Erasure Decoding of Reed-Solomon Codes

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

Overview

Erasure Decoding RS - McAuley

Example: RS - McAuley

Erasure Decoding RS - Rizzo

Example: RS - Rizzo

1. Erasure Decoding RS - McAuley

a set of equations can be formed by $\rightarrow$ every codeword $c \in C(x)$, $C(x)$ a (n, k) RS code: $c(x) = m(x)g(x)$

$g(x) \rightarrow$ generator polynomial $\rightarrow$ $n - k$ roots that are consecutive powers of α

$$g(x) = (x - \alpha^{0+\beta})(x - \alpha^{1+\beta})(x - \alpha^{2+\beta})\ldots(x - \alpha^{n-k-1+\beta}), \quad (1)$$

(β is some offset. Normally $\beta = 1$)

1. Erasure Decoding RS - McAuley

$\therefore c(x) \in C = \langle g(x) \rangle$ has the same $n-k$ roots as $g(x)$

form up to $n-k$ linear equations by substituting roots of $g(x)$ into received polynomial $\rightarrow$ result of each substitution should be zero.

McAuley used Gaussian elimination to solve the set of linear equations.

2. Example: RS - McAuley

As a simple example, consider the Reed-Solomon code with the following parameters:

- $n = 7$ (Code length)
- $k = 4$ (Number of data elements)
- $r = n - k = 3$ (Number of redundant elements)
- $d_{min} = n - k + 1 = 4$, thus 3 erasures can be corrected.
- $GF(2^3)$ constructed with primitive polynomial $p(x) = x^3 + x + 1$
- $g(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^3) = x^3 + \alpha^6 x^2 + \alpha^1 x + \alpha^6$
- $d(x) = \alpha^3 x^3 + \alpha^6 x^2 + 1$

2. Example: RS - McAuley

The code polynomial after systematic encoding is:

$$c(x) \quad =$$

2. Example: RS - McAuley

The code polynomial after systematic encoding is:

$$\begin{aligned} c(x) &= d(x) \cdot x^3 + (d(x) \cdot x^3 \mod g(x)) \\ &= (\alpha^3 x^6 + \alpha^6 x^5 + 1x^3) + \\ &\quad ((\alpha^3 x^6 + \alpha^7 x^5 + 1x^3) \mod (x^3 + \alpha^6 x^2 + \alpha^1 x + \alpha^6)) \\ &= \alpha^3 x^6 + \alpha^6 x^5 + 1x^3 + \alpha^5 x^2 + \alpha^1 x + \alpha^2. \end{aligned} \tag{2}$$

2. Example: RS - McAuley

Assume coefficients of the terms of degree 2, 5 and 6 are erased ($\mathbb{E} = \{2, 5, 6\}$).:

$$r(x) = 0x^6 + 0x^5 + 1x^3 + 0x^2 + \alpha^1 x + \alpha^2, \tag{3}$$

Substitute roots α^1, α^2 and α^3 into $r(x)$ (Replace the erased coefficients with variables A, B and C):

$$\begin{aligned}
A(\alpha^1)^6 + B(\alpha^1)^5 + 1(\alpha^1)^3 + C(\alpha^1)^2 + \alpha^1(\alpha^1) + \alpha^2 &= 0 \\
A(\alpha^2)^6 + B(\alpha^2)^5 + 1(\alpha^2)^3 + C(\alpha^2)^2 + \alpha^1(\alpha^2) + \alpha^2 &= 0 \\
A(\alpha^3)^6 + B(\alpha^3)^5 + 1(\alpha^3)^3 + C(\alpha^3)^2 + \alpha^1(\alpha^3) + \alpha^2 &= 0
\end{aligned}$$

2. Example: RS - McAuley

These equations can be reduced to the following set of linear equations.

$$\begin{aligned} \alpha^6 \cdot A + \alpha^5 \cdot B + \alpha^2 \cdot C &= \alpha^3 \\ \alpha^5 \cdot A + \alpha^3 \cdot B + \alpha^4 \cdot C &= \alpha^1 \\ \alpha^4 \cdot A + \alpha^1 \cdot B + \alpha^6 \cdot C &= \alpha^4 \end{aligned}$$

Solving the set of linear equations yields $C = \alpha^5$, $B = \alpha^6$ and $A = \alpha^3$, which gives the correct coefficients for the erased terms. (Homework, Matlab/Octave/Magma/GAP)

3. Erasure Decoding RS - Rizzo

1. Determine the submatrix G^* of the generator matrix
2. Compute the inverse of a G^*
3. Multiply G^* by the compacted received vector $\overline{b}$ of length k.

