Three polynomials

1) Syndrome polynomial
\[ S(x) = \sum_{m=1}^{n-k} s_m x^{m-1} \]

2) Error locator polynomial
\[ E(x) = \prod_{t \in T} \left(1 - \frac{1}{x - t}\right) \]
\[ \text{deg}(S(x)) \leq 2^{\delta_1} \]
\[ \text{deg}(E(x)) \leq 2^{\delta_1 - 1} \]

3) Error evaluator polynomial
\[ \Gamma(x) = \sum_{j \in T} \epsilon_j x^{j-1} \]
\[ \text{deg}(\Gamma(x)) \leq 2^{\delta_1 - 1} \]

Properties

- \text{gcd}(E(x), \Gamma(x)) = 1
- For \( j \in T \), \( \Gamma(x^{j-1}) = \epsilon_j x^{j-1} \)
- \( E(x) \Gamma(x) \equiv 1 \mod x^{n-k} \)
- \( E(x) \equiv \Gamma(x) \mod x^{n-k} \)

Key equation
\[ E(x) S(x) \equiv \Gamma(x) \mod x^{n-k} \]

In principle, \( E(x) S(x) \) has monomial terms
- Degree of \( \epsilon_j x^{j-1} \) is \( j \)
- Degree of \( \epsilon_j x^{j-1} \) is \( j \)
- Degree of \( \epsilon_j x^{j-1} \) is \( j \)

\( \Gamma(x) \) has monomial terms of degree
- \( 0, 1, 2, \ldots, 2^{\delta_1} - 1 \)

What is \( \beta_0, \beta_1, \ldots, \beta_{n-k} \)?

In general, \( \beta_0, \beta_1, \ldots, \beta_{n-k} \) is zero

But degree in term in \( E(x) S(x) - \Gamma(x) \) does not exist where \( m < n-k \)

\[ \beta_m = 0 \]

\[ \beta_{n-k} = 0 \]