Properties of the Error Locator and the Error Evaluator Polynomials

Let $S(x) = S_1 + S_2x + \ldots + S_{2t}x^{2t-1}$ be the syndrome polynomial where

$$S_i = \sum_{l=1}^{\nu} \delta_l \beta_l^i, \tag{1}$$

$1 \leq \nu \leq t$, the δ_l's are nonzero elements, and the β_l's are nonzero distinct elements.

The error locator polynomial is given by

$$\sigma(x) = \prod_{j=1}^{\nu}(1 - \beta_j x) \tag{2}$$

and the error evaluator polynomial is given by

$$Z_0(x) = \sum_{l=1}^{\nu} \delta_l \beta_l \prod_{j=1, j \neq l}^{\nu} (1 - \beta_j x). \tag{3}$$

Lemma 1 *The polynomials $\sigma(x)$ and $Z_0(x)$ are nonzero and $\sigma(0) = 1$. We also have*

1. $\sigma(x)S(x) \equiv Z_0(x) \pmod{x^{2t}}$. *This is called the key equation.*

2. $\deg Z_0(x) < \deg \sigma(x) \leq t$.

3. $\mathrm{GCD}(\sigma(x), Z_0(x)) = 1$.

Proof. Clearly, $\sigma(x)$ is a nonzero polynomial with $\sigma(0) = 1$. From (1), we have

$$\begin{aligned}
S(x) &= \sum_{i=1}^{2t} S_i x^{i-1} \\
&= \sum_{i=1}^{2t} \sum_{l=1}^{\nu} \delta_l \beta_l^i x^{i-1} \\
&= \sum_{l=1}^{\nu} \delta_l \beta_l \sum_{i=1}^{2t} \beta_l^{i-1} x^{i-1} \\
&= \sum_{l=1}^{\nu} \delta_l \beta_l \sum_{i=0}^{2t-1} (\beta_l x)^i \\
&\equiv \sum_{l=1}^{\nu} \frac{\delta_l \beta_l}{1 - \beta_l x} \pmod{x^{2t}},
\end{aligned}$$

where the congruency follows from the fact that

$$\frac{1}{1-\beta_l x} = \sum_{i=0}^{\infty}(\beta_l x)^i \equiv \sum_{i=0}^{2t-1}(\beta_l x)^i \pmod{x^{2t}}.$$

From (2) and (3), we have

$$\begin{aligned}
\sigma(x)S(x) &\equiv \prod_{j=1}^{\nu}(1-\beta_j x)\sum_{l=1}^{\nu}\frac{\delta_l\beta_l}{1-\beta_l x} \pmod{x^{2t}} \\
&\equiv \sum_{l=1}^{\nu}\delta_l\beta_l \prod_{j=1, j\neq l}^{\nu}(1-\beta_j x) \pmod{x^{2t}} \\
&\equiv Z_0(x) \pmod{x^{2t}}.
\end{aligned}$$

This proves 1) in the lemma. From (2) and (3), $\deg \sigma(x) = \nu$ and $\deg Z_0(x) < \nu$. Since $\nu \le t$, this proves 2) in the lemma. From (2), it follows that if $\mathrm{GCD}(\sigma(x), Z_0(x)) \neq 1$, then $Z_0(x)$ is divisible by $1-\beta_i x$ for some i, $1 \le i \le \nu$, which implies that $Z_0(\beta_i^{-1}) = 0$. However,

$$\begin{aligned}
Z_0(\beta_i^{-1}) &= \sum_{l=1}^{\nu}\delta_l\beta_l \prod_{j=1, j\neq l}^{\nu}(1-\beta_j\beta_i^{-1}) \\
&= \delta_i\beta_i \prod_{j=1, j\neq i}^{\nu}(1-\beta_j\beta_i^{-1}) \\
&\neq 0.
\end{aligned}$$

This proves 3) in the lemma and also proves that $Z_0(x)$ is a nonzero polynomial. $\square$

Extended Euclid's Algorithm for Polynomials

Let $a(x)$ and $b(x)$ be nonzero polynomials over some field where $a(x) \neq 0$ and $\deg a(x) > \deg b(x)$. Consider the following algorithm for computing the polynomials $r_i(x)$, $f_i(x)$, and $g_i(x)$.

Initialization:

$$\begin{array}{lll} r_{-1}(x) = a(x), & f_{-1}(x) = 1, & g_{-1}(x) = 0, \\ r_0(x) = b(x), & f_0(x) = 0, & g_0(x) = 1. \end{array}$$

for $(i = 1; r_{i-1}(x) \neq 0; i = i + 1)$

$q_i(x)$ is the quotient obtained by dividing $r_{i-2}(x)$ by $r_{i-1}(x)$.

$$\begin{aligned} r_i(x) &= r_{i-2}(x) - q_i(x) r_{i-1}(x) \\ f_i(x) &= f_{i-2}(x) - q_i(x) f_{i-1}(x) \\ g_i(x) &= g_{i-2}(x) - q_i(x) g_{i-1}(x) \end{aligned}$$

end for

Let $i_{\max}$ be the maximum value of $i \geq -1$ for which $r_i(x) \neq 0$.

