Űrkommunikáció
Space Communication
2023/9.

Decoding of Reed-Solomon codes

Using the matrix $\bar{\bar{H}}$ and the received vector $\bar{v}$ the decoder could calculate the so called syndrome vector:

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \bar{\bar{H}} \cdot [\bar{c} + \bar{e}]^T = \underbrace{\bar{\bar{H}} \cdot \bar{c}^T}_{\bar{0}} + \bar{\bar{H}} \cdot \bar{e}^T = \bar{\bar{H}} \cdot \bar{e}^T$$

Decision in the case of $\bar{s}^T = \bar{0}^T$:

- Trivial: $\bar{v} = \bar{c_i}$
- Unsolvable: $\bar{v} = \bar{c_j} \neq \bar{c_i}$ that we sent

Remark: Error processing in general

In the case of $\bar{s}^T \neq \bar{0}^T$ an equation system of N-K equations should be solved for $2 \cdot t_{corr}$ unknowns (each errors have two attributes: position and value)

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{e}^T$$

The parity check matrix and the error vector:

$$\bar{\bar{H}} = [\bar{h}_1^T \quad \bar{h}_2^T \quad \dots \quad \bar{h}_N^T]$$

The column vectors should be different and excluding $\bar{0}^T$, because they localizing the errors.

$$\bar{e} = [0, 0, \dots, e_i, \dots, e_j, \dots, 0, \dots, 0]$$

Decoding of Reed-Solomon codes

In the case of $\bar{s}^T \neq \bar{0}^T$ an equation system of N-K equations should be solved for $2 \cdot t_{corr}$ unknowns (each errors have two attributes: position and value)

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{e}^T \text{ where } \bar{e} = \left[0, 0, \dots, e_i, \dots, e_j, \dots, 0, \dots, 0\right] \text{ and}$$

$$\bar{\bar{H}} = [\bar{h}_1^T \quad \bar{h}_2^T \quad \dots \quad \bar{h}_N^T] = \begin{bmatrix} 1 & \alpha^1 & \alpha^{2\cdot 1} & \vdots\vdots & h_i^1 & \vdots\vdots & h_j^1 & \vdots\vdots & \alpha^{(N-1)\cdot 1} \\ 1 & \alpha^2 & \alpha^{2\cdot 2} & & h_i^2 & & h_j^2 & & \alpha^{(N-1)\cdot 2} \\ 1 & \alpha^3 & \alpha^{2\cdot 3} & & h_i^3 & & h_j^3 & & \alpha^{(N-1)\cdot 3} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 1 & \alpha^{N-K} & \alpha^{2\cdot(N-K)} & & h_i^{(N-K)} & & h_j^{(N-K)} & & \alpha^{(N-1)\cdot(N-K)} \end{bmatrix}$$

The column vectors are different and excluding $\bar{0}^T$, therefore localizing the errors.
The syndrome vector:

$$\bar{s}^T = \sum_n e_n \cdot \bar{h}_n^T = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{N-K} \end{bmatrix}$$

Or the corresponding non-linear equation system of N-K equations:

$$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1 + e_k \cdot h_k^1 + \cdots$$
$$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2 + e_k \cdot h_k^2 + \cdots$$

$$s_{N-K} = e_i \cdot h_i^{(N-K)} + e_j \cdot h_j^{(N-K)} + e_k \cdot h_k^{(N-K)} + \cdots$$

Peterson-Gorenstein-Zierler algorithm

Peterson-Gorenstein-Zierler algorithm is an efficient method to solve the non-linear equation system for small number of errors.

Suppose two errors to be corrected:

$\bar{e} = [0, 0, \dots, e_i, \dots, e_j, \dots, 0],$ $\qquad t_{corr} = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{N-K}{2} \right\rfloor = 2 \xrightarrow{\text{yields}} N-K=4$

The goal is the determination of the error locators: h_i^1 and h_j^1 and the error values e_i and e_j.

Let L(x) the error locator polynomial with roots h_i^1 and h_j^1: $L(h_i)=0$ and $L(h_j)=0$

$$L(x) = (x-h_i)\cdot(x-h_j) = x^2 \underbrace{-(h_i+h_j)}_{L_1} \cdot x \underbrace{+ h_i \cdot h_j}_{L_0} = x^2 + L_1 \cdot x + L_0$$

Step A: Calculate the syndrome vector: $\bar{s}^T = \overline{\overline{H}} \cdot \bar{v}^T = \overline{\overline{H}} \cdot \bar{e}^T$

The equation system to be solved:

