LESSON 8

REED MULLER CODES

REED MULLER CODES II
ERROR CORRECTION

Recall
We review using an example

Begin by picking an integer n, letting $m = 2^n - 1$ and $f(x) = x^m - 1$. We pick $n = 4$, $m = 15$ and $f(x) = x^{15} - 1$.
We find a primitive factor of $f(x)$ which has degree $n = 4$

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

We will need the finite field of order 2^n that is constructed from $p(x)$ and its power - polynomial table. We have constructed this a number of times already but we need it for computations

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

We decide we want to correct τ errors for which we use the generator polynomial

$$g(x) = (x-a)(x-a^2)\cdots(x-a^{2\tau})$$

Here we pick $t = 2$

$$g(x) = (x-a)(x-a^2)(x-a^3)(x-a^4)$$
$$= (x^2+(a^2+a)x+a^2)(x^2+(a^4+a^3)x+a^7)$$
$$= (x^2+a^5x+a^3)(x^2+a^7x+a^7)$$
$$= x^4+a^{13}x^3+a^6x^2+a^3x+a^{10}$$

where we have used the table often.

$C =$ multiples of $g(x)$ of degree $\leq 2^n-2$

Here code polynomials have degree ≤ 14.

$$\dim C = 2^n-1-\deg g(x)$$
$$= 2^n-1-2\tau.$$

Here $\dim C = 11$

This is a $RS(2^n-1, t)$ Reed Soloman code Here it is $RS(15, 2)$

An example of a code word here:

$$c(x) = (a^{10}x^9+a^3x^5+a^2x^3)g(x)$$
$$= a^{10}x^{13}+a^8x^{12}+ax^{11}+a^{13}x^{10}+$$
$$a^{11}x^9+ax^8+a^{11}x^7+$$
$$a^{13}x^6+a^3x^5+a^5x^4+a^{12}x^3$$

Keep in mind in calculations we always have

$p(a) = 0$ Here $a^4 = a+1$

$f(a) = 0$ Here $a^{15} = 1$

We can no longer use the time saving device

$h(a^{2n}) = h(a^n)^2$ because the coefficients of the polynomials are powers of a, not 0 and 1.

We also need a way to get our polynomials into bit strings and conversly.

So given the polynomial with coefficents as powers of a, we write each power of a as a polynomial in a (using the power-polynomial table.

We have

$$c(x) = a^{12}x^3 + a^5x^4 + a^3x^5 + a^{13}x^6 + a^{11}x^7 + a\,x^8 + a^{11}x^9 + a^{13}x^{10} + a\,x^{11} + a^8x^{12} + a^{10}x^{13}$$

$$= (1+a+a^2+a^3)x^3 + (a+a^2)x^4 + a^3x^5 + (1+a+a^3)x^6 + (a+a^2+a^3)x^7 + a\,x^8 + (a+a^2+a^3)x^9 + (1+a^2+a^3)x^{10} + a\,x^{11} + (1+a^2)x^{12} + (1+a+a^3)x^{13}$$

Each of these coefficents can be written as 4 digit terms, The digits are 0 or 1 depending if a appears or not

The coefficents of

x^3 is 1111

x^4 is 0110

x^5 is 0001

x^6 is 1101 etc

Then we list these as a string of length $n \cdot 2^n - 1$

= (degrees of polynomials in a) degrees of polynomials in x)

Here we get

0000 0000 0000 1111 0110 0001

1101 0111 0100 0111 1011 0100

1010 1110 0000

This is the bit string used in sending and receiving messages

We can reverse the steps to get the polynomials used in erro correction

ERROR CORRECTION

We first find a way of deciding if a received vector is a code word. It is the same result as for BCH codes

Thm Let C be a $RS(2^n-1, t)$ code $c(x)$ is in C if and only if $c(a^l)=0$ for $l=1,..2t$.

Proof. The same as for BCH codes

Let $S_l = r(a^l)$ $l=1,..2t$. These are called the syndromes of $r(x)$. The Theorem says $r(x) \in C$ if and only if every syndrome is 0. While checking to see if Theorem holds, we compute the syndromes. They will be used in error correction

Again, $r(x) = c(x) + e(x)$ and $c(a^l)=0$ $l=1,..2t$. So $r(a^l) = e(a^l)$ and we know $r(a^l)$. Thus we know $e(a^l) = S_l$. From ~~knowing~~ knowing the syndromes, we will find $e(x)$

Steps

1. Find the S_i and form
$$S(z) = S_1 + S_2 z + \cdots + S_{2t} z^{2t-1}$$
This requires a good amount of computation. $S(z)$ is called the syndrome polynomial for $r(x)$. We can not use
$$r(a^2) = r(a)^2$$
as the coefficients are not all 0's and 1's.

