Lisa Giang
Laura Yamashiro
Anita Nensey
MATH 590

BCH Code Size 32

Start with an irreducible polynomial, $x^5 + x^3 + 1$ and it is irreducible

$x^2 + x + 1$ isan irreducible in $Z_2[x]$ and since $x^2 + x + 1$ does not divide $x^5 + x^3 + 1, x^5 + x^3 + 1$, is an irreducible polynomial in Z_2

Proof: Let $p(x) = x^5 + x^3 + 1$ in Z_2. To show that p is an irreducible polynomial, let's consider the ways to partition 5. The only partitions of 5 are 1 and 4 or 2 and 3.
CASE 1: 5 is partitioned into 1 and 4
If 5 is partitioned into 1 and 4, then possible factors of p are x and $x + 1$. If x is a factor, then $x = 0$ would be a root of p. If $x + 1$ is a factor, then $x = 1$ would be a root of p. However, $p(0) = p(1) = 1$. Thus, neither 0 nor 1 is a root of p, so therefore $x + 1$ nor x can be factors of p. Since p has no linear factors, p also cannot have any factors that are powers of 4.
CASE 2: 5 is partitioned into 2 and 3
If 5 is partitioned into 2 and 3, then possible factors of p are $x^2 + x + 1$, $x^2 + 1$, $x^2 + x$, and x^2. Again, since $p(0) = p(1) = 1$, then $x^2 + 1$, $x^2 + x$, and x^2cannot be factors of p. The only irreducible quadratic in $Z_2[x]$ is $x^2 + x + 1$, but $x^2 + x + 1$ does not divide p. Therefore, p is irreducible in $Z_2[x]$.

Using this information, we were able to translate the matrix into a companion matrix:

$$\text{Companion matrix} = \begin{array}{cc} \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} & \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{matrix} \end{array}$$

**like how we did on the exam, the first column of each matrix and below is the cube of it.

$$A^2, A^3, \dots, A^{31} = I_5$$

We then found all the powers until we got back to the identity matrix I_5. So that means the companion matrix has order 31.

Using the way we did on the exam, we were able to build the matrix M   Sum of rows:

$$V = \begin{array}{cc} \begin{pmatrix}
0&0&0&0&1&0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1 \\
1&0&0&0&0&1&0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0 \\
0&1&0&0&0&0&1&0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0 \\
0&0&1&0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0&0 \\
0&0&0&1&0&1&0&1&1&1&0&1&1&0&0&0&1&1&1&1&1&0&0&1&1&0&1&0&0&1&0 \\
0&0&1&0&0&1&1&0&0&0&0&1&0&1&1&0&1&0&1&0&0&0&1&1&1&0&1&1&1&1&1 \\
0&1&0&1&1&0&1&0&1&0&0&0&1&1&1&0&1&1&1&1&1&0&0&1&0&0&1&1&0&0&0 \\
0&0&1&1&1&0&1&1&1&1&1&0&0&1&0&0&1&1&0&0&0&0&1&0&1&1&0&1&0&1&0 \\
1&0&1&1&0&1&0&1&0&0&0&1&1&1&0&1&1&1&1&1&0&0&1&0&0&1&1&0&0&0&0 \\
0&1&1&1&0&1&1&1&1&1&0&0&1&0&0&1&1&0&0&0&0&1&0&1&1&0&1&0&1&0&0
\end{pmatrix} & \begin{matrix} 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \end{matrix} \end{array}$$

Some facts we know about M:

a. No powers of V is of smaller order because 31 is prime
b. V is a dual code because $MM^T \equiv 0 mod 2$
c. VV^P will give us the number of 1's any two rows of M have in common which means that
    i. No two columns add up to zero
    ii. No three columns add up to zero
    iii. No four columns add up to zero
d. The rank of Vis 10 and the dimension of V^P is of dimension 21
e. V^P is contained in V
f. Using this information, this leads to knowing more about the weight enumerator of V^P

Weight enumerator:

a. Since the rank of V is 10, there are $2^{10} = 1024$ words
b. The minimum weight is 5 (proof is below)
c. $W_{12} = W_{20}$

Proof that the minimum weight is 5:

There are no words of weight 2, because all columns of the matrix are distinct.

There are no words of weight 3. Let *a, b,* and *c* be the first columns of any three matrices in the field. Suppose there are words of weight 3. Since M was built by stacking the first column of each matrix on top of the first column of the cube of that power, then if $a + b + c = 0$, it must also hold that $a^3 + b^3 + c^3 = 0$. If $a^3 + b^3 + c^3 = 0$, then $(a + b)(b + c)(c + a) = 0$. Thus, we have

$$a + b = 0, b + c = 0, c + a = 0.$$

Since we are in Z_2, then

$$a = b, b = c, c = a.$$

However, this is a contradiction as the columns are all distinct.

