BCH CODES

I. FINITE FIELDS

We begin by discussing information on finite fields that are needed for this chapter.

Let Z_p be the ring of integers mod p where p is a prime. Since p is a prime, Z_p is a field

Let $Z_p[x]$ be the ring of polynomials with coefficients from Z_p. If $m(x) \in Z_p[x]$, then $Z_p[x]/(m(x)) = R$ is a ring with multiplication mod $m(x)$. This ring consists of all polynomials of degree $<$ degree$(m(x)) \equiv n$. It is also a vector space of dimension n with basis $1, x, \ldots x^{n-1}$ and has p^n elements.

If $m(x)$ is irreducible, then R is a field. Since R is a finite field, the non-zero elements are a cyclic group. It is useful to consider the elements of R both as polynomials and as powers of a cyclic generator. Frequently, the cyclic generator corresponds to a root of $m(x)$. In that case $m(x)$ is called primitive.

We now let $p=2$, the case we are interested in. Then $(x+y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$ and this extends; for instance $(x+y+z)^2 = x^2 + y^2 + z^2$. Now suppose $m(x) = a_n x^n + \cdots + a_0$, each $a_i = 0$ or 1. Then

$$m(a) = a_n a^n + \cdots + a_0 \text{ and}$$
$$m(a^2) = a_n a^{2n} + \cdots + a_0 = (a_n a^n + \cdots + a_0)^2.$$

So, if a is a root of $m(x)$, then so is a^2 (and a^4, a^8)

Ex. Let $m(x) = x^4 + x + 1 \in \mathbb{Z}_2(x)$

$m(x)$ is irreducible, hence $R = \mathbb{Z}_2(x)/(m(x))$ is a field of order $2^4 = 16$ elements. Let a be a root of $m(x)$. Then a^2, a^4, a^8 are all the roots of $m(x)$. We have a power-polynomial table

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

Since a has order 15 in a group of order 15, a is a cyclic generator

Let $m(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$

$m(x)$ is irreducible. Let a be a root. Show that $a^5 = 1$, so a is not a cyclic generator and $m(x)$ is not primitive. The field has a cyclic generator, it is just not a root of $m(x)$

B-C-H CODES CONSTRUCTION

Let m be a positive integer and $n = 2^m - 1$. Let $f(x) = x^n - 1$ and $V = Z_2[x]/(f(x))$. V has dimension n and consists of 2^n elements written as polynomials of degree $< n$. This is the space of vectors in which the B.C.H code is a subspace.

If $m(x)$ is an irreducible polynomial of degree m, then $m(x)$ can be used to construct a finite field F of ~~degree~~ order 2^m. as in the last section the non zero elements are a cyclic group and satisfy $x^{n-1} = 1$. The roots of $m(x)$ are roots of $f(x) = x^{n-1} - 1$ and, since $m(x)$ is irreducible, $m(x)$ divides $f(x)$ evenly.

Ex. Let $m=4$, $n=2^m-1=15$ $f(x)=x^{15}-1$

$\dim V=15$ $|V|=2^{15}$ Now

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

is the decomposition of $f(x)$ into irreducible factors in $Z_2[x]$ (This can be found using MAPLE, etc or found in extensive tables, or computed) We have seen ~~that~~ that $m(x)=x^4+x+1$ is used to construct a field with $2^4=16$ elements, every non zero element satisfies $f(x)=x^{15}-1$ ~~and m(x)~~ In the last section we computed a power-polynomial table

To construct C, decide how many errors we want our code to correct. If it is t, we need the first $2t$ powers of the root, a.

Each of those is a root of $f(x)$, so is a root of one of the factors we have displayed. Find each polynomial for the 2^t powers of a and let $g(x)$ = product of these polynomials, using each one just once. If $\deg g(x) = d$, then $C = \{r(x)g(x);$ $\deg r(x) < 2^m - 1 - \deg g(x)\}$ $(n = 2^m - 1)$ and $\dim C = n - d$

Ex Let $t=2$ and a be a root of $m(x) = x^4 + x + 1$. a^2 is also a root as is a^4. a^3 is a root of $x^4 + x^3 + x^2 + x + 1$. Thus

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

$\deg g(x) = 8$, $\dim C = 15 - 8$ with basis $g(x), x\,g(x), x^2 g(x), \ldots x^6 g(x)$.

