

4. REED-SOLOMON CODE

The Reed-Solomon code is a simple algebraic code using polynomials over finite fields. It is used on all CD's and the Berlekamp-Massey decoding algorithm allows the CD player to correct 16 mistakes out of 255 bytes.

4.1. **the code.** The encoding formula is extremely simple. Start with:

- (1) F a finite field (usually $F = \mathbb{F}(2^8)$, the field with $q = 2^8$ elements).
- (2) k is a positive integer less than q elements (usually $k = 223$).
- (3) n is a positive integer

$$k < n < q = |F|.$$

(usually $n = 255$)

- (4) $r = n - k$ is a positive even integer (usually $r = 255 - 223 = 32$)
- (5) $m = r/2$ is usually 16.

You start with data:

$$a_0, a_1, \dots, a_{k-1} \in F.$$

You take this block of data and make it into a monic polynomial of degree k :

$$f(X) = X^k + a_{k-1}X^{k-1} + \dots + a_0 \in F[X].$$

You take n fixed nonzero elements $\alpha_1, \dots, \alpha_n \in F$. Then the *Reed-Solomon code* is the n -tuple of elements of F given by:

$$(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \in F^n.$$

Usually you let $n = q - 1$ and you take all of the nonzero elements of the field.

The theorem of Berlekamp and Massey is that, assuming that at most $r/2$ of the number $f(\alpha_i)$ are read incorrectly, we can efficiently determine the original polynomial $f(X)$.

4.2. **decoding with no errors.** There is a simple formula to recover $f(X)$ if we know $f(\alpha_i)$ for more than k choices of α_i .

Definition 4.1. Let $L(X) \in F[X]$ be the monic degree n polynomial given by

$$L(X) = \prod_{j=1}^n (X - \alpha_j).$$

And, for each i , let

$$L_i(X) = \frac{L(X)}{X - \alpha_i} = \prod_{j \neq i} (X - \alpha_j).$$

If $n = q - 1$ and $\{\alpha_i\} = F^\times$ then

$$L(X) = X^n - 1$$

and

$$L_i(X) = \frac{X^n - 1}{X - \alpha_i}.$$

Since $L_i(\alpha_j) = 0$ for $i \neq j$ we have the following formula.

$$(4.1) \quad \frac{L_i(\alpha_j)}{L_i(\alpha_i)} = \delta_{ij}.$$

Theorem 4.2. *If $f(X)$ is a polynomial of degree less than n then*

$$f(X) = \sum_{i=1}^n \frac{L_i(X)}{L_i(\alpha_i)} f(\alpha_i).$$

Proof. The equation holds for $X = \alpha_i$ for all i by (4.1). This means the difference between the two polynomials is a polynomial of degree $< n$ with n roots. So, this difference must be zero. \square

Since $f(X)$ has degree k , we can multiply $f(X)$ by another polynomial of degree $< n - k$ and still have the same equation:

Corollary 4.3 (orthogonality condition). *For $0 \leq s < r = n - k$ we have:*

$$f(X)X^s = \sum_{i=1}^n \frac{L_i(X)}{L_i(\alpha_i)} f(\alpha_i)\alpha_i^s.$$

Comparing coefficients we get:

$$\sum_{i=1}^n \frac{f(\alpha_i)\alpha_i^s}{L_i(\alpha_i)} = \delta_{s,r-1} = \begin{cases} 1 & \text{if } s = r - 1 \\ 0 & \text{if } s \leq r - 2 \end{cases}$$

4.3. errors. Suppose that there are errors in the transmission or reading of the code. Let A be the set of indices i for which the value $f(\alpha_i)$ is misread and let $B = \{1, 2, \dots, n\} - A$ be the complement. Thus we have the correct values of $f(\alpha_j)$ for $j \in B$ but we don't know what $f(\alpha_i)$ is for any $i \in A$. Let $L_A(X) = L^B(X)$ be defined by

$$L_A(X) = L^B(X) = \prod_{j \notin A} (X - \alpha_j) = \prod_{j \in B} (X - \alpha_j)$$

This is a polynomial of degree $n - |A| = |B|$. Let

$$L_i^B(X) = \prod_{j \in B, j \neq i} (X - \alpha_j) = \frac{L_A(X)}{X - \alpha_i}$$

for all $i \in B$. Then, as a special case of Theorem 4.2, we have:

Corollary 4.4. *For any polynomial $f(X) \in F[X]$ of degree $< |B|$ (i.e., if $|A| < r = n - k$) we have*

$$f(X) = \sum_{i \in B} \frac{L_{i,A}(X)}{L_{i,A}(\alpha_i)} f(\alpha_i).$$

The conclusion is: We need to know the set A of indices for which $f(\alpha_i)$ has been misread and we need $|A| < r$.

