Binary BCH Codes

- Block length $n = 2^m - 1$
for som $m \geqslant 3$.
- Number of Parity-check bits $n - k \leqslant mt$
- Minimum Distance $d_{min} \geqslant 2t+1$

The generator polynomial is defined in terms of its roots over $GF(2^m)$.

For a t-error Correcting BCH code, $g(X)$ is the lowest-degree polynomial with roots $\alpha, \alpha^2, \cdots, \alpha^{2t}$.

Let $\phi_i(X)$ be the minimal polynomial of α^i for $i = 1, 2, \cdots, 2t$. Then:

$$g(X) = LCM\{\phi_1(X), \phi_2(X), \cdots, \phi_{2t}(X)\}$$

where LCM stands for least common multiple.

If i is even then we can write

$$i = i' \cdot 2^{\ell},$$

where i' is odd an $\ell \geqslant 1$. Then

$$\alpha^i = (\alpha^{i'})^{2\ell}.$$

So α^i and $\alpha^{i'}$ are conjugate of each other and have the same minimal polynomial. So,

$$g(X) = LCM\{\Phi_1(X), \Phi_3(X), \cdots, \Phi_{2t-1}(X)\}$$

Since the degree of each of $\Phi_i(X)$, $i = 1, 3, \ldots$ is less than or equal to m, the degree of $g(X)$ is less than or equal to mt. So,

$$n - k \leq mt$$

as the degree of $g(X)$ is $n-k$.

Table 6.1 lists BCH codes for lengths $2^m - 1$, $m = 3, \ldots 10$ that is length 7 to 1023.

These are narrow sense or primitive BCH codes.

In general α does not need to be primitive and root can be non-consecutive.

TABLE 6.1: BCH codes generated by primitive elements of order less than 2^{10}.

n	k	t	n	k	t	n	k	t
7	4	1	127	50	13	255	71	29
15	11	1		43	14		63	30
	7	2		36	14		55	31
	5	3		29	21		47	42
31	26	1		22	23		45	43
	21	2		15	27		37	45
	16	3		8	31		29	47
	11	5	255	247	1		21	55
	6	7		239	2		13	59
63	57	1		231	3		9	63
	51	2		223	4	511	502	1
	45	3		215	5		493	2
	39	4		207	6		484	3
	36	5		199	7		475	4
	30	6		191	8		466	5
	24	7		187	9		457	6

TABLE 6.1: (*continued*)

n	*k*	*t*	*n*	*k*	*t*	*n*	*k*	*t*
	18	10		179	10		448	7
	16	11		171	11		439	8
	10	13		163	12		430	9
	7	15		155	13		421	10
127	120	1		147	14		412	11
	113	2		139	18		403	12
	106	3		131	19		394	13
	99	4		123	21		385	14
	92	5		115	22		376	15
	85	6		107	23		367	16
	78	7		99	24		358	18
	71	9		91	25		349	19
	64	10		87	26		340	20
	57	11		79	27		331	21
511	322	22	511	166	47	511	10	121
	313	23		157	51	1023	1013	1
	304	25		148	53		1003	2
	295	26		139	54		993	3
	286	27		130	55		983	4
	277	28		121	58		973	5
	268	29		112	59		963	6
	259	30		103	61		953	7
	250	31		94	62		943	8
	241	36		85	63		933	9
	238	37		76	85		923	10
	229	38		67	87		913	11
	220	39		58	91		903	12
	211	41		49	93		893	13
	202	42		40	95		883	14
	193	43		31	109		873	15
	184	45		28	111		863	16
	175	46		19	119		858	17
1023	848	18	1023	553	52	1023	268	103
	838	19		543	53		258	106
	828	20		533	54		249	107
	818	21		523	55		238	109
	808	22		513	57		228	110
	798	23		503	58		218	111
	788	24		493	59		208	115
	778	25		483	60		203	117
	768	26		473	61		193	118
	758	27		463	62		183	119
	748	28		453	63		173	122
	738	29		443	73		163	123

TABLE 6.1: (*continued*)

n	k	t	n	k	t	n	k	t
	728	30		433	74		153	125
	718	31		423	75		143	126
	708	34		413	77		133	127
	698	35		403	78		123	170
	688	36		393	79		121	171
	678	37		383	82		111	173
	668	38		378	83		101	175
	658	39		368	85		91	181
	648	41		358	86		86	183
	638	42		348	87		76	187
	628	43		338	89		66	189
	618	44		328	90		56	191
	608	45		318	91		46	219
	598	46		308	93		36	223
	588	47		298	94		26	239
	578	49		288	95		16	147
	573	50		278	102		11	255
	563	51						

Refer to Appendix C for the list of BCH Codes and their generating polynomial.

