B. Cyclic Codes

A cyclic code is a linear block code with the further property that a shift of a codeword results in another codeword.
These are based on polynomials whose elements are coefficients from GF(2). These polynomials can be added, (subtracted), multiplied and (divided) in the usual way, remembering that 1+1=0=1-1; 1*1=1.

There are 2 basic properties of polynomials over GF(2).

1. A polynomial of degree m is irreducible over GF(2), if it is not divisible by any other polynomial of degree less than m over GF(2).
2. Further, an irreducible polynomial of degree m, is said to be a primitive polynomial, if it is divisible by the polynomial $X^n + 1$, where $n = (2^m – 1)$, and is not divisible by any polynomial of degree less than $(2^m – 1)$.

Primitive polynomials are the generator polynomials of cyclic codes.

The Galois field over GF(2), (with elements 0 and 1), can be extended to one of 2^m elements, $GF(2^m)$. These will be developed when dealing with BCH codes.

The generator polynomial of a cyclic code has the following properties.

(i) For an (n,k) code the degree of g(X) is (n-k) = m and n = $(2^m – 1)$.
(ii) g(X) must have the element 1 as its first element.
(iii) g(X) is a primitive polynomial of $X^n +1$;
(iv) every codeword has degree that is (n-1) or less
(v) every codeword is a multiple of g(X), the multiple being all possible polynomials of degree m or less.

Example: The polynomial $X^7 + 1$ has three factors given by

$$(1+X)(1+X+X^3)(1+X^2+ X^3)$$

All three are irreducible. However (1+X) is not primitive. Both polynomials of degree 3 can be used as generator polynomials for a (7,4) cyclic code.

Systematic code

Given a g(X), the code can be put into systematic form, using the following steps:

(i) Premultiply the message u(X) by $X^{(n-k)}$.
(ii) Obtain the remainder r(X), that gives the parity-check bits, by dividing $X^{(n-k)}.u(X)$ by the g(X)
(iii) Combine r(X) and $X^{(n-k)}.u(X)$ to obtain the code polynomial
$$r(X) + X^{(n-k)}.u(X)$$

The format of this systematic code is [P , U] where P are the parity bits and U are the data bits.

Using as g(X), $(1+X^2+ X^3)$ the systematic code is obtained as follows. Note that the polynomial is in reverse order ie 1100 is 1+X and NOT $X^3 + X^2$.

Message	Codeword	Polynomial
0000	000 0000	0.g(X)
1000	101 1000	1.g(X)
0100	111 0100	$1+X+ X^2+ X^4 = (1+ X).g(X)$
1100	010 1100	$X + X^3+ X^4 = X.g(X)$
0010	110 0010	$1 + X + X^5 = (1 + X+ X^2). g(X)$
1010	011 1010	$X + X^2 + X^3 + X^5 = (X+ X^2).g(X)$
0110	001 0110	$X^2 + X^4 + X^5 = X^2.g(X)$
1110	100 1110	$1 + X^3 + X^4 + X^5 = (1 + X^2).g(X)$
0001	011 0001	$X + X^2 + X^6 = (X + X^2 + X^3).g(X)$
1001	110 1001	$1 + X + X^3 + X^6 = (1 + X + X^2 + X^3).g(X)$
0101	100 0101	$1 + X^4 + X^6 = (1 + X^2 + X^3)g(X)$
1101	001 1101	$X^2 + X^3 + X^4 + X^6 = (X^2 + X^3).g(X)$
0011	101 0011	$1 + X^2 + X^5 + X^6 = (1 + X^3).g(X)$
1011	000 1011	$X^3 + X^5 + X^6 = (X^3).g(X)$
0111	010 0111	$X + X^4 + X^5 + X^6 = (X + X^3).g(X)$
1111	111 1111	$1+X+X^2+X^3+X^4+X^5+X^6 = (1 + X + X^3).g(X)$

Generator and Parity-Check Matrices

A generator polynomial g(X) of order (n-k) can be made to span the code C of dimension n, by shifting the g(X) , k positions (rows). For example for the g(X) above the Generator Matrix, G is given by

$$G = \begin{bmatrix} 1\,0\,1\,1\,0\,0\,0 \\ 0\,1\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1 \end{bmatrix}$$

G is not in systematic form, but can be using row operations.using row1+row2 for row2; rows 1,2,and 3 for row3, and rows 2,3,and 4 for row 4 resulting in

$$G = \begin{bmatrix} 1\,0\,1\,1\,0\,0\,0 \\ 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,0\,0\,1\,0 \\ 0\,1\,1\,0\,0\,0\,1 \end{bmatrix}$$

which is now in systematic form.