2. Construct the Euclidean algorithm table using z^{2t} and $S(z)$. In the table, stop when $\deg(r_j) < t$. Then set
$$R(z) = r_j \quad \text{and} \quad V(z) = v_j$$

3. To find the error positions in $r(x)$, find the roots of $V(z)$. Say they are $a^{l_1}, \ldots, a^{l_k}$. Then the error positions are
$x^{-l_1}, \ldots, x^{-l_k}$. To find the coefficient of $e(x)$ at each of these positions, Denote the coefficient of $e(x)$ at these error positions,
$$e_{l_i} = \frac{R(a^{l_i})}{V'(a^{l_i})}$$
is the coefficient of x^{-l_i}

Ex We continue the last example

In the RS(15, 2) code

$$g(x) = x^4 + a^{13}x^3 + a^6x^2 + a^8x + a^{10}$$

STEP I FIND SYNDRONES

Suppose the received vector is

0000 0000 0000 1111 0110 0001
1011 0111 0100 0111 0010
1001 1010 1110 0000

The polynomial is

$$r(x) = (1+a+a^2+a^3)x^3 + (a+a^2)x^4 + a^3x^5 + (1+a^2+a^3)x^6 + (a+a^2+a^3)x^7 + ax^8 + (a+a^2+a^3)x^9 + a^2x^{10} + (1+a^3)x^{11} (1+a^2)x^{12} + (1+a+a^2)x^{13}$$

$$r(x) = a^{12}x^3 + a^5x^4 + a^3x^5 + a^{13}x^6 + a^{11}x^7 + ax^8 + a^{11}x^9 + a^2x^{10} + a^{14}x^{11} + a^8x^{12} + a^{10}x^{13}$$

It is from this polynomial that we compute the syndromes. Since $t = 2$, we need the first 4

$S_1 = r(a) = a$

$S_2 = r(a^2) = a^9$

$S_3 = r(a^3) = a^{11}$

$S_4 = r(a^4) = a^5$

This takes some calculation with the table and 2 identies

$a^{15} = 1 \quad a^4 = a+1$

8

$$S(z) = a + a^9 z + a^{11} z^2 + a^5 z^3$$

STEP 2

~~Find~~

FIND $R(z)$ and $V(z)$ using The Euclidean algorithm

Ex We use the Euclidean algorithm on z^4 and $a^5 z^3 + a^9 z + a$

$$z^4 = (a^5 z^3 + a^9 z + a)(a^{10} z + a) + (a^6 z^2 + a^{14} z + a^2)$$

$$a^5 z^3 + a^9 z + a = (a^6 z^2 + a^{14} z + a^2) \cdot (a^{14} z + a^{13}) + (a^{10} z + a^4)$$

Here, the degree of $r = a^{10} z + a^4$ is less than $t = 2$ so we can move to the table

Row	Q	R	V
-1	–	z^4	0
0	–	$S(z)$	1
1	$a^{10} z + a$	$a^6 z^2 + a^{14} z + a^2$	$a^{10} z + a$
2	$a^{14} z + a^{13}$	$a^{10} z + a^4$	$a^9 z^2 + a^2 z + a^3$

Reading off row 2

$$R = a^{10} z + a^4$$
$$V = a^9 z^2 + a^2 z + a^3$$

The roots of V are needed

Trial and error gives

$$V(a^4) = a^9 a^8 + a^2 a^4 = a^{17} + a^6 = a^2 + a^3 + a^2$$

$$V(a^4) = a^9 a^8 + a^2 a^4 + a^3 = a^{17} + a^6 + a^3$$
$$= a^2 + (a^3 + a^2) + a^3 = 0$$

$$V(a^5) = a^9 a^{10} + a^2 a^5 + a^3 = a^4 + a^7 + a^3$$
$$= (a+1) + (a^3 + a + 1) + a^3 = 0$$

Positions $x^{-4} = x^{11}$ $\quad x^{-5} = x^{10}$

$$V'(x) = a^2$$

$$e_{10} = \frac{R(a^5)}{V'(a^5)} = \frac{a^{15} + a^4}{a^2} = \frac{a}{a^2} = a^{14}$$

$$e_{11} = \frac{R(a^4)}{V'(a^4)} = \frac{a^{14} + a^6}{a^2} = \frac{a^9}{a^2} = a^7$$

$$e(x) = e_{10} x^{10} + e_{11} x^{11}$$
$$= a^{14} x^{10} + a^7 x^{11}$$

Then

$$c(x) = r(x) + e(x) \quad \text{as usual}$$

PROBLEMS

PAGE 168 2, 5, 7