Algebraic Geometric Codes

Recitation 14

Shir Peleg

Tel Aviv University

June 7, 2022

A Tower over $\mathbb{F}_4$

Consider the tower $\mathcal{T}_1 := F_0 = \mathbb{F}_4(x_0) \subseteq F_1 = \mathbb{F}_4(x_0, x_1) \subseteq \ldots$ over $\mathbb{F}_4$ defined by the equation

$$Y^3 = \frac{X^3}{X^2 + X + 1}.$$

i.e in each step we have $x_i^3 = \frac{x_{i-1}^3}{x_{i-1}^2 + x_{i-1} + 1}$.

A Tower over $\mathbb{F}_4$

Consider the tower $\mathcal{T}_1 := F_0 = \mathbb{F}_4(x_0) \subseteq F_1 = \mathbb{F}_4(x_0, x_1) \subseteq \ldots$ over $\mathbb{F}_4$ defined by the equation

$$Y^3 = \frac{X^3}{X^2 + X + 1}.$$

i.e in each step we have $x_i^3 = \frac{x_{i-1}^3}{x_{i-1}^2 + x_{i-1} + 1}$.
We will study this tower, in two ways.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\infty$: $v_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\infty$: $v_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_\infty(x_1^3) = 3\tilde{v}_\infty(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\infty$: $v_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_\infty(x_1^3) = 3\tilde{v}_\infty(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$. Thus $e(\mathfrak{P}/\mathfrak{p}) = 3$. We can write $\mathfrak{P}_\infty$ the unique place over $\mathfrak{P}_\infty$. It satisfies $v_{\mathfrak{P}_\infty}(x_1) = -1$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\infty$: $v_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_\infty(x_1^3) = 3\tilde{v}_\infty(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$. Thus $e(\mathfrak{P}/\mathfrak{p}) = 3$. We can write $\mathfrak{P}_\infty$ the unique place over $\mathfrak{P}_\infty$. It satisfies $v_{\mathfrak{P}_\infty}(x_1) = -1$.
- $\mathfrak{p}_0$: here, Kummers theorem will not help as the corresponding polynomial is $Y^3 - \mathfrak{p}_0(\frac{x_0^3}{x_0^2+x_0+1}) = Y^3 - 0$ which promises use one place.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\infty$: $v_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_\infty(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_\infty(x_1^3) = 3\tilde{v}_\infty(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$. Thus $e(\mathfrak{P}/\mathfrak{p}) = 3$. We can write $\mathfrak{P}_\infty$ the unique place over $\mathfrak{P}_\infty$. It satisfies $v_{\mathfrak{P}_\infty}(x_1) = -1$.
- $\mathfrak{p}_0$: here, Kummers theorem will not help as the corresponding polynomial is $Y^3 - \mathfrak{p}_0(\frac{x_0^3}{x_0^2+x_0+1}) = Y^3 - 0$ which promises use one place. Fortunately, we can write $(\frac{x_1}{x_0})^3 = \frac{1}{x_0^2+x_0+1}$. Thus from Kummers theorem $\mathfrak{p}_0$ splits completely, into $\mathfrak{P}_0^1, \mathfrak{P}_0^2, \mathfrak{P}_0^3$ where $\mathfrak{P}_0^i(x_1) = 0$, and $\mathfrak{P}_0^i(\frac{x_1}{x_0}) \in \{1, \delta, \delta+1\}$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\delta, p_{\delta+1}$: $v_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\delta, p_{\delta+1}$: $v_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_{\delta+i}(x_1^3) = 3\tilde{v}_{\delta+i}(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\delta, p_{\delta+1}$: $v_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_{\delta+i}(x_1^3) = 3\tilde{v}_{\delta+i}(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$. Thus $e(\mathfrak{P}/\mathfrak{p}) = 3$. We can write $\mathfrak{P}_{\delta+i}$ the unique place over $\mathfrak{P}_{\delta+i}$. It satisfies $v_{\mathfrak{P}_\infty}(x_1) = -1$.

Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

- $\mathfrak{p}_\delta, p_{\delta+1}$: $v_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_{\delta+i}(x_1^3) = 3\tilde{v}_{\delta+i}(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$. Thus $e(\mathfrak{P}/\mathfrak{p}) = 3$. We can write $\mathfrak{P}_{\delta+i}$ the unique place over $\mathfrak{P}_{\delta+i}$. It satisfies $v_{\mathfrak{P}_\infty}(x_1) = -1$.
- $\mathfrak{p}_1$: From Kummers theorem $\mathfrak{p}_1$ splits completely, into $\mathfrak{P}_{1,1}, \mathfrak{P}_{1,\delta}\mathfrak{P}_{1,\delta+1}$ where $\mathfrak{P}_{0,t}(x_1) = t$.

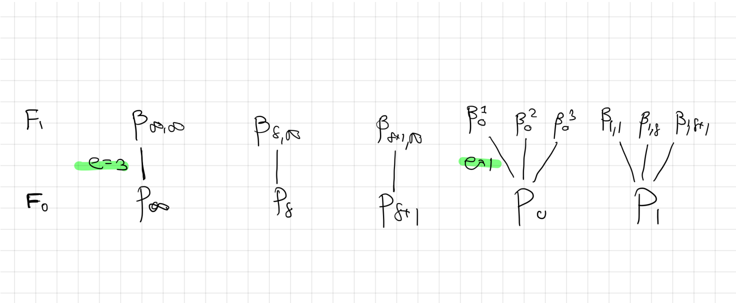
Rational places

F_0 has 5 rational places: $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{\delta+1}$. How do they split in F_1?.

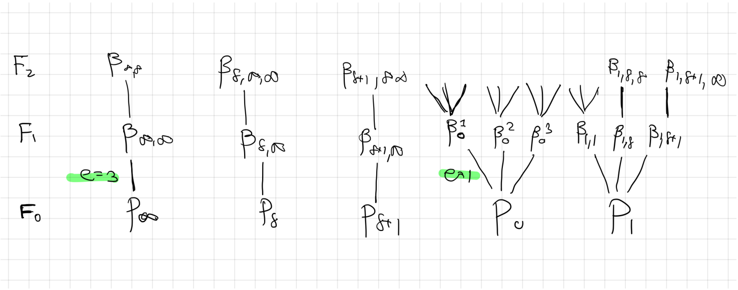
- $\mathfrak{p}_\delta, p_{\delta+1}$: $v_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -1$. Thus $\tilde{v}_{\delta+i}(\frac{x_0^3}{x_0^2+x_0+1}) = -e(\mathfrak{P}/\mathfrak{p})$. On the other hand $\tilde{v}_{\delta+i}(x_1^3) = 3\tilde{v}_{\delta+i}(x_1)$ and $e(\mathfrak{P}/\mathfrak{p}) \leq [F_1 : F_0] \leq 3$. Thus $e(\mathfrak{P}/\mathfrak{p}) = 3$. We can write $\mathfrak{P}_{\delta+i}$ the unique place over $\mathfrak{P}_{\delta+i}$. It satisfies $v_{\mathfrak{P}_\infty}(x_1) = -1$.
- $\mathfrak{p}_1$: From Kummers theorem $\mathfrak{p}_1$ splits completely, into $\mathfrak{P}_{1,1}, \mathfrak{P}_{1,\delta}\mathfrak{P}_{1,\delta+1}$ where $\mathfrak{P}_{0,t}(x_1) = t$.

Finally, From Kummers theorem no place of degree ≥ 2 can be ramified (as it is not a zero or pole of $\frac{x_0^3}{x_0^2+x_0+1}$).

Illustration



Illustration



$\lambda(\mathcal{T}_1)$

$$n_i \geq 3^i$$

As all the places above $\mathfrak{p}_0$ splits fully.