Lemma 2 *$f_i(x)g_{i-1}(x) - f_{i-1}(x)g_i(x) = (-1)^{i+1}$ for $i = 0, 1, \ldots, i_{\max} + 1$.*

Proof. Equality holds for $i = 0$. Suppose it holds for values less than $i \geq 1$. Then,

$$\begin{aligned} f_i(x)g_{i-1}(x) - f_{i-1}(x)g_i(x) &= (f_{i-2}(x) - q_i(x)f_{i-1}(x))g_{i-1}(x) \\ &\qquad - f_{i-1}(x)(g_{i-2}(x) - q_i(x)g_{i-1}(x)) \\ &= -(f_{i-1}(x)g_{i-2}(x) - f_{i-2}(x)g_{i-1}(x)) \\ &= -(-1)^{(i-1)+1} \quad \text{(by the induction hypothesis)} \\ &= (-1)^{i+1}. \end{aligned}$$

Lemma 3 *$f_i(x)a(x) + g_i(x)b(x) = r_i(x)$ for $i = -1, 0, \ldots, i_{\max} + 1$.*

Proof. Equality holds for $i = -1$ and $i = 0$. Suppose it holds for values less than $i \geq 1$. Then,

$$f_i(x)a(x) + g_i(x)b(x) = (f_{i-2}(x) - q_i(x)f_{i-1}(x))a(x) + (g_{i-2}(x) - q_i(x)g_{i-1}(x))b(x)$$

$$
\begin{aligned}
&= (f_{i-2}(x)a(x) + g_{i-2}(x)b(x)) - q_i(x)(f_{i-1}(x)a(x) + g_{i-1}(x)b(x)) \\
&= r_{i-2}(x) - q_i(x)r_{i-1}(x) \quad \text{(by the induction hypothesis)} \\
&= r_i(x).
\end{aligned}
$$

□

Lemma 4 $\deg g_i(x) + \deg r_{i-1}(x) = \deg a(x)$ *for* $i = 0, 1, \ldots, i_{\max} + 1$.

Proof. Equality holds for $i = 0$. Suppose it holds for values less than $i \geq 1$. Notice that $\deg r_{-1}(x) > \deg r_0(x) > \deg r_1(x) > \cdots > \deg r_{i_{\max}}(x)$ as $r_i(x)$ is the remainder obtained by dividing $r_{i-2}(x)$ by $r_{i-1}(x)$ for $i = 1, 2, \ldots, i_{\max}$. We conclude based on the induction hypothesis that $\deg g_0(x) < \deg g_1(x) < \cdots < \deg g_{i-1}(x)$. Notice that $r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x)$ with $\deg r_i(x) < \deg r_{i-1}(x)$ implies that

$$\deg r_{i-2}(x) = \deg(q_i(x)r_{i-1}(x)) = \deg q_i(x) + \deg r_{i-1}(x). \tag{4}$$

Also, $g_i(x) = g_{i-2}(x) - q_i(x)g_{i-1}(x)$ with $\deg g_{i-2}(x) < \deg g_{i-1}(x)$ implies that

$$\deg g_i(x) = \deg(q_i(x)g_{i-1}(x)) = \deg q_i(x) + \deg g_{i-1}(x). \tag{5}$$

From (4) and (5), we have

$$
\begin{aligned}
\deg g_i(x) + \deg r_{i-1}(x) &= (\deg q_i(x) + \deg g_{i-1}(x)) + (\deg r_{i-2}(x) - \deg q_i(x)) \\
&= \deg g_{i-1}(x) + \deg r_{i-2}(x) \\
&= \deg a(x) \quad \text{(by the induction hypothesis)}
\end{aligned}
$$

□

Lemma 5 $\deg f_i(x) + \deg r_{i-1}(x) = \deg b(x)$ *for* $i = 1, 2, \ldots, i_{\max} + 1$.

Proof. Equality holds for $i = 1$ since $f_1(x) = f_{-1}(x) - q_1(x)f_0(x) = f_{-1}(x) = 1$ and $r_0(x) = b(x)$. We then use induction on i as in the proof of Lemma 4. □

Lemma 6 *Any divisor of* $a(x)$ *and* $b(x)$ *divides* $r_i(x)$ *for* $i = -1, 0, \ldots, i_{\max} + 1$.

