b-1}(q-1)$ burst patterns of length b or less so $r \geq \log_q [1 + N q^{b-1}(q-1)]$

Q.E.D.

Maximum Likelihood Burst Error Correction

It will be assumed that the channel is such that bursts of smaller length (regular or end-around bursts) are more likely. The maximum likelihood decoder would then calculate

$$E_i(D) = y(D) - X_i(D) \quad \text{for } i = 1, \cdots, q^k$$

and choose the $X_i(D)$ resulting in the $E(D)$ that is one of the ~~smallest~~ minimal length bursts consistent with the syndrome $y(D) \bmod g(D) = s(D)$. Since $s(D)$ is itself a valid error pattern. ~~assuming that no bursts of length greater than b occur and that the code can correct all these bursts~~

The following procedure results in maximum likelihood decoding:

(a) Let $\{D^{r+i} y(D)\} \bmod g(D) = r_i(D)$ for $i = 0, \cdots, N-$ where $\deg g = r$,

(b) Let $r_{i^*}(D)$ be the remainder of smallest degree for $i = 0, \cdots, N-1$

(c) decode to $\hat{X}(D) = \{D^{2N-r-i^*}[D^{r+i^*} y(D) - r_{i^*}(D)]\} \bmod (D^N-$

$$= y(D) - \{D^{2N-r-i^*} r_{i^*}(D)\}^{\bmod (D^N-1)} = \hat{x}(D)$$

~~since $\deg r_{i^*} \le r-1$~~ $= \begin{cases} y(D) - D^{N-r-i^*} r_{i^*}(D) & \text{for } 0 \le i^* \le N-r \\ y(D) - \{D^{2N-r-i^*} r_{i^*}(D)\} \bmod (D^N-1) & \text{for } N-r+1 \le i^* \end{cases}$

