A GRS decoding example

Consider the code $GRS_{10,4}(\boldsymbol{\alpha}, \mathbf{v})$ over $\mathbb{F}_{11}$ with

$$\boldsymbol{\alpha} = \mathbf{v} = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)\,,$$

hence (by direct calculation or Problems 5.1.3/5.1.5) we may take

$$\mathbf{u} = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1)\,.$$

Note that here $r = 10 - 4 = 6$, so we can correct up to $r/2 = 3$ errors.

We wish to decode the received word

$$\mathbf{p} = (0, 0, 8, 0, 0, 2, 0, 0, 7, 0)\,.$$

First calculate the syndrome polynomial:

$$S_{\mathbf{p}}(z) = \sum_{j=1}^{10} \frac{u_j \cdot p_j}{1 - \alpha_j z} = \frac{1 \cdot 8}{1 - 8z} + \frac{1 \cdot 2}{1 - 5z} + \frac{1 \cdot 7}{1 - 2z} \pmod{z^6}$$

$$\begin{array}{rlllllll} = & 8(& 1 & +8z & +9z^2 & +6z^3 & +4z^4 & +10z^5) \\ & +2(& 1 & +5z & +3z^2 & +4z^3 & +9z^4 & +z^5) \quad \pmod{z^6} \\ & +7(& 1 & +2z & +4z^2 & +8z^3 & +5z^4 & +10z^5) \end{array}$$

$$= 6 + 0z + 7z^2 + 2z^3 + 8z^4 + 9z^5\,.$$

We now (partially) calculate $\gcd(z^6, 9z^5 + 8z^4 + 2z^3 + 7z^2 + 6) = 1$ over $\mathbb{F}_{11}$, the Euclidean Algorithm example discussed in class (and on a handout).

In our Euclidean Algorithm example, Step 3, where $r_3(z) = 10z^2 + 5z + 7$, is the first step j for which the degree of $r_j(z)$ is less than $r/2 = 3$. So, in decoding, we stop at this step.

We have $t_3(z) = 2z^3 + 10z + 3$, hence $t_3(0)^{-1} = 3^{-1} = 4$. We thus set

$\sigma(z) = 4(2z^3 + 10z + 3) = 8z^3 + 7z + 1$ and $\omega(z) = 4(10z^2 + 5z + 7) = 7z^2 + 9z + 6$

(These are really our guesses $\hat{\sigma}(z)$ and $\hat{\omega}(z)$.)

The polynomial $\sigma(z) = 8z^3 + 7z + 1$ has roots 6, 7, and 9:

$$\begin{aligned} 0 &= 8 \times 6^3 + 7 \times 6 + 1 = 8 \times 7 + 7 \times 6 + 1 = 56 + 42 + 1 = 99 \pmod{11} \\ 0 &= 8 \times 7^3 + 7 \times 7 + 1 = 8 \times 2 + 7 \times 7 + 1 = 16 + 49 + 1 = 66 \pmod{11} \\ 0 &= 8 \times 9^3 + 7 \times 9 + 1 = 8 \times 3 + 7 \times 9 + 1 = 24 + 63 + 1 = 88 \pmod{11}\,. \end{aligned}$$

We then have

$$\begin{aligned} 6^{-1} = 2 &= \alpha_9 \\ 7^{-1} = 8 &= \alpha_3 \\ 9^{-1} = 5 &= \alpha_6 \end{aligned}$$

Therefore we assume that the errors are located at positions 3, 6, and 9.

To calculate the associated error values, in addition to the error evaluator polynomial $\omega(z) = 7z^2 + 9z + 6$ we also need

$$\sigma'(z) = (8z^3 + 7z + 1)' = 24z^2 + 7 + 0 = 2z^2 + 7\,.$$

Now

$$\begin{aligned} e_3 &= \frac{-\alpha_3\,\omega(\alpha_3^{-1})}{u_3\,\sigma'(\alpha_3^{-1})} = \frac{-8 \times \omega(8^{-1})}{1 \times \sigma'(8^{-1})} = \frac{3 \times (7 \times 7^2 + 9 \times 7 + 6)}{2 \times 7^2 + 7} \\ &= \frac{3 \times (7 \times 5 + 63 + 6)}{2 \times 5 + 7} = \frac{3 \times (2 + 8 + 6)}{6} \\ &= \frac{3 \times 5}{6} = 4 \times 6^{-1} = 4 \times 2 = 8\ ; \end{aligned}$$

and

$$\begin{aligned} e_6 &= \frac{-\alpha_6\,\omega(\alpha_6^{-1})}{u_6\,\sigma'(\alpha_6^{-1})} = \frac{-5 \times \omega(5^{-1})}{1 \times \sigma'(5^{-1})} = \frac{6 \times (7 \times 9^2 + 9 \times 9 + 6)}{2 \times 9^2 + 7} \\ &= \frac{6 \times 5}{4} = \frac{8}{4} = 2\ ; \end{aligned}$$

and

$$\begin{aligned} e_9 &= \frac{-\alpha_9\,\omega(\alpha_9^{-1})}{u_9\,\sigma'(\alpha_9^{-1})} = \frac{-2 \times \omega(2^{-1})}{1 \times \sigma'(2^{-1})} = \frac{9 \times (7 \times 6^2 + 9 \times 6 + 6)}{2 \times 6^2 + 7} \\ &= \frac{9 \times 4}{2} = 9 \times 2 = 7\ . \end{aligned}$$

Therefore the error vector is equal to $(0,0,8,0,0,2,0,0,7,0)$. This was also the received vector $\mathbf{p}$, so we decode to

$$(0,0,8,0,0,2,0,0,7,0) - (0,0,8,0,0,2,0,0,7,0) = (0,0,0,0,0,0,0,0,0,0)\,.$$

This is the expected result, since the minimal weight of the code is $n - k + 1 = 10 - 4 + 1 = 7$. The codeword $\mathbf{0}$ is the unique closest codeword to the weight 3 received vector $\mathbf{p}$.