Cyclic Codes – BCH Codes

Galois Fields GF(2^m)

A Galois field of 2^m elements can be obtained using the symbols 0, 1, α, and the elements being 0, 1, α, α^2, α^3, . . . α^{2^m-1} so that field F* is closed under multiplication with 2^m elements.
The operator '+' is defined by dividing X^i by p(X) where p(X) is a primitive irreducible polynomial in GF(2^m).

X^i = q(X). p(X) + $a_i(X)$ where $a_i(X)$ is a polynomial of degree (m-1) or less over GF(2). The outcome is a set of (2^m –1) non zero polynomials of α over GF(2^m) with degree (m-1) or less.

Example.. Starting with m = 4, p(X) = $X^4 + X^3 + 1$, which is a primitive polynomial over GF(2) and a factor of (X^{15} + 1), Set p(α) = $\alpha^4 + \alpha^3 + 1 = 0$. Hence $\alpha^4 = 1 + \alpha^3$ and the GF(2^4) can be constructed and is given by Table 4.1

Elements of GF(2^4) using p(X) = $X^4 + X^3 + 1$ over GF(2^4)

Power Elements	Polynomial	4-Tuple
0	0	0 0 0 0
1	1	1 0 0 0
α	α	0 1 0 0
α^2	α^2	0 0 1 0
α^3	α^3	0 0 0 1
α^4	$1 + \alpha^3$	1 0 0 1
α^5	$1 + \alpha + \alpha^3$	1 1 0 1
α^6	$1 + \alpha + \alpha^2 + \alpha^3$	1 1 1 1
α^7	$1 + \alpha + \alpha^2$	1 1 1 0
α^8	$\alpha + \alpha^2 + \alpha^3$	0 1 1 1
α^9	$1 + \alpha^2$	1 0 1 0
α^{10}	$\alpha + \alpha^3$	0 1 0 1
α^{11}	$1 + \alpha^2 + \alpha^3$	1 0 1 1
α^{12}	$1 + \alpha$	1 1 0 0
α^{13}	$\alpha + \alpha^2$	0 1 1 0
α^{14}	$\alpha^2 + \alpha^3$	0 0 1 1

Table 4.1

(X^4 + X + 1) is irreducible over GF(2) and does not have roots over GF(2), but it has 4 roots over GF(2^4). These are given by α^7 , α^{11} , α^{13} and α^{14} . It can be shown, using Table 4.1, that $(X + \alpha^7)(X + \alpha^{11})(X + \alpha^{13})(X + \alpha^{14}) = 1 + X + X^4$.

Further Fields

A new field element β is introduced in an extension field of GF(2) with β a root of a polynomial f(X) so that f(β) = 0.
For any $l \geq 0$, β^{2^L} is also a root of f(X) so that f(β^{2^L}) = 0. The element β^{2^L} is the conjugate of β. This also implies that if β , an element in GF(2^m) is a root of f(X) over GF(2), then all the distinct conjugates of β, also elements of GF(2^m) are roots of f(X).

Example
Using f(X) = (X^4 + X + 1) (X^2 + X + 1) = ($X^6 + X^5 + X^4 + X^3$ +1), α^7 is a root. The conjugates of α^7 are $(\alpha^7)^2$, $(\alpha^7)^{2^2}$, $(\alpha^7)^{2^3}$. Note that $(\alpha^7)^{2^4}$ is $\alpha^{112} = \alpha^{112}/\alpha^{105} = \alpha^7$ and hence closes the group.
The conjugates of α^7 are α^{14} , $\alpha^{28}/\alpha^{15} = \alpha^{13}$, and $\alpha^{56}/\alpha^{45} = \alpha^{11}$. The other 2 primitive roots are α^5 and α^{10} .
Further since β is an element of GF(2^m), in general, $\beta^{2^m-1}=1$, and $\beta^{2^m-1}+1=0$, and the 2^m – 1 nonzero elements of GF(2^m) form all the primitive roots of $X^{2^m-1}+1=0$.
Also since the zero element 0 of GF(2^m) is the root of X, then the 2^m elements form all the roots of $X^{2^m}+X$.

