4 Decoding of AG Codes

Throughout this section we will fix a algebraic geometry code $\mathcal{C}_{D,G}$ constructed on the curve $\mathcal{X}$ of genus g. We will describe and show the correctness of an t-error decoding algorithm for $\mathcal{C}_{D,G}$ with

$$t \leq \left\lfloor \frac{d^* - 1}{2} - \frac{g}{2} \right\rfloor$$

The term $\frac{g}{2}$ is called the *genus penalty*. Our treatment will be based on Couvreur and Randriambololona (2020)[Section 6.1]

We start by proving the following proposition, which will guide our search for such an decoding algorithm.

Proposition 4.1. *Let $\mathcal{C}$ be a $[n, k, d]_q$ code with parity check matrix H. Furthermore let $y = c + e$ where $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$ and $J \subseteq \{1, \ldots, n\}$, such that* $\operatorname{supp}(e) \subseteq J$ *and $|J| < d$. Then e is the unique solution to the system:*

$$\begin{cases} He = Hy \\ e_i = 0 \text{ for all } i \in \{1, \ldots, n\} \setminus J \end{cases} \tag{4.1}$$

Proof. Clearly e is a solution to the system in Equation (4.1) since $Hy = Hc + He = He$. Additionally if e' is another solution to $He' = Hy$ such that $\operatorname{supp}(e) \subseteq J$, then $e - e' \in \operatorname{null}(H) = \mathcal{C}$, however as $|J| < d$ the codeword $e' - e$ has weight $\operatorname{wt}(e' - e) \leq d$ meaning $e' - e = 0$. ■

For the remaining part of the section we will let $y = c + e$ with $c \in \mathcal{C}_{D,G}$, meaning $c = (f(P_1), f(P_2), \ldots, f(P_n))$ for some $f \in L(G)$, and $e \in \mathbb{F}_q^n$ such that $\operatorname{wt}(e) \leq t$, unless otherwise specified. Proposition 4.1, implies that if we can find a small subset J such that $\operatorname{supp}(e) \subseteq J$, correcting the errors in the recived vector y is simply a matter of solving the linear system presented in Equation (4.1) for $e \in \mathbb{F}_q^n$. To find such a subset J we introduce the concept of an *error locating function.*

We will now describe a procedure for locating the errors. Let F be a divisor such that $\operatorname{supp}(F) \cap \operatorname{supp}(D) = \emptyset$. If $\lambda \in L(F)$ vanishes at every point P_i where $i \in \operatorname{supp}(e)$ then:

$$\lambda(P_i)y_i = \lambda(P_i)f(P_i) \text{ for all } i \in \{1, \ldots, n\}.$$

Since either $e_i = 0$ meaning $y_i = f(P_i)$ or alternatively if $i \in \operatorname{supp}(e)$ then $\lambda(P_i) = 0$. Hence λ can be used to locate the $\operatorname{supp}(e)$.

Remark 4.2. If $f \in L(G)$ and $\lambda \in L(F)$, then $\lambda f \in L(G + F)$. This can be seen as follows

$$(\lambda f) = \sum_{P \in \mathcal{X}} v_P(\lambda f)P \overset{(a)}{=} \sum_{P \in \mathcal{X}} (v_P(\lambda) + v_P(f))P = (\lambda) + (f)$$

where (a) follows as v_P is a discrete valuation. Now since $(f) + G$ and $(\lambda) + F$ are effective divisors, we see that $(\lambda f) + (G + F) = (\lambda) + (f) + G + F$ is effective.

The contents of Remark 4.2, motivates the following definition:

Definition 4.3. Let F be a divisor on $\mathcal{X}$ such that $\operatorname{supp}(F) \cap \operatorname{supp}(D) = \emptyset$, then we define the set of *error locating functions* as:

$$K_y(F) := \{\lambda \in L(F) \mid (\lambda(P_1)y_1, \lambda(P_2)y_2, \ldots, \lambda(P_n)y_n) \in \mathcal{C}_{D,G+F}\}$$

By now we can finally state the basic algorithm.

Algorithm 4.4 Basic Decoding Algorithm

```
procedure Basic Decoding($y$: received word with a maximum of $t$ errors
                         $f_1, f_2, \ldots, f_m$: a basis for $L(F)$,
                         $(H, H')$: parity check matrices for $\mathcal{C}_{D,G}$ and $\mathcal{C}_{D,G+F}$)
    Compute $K_y(F)$
    if $K_y(F) = \{0\}$ then
        return ?
    else
        ▷ Both $f_1, f_2, \ldots, f_m$ and $H'$ are used implicitly to find $\lambda \in K_y(F) \setminus \{0\}$.
        $J \leftarrow \{i \in \{1, \ldots, n\} | \lambda(P_i) = 0\}$ for some $\lambda \in K_y(F) \setminus \{0\}$
        $S \leftarrow \{e \in \mathbb{F}_q^n | He = Hy$ and $e_i = 0$ for all $i \in \{1, \ldots, n\} \setminus J\}$
        if $|S| \neq 1$ then
            return ?
        else
            return $y - e$ where $e$ is the unique solution in $S$.
```

Next we will show that correctness of Algorithm 4.4, we start by proving the following lemma.

Lemma 4.5. *Let $D_e = \sum_{i \in \operatorname{supp}(e)} P_i$. If $t \leq d^* - \deg(F) - 1$, then $K_y(F) = L(F - D_e)$.*

Proof. We start by showing that $K_y(F) \supseteq L(F - D_e)$. So assume that $\lambda \in L(F - D_e)$. Then $\lambda(P_i) = 0$ for all $i \in \operatorname{supp}(e)$, as $\operatorname{supp}(F) \cap \operatorname{supp}(D_e) \subseteq \operatorname{supp}(F) \cap \operatorname{supp}(D) = \emptyset$, hence $\lambda(P_i)y_i = \lambda(P_i)f(P_i)$ for all $i \in \{1, \ldots, n\}$, hence $(\lambda(P_1)y_1, \lambda(P_2)y_2, \ldots, \lambda(P_n)y_n) \in \mathcal{C}_{D,G+F}$ as $\lambda f \in L(G + F)$, by Remark 4.2.

Next we show that $K_y(F) \subseteq L(F - D_e)$. Let $c_y = (\lambda(P_1)y_1, \lambda(P_2)y_2, \ldots \lambda(P_n)y_n) \in \mathcal{C}_{D,G+F}$. Now since $\lambda f \in L(G + F)$, we see that $c_f = (\lambda(P_1)f(P_1), \lambda(P_2)f(P_2), \ldots, \lambda(P_n)f(P_n)) \in \mathcal{C}_{D,G+F}$. Since $\mathcal{C}_{D,G+F}$ is a linear subspace, we see that:

$$c_e = c_y - c_f = (\lambda(P_1)e_1, \lambda(P_2)e_2, \ldots, \lambda(P_n)e_n) \in \mathcal{C}_{D,G+F}$$

additionally we note that $\operatorname{wt}(c_e) \leq \operatorname{wt}(e) \leq t$. Now applying Theorem 3.2(ii) we see that the minimum distance of $\mathcal{C}_{D,G+F}$ is at least $n - \deg(G + F)$. However $\operatorname{wt}(c_e) \leq t \leq d^* - \deg(F) - 1 = n - \deg(G + F) - 1 < n - \deg(G + F)$. Hence $c_e = 0$ and $\lambda(P_i) = 0$ for all $i \in \operatorname{supp}(e)$, so $\lambda \in L(F - D_e)$. ■

By now we are finally able to state and prove the correctness of the basic decoding algorithm.