4.4. finding the errors. We assume that the error set A has at most $r/2$ elements. The correct code is $f(\alpha_i)$. But, with errors we will read this as

$$c_i = f(\alpha_i) + \epsilon_i$$

where ϵ_i is the *error*. Thus $\epsilon_i \neq 0$ only for $i \in A$. The orthogonality condition Corollary 4.3 implies that

$$\sum_{i=1}^n \frac{c_i \alpha_i^s}{L_i(\alpha_i)} = \sum_{i=1}^n \frac{f(\alpha_i) \alpha_i^s}{L_i(\alpha_i)} + \sum_{i=1}^n \frac{\epsilon_i \alpha_i^s}{L_i(\alpha_i)} = \delta_{s,r-1} + \sum_{i=1}^n \frac{\epsilon_i \alpha_i^s}{L_i(\alpha_i)}.$$

Thus we can compute the sequence of r numbers:

$$d_s := \sum_{i \in A} \frac{\epsilon_i \alpha_i^s}{L_i(\alpha_i)} = \sum_{i=1}^n \frac{c_i \alpha_i^s}{L_i(\alpha_i)} - \delta_{s,r-1}$$

for $0 \leq s < r$. The key point is:

Theorem 4.5. *The numbers d_s satisfy a homogeneous linear recurrence of degree $|A|$ and the roots of the minimal polynomial $p(X)$ of this recurrence are α_i for $i \in A$. Furthermore, if $|A| \leq r/2$, this linear recurrence and the polynomial $p(X)$ are uniquely determined.*

To see this we need to review the solution of homogeneous linear recurrences.

4.5. homogeneous linear recurrence.

Definition 4.6. We say that a sequence of elements $d_0, d_1, \dots \in F$ satisfies a *homogeneous linear recurrence* of order m if there are fixed elements $a_0, a_1, \dots, a_{m-1} \in F$ so that

$$d_s + a_{m-1}d_{s-1} + a_{m-2}d_{s-2} + \dots + a_0d_{s-m} = 0$$

for all $s \geq m$. If m is minimal, the degree m monic polynomial

$$p(X) = X^m + a_{m-1}X^{m-1} + \dots + a_0 \in F[X]$$

is called the *minimal polynomial* of the recurrence.

In class I used the *Fibonacci sequence*

$$1, 1, 2, 3, 5, 8, \dots$$

which satisfies the degree 2 homogeneous recurrence

$$d_s - d_{s-1} - d_{s-2} = 0$$

with minimal polynomial $p(X) = X^2 - X - 1$. To solve the recurrence we set

$$d_s = C^s.$$

Then the equation is

$$C^s - C^{s-1} - C^{s-2} = 0.$$

Assuming $C \neq 0$ we get

$$C^2 - C - 1 = 0.$$

I.e., C is a root of the polynomial $p(X)$. So,

$$C = C_{\pm} = \frac{1 \pm \sqrt{5}}{2}.$$

This means that the general solution of the recurrence is

$$d_s = e_0 C_+^s + e_1 C_-^s$$

where e_0, e_1 are obtained from the initial conditions $d_0 = 1, d_1 = 1$.

This elementary argument works in general. Given any root α of the polynomial $p(X)$, the sequence $d_s = \alpha^s$ is a solution of the homogenous linear recurrence with minimal polynomial $p(X)$. If $p(X)$ has m distinct roots $\alpha_1, \dots, \alpha_m$ then the general solution of the recurrence is

$$d_s = \sum_{i=1}^m e_i \alpha_i^s$$

where e_i are determined by the initial values d_0, \dots, d_{m-1} . If we insert

$$e_i = \frac{\epsilon_i}{L_i(\alpha_i)}$$

we get the numbers from the Reed-Solomon code (assuming $A = \{1, 2, \dots, m\}$). Since we are assuming that $m \leq r/2$, the problem is now reduced to the question:

Given the numbers d_0, \dots, d_{2m-1} can we find the degree m linear recurrence satisfied by these numbers?