Minimal polynomials

The field element β can also be a root of a polynomial of degree less than 2^m. The polynomial of smallest degree over GF(2) for which f(X) = f(β) = 0 is known as the minimal polynomial of β, and denoted by Φ(X). This polynomial is also irreducible. Further if f(X), a polynomial over GF(2) has β as a root, then f(X) in general is divisible by Φ(X), the minimal polynomial. If f(X) itself is an irreducible polynomial then f(X) = Φ(X). It follows that the conjugates of β, β^2, β^{2^2} , β^{2^3} , . . β^{2^i} are also roots of Φ(X) = Φ(β). It can be shown that

$$f(X)=\prod_{i=0}^{L-1}(X+\beta^{2^i}) = \Phi(X)$$

Example:
For GF(2^4) and the field elements of Table 4.1, starting from $\beta = \alpha^3$, we obtain $\beta^2 = \alpha^6$, $\beta^4 = \alpha^{12}$, $\beta^8 = \alpha^{24}$. These result in the polynomial

$(X + \alpha^3)(X + 1 + \alpha + \alpha^2 + \alpha^3)(X + 1 + \alpha)(X + 1 + \alpha^2)$ resulting in

$(X^2 +(1+ \alpha+ \alpha^2)X + 1+ \alpha^2)(X^2 + (\alpha+ \alpha^2)X + 1 + \alpha + \alpha^2 + \alpha^3)$ finally resulting in

the minimal polynomial ($X^4 + X^3 + X^2 + X+1$).

Another way to obtain the minimal polynomial is the following. Let γ = α in GF(2^4) be used as the primitive element. Hence $\gamma^2 = \alpha^2$, $\gamma^4 = \alpha^4$, $\gamma^8 = \alpha^8$, and $\gamma^{16} = \alpha^{16} = \gamma$ closes the group. Hence Φ(X) of degree 4 must have the following form.
$\Phi(X) = a_0 + a_1X+ a_2X^2+ a_3X^3+ a_4 X^4$.
Using the polynomial representation and substituting for γ = α,
$\Phi(X) = a_0 + a_1\alpha+ a_2\alpha^2+ a_3\alpha^3+ a_4 \alpha^4$.

This results in
$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4(\alpha^3+1) = 0$. This is rearranged to get
$(a_0 + a_4) + a_1\alpha + a_2\alpha^2 + (a_3 + a_4)\alpha^3 = 0$

Hence
$(a_0 + a_4) = 0$
$a_1 = 0$
$a_2 = 0$
$(a_3 + a_4) = 0$

This results in $a_3 = a_4 = a_0 = 1$; $a_1 = a_2 = 0$; and therefore the polynomial

$(1 + X^3 + X^4) = \Phi(X)$. The Table 4.2 shows the minimal polynomials with the primitive elements as the primitive roots of the minimal polynomials using $p(X) = (1 + X^3 + X^4)$

Conjugate roots	Minimal polynomial	
0	X	
1	$(X+1)$	$\Phi_0(X)$
$\alpha, \alpha^2, \alpha^4, \alpha^8,$	$(1 + X^3 + X^4)$	$\Phi_1(X)$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12},$	$(X^4 + X^3 + X^2 + X + 1)$	$\Phi_3(X)$
$\alpha^5, \alpha^{10},$	$(X^2 + X + 1)$	$\Phi_5(X)$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14},$	$(1 + X + X^4)$	$\Phi_7(X)$

Table 4.2

Table 4.2 shows that the degree of each minimal polynomial in $GF(2^4)$ using $(1 + X^3 + X^4)$ as the primitive polynomial $g(X)$. Note that building up other generator polynomials $g'(X)$ from $g(X)$, still uses $g(X)$ so that $g'(X)$ will always include the primitive root α.

BCH Code

It is characterised by the following:
Block length $n = 2^m - 1$; Parity checks $(n-k) \le mt$; Minimum distance $d_{min} \ge 2t+1$;

The generator polynomial $g(X)$ is specified in terms of its roots in $GF(2^m)$. Every primitive element α^i is a root of a minimal polynomial $\Phi_i(X)$. It can be shown that all even powers of α^i, belong to a minimal polynomial with a preceding odd power as one of its roots. This is illustrated by Table 4.2 above.

BCH Bound: The minimum distance of the code generated by $g(X)$ is greater than the largest number of *consecutive primitive roots* of $g(X)$. Using a generator polynomial $g(X) = \Phi_0(X). \Phi_1(X). \Phi_7(X)$ yields the set of primitive roots whose index is
0, 1. 2, 4, , , 7, 8, , , 11, , 13, 14.
Note that there are 5 consecutive primitive roots in the sequence so that $g(X)$ has a minimum distance of at least 6.
Looking at Table 4.2, it can be seen that every odd root i is in the same polynomial as 2i. Hence t consecutive odd roots guarantee 2t consecutive roots. Also it can be shown

that the degree of every divisor of $X^{2^m-1}+1$, cannot exceed m. Since at most t minimum polynomials are required to guarantee that g(X) has t consecutive odd roots, the order of g(X) is *m.t* and, at most, *m.t* parity checks are required.

