LESSON 5

BCH CODES
CORRECTION

Ex Use the primitive polynomial

$$p(x) = x^4 + x^3 + 1$$

to construct a 2 error correcting code.

Since $p(x)$ has degree 4

$f(x) = x^{15} - 1$ which factors as

$(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x+1)$

We need the power polynomial table for $p(x)$

		Rewrite col. 2
a	a	a
a^2	a^2	a^2
a^3	a^3	a^3
a^4	a^3+1	a^3+1
a^5	$(a^3+1)+a$	a^3+a+1
a^6	$(a^3+1)+a+a^2$	a^3+a^2+a+1
a^7	$(a^3+1)+a+a^2+a^3 = a^2+a+1$	a^2+a+1
a^8	a^3+a^2+a	a^3+a^2+a
a^9	$a^3+1+a^3+a^2 = a^2+1$	a^2+1
a^{10}	a^3+a	a^3+a
a^{11}	$(a^3+1)+a^2$	a^3+a^2+1
a^{12}	$(a^3+1)+a+a^3 = a+1$	$a+1$
a^{13}	a^2+a	a^2+a
a^{14}	a^3+a^2	a^3+a^2
a^{15}	$(a^3+1)+a^3 = 1$	1

Since the code is 2 error correcting we need the polynomials tha ~~T~~ ~~a~~ ~~is a, a^2, a^3, a^4~~ ~~root~~ of

a, a^2, a^3, a^4 is a root of where a is a root of $p(x) = x^4 + x + 1$.

Then a, a^2 and a^4 are all roots of $p(x)$

For a^3 consider

$$m_3(x) = x^4 + x^3 + x^2 + x + 1$$

$$m_3(a^3) = a^{12} + a^9 + a^6 + a^3 + 1$$
$$= (a+1) + (a^2+1) + (a^3 + 1 + a + a^2)$$
$$+ a^3 + 1 = 0$$

So $m_3(x)$ has a^3 as a root

Then

$$g(x) = m_1(x)\, m_3(x) =$$
$$(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

BCH CODES
ERROR CORRECTION

We have seen how to construct BCH codes. In particular, they can be designed to correct t errors. If $c(x)$ is sent and $r(x)$ is received, then

$$r(x) = c(x) + e(x)$$

where $e(x)$ is the error

$$e(x) = x^{m_1} + \cdots + x^{m_p} \quad \text{with } p \le t.$$

If $m_1, \ldots m_p$ can be found, then $e(x)$ is known and $c(x)$ can be found as usual.

In constructing the code, a primitive polynomial is found and a root of the polynomial is used. Let $p(x)$ be the polynomial and a be a root. We use $a, a^2, \ldots a^{2t}$ to correct t errors. The generating polynomial for the code is $g(x)$, which we know how to find, and $c(x) = g(x)h(x)$. Then $c(a^i) = g(a^i)h(a^i) = 0$ since $g(a^i) = 0$. Hence if $c(x)$

is a code word, then $c(a^i)=0$ for $i=1,\dots,2t$. Conversely if $c(a^i)=0$ for $i=1,\dots,2t$, then $m_i(x)$ (related to a^i) has a^i as a root so

$$m_i(a^i)=0 \rightarrow$$
$$g(a^i)=0 \rightarrow$$
$$c(a^i)=0.$$

Thus

Theorem. In the BCH code, $c(x)$ if a code word if and only if $c(a^i)=0$ for $i=1,\dots,2t$.

Error Correction

$$r(x) = c(x) + e(x) \rightarrow$$
$$r(a^i) = c(a^i) + e(a^i) = e(a^i)$$

for $i=1,\dots,2t$. Since we know $r(x)$ and a^i, $e(a^i)$ can be computed. We will use

$$S_i = r(a^i) \quad i=1,\dots,2t.$$

The S_i are called the syndromes for ~~to~~ $r(x)$ and are computed to be used in the correction

We define the Error Locator Polynomial

$$E(z) = (z-a^{m_1})\cdots(z-a^{m_p})$$
$$= z^p + \sigma_1 z^{p-1} + \cdots \sigma_p$$