Relationship to <u>Hamming</u> Codes.

Consider a single error correcting BCH Code of length $n = 2^m - 1$. Then

$$g(X) = \phi_1(X)$$

$\phi_1(X)$ is a polynomial of degree m. So,

$$n - k = m \Rightarrow k = 2^m - 1 - m.$$

So, a Hamming Code is just a single error correcting BCH Code.

Example: Design a triple error correcting BCH Code of length 15.

$$n = 15 = 2^m - 1 \Rightarrow m = 4$$

So, we need to find primitive element α over $GF(2^4)$ and form:

$$g(X) = LCM\{\phi_1(X), \phi_3(X), \phi_5(X)\}$$

TABLE 2.9: Minimal polynomials of the elements in $GF(2^4)$ generated by $p(X) = X^4 + X + 1$. *

Conjugate roots	Minimal polynomials
0	X
1	$X + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$

From Table 2.9, we have:

$$\phi_1(X) = 1 + X + X^4$$

$$\phi_3(X) = 1 + X + X^2 + X^3 + X^4$$

$$\phi_5(X) = 1 + X + X^2$$

So,

$$g(X) = (1 + X + X^4)(1 + X + X^2 + X^3 + X^4)(1 + X + X^2)$$
$$= 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}$$

So $n - k = 10 \Rightarrow (15, 5)$ BCH Code with $d_{min} = 7 \Rightarrow t = 3$.

*See Appendix B for minimal polynomials for $m = 2, \ldots, 10$.

BCH Codes over $GF(2^6)$.

Do this derivation of $g(X)$ for all BCH codes of length $2^6-1=63$ in order to become familiar with concepts involved.

First, using the primitive polynomial $p(X)=1+X+X^6$, generate all elements of $GF(2^6)$. They are listed below, but I strongly encourage you to create the table yourself manually (don't use a computer program).

TABLE 6.2: Galois field $GF(2^6)$ with $\mathbf{p}(\alpha)=1+\alpha+\alpha^6=0$.

0	0	(0 0 0 0 0 0)
1	1	(1 0 0 0 0 0)
α	α	(0 1 0 0 0 0)
α^2	α^2	(0 0 1 0 0 0)
α^3	α^3	(0 0 0 1 0 0)
α^4	α^4	(0 0 0 0 1 0)
α^5	α^5	(0 0 0 0 0 1)
α^6	$1+\alpha$	(1 1 0 0 0 0)
α^7	$\alpha+\alpha^2$	(0 1 1 0 0 0)
α^8	$\alpha^2+\alpha^3$	(0 0 1 1 0 0)
α^9	$\alpha^3+\alpha^4$	(0 0 0 1 1 0)
α^{10}	$\alpha^4+\alpha^5$	(0 0 0 0 1 1)
α^{11}	$1+\alpha+\alpha^5$	(1 1 0 0 0 1)
α^{12}	$1+\alpha^2$	(1 0 1 0 0 0)
α^{13}	$\alpha+\alpha^3$	(0 1 0 1 0 0)
α^{14}	$\alpha^2+\alpha^4$	(0 0 1 0 1 0)
α^{15}	$\alpha^3+\alpha^5$	(0 0 0 1 0 1)
α^{16}	$1+\alpha+\alpha^4$	(1 1 0 0 1 0)
α^{17}	$\alpha+\alpha^2+\alpha^5$	(0 1 1 0 0 1)
α^{18}	$1+\alpha+\alpha^2+\alpha^3$	(1 1 1 1 0 0)
α^{19}	$\alpha+\alpha^2+\alpha^3+\alpha^4$	(0 1 1 1 1 0)
α^{20}	$\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(0 0 1 1 1 1)

TABLE 6.2: (*continued*)