Encoding a BCH codeword.

The encoding process is identical to the standard cyclic code. For a k-bit data d(X) the resultant parity bits are found from

rem $\{(X^{(n-k)}.d(X)\}/ g(X)$ which are appended to the front of the d(X) to obtain the codeword v(X).
Every codeword v(X) in a BCH code is a codeword if it is divisible by the $GF(2^m)$ roots, $\alpha, \alpha^2, \ldots \alpha^{2t}$.

Decoding a BCH codeword.

Assume a codeword v(X) sent, and r(X) is received. Then the error pattern can be derived from $r(X) = v(X) + e(X)$.
The syndrome of a t-correcting BCH code is given by $S = (S_1, S_2, .. S_{2t})$, and
$S_i = r(\alpha^i)$

Divide r(X), in turn, by each of the minimal polynomials comprising g(X). In each case a remainder term b(X) is obtained. This remainder is in GF(2). This is substituted by the corresponding primitive root belonging to the minimal polynomial.

Example: Using $g(X) = 1 + X^3 + X^4$ in $GF(2^4)$ the (15,7) code uses as primitive polynomials, $\Phi_1(X) = 1 + X^3 + X^4$, and $\Phi_3(X) = (X^4 + X^3 + X^2 + X+1)$.

This gives $g'(X) = 1 + X + X^2 + X^4 + X^8$ for a (15,7) code. Using a data pattern [1001001] that gives $d(X) = 1 + X^3 + X^6$, a code word is built given by $v(X) = X^2 + X^5 + X^8 + X^{11} + X^{14}$. Let r(X) be $1 + X^8 + X^{11} + X^{14}$. This results in an $e(X) = 1 + X^2 + X^5$.

To determine the syndrome $S = (S_1, S_2, S_3, S_4)$ the r(X) is divided by each of the minimal polynomials. Using $\Phi_1(X) = 1 + X^3 + X^4$, the remainder is $b_1(X) = (1 + X^2 + X^3)$. Using the roots of the minimal polynomial, $\alpha, \alpha^2, \alpha^4$,
Hence $S_1 = 1+ \alpha^2 + \alpha^3 = \alpha^{11}$
$S_2 = 1 + \alpha^4 + \alpha^6 = 1 + \alpha + \alpha^2 = \alpha^7$
$S_4 = 1 + \alpha^8 + \alpha^{12} = \alpha^2 + \alpha^3 = \alpha^{14}$

S_3 is obtained from $\Phi_3(X) = (X^4 + X^3 + X^2 + X+1)$. The remainder is $b_3(X) = (1 + X + X^2)$. Using the first root of this minimal polynomial, α^3,
$S_3 = 1 + \alpha^3 + \alpha^6 = \alpha + \alpha^2 = \alpha^{13}$.

Hence $S = (\alpha^{11}, \alpha^7, \alpha^{14}, \alpha^{13})$

The second step, after determining the syndrome in terms of the primitive elements is to determine the error location polynomial σ(X) from the syndrome components. There are various methods available. They are based on a general solution involving the following. Given the v errors, $v \le t$, the error positions are denoted by $\alpha^{j_1}, \alpha^{j_2}, .. \alpha^{j_v}$ Since the syndromes $S_i = e(\alpha^i)$, every syndrome is related directly to the error parameters. This gives rise to a set of equations

$$\begin{bmatrix} S_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_v} \\ S_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_v})^2 \\ \vdots \\ S_{2t} = (\alpha^{j_1})^{2t} + (\alpha^{j_2})^{2t} + \ldots + (\alpha^{j_v})^{2t} \end{bmatrix}$$

Define the error locator polynomial as

$$\sigma(X) = \prod_{l=1}^{v} (1+\alpha^{j_l} X) = 1+\sigma_1(X)+\sigma_2 X^2 + \cdots + \sigma_v X^v$$

The primitive element roots of this polynomial are the inverse error location positions. It is easy to show from the above the set of Newton Identities given by

$S_1 + \sigma_1 = 0$
$S_2 + \sigma_1 S_1 + 2\sigma_2 = 0$
$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3 = 0$
. . . .

