Decoding Reed-Solomon II

CS6025 Data Encoding

Yizong Cheng

4-16-15

Up to Eight Erroneous Codewords

- The error polynomial $E(x)$ is added (XORed) to $C(x)$ after transmission/ strage and the result is $C'(x) = C(x) + E(x)$.
- If $E(x)$ is not zero, the syndromes are no longer zero, too.
- $S_i = C'(\alpha^i) = C(\alpha^i) + E(\alpha^i) = E(\alpha^i)$ because $C(\alpha^i) = 0$ for $i = 0,\ldots,16$
- Let eight codewords at locations $p(j)$ for $j = 0,\ldots,7$ be the ones with errors $E(j)$.
- $E(x) = E(0)x^{p(0)} + E(1)x^{p(1)} + \ldots + E(7)x^{p(7)}$.
- $S_i = E(\alpha^i) = E(0)\,\alpha^{i\,p(0)} + E(1)\,\alpha^{i\,p(1)} + \ldots + E(7)\,\alpha^{i\,p(7)}$
- $\quad = E(0)\,(\alpha^{p(0)})^i + E(1)\,(\alpha^{p(1)})^i + \ldots + E(7)\,(\alpha^{p(7)})^i$.

Arrays Representing Polynomials

- Message: $64x^{25} + 69x^{24} + 102x^{23} \ldots + 182x + 8$
- Error position: 2, 3, 5, 8, ..., 24 (array subscripts)
- Message with errors: $64x^{25} + 69x^{24} + 36x^{23} \ldots + 166x + 8$

```
Original Message  64 69 102 87 35 16 236 17 236 150 106 201 175 226 23 128
154 76 96 209 69 45 171 227 182 8
Random Error Positions  5 8 3 18 2 11 16 24
Random Error Magnitudes  144 2 9 54 66 68 82 16
Message with Errors  64 69 36 94 35 128 236 17 238 150 106 141 175 226 23
128 200 76 86 209 69 45 171 227 166 8
Syndromes  233 247 231 103 70 74 103 166 138 150 164 251 223 61 198 233 2
```

ErrorPositions[i] + p[i] = capacity - 1

- So the array errorPositions and thus errorMagnitudes actually contains capacity – 1 – p(i) (for errorPositions[i]) and E(i) for the polynomial coefficient at p(i) or term $x^{p(i)}$.
- In solveErrorPositions(), we evaluate the error-location polynomial (locators) with β_j^{-1} = inverse of alog[j] for j = 0 to capacity -1.
- When evaluatePolynomial(locators, β_j^{-1}) == 0, we find a root of locators and j is an error position at term x^j .
- This root position j = p(i) for some i and is capacity – 1 - errorPositions[i].

17 Equations for 16 Unknowns

- Let $\beta_i = \alpha^{p(i)}$. Then $p(i) = \log2[\beta_i]$.
- $S_0 = E(0) + E(1) + ... + E(7)$
- $S_1 = E(0)\,\beta_0 + E(1)\,\beta_1 + ... + E(7)\,\beta_7$
- $S_2 = E(0)\,(\beta_0)^2 + E(1)\,(\beta_1)^2 + ... + E(7)\,(\beta_7)^2$
- …
- $S_{16} = E(0)\,(\beta_0)^{16} + E(1)\,(\beta_1)^{16} + ... + E(7)\,(\beta_7)^{16}$
- Unknowns: $E(0), ..., E(7), \beta_0 , ..., \beta_7$
- Now we know $\beta_0 , ..., \beta_7$ and 8 unknowns $E(0), ..., E(7)$ to be solved.

Gaussian Elimination?

- $S_0 = E(0) + E(1) + \ldots + E(7)$
  - $E(7) = S_0 + E(0) + \ldots + E(6)$,
- $S_1 = E(0)\,\beta_0 + E(1)\,\beta_1 + \ldots + E(7)\,\beta_7$
- $S_1\,\beta_7^{-1} = E(0)\,\beta_0\,\beta_7^{-1} + E(1)\,\beta_1\,\beta_7^{-1} + \ldots + E(7)$
- $S_0 + S_1\,\beta_7^{-1} = E(0)(1 + \beta_0\,\beta_7^{-1}) + E(1)(1 + \beta_1\,\beta_7^{-1}) + \ldots + E(6)(1 + \beta_6\,\beta_7^{-1})$

Berlekamp's Method

- Define $Z(x) = 1 + (S_1 + \sigma_1)x + (S_2 + \sigma_1 S_1 + \sigma_2)x^2 + ... +$
- $(S_8 + \sigma_1 S_7 + \sigma_2 S_6 + ... + \sigma_8)x^8$
- $E(i) = Z(\beta_i^{-1}) / \Pi_{k!=i}(1+ \beta_k \beta_i^{-1})$

Homework 24: due 4-22-15

- Implement H24.java by adding Berlekamp’s method of finding error magnitudes.
- We can use the randomly generated errorPositions for the computation.