α^{21}	$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^5$	(1 1 0 1 1 1)
α^{22}	$1 + \alpha^2 + \alpha^4 + \alpha^5$	(1 0 1 0 1 1)
α^{23}	$1 + \alpha^3 + \alpha^5$	(1 0 0 1 0 1)
α^{24}	$1 + \alpha^4$	(1 0 0 0 1 0)
α^{25}	$\alpha + \alpha^5$	(0 1 0 0 0 1)
α^{26}	$1 + \alpha + \alpha^2$	(1 1 1 0 0 0)
α^{27}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1 0 0)
α^{28}	$\alpha^2 + \alpha^3 + \alpha^4$	(0 0 1 1 1 0)
α^{29}	$\alpha^3 + \alpha^4 + \alpha^5$	(0 0 0 1 1 1)
α^{30}	$1 + \alpha$	(1 1 0 0 1 1)
α^{31}	$1 + \alpha^2 + \alpha^5$	(1 0 1 0 0 1)
α^{32}	$1 + \alpha^3$	(1 0 0 1 0 0)
α^{33}	$\alpha \quad \alpha^4$	(0 1 0 0 1 0)
α^{34}	$\alpha^2 + \alpha^5$	(0 0 1 0 0 1)
α^{35}	$1 + \alpha + \alpha^3$	(1 1 0 1 0 0)
α^{36}	$\alpha + \alpha^2 + \alpha^4$	(0 1 1 0 1 0)
α^{37}	$\alpha^2 \quad \alpha^3 + \alpha^5$	(0 0 1 1 0 1)
α^{38}	$1 + \alpha + \alpha^3 + \alpha^4$	(1 1 0 1 1 0)
α^{39}	$\alpha + \alpha^2 + \alpha^4 + \alpha^5$	(0 1 1 0 1 1)
α^{40}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^5$	(1 1 1 1 0 1)
α^{41}	$1 + \alpha^2 + \alpha^3 + \alpha^4$	(1 0 1 1 1 0)
α^{42}	$\alpha + \alpha^3 + \alpha^4 + \alpha^5$	(0 1 0 1 1 1)
α^{43}	$1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5$	(1 1 1 0 1 1)
α^{44}	$1 + \alpha^2 + \alpha^3 + \alpha^5$	(1 0 1 1 0 1)
α^{45}	$1 + \alpha^3 + \alpha^4$	(1 0 0 1 1 0)
α^{46}	$\alpha + \alpha^4 + \alpha^5$	(0 1 0 0 1 1)
α^{47}	$1 + \alpha + \alpha^2 + \alpha^5$	(1 1 1 0 0 1)
α^{48}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1 0 0)
α^{49}	$\alpha + \alpha^3 + \alpha^4$	(0 1 0 1 1 0)
α^{50}	$\alpha^2 + \alpha^4 \quad \alpha^5$	(0 0 1 0 1 1)
α^{51}	$1 + \alpha + \alpha^3 + \alpha^5$	(1 1 0 1 0 1)
α^{52}	$1 + \alpha^2 + \alpha^4$	(1 0 1 0 1 0)
α^{53}	$\alpha + \alpha^3 + \alpha^5$	(0 1 0 1 0 1)
α^{54}	$1 + \alpha + \alpha^2 + \alpha^4$	(1 1 1 0 1 0)
α^{55}	$\alpha + \alpha^2 + \alpha^3 + \alpha^5$	(0 1 1 1 0 1)
α^{56}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	(1 1 1 1 1 0)
α^{57}	$\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	(0 1 1 1 1 1)
α^{58}	$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	(1 1 1 1 1 1)
α^{59}	$1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5$	(1 0 1 1 1 1)
α^{60}	$1 + \alpha^3 + \alpha^4 + \alpha^5$	(1 0 0 1 1 1)
α^{61}	$1 + \alpha^4 + \alpha^5$	(1 0 0 0 1 1)
α^{62}	$1 + \alpha^5$	(1 0 0 0 0 1)
	$\boxed{\alpha^{63} = 1}$	

- From the above table you can find minimal polynomial for all elements of $GF(2^6)$:

TABLE 6.3: Minimal polynomials of the elements in $GF(2^6)$.

