

LESSON 5

BCH CODES I

1

BCH CODES

POLYNOMIAL RINGS

Let $\mathbb{Z}_2[x]$ be the collection of all polynomials with coefficients from \mathbb{Z}_2 . with the usual polynomial addition and multiplication.

$$\text{Ex } f(x) = x^5 + x^2 + x$$

If $f(x) \in \mathbb{Z}_2[x]$, then $R = \mathbb{Z}_2[x]/(f(x))$ stands for all polynomials of degree less than $\deg(f(x))$ and addition and multiplication are $\text{mod}(f(x))$. In particular, if $g(x), h(x) \in R$, to compute $g(x)h(x)$, first multiply them as usual, then divide by $f(x)$ and the remainder, $r(x)$ is the product

$$g(x)h(x) = r(x) \text{ mod}(f(x))$$

$$\text{Ex } f(x) = x^4 - 1 \quad g(x) = x^3 + x \quad h(x) = x^3 + x^2$$

$$\text{Then } g(x)h(x) = x^6 + x^5 + x^4 + x^3$$

Then $x^4 - 1$ divides into $g(x)h(x)$ to get $x^2 + x + 1$

Thus,

$$(x^3 + x)(x^3 + x) = x^6 + x^5 + x^4 + x^3 \text{ in } R$$

$$\text{So } g(x) h(x) = x^3 + x^2 + x + 1 \text{ in } R$$

A discussion of these ideas is in Chapter 1 of the Text.

R is a ring and a vector space over \mathbb{Z}_2 . It has basis $1, x, \dots, x^{n-1}$ where $n = \deg f(x)$. Also R has dimension n and contains 2^n elements.

For BCH codes, let $n = 2^m - 1$ and $f(x) = x^n - 1$. R is the space of all vectors in the code. Let $g(x)$ be a polynomial that divides $f(x)$. C consists of all multiples of $g(x)$ whose degree is less than n .

$$\text{Ex} \quad \text{Let } m = 3 \quad n = 2^3 - 1 = 7 \quad f(x) = x^7 - 1$$

$$g(x) = x^3 + x + 1.$$

$$C = \langle x^3 + x + 1, x(x^3 + x + 1), x^2(x^3 + x + 1), x^3(x^3 + x + 1) \rangle$$

C has dimension 4, with basis The elements displayed.

To construct a BCH code we first need to construct

3

a field. To do this, we take the $g(x)$ above to be irreducible over \mathbb{Z}_2 . It also has a special property: it's root will be a cyclic generator of the field. Not all irreducible polynomials have this property, so we need to check that the one we pick does have it.

It is a very important fact that for any finite field, such a polynomial exists.

Ex Let $f(x) = x^7 - 1$. Let $p(x) = x^3 + x + 1$
 In the finite field $\mathbb{Z}_2[x]/(p(x))$
 $p(x) = 0$ is an identity. In the finite field, to avoid confusion, we let a be a root and the identity is $a^3 + a + 1 = 0$. Now the field has $2^{\deg p(x)} = 2^3 = 8$ elements.
 We construct a table to be used in calculations

Powers of a Polynomial

a	a
a^2	a^2
a^3	$a + 1$
a^4	$a^2 + a$
a^5	$a^2 + a + 1$
a^6	$a^3 + 1$
a^7	1

This Table shows that a is a cyclic generator for the group of non-zero elements, so $p(x)$ is primitive. Adding 0 to the list gives the finite field

Summary So Far.

Pick m , $n = 2^m - 1$, $f(x) = x^n - 1$

We construct a finite field with 2^m elements by using a primitive polynomial $g(x)$ that is a divisor of $f(x)$ and has degree m . We compute the power-polynomial table using that for a root α of $g(x)$, $g(\alpha) = 0$.