$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1$

$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2$

$s_3 = e_i \cdot h_i^3 + e_j \cdot h_j^3$

$s_4 = e_i \cdot h_i^4 + e_j \cdot h_j^4$

Because h_i^1 and h_j^1 are roots of L(x):

a) $0 = e_i \cdot h_i^1 \cdot L(h_i^1) = e_i \cdot h_i^3 + L_1 \cdot e_i \cdot h_i^2 + L_0 \cdot e_i \cdot h_i^1$

b) $0 = e_j \cdot h_j^1 \cdot L(h_j^1) = e_j \cdot h_j^3 + L_1 \cdot e_j \cdot h_j^2 + L_0 \cdot e_j \cdot h_j^1$

c) $0 = e_i \cdot h_i^2 \cdot L(h_i^1) = e_i \cdot h_i^4 + L_1 \cdot e_i \cdot h_i^3 + L_0 \cdot e_i \cdot h_i^2$

d) $0 = e_j \cdot h_j^2 \cdot L(h_j^1) = e_j \cdot h_j^4 + L_1 \cdot e_j \cdot h_j^3 + L_0 \cdot e_j \cdot h_j^2$

Step B: Solve the equation system of two linear equations for the coefficients of L(x):

a)+b): $0 = s_3 + L_1 \cdot s_2 + L_0 \cdot s_1$

c)+d): $0 = s_4 + L_1 \cdot s_3 + L_0 \cdot s_2 \xrightarrow{\text{yields}} L_1 \text{ and } L_0$

Peterson-Gorenstein-Zierler algorithm

Step C: Solve (find the roots) the quadratic equation for h_i^1 and h_j^1 error locators:

$$x^2 + L_1 \cdot x + L_0 = 0 \xrightarrow{\text{yields}} \hat{h}_i \textit{ and } \hat{h}_j; \qquad \hat{h}_{i,j} = -\frac{L_1}{2} \pm \sqrt[2]{\left(\frac{L_1}{2}\right)^2 - L_0}$$

Step D: Solve the equation system of two equations for the error values e_i and e_j

$$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1$$

$$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2 \xrightarrow{\text{yields}} \hat{e}_i \text{ and } \hat{e}_j$$

Last steps for decoding:

Decided error vector: $\hat{\hat{e}} = [0, 0, \cdots, \hat{e}_i, \dots, \hat{e}_j, \dots, 0]$

Decided code vector: $\hat{\hat{c}} = \bar{v} - \hat{\hat{e}}$

Remark: The algorithm is also applicable for more errors but not very efficiently. E.g. y errors:

$$L(x) = \underbrace{(x - h_i) \cdot (x - h_j) \cdots (x - h_k)}_{y} = x^y + L_{y-1} \cdot x^{y-1} + \cdots + L_1 \cdot x + L_0$$

$$0 = e_i \cdot h_i^1 \cdot L(h_i^1) = e_i \cdot h_i^{y+1} + L_{y-1} \cdot e_i \cdot h_i^y + \cdots + L_1 \cdot e_i \cdot h_i^2 + L_0 \cdot e_i \cdot h_i^1$$

$$0 = e_j \cdot h_j^1 \cdot L(h_j^1) = e_j \cdot h_j^{y+1} + L_{y-1} \cdot e_j \cdot h_j^y + \cdots + L_1 \cdot e_j \cdot h_j^2 + L_0 \cdot e_j \cdot h_j^1$$

$$\dots$$

$$0 = e_k \cdot h_k^1 \cdot L(h_k^1) = e_k \cdot h_k^{y+1} + L_{y-1} \cdot e_k \cdot h_k^y + \cdots + L_1 \cdot e_k \cdot h_k^2 + L_0 \cdot e_k \cdot h_k^1$$

$$\dots$$

$$0 = s_{y+1} + L_{y-1} \cdot s_y + \cdots + L_1 \cdot s_2 + L_0 \cdot s_1$$

…

Example: Reed-Solomon code over GF(q)

Defining the parameters (N,K,q, α):

- order of primitive element α is m=q-1
- $N \leq m = q - 1$ *(remember Method A)*
- MDS: $t_{corr} = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{N-K}{2} \right\rfloor \xrightarrow{\text{yields}} K = N - 2 \cdot t_{corr}$

Correction of two errors:

Smallest appropriate q=7, N=6 max., K=2, use α=3: (N=6,K=2,q=7, $\alpha = 3$)

Defining the generator matrix *(remember Method B)*

$$\bar{\bar{G}} = \begin{bmatrix} 1 & 1 & 1 & & 1 & 1 \\ 1 & \alpha & \alpha^2 & & \alpha^{N-2} & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \vdots\ \vdots & \alpha^{2(N-2)} & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & \alpha^{K-1} & \alpha^{2(K-1)} & & \alpha^{(K-1)(N-2)} & \alpha^{(K-1)(N-1)} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix}$$