C is a $[2^t - 1, 2^t - 1 - \cancel{\dim C}\ \deg g(x)] = [15, 7]$ code

$= [\dim V, \dim C]$

Ex Continue with $t=3$

We need the factors whose roots are a a^2 a^3 a^4 a^5 a^6

x^4+x+1 has roots a a^2 a^4

$x^4+x^3+x^2+x+1$ has root a^3, hence also a^6

x^2+x+1 has a^5 as a root

$g(x)$ = product of these three polynomials $= x^{10}+x^8+ \quad + x^4+x^2+x+1$

$\dim C = 15-10=5$

$C = \langle g(x), xg(x), \ldots x^4 g(x) \rangle$

This code is all polynomials of degree < 15 which have $g(x)$ as a factor. This is a $[15,5]$ code, $15 = \dim V$, $5 = \dim C$

ERROR CORRECTION

Theorem. Let $p(x) \in Z_2(x)$ be a primitive polynomial of degree n and let C be the BCH code that results from the first s powers of $a = x$ in $Z_2(x)/(p(x))$. Then $c(x) \in Z_2(x)$ is in C if and only if $c(a^i) = 0$ for $i = 1, \ldots, s$

Proof Let $m_i(x)$ be the smallest polynomial that a^i satisfies, $i = 1, \ldots, s$. and $g(x)$ is the least common multiple of the $m_i(x)$. If $c(x) \in C$, then $c(x) = g(x)h(x)$ for some $h(x)$.. Then $c(a^i) = g(a^i)h(a^i)$ $= 0\, h(a^i) = 0$ for $i = 1, \ldots, s$ Conversely if $c(a^i) = 0$ for $i = 1, \ldots, s$, then $m_i(x)$ divides $c(x)$ since they have a common root, a^i, and $m_i(x)$ is irreducible Thus $g(x)$ divides $c(x)$ and $c(x) \in C$

Let $p(x) \in Z_2[x]$ be a primitive polynomial of degree n and let C be the BCH code that results from the first $2t$ powers of $a = x$ in $Z_2[x]/(p(x))$. It can be shown that C is t-error correcting. If $c(x)$ is sent and $r(x)$ is received, $r(x) = c(x) + e(x)$ where $e(x) = x^{m_1} + \cdots + x^{m_p}$, $m_1 < m_2 < \cdots < m_p$ and $p \le t$ giving the error positions. Note that $r(a^i) = c(a^i) + e(a^i) = e(a^i)$, $i = 1, \ldots, 2t$. The $r(a^i)$ are called the syndromes. Let $S_1 = r(a^1)$, $S_2 = r(a^2), \ldots S_{2t} = r(a^{2t})$. The Error Locator Polynomial is

$$E(z) = (z - a^{m_1})(z - a^{m_2}) \cdots (z - a^{m_p})$$
$$= z^p + \sigma_1 z^{p-1} + \cdots + \sigma_p \quad \text{where}$$

The σ_i are elementary symmetric functions in $a^{m_1}, \ldots a^{m_p}$:

$$\sigma_1 = \sum_{i=1}^{p} a^{m_i}$$

$$\sigma_2 = \sum_{1 \le m_i < m_j \le p} a^{m_i} a^{m_j}$$

$$\sigma_3 = \sum_{1 \le i < j < k \le p} a^{m_i} a^{m_j} a^{m_k}$$

$$\vdots$$

$$\sigma_p = a^{m_1} \cdots a^{m_p}$$

Note that $E(z)$ has been theoretically constructed. We do not know the a^{m_i}; in fact, is they that we want to find. The following constructions are all theoretical as well.