$S_v + \sigma_1 S_{v-1} + \ldots + \sigma_{v-1} S_1 + v\sigma_v = 0$

Note that since in GF(2) 1 + 1 = 2 = 0, $i\sigma_i = \sigma_i$ for i odd, and 0 for i even.

The Berlekamp-Massey Algorithm will be used for the solution of the Newton Identities.
The goal of the algorithm is to find at iteration (i+1) (connection) polynomial $\sigma^{i+1}(X)$ in terms of the error polynomial primitive elements, and given by

$$\sigma^{(i)}(X) = 1+\sigma_1^{(i)} X + \sigma_2^{(i)} X^2 \cdots + \sigma_v^{(i)} X^v$$

using as the error discrepancy that becomes a correction factor the value, d_i , using

$$d_i = S_{i=1} \quad + S_i \sigma_1^{(i)} + S_{i-1} \sigma_2^{(i)} + \cdots$$

where the upper indices (i) associated with σ indicate the coefficient value associated with an appropriate X in the equation σ(X)at the i^{th} iteration.
If $d_i = 0$, then there is no discrepancy at that stage, and the present value of σ(X), $\sigma^{(i)}(X)$, is carried to the next iteration $\sigma^{(i+1)}(X)$.
If $d_i \ne 0$, find a previous iteration row, ρ, for which $d_i \ne 0$, and the value of $(\rho - l_\rho)$ where l_ρ denotes the order of $\sigma^{(\rho)}(X)$. Then work out the value of the next iteration $\sigma^{(i+1)}(X)$ using

$$\sigma^{(i+1)}(X) = \sigma^{(i)}(X) + d_i d_\rho^{-1} X^{i-\rho} \sigma^{(\rho)}(X)$$
$$l_{i+1} = \max(l_i, l_\rho + i - \rho) \qquad (4.3)$$

The iterations are continued until the quantity, $i \ge l_i + t - 1$ becomes valid

Example:

The BCH (15,5) code, which has t=3, is generated using
$\Phi_1(X) = (1 + X^3 + X^4)$; $\Phi_3(X) = (X^4 + X^3 + X^2 + X+1)$; $\Phi_5(X) = (X^2+X+1)$. This results in a $g(X) = 1 + X^2 + X^5 + X^6 + X^8 + X^9 + X^{10}$.
A code polynomial is built using the data pattern [01101] which is $d(X) = X + X^2 + X^4$. The codeword v(X) is built by using $X^{10}d(X)/ g(X)$ to obtain the remainder. In this case the remainder is given by $(1 + X + X^6 + X^8)$ so that the codeword $v(X) = (1 + X + X^6 + X^8 + X^{11} + X^{12} + X^{14})$. The received word is $r(X) = (X + X^8 + X^{11} + X^{14})$. This implies an error polynomial $e(X) = 1 + X^6 + X^{12}$. Of course the decoder does not know this.

The procedure for decoding starts with the syndrome calculation, obtained by dividing the received word r(X) by each minimal polynomial in turn to work out the corresponding primitive element associated with the syndrome element. In this case
$S = [S_1, S_2, S_3, S_4, S_5, S_6]$.
Since $\alpha, \alpha^2, \alpha^4$, are obtained from the same polynomial $\Phi_1(X) = 1 + X^3 + X^4$, r(X) is divided by $\Phi_1(X)$, to obtain $b_1(X) = 1 + X^2 + X^3$ Hence
$S_1 = 1 + \alpha^2 + \alpha^3$, and using the $GF(2^4)$ arithmetic, based on $1 + X^3 = X^4$, and Table 4.1
$S_1 = \alpha^{11}$. Using α^2,
$S_2 = 1 + \alpha^4 + \alpha^6 = 1 + \alpha + \alpha^2 = \alpha^7$. Using α^4,
$S_4 = 1 + \alpha^8 + \alpha^{12} = \alpha^2 + \alpha^3 = \alpha^{14}$.

α^3, α^6, are obtained from $\Phi_3(X) = (X^4+ X^3+ X^2+ X+1)$, to obtain $b_3(X) = 1+X+X^2$, and using the primitive elements, α^3
$S_3 = 1 + \alpha^3 + \alpha^6 = \alpha + \alpha^2 = \alpha^{13}$ and using α^6
$S_6 = 1 + \alpha^6 + \alpha^{12} = 1 + \alpha^2 + \alpha^3 = \alpha^{11}$.
Finally α^5 is obtained from $\Phi_5(X) = (X^2+X+1)$, to obtain $b_5(X) = 1$. Therefore
$S_5 = 1$.