We do not know the m_i so $E(z)$ has been defined theoretically but we do not know it. Is our intent to find it and so find the m_i. The following calculations are theoretical to prove the forthcoming method but we do not do them in practice.

$$E(a^{m_j}) = (a^{m_j})^p + \sigma_1 (a^{m_j})^{p-1} + \cdots + \sigma_p = 0$$

for $j = 1, \ldots p$. The value is 0 since a^{m_j} is a root of $E(z)$. Multiply each row by $(a^{m_j})^k$:

$$(a^{m_1})^k \left[(a^{m_1})^p + \sigma_1 (a^{m_1})^{p-1} + \cdots + \sigma_p \right] = 0$$

$$(a^{m_2})^k \left[(a^{m_2})^p + \sigma_1 (a^{m_2})^{p-1} + \cdots + \sigma_p \right] = 0$$

$$(a^{m_p})^k \left[(a^{m_p})^p + \sigma_1 (a^{m_p})^{p-1} + \cdots + \sigma_p \right] = 0$$

Distribute the leading term, then add down each column to get

$$e(a^{k+p}) + \sigma_1 e(a^{k+p-1}) + \cdots + \sigma_p e(a^k) = 0$$

$$= r(a^{k+p}) + \sigma_1 r(a^{k+p-1}) + \cdots + \sigma_p r(a^k) = 0$$

$$= S_{k+p} + \sigma_1 S_{k+p-1} + \cdots + \sigma_p S_k = 0$$

where the S's are the syndromes

Let $k = 1, \ldots, p$ and we get p equations, the first of which is

$$S_{1+p} + \sigma_1 S_{1+p-1} + \cdots + \sigma_p S_1 = 0$$

These equations can be represented by a matrix equation

$$\begin{bmatrix} S_1 & S_2 & & S_p \\ S_2 & S_3 & & S_{p+1} \\ & \vdots & & \\ S_p & S_{p+1} & & S_{2p-1} \end{bmatrix} \begin{pmatrix} \sigma_p \\ \\ \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_{p+1} \\ S_{p+2} \\ \\ S_{2p} \end{pmatrix}$$

We have gone from a hypothetical situation to a concrete one since we know $S_1, \ldots S_{2p}$. We solve the matrix equation to find $\sigma_p, \ldots \sigma_1$. Then we know $\epsilon(z)$ and can find the roots a^{m_i}, just what we need for then the error, $e(x)$, can be found

In the process, we do not know p so we assume the maximal number of errors $p = t$.

If t is too big, the matrix will not have an inverse; it has determinant 0, so we try to solve the problem assuming $t-1$ errors. Continue this process until we get an answer

Throughout this process we continually use the power polynomial table for the computations

Ex Let C be the $[15, 5]$ code constructed last time with generator polynomial

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

We constructed this to correct 3 errors and used the primitive polynomial $m(x) = x^4 + x + 1$ with root a. We constructed the table

a	a	a^6	a^3+a^2	a^{11}	a^3+a^2+a
a^2	a^2	a^7	a^3+a+1	a^{12}	a^3+a^2+a+1
a^3	a^3	a^8	a^2+1	a^{13}	a^3+a^2+1
a^4	$a+1$	a^9	a^3+a	a^{14}	a^3+1
a^5	a^2+a	a^{10}	a^2+a+1	a^{15}	1

We use this in the many computations

Suppose $r = (101111110010000)$ is received. This becomes polynomial

$$r(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{10}$$

$\in \mathbb{Z}_2[x]$. As the code is 3 error correcting, 6 syndromes are needed

$$S_1 = r(a) = 1 + a^2 + a^3 + a^4 + a^5 + a^6 + a^7 + a^{10}$$
$$= 1 + a^2 + a^3 + (a+1) + (a^2+a) + (a^3+a^2) + (a^3+a+1) + (a^2+a+1)$$
$$= a^3$$

$$S_2 = r(a^2) = r(a)^2 = a^6$$

$$S_3 = r(a^3) = 1 + a^6 + a^9 + a^{12} + a^{15} + a^{18} + a^{21} + a^{30}$$
$$= 1 + a^6 + a^9 + a^{12} + 1 + a^3 + a^6 + 1$$
$$= 1 + a^3 + a^9 + a^{12}$$
$$= 1 + a^3 + (a^3 + a) + (a^3 + a^2 + a + 1)$$
$$= a^3 + a^2 = a^6$$