Theorem 4.6. *Let $\mathcal{C}_L(\mathcal{X}, D, G)$ be a $[n, k, d]$ AG-code with designed minimum distance d^*. Furthermore let F be a divisor on $\mathcal{X}$ such that $\operatorname{supp}(F) \cap \operatorname{supp}(D) = \emptyset$ and $\deg(F) = t + g$ where $t \le \left\lfloor \frac{d^*-1}{2} - \frac{g}{2} \right\rfloor$ and g is the genus of $\mathcal{X}$. Then Algorithm 4.4 is a t-error decoding algorithm for $\mathcal{C}_L(\mathcal{X}, D, G)$. Furthermore if $\deg(F) < n$ then the algorithm returns the good solution in $O(n^\omega)$ operations in $\mathbb{F}_q$ with $\omega \le 3$.*

Proof. **TODO** der er noget iffy med det her bevis. I starten (altså før det med tidskompleksitet). The condition $t \le \left\lfloor \frac{d^*-1}{2} - \frac{g}{2} \right\rfloor$ implies that

$$2t + g \le d^* - 1$$

which in turn implies that $t \le d^* - \deg(F) - 1$, applying Lemma 4.5, we see $K_y(F) = L(F + D_e)$ and in particular that $K_y(F) \neq \{0\}$ as $\ell(F - D_e) > 0$, by Propsition B.1, as $\deg(F) \ge t + g$ implies $\deg(F - D_e) \ge g$ since $\deg(D_e) \le t$. Hence one can take a non-zero rational function $\lambda \in K_y(F)$. Now as $\lambda \in K_y = L(F - D_e)$, we know that $\deg((\lambda)_0) \le \deg(F)$. In addition we noted earlier that $t \le d^* - \deg(F) - 1$, meaning $\deg((\lambda)_0) \le \deg(F) \le d^* - 1 < d^*$. So $|\ker(\lambda)| < d^* < d(C_{D,G})$. Applying Proposition 4.1, we see that there will exist a unique solution to the system: $He = Hy$ and $e_i = 0$ for all $i \in \{1, \ldots, n\}$ such that $\lambda(P_i) \neq 0$.

Next we show that Algorithm 4.4 has time complexity $O(n^\omega)$. We start by noting that solving a linear system such as $He = Hy$ under the constraint that $e_i = 0$ for all $i \in \{1, 2, \ldots, n\} \setminus J$ can be done in $O(n^\omega)$, with $\omega \le 3$ (Should probaly have a source). We will show that finding a non-zero $\lambda \in K_y(F)$, boils down to solving a linear system of similar dimensions. Suppose $\lambda \in L(F)$, we note that $c_\lambda := (\lambda(P_1), \lambda(P_2), \ldots, \lambda(P_n)) * y \in \mathcal{C}_{D,G+F}$ if and only if:

$$0 = H'(c_\lambda * y) = \sum_{j=1}^{n} h'_j (c_\lambda)_j y_j = \underbrace{\begin{bmatrix} h'_1 y_1 & h'_2 y_2 & \cdots & h'_n y_n \end{bmatrix}}_{:=H'_y} c_\lambda$$

Additionally since $\lambda \in L(F)$, there exists some $a_1, a_2, \ldots, a_m \in \mathbb{F}_q$, where $m = \ell(F)$, such that $\lambda = \sum_{i=1}^m a_i f_i$ thus:

$$c_\lambda = \begin{bmatrix} f_1(P_1) & f_2(P_1) & \cdots & f_m(P_1) \\ f_1(P_2) & f_2(P_2) & \cdots & f_m(P_2) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(P_n) & f_2(P_n) & \cdots & f_m(P_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}$$

Hence we can find a non-zero $\lambda \in K_y$ by finding a non-zero solution to:

$$H'_y \begin{bmatrix} f_1(P_1) & f_2(P_1) & \cdots & f_m(P_1) \\ f_1(P_2) & f_2(P_2) & \cdots & f_m(P_2) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(P_n) & f_2(P_n) & \cdots & f_m(P_n) \end{bmatrix} a = 0 \tag{4.2}$$

and setting $\lambda = \sum_{i=1}^m a_i f_i$, since a non-zero solution to Equation (4.2) can be found in $O(\max\{k, m\}^\omega)$. Considering the AG-code $\mathcal{C}_L(\mathcal{X}, D, F)$ applying Theorem 3.2(iii) we see that $\dim_{\mathbb{F}_q}(\mathcal{C}(\mathcal{X}, D, F)) = \ell(F) = m$. Finally since the length of $\mathcal{C}(\mathcal{X}, D, F)$ is n we see that $m < n$ and that a non-zero λ can be found using $O(n^\omega)$ operations. Thus the total time complexity of the basic algorithm is $O(n^\omega)$. ■

4.1 Error Correcting Pairs

In this section we will discuss an generalization of the basic algorithm, to the level of codes. The algorithm is the error correcting pairs algorithm (ECP algorithm). The primary principal of the algorithm is the same (locate the errors, and subsequently correct them using Proposition 4.1). Our treatment will be based on Panaccione (2021)[Subsections 1.6.2 and 1.8.1] as well as Couvreur and Randriambololona (2020)[Subsection 6.1.2].

We start by noting that $\mathbb{F}_q^n$ is the product of n fields, hence it forms a ring, together with element wise addition and multiplication, this motivates the following definition:

Definition 4.7. Let $a, b \in \mathbb{F}_q^n$ then we define the *hadaman* product of a and b as:

$$a * b := (a_1b_1, a_2b_2, \dots, a_nb_n)$$

Additionally if $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$ are linear codes, we define their *hadaman* product as

$$\mathcal{A} * \mathcal{B} := \operatorname{span}_{\mathbb{F}_q} \{a * b | a \in \mathcal{A}, b \in \mathcal{B}\}$$

Remark 4.8. If $a, b, c \in \mathbb{F}_q^n$, then $\langle a * b, c\rangle = \langle a, b * c\rangle = \langle a * c, b\rangle$ where $\langle \cdot, \cdot \rangle$ denotes the canonical inner product in $\mathbb{F}_q^n$.

Lemma 4.9. *Let $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^n$ be linear codes, then $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^\perp$ if and only if $\mathcal{A} * \mathcal{C} \subseteq \mathcal{B}^\perp$.*

Proof. Assume $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^\perp$. Hence if $a \in \mathcal{A}$, $b \in \mathcal{B}$ and $c \in \mathcal{C}$, then $\langle a * b, c\rangle = 0$, the rest follows by combining this with Remark 4.8 which states that $\langle a * b, c\rangle = \langle a * c, b\rangle$. A similar argument can be constructed to show the other implication. ■

We need to introduce some special notation before we can describe the error correcting pairs algorithm.