ordinary p

end erro

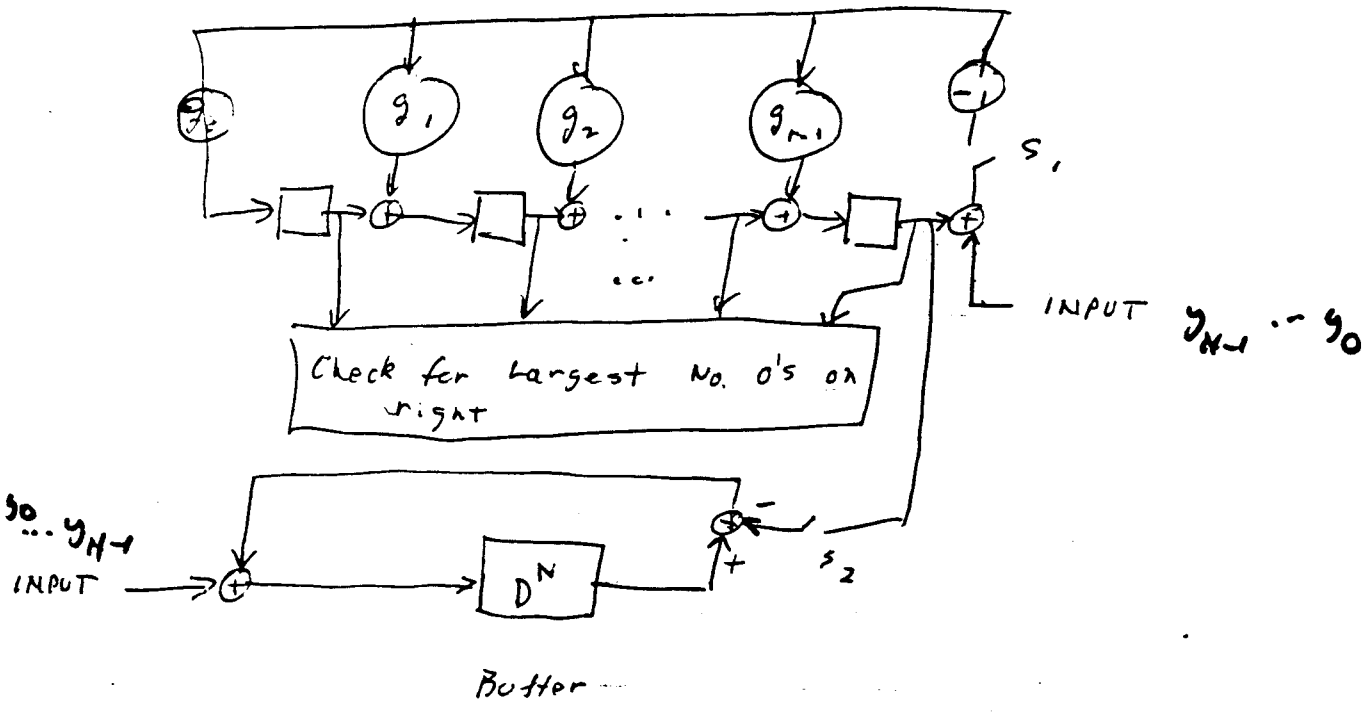
<u>Proof:</u>

$D^{r+i^*} y(D) - r_{i^*}(D)$ is a multiple of $g(D)$ so that $\hat{x}(D)$ is a codeword. Now suppose that another codeword $\bar{x}(D)$ exists such that $y(D) - \bar{x}(D) = \bar{E}(D)$ where $\bar{E}(D) = [D^j \bar{r}(D)] \bmod (D^N - 1)$ with $\deg \bar{r} < \deg r_{i^*}$. If this were true then $D^{N-j} y(D) = D^{N-r-(j-r)} y(D)$ would have a remainder of degree smaller than that of $r_{i^*}(D)$. Since $\{D^{N-j} y(D)\} \bmod g(D) = \{D^{N-j} \bar{x}(D) + D^{N-j} \bar{E}(D)\} \bmod g(D)$

$$= \bar{r}(D).$$

Therefore $\{D^{2N-r-i^*} r_{i^*}(D)\}^{\bmod (D^N-1)}$ is ~~the~~ a most likely error burst.

Decoding Circuit



Circuit Operation

1. Close s_1, open s_2 and shift received word into buffer and register starting with y_{N-1}.
2. Shift register N times so that logic circuit can check for smallest burst.
3. Assume that the smallest burst occurred on the i'th shift in step 2. Begin shifting the buffer and the register simultaneously. On the ith shift open s_1, close s_2 and continue shifting for a total of $2N$ shifts in step 3. The corrected word remains in the buffer.

Analysis of Circuit Operation

Assume that a correctable burst $E(D) = \{D^k B(D)\} \bmod (D^N - 1)$ with $b_0 \neq 0$ and $\deg B < r$ has occurred so that $y(D) = X(D) + E(D)$. After i shifts in step 2 the register contains

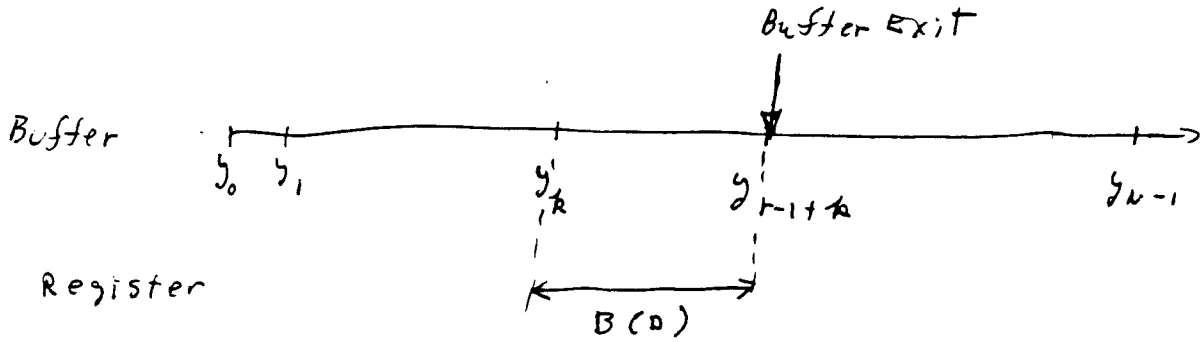
$$r_i(D) = \{D^{r+i} y(D)\} \bmod g(D) = \{D^{r+i}\{D^k B(D)\} \bmod (D^N - 1)\} \bmod$$
$$= \{D^{r+i+k} B(D)\} \bmod g(D)$$

since $\{D^k B(D)\} \bmod (D^N - 1) = D^k B(D) - a(D)(D^N - 1)$ and $g(D)$ divides $D^N - 1$. If $E(D)$ is an ordinary burst $0 \le k \le N - r$. In this case after $N - r - k$ shifts the burst pattern $B(D)$ appears in the register since

$$r_{N-r-k}(D) = \{D^N B(D)\} \bmod g(D) = \{[h(D) g(D) + 1] B(D)\} \bmod g$$
$$= B(D)$$