$$S_4 = r(a^4) = r(a^2)^2 = a^{12}$$

$$S_5 = r(a^5) = 1 + a^{10} + 1 + a^5 + a^{10} + 1 + a^5 + a^5$$
$$= a^2 + a + 1 = a^{10}$$

$$S_6 = r(a^6) = r(a^3)^2 = a^{12}$$

Recall $a^{15} = 1$ since we started with $f(x) = x^{15} - 1$ and $f(a) = a^{15} - 1 = 0$

Then

$$\begin{pmatrix} a^3 & a^6 & a^6 \\ a^6 & a^6 & a^{12} \\ a^6 & a^{12} & a^{10} \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^{12} \\ a^{10} \\ a^{12} \end{pmatrix}$$

We use Cramer's Rule

Let A be the coefficent matrix

$$\begin{aligned} \det A &= a^{19} + a^{24} + a^{24} + a^{18} + a^{27} + a^{22} \\ &= a^4 + a^3 + a^{12} + a^7 \\ &= a+1 + a^3 + a^3 + a^2 + a + 1 + a^3 + a + 1 \\ &= a^{12} \end{aligned}$$

Since $\det A \neq 0$, there are 3 errors, the maximum number

To find σ_3, replace the first column of A by the right hand side of the equation:

$$B = \begin{pmatrix} a^{12} & a^6 & a^6 \\ a^{10} & a^6 & a^{12} \\ a^{12} & a^{12} & a^{10} \end{pmatrix}$$

$\det B = a^{14}$. $\sigma_3 = \dfrac{\det B}{\det A} = \dfrac{a^{14}}{a^{12}} = a^2$

To find σ_2 replace the second column of A by the right hand side of the equation

$$C = \begin{pmatrix} a^3 & a^{12} & a^6 \\ a^6 & a^{10} & a^{12} \\ a^6 & a^{12} & a^{10} \end{pmatrix}$$

$$\det C = a^{10}$$

$$\sigma_2 = \frac{a^{10}}{a^{12}} = a^{-2} = a^{13}$$

(Recall $a^{15} = 1$)

For σ_1

$$D = \begin{pmatrix} a^3 & a^6 & a^{12} \\ a^6 & a^6 & a^{10} \\ a^6 & a^{12} & a^{12} \end{pmatrix}$$

$$\det D = 1$$

$$\sigma_1 = \frac{1}{a^{12}} = a^{-12} = a^3$$

So

$$E(z) = z^3 + a^3 z^2 + a^{13} z + a^2$$
$$= z^3 + \sigma_1 z^2 + \sigma_2 z + \sigma_3$$

Which a^2 are roots?

Trial and error gives: $1, a^5, a^{12}$

So $e(x) = 1 + x^5 + x^{12}$ and

$$c(x) = r(x) + e(x) = x^2 + x^3 + x^4 + x^6 + x^7 + x^{10} + x^{12}$$

Ex In a code designed for 3 errors, what happens if fewer than 3 errors have been made?

Using the same code as in the last example, suppose

$$r = (1001000100110101)$$

This becomes the polynomial

$$r(x) = 1 + x^3 + x^7 + x^{10} + x^{11} + x^{13}$$

The syndromes are found

$$S_1 = a^5 \qquad S_4 = a^5$$
$$S_2 = a^{10} \qquad S_5 = 1$$
$$S_3 = a^2 \qquad S_6 = a^4$$

Setting up the matrix equation

$$\begin{pmatrix} a^5 & a^{10} & a^2 \\ a^{10} & a^2 & a^5 \\ a^2 & a^5 & 1 \end{pmatrix} \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^5 \\ 1 \\ a^4 \end{pmatrix}$$

The coefficent matrix A has

$$\det A = a^7 + a^{17} + a^{17} + a^6 + a^{15} + a^{20}$$
$$= a^7 + a^2 + a^2 + a^6 + 1 + a^5$$
$$= (a^3 + a + 1) + (a^3 + a^2) + 1 + (a^2 + a)$$
$$= 0$$

