Reed-Solomon Decoding

Kwame Ackah Bohulu

July 12, 2018

1 Introduction

We aim to find $\mathbf{e}_{\hat{u}}$ which minimizes the weight of $\mathbf{e}$ To begin we assume that a (n,k) t-error correcting Reed-Solomon (RS) code is transmitted over an AWGN channel and received by the receiver. This received sequence can be written as a polynomial as shown below

$$r(X) = r_0 + r_1 X^1 + r_2 X^2 + \cdots + r_{n-1} X^{n-1} \tag{1}$$

Also for each codeword $\mathbf{c} \in \mathbb{C}$ in polynomial form

$$c(X) = c_0 + c_1 X^1 + c_2 X^2 + \cdots + c_{n-1} X^{n-1} \tag{2}$$

$$\begin{aligned}
&c(\alpha^1) = c_0 + c_1\alpha^1 + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0 \\
&c(\alpha^2) = c_0 + c_1(\alpha^1)^2 + c_2(\alpha^2)^2 + \cdots + c_{n-1}(\alpha^{n-1})^2 = 0 \\
&. \\
&. \\
&. \\
&c(\alpha^{2t}) = c_0 + r_1(\alpha^1)^{2t} + r_2(\alpha^2)^{2t} + \cdots + r_{n-1}(\alpha^{n-1})^{2t} = 0
\end{aligned} \tag{3}$$

Which means $\mathbf{c}\mathbf{H}^T = \mathbf{0}_{2t}$ We also define the following matrices

$$\mathbf{H} = \begin{bmatrix}
1 & \alpha^1 & \alpha^2 & \dots & \alpha^{(2^m-1)} \\
1 & (\alpha)^2 & \alpha^{(2)2} & \dots & \alpha^{2(2^m-1)} \\
 & & & \vdots & \\
1 & (\alpha^{2t-1}) & \alpha^{(2t-1)2} & \dots & \alpha^{(2t-1)(2^m-1)} \\
1 & (\alpha^{2t}) & \alpha^{(2t)2} & \dots & \alpha^{2t(2^m-1)}
\end{bmatrix} \tag{4}$$

$$\mathbf{G} = \begin{bmatrix}
1 & \alpha^{2t+1} & \alpha^{(2t+1)2} & \dots & \alpha^{(2t+1)(2^m-1)} \\
1 & (\alpha)^{2t+2} & \alpha^{(2t+2)2} & \dots & \alpha^{(2t+2)(2^m-1)} \\
 & & & \vdots & \\
1 & (\alpha^{2^m-2}) & \alpha^{(2^m-2)2} & \dots & \alpha^{(2^m-2)(2^m-1)} \\
1 & 1 & 1 & \dots & 1
\end{bmatrix} \tag{5}$$

Where $\mathbf{H}$ and $\mathbf{G}$ are the Parity-Check and Generator matrices for the transmitted RS code. We then proceed to define $\mathbf{A}$ as follows

$$\mathbf{A} = \begin{bmatrix} \mathbf{H} \\ \mathbf{G} \end{bmatrix} \tag{6}$$

We note that inverse of $\mathbf{A}$ is its conjugate. Assuming the received sequence is in error, we may write $\mathbf{r}$ as

$$\mathbf{r} = \mathbf{c} + \mathbf{e} \tag{7}$$

where $\mathbf{c} = \begin{bmatrix} c_0 & c_1 & \dots & c_{n-2} & c_{n-1} \end{bmatrix}$ is the codeword vector and
where $\mathbf{e} = \begin{bmatrix} e_0 & e_1 & \dots & e_{n-2} & e_{n-1} \end{bmatrix}$ is the error vector
multiplying $\mathbf{r}$ by $\mathbf{A}$ gives us

$$\mathbf{r} \cdot \mathbf{A}^T = \mathbf{c}\mathbf{A}^T + \mathbf{e}\mathbf{A}^T \tag{8}$$