The Berkelamp-Massey Algorithm is now used.
Initialisation
Iteration 0: $\sigma^{(-1)}(X) = 1$; $d_{-1}=0$; $L_1=0$; $i- l_i=(0-0)=0$; since $d_{-1}=0$;
$\sigma^{(0)}(X) = 1$;
Iteration1: $i=0$; $d_0=S_1= \alpha^{11}$ and using (4.3)
$\sigma^{(1)}(X) = \sigma^{(0)}(X) + \alpha^{11}X$. Therefore at end of iteration the entry is

1 $1+ \alpha^{11}X$. 0 1 0
Check on d_1: $d_1= S_2 + S_1\sigma_1^{(1)} = \alpha^7 + \alpha^{11}.\alpha^{11} = \alpha^7 + \alpha^{22} = \alpha^7 + \alpha^7 = 0$

Iteration 2: $i=1$; $d_1= 0$; Hence $\sigma^{(2)}(X) = \sigma^{(1)}(X)$; $l_2=1$; $i- l_i= 1$;

$d_2 = S_3 + S_2\sigma_1^{(2)} = \alpha^{13} + \alpha^9.\alpha^{11} = \alpha^{13} + \alpha^{18} = \alpha + \alpha^2 + \alpha^3 = \alpha^8$. Entry

2 $1+ \alpha^{11}X$. α^8 1 1

Iteration 3: $i=2$; $d_2= \alpha^8$; Hence update $\sigma^{(2)}(X)$, using row (iteration) 0, to obtain

$\sigma^{(3)}(X) = \sigma^{(2)}(X) + d_2.(d_0)^{-1}.X^{(2-0)}. \sigma^{(0)}(X) = \sigma^{(2)}(X) + \alpha^8. (1/ \alpha^{11}).X^2.1 = \sigma^{(2)}(X) + \alpha^{12}.X^2.$

Hence $\sigma^{(3)}(X) = 1+ \alpha^{11}X + \alpha^{12}.X^2$. Entry on Iteration 3 is

3 $1+ \alpha^{11}X + \alpha^{12}.X^2.$ 0 2 1

Check on d_3: $d_3= S_4 + S_3\sigma_1^{(3)} + S_2\sigma_2^{(3)} = \alpha^{14} + \alpha^{13}.\alpha^{11} + \alpha^7.\alpha^{12} = \alpha^{14} + \alpha^9 + \alpha^4= 0$

Iteration 4: : i=3; d_3= 0; Hence $\sigma^{(4)}(X) = \sigma^{(3)}(X)$; $l_4= l_3=2$; $i- l_i= 2$;
Check : $l_4+ 3 – 1 = 4$. therefore ≤ 3 is not valid. Continue. Current entry

4 $1+ \alpha^{11}X + \alpha^{12}.X^2.$ d_4 2 2

$d_4= S_5 + S_4\sigma_1^{(4)} + S_3\sigma_2^{(4)} = 1 + \alpha^{14}.\alpha^{11} + \alpha^{13}.\alpha^{12} = 1 + \alpha^{25} + \alpha^{25} = 1$

Iteration 5: i=4; d_4= 1; Hence update $\sigma^{(4)}(X)$ to $\sigma^{(5)}(X)$, using row (iteration) 2, to obtain

$$\begin{aligned}\sigma^{(5)}(X) &= \sigma^{(4)}(X) + d_4.(d_2)^{-1}.X^{(4-2)}. \sigma^{(2)}(X) = 1. (1/ \alpha^8)X^2.(1+ \alpha^{11}X)\\ &= \sigma^{(4)}(X) + \alpha^7X^2 + \alpha^{18}X^3\\ &= 1+ \alpha^{11}X + (\alpha^{12}+ \alpha^7)X^2 + \alpha^{18}X^3\\ &= 1+ \alpha^{11}X + \alpha^2X^2 + \alpha^3X^3.\end{aligned}$$
Entry for iteration 5

5 $1+ \alpha^{11}X + \alpha^2X^2 + \alpha^3X^3$ 0 3 2

Check on d_5: $d_5= S_6 + S_5\sigma_1^{(5)} + S_4\sigma_2^{(5)} + S_3\sigma_3^{(5)}= \alpha^{11} + 1.\alpha^{11} + \alpha^{14}.\alpha^2 + \alpha^{13}.\alpha^3 = 0$

Iteration 6: i=5; d_5= 0; Hence $\sigma^{(6)}(X) = \sigma^{(5)}(X)$; $l_6= l_5=3$; $i- l_i= 3$;
Check : $l_6+ 3 – 1 = 5$. therefore ≤ 5 is true.
Iteration stopped.