Definition 4.10. Let $J = \{j_1, j_2, \dots, j_m\} \subseteq \{1, \dots, n\}$ and $x \in \mathbb{F}_q^n$. Then we let x_J denote $(x_{j_1}, x_{j_2}, \dots, x_{j_m})$, that is the projection of x on the coordinates in J and let $Z(x) := \{i \in \{1, \dots, n\} | x_i = 0\}$.
In addition for $A \subseteq \mathbb{F}_q^n$ we define:

(i) $A_J = \{a_J | a \in A\} \subseteq \mathbb{F}_q^{|J|}$ (extracting)

(ii) $A(J) := \{a \in A | a_J = 0\}$ (shortening)

(iii) $Z(A) := \{i \in \{1, \dots, n\} | a_i = 0 \text{ for all } a \in A\}$

Remark 4.11. Let $\mathcal{C}$ be a $[n, k]_q$ code with generator matrix $G \in \mathbb{F}_q^{n \times k}$, then if I is an information set, then $\mathcal{C}_I = \mathbb{F}_q^k$, since $|I| = k$ and G_I is non-singular.

We note that this notation differs from the normal notation used in coding theory. For instance the shortening of set $A \subseteq \mathbb{F}_q^n$ normally referees the set $\{a_I | a \in A(J)\}$ where $I = \{1, 2, \dots, n\} \setminus J$. We use this alternative notation because we want to be able to apply the hadaman product.

Example 4.12. Consider the $[2,2]_3$ code $\mathcal{C}$. With generator matrix: $G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \end{bmatrix}$, Then:

$$\mathcal{C} = \{(0,0),(0,2,1),(0,1,2),(1,2,1),(1,1,2),(2,1,2)\}$$

hence $\mathcal{C}(\{1\}) = \{(0,0,0),(0,2,1),(0,1,2)\}$ while $\mathcal{C}_{\{2,3\}} = \{(0,0),(2,1),(1,2)\}$. □

Definition 4.13. Let $\mathcal{A},\mathcal{B},\mathcal{C} \subseteq \mathbb{F}_q^n$ be linear codes. Then the pair $(\mathcal{A},\mathcal{B})$ is called a *t-error correcting pair* for $\mathcal{C}$ if the following conditions are satisfied:

(ECP1) $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^\perp$

(ECP2) $\dim_{\mathbb{F}_q}(\mathcal{A}) > t$

(ECP3) $d(\mathcal{B}^\perp) > t$

(ECP4) $d(\mathcal{A}) + d(\mathcal{C}) > n$

The definition might seem abstract, however each of the conditions (ECP1)-(ECP4), will be used to prove the correctness of the ECP algorithm. For an overview of the primary roles of each of the conditions, we refer the reader to Table 4.1. Before moving on we will show our first example of a t-error correcting pair.

Example 4.14. Let $\mathcal{C}$ be a $[n,k,n-k+1]_q$ Reed-Solomon code and $t \le \left\lfloor \frac{n-k}{2} \right\rfloor$. In addition let $\mathcal{A}$ be a Reed-Solomon code of dimension $t+1$, and $\mathcal{B}$ the dual code of a Reed-Solomon code of dimension $t+k$. If $\mathcal{A}$, $\mathcal{B}^\perp$ and $\mathcal{C}$ share the same evaluation points, say $P_1, P_2, \dots, P_n$, then $(\mathcal{A},\mathcal{B})$ is a t-error correcting pair for $\mathcal{C}$. We start by showing condition (ECP1). Suppose $a \in \mathcal{A}$ and $c \in \mathcal{C}$, then $a = (F(P_1), F(P_2), \dots, F(P_n))$ for some $F \in \mathbb{F}_q[X]_{<t+1}$ and $c = (g(P_1), g(P_2), \dots, g(P_n))$ for some $G \in \mathbb{F}_q[X]_{<k}$. We see that:

$$a * c = (FG(p_1), FG(p_2), \dots, FG(p_n)) \in \mathcal{B}^\perp$$

as $\deg(FG) < k+t$, since $\deg(F) < t+1$ and $\deg(G) < k$. The rest follows by applying Lemma 4.9. Condition (ECP2) is clearly meet, since $\dim_{\mathbb{F}_q}(\mathcal{A}) = t+1$ by our construction, and condition (ECP3) follows as $d(\mathcal{B}^\perp) = n-(t+k)+1 \ge n - \frac{n-k}{2} - k + 1 = \frac{n-k}{2} + 1 > t$. Finally:

$$\begin{aligned} d(\mathcal{A}) + d(\mathcal{C}) &= (n-(t+1)+1) + (n-k+1) \\ &\ge 2n-k+2-\frac{n-k}{2} = \frac{2n+(n-k+1)+3}{2} > n + \frac{3}{2} > n \end{aligned}$$

since $0 < d(\mathcal{C}) = n-k+1$, which shows that (ECP4) is satisfied. □

We can now describe the ECP algorithm. We fix $y := c+e$ such that $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$ with $\mathrm{wt}(e) \le t$ for the rest of the section. Just like in the basic algorithm, the ECP algorithm consists of two steps: First we locate the errors by finding a subset $J \subseteq \{1,\dots,n\}$ such that $\mathrm{supp}(e) \subseteq J$, secondly we apply Proposition 4.1, to find e, if possible.

One of the main ideas is to investigate the space:

$$\{a \in \mathcal{A} | a * e = 0\} = \mathcal{A}(\mathrm{supp}(e))$$

the equality follows as $a * e = 0$ if and only if $a_i = 0$ for all $i \in \mathrm{supp}(e)$. This vector space consists of vectors whose entries indexed by $\mathrm{supp}(e)$ are all 0, hence they can be used to locate the errors. Thus we want $\mathcal{A}(\mathrm{supp}(e))$ to contain at least one non-zero vector, which we can use to locate the errors.

Lemma 4.15. *Let $(\mathcal{A}, \mathcal{B})$ be a t-error correcting pair for $\mathcal{C}$ and $y = c + e$ with $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$ with* $\operatorname{wt}(e) \leq t$. *Then:*

$$\mathcal{A}(\operatorname{supp}(e)) \neq \{0\}$$

Proof. Let $m = \dim_{\mathbb{F}_q}(\mathcal{A})$ and $a_1, a_2, \ldots, a_m \in \mathbb{F}_q^n$ form a basis of $\mathcal{A}$. Consider the vectors $a_1 * e, a_2 * e, \ldots, a_m * e$, then $\operatorname{wt}(a_i * e) \leq t$ as $\operatorname{wt}(e) \leq t$. Now since $\operatorname{supp}(a_i * e) \subseteq \operatorname{supp}(e)$ and $|\operatorname{supp}(e)| = \operatorname{wt}(e) \leq t < m$, by (ECP2). Using this information we can conclude that the vectors $a_1 * e, a_2 * e, \ldots, a_m * e$ are $\mathbb{F}_q$-linearly dependent, thus the equation:

$$\sum_{i=1}^{m} x_i(a_i * e) = 0$$

has no unique solution, where $x \in \mathbb{F}_q^m$, meaning multiple $a \in \mathcal{A}$ exists such that $a * e = 0$. ■

This is all quite theoretical, since e and in particular $\operatorname{supp}(e)$ is unknown in practical applications, we do not have any information about $A(\operatorname{supp}(e))$. Instead we consider the following vector space:

Definition 4.16. Let $(\mathcal{A}, \mathcal{B})$ be a t-error correcting pair for $\mathcal{C}$, and $y = c + e$, with $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$ such that $\operatorname{wt}(e) \leq t$. Then we define:

$$M_{ECP} := \left\{ a \in \mathcal{A} \middle| a * y \in \mathcal{B}^{\perp} \right\}$$

The vector space M_{ECP} will play a similar role, in the ECP algorithm, to the role of the set $K_y(F)$ in the basic algorithm.