Elements	Minimal polynomials
$\alpha, \alpha^2, \alpha^4, \alpha^{16}, \alpha^{32}$	$1 + X + X^6$
$\alpha^3, \alpha^6, \alpha^{12}\alpha^{24}, \alpha^{48}\alpha^{33}$	$1 + X + X^2 + X^4 + X^6$
$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	$1 + X + X^2 + X^5 + X^6$
$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$	$1 + X^3 + X^6$
$\alpha^9, \alpha^{18}, \alpha^{36}$	$1 + X^2 + X^3$
$\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}$	$1 + X^2 + X^3 + X^5 + X^6$
$\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}$	$1 + X + X^3 + X^4 + X^6$
$\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51}, \alpha^{39}$	$1 + X^2 + X^4 + X^5 + X^6$
α^{21}, α^{42}	$1 + X + X^2$
$\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}$	$1 + X + X^4 + X^5 + X^6$
$\alpha^{27}, \alpha^{54}, \alpha^{45}$	$1 + X + X^3$
$\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}$	$1 + X^5 + X^6$

Finally for any value of t generate

$$g(X) = \mathrm{LCM}\{\phi_1(X), \phi_3(X), \ldots \phi_{2t-1}(X)\}$$

TABLE 6.4: Generator polynomials of all the BCH codes of length 63.

n	k	t	$g(X)$
63	57	1	$g_1(X) = 1 + X + X^6$
	51	2	$g_2(X) = (1 + X + X^6)(1 + X + X^2 + X^4 + X^6)$
	45	3	$g_3(X) = (1 + X + X^2 + X^5 + X^6)g_2(X)$
	39	4	$g_4(X) = (1 + X^3 + X^6)g_3(X)$
	36	5	$g_5(X) = (1 + X^2 + X^3)g_4(X)$
	30	6	$g_6(X) = (1 + X^2 + X^3 + X^5 + X^6)g_5(X)$
	24	7	$g_7(X) = (1 + X + X^3 + X^4 + X^6)g_6(X)$
	18	10	$g_{10}(X) = (1 + X^2 + X^4 + X^5 + X^6)g_7(X)$
	16	11	$g_{11}(X) = (1 + X + X^2)g_{10}(X)$
	10	13	$g_{13}(X) = (1 + X + X^4 + X^5 + X^6)g_{11}(X)$
	7	15	$g_{15}(X) = (1 + X + X^3)g_{13}(X)$

Parity-check matrix of BCH Codes.

We know that each Code polynomial $v(X)$ is divisible by $g(X)$ and that $g(X)$ is:

$$g(X) = LCM\{g_1(X), g_2(X), \cdots g_{2t}(X)\}$$

So, $\alpha, \alpha^2, \alpha^3, \cdots \alpha^{2t}$ are the roots of $v(X)$, i.e.,

$$v(\alpha^i) = v_0 + v_1\alpha^i + v_2\alpha^{2i} + \cdots + v_{n-1}\alpha^{(n-1)i} = 0$$

for $i = 1, 2, \cdots, 2t$

If we form

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & & \vdots & & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix}$$

We have

$$\underline{v} \cdot H^T = \underline{0}$$

For any Codevector $\underline{v} = (v_0, v_1, \cdots, v_{n-1})$

Since if α^j is Conjugate of α^i then $v(\alpha^i) = 0$ implies $v(\alpha^j) = 0$ and vice versa.

So, we can drop even rows and write:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2, & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\ 1 & \alpha^5 & (\alpha^5)^2, & (\alpha_5)^3 & \cdots & (\alpha^5)^{n-1} \\ \vdots & & & & & \\ 1 & \alpha^{2t-1} & (\alpha^{2t-1})^2, & (\alpha^{2t-1})^3 & \cdots & (\alpha^{2t-1})^{n-1} \end{bmatrix}$$

Example: Consider double-error correcting BCH Code of length 15.

$15 = 2^4 - 1 \Rightarrow m = 4$ and from Table 2.9:

$$\phi_1(X) = 1 + X + X^4$$

$$\phi_3(X) = 1 + X + X^2 + X^3 + X^4$$

So

$$g(X) = \phi_1(X)\,\phi_3(X) = 1 + X^4 + X^6 + X^7 + X^8$$

So $n-k = 8 \Rightarrow k = 15 - 8 = 7$

So, this is the BCH Code $(15, 7)$ with $d_{min} = 5$, i.e., $t = 2$.