We know that

$$\mathbf{c}\mathbf{A}^T = \begin{bmatrix} \mathbf{0}_{2t} & \mathbf{u}_k \end{bmatrix}$$

and

$$\mathbf{e}\mathbf{A}^T = \begin{bmatrix} \mathbf{s} & \mathbf{v} \end{bmatrix}$$

where $\mathbf{s} = \mathbf{e}\mathbf{H}^T$ is the syndrome and $\mathbf{v} = \mathbf{e}\mathbf{G}^T$
We seek to find $\min w_{\min}(\mathbf{e})$ such that $\mathbf{e} \cdot \mathbf{H}^T = \mathbf{e}_H$

$$\begin{aligned} &\mathbf{e} \cdot \mathbf{A}^T = \begin{bmatrix} \mathbf{s} & \mathbf{v} \end{bmatrix} \\ &\mathbf{e} \cdot \mathbf{A}^T \cdot \mathbf{A}^H = \mathbf{e}\mathbf{I} = \begin{bmatrix} \mathbf{s} & \mathbf{v} \end{bmatrix} \cdot \mathbf{A}^H \\ &= \begin{bmatrix} \mathbf{s} & \mathbf{0} \end{bmatrix} \mathbf{A}^H + = \begin{bmatrix} \mathbf{0} & \mathbf{v} \end{bmatrix} \mathbf{A}^H \end{aligned} \tag{9}$$

which means

$$\mathbf{e} = \mathbf{s}\mathbf{H}^* + \mathbf{v}\mathbf{G}^* \tag{10}$$

where $\mathbf{H}^*, \mathbf{G}^*$ are the conjugates of $\mathbf{H}$ and $\mathbf{G}$ respectively.

$$\mathbf{H}^* = \begin{bmatrix} 1 & \alpha^{(2^m-1)} & \alpha^{(2^m-2)} & \dots & \alpha^1 \\ 1 & \alpha^{2(2^m-1)} & \alpha^{(2)(2^m-2)} & \dots & (\alpha)^2 \\ & & & \vdots & \\ 1 & \alpha^{2t-1(2^m-1)} & \alpha^{(2t-1)(2^m-2)} & \dots & (\alpha^{2t-1}) \\ 1 & (\alpha^{2t}) & \alpha^{(2t)2} & \dots & \alpha^{2t(2^m-1)} \end{bmatrix} \tag{11}$$

$$\mathbf{G}^* = \begin{bmatrix} 1 & \alpha^{2t+1(2^m-1)} & \alpha^{(2t+1)(2^m-2)} & \dots & \alpha^{2t+1} \\ 1 & \alpha^{2t+2(2^m-1)} & \alpha^{(2t+2)(2^m-2)} & \dots & (\alpha)^{2t+2} \\ & & & \vdots & \\ 1 & \alpha^{2^m-2(2^m-1)} & \alpha^{(2^m-2)(2^m-2)} & \dots & (\alpha_{2^m-2}) \\ 1 & 1 & 1 & \dots & 1 \end{bmatrix} \tag{12}$$

And

$$\mathbf{A}^H = \begin{bmatrix} \mathbf{H}^* \\ \mathbf{G}^* \end{bmatrix} \tag{13}$$

We rewrite (8) as

$$\begin{aligned} \mathbf{r}\mathbf{A}^T &= \begin{bmatrix} \mathbf{r}\mathbf{H}^T & \mathbf{r}\mathbf{G}^T \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{s} & \mathbf{w} \end{bmatrix} \end{aligned} \tag{14}$$

where $\mathbf{s} = \mathbf{r}\mathbf{H}^T$ and $\mathbf{w} = \mathbf{r}\mathbf{G}^T$
which means

$$\begin{aligned} \mathbf{r} \cdot \mathbf{A}^T \cdot \mathbf{A}^H =& \begin{bmatrix} \mathbf{s} & \mathbf{w} \end{bmatrix} \mathbf{A}^H \\ \mathbf{r} =& \mathbf{sH}^* + \mathbf{wG}^* \\ \mathbf{sH}^* =& \mathbf{wG}^* + \mathbf{r} \end{aligned} \tag{15}$$

Substituting (15) into (10) we get

$$\begin{aligned} \mathbf{e} =& \mathbf{wG}^* + \mathbf{r} + \mathbf{vG}^* \\ =& (\mathbf{w} + \mathbf{v})\mathbf{G}^* + \mathbf{r} \end{aligned} \tag{16}$$

Assuming that the weight of the codeword is the summation of the decimal representation of the non-zero elements of the codeword, we want to find a value of v that when inserted into (10) gives an error vector $\mathbf{e}$ with weight less than or equal to $\mathbf{r}$.

2 Decoding Algorithm

- set $\mathbf{w} = \mathbf{v} + \begin{bmatrix} \alpha^i & \mathbf{0}_{k-1} \end{bmatrix}, i = 1, 2, ..., n-1$
- for each value of $\mathbf{w}$ find the corresponding value $\mathbf{e}$ using (16) and weight $W_H(\mathbf{e}_i)$of $\mathbf{e}$
- select