

Solving the Key Equation for RS Codes

1 Euclid's Algorithm

- The Key Equation
- Euclid's Algorithm
- Solving the Key Equation
- An Example

The Key Equation

Define the **error locator polynomial**:

$$\sigma(x) = \prod_{i=1}^t (x - \alpha^{-j_i})$$

Define the **error evaluator polynomial**:

$$W(x) \triangleq \sum_{\ell=1}^t e_{j_\ell} \prod_{\substack{i=1 \\ i \neq \ell}}^t (x - \alpha^{-j_i})$$

Then, for $\alpha^{j_\ell} \in GF(2^m)$,

$$W(\alpha^{j_\ell}) = e_{j_\ell} \prod_{\substack{i=1 \\ i \neq \ell}}^t (\alpha^{j_\ell} - \alpha^{-j_i}) \quad (1)$$

Easy to see:

$$\sigma'(x) = \sum_{i=1}^t \prod_{\substack{i=1 \\ i \neq \ell}}^t (x - \alpha^{-j_i})$$

So

$$\sigma'(\alpha^{-j_\ell}) = \prod_{\substack{i=1 \\ i \neq \ell}}^t (\alpha^{-j_\ell} - \alpha^{-j_i}) \quad (2)$$

Combining (1) and (2) gives,

$$e_{j_\ell} = \frac{W(\alpha^{-j_\ell})}{\sigma'(\alpha^{-j_\ell})} \quad (3)$$

Theorem 1 *There exists a polynomial $\mu(x)$ such that*

$$\sigma(x)S(x) = -W(x) + \mu(x)x^{n-k} \quad (4)$$

□

(See example, p 123-125 of Castiñera Moriera and Farrell.)

Euclid's Algorithm

Integers

Consider $A, B \in \mathbb{Z}$, $A \geq B$. Let

$$\begin{aligned} r_{-1} &\triangleq A \\ r_0 &\triangleq B \end{aligned}$$

Divide A by B . Then divide B by the previous remainder. Repeat

$$\begin{aligned}
r_{-1} &= q_1 r_0 + r_1 \\
r_0 &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\vdots \\
r_{i-2} &= q_i r_{i-1} + r_i \\
r_{i-1} &= q_{i+1} r_i + 0
\end{aligned}$$

The last condition will always be reached. (Thought problem.)

Then $r_i | r_{i-1}$ and the previous eq shows that this requires $r_i | r_{i-2}$. Recursion shows that $r_i | A$ and B .

Therefore, r_i is a common divisor of A and B .

Also, $r_{j+1} < r_j$ (for if it were not, then we would increase q_j). So r_i is the first (largest, for they are decreasing) common divisor of A and B . \square

Polynomials

The development for the GCD of two polynomials takes a parallel path:

Let $A(x), B(x)$ be two polynomials over (with coefficients from) any field. Let

$$A(x) \triangleq r_{-1}(x)$$

$$B(x) \triangleq r_0(x)$$

Divide $A(x)$ by $B(x)$, then divide each previous remainder by the latest one:

$$r_{-1}(x) = q_1(x)r_0(x) + r_1(x)$$

$$r_0(x) = q_2(x)r_1(x) + r_2(x)$$

$$\vdots$$

$$r_{i-1}(x) = q_{i+1}(x)r_i(x) + 0$$

Reasoning as before, we conclude that $r_i(x)$ divides both $A(x)$ and $B(x)$.

For every j , $\deg[r_j(x)] < \deg[r_{j+1}(x)]$ for, if it were not, then the degree of $q_j(x)$ should be increased until it is.

Therefore, $r_i(x)$ is the largest degree polynomial that divides both $A(x)$ and $B(x)$ and is, therefore, their GCD. □

Solving the Key Equation

$$\sigma(x)S(x) - \mu(x)x^{n-k} = -W(x)$$

Also, recall that $2t = n - k$ and notice that the key equation can also be written:

$$[\sigma(x)S(x) + W(x)] \equiv 0, \quad \text{mod } x^{2t}$$

Solving the key equation involves finding $r_i(x) = \text{GCD}[S(x), x^{n-k}]$.

Then

$$r_i(x) | W(x)$$

Write $S(x) = r_i(x) \cdot b(x)$

$$[r_i(x) \cdot b(x) + W(x)] \equiv 0 \pmod{x^{n-k}}$$

So, the degree of the LHS $\leq n - k - 1$ and $\deg[S(x)] \leq n - k - 1$. Thus

$$\deg[r_i(x)] \leq \left\lfloor \frac{n-k}{2} \right\rfloor + 1$$

But $\deg[\sigma(x)] \leq (n-k)/2$ and $\deg[W(x)] \leq (n-k)/2$ so it must be that

$$W(x) = -\lambda r_i(x)$$

And writing $r_i(x) = a_k(x)x^{n-1} + b_i(x)S(x)$ yields

$$\sigma(x) = \lambda b_i(x)$$

Since $b_i(x)$ is determined from the LCD procedure, $\sigma(x)$ is now known and can be solved for the error locators. Then (3) is used to find the error values, and decoding is complete.

2 Berlekamp's Algorithm (BMA)

...an *iterative algorithm* for finding $\sigma(x)$, the minimum degree polynomial satisfied by the error locators

...iteatively find sequence of $\sigma^{(\ell)}(x)$, $\ell = 1, 2, \dots$ where the i^{th} polynomial satisfies the i^{th} of Newton's Identities.