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} & \alpha^{24} & \alpha^{27} & \alpha^{30} & \alpha^{33} & \alpha^{36} & \alpha^{39} & \alpha^{42} \end{bmatrix}$$

Substituting α^i's, we get

$$\mathbf{H} = \left[\begin{array}{ccccccccccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hdashline 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

Example of a non-primitive BCH Code:

Consider $GF(2^6)$

Take $\beta = \alpha^3$.

β has order $n = 21$.

$$\beta^{21} = (\alpha^3)^{21} = \alpha^{63} = 1$$

Let $g(X)$ be the minimal degree polynomial with roots: $\beta, \beta^2, \beta^3, \beta^4$

β, β^2 and β^4 have the same minimal polynomial:

$$\varphi_1(X) = 1 + X + X^2 + X^4 + X^6$$

and β^3 has:

$$\varphi_3(X) = 1 + X^2 + X^3$$

So

$$g(X) = \varphi_1(X)\varphi_3(X) = 1 + X + X^4 + X^5 + X^7 + X^8 + X^9$$

It can be easily verified that $g(X)$ divides $X^{21}+1$. The Code generated by $g(X)$ is a $(21, 12)$ non-primitive BCH Code that corrects two errors.

Decoding of BCH Codes

Let codeword $\underline{v}$ represented by code polynomial

$$v(X) = v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-1} X^{n-1}$$

be the transmitted codeword.

The received polynomial is:

$$r(X) = r_0 + r_1 X + r_2 X^2 + \cdots + r_{n-1} X^{n-1}$$

Denoting the <u>error</u> polynomial by $e(X)$, we have:

$$r(X) = v(X) + e(X)$$

The syndrome is calculated multiplying $\underline{r}$ by H^T:

$$\underline{S} = (S_1, S_2, \ldots, S_{2t}) = \underline{r} \cdot H^T$$

That is, the i-th component of $\underline{S}$ is:

$$S_i = r(\alpha^i) = r_0 + r_1 \alpha^i + r_2 \alpha^{2i} + \cdots + r_{n-1} \alpha^{(n-1)i}$$

for $i = 1, 2, \ldots, 2t$.

Let's divide $r(X)$ by $\phi_i(X)$, i.e., the minimal polynomial of α^i:

$$r(X) = a_i(X)\phi_i(X) + b_i(X)$$

$\phi_i(\alpha^i) = 0$, therefore,

$$S_i = r(\alpha^i) = b_i(\alpha^i)$$

Example :

Consider (15, 7) BCH Code.

Let the received vector be

$$(1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0)$$

So,

$$r(X) = 1 + X^8$$

Let's find,

$$\underline{S} = (S_1, S_2, S_3, S_4)$$

The minimal polynomial for $\alpha, \alpha^2, \alpha^4$ is the same,

$$\phi_1(X) = \phi_2(X) = \phi_4(X) = 1 + X + X^4$$

and for ϕ^3, we have,

$$\phi_3(X) = 1 + X + X^2 + X^3 + X^4$$

dividing $r(X) = 1 + X^8$ by $\phi_1(X)$ we get

$$b_1(X) = X^2$$

Dividing $r(X)$ by $\phi_3(X)$, we get

$$b_3(X) = 1 + X^3$$

So $S_1 = b_1(\alpha) = \alpha^2$, $S_2 = \alpha^4$, $S_4 = \alpha^8$

and $S_3 = b_3(\alpha^3) = 1+\alpha^9 = 1+\alpha+\alpha^3 = \alpha^7$

So,

$$\underline{S} = (\alpha^2, \alpha^4, \alpha^7, \alpha^8)$$

Since $v(\alpha^i) = 0$ for $i = 1, 2, \cdots, 2t$

we have

$$S_i = r(\alpha^i) = v(\alpha^i) + e(\alpha^i) = e(\alpha^i)$$

Now, assume that we have ν errors at locations $j_1, j_2, \cdots, j_\nu$. That is,

$$e(X) = X^{j_1} + X^{j_2} + \cdots + X^{j_\nu}$$

Then we have

$$S_1 = \alpha^{j_1} + \alpha^{j_2} + \cdots + \alpha^{j_\nu}$$

$$S_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \cdots + (\alpha^{j_\nu})^2$$

$$\vdots$$

$$S_{2t} = (\alpha^{j_1})^{2t} + (\alpha^{j_2})^{2t} + \cdots + (\alpha^{j_\nu})^{2t}$$

Denote $\beta_1 = e^{j_1}$, $\beta_2 = e^{j_2}$, $\cdots$, $\beta_{\nu} = e^{j_\nu}$

$\beta_1, \beta_2, \cdots, \beta_{\nu}$ are called error location numbers.