The outcome of the algorithm is

$\sigma^{(6)}(X) = 1+ \alpha^{11}X + \alpha^2X^2 + \alpha^3X^3.$

The roots of this cubic polynomial are found to be (in this case by a process of trial and error on the fifteen primitive elements)
$X = 1$; $X = \alpha^3$; $X = \alpha^9$; (eg for $X =1$; $1+ \alpha^{11} + \alpha^2 + \alpha^3 = 1+ 1\ \alpha^2 + \alpha^3 + \alpha^2 + \alpha^3 = 0$)

The error locations in e(X) are the inverse of these roots. So error locations are at position 1, 6, 12.
This is the expected result.

The overall iterations are given in the Table 4.3 below

I	$\sigma^{(i)}(X)$	d_i	l_i	$i- l_i$
-1	1	0	0	-1
0	1	α^{11}	0	0
1	$1+ \alpha^{11}X$	0	1	0
2	$1+ \alpha^{11}X$	α^8	1	1
3	$1+ \alpha^{11}X + \alpha^{12}.X^2.$	0	2	1
4	$1+ \alpha^{11}X + \alpha^{12}.X^2.$	1	2	2
5	$1+ \alpha^{11}X + \alpha^2X^2 + \alpha^3X^3$	0	3	2
6	$1+ \alpha^{11}X + \alpha^2X^2 + \alpha^3X^3$	-	-	-

Table 4.3

Other BCH Codes

Binary BCH codes with length $n \neq 2^m - 1$ can be constructed as for those with $n = (2^m - 1)$. Let β be an element of order n in $GF(2^m)$. Consider a polynomial that has as roots $\beta, \beta^2, \beta^3,. . . , \beta^{2t}$. n itself is a factor of some $2^m - 1$. All the elements are roots of X^n+1. Therefore this is a cyclic code. In particular, for a sequence of 2t roots, the g(X) that is the LCM of the minimal polynomials of all the roots, generates a t-error correcting BCH code. Since β is not a primitive element of $GF(2^m)$ and $n \neq 2^m - 1$, the BCH code generated is called a nonprimitive BCH code.

Non-binary BCH codes – Reed Solomon Codes

Binary BCH codes can be generalized to any GF(q) where p is a prime number and q any power of p to obtain a q-ary code. An (n,k) q-ary cyclic code is generated by a polynomial of degree (n-k) with coefficients from GF(q) which is a factor of X^n+1. Let α be a primitive element, in $GF(q^s)$, where $n = q^s - 1$. For a t error correcting code the generator polynomial g(X) has 2t roots from GF(q) given by $\alpha, \alpha^2, .., \alpha^{2t}$. The degree of each minimal polynomial is s or less, and hence the number of parity check digits generated by by g(X) is no more than 2st.

The special subclass for which s=1 is the most important subclass of q-ary BCH codes. These codes are usually called Reed-Solomon codes. A t-error correcting RS code with symbols from GF(q) has the following parameters

Block length $n = q - 1$
Number of parity-check digits $n-k = 2t$
Minimum distance $d_{min} = 2t+1$.

Using $GF(q) = GF(2^m)$, and using α as a primitive element in $GF((2^m)$, a Reed-Solomon code, t-error correcting, can be generated using a
$g(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)\ldots.(X+\alpha^{2t})$ so that

$g(X) = g_0 + g_1X + g_2X^2 + \ldots + g_{2t-1}X^{2t-1} + X^{2t}$, so that the g_i's are now not from GF(2) but from $GF(2^m)$.

Generating a codeword is still the process of dividing $X^{2t}d(X)$ by g(X) and using the remainder to build up the systematic codeword.

Decoding follows the lines of a BCH code involving:

1. Syndrome calculation
2. Error location using an error location polynomial, and an algorithm for the solution such as the Berlekamp-Massey algorithm for the solution of $\sigma(X)$
3. Obtain from the error location polynomial, the error values, $Z(X)$, in terms of α's using Newton's identities
4. Finally obtain the error values at the locations obtained from the error location polynomial using an equation relating the error locations and $Z(X)$.