Theorem 4.17. *Let $(\mathcal{A}, \mathcal{B})$ be a t-error correcting pair for $\mathcal{C}$. Furthermore let $y = c + e$ with $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$ with* $\operatorname{wt}(e) \leq t$. *Then:*

(i) $\mathcal{A}(\operatorname{supp}(e)) \subseteq M_{ECP} \subseteq \mathcal{A}$.

(ii) *If $d(\mathcal{B}^{\perp}) > t$, then* $\mathcal{A}(\operatorname{supp}(e)) = M_{ECP}$.

Proof. We start by proving Assertion (i), the inclusion $M_{ECP} \subseteq \mathcal{A}$ follows straight away from the definition of M_{ECP}. Next assume that $a \in \mathcal{A}(\operatorname{supp}(e))$, then for all $b \in \mathcal{B}$ we have:

$$\langle a * y, b \rangle \overset{(a)}{=} \langle a * c, b \rangle + \langle a * e, b \rangle \overset{(b)}{=} \langle a * b, c \rangle + \langle a * e, b \rangle \overset{(c)}{=} 0 \tag{4.3}$$

where (a) follows since $\langle \cdot, \cdot \rangle$ is linear in the first argument, (b) follows by Remark 4.8 and (c) as $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^{\perp}$, by (ECP1) and $a * e = 0$. From Equation (4.3) we see that $a * y \in \mathcal{B}^{\perp}$ and hence $\mathcal{A}(\operatorname{supp}(e)) \subseteq M_{ECP}$.
Continuing with Assertion (ii). We only need to prove that $A(\operatorname{supp}(e)) \supseteq M_{ECP}$. Hence let $a \in M_{ECP}$, then $a*y = a*c + a*e$, so $a*e = a*y - a*c \in \mathcal{B}^{\perp}$, since $a*y \in \mathcal{B}^{\perp}$ by definition and $\mathcal{A} * \mathcal{C} \subseteq \mathcal{B}^{\perp}$ by Lemma 4.9 and (ECP1). Finally $\operatorname{wt}(a * e) \leq \operatorname{wt}(e) \leq t < d(\mathcal{B}^{\perp})$, by (ECP3), so $a * e = 0$, meaning $a \in \mathcal{A}(\operatorname{supp}(e))$. ■

Lemma 4.18. *Let $(\mathcal{A}, \mathcal{B})$ be a t-error correcting pair for the linear code $\mathcal{C}$, and $y = c + e$ with $c \in \mathcal{C}$ and $e \in \mathbb{F}_q^n$ such that* $\operatorname{wt}(e) \leq t$. *Then $|Z(M_{ECP})| \leq d(\mathcal{C})$.*

Proof. By Theorem 4.17(i) and Lemma 4.15 there exists a $a \in \mathcal{A}(\text{supp}(e)) \setminus \{0\} \subseteq M_{ECP}$. Since $Z(M_{ECP}) \subseteq Z(a)$ we get that:

$$|Z(M_{ECP})| \leq |Z(a)| = n - \text{wt}(a) \leq n - d(\mathcal{A}) \leq d(\mathcal{C})$$

by (ECP4). ■

This means that we can apply Proposition 4.1, to find the error e. This was the final piece of the puzzle, so we can now describe the ECP decoding algorithm.

Algorithm 4.19 Error Correcting Pairs Decoding Algorithm

```
procedure ECP DECODING($y$: a received word with a maximum of $t$ errors,
                        $(\mathcal{A}, \mathcal{B})$: a $t$-error correcting pair for $\mathcal{C}$,
                        $H$: a parity check matrix for $\mathcal{C}$)
    $M_{ECP} \leftarrow \{a \in \mathcal{A} | a * y \in \mathcal{B}^{\perp}\}$
    $I \leftarrow Z(M_{ECP})$
    $S \leftarrow \{e \in \mathbb{F}_q^n | He = Hy$ and $e_i = 0$ for all $i \in \{1, \ldots, n\} \setminus I\}$
    if $|S| \neq 1$ then
        return ?
    else
        return $y - e$ where $e$ is the unique solution in $S$.
```

Remark 4.20. The time complexity of Algorithm 4.19, is also $O(n^{\omega})$ with $\omega \leq 3$. This is can be seen as follows: The set S is simply a solution set to a linear system, hence it can be computed in $O(n^{\omega})$. Additionally computing M_{ECP} can be done in $O(n^{\omega})$ assuming we have a generator matrices $G_{\mathcal{A}}$ and $G_{\mathcal{B}}$ of $\mathcal{A}$ and $\mathcal{B}$ respectively. Then M_{ECP} is nothing but the solution space to the equation:

$$G_{\mathcal{B}}(y^T * a^T) = 0 \tag{4.4}$$

Using $G'_{\mathcal{B}} := \begin{bmatrix} G'_{\mathcal{B}_{*,1}} y_1 & G'_{\mathcal{B}_{*,2}} y_2 & \cdot & G'_{\mathcal{B}_{*,n}} y_n \end{bmatrix}$ we may rewrite Equation (4.4) as $G'_{\mathcal{B}} a = 0$. Additionally we may substitue a with $x^T G_{\mathcal{A}}$ and solve for x instead, since $a \in \mathcal{A}$. Then we obtain

$$G'_{\mathcal{B}}(x^T G_{\mathcal{A}})^T = 0 \iff (G'_{\mathcal{B}} G_{\mathcal{A}}^T) x = 0$$

solving this equation for x we get a solution in parametric form. Say $x = v_0 + \sum_{i=1}^{m} c_i v_i$ with $v_i \in \mathbb{F}_q^k$ fixed and c_i arbitrary. Thus:

$$M_{ECP} = \left\{ \left(v_0^T + \sum_{i=1}^{m} c_i v_i^T \right) G_{\mathcal{A}} \middle| c_1, c_2, \ldots, c_m \in \mathbb{F}_q \right\} \tag{4.5}$$

TODO when is $a_i = 0$ for all $a \in M_{ECP}$.

Below in Table 4.1, the role of each ECP condition, is briefly explained, we note that there is a natural overlap, between the roles of some the conditions.

Condition	**Role in the ECP algorithm**
(ECP1)	Use to ensure $A(\text{supp}(e)) \subseteq M_{ECP}$ and that $\mathcal{A}(\text{supp}(e)) = M_{ECP}$.
(ECP2)	Ensures that $A(\text{supp}(e)) \neq \{0\}$ and $M_{ECP} \neq \{0\}$.
(ECP3)	Ensures that $A(\text{supp}(e)) = M_{ECP}$.
(ECP4)	Ensures that $|Z(M_{ECP})| \leq d(\mathcal{C})$, thus Proposition 4.1 can be applied.