Defining the matrix *(remember Method C)*

$$\bar{\bar{H}} = \begin{bmatrix} 1 & \alpha^1 & \alpha^{2\cdot 1} & & \alpha^{(N-2)\cdot 1} & \alpha^{(N-1)\cdot 1} \\ 1 & \alpha^2 & \alpha^{2\cdot 2} & & \alpha^{(N-2)\cdot 2} & \alpha^{(N-1)\cdot 2} \\ 1 & \alpha^3 & \alpha^{2\cdot 3} & \vdots\ \vdots & \alpha^{(N-2)\cdot 3} & \alpha^{(N-1)\cdot 3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & \alpha^{N-K} & \alpha^{2\cdot(N-K)} & & \alpha^{(N-2)\cdot(N-K)} & \alpha^{(N-1)\cdot(N-K)} \end{bmatrix} = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

Example: Reed-Solomon code over GF(q)

Let the message vector.

$$\bar{u} = [3 \quad 4]$$

The corresponding code vector:

$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [3 \quad 4] \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix} = [0 \quad 1 \quad 4 \quad 6 \quad 5 \quad 2]$$

Let the two errors represented by:

$$\bar{e} = [0 \quad 5 \quad 0 \quad 4 \quad 0 \quad 0]$$

Then the received vector:

$$\bar{v} = \bar{c} + \bar{e} = [0 \quad 6 \quad 4 \quad 3 \quad 5 \quad 2]$$

Step A: Calculate the syndrome vector:

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \bar{\bar{H}} \cdot \bar{e}^T = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 6 \\ 4 \\ 3 \\ 5 \\ 2 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \\ 5 \\ 3 \end{bmatrix}$$

Step B: Solve the equation system of two linear equations for the coefficients of L(x):

$$0 = 5 + L_1 \cdot 0 + L_0 \cdot 4 \xrightarrow{\text{yields}} L_0 = \frac{-5}{4} = \frac{2}{4} = 4$$

$$0 = 3 + L_1 \cdot 5 + L_0 \cdot 0 \xrightarrow{\text{yields}} L_1 = \frac{-3}{5} = \frac{4}{5} = 5$$

Example: Reed-Solomon code over GF(q)

Step C: Solve the quadratic equation for h_i^1 and h_j^1 error locators:

$$x^2 + L_1 \cdot x + L_0 = 0 \xrightarrow{\text{yields}} \hat{h}_i \; and \; \hat{h}_j; \qquad \hat{h}_{i,j} = -\frac{L_1}{2} \pm \sqrt[2]{\left(\frac{L_1}{2}\right)^2 - L_0}$$

$$x^2 + 5 \cdot x + 4 = 0; \hat{h}_{i,j} = -\frac{5}{2} \pm \sqrt[2]{\left(\frac{5}{2}\right)^2 - 4} = \frac{2}{2} \pm \sqrt[2]{(6)^2 - 4} = 1 \pm \sqrt[2]{4} = 1 \pm 2;$$

$$\hat{h}_i = 3 \; and \; \hat{h}_j = 6 \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

Step D: Solve the equation system of two equations for the error values e_i and e_j

$$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1$$

$$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2 \xrightarrow{\text{yields}} \hat{e}_i \text{ and } \hat{e}_j$$

a) $4 = e_i \cdot 3 + e_j \cdot 6$

b) $0 = e_i \cdot 2 + e_j \cdot 1$

6xb) $0 = e_i \cdot 5 + e_j \cdot 6$

a)-6xb) $4 = e_i \cdot 5$ $\qquad e_i = \frac{4}{5} = 5$ $\qquad$ From b) $0 = 3 + e_j \cdot 1$ $\qquad e_j = -3 = 4$

Last steps for decoding:

Decided error vector: $\hat{\bar{e}} = [0, 5, 0, 4, 0, 0]$

Decided code vector: $\hat{\bar{c}} = \bar{v} - \hat{\bar{e}}$

2nd Example: Reed-Solomon code over GF(q)

Let the message vector.

$$\bar{u} = [2 \quad 4]$$

The corresponding code vector:

$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [2 \quad 4] \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix} = [6 \quad 0 \quad 3 \quad 5 \quad 4 \quad 1]$$

Let the two errors represented by:

$$\bar{e} = [3 \quad 0 \quad 0 \quad 0 \quad 4 \quad 0]$$

Then the received vector:

$$\bar{v} = \bar{c} + \bar{e} = [2 \quad 0 \quad 3 \quad 5 \quad 1 \quad 1]$$

Step A: Calculate the syndrome vector:

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \bar{\bar{H}} \cdot \bar{e}^T = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 0 \\ 3 \\ 5 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \\ 0 \\ 5 \end{bmatrix}$$