$\lambda(\mathcal{T}_1)$

$$n_i \geq 3^i$$

As all the places above $\mathfrak{p}_0$ splits fully.

$$\deg(\mathrm{Diff}(F_i/F_{i-1})) = \sum_{\mathfrak{p} \text{ ramified } \in \mathbb{P}(F_{i-1})} (e(\mathfrak{P}/\mathfrak{p}) - 1) \cdot \deg(\mathfrak{p}).$$

$\lambda(\mathcal{T}_1)$

$$n_i \geq 3^i$$

As all the places above $\mathfrak{p}_0$ splits fully.

$$\deg(\mathrm{Diff}(F_i/F_{i-1})) = \sum_{\mathfrak{p} \text{ ramified } \in \mathbb{P}(F_{i-\mathbf{1}})} (e(\mathfrak{P}/\mathfrak{p}) - 1) \cdot \deg(\mathfrak{p}).$$

$$= 2 \cdot \text{number of ramified places.} = 2 \cdot (3 + 2 \cdot (i-1)) = 4 \cdot i + 2$$

$\lambda(\mathcal{T}_1)$

$$n_i \geq 3^i$$

As all the places above $\mathfrak{p}_0$ splits fully.

$$\deg(\mathrm{Diff}(F_i/F_{i-1})) = \sum_{\mathfrak{p} \text{ ramified } \in \mathbb{P}(F_{i-\mathbf{1}})} (e(\mathfrak{P}/\mathfrak{p}) - 1) \cdot \deg(\mathfrak{p}).$$

$$= 2 \cdot \text{number of ramified places.} = 2 \cdot (3 + 2 \cdot (i-1)) = 4 \cdot i + 2$$

Therefore, $2g_i - 2 = 3(2g_{i-1} - 2) + 2 + 4 \cdot i \Rightarrow g_i = 3g_{i-1} + 2 \cdot i - 1$

$\lambda(\mathcal{T}_1)$

$$n_i \geq 3^i$$

As all the places above $\mathfrak{p}_0$ splits fully.

$$\deg(\mathrm{Diff}(F_i/F_{i-1})) = \sum_{\mathfrak{p} \text{ ramified } \in \mathbb{P}(F_{i-1})} (e(\mathfrak{P}/\mathfrak{p}) - 1) \cdot \deg(\mathfrak{p}).$$

$$= 2 \cdot \text{number of ramified places.} = 2 \cdot (3 + 2 \cdot (i-1)) = 4 \cdot i + 2$$

Therefore, $2g_i - 2 = 3(2g_{i-1} - 2) + 2 + 4 \cdot i \Rightarrow g_i = 3g_{i-1} + 2 \cdot i - 1$ implies that

$$g_i = 3^i - i - 1$$

$\lambda(\mathcal{T}_1)$

$$n_i \geq 3^i$$

As all the places above $\mathfrak{p}_0$ splits fully.

$$\deg(\mathrm{Diff}(F_i/F_{i-1})) = \sum_{\mathfrak{p} \text{ ramified } \in \mathbb{P}(F_{i-\mathbf{1}})} (e(\mathfrak{P}/\mathfrak{p}) - 1) \cdot \deg(\mathfrak{p}).$$

$$= 2 \cdot \text{number of ramified places.} = 2 \cdot (3 + 2 \cdot (i-1)) = 4 \cdot i + 2$$

Therefore, $2g_i - 2 = 3(2g_{i-1} - 2) + 2 + 4 \cdot i \Rightarrow g_i = 3g_{i-1} + 2 \cdot i - 1$ implies that

$$g_i = 3^i - i - 1$$

Therefore

$$\lambda(\mathcal{T}_1) \geq \lim_{i \to \infty} \frac{3^i}{3^i - i - 1} = 1 = \sqrt{4} - 1$$

Simpler calculation

Recall,

Definition 1

Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$. The set

$$\mathrm{Split}(\mathcal{F}) = \{\mathfrak{p} \in \mathbb{P}_1(F_0) \mid \mathfrak{p} \text{ splits completely in all extesnions } F_i/F_0\}$$

is called the *splitting locus* of $\mathcal{F}$.