We write:

$$S_1 = \beta_1 + \beta_2 + \cdots + \beta_\nu$$

$$S_2 = \beta_1^2 + \beta_2^2 + \cdots + \beta_\nu^2$$

$$\vdots$$

$$S_{2t} = \beta_1^{2t} + \beta_2^{2t} + \cdots + \beta_\nu^{2t}$$

These $2t$ equations are symmetric functions of $\beta_1, \beta_2, \ldots, \beta_\nu$

Define the following polynomial

$$\sigma(X) = (1+\beta_1 X)(1+\beta_2 X)(1+\beta_3 X)\cdots(1+\beta_\nu X)$$

This is called the error locator polynomial and has $\beta_1^{-1}, \beta_2^{-1}, \ldots \beta_\nu^{-1}$ as its roots.

$\sigma(X)$ can be also represented as:

$$\sigma(X) = \sigma_0 + \sigma_1 X + \sigma_2 X^2 + \cdots + \sigma_\nu X^\nu$$

It is clear that:

$$\sigma_0 = 1$$

$$\sigma_1 = \beta_1 + \beta_2 + \cdots + \beta_\nu$$

$$\sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \cdots + \beta_{\nu-1}\beta_\nu$$

$$\vdots$$

$$\sigma_\nu = \beta_1 \beta_2 \cdots \beta_\nu .$$

σ_i's can be shown to be related to Syndromes as follows:

$$S_1 + \sigma_1 = 0$$

$$S_2 + \sigma_1 S_1 + 2\sigma_2 = 0$$

$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + 3 S_3 = 0$$

$$\vdots$$

$$S_\nu + \sigma_1 S_{\nu-1} + \cdots + \sigma_{\nu-1} S_1 + \nu\sigma_\nu = 0$$

$$S_{\nu+1} + \sigma_1 S_\nu + \cdots + \nu_{n-1} S_2 + \sigma_\nu S_1 = 0$$

These are called Newton identities.

For the binary cas

$$i\sigma_i = \begin{cases} \sigma_i & \text{for odd } i \\ 0 & \text{for even } i \end{cases}$$

Iterative algorithm for finding Error-Location Polynomial:

This algorithm (Berlekamp Algorithm) tries to generate polynomials of degree 1, 2, ... that has $\beta_1, \beta_2, \ldots$ as its roots.

First we define $\sigma^{(1)}(X)$ that satisfies the first Newton equality: $\sigma^{(1)}(X) = 1 + S_1 X$

since $S_1 + \sigma_1 = 0 \Rightarrow \sigma_1 = S_1$.

Then we check whether $\sigma^{(1)}(X)$ satisfies the second Newton equality or not. If it satisfies we let $\sigma^{(2)}(X) = \sigma^{(1)}(X)$ otherwise we add another term to $\sigma^{(1)}(X)$ to form $\sigma^{(2)}(X)$ that satisfies the first and second equalities.

Note that for the case of $\sigma^{(2)}(X)$ always $\sigma^{(1)}(X)$ satisfies the second equality as:

$$S_2 + \sigma_1 S_1 + 2\sigma_2 = S_2 + S_1 \cdot S_1 + 0 = S_2 + S_1^2 = 0$$

So, always $\sigma^{(2)}(X) = \sigma^{(1)}(X)$.

Then for $\sigma^{(3)}(X)$: if $\sigma^{(2)}(X)$ satisfies the third equality we let $\sigma^{(3)}(X) = \sigma^{(2)}(X)$ otherwise add a correction term that makes $\sigma^{(3)}(X)$ satisfy the first three equalities.

We continue this iterative approach until we get $\sigma^{(2t)}(X)$ and set $\sigma(X) = \sigma^{(2t)}(X)$.

Now let's see how we can go from one stage say μ to $\mu+1$.