Step B: Solve the equation system of two linear equations for the coefficients of L(x):

$$0 = 0 \quad + L_1 \cdot \quad 4 + L_0 \cdot \quad 5 \xrightarrow{\text{yields}} L_0 = 2/4 = 4$$

$$0 = 5 \quad + L_1 \cdot \quad 0 + L_0 \cdot \quad 4 \xrightarrow{\text{yields}} L_1 = -6/4 = 1/4 = 2$$

-5=4L0; L0=-5/4; L0=2/4=4

Example: Reed-Solomon code over GF(q)

Step C: Solve the quadratic equation for h_i^1 and h_j^1 error locators:

$$x^2 + L_1 \cdot x + L_0 = 0 \xrightarrow{\text{yields}} \hat{h}_i \text{ and } \hat{h}_j; \qquad \hat{h}_{i,j} = -\frac{L_1}{2} \pm \sqrt[2]{\left(\frac{L_1}{2}\right)^2 - L_0}$$

$$x^2 + \ 2 \cdot x + 4 = 0; \qquad \hat{h}_{i,j} = -\frac{2}{2} \pm \sqrt[2]{\left(\frac{2}{2}\right)^2 - 4} = 6 \pm \sqrt[2]{(1)^2 - 4} = 6 \pm \sqrt[2]{4} = 6 \pm 2;$$

$$\hat{h}_i = 1 \ \ and \ \hat{h}_j = 4 \qquad \begin{bmatrix} \color{red}{1} & 3 & 2 & 6 & \color{red}{4} & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

Step D: Solve the equation system of two linear equations for the error values e_i and e_j

$$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1$$

$$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2 \xrightarrow{\text{yields}} \hat{e}_i \text{ and } \hat{e}_j$$

a) $5 = e_i \cdot 1 + e_j \cdot 4$

b) $4 = e_i \cdot 1 + e_j \cdot 2$

$e_i = 3$ $\qquad$ $e_j = 4$

Last steps for decoding:

Decided error vector: $\hat{\bar{e}} = [3, 0, 0, 0, 4, 0]$

Decided code vector: $\hat{\bar{c}} = \bar{v} - \hat{\bar{e}}$

Optional home work: Reed-Solomon code over GF(q)

Let the message vector.

$$\bar{u} = [\qquad\qquad]$$

The corresponding code vector:

$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = [\qquad\qquad] \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix} = [\qquad\qquad\qquad\qquad\qquad\qquad\qquad]$$

Let the two errors represented by:

$$\bar{e} = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$$

Then the received vector:

$$\bar{v} = \bar{c} + \bar{e} = [\qquad\qquad\qquad\qquad\qquad\qquad\qquad]$$

Step A: Calculate the syndrome vector:

$$\bar{s}^T = \bar{\bar{H}} \cdot \bar{v}^T = \bar{\bar{H}} \cdot \bar{e}^T = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix} \cdot \begin{bmatrix} \\ \\ \\ \\ \\ \\ \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} \\ \\ \\ \\ \end{bmatrix}$$

Step B: Solve the equation system of two linear equations for the coefficients of L(x):

$$0 = \qquad +L_1 \cdot \qquad + L_0 \cdot \qquad \xrightarrow{\text{yields}} L_0 =$$

$$0 = \qquad +L_1 \cdot \qquad + L_0 \cdot \qquad \xrightarrow{\text{yields}} L_1 =$$

Example: Reed-Solomon code over GF(q)

Step C: Solve the quadratic equation for h_i^1 and h_j^1 error locators:

$$x^2 + L_1 \cdot x + L_0 = 0 \xrightarrow{\text{yields}} \hat{h}_i \; and \; \hat{h}_j; \qquad \hat{h}_{i,j} = -\frac{L_1}{2} \pm \sqrt[2]{\left(\frac{L_1}{2}\right)^2 - L_0}$$

$$x^2 + \quad \cdot x + \quad = 0; \quad \hat{h}_{i,j} = -- \pm \sqrt[2]{\left(-\right)^2 -} = - \pm \sqrt[2]{(\quad)^2 -} = \pm \sqrt[2]{\quad} = \pm \; ;$$

$$\hat{h}_i = \quad and \; \hat{h}_j = \quad \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

Step D: Solve the equation system of two linear equations for the error values e_i and e_j

$$s_1 = e_i \cdot h_i^1 + e_j \cdot h_j^1$$

$$s_2 = e_i \cdot h_i^2 + e_j \cdot h_j^2 \xrightarrow{\text{yields}} \hat{e}_i \text{ and } \hat{e}_j$$

a) $\quad = e_i \cdot + e_j \cdot$

b) $\quad = e_i \cdot + e_j \cdot$

$e_i =$ $\qquad$ $e_j =$

Last steps for decoding:

Decided error vector: $\hat{\hat{e}} = [0, 0, 0, 0, 0, 0]$

Decided code vector: $\hat{\hat{c}} = \bar{v} - \hat{\hat{e}}$