Table 4.1: *The roles of each ECP condition.*

Finally to apply the theory of t-error correcting pairs to AG codes we a way to find a t-error correcting pair for a given AG code, luckily the next theorem provides exactly this. In addition it is a "natural" generalization of the approach taken in Example 4.14.

Theorem 4.21. *Let $\mathcal{X}$ be a regular absolutely projective algebraic curve of genus g over $\mathbb{F}_q$, and $\mathcal{C}_{D,G}$ be an AG code, constructed on $\mathcal{X}$, with $D = \sum_{i=1}^{n} P_i$. Let $t \leq \lfloor \frac{d^*-1}{2} - \frac{g}{2} \rfloor$ and let F be a divisor on $\mathcal{X}$ such that* $\operatorname{supp}(F) \cap \operatorname{supp}(D) = \emptyset$ *and* $\deg(F) = t + g$ *as well as* $\deg(F+G) < n$. *Then $(\mathcal{C}_{D,F}, \mathcal{C}_{D,F+G}^{\perp})$ forms a t-error correcting pair for $\mathcal{C}_{D,G}$.*

Proof. For the sake of simplicity we let $\mathcal{A} := \mathcal{C}_{D,F}$ and $\mathcal{B} := \mathcal{C}_{D,F+G}^{\perp}$ We start by showing that (ECP1) holds. Let $a \in \mathcal{C}_{D,F} = \mathcal{A}$ and $c \in \mathcal{C}_{D,G}$ then there exists some $f \in L(F)$ and $h \in L(G)$ such that $a = (f(P_1), f(P_2), \ldots, f(P_n))$ and $c = (h(P_1), h(P_2), \ldots, h(P_n)) \in L(G)$. using this information we see that:

$$a * c = (fh(P_1), fh(P_2), \ldots, fh(P_n)) \in \mathcal{C}_{D,F+G}$$

since $L(F)L(G) \subseteq L(F+G)$ by Remark 4.2. Thus:

$$\mathcal{A} * \mathcal{C}_{D,F} = \mathcal{C}_{D,F} * \mathcal{C}_{D,G} \subseteq C_{D,F+G} = \mathcal{B}^{\perp}$$

Continuing using $\deg(F) < \deg(F+G) < n$, since $\operatorname{supp}(F) \cap \operatorname{supp}(G) = \emptyset$, we see that:

$$\dim_{\mathbb{F}_q}(\mathcal{A}) \overset{(a)}{=} \ell(F) \overset{(b)}{\geq} \deg(F) - g + 1 = t + g - g + 1 = t + 1$$

where (a) follows by Theorem 3.2(iii) and (b) by the Riemann-Roch Theorem B.2. This shows that $\mathcal{A}$ satisfies (ECP2). Combining Theorem 3.2(ii) and the fact that $\deg(G+F) = \deg(G) + t + g$ yields (ECP3). This is seen as follows:

$$\begin{aligned} d(\mathcal{B}^{\perp}) \geq n - \deg(G+F) &= n - \deg(G) - t - g \\ &\overset{(c)}{\geq} n - \deg(G) - \frac{n - \deg(G) - g - 1}{2} - g \\ &= \frac{n - \deg(G) - g - 1}{2} \overset{(d)}{\geq} t \end{aligned}$$

where (c) and (d) follows as $t \leq \left\lfloor \frac{d^*-g-1}{2} \right\rfloor$ with $d^* = n - \deg(G)$. Finally we need to verify that (ECP4) holds. By applying Theorem 3.2(ii) we see that:

$$d(\mathcal{A}) + d(\mathcal{C}_{D,G}) > n - \deg(F) + n - \deg(G) = \deg(F+G) > n$$

by our original assumption. ■

4.2 Error Correcting Arrays

As we have seen previously both the basic algorithm described in Algorithm 4.4 and the error correcting pairs algorithm described in Algorithm 4.19, suffers under a genus penalty, meaning they can correct up to:

$$\left\lfloor \frac{d^*-1}{2} - \frac{g}{2} \right\rfloor$$

where d^* is the designed minimum distance of $\mathcal{C}_L(\mathcal{X}, D, G)$ and g is the genus of $\mathcal{X}$. This isn't a problem when $g = 0$, which is the case when $\mathcal{X} = \mathbb{P}^1$ (atleast in the planar case.).

5 Classical Goppa Codes

Next we introduce classical Goppa codes. The original proposal of McElice used these codes in its construction. In addition they remain as one of the few classes codes proposed for with no publicly known structural attacks, at least if they are chosen correctly.

Theorem 5.1. *Let $f \in \mathbb{F}_q[X]$ and $\alpha \in \mathbb{F}_q$ such that $f(\alpha) \neq 0$, then the inverse of $(X - \alpha)$ exists in the quotient ring $\frac{\mathbb{F}_q[X]}{\langle f \rangle}$, and may be computed as $-\left(\frac{f(X)-f(\alpha)}{X-\alpha}\right) f(\alpha)^{-1}$.*

Proof. Follows from the fact that:

$$\begin{aligned} -\left(\frac{f(X)-f(\alpha)}{X-\alpha}\right) f(\alpha)^{-1}(X-\alpha) &= -f(\alpha)^{-1}(f(X)-f(\alpha)) \\ &= -f(\alpha)^{-1}f(X) + 1 \equiv 1 \mod f \end{aligned}$$

Which is equivalent with $-\left(\frac{f(X)-f(\alpha)}{X-\alpha}\right) f(\alpha)^{-1}(X-\alpha) = 1 \in \frac{\mathbb{F}_q[X]}{\langle f \rangle}$. ■

Definition 5.2. Let $x \in \mathbb{F}_q^n$ and $f \in \mathbb{F}_q[X]$ such that $f(x_i) \neq 0$ for $i = 1, 2, \ldots, n$ and $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$ be a subfield, then the *classical Goppa code* associated with $(x, f, \mathbb{F}_{q_0})$ is defined as:

$$\begin{aligned} \Gamma(x, f, \mathbb{F}_{q_0}) :&= \left\{ c \in \mathbb{F}_{q_0}^n \;\middle|\; \sum_{i=1}^{n} \frac{c_i}{X - x_i} \equiv 0 \mod f \right\} \\ &= \left\{ c \in \mathbb{F}_{q_0}^n \;\middle|\; \sum_{i=1}^{n} \frac{c_i}{X - x_i} = 0 \in \frac{\mathbb{F}_q[X]}{\langle f \rangle} \right\} \end{aligned}$$

If f is irreducible, then $\Gamma(x, f, \mathbb{F}_{q_0})$ is also called irreducible.

Remark 5.3. If f is irreducible and $\deg(f) = l$, then $\mathbb{F}_q[X]/\langle f \rangle$ is a finite field with q^l elements.