There are no words of weight 4. Suppose there are words of weight 4. Let *a, b, c,* and *d* be the first columns of any four matrices in the field. Then, if $a + b + c + d =0$, it must also hold that $a^3 + b^3 + c^3 + d^3 = 0$. Since we are in Z_2, we can let $d = a + b + c$, and

$$a^3 + b^3 = c^3 + d^3$$

$$a^3 + b^3 = c^3 + (a + b + c)^3$$

$$a^3 + b^3 = c^3 + a^3 + b^3 + c^3 + (a + b)(b + c)(c + a)$$

$$0 = (a + b)(b + c)(c + a).$$

Using the Zero Product Property,

$$a + b = 0, b + c = 0, c + a = 0$$

$$a = b, \text{ or } b = c, \text{ or } c = a.$$

However, all the columns are distinct, so there are no words of weight 4, which means the minimum weight is 5

By hand, this is some information that was found:

How Many Words of Weight	*So far…*
0	1
12	84
16	191
20	45
31	1
	322

Combination of Rows	
C(10,0)	1
C(10,1)	10
C(10,2)	45
C(10,3)	120
C(10,4)	210
C(10,5)	252
C(10,6)	210
C(10,7)	120
C(10,8)	45
C(10,9)	10
C(10,10)	1
	1024

More about the weight enumerator:

Parity-Check Matrix:

w(x) = $1 + ax^{12} + (1023 - 2a)x^{16} + ax^{16}$

Generating Matrix:

Suppose $\overline{w}(x) = \frac{1}{1024}(1+x)^{11}[(1+x)^{20} + a(1-x)^{12}(1+x)^{8} + 1023(1-x)^{16}(1+x)^{4} - 2a(1-x)^{16}(1+x)^{4} + a(1-x)^{20}]$

$$\overline{w}(x) = \frac{1}{1024}(1+x)^{11} * x^{8}\,a(1-x)^{12} + 8\,x^{7}\,a(1-x)^{12} + 28\,x^{6}\,a(1-x)^{12} + 56\,x^{5}\,a(1-x)^{12} - 2\,x^{4}\,a(1-x)^{16} + 70\,x^{4}\,a(1-x)^{12} - 8\,x^{3}\,a(1-x)^{16} + 56\,x^{3}\,a(1-x)^{12} - 12\,x^{2}\,a(1-x)^{16} + 28\,x^{2}\,a(1-x)^{12} - 8\,x\,a(1-x)^{16} + 8\,x\,a(1-x)^{12} + a(1-x)^{20} - 2\,a(1-x)^{16} + a(1-x)^{12} + 1024\,x^{20} - 12256\,x^{19} + 63616\,x^{18} - 174816\,x^{17} + 247296\,x^{16} + 31872\,x^{15} - 640512\,x^{14} + 1206912\,x^{13} - 379392\,x^{12} - 789568\,x^{11} + 1940224\,x^{10} - 789568\,x^{9} - 379392\,x^{8} + 1206912\,x^{7} - 640512\,x^{6} + 31872\,x^{5} + 247296\,x^{4} - 174816\,x^{3} + 63616\,x^{2} - 12256\,x + 1024$$

Trying to solve for a:

- Focusing on the coefficient of x and the constant of $(1+x)^{11}$, which is 11x + 1
- Take the following parts the equation above of $\overline{w}(x)$ and multiply it by (11x+1), then we just took the coefficients of x and the constants to help solve for "a."
  - $-8xa(11x+1)(1-x)^{16}$→**-8ax**
  - $8xa(11x+1)(1-x)^{12}$→**8ax**
  - $a(11x+1)(1-x)^{20}$→**-20ax + 11ax + a = -9ax + a**
  - $-2a(11x+1)(1-x)^{16}$→**32ax – 22ax – 2a = 10ax – 2a**
  - $a(11x+1)(1-x)^{12}$→**-12ax + 11ax + a = -ax + a**

- Looking at the equation of $\overline{w}(x)$, you can see that -12256x and 1024 are the two terms that will help us solve for "a"
- Set -12256x = -8ax + 8ax – 9ax + 10ax – ax

  From there we get -12256x = 0ax

  So we get a = 0 or we did something incorrect

- Same goes for the constants, set 1024 = a – 2a + a

  So we get a = 0 again or we did something incorrect.

Conclusions:

Our initial assumption must be wrong because the equation says we have words of weight 1 when do we do not. So regarding the weight enumerator, we did not find much about the generating matrix, except how it looks and its dimensions and has a minimum weight of 5, words of weight 0 and 31.