Since g(X) is a factor of $(X^n + 1)$,

$$(X^n + 1) = g(X).\, h(X)$$

where h(X) has degree k of the form $h(X) = h_0 + h_1X+ . . . + h_kX^k$ and $h_0 = h_k = 1$. h(X) is the parity polynomial of the code, and $X^k\, h(X^{-1})$ is a polynomial that generates an (n,n-k) cyclic code. It is defined as

$X^k\, h(X^{-1}) = h_k + h_{k-1}X+ . . . + h_0X^k$. It can be shown that every code vector in the code of g(X) is orthogonal to every row of the matrix H generated by $X^k\, h(X^{-1})$, and therefore H is the parity-check matrix for G.

Starting from (X^7 + 1) and g(X) = ($1+X^2+ X^3$) it follows that h(X) is given by
h(X) = $1 + X^2 + X^3 + X^4$ and X^4 h(X^{-1}) = $1 + X + X^2 + X^4$ Hence H is obtained as

$$H = \begin{vmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,1\,0\,1 \end{vmatrix}$$

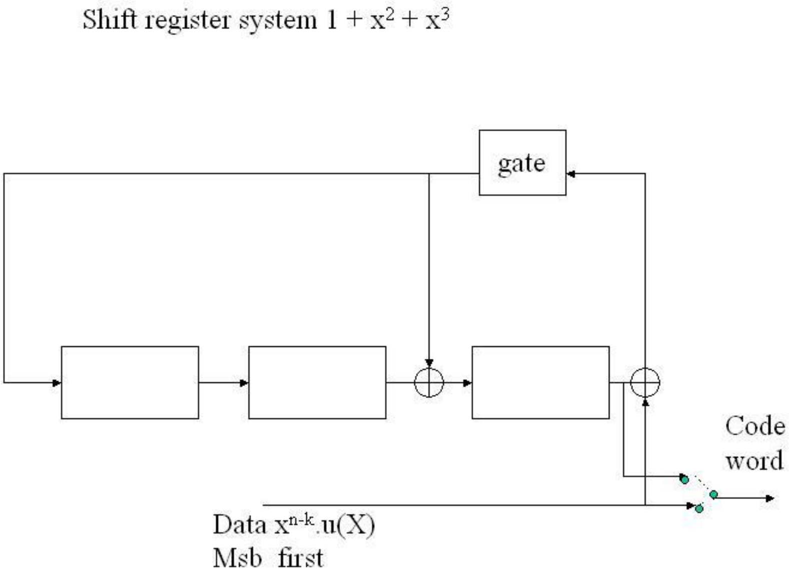
H is an (n, n-k) matrix in this case a (7,3) matrix. Adding row 1,row 3 in row3 for a systematic form H, given by

$$H = \begin{vmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0 \\ 1\,1\,0\,1\,0\,0\,1 \end{vmatrix}$$

. It can easily be shown that the syndrome of any code vector from the code polynomials above results in $v.H^T = 0$, and s =[0 0 0]

Encoding of a cyclic code

A shift register system based on g(x) is used to generate a code word, Figure 4.1



Figur 4.1

Note the connections of XOR's at position 2 and position3. The data bits are passed to the output and into the feedback register system, msb first. Then the switch is moved to the feedback register output and the parity bits are passed out.

For an input 1011 the system shifts are

		Registers
Initial		0 0 0
Shift 1	1	1 0 1
Shift 2	1	0 1 0
Shift 3	0	0 0 1
Shift 4	1	0 0 0

Final codeword is 0 0 0 1 0 1 1

Syndrome Computation

Given a received word r(X), the syndrome is obtained as the remainder of r(X)/g(X). The remainder must be a polynomial of degree (n-k-1) or less.
With cyclic codes the syndrome can be obtained through a feedback shift register circuit quite similar to the encoder.
The syndrome circuit for the (7,4) code with g(X) = (1 + X^2 + X^3) is shown below. Note that the received word is input from the left, unlike the data bits input from the right in the circuit of Figure 4.1.