After $i^* = N - r - k$ shifts in step 3 the buffer and register contents have the relationship shown

below

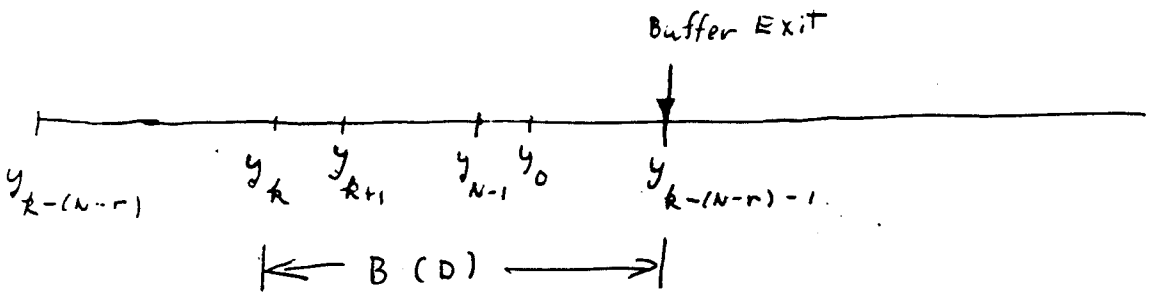


so that the burst pattern appears in the register just as the symbols to be corrected begin to leave the buffer. For end-around bursts $N-r < k \leq N-1$. In this case $B(D)$ appears in the register after $i^* = 2N-r-k$ shifts since

$$r_{i^*}(D) = \{ D^{2N} B(D) \} \bmod g(D) = B(D)$$

since $D^N = g(D)h(D) + 1 \longrightarrow D^{2N} = D^N g(D)h(D) + g(D)h(D) + 1$

In this case the buffer and register have the relation shown below after i^* shifts



The actual burst $E(D) = \{ D^k B(D) \} \bmod (D^N - 1)$

$$= \left(b_0 D^k + b_1 D^{k+1} + \cdots + b_{N-k-1} D^{N-1} \right) + \left(b_{N-k} + \cdots + b_{r-1} D^{k-(N-r)-1} \right)$$

so that the burst pattern once again appears in the register just as it is about to emerge from the buffer.

If a code is capable of correcting all bursts of length b or less, the "error trapping" decoder just described will always decode correctly when a correctable burst is present. In this case, each burst of length b or less must have a distinct syndrome $\{D^r y(D)\} \bmod g(D)$. Each syndrome equal to a correctable burst is generated by the corresponding error pattern in the highest order $N-K=r$ information symbols. Thus no other correctable burst can result in a syndrome that is a burst of length b or less until it has been cycled into the highest order r information positions. If the burst has length greater than b it may or may not be decoded correctly. Since there are q^r syndromes and $N(q-1)q^{b-1}$ bursts of length b or less, frequently only a small percentage of the syndromes are used for burst correction and it would not seem unreasonable that many bursts of length greater than b might be correctable by the error trapping procedure. Gallager (Ch 6) has derived bounds on the percentage of bursts of length $> b$ that are correctable by error trapping.

If the code corrects all bursts of length b or less and end around bursts are neglected, the error trapping decoder

can be simplified as follows:

(1) Same as before

(2) The logic circuit checks for $r-b$ 0's in the left hand side of the syndrome register. If this occurs a correctable burst is in the register. S_1 is opened, S_2 is closed and the rest of the word is shifted out of the buffer.

<u>Fire Codes</u> (Peterson, Ch. 10)

<u>Definition:</u> The generator polynomial for a Fire code with symbols from $GF(q)$ has the form $g(D) = f(D)(D^c - 1)$ where $f(D)$ is an irreducible polynomial of degree m over $GF(q)$ whose roots have order e, and c is not divisible by e. The length of the code is the least common multiple of e and c, since $f(D)$ divides $D^n - 1$ iff n is a multiple of e and $D^c - 1$ divides $D^n - 1$ iff n is a multiple of c. Therefore the smallest value of n such that $g(D)$ divides $D^n - 1$ is $\text{lcm}(c, e)$.

<u>Error Correction and Detection Capability</u>

a Fire code can correct any single burst of length b or less and detect bursts of length $d \geq b$ or less if $c \geq d+b-1$ and $m \geq b$. For detection alone, the code can detect all bursts of length $c+m$ or less and

also any error pattern that is the sum of two bursts when the length of the shorter burst is no greater than m and the sum of the lengths is no more than $c+1$.

Proof:

The fact that the code can detect all bursts of length $c+m$ or less follows from Theorem 23 on p. 186.