Assume that at stage μ, the polynomial is

$$\sigma^{(\mu)}(X) = 1 + \sigma_1^{(\mu)} X + \sigma_2^{(\mu)} X^2 + \cdots + \sigma_{L_\mu}^{(\mu)} X^{L_\mu}$$

If $\sigma^{(\mu)}(x)$ satisfies also $\mu+1$-st equality, then, $S_{\mu+1}$ should be

$$\sigma_1^{(\mu)} S_\mu + \sigma_2^{(\mu)} S_{\mu-1} + \cdots + \sigma_{L_\mu}^{(\mu)} S_{\mu+1-L_\mu}$$

We compare this with actual $S_{\mu+1}$. That is, we add this to $S_{\mu+1}$ and check whether we get zero or not. Let the sum be denoted by d_μ and call it discrepancy

$$d_\mu = S_{\mu+1} + \sigma_1^{(\mu)} S_\mu + \sigma_2^{(\mu)} S_{\mu-1} + \cdots + \sigma_{L_\mu}^{(\mu)} S_{\mu+1-L_\mu}$$

If this is zero, then $\sigma_1^{(\mu)}(x)$ also satisfies the $\mu+1$-st equality and therefore,

$$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x).$$

But if $d_\mu \neq 0$, then $\sigma^{(\mu)}(x)$ does not satisfy the $\mu+1$-st equality.

Note that:

$$d_\mu = \sum_{i=0}^{L_\mu} \sigma_i^{(\mu)} S_{\mu+1-i}$$

Now, let's go to a previous stage say, ρ, where $d_\rho \neq 0$.

$$d_\rho = \sum_{i=0}^{L_\rho} \sigma_i^{(\rho)} S_{\rho+1-i}.$$

and,

$$\sigma^{(\rho)}(X) = 1 + \sigma_1^{(\rho)} X + \sigma_2^{(\rho)} X^2 + \cdots + \sigma_{L_\rho}^{(\rho)} X^{L_\rho}$$

Let's form $\sigma^{(\mu+1)}(X)$ as:

$$\sigma^{(\mu+1)}(X) = \sigma^{(\mu)}(X) + A X^{\mu-\rho} \sigma^{(\rho)}(X)$$

Then,

$$d'_\mu = \sum_{i=0}^{L_\mu} \sigma_i^{(\mu)} S_{\mu+1-i} + \sum_{i=0}^{L_\rho} \sigma_i^{(\rho)} S_{\mu-\rho+1-i}$$

or,

$$d'_\mu = d_\mu + A d_\rho$$

in order for $d'_\mu = 0$ we need

$$A = d_\mu / d_\rho .$$

So, the procedure is as follows:

<u>Initialization</u>: Start with the first two rows according to the following Table:

Berlekamp's iterative procedure for finding the error-location polynomial of a BCH code.

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$
−1	1	1	0	−1
0	1	S_1	0	0
1				
2				
⋮				
$2t$				

<u>Iteration</u>:

For each μ form $d_\mu = S_{\mu+1} + \sigma_1^{(\mu)} S_\mu + \cdots + \sigma_{L_\mu}^{(\mu)} X$

where L_μ is the degree of $\sigma^{(\mu)}(X)$.

1) If $d_\mu = 0$ then $\sigma^{(\mu+1)}(X) = \sigma^{(\mu)}(X)$.

2) If $d_\mu \neq 0$ then:

$$\sigma^{(\mu+1)}(X) = \sigma^{(\mu)}(X) + d_\mu d_\rho^{-1} X^{\mu-\rho} \sigma^{(\rho)}(X)$$

where ρ is the row (the stage) where $d_\rho \neq 0$ and is closest to μ, i.e., $\mu - \rho$ is the smallest.

Termination:

Continue until you find $\sigma^{(2t)}(X)$ and let:

$$\sigma(X) = \sigma^{(2t)}(X).$$

Example:

Consider the (15, 5) Code we saw previously

Assume that

$$\underline{v} = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$$

is transmitted and

$$r = (000101000000100)$$

is received. Then $r(X) = X^3 + X^5 + X^{12}$.