We note that $\Gamma(x, f, \mathbb{F}_{q_0})$ does indeed form a linear subspace of $\mathbb{F}_{q_0}^n$ since: If $c, c' \in \Gamma(x, f, \mathbb{F}_{q_0})$, we will show that this implies that $c + c' = \left[c_1 + c_1', c_2 + c_2', \ldots, c_n + c_n'\right] \in \Gamma(x, f, \mathbb{F}_{q_0})$. This follows since:

$$\sum_{i=1}^{n} \frac{c_i + c_i'}{X - x_i} = \sum_{i=1}^{n} \frac{c_i}{X - x_i} + \sum_{i=1}^{n} \frac{c_i'}{X - x_i} \equiv 0 \mod f$$

Additionally if $c \in \Gamma(x, f, \mathbb{F}_{q_0})$, then $kc \in \Gamma(x, f, \mathbb{F}_{q_0})$ for all $k \in \mathbb{F}_{q_0}$, since:

$$\sum_{i=1}^{n} \frac{kc_i}{X - x_i} = k \sum_{i=1}^{n} \frac{c_i}{X - x_i} \equiv 0 \mod f$$

From Theorem 5.1 and Definition 5.2 it follows that $c = (c_1, c_2, \ldots, c_n) \in \Gamma(x, f, \mathbb{F}_{q0})$ if and only if

$$-\sum_{i=1}^{n} c_i \frac{1}{f(x_i)} \frac{f(X) - f(x_i)}{X - x_i} = 0 \in \frac{\mathbb{F}_q[X]}{\langle f \rangle} \tag{5.1}$$

additionally if $f = \sum_{j=0}^{\deg(f)} a_j X^j$, then:

$$\begin{aligned} -\frac{1}{f(x_i)} \frac{f(X) - f(x_i)}{X - x_i} &= -\frac{1}{f(x_i)} \frac{\sum_{j=0}^{\deg(f)} a_j (X^j - x_i^j)}{X - x_i} \\ &\overset{(a)}{=} -\frac{1}{f(x_i)} \sum_{j=1}^{\deg(f)} a_j \sum_{k=0}^{j-1} X^k x_i^{j-1-k} \\ &\overset{(b)}{=} -\frac{1}{f(x_i)} \sum_{k=0}^{\deg(f)-1} X^k \left(\sum_{j=k+1}^{\deg(f)} a_j x_i^{j-1-k} \right) \end{aligned}$$

where (a) follows by polynomial division and (b) from interchanging the sums. Thus:

$$\sum_{i=1}^{n} \frac{c_i}{X - x_i} = -\sum_{i=1}^{n} \frac{c_i}{f(x_i)} \sum_{k=0}^{\deg(f)-1} X^k \sum_{j=k+1}^{\deg(f)} a_j x_i^{j-1-k} \tag{5.2}$$

Equation (5.2) must equal 0 since $c \in \Gamma(x, f, \mathbb{F}_{q0})$ which is the case if and only if the coefficients of each X^k is zero, which yields the following proposition:

Proposition 5.4. *Let $x \in \mathbb{F}_q^n$ and $f \in \mathbb{F}_q[X]$ with $l := \deg(f)$, then the classical gopppa code $\Gamma(x, f, \mathbb{F}_{q0})$ has parity check matrix:*

$$H = \begin{bmatrix} f(x_1)^{-1} a_l & f(x_2)^{-1} a_l & \cdots & f(x_n)^{-1} a_l \\ f(x_1)^{-1}(a_l + a_{l-1} x_1) & f(x_2)^{-1}(a_l + a_{l-1} x_2) & \cdots & f(x_n)^{-1}(a_l + a_{l-1} x_n) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_1)^{-1} \sum_{j=1}^{l} a_j x_1^{j-1} & f(x_2)^{-1} \sum_{j=1}^{l} a_j x_2^{j-1} & \cdots & f(x_n)^{-1} \sum_{j=1}^{l} a_j x_n^{j-1} \end{bmatrix}$$

over $\mathbb{F}_q$.

The following Corollary uses some elementary results from Galois theory, namely that if $\mathbb{F}_{q0}$ is a subfield of the finite field $\mathbb{F}_q$, then there exists a $\mathbb{F}_{q0}$-basis of $\mathbb{F}_q$. We will denote the length of such a basis by $[\mathbb{F}_q : \mathbb{F}_{q0}]$ an call it the *degree* of the field extension $\mathbb{F}_q/\mathbb{F}_{q0}$. Could be proven in an appendix.

Corollary 5.5. *Let $\Gamma(x, f, \mathbb{F}_{q0})$ be a classical goppa code with $x \in \mathbb{F}_q$ and $f \in \mathbb{F}_q[X]$ then:*

$$\dim_{\mathbb{F}_{q0}}(\Gamma(x, f, \mathbb{F}_{q0})) \geq n - m \deg(f)$$

where $m = [\mathbb{F}_q : \mathbb{F}_{q0}]$.

Proof. Fixing a $\mathbb{F}_{q0}$-basis of $\mathbb{F}_q$ say $b_1, b_2, \ldots, b_m \in \mathbb{F}_q$, each entry in H can be viewed as a vector in $\mathbb{F}_{q0}^m$, by the vector space isomorphism:

$$\mathbb{F}_q \ni x = x_1 b_1 + x_2 b_2 + \cdots + x_m b_m \mapsto \begin{bmatrix} x_1 & x_2 & \cdots & x_m \end{bmatrix}^T \in \mathbb{F}_{q0}^m$$

Thus H from Proposition 5.4 can be viewed as a $\mathbb{F}_{q0}$-matrix H' with dimensions $m \deg(f) \times n$. Since H' has mt rows, we see that $\operatorname{rank}(H') \leq m \deg(f)$, hence

$$\dim_{\mathbb{F}_{q0}}(\Gamma(x, f, \mathbb{F}_{q0})) = \dim_{\mathbb{F}_{q0}}(\operatorname{null}(H')) = n - \operatorname{rank}(H') \geq n - m \deg(f) \qquad \blacksquare$$

Example 5.6. Let $\mathbb{F}_4$ be the finite field with the four elements $0, 1, \alpha, 1+\alpha$ where $\alpha^2 = 1+\alpha$ and $x + x = 0$ for all $x \in \mathbb{F}_4$. We will let $f(X) = \alpha X^2 + X + (1+\alpha) \in \mathbb{F}_4[X]$ and $x = \begin{bmatrix} 0 & \alpha & 1+\alpha \end{bmatrix}$. We see that $f(x_1) = 1+\alpha$, $f(x_2) = \alpha$ while $f(x_3) = 1$. Next we will consider the Goppa code $\Gamma(x, f, \mathbb{F}_4)$. Applying proposition 5.4 to get a parity check matrix H, for $\Gamma(x, f, \mathbb{F}_4)$ we get:

$$H = \begin{bmatrix} 0 & 0 & 0 \\ (1+\alpha) & 1 & \alpha \\ (1+\alpha) & 0 & 1 \end{bmatrix}$$

Next we solve the linear system $Hc = 0$ to find the codewords of $\Gamma(x, f, \mathbb{F}_4)$, we start by noting that the augmented matrix $\begin{bmatrix} H | 0 \end{bmatrix}$ is row equivilent with:

$$\begin{bmatrix} 1 & 0 & \alpha & 0 \\ 0 & 1 & (1+\alpha) & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Thus:

$$c = c_3 \begin{bmatrix} \alpha \\ (1+\alpha) \\ 1 \end{bmatrix} \iff c \in \Gamma(x, f, \mathbb{F}_4)$$

for all $c_3 \in \mathbb{F}_4$. Hence $\Gamma(x, f, \mathbb{F}_4) = \{(0,0,0), (\alpha, 1+\alpha, 1), (1+\alpha, 1, \alpha), (1, \alpha, 1+\alpha)\}$. Furthermore we note that $\Gamma(x, f, \mathbb{F}_4)$ is a $[3,1,3]_4$ code, meaning $\Gamma(x, f, \mathbb{F}_4)$ MDS code. □

Finally we reach the main theorem of this chapter.