For a code to be able to correct all bursts of length b or less and detect all bursts of length $d \geq b$ or less, it is necessary and sufficient that for every burst of length b or less no other burst of length d or less has the same syndrome. Let $A(D) = a_0 + \cdots + a_{b-1} D^{b-1}$ and $B(D) = b_0 + \cdots + b_{d-1} D^{d-1}$ with a_0 and $b_0 \neq 0$ and $0 \leq i, j < N$. Then $\{D^i A(D)\} \bmod (D^N - 1)$ and $\{D^j B(D)\} \bmod (D^N - 1)$ are bursts of length $\leq b$ and $\leq d$ respectively. Thus if $[\{D^i A(D)\} \bmod (D^N-1)] \bmod g(D) \neq$

$$[\{D^j B(D)\} \bmod (D^N-1)] \bmod g(D)$$

then

$$[\{D^i A(D) - D^j B(D)\} \bmod (D^N-1)] \bmod g(D) \neq 0$$

so that the sum of a burst of length $\leq b$ and a burst of length $\leq d$ can not be a codeword. To show that the sum of a burst of length $\leq d$ and a burst of length $\leq b$ can not be a codeword in a Fire code if $b+d-1 \leq c$ and m is at least as large as the smaller of b and d, first assume that

$D^c - 1$ divides $U(D) = \{D^i A(D) - D^j B(D)\}$ mod $(D^N - 1)$ or equivalently $U_1(D) = D^i A(D) - D^j B(D)$. Without loss of generality assume $i < j$ and $j - i = cs + r$ with $0 \le r < c$. Then

$$D^i A(D) - D^j B(D) = D^i [A(D) - D^r B(D)] - D^{i+r} B(D) [D^{cs} - 1].$$

But $D^c - 1$ divides $D^{cs} - 1$ so it must also divide $D^i \{A(D) - D^r B(D)\}$. Let

$$A(D) - D^r B(D) = (D^c - 1) V(D) \qquad \text{Eq. (F1)}$$

and assume $V(D) \neq 0$. Let v be the degree of $V(D)$. Then the degree of the right hand side is $c + v$ and the $\deg \{A(D) - D^r B(D)\} \le r + d - 1$, i.e.,

$$c + v \le r + d - 1$$

or

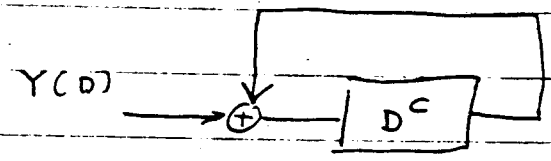
$$r \ge c - d + 1 + v$$

But by hypothesis $b + d - 1 \le c$ or $c - d + 1 \ge b$ so $r \ge b + v$ and since $b \ge 1$, $r \ge b$ and $r > v$. In Eq. (F1) there is a term of degree r on the left but none on the right since $c > r > v$. Thus $V(D) = 0$, $r = 0$, $A(D) = B(D)$ and $U_1(D) = D^i A(D) - D^j B(D) = D^i B(D) [D^{cs} - 1]$. Now consider whether $U_1(D)$ is divisible by $f(D)$. Since $A(D) = B(D)$ and the degree m of $f(D) \ge b$, $f(D)$ does not divide $B(D)$. It also does not divide D^i. Since $j - i < N$, $cs < N$. So $f(D)$ divides $D^{cs} - 1$ iff cs is a multiple of e the order of the roots of $f(D)$ and $cs \ge N$. This is impossible so $f(D)$ cannot divide $D^{cs} - 1$ and $U(D)$ is not divisible by $g(D)$.

(cs is multiple of c and e so $cs \ge \text{lcm}(c, e) = N$)

Q.E.D.

The proof above does not make clear the philosophy for the design of the Fire codes. Consider the parity checks associated with the factor $D^c - 1$. These can be generated by the circuit below.



Thus these c parity checks are

$$s'_k = \sum_m y_{mc+k} \quad \text{for } k = 0, \cdots, c-1$$

Since the symbols involved in each check are spaced c symbols apart, each check will be affected by no more than one error in a burst of length c or less. Thus S(D) gives a sort of picture of the burst. If $b + d - 1 = c$, any burst of length b or less will leave at least d-1 cyclically successive checks zero. This is sufficient to determine which symbol is at the beginning of the burst. It is also sufficient to distinguish between a burst of length b of the form

$$1 \underbrace{0 \cdots 0}_{b-2} 1$$

and a burst of length d of the form

$$1 \underbrace{0 \cdots 0}_{d-2} 1$$

These are the extreme cases for error detection.

Thus the factor $D^c - 1$ is sufficient to detect all bursts of length c or less and exactly determine the error pattern for bursts of length b or less. However, it can not determine the exact location of the burst since $D^i A(D) \bmod (D^c - 1) = D^j A(D) \bmod (D^c - 1)$ or equivalently $[D^i A(D) - D^j A(D)] \bmod (D^c - 1) = 0$ iff $j - i = cs$. However, in the proof it is shown that when $D^i A(D) - D^j A(D)$ is divisible by $D^c - 1$ it is not divisible by $f(D)$ so that $f(D)$ determines the burst location.