Recall **Newton's Identities** :

$$s_1 + \sigma_1 = 0$$

$$s_2 + \sigma_1 s_1 + 2s_2 = 0$$

$$s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0$$

$$\vdots$$

$$s_\mu + \sigma_1 s_{\nu-1} + \sigma_2 s_{\nu-2} + \cdots + \nu\sigma_\nu = 0$$

$$s_{\nu+1} + \sigma_1 s_\nu + \cdots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0$$

$$s_{\nu+2} + \sigma_1 s_{\nu+1} + \cdots + \sigma_\nu s_2 + \sigma_\nu s_2 = 0$$

$$\dots$$

$$s_{2t} + \sigma_1 s_{2t-1} + \sigma_2 s_{2t-2} + \cdots + \sigma_\nu s_{2t-\nu} = 0$$

Steps:

1. Find the **minimum degree** polynomial $\sigma^{(1)}(x)$, the coefficients of which satisfy the **first Newton Identity**: $s_1 + \sigma_1 = 0$.

$$\begin{aligned}\sigma^{(1)}(x) &= 1 + \sigma^{(1)}x \\ &= 1 + s_1x\end{aligned}$$

2. **Test** whether $\sigma^{(1)}(x)$ satisfies the **second Newton Identity**: $s_2 + s_1\sigma_1 + 2\sigma_2 = 0$.

- *i.e.*, test:

$$\begin{aligned}s_2 + \sigma_1^{(1)}s_1 + 2\sigma_2^{(1)} &\stackrel{?}{=} 0 \\ s_2 + s_1^2 &\stackrel{?}{=} 0\end{aligned}$$

- If $s_2 + s_1^2 = 0$, then $\sigma^{(2)}(x) = \sigma^{(1)}(x)$. Otherwise, find **correction term** s.t:

$$\sigma^{(2)}(x) = \sigma^{(1)}(x) + c.t.,$$

in order that $\sigma^{(2)}(x)$ is of smallest degree to satisfy the **first and second of Newton's Identities**.

3. Now test whether the coefficients of $\sigma^{(2)}(x)$ satisfy the third of Newton's Identities, *i.e.*,

$$s_3 + \sigma_1^{(2)} s_2 + \sigma_2^{(2)} s_1 + 3\sigma_3^{(2)} \stackrel{?}{=} 0$$

If "yes," then $\sigma^{(3)}(x) = \sigma^{(2)}(x)$. *Otherwise*, must find *c.t.*:

$$\sigma^{(3)}(x) = \sigma^{(2)}(x) + c.t.$$

... Continue until $\sigma^{(2t)}(x) = \sigma(x)$ (the *e.l.p.*) has been found. In general...

4. Suppose the μ th step has been successfully completed. For the $(\mu + 1)^{st}$ step, the recursion is

$$s_{\mu+1} + \sigma_1^{(\mu)} + \dots + \sigma I_{\mu}^{(\mu)} s_{\mu-1-I_{\mu}} \stackrel{?}{=} 0$$

This inspires...

Definition 1 The μ^{th} discrepancy is

$$d_\mu \triangleq s_{\mu+1} + \sigma_1^{(\mu)} s_\mu + \sigma_2^{(\mu)} s_{\mu-1} + \cdots + \sigma_{I_\mu} s_{\mu+1-I_\mu}$$

where I_μ is the degree of $\sigma^\mu(x)$. □

(Note: compare d_μ with the μ^{th} of Newton's Identities.)

So, if $d_\mu = 0$, then

$$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x)$$

But if $d_\mu \neq 0$, then

$$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) + c.t.$$

So, how to find the correction term $c.t.$?

Rule:

- Examine the steps prior to the ν^{th} .
- Find $\sigma^{(\rho)}(x)$ such that
 - $d_\rho \neq 0$ and
 - ρ maximizes $\rho - I_\rho$

where $I_\rho = \deg [\sigma^{(\rho)}(x)]$. Then,

$$\sigma^{(\mu+1)} = \sigma^{(\mu)}(x) + d_\mu d_\rho^{-1} x^{\mu-\rho} \sigma^{(\rho)}(x)$$

is the solution at step $\mu + 1$.

Continue until $\sigma^{(2t)}$ is obtained. This will be $\sigma(x)$. Note:

Proofs can be found in Peterson and Weldon (MIT Press 1972) and in Berlekamp (Aegean Park Press, 1984).

Example:

It is helpful to build a decoding table.

μ	$\sigma^{(\mu)}(x)$	d_μ	I_μ	$\mu - I_\mu$
-1	1	1	0	-1
0	1	s_1	0	0
1	$1 - s_1x$			

Consider a 3-error correcting RS code over $GF(2^4)$.

$$t = 3 \Rightarrow n - k = 6 \text{ and } n = 15$$

Then

$$\begin{aligned}
 g(x) &= \prod_{\ell=1}^6 (x - \alpha^\ell) \\
 &= \alpha^6 + \alpha^9x + \alpha^6x^2 + \alpha^4x^3 + \alpha^{14}x^4 + \alpha^{10}x^5 + x^5
 \end{aligned}$$

Suppose $\mathbf{c} = \mathbf{0}$ is transmitted and \mathbf{r} is received:

$$\mathbf{r} = (000\alpha^7 00\alpha^3 00000\alpha^4 00)$$

So we know how to compute

$$\begin{aligned} s_1 &= \alpha^{10} + \alpha^9 + \alpha = \alpha^{12} \\ s_2 &= 1 \\ s_3 &= \alpha^{14} \\ s_4 &= \alpha^{10} \\ s_5 &= 0 \\ s_6 &= \alpha^{12} \end{aligned}$$

...more to come...