Syndrome generating circuit for g(X)= 1 + x^2 + x^3

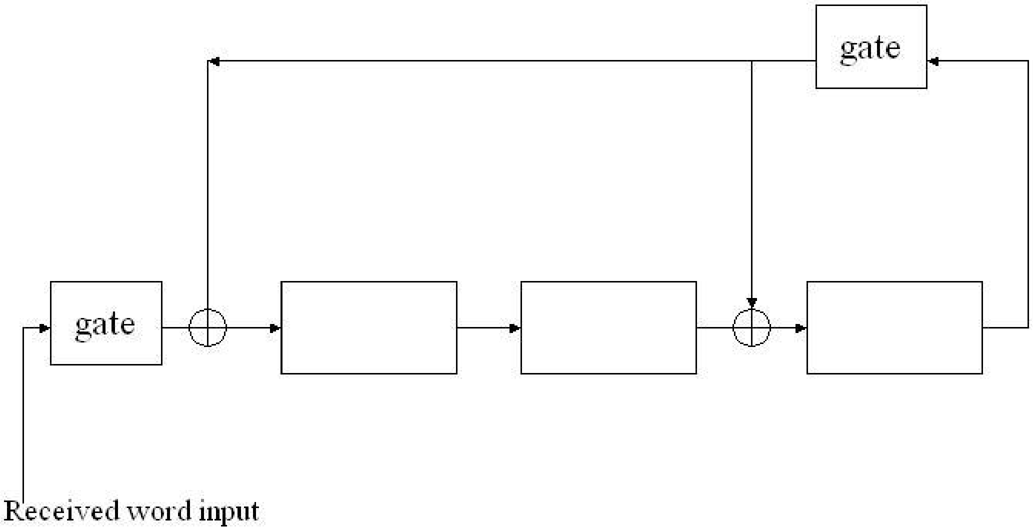


Figure 4.2

Given the received n-tuple r(X) = [1 0 0 1 0 1 1] the register contents results in

Shift	Input	Register Contents
		0 0 0
1	1	1 0 0
2	1	1 1 0
3	0	0 1 1
4	1	0 0 0
5	0	0 0 0
6	0	0 0 0
7	1	1 0 0
8	-	0 1 0

The resulting syndrome is [1 0 0] . Note that a cyclic shift of the syndrome results in the syndrome for the cyclic shift of the received word given by X.r(X)
Because of the cyclic shift property a cyclic code is capable of detecting any error burst of length (n-k) or less, including the end-around bursts.

Cyclic Codes Decoding

Cyclic codes can be decoded in the same way as linear block codes, using the standard array and the coset leaders, as error vectors, in relation to the syndrome pattern obtained after decoding. This still requires a decoding table to associate the syndrome to its corresponding error pattern.
Because of the cyclic nature, the error pattern and its corresponding syndrome are obtained directly either through dividing by g(x) or the syndrome circuit. The syndrome error pattern table for the (7,4) code with $g(X) = (1 + X^2 + X^3)$ is shown below. Ei represents the error bit in the received r(X). For no errors s = [000].

E6 = [011]
E5 = [110]
E4 = [111]
E3 = [101]
E2 = [001]
E1 = [010]
E0 = [100]

A decoding circuit can be designed to automatically detect, and correct a single-bit error based on the cyclic property. The pattern for E6 = [011] is used to compare to the syndrome of the particular bit error. The stored received word is shifted out bit by bit, as the syndrome pattern obtained is compared. Based on s = E6, since the syndrome s^i represented by the i-th shift of the s, corresponds to the syndrome of the $r^i(X)$ the i-th shift of the received word r(X), the error bit can be corrected as the received word is passed out from the buffer. The circuit is shown in Figure 4.3 below.