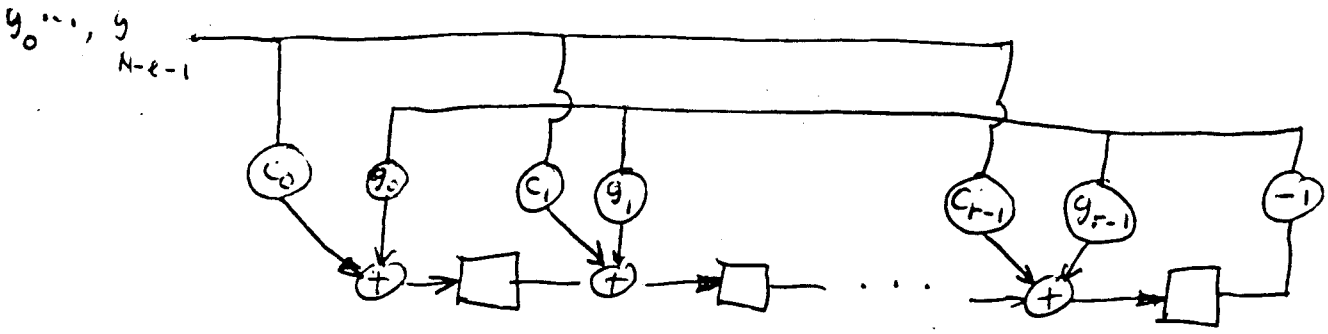
EXAMPLE

Let $f(D) = D^7 + D^3 + 1$ which is a primitive polynomial of degree $m = 7$ so $e = 2^7 - 1 = 127$, a prime number and let $c = 16$. Therefore $N = 127 \times 16 = 2032$ resulting in a $(2032, 2009)$ code with generator polynomial $g(D) = (D^{16} + 1)(D^7 + D^3 + 1)$. From the bounds $m \geq b$ and $b + d - 1 \leq c$ it follows that the code could correct all bursts of length 7 or less and detect all bursts of length 10 or less, etc. For pure detection, it could detect all single bursts of length 23 or less and all error patterns that are the sum of a burst of length $b = 7$ or less and a burst of length d or less if $b + d \leq 17$.

Shortened Codes

It may be that a code has desirable

error correction properties but that it's natural length is too long. The code can be shortened to a desirable length without changing the error correction capability by making the first l information symbols zero. The burst trapping decoder designed to neglect end-around bursts and correct only bursts of length b or less can be modified so that it is only necessary to store the $N-l$ received symbols and not shift the syndrome register l times initially to account for the first l symbols that are known to be zero. This is accomplished by premultiplying the syndrome by D^l, i.e., by calculating $\{D^{l+r} y(D)\} \bmod g(D)$. If $D^{l+r} \bmod g(D) = c_0 + c_1 D + \cdots + c_{r-1} D^{r-1}$, the circuit shown below makes this calculation.



The rest of the decoding procedure is the same as described previously.

<u>Interleaving</u>

Unfortunately many real channels are not strictly random error channels or burst

error channels. They may vary in time from one to the other as in the case of fading radio links or may be inherently always a mixture of both types. Codes designed strictly for burst correction usually can not cope with random errors. One solution is to interleave l relatively short random error correcting codes. The codewords $\vec{x}_i = \{x_{i0}, \cdots, x_{i,N-1}\}$ $i = 1, \cdots, l$ are interleaved by forming the sequence of lN symbols

$$x_{10}\ x_{20} \cdots x_{l0}\ \ x_{11}\ x_{21} \cdots x_{l1} \cdots x_{1,N-1}\ x_{2,N-1} \cdots x_{l,N-1}$$

This sequence is transmitted sequentially starting with $x_{1,N-1}$. At the receiver, the sequence is de-interleaved into l blocks corresponding to the l initial code words. If the channel introduces a burst of length lb or less, the de-interleaved blocks can only contain bursts of length b or less. If the basic code has the generator $g(D)$, it is easy to see that the interleaved sequence is a codeword in the (lN, lK) cyclic code generated by $g(D^l)$. This leads to the following theorem:

<u>Interleaving Theorem</u>

If a cyclic (N, K) code with generator $g(D)$ can correct all bursts of length b or less, the (lN, lK) code with generator $g(D^l)$ can correct all bursts of length lb or less.