Proof. This follows from Lemma 3. □

Lemma 7 *$r_{i_{\max}}(x)$ divides $r_i(x)$ for $i = i_{\max} - 1, i_{\max} - 2, \ldots, 0, -1$.*

Proof. We have $r_{i_{\max}+1}(x) = r_{i_{\max}-1}(x) - q_{i_{\max}+1}(x) r_{i_{\max}}$. Since $r_{i_{\max}+1}(x) = 0$, then $r_{i_{\max}}(x)$ divides $r_{i_{\max}-1}(x)$. Suppose the lemma holds for values greater than $i \leq i_{\max} - 2$. Then, $r_{i_{\max}}(x)$ divides $r_{i+1}(x)$ and $r_{i+2}(x)$. From $r_{i+2}(x) = r_i(x) - q_{i+2}(x) r_{i+1}(x)$, it follows that $r_{i_{\max}}(x)$ divides $r_i(x)$. □

Lemma 8 *$r_{i_{\max}}(x) = \mathrm{GCD}(a(x), b(x))$.*

Proof. Since $r_{-1}(x) = a(x)$ and $r_0(x) = b(x)$, it follows from Lemma 7 that $r_{i_{\max}}(x)$ divides $a(x)$ and $b(x)$. From Lemma 6, any divisor of $a(x)$ and $b(x)$ divides $r_{i_{\max}}(x)$. □

Lemma 9 *Let $g(x)$ and $r(x)$ be nonzero polynomials such that*

1. $g(x) b(x) \equiv r(x) \pmod{a(x)}$.

2. $\deg g(x) + \deg r(x) < \deg a(x)$.

3. $\mathrm{GCD}(g(x), r(x)) = 1$.

Then, there is an index j, $0 \leq j \leq i_{max}$, and a nonzero constant β such that $g(x) = \beta g_j(x)$ and $r(x) = \beta r_j(x)$.

Proof. Since $r_{-1}(x) = a(x)$, then $\deg r_{-1}(x) = \deg a(x) > \deg r(x)$. Also, the degree of $r_i(x)$ is decreasing with $r_{i_{\max}+1}(x) = 0$, i.e., a polynomial of degree $-\infty$. Hence, for some index j, $0 \leq j \leq i_{max} + 1$,

$$\deg r_j(x) \leq \deg r(x) < \deg r_{j-1}(x). \tag{6}$$

From Lemma 3,

$$f_j(x) a(x) + g_j(x) b(x) = r_j(x). \tag{7}$$

From the first condition in the lemma, there exists a polynomial $f(x)$ such that

$$f(x)a(x) + g(x)b(x) = r(x). \tag{8}$$

Multiplying (7) by $g(x)$ and (8) by $g_j(x)$ and subtracting, we get

$$(f_j(x)g(x) - f(x)g_j(x))a(x) = g(x)r_j(x) - g_j(x)r(x). \tag{9}$$

Next, notice by the the second condition in the lemma and (6) that

$$\deg g(x) + \deg r_j(x) \leq \deg g(x) + \deg r(x) < \deg a(x)$$

and by Lemma 4 and (6),

$$\deg g_j(x) + \deg r(x) = \deg a(x) - \deg r_{j-1}(x) + \deg r(x) < \deg a(x).$$

Hence, the right hand side of (9) has degree less than that of $a(x)$. Therefore, the left hand side, which is a multiple of $a(x)$, is zero. Hence,

$$g(x)r_j(x) = g_j(x)r(x).$$

From the third condition in the lemma, $r(x)$ divides $r_j(x)$. Notice that $r_j(x) = 0$ if and only if $j = i_{\max} + 1$. In this case, $g_{i_{\max}+1}(x) = 0$ since $r(x) \neq 0$ by assumption. However, from Lemma 4,

$$\deg g_{i_{\max}+1}(x) = \deg a(x) - \deg r_{i_{\max}}(x) \geq \deg a(x) - \deg r_{-1}(x) = 0.$$

Hence, $g_{i_{\max}+1}(x)$ is not equal to zero. We conclude that $r_j(x) \neq 0$ and $j \leq i_{\max}$. From (6), it follows that $r(x) = \beta r_j(x)$ for some nonzero constant β. This implies that $g(x) = \beta g_j(x)$. □

Lemma 9 shows that Euclid's algorithm yields the polynomials $g(x)$ and $r(x)$ up to a constant mutliple. Next, we want to uniquely specify the index j such that $g_j(x)$ and $r_j(x)$ are nonzero constant multiples of $g(x)$ and $r(x)$, respectively. For this purpose, we bound their degrees as shown in the next lemma.