Compute

$$* \; a^{m_j} E(a^{m_j}) = a^{m_j}\left[a_{m_j}^{p} + \sigma_1 (a^{m_j})^{p-1} + \cdots + \sigma_p\right] = 0$$

(since a^{m_j} is a root of $E(z)$) for each $j = 1, \ldots, p$

Add those expressions to get

$$e(a^{k+p}) + \sigma_1 e(a^{k+p-1}) + \sigma_2 e(a^{k+p-2}) + \sigma_p e(a^k) = 0$$

Since $r(a^i) = e(a^i)$ for each i,

$$S_{k+p} + \sigma_1 S_{k+p-1} + \sigma_2 S_{k+p-2} + \cdots \sigma_p S_k = 0$$

which holds for $1 \le k \le p$

In matrix form

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

If the coefficient matrix is non-singular, then we can solve for $\sigma_1, \ldots \sigma_p$ and then we know the Error Locator Polynomial. We find the a^{m_i} by plugging in each a^i and seeing which ones give us 0. ie compute $E(a^i)$ for each i.

If the coefficient matrix is singular, then there are less than t errors. We then set up the problem to search for $t-1$ errors. We now show examples of each of these situations.

13

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

$$A \begin{pmatrix} \sigma_3 \\ \sigma_2 \\ \sigma_1 \end{pmatrix}$$

$$\det A = a^{19} + a^{24} + a^{24} + a^{18} + a^{27} + a^{22}$$

$$= a^4 + a^3 + a^{12} + a^7$$

$$= a+1 + a^3 + (a^3+a^2+a+1) + (a^3+a+1)$$

$$= a^{12} \neq 0 \quad A \text{ is non-singular}$$

We use Cramers Rule

For σ_3

$$\det \begin{pmatrix} a^{12} & a^6 & a^6 \\ a^{10} & a^6 & a^{12} \\ a^{12} & a^{12} & a^{10} \end{pmatrix} = a^{14} \qquad \sigma_3 = \frac{a^{14}}{a^{12}} = a^2$$

For σ_2

$$\det \begin{pmatrix} a^3 & a^{12} & a^6 \\ a^6 & a^{10} & a^{12} \\ a^6 & a^{12} & a^{10} \end{pmatrix} = a^{10} \qquad \sigma_2 = \frac{a^{10}}{a^{12}} = \frac{1}{a^2} = a^{13}$$

For σ_1

$$\det \begin{pmatrix} a^3 & a^6 & a^{12} \\ a^6 & a^6 & a^{10} \\ a^6 & a^{12} & a^{12} \end{pmatrix} = 1 \qquad \sigma_1 = \frac{1}{a^{12}} = a^3$$

$$E(z) = z^3 + a^3 z^2 + a^{13} z + a^2$$

The roots are $1 + a^5, a^{12}$

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

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

Example Let C be the BCH code with $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$.

Suppose $r = (1\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0)$ is received. Turn this into

$$r(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{10} \in \mathbb{Z}_2[x]$$

C is 3 error correcting so we use 6 powers of a

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

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

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

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

$$S_5 = r(a^5) = 1 + a^{10} + a^{15} + a^{20} + a^{25} + a^{30} + a^{35} + a^{50}$$
$$= 1 + a^{10} + 1 + a^5 + a^{10} + 1 + a^5 + a^5$$
$$= 1 + a^5 = a^{10}$$

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

Continue example

If $r = (1\,0\,0\,1\,0\,0\,0\,1\,1\,0\,1\,0)$

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

Now $S_1 = a^5$

$S_2 = a^{10}$

$S_3 = a^2$

$S_4 = a^5$

$S_5 = 1$

$S_6 = a^4$

$$A = \begin{pmatrix} a^5 & a^{10} & a^2 \\ a^{10} & a^2 & a^5 \\ a^2 & a^5 & 1 \end{pmatrix} = 0$$

So 3 errors were not committed

Try 2 errors

Using the same syndromes

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

$\det A \neq 0$. So look for 2 errors

Use Cramer's Rule

For σ_2

$$\det \begin{pmatrix} a^2 & a^{10} \\ a^5 & a^2 \end{pmatrix} = a^4 + a^{15} \qquad \sigma_2 = a^3$$

$$\det \begin{pmatrix} a^5 & a^2 \\ a^{10} & a^5 \end{pmatrix} = a^{10} + a^{12} \qquad \sigma_1 = a^5$$

$$\epsilon(z) = z^2 + a^5 z + a^3$$

Roots: a, a^2

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

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