The answer is given by the Euclidean division algorithm.

4.6. Euclidean algorithm. Suppose we have polynomials $f(X), g(X) \in F[X]$ and we want to find the greatest common divisor $h(X)$. Since $h(X)$ is the generator of the ideal (f, g) generated by f and g , there are polynomials $a(X), b(X)$ so that

$$(4.2) \quad h(X) = a(X)f(X) + b(X)g(X).$$

The Euclidean algorithm will find all three: $h(X), a(X), b(X)$.

4.6.1. *the usual algorithm.* Note that the equation (4.2) is a matrix product:

$$h(X) = (a, b) \begin{pmatrix} f \\ g \end{pmatrix}.$$

The Euclidean algorithm starts with the two solutions of this equation:

$$\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}.$$

These are the first two rows of an array which will have the solution at the bottom. The third line is obtained by multiplying the second line by $Q_1(X)$ and subtracting from the first line. Here $Q_1(X)$ is the quotient f/g :

$$f(X) = Q_1(X)g(X) + R_1(X)$$

where $\deg R(X) < \deg g(X)$. This produces:

	h	a	b
$f(X)$	1	0	
$g(X)$	0	1	
$f - Q_1g = R_1(X)$	1	$-Q_1(X)$	

Next, divide $R_1(X)$ into $g(X)$:

$$g(X) = Q_2(X)R_1(X) + R_2(X)$$

to get:

	h	a	b
$f(X)$	1	0	
$g(X)$	0	1	
$f - Q_1g = R_1(X)$	1	$-Q_1(X)$	
$g - Q_2R_1 = R_2(X)$	$-Q_2(X)$	$1 + Q_1Q_2$	

In each row, the term on the left has strictly smaller degree and Equation (4.2) holds. The last nonzero remainder is the greatest common divisor.

4.6.2. *finding the recurrence polynomial.* Suppose we have a recurrence $d_0, d_1, \dots, d_{2m-1}$. Then the procedure is to take $f(X) = X^{2m}$,

$$g(X) = d_{2m-1}X^{2m-1} + \dots + d_0$$

and perform the Euclidean division algorithm only half way. You stop as soon as the remainder has degree less than m .

Here is an example. Take the sequence: 1,1,2,3. Then $f(X) = X^4$ and $g(X) = 1 + X + 2X^2 + 3X^3$. The algorithm gives:

Q	h	a	b
	X^4	1	0
	$3X^3 + 2X^2 + X + 1$	0	1
$\frac{1}{9}(3X - 2)$	$\frac{1}{9}(X^2 - X + 2)$	1	$-\frac{1}{9}(3X - 2)$
$9(3X + 5)$	-9	$-9(3X + 5)$	$9(X^2 + X - 1)$

Remark 4.7. Since the Q 's are quotients of successive terms in the h column, their degrees add up to the difference in degrees between the first term X^{2m} and the second to last term in the h column which has degree $\geq m$ (otherwise we would have stopped). The last b has degree equal to the product of the Q 's (by induction). So, $\deg b \leq m$.

Theorem 4.8. *The polynomial of the recurrence is given by*

$$p(X) = \frac{X^{\deg b}}{b(0)}b(1/X).$$

The formula $X^{\deg b}b(1/X)$ reverses the coefficients of the polynomial $b(X)$. You need to divide by $b(0)$ to make $p(X)$ into a monic polynomial. In the example we get:

$$p(X) = \frac{X^2}{-9}9 \left(1 + \frac{1}{X} - \frac{1}{X^2} \right) = X^2 - X - 1.$$

Proof. To see why this is the polynomial of the recurrence, note that the last row of our chart gives:

$$b(X)g(X) = h(X) - a(X)X^{2m}$$

Since $h(X)$ has degree $< m$, there are no terms of degree s for $s = m, m+1, m+2, \dots, 2m-1$. This means that

$$b_0d_s + b_1d_{s-1} + \dots + b_md_{s-m} = 0$$

for all $m \leq s < 2m$ where $b(X) = b_0 + b_1X + \dots + b_mX^m$. This is the linear recurrence with coefficients indexed backwards. So, the reverse polynomial $p(X)$ is the polynomial of the the recurrence. \square