Simpler calculation

Recall,

Definition 1

Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$. The set

$$\text{Split}(\mathcal{F}) = \{\mathfrak{p} \in \mathbb{P}_1(F_0) \mid \mathfrak{p} \text{ splits completely in all extesnions } F_i/F_0\}$$

is called the *splitting locus* of $\mathcal{F}$.

Let F/L be an extension of E/K. A prime divisor $\mathfrak{p}$ of E/K is said to *ramify* in the extension F/L of E/K if $\exists \mathfrak{P}/\mathfrak{p}$ s.t. $e(\mathfrak{P}/\mathfrak{p}) > 1$.

Definition 2

Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$. The set

$$\text{Ram}(\mathcal{F}) = \{\mathfrak{p} \in \mathbb{P}(F_0) \mid \mathfrak{p} \text{ is ramified in } F_i/F_0 \text{ for some } i \geq 1\}$$

is called the *ramification locus* of $\mathcal{F}$.

Simpler calculation

We saw in class that in Kummer extensions, if we denote $r = \sum_{p \in \mathrm{Ram}(\mathcal{F})} \deg \mathfrak{p}$ and $s = |\mathrm{Split}(\mathcal{F})|$ then

$$\lambda(\mathcal{F}) \geq \frac{2s}{r-2}$$

Simpler calculation

We saw in class that in Kummer extensions, if we denote $r = \sum_{p \in \mathrm{Ram}(\mathcal{F})} \deg \mathfrak{p}$ and $s = |\mathrm{Split}(\mathcal{F})|$ then

$$\lambda(\mathcal{F}) \geq \frac{2s}{r-2}$$

In our example $\mathcal{T}_1$ we have that:
$\mathrm{Ram}(\mathcal{F}) = \{\mathfrak{p}_\infty, \mathfrak{p}_1, \mathfrak{p}_\delta, \mathfrak{p}_{\delta+1}\}$ and $\mathrm{Split}(\mathcal{F}) = \{\mathfrak{p}_0\}$, and so:

$$\lambda(\mathcal{T}_1) \geq \frac{2 \cdot 1}{4-2}$$

Simpler calculation

We saw in class that in Kummer extensions, if we denote $r = \sum_{p \in \mathrm{Ram}(\mathcal{F})} \deg \mathfrak{p}$ and $s = |\mathrm{Split}(\mathcal{F})|$ then

$$\lambda(\mathcal{F}) \geq \frac{2s}{r-2}$$

In our example $\mathcal{T}_1$ we have that:
$\mathrm{Ram}(\mathcal{F}) = \{\mathfrak{p}_\infty, \mathfrak{p}_1, \mathfrak{p}_\delta, \mathfrak{p}_{\delta+1}\}$ and $\mathrm{Split}(\mathcal{F}) = \{\mathfrak{p}_0\}$, and so:

$$\lambda(\mathcal{T}_1) \geq \frac{2 \cdot 1}{4-2}$$

Consider the variable transform $z_i = \frac{1}{x_i}$. We have here that $F_i = F_{i-1}(z_i)$ and the tower is defined by the equation

$$y^3 = (x+1)^3 - 1.$$

The tower $\mathcal{T}_2$

Let ℓ be a prime power and $q = \ell^r$ for $r \geq 2$. Let $m = \frac{q-1}{\ell-1}$, note that m and ℓ are coprime.

The tower $\mathcal{T}_2$

Let ℓ be a prime power and $q = \ell^r$ for $r \geq 2$. Let $m = \frac{q-1}{\ell-1}$, note that m and ℓ are coprime. We will show that the sequence $\mathcal{T}_2 = (F_0, F_1, \ldots)$ that is recursively defined by

$$Y^m = (X+1)^m - 1.$$

is a tower over $\mathbb{F}_q$. So, we need to prove that

1. $F_i \neq F_{i+1}$;
2. F_{i+1}/F_i is separable
3. $\mathbb{F}_q$ is the constant field of F_i; and
4. $g(F_j) \geq 2$ for some j.