The minimal polynomial for α, α^2 and α^4 is

$$\phi_1(X) = \phi_2(X) = \phi_4(X) = 1 + X + X^4.$$

For α^3 and α^6

$$\phi_3(X) = \phi_6(X) = 1 + X + X^2 + X^3 + X^4$$

For α^5,

$$\phi_5(X) = 1 + X + X^2.$$

Dividing $r(X)$ by $\phi_1(X)$, we get

$$b_1(X) = 1$$

Dividing $r(X)$ by $\phi_3(X)$, we get

$$b_3(X) = 1 + X^2 + X^3$$

and dividing by $\phi_5(X)$,

$$b_5(X) = X^2.$$

So:

$$S_1 = S_2 = S_4 = 1$$

and

$$S_3 = 1 + \alpha^6 + \alpha^9 = \alpha^{10}$$

$$S_6 = 1 + \alpha^{12} + \alpha^{18} = \alpha^5$$

and

$$S_5 = \alpha^{10}$$

Using Berlekamp method, we get $\sigma(X) = \sigma^{(6)}(X) = 1 + X + \alpha^5 X^3$

μ	$\sigma^{(\mu)}(X)$	d_μ	l_μ	$\mu - l_\mu$
-1	1	1	0	-1
0	1	1	0	0
1	$1+X$	0	1	0 (take $\rho = -1$)
2	$1+X$	α^5	1	1
3	$1+X+\alpha^5X^2$	0	2	1 (take $\rho = 0$)
4	$1+X+\alpha^5X^2$	α^{10}	2	2
5	$1+X+\alpha^5X^3$	0	3	2 (take $\rho = 2$)
6	$1+X+\alpha^5X^3$	—	—	—

We can verify that α^3, α^{10} and α^{12} are the roots of $\sigma(X)$.

$$(\alpha^3)^{-1} = \alpha^{12}$$

$$(\alpha^{10})^{-1} = \alpha^5$$

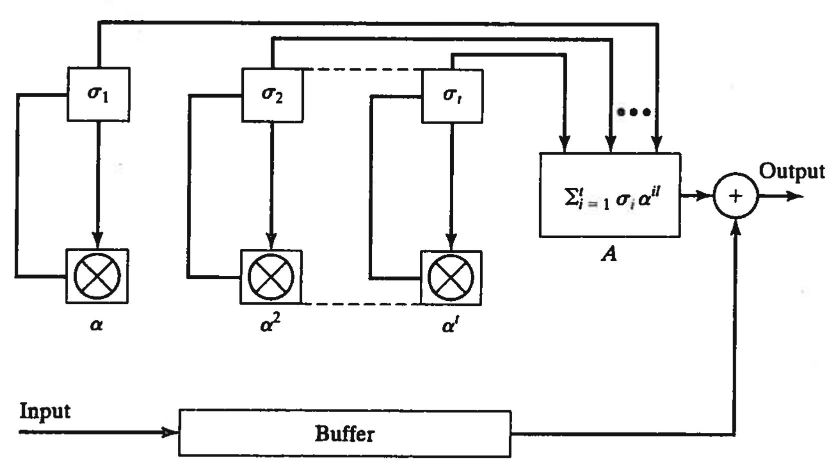
and $$(\alpha^{12})^{-1} = \alpha^3$$

So:

$$e(X) = X^3 + X^5 + X^{12}.$$

Error Correction Procedure:

1) Calculate Syndrome.
2) Form error-location polynomial $\sigma(X)$
3) Solve $\sigma(X)$ to get error locations (Chien Search).



Cyclic error location search unit.

Chien Search:

1) Load $\sigma_1, \sigma_2, \ldots, \sigma_{2t}$ in $2t$ registers.

(If $\sigma(X)$ has degree less than $2t$, i.e., $\mu < 2t$ then $\sigma_{\mu+1} = \sigma_{\mu+2} = \cdots = \sigma_{2t} = 0$)

2) The multipliers multiply σ_i by α^i and the circuit generates

$$\sigma_1 \alpha + \sigma_2 \alpha^2 + \cdots + \sigma_\mu \alpha^\mu$$

If α is a root of $\sigma(X)$ then

$$1 + \sigma_1 \alpha + \sigma_2 \alpha^2 + \cdots + \sigma_\mu \alpha^\mu = 0$$

or the output of A is 1.

So if output of A is 1 then α is a root and $\alpha^{-1} = \alpha^{n-1}$ is error location and r_{n-1} should be corrected.

3) Multipliers are clocked so we get

$$\alpha^2, (\alpha^2)^2, \ldots (\alpha^2)^\mu$$

or the output of A is

$$\sigma_1 \alpha^2 + \sigma_2 (\alpha^2)^2 + \cdots \sigma_\mu (\alpha^2)^\mu$$

if this is 1, r_{n-2} should be corrected.

and so on for $3, \ldots, \nu$