Lemma 10 *If* $r(x)$ *and* $g(x)$ *in Lemma 9 satisfy*

$$\deg g(x) \leq \frac{1}{2}\deg a(x) \ \textit{and} \ \deg r(x) < \frac{1}{2}\deg a(x),$$

then j, $0 \leq j \leq i_{\max}$ *is the unique index for which*

$$\deg r_j(x) < \frac{1}{2}\deg a(x) \leq \deg r_{j-1}(x).$$

Proof. If $i < j$, then $\deg r_i(x) \geq \deg r_{j-1}(x) \geq \frac{1}{2}\deg a(x)$, and, therefore, $r(x) \neq \beta r_i(x)$ for a nonzero constant β. If $i > j$, then from Lemma 4,

$$\begin{aligned}
\deg g_i(x) &= \deg a(x) - \deg r_{i-1}(x) \\
&\geq \deg a(x) - \deg r_j(x) \\
&> \deg a(x) - \frac{1}{2}\deg a(x) \\
&= \frac{1}{2}\deg a(x),
\end{aligned}$$

and, therefore, $g(x) \neq \beta g_i(x)$ for a nonzero constant multiple β. □

Lemma 11 *Let* $g(x)$ *and* $r(x)$ *be nonzero polynomials such that*

1. $g(x)b(x) \equiv r(x) \pmod{a(x)}$.

2. $\deg r(x) < \deg g(x) \leq \frac{1}{2}\deg a(x)$.

3. $\mathrm{GCD}(g(x), r(x)) = 1$.

Then, $g(x) = \beta g_j(x)$ *and* $r(x) = \beta r_j(x)$ *for a nonzero constant* β *and the unique index* j, $0 \leq j \leq i_{\max}$, *satisfying*

$$\deg r_j(x) < \frac{1}{2}\deg a(x) \leq \deg r_{j-1}(x). \tag{10}$$

Furthermore, this j *is the unique index* j' *satisfying*

$$\deg r_{j'}(x) < \deg g_{j'}(x) \leq \frac{1}{2}\deg a(x). \tag{11}$$

Proof. From the second condition on $r(x)$ and $g(x)$, it follows that $\deg g(x) + \deg r(x) < \deg a(x)$. Hence, $r(x)$ and $g(x)$ satisfy the conditions in Lemma 9. We conclude that $g(x) = \beta g_j(x)$ and $r(x) = \beta r_j(x)$ for the unique index j satsfying (10). This implies that

$$\deg r_j(x) < \deg g_j(x) \le \frac{1}{2} \deg a(x).$$

It remains to argue that if (11) holds, then $j' = j$. Indeed, from Lemma 4, we have $\deg g_{j'}(x) + \deg r_{j'-1}(x) = \deg a(x)$. Hence, if (11) holds, then

$$\deg r_{j'}(x) < \frac{1}{2} \deg a(x) \le \deg r_{j'-1}(x)$$

holds. By the uniqueness of the index j satisfying (10), it follows that $j' = j$. $\square$

Example 1 Let $a(x)$ and $b(x)$ be real polynomials given by

$$\begin{aligned} a(x) &= x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5 \\ b(x) &= x^4 - x^2 - 2x - 1. \end{aligned}$$

Find nonzero polynomials $g(x)$ and $r(x)$ such that

1. $g(x)b(x) \equiv r(x) \pmod{a(x)}$.
2. $\deg r(x) < \deg g(x) \le \frac{1}{2} \deg a(x)$.
3. $\mathrm{GCD}(g(x), r(x)) = 1$.

i	$r_i(x)$	$q_i(x)$	$f_i(x)$	$g_i(x)$
-1	$x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5$		1	0
0	$x^4 - x^2 - 2x - 1$		0	1
1	$x^3 - x^2 - x - 2$	$x^2 + 2x + 3$	1	$-x^2 - 2x - 3$
2	$x^2 + x + 1$	$x + 1$	$-x - 1$	$x^3 + 3x^2 + 5x + 4$
3	0	$x - 2$	$x^2 - x - 1$	$-x^4 - x^3 + 4x + 5$

Solution:

$$\begin{aligned} g(x) &= \beta(x^3 + 3x^2 + 5x + 4) \\ r(x) &= \beta(x^2 + x + 1), \end{aligned}$$

where β is a nonzero number.

Decoding of BCH and RS Codes Using Euclid's Algorithm

We apply Euclid's algorithm with $a(x) = x^{2t}$ and $b(x) = S(x)$. From Lemmas 1 and 11, $\sigma(x) = \beta g_j(x)$ and $Z_0(x) = \beta r_j(x)$ for the unique index j, $0 \leq j \leq i_{\max}$ satisfying

$$\deg r_j(x) < t \leq \deg r_{j-1}(x)$$

or equivalently

$$\deg r_j(x) < \deg g_j(x) \leq t.$$

Since $\sigma(0) = 1$ as stated in Lemma 1, $\beta = g_j^{-1}(0)$.