Theorem 5.7. *Let $\Gamma(x, f, \mathbb{F}_q)$ be a classical Goppa code, $P_i = (x_i : 1)$ for $i = 1, 2, \ldots, n$ and $D = \sum_{i=1}^{n} P_i$. Then:*

$$\Gamma(x, f, \mathbb{F}_q) = \mathcal{C}_\Omega(\mathbb{P}^1, D, (f)_0 - P_\infty) = \mathcal{C}_L(\mathbb{P}^1, D, (\omega) + D - (f_0) + P_\infty) \tag{5.3}$$

with $\omega := \frac{dh}{h}$ where $h(x) := \prod_{i=1}^{n}(x - x_i)$.

Proof. The last equality in Equation (5.3) follows by Theorem 3.16. Hence it will be sufficient to show the first equality. We start by showing that $\Gamma(x, f, \mathbb{F}_q) \subseteq \mathcal{C}_\Omega(\mathbb{P}^1, D, (f)_0 - P_\infty)$. Hence let $c \in \Gamma(x, f, \mathbb{F}_q)$ and

$$\omega_c := \left(\sum_{i=1}^{n} \frac{c_i}{x - x_i} \right) dx$$

We note that x is a local parameter at all of the P_i's. By the definition of $\Gamma(x, f, \mathbb{F}_q)$ we see that the ω_c vanishes at all $P \in \operatorname{supp}((f)_0)$, meaning $v_P(\omega_c) > 0$, afterall $\sum_{i=1}^{n} \frac{c_i}{x - x_i} \equiv 0 \mod f$. In addition we note that $v_{P_i}(\omega_c) = -1$ and ω_c is regular at any other point $\mathbb{P}^1 \setminus \{P_\infty\}$. Finally we compute $v_{P_\infty}(\omega_c)$ by substituting x with $1/u$, we see that:

$$\omega_c \overset{(a)}{=} \sum_{i=1}^{n} \frac{-c_i \frac{du}{u^2}}{\frac{1}{u} - x_i} = -\sum_{i=1}^{n} \frac{c_i du}{u(1 - x_i u)} \tag{5.4}$$

where (a) follows since Remark 3.4 implies:

$$0 = D\left(\frac{1}{u}u\right) = D(u)\frac{1}{u} + uD\left(\frac{1}{u}\right)$$

which in turn impleis that $D\left(\frac{1}{u}\right) = -\frac{1}{u^2}D(u)$ for all derivations $D : \mathbb{F}(\mathcal{X}) \to \mathbb{F}(\mathcal{X})$. Thus by Equation (5.4) $v_{P_\infty}(\omega_c) \geq -1$ and hence $\omega_c \in \Omega((f)_0 - P_\infty - D)$ meaning $\Gamma(x, f, \mathbb{F}_q) \subseteq \mathcal{C}_\Omega(\mathbb{P}^1, D, (f)_0 - P_\infty)$. Conversely, given $\omega \in \Omega((f)_0 - P_\infty - D)$ we want to show that the codeword $c = (\mathrm{Res}_{P_1}(\omega), \mathrm{Res}_{P_2}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega))$ is in $\Gamma(x, f, \mathbb{F}_q)$. Consider the differential:

$$\eta = \sum_{i=1}^{n} \frac{\mathrm{Res}_{P_i}(\omega)dx}{x - x_i}$$

Using the same argument as previously we see that the poles of η are contained in $\{P_1, P_2, \ldots, P_n, P_\infty\}$. We also note that $\mathrm{Res}_{P_i}(\eta) = \mathrm{Res}_{P_i}(\omega)$ for $i = 1, 2, \ldots, n$. Hence by the Residue Theorem 3.19 we see that $\mathrm{Res}_{P_\infty}(\eta) = \mathrm{Res}_{P_\infty}(\omega)$ since the residues of differentials at regular points are 0. Thus the differential $\eta - \omega$ has no poles on $\mathbb{P}^1$, all the residues are zero afterall. However the degree of a non-zero canonical divisor is $2g - 2 = -2$ by Proposition 3.12, as the genus of $\mathbb{P}^1$ is zero. Thus $\eta - \omega = 0$ meaning $\eta = \omega$ and thus $\sum_{i=1}^{n} \frac{\mathrm{Res}_{P_i}(\omega)}{x - x_i}$ vanishes on $(f)_0$, since $\eta = \omega \in \Omega((f)_0 - P_\infty - D)$. Moreover $\sum_{i=1}^{n} \frac{\mathrm{Res}_{P_i}(\omega)}{x - x_i}$ vanishing on $(f)_0$ is equivilent with:

$$\sum_{i=1}^{n} \frac{\mathrm{Res}_{P_i}(\omega)}{x - x_i} \equiv 0 \mod f$$

meaning $c \in \Gamma(x, f, \mathbb{F}_q)$. Since c was chosen arbitrarily, this shows that $\mathcal{C}_\Omega(\mathbb{P}^1, D, (f)_0 - P_\infty) \subseteq \Gamma(x, f, \mathbb{F}_q)$ concluding the proof. ■

Since Theorem 5.7 shows that classical Goppa codes are in fact AG codes it makes sense to speak about their designed minimum distance. This leads us to the following corollary:

Corollary 5.8. *If $f \in \mathbb{F}_q[X]$ splits into linear factors over $\mathbb{F}_q$, then:*

$$d^* \left(\Gamma(f, x, \mathbb{F}_q)\right) = \deg(f) + 1$$

Proof. From Corollary 3.17 it follows that the designed minimum distance of $\Gamma(f, x, \mathbb{F}_q)$ is $\deg((f)_0 - P_\infty) = \deg(f) - 1 + 2 = \deg(f) + 1$ ■

5.1 Subfield Subcodes

The following section is concerned with what happends if we only consider the codewords, of a linear code over $\mathbb{F}_q$, with entries in a subfield of $\mathbb{F}_q$. We start by motivating the concept by the following proposition:

Proposition 5.9. *Let $x \in \mathbb{F}_q^n$ and $f \in \mathbb{F}_q[X]$, such that $f(x_i) \neq 0$ for $i = 1, 2, \ldots, n$. Suppose $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$ then:*

$$\Gamma(x, f, \mathbb{F}_{q_0}) = \Gamma(x, f, \mathbb{F}_q) \cap \mathbb{F}_{q_0}^n$$

Proof. Follows straight from the definition, namely:

$$\begin{aligned}\Gamma(x, f, \mathbb{F}_{q_0}) &= \left\{ c \in \mathbb{F}_{q_0}^n \,\middle|\, \sum_{i=1}^{n} \frac{c_i}{X - x_i} \equiv 0 \mod f \right\} \\ &= \left\{ c \in \mathbb{F}_q^n \,\middle|\, \sum_{i=1}^{n} \frac{c_i}{X - x_i} \equiv 0 \mod f \right\} \cap \mathbb{F}_{q_0}^n = \Gamma(x, f, \mathbb{F}_q) \cap \mathbb{F}_{q_0}^n \end{aligned}$$ ■

We generalize the concept described in Proposition 5.9, with the following definition.