The tower $\mathcal{T}_2$

To prove Items 1,2,3 using a claim from class we will find, for each $i \in \mathbb{N}$

$$\mathfrak{p}_i \in \mathbb{P}(F_i), \mathfrak{P}_i \in \mathbb{P}(F_{i+1}) \quad \text{s.t.} \quad \mathfrak{P}_i/\mathfrak{p}_i \quad \text{and} \quad e(\mathfrak{P}_i/\mathfrak{p}_i) = m.$$

The tower $\mathcal{T}_2$

To prove Items 1,2,3 using a claim from class we will find, for each $i \in \mathbb{N}$

$$\mathfrak{p}_i \in \mathbb{P}(F_i), \mathfrak{P}_i \in \mathbb{P}(F_{i+1}) \quad \text{s.t.} \quad \mathfrak{P}_i/\mathfrak{p}_i \quad \text{and} \quad e(\mathfrak{P}_i/\mathfrak{p}_i) = m.$$

Let $\mathfrak{p}_0$ be the unique zero of x_0 in $F_0 = \mathbb{F}_q(x_0)$. Let $\mathfrak{P}_0/\mathfrak{p}_0$ in $\mathbb{P}(F_1)$. We have that

$$m \cdot v_{\mathfrak{P}_0}(x_1) = v_{\mathfrak{P}_0}(x_1^m) = e(\mathfrak{P}_0/\mathfrak{p}_0) \cdot v_{\mathfrak{p}_0}\left((x_0+1)^m - 1\right) = e(\mathfrak{P}_0/\mathfrak{p}_0).$$

Thus, using also the fundamental equality, $e(\mathfrak{P}_0/\mathfrak{p}_0) = m$ as desired.

The tower $\mathcal{T}_2$

To prove Items 1,2,3 using a claim from class we will find, for each $i \in \mathbb{N}$

$$\mathfrak{p}_i \in \mathbb{P}(F_i), \mathfrak{P}_i \in \mathbb{P}(F_{i+1}) \quad \text{s.t.} \quad \mathfrak{P}_i/\mathfrak{p}_i \quad \text{and} \quad e(\mathfrak{P}_i/\mathfrak{p}_i) = m.$$

Let $\mathfrak{p}_0$ be the unique zero of x_0 in $F_0 = \mathbb{F}_q(x_0)$. Let $\mathfrak{P}_0/\mathfrak{p}_0$ in $\mathbb{P}(F_1)$. We have that

$$m \cdot v_{\mathfrak{P}_0}(x_1) = v_{\mathfrak{P}_0}(x_1^m) = e(\mathfrak{P}_0/\mathfrak{p}_0) \cdot v_{\mathfrak{p}_0}\left((x_0+1)^m - 1\right) = e(\mathfrak{P}_0/\mathfrak{p}_0).$$

Thus, using also the fundamental equality, $e(\mathfrak{P}_0/\mathfrak{p}_0) = m$ as desired. Moreover, note that $v_{\mathfrak{P}_0}(x_1) = 1$ and so we can iterate this argument for all $i \in \mathbb{N}$.

The tower $\mathcal{T}_2$

To prove Items 1,2,3 using a claim from class we will find, for each $i \in \mathbb{N}$

$$\mathfrak{p}_i \in \mathbb{P}(F_i), \mathfrak{P}_i \in \mathbb{P}(F_{i+1}) \quad \text{s.t.} \quad \mathfrak{P}_i/\mathfrak{p}_i \quad \text{and} \quad e(\mathfrak{P}_i/\mathfrak{p}_i) = m.$$

Let $\mathfrak{p}_0$ be the unique zero of x_0 in $F_0 = \mathbb{F}_q(x_0)$. Let $\mathfrak{P}_0/\mathfrak{p}_0$ in $\mathbb{P}(F_1)$. We have that

$$m \cdot v_{\mathfrak{P}_0}(x_1) = v_{\mathfrak{P}_0}(x_1^m) = e(\mathfrak{P}_0/\mathfrak{p}_0) \cdot v_{\mathfrak{p}_0}\left((x_0+1)^m - 1\right) = e(\mathfrak{P}_0/\mathfrak{p}_0).$$

Thus, using also the fundamental equality, $e(\mathfrak{P}_0/\mathfrak{p}_0) = m$ as desired. Moreover, note that $v_{\mathfrak{P}_0}(x_1) = 1$ and so we can iterate this argument for all $i \in \mathbb{N}$. item 4 will follow from the general analysis of $\mathrm{Split}(\mathcal{T}_2), \mathrm{Ram}(\mathcal{T}_2)$.