Decoding circuit for (7,4) code with $g(X) = (1 + X^2 + X^3)$

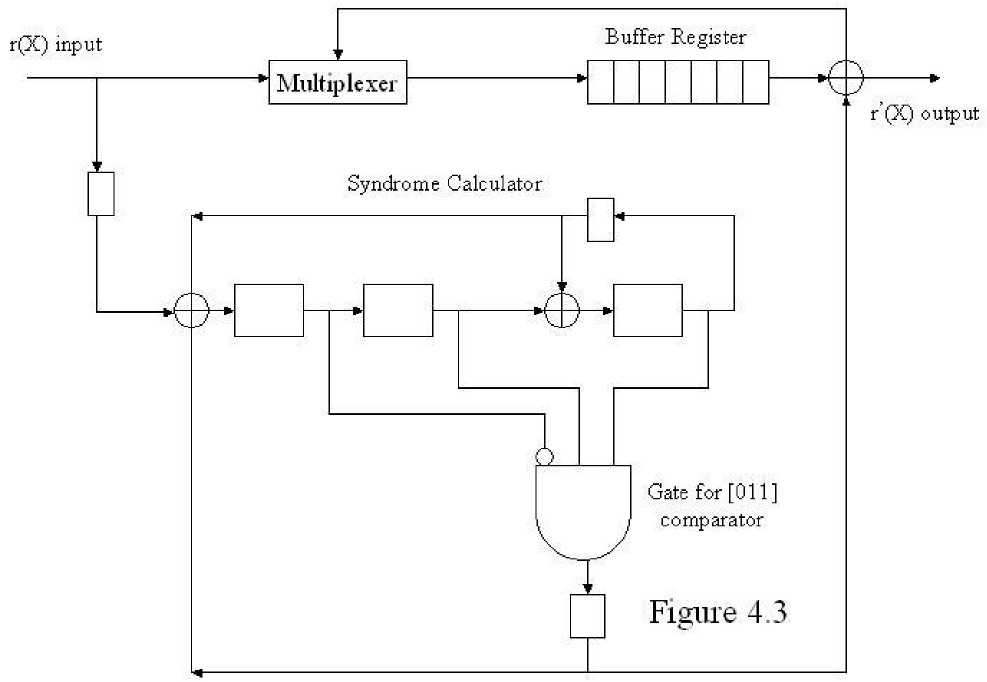


Figure 4.3

This type of decoder is also known as a Meggitt Decoder.

Another important property of a cyclic code is the capability of detecting burst errors. An (n.k) cyclic code can detect any error burst, of length (n-k) nor less, including end around bursts.
For example the CRC check based on

$$g(X) = 1 + X^2 + X^{15} + X^{16}$$

with $n = 2^{16} - 1 = 32767$; $n-k = 16$; and $k = 32751$
is capable of detecting all error bursts of 16 or less.

Cyclic Hamming Codes
A cyclic Hamming code of length $2^m - 1$, with $m \geq 3$ is generated by a primitive polynomial p(X) of degree m. Note that since the degree of g(X) is $(n-k) = (m - 1)$, the number of information bits k is $2^m - m - 1$
In general the codeword is obtained, using a generator polynomial p(X) from

$X^{m+i} = a_i(X).p(X) + b_i(X)$ where the remainder $b_i(X)$, of degree (m-1) or less forms the parity checks, with at least two 1's.
Given $H = \{I_m\ Q\}$ where Q is an m x $(2^m - m - 1)$ matrix, the $b_i(X)$'s form the columns of Q.

For example using the primitive polynomial $1+X+X^3$ a (7,4) cyclic Hamming code can be generated. This code can correct one bit in error.

Modified Hamming Code

A Hamming code $H = [I_m\ Q]$ can be modified to $H^{'} = [I_m\ Q']$ where Q' consists of $2^m - m$ (instead of $2^m - m - 1$) columns.
This new code is capable of correcting single errors and detecting double errors. In terms of cyclic codes this is obtained by modifying g(X) to g'(X) = (1+X) g(X). The minimum distance of the resulting code is 4.
The decoding circuit of the single correcting code is modified as follows.
Let r(X) be the received word.

(i) Divide X^m. r(X) by g(X) to obtain a remainder that is the syndrome s(X) of degree m-1 or less
(ii) Divide r(X) by (X+1) to obtain a remainder, ρ, whose value is either 0 or 1.

The detection circuit has the following scheme.

Step 1 if $\rho = 0$, and $s(X) = 0$ then the r(X) is a codeword c(X)
Step 2 if $\rho = 1$, and $s(X) \neq 0$, one error has occurred and it can be corrected
Step 3 if $\rho = 0$, and $s(X) \neq 0$, two errors are detected, hence alarm signal of a detected but uncorrectable error pattern.
Step 4 if $\rho = 1$, and $s(X) = 0$, there are at least 3 errors such that r(X) has been changed to a c(X). Indication of an undetectable error.

Probability of undetectable error.

The extended code C' with minimum distance 4, consists of the even weighted code vectors of the original code C, with minimum distance 3.