This says the coefficient matrix has no inverse, There is no solution. Hence there are less than 3 errors. We look for two errors:

$$\begin{pmatrix} a^5 & a^{10} \\ a^{10} & a^2 \end{pmatrix} \begin{pmatrix} \sigma_2 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} a^2 \\ a^5 \end{pmatrix}$$

where we have used only syndromes S_1, S_2, S_3 and S_4

$$\det A = a^{20} + a^{20} = (a^3 + a + 1) + a^5$$
$$= a^3 + a + 1 + a^2 + a = a^{13}$$

To find σ_2

$$\det \begin{pmatrix} a^2 & a^{10} \\ a^5 & a^2 \end{pmatrix} = a^4 + a^{15} = a + a + 1 + 1$$
$$= a + a = a$$

$$\sigma_2 = \frac{a}{a^{13}} = \frac{1}{a^{12}} = a^3$$

To find σ_1

$$\det \begin{pmatrix} a^5 & a^2 \\ a^{10} & a^5 \end{pmatrix} = a^{10} + a^{12}$$
$$= (a^2 + a + 1) + (a^3 + a^2 + a + 1) =$$
$$a^3$$

$$\sigma_1 = \frac{a^3}{a^{13}} = \frac{1}{a^{10}} = a^5$$

$$E(z) = z^2 + a^5 z + a^3$$

Trial and error finds the roots, a and a^2. Thus

$$e(x) = x + x^2$$

$$c(x) = 1 + x + x^2 + x^3 + x^7 + x^{10} + x^{11} + x^{13}$$

Thm. If we use the first $2t$ powers of a root of a primitive polynomial, the above process corrects t errors.

Proof As before we start with n, compute $m = 2^n - 1$ to get the polynomial and root a

let
$$H = \begin{pmatrix} 1 & a & a^2 & & a^{m-1} \\ 1 & a^2 & (a^2)^2 & & (a^2)^{m-1} \\ 1 & a^3 & (a^3)^2 & & (a^3)^{m-1} \\ \vdots & & & & \\ 1 & a^{2t} & (a^{2t})^2 & & (a^{2t})^{m-1} \end{pmatrix}$$

For any polynomial

$$r(x) = b_0 + b_1 x \quad + b_{m-1} x^{m-1},$$

let $b = (b_0, \ldots b_{m-1})$ Then

$$H b^T = (s_1, \ldots s_{2t})^T \text{ are}$$

the syndromes

So $r(x) \in C$ iff $Hb^T = 0$ and H is a parity check matrix for C. The minimum number of linearly dependent vectors is $2t+1$. First, any $2t$ columns are linearly independent. Choose columns in positions $j_1 < \cdots < j_{2t}$. The columns in these positions give

$$\begin{pmatrix} a^{j_1} & a^{j_2} & & a^{j_{2t}} \\ (a^2)^{j_1} & (a^2)^{j_2} & & (a^2)^{j_{2t}} \\ & & & \\ (a^{2t})^{j_1} & (a^{2t})^{j_2} & & (a^{2t})^{j_{2t}} \end{pmatrix}$$

The determinant is

$$\begin{pmatrix} 1 & 1 & & 1 \\ a^{j_1} & a^{j_2} & & a^{j_{2t}} \\ & & & \\ (a^{j_1})^{2t-1} & (a^{j_2})^{2t-1} & & (a^{j_{2t}})^{2t-1} \end{pmatrix}$$

$\neq 0$ since this is a Vandermonde determinant. Hence any $2t$ columns are linearly independent as is always true for non-singular matrices (those whose determinant is not 0

H has $2t$ rows so any $2t+1$ columns are linearly dependent. This shows the claim and by a previous result, C is t-error correcting.

Problems

1. Use $p(x) = x^4 + x + 1$ to construct a generator matrix for a [15, 7] code. How many errors can be corrected? How many codewords are there?

2. Correct the following using the code in problem 1

$r = (110011001100011)$
$r = (001101111100110)$
$r = (100001111110010)$

3. Problem 17 page 134
(Be careful, there is one place that you could make an error if not careful)