3. Erasure Decoding RS - Rizzo

G^* is constructed as follows.

Suppose we receive a vector $\overline{r}$ with received indices $M = \{j_0, j_1, \ldots, j_{k-1}\}$, i.e. $|M| = k$.

Construct a submatrix G^* by picking the columns $j_0, j_1 \ldots, j_{k-1}$, $G^* = [C_{j_0}, C_{j_1}, \cdots, C_{j_{k-1}}]$, where C_i is the i-th column of G.

The multiplication of the compacted received vector $\overline{b} = (r_{j_0}, r_{j_1}, \cdots, r_{j_{k-1}})$ by $(G^*)^{-1}$ results in the original information set $\mathcal{I}$.

4. Example: RS - Rizzo

Consider the same code and parameters as in the Example of McAuley.

The systematic generator matrix for this code is given as

$$G =$$

4. Example: RS - Rizzo

Consider the same code and parameters as in the Example of McAuley.

The systematic generator matrix for this code is given as

$$G = \begin{bmatrix} \alpha^6 & \alpha^1 & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^5 & \alpha^2 & \alpha^6 & 0 & 1 & 0 & 0 \\ \alpha^5 & \alpha^4 & \alpha^3 & 0 & 0 & 1 & 0 \\ \alpha^2 & \alpha^0 & \alpha^1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4}$$

4. Example: RS - Rizzo

Transmitted codeword $\rightarrow \overline{c} = (\alpha^2, \alpha^1, \alpha^5, 1, 0, \alpha^6, \alpha^3)$

Received vector $\overline{r}$ is

$$\overline{r} = (\alpha^2, \alpha^1, 0, 1, 0, 0, 0), \tag{5}$$

where the second, fifth and sixth elements have been erased.

elements in positions $\{0, 1, 3, 4\}$ are correctly received.

Form the compacted received vector $\overline{b}$ as $(\alpha^2, \alpha^1, 1, 0)$ and the matrix G^* as

$$G^* = \begin{bmatrix} \alpha^6 & \alpha^1 & 1 & 0 \\ \alpha^5 & \alpha^2 & 0 & 1 \\ \alpha^5 & \alpha^4 & 0 & 0 \\ \alpha^2 & \alpha^0 & 0 & 0 \end{bmatrix}. \tag{6}$$

4. Example: RS - Rizzo

The matrix $(G^*)^{-1}$ is computed as

$$(G^*)^{-1} = \begin{bmatrix} 0 & 0 & \alpha^6 & \alpha^3 \\ 0 & 0 & \alpha^1 & \alpha^4 \\ 1 & 0 & \alpha^3 & \alpha^3 \\ 0 & 1 & \alpha^6 & \alpha^5 \end{bmatrix}. \quad (7)$$

Homework

4. Example: RS - Rizzo

Decoding is accomplished by the following multiplication

$$\begin{aligned} \mathcal{I}^* &= \overline{b} \cdot (G^*)^{-1} \\ &= (\alpha^2, \alpha^1, 1, 0) \begin{bmatrix} 0 & 0 & \alpha^6 & \alpha^3 \\ 0 & 0 & \alpha^1 & \alpha^4 \\ 1 & 0 & \alpha^3 & \alpha^3 \\ 0 & 1 & \alpha^6 & \alpha^5 \end{bmatrix} \\ &= (1, 0, \alpha^6, \alpha^3), \end{aligned} \tag{8}$$

yielding the original information set $\mathcal{I}^* = \mathcal{I}$.

Overview

Erasure Decoding RS - McAuley

Example: RS - McAuley

Erasure Decoding RS - Rizzo

Example: RS - Rizzo