The original weight distribution polynomial, for the Hamming Code, (n, k) is given by

$$A(z) = \frac{1}{n-1}\{(1+z)^n + n(1-z)(1-z^2)^{(n-1)/2}\} \quad (4.1)$$

and the weight distribution of the new code C’, A’(z), is made up of the even power terms of A(z), given by A’(z) = ½[A(z) + A(-z)], and using A(z) above to obtain

$$A'(z) = \frac{1}{2(n+1)}\{(1+z)^n + (1-z)^n + 2n(1-z^2)^{(n-1)/2}\} \quad (4.2)$$

Using $P_u(E) = \sum_{i=1}^{n} A_i \, p^i (1-p)^{n-i}$ (4.3)

and (4.2) $P_u(E)$ can be calculated in terms of A’(z).

This can also be calculated from the dual code. The dual of a distance 4 Hamming code has a weight distribution B’(z) given by

$$B'(z) = 1 + (2^m - 1)z^{2^{m-1}-1} + (2^m - 1)z^{2^{m-1}} + z^{2^m - 1} \quad (4.4)$$

Using (3.9) and (4.4) $P_u(E)$ can be calculated. In terms of B’(z).

$$P_u(E) = 2^{-(m+1)}\{1 + 2(2^m - 1)(1-p)(1-2p)^{2^{m-1}-1} + (1-2p)^{2^m - 1}\} - (1-p)^{2^m - 1} \quad (4.5)$$

It can be shown that $P_u(E)$ in (4.5) satisfies the upper bound $2^{-(n-k)}$ (= $2^{-(m+1)}$)

Shortened Cyclic Codes

An (n,k) cyclic code can be altered to an (n-l, k-l) code, shortened by l bits. This code is strictly a shortened cyclic code. It consists of a subset of the original codewords of degree (n-i) or less, still using the same g(X) and generating the same syndrome during decoding.

However, when decoding, the (n-l) shifts that are used to input the received word, still require a further l-shifts to align to the syndrome pattern, and eventually to an error position X^{n-l-i}.

To remove the extra shifts, either the connections to the syndrome register, or the syndrome pattern can be shifted to the appropriate start pattern, to align the syndrome pattern to the first potential error bit.

Figure 4.4 shows the decoding circuit for a (31,26) cyclic code with the AND gate looking for the first error pattern 00001.

When Figure 4.4 is adapted to a shortened cyclic code (28,23) with l =3, the new start syndrome, for the same circuit but having a 28-bit shift register, is given by 01000

Decoding circuit for (31,26 code with $g(X) = (1 + X^2 + X^5)$

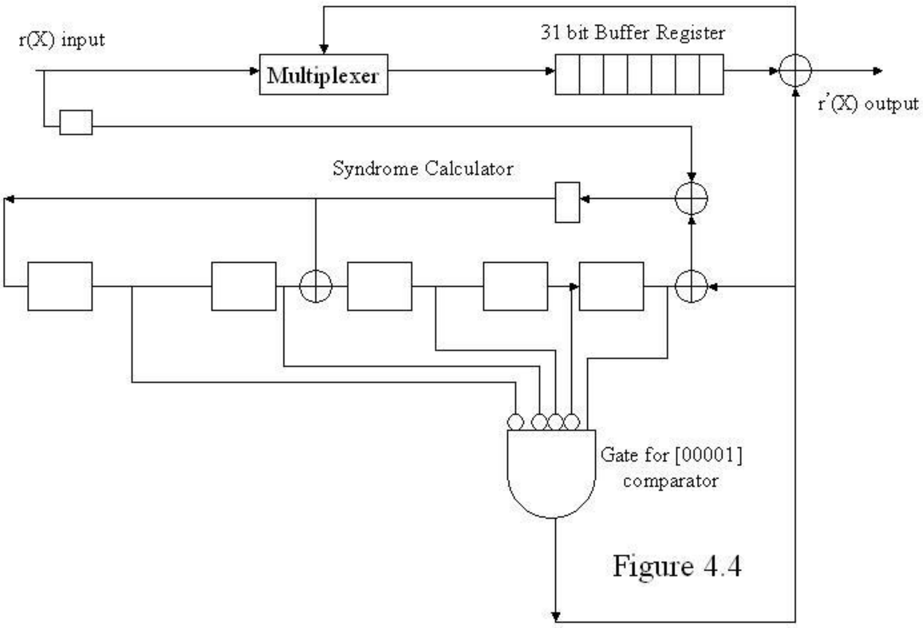


Figure 4.4