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

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

into irreducible polynomials. We need a factor of degree $m = 4$, and we need it to be primitive. There are tables of this information and it can be found using a computer algebra package like Python or Sage. The first 3 factors have ~~the~~^{The} correct degree

5

but only the first 2 are primitive. We would find that the third one does not work by computing a power-polynomial table and finding we get a power equal to 1 before $a^n = a^r$.

We use the first factor

$$a^4 + a + 1 = 0$$

Power	Polynomial	Power	Poly	Power	Poly
a^0	a^0	a^1	$a^3 + a^2$	a^{11}	$a^3 + a + 1$
a^1	a^1	a^2	$a^3 + a + 1$	a^{12}	$a^3 + a^2 + a + 1$
a^3	a^3	a^4	$a^2 + 1$	a^{13}	$a^3 + a^2 + 1$
a^4	$a + 1$	a^5	$a^3 + a$	a^{14}	$a^3 + 1$
a^r	$a^r + a$	a^{10}	$a^2 + a + 1$	a	1

For example: $a^{12} = a^3 + a^2 + a + 1$,
 $a \cdot a^{12} = a^{13} = a^4 + a^3 + a^2 + a = (a + 1) + a^3 + a^2 + a$
 $= a^3 + a^2 + 1$

To continue on constructing the code, we decide how many errors we want the code to correct. Say it is t . We take the first $2t$ powers of a

Ex Suppose $t=2$. Take a, a^1, a^3, a^4 .

Now each of these is a root of $x^{15}-1$ since they are in the group of non zero elements

6

in the field we constructed. The field has 16 elements, 15 make up the non zero ones. The group has order 15 and Lagrange's Theorem tells us $b^{15} = 1$ for any b in a group of order 15. That is $f(a^k) = (a^k)^{15} - 1 = 0$. Since a^k is a root of $f(x)$, it is a root of one of the factors. We find which factors a, a^3, \dots, a^{15} are roots of and multiply those factors together (using each just once) to get the polynomial which constructs the code.

We have some help since we are working in a finite field where $x = -x$ i.e. $2x = 0$. Then

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$$

So if $f(a) = 0$

Then $h(a^2) = h(a)^2 = 0$. If a is a root so is a^2, a^4, a^8 etc. This is very helpful.

Ex We continue the example where

$$f(x) = x^5 - 1$$

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

If $t=2$ errors are to be corrected, we need to find the factors for which $\alpha, \alpha^2, \alpha^3, \alpha^4$ are roots

We have by earlier construction that α is a root of

$$m_1(x) = x^4 + x + 1$$

Thus α^2 and α^4 are also roots of $m_1(x)$. Only α^3 remains

$$\text{Thus } m_2(x) = x^4 + x^3 + 1$$

$$\begin{aligned} m_2(\alpha^3) &= \alpha^{12} + \alpha^9 + 1 = \\ (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha) + 1 &= \alpha^2 + 6 \end{aligned}$$

$$\text{Thus } m_3(x) = x^4 + x^3 + x^2 + x + 1$$

$$\begin{aligned} m_3(\alpha^3) &= \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 \\ &= (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha) + (\alpha^3 + \alpha^2) + \alpha^3 + 1 \\ &= 0 \end{aligned}$$

So $m_3(x)$ is the poly we are looking for now

$$\begin{aligned} P(x) &= m_1(x)m_3(x) \\ &= (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) \\ &= x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

The code space is all multiples of $p(x)$ up to degree 14

A basis for C :

$$P(x), xP(x), x^2P(x), x^3P(x), x^4P(x), x^5P(x), x^6P(x)$$

dim C has dimension $7 = 15 - \deg p(x)$

This is a $[15, 7]$ code

Homework

1. Use this $f(x) = x^r - 1$ to correct 3 errors. What is $p(x)$ and C . What is dimension C ? What are the parameters of the code?
2. Use $f(x) = x^7 - 1$ to construct
 - a. 1 error. What is $p(x)$ and C ?
 - b. 2 errors. What is $p(x)$ and C ?

3 Problem 17 page 134