> **Definition 5.10.** Let $\mathcal{C}$ be a $\mathbb{F}_q$ linear code and $\mathbb{F}_{q_0}$ be a subfield of $\mathbb{F}_q$, then the $\mathbb{F}_{q_0}$ linear code:
> $$\mathcal{C}|_{\mathbb{F}_{q_0}} := \mathcal{C} \cap \mathbb{F}_{q_0}^n$$
> is called a *subfield subcode* of $\mathcal{C}$.

Let $c_1, c_2 \in \mathcal{C}|_{\mathbb{F}_{q_0}}$, then $c_1 + c_2 \in \mathcal{C}|_{\mathbb{F}_{q_0}}$, since they are both in $\mathcal{C}$ and $\mathbb{F}_{q_0}^n$. Additionally $c \in \mathcal{C}|_{\mathbb{F}_{q_0}}$ implies that $kc \in \mathcal{C}|_{\mathbb{F}_{q_0}}$ for all $k \in \mathbb{F}_{q_0}$, since $kc \in \mathcal{C}$ and $kc \in \mathbb{F}_{q_0}^n$. Hence $\mathcal{C}|_{\mathbb{F}_{q_0}}$ is a $\mathbb{F}_{q_0}$ linear code.

Proposition 5.11. *If $\mathcal{C}$ is a $\mathbb{F}_q$ linear code and $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$, then $d(\mathcal{C}) \leq d(\mathcal{C}|_{\mathbb{F}_{q_0}})$.*

Proof. We have $d(\mathcal{C}) = \min_{c\in\mathcal{C}} \mathrm{wt}(c) \leq \min_{c\in\mathcal{C}|_{\mathbb{F}_{q_0}}} \mathrm{wt}(c) = d(\mathcal{C}|_{\mathbb{F}_{q_0}})$ since $\mathcal{C}|_{\mathbb{F}_{q_0}} \subseteq \mathcal{C}$. ■

If $\mathcal{C}$ is a $[n,k]_q$ code we generally do not have $d(\mathcal{C}) = d(\mathcal{C}|_{\mathbb{F}_{q_0}})$, where $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$. This is illustrated with the following example.

Example 5.12. We once again consider the finite field $\mathbb{F}_4$. Consider the $[3,2]_4$ linear code $\mathcal{C}$ with generator matrix:

$$G = \begin{bmatrix} \alpha & 0 & 1+\alpha \\ 1 & 1 & 1 \end{bmatrix}$$

We will show that $\mathcal{C}|_{\mathbb{F}_2}$ is nothing but the $[3,1]_2$ repetition code. Hence we assume that $c \in \mathcal{C}|_{\mathbb{F}_2}$, then

$$c = x_1 G_{*,1} + x_2 G_{*,2} \tag{5.5}$$

for some $x \in \mathbb{F}_4$. Notice that since $c_2 \in \mathbb{F}_2$ we must have $x_2 \in \mathbb{F}_2$, as $G_{0,1} = 0$ and $G_{0,2} = 1$. We will show that we must have $x_1 = 0$. Combining the $x_1 G_{*,1} = \begin{bmatrix} x_1\alpha & 0 & x_1 + \alpha x_1 \end{bmatrix}$ with Equation 5.5 we get that we must have:

$$x_1 + x_2 \in \mathbb{F}_2 \text{ and } (x_1 + \alpha x_1) + x_2 \in \mathbb{F}_2$$

The condition that $x_1 + x_2 \in \mathbb{F}_2$ yields that $x_1 \in \mathbb{F}_2$, since if $x_2 = 1$, then $1 + x_1 \in \mathbb{F}_2$ if and only if $x_1 \in \mathbb{F}_2$ as $1+\alpha \notin \mathbb{F}_2$ and $1 + (1+\alpha) = \alpha \notin \mathbb{F}_2$. Additionally the condition that $(x_1 + \alpha x_1) + x_2 \in \mathbb{F}_2$ implies that $x_1 = 0$, since $x_1 = 1$ gives $1 + \alpha + x_2 \in \mathbb{F}_2$ which would imply that $x_2 \in \{\alpha, 1+\alpha\}$. Hence $\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ is a generator matrix for $\mathcal{C}|_{\mathbb{F}_2}$. Meaning $\mathcal{C}|_{\mathbb{F}_2}$ is nothing but the $[3,1]_2$ repetition code. Hence $d(\mathcal{C}|_{\mathbb{F}_2}) = 3$ however $d(\mathcal{C}) = \min\{\mathrm{wt}(c) | c \in \mathcal{C} \setminus \{0\}\} \leq 2$ since $\mathrm{wt}(G_{*,1}) = 2$. □

Remark 5.13. If we have a t-error correcting decoder for $\mathcal{C}$, then we may apply it on $\mathcal{C}|_{\mathbb{F}_{q_0}}$, however we might have $d(\mathcal{C}|_{\mathbb{F}_{q_0}}) > d(\mathcal{C})$, confer Example 5.12. Hence there might exist a decoding algorithm with a higher error correcting radius.

Theorem 5.14. *Let $x \in \mathbb{F}_q^n$ and $f \in \mathbb{F}_q[X]$ such that $f(x_i) \neq 0$ for all $i = 1, 2, \ldots, n$. Let $\mathbb{F}_{q_0}$ be a subfield of $\mathbb{F}_q$ then:*

(i) *The minimum distance of $\Gamma(x, f, \mathbb{F}_{q_0})$ atleast* $\deg(f) + 1$.

(ii) *Any word $y = c + e$ where $c \in \Gamma(x, f, \mathbb{F}_{q_0})$ and $e \in \mathbb{F}_q^n$ with* $\mathrm{wt}(e) \leq \left\lfloor \frac{\deg(f)+1}{2} \right\rfloor$ *can a decoded using either one of Algorithms 4.4 and 4.19.*

Proof. We start by showing Assertion (i). Note that since $\overline{\mathbb{F}}_q = \bigcup_{k=1}^{\infty} \mathbb{F}_{q^k}$ there exists an $N \in \mathbb{N}$ such that f splits into irreducible factors over $\mathbb{F}_{q^N}$, hence $d\left(\Gamma(x, f, \mathbb{F}_{q^N})\right) = \deg(f)+1$ by Corollary 5.8. The rest follows by Proposition 5.11.
Assertion (ii) follows since $\Gamma(x, f, \mathbb{F}_{q_0})$ is a subfield subcode of $\Gamma(x, f, \mathbb{F}_{q^N})$. Furthermore $\Gamma(x, f, \mathbb{F}_{q^N})$ has $\left\lfloor \frac{\deg(f)+1}{2} \right\rfloor$-error decoding algorithms by Theorems 4.6 and 4.21. ■