There are several theoretical results of importance for our Euclidean Algorithm based decoding of *GRS* codes.

Appendix:

(2.16) THEOREM. *In $F[x]$, F a field, let $a(x)$ and $b(x)$ be two polynomials not both equal to 0. Then there is a unique monic polynomial $g(x)$ in $F[x]$ such that:*
(i) $a(x)$ and $b(x)$ are multiples of $g(x)$;
(ii) if $n(x)$ divides both $a(x)$ and $b(x)$ then $g(x)$ is a multiple of $n(x)$.
Indeed $g(x)$ is the unique monic polynomial of minimal degree in the set

$$G = \{\, s(x)a(x) + t(x)b(x) \mid s(x), t(x) \in F[x] \,\}\,.$$

Chapter 5:

(2.2) THEOREM. *Given r and $S(z) \in F[z]$ there is at most one pair of polynomials $\sigma(z), \omega(z)$ in $F[z]$ satisfying:*
(1) $\sigma(z)S(z) = \omega(z) \pmod{z^r}$;
(2) $\deg(\sigma(z)) \le r/2$ *and* $\deg(\omega(z)) < r/2$;
(3) $\gcd(\sigma(z), \omega(z)) = 1$ *and* $\sigma(0) = 1$.

Appendix:

(3.1) THEOREM. *(THE EUCLIDEAN ALGORITHM.)*
Assume that $\deg(a(x)) \ge \deg(b(x))$ with $a(x) \neq 0$. At Step i we construct the equation

$$\mathbf{E_i} : r_i(x) = s_i(x)a(x) + t_i(x)b(x).$$

Equation $\mathbf{E_i}$ is constructed from $\mathbf{E_{i-1}}$ and $\mathbf{E_{i-2}}$, the appropriate initialization being provided by (4) and (5):

$$\begin{aligned} r_{-1}(x) = a(x);\quad s_{-1}(x) = 1;\quad t_{-1}(x) = 0;\\ r_0(x) = b(x);\quad s_0(x) = 0;\quad t_0(x) = 1. \end{aligned}$$

Step i. Starting with $r_{i-2}(x)$ and $r_{i-1}(x)$ $(\neq 0)$ use the Division Algorithm A.2.5 to define $q_i(x)$ and $r_i(x)$:

$$r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x) \text{ with } \deg(r_i(x)) < \deg(r_{i-1}(x)).$$

Next define $s_i(x)$ and $t_i(x)$ by:

$$\begin{aligned} s_i(x) &= s_{i-2}(x) - q_i(x)s_{i-1}(x);\\ t_i(x) &= t_{i-2}(x) - q_i(x)t_{i-1}(x). \end{aligned}$$

We then have the equation

$$\mathbf{E_i} : r_i(x) = s_i(x)a(x) + t_i(x)b(x).$$

Begin with $i = 0$. If we have $r_i(x) \neq 0$, then proceed to Step i+1. Eventually there will be an i with $r_i(x) = 0$. At that point halt and declare $\gcd(a(x), b(x))$ *to be the unique monic scalar multiple of the nonzero polynomial $r_{i-1}(x)$.*

Chapter 5:

(2.4) THEOREM. *(*DECODING *GRS* USING THE EUCLIDEAN ALGORITHM.*) Consider the code $GRS_{n,k}(\boldsymbol{\alpha}, \mathbf{v})$ over F, and set $r = n - k$. Given a syndrome polynomial $S(z)$ (of degree less than r), the following algorithm halts, producing polynomials $\tilde{\sigma}(z)$ and $\tilde{\omega}(z)$:*

Set $a(z) = z^r$ and $b(z) = S(z)$. *Step through the Euclidean Algorithm A.3.1* *until at Step j, $\deg(r_j(z)) < r/2$.* *Set $\tilde{\sigma}(z) = t_j(z)$* *and $\tilde{\omega}(z) = r_j(z)$.*

If there is an error word $\mathbf{e}$ of weight at most $r/2 = (d_{min} - 1)/2$ with $S_{\mathbf{e}}(z) = S(z)$, then $\widehat{\sigma}(z) = \tilde{\sigma}(0)^{-1}\tilde{\sigma}(z)$ and $\widehat{\omega}(z) = \tilde{\sigma}(0)^{-1}\tilde{\omega}(z)$ are the error locator and evaluator polynomials for $\mathbf{e}$.

Given the polynomials $\sigma(z) = \sigma_{\mathbf{e}}(z)$ and $\omega(z) = \omega_{\mathbf{e}}(z)$, we can reconstruct the error vector $\mathbf{e}$. *We assume that none of the α_i are equal to* 0. Then:

$$B = \{\, b \,|\, \sigma(\alpha_b^{-1}) = 0 \,\}$$

and, for each $b \in B$,

$$e_b = \frac{-\alpha_b \omega(\alpha_b^{-1})}{u_b \sigma'(\alpha_b^{-1})} \ ,$$

where $\sigma'(z)$ is the formal derivative of $\sigma(z)$.