Lemma 3

Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a recursive tower over $\mathbb{F}_q$ defined by the equation

$$f(Y) = h(X),$$

with a basic function field F. Define

$$\Lambda_0 := \{x(\mathfrak{p}) \mid \mathfrak{p} \in \mathbb{F}_q(x) \text{ is ramified in } \mathbb{F}_q(x,y)/\mathbb{F}_q(x)\} \subseteq \overline{\mathbb{F}_q} \cup \{\infty\}.$$

Suppose that $\Lambda \subseteq \overline{\mathbb{F}_q} \cup \{\infty\}$ satisfies:

1. *$\Lambda_0 \subseteq \Lambda$; and*
2. *$\forall \beta \in \Lambda$, any solution $\alpha \in \overline{\mathbb{F}_q} \cup \{\infty\}$ to the equation $f(\beta) = h(\alpha)$ in fact satisfies $\alpha \in \Lambda$.*

Then, the ramification locus $\mathrm{Ram}(\mathcal{F})$ is finite and

$$\mathrm{Ram}(\mathcal{F}) \subseteq \{\mathfrak{p} \in \mathbb{P}(\mathbb{F}_q(x_0)) \mid x_0(\mathfrak{p}) \in \Lambda\}.$$

Λ for $\mathcal{T}_2$

First we note that $(x+1)^m - 1$ splits into different prime factors as $gcd((x+1)^m - 1, m(x+1)^{m-1}) = 1$. Thus, this is a tame cyclic extension and

$$\Lambda_0 = \{\beta \in \overline{\mathbb{F}_q} \mid (\beta+1)^m = 1\}$$

Λ for $\mathcal{T}_2$

First we note that $(x+1)^m - 1$ splits into different prime factors as $gcd((x+1)^m - 1, m(x+1)^{m-1}) = 1$. Thus, this is a tame cyclic extension and

$$\Lambda_0 = \{\beta \in \overline{\mathbb{F}_q} \mid (\beta+1)^m = 1\}$$

First we note that $\Lambda_0 \subseteq \mathbb{F}_q$. Recall that $Gal(\mathbb{F}_q/\mathbb{F}_\ell) = (Frob_\ell^i)_{i=0}^{r-1}$. Therefore, for $x \in \mathbb{F}_q$

$$Norm_{\mathbb{F}_\ell}(x) = \prod x^{\ell^i} = x^{\sum \ell^i} = x^m.$$

Λ for $\mathcal{T}_2$

First we note that $(x+1)^m - 1$ splits into different prime factors as $gcd((x+1)^m - 1, m(x+1)^{m-1}) = 1$. Thus, this is a tame cyclic extension and

$$\Lambda_0 = \{\beta \in \overline{\mathbb{F}_q} \mid (\beta+1)^m = 1\}$$

First we note that $\Lambda_0 \subseteq \mathbb{F}_q$. Recall that $Gal(\mathbb{F}_q/\mathbb{F}_\ell) = (Frob_\ell^i)_{i=0}^{r-1}$. Therefore, for $x \in \mathbb{F}_q$

$$Norm_{\mathbb{F}_\ell}(x) = \prod x^{\ell^i} = x^{\sum \ell^i} = x^m.$$

Finally, as $Norm_{\mathbb{F}_\ell} : \mathbb{F}_q^\times \to \mathbb{F}_\ell^\times$ is a group homomorphism there are exactly $m = \frac{q-1}{\ell-1}$ solutions to the equation $Norm(x) = 1$ in $\mathbb{F}_q$, which are all the solutions.

Λ for $\mathcal{T}_2$

First we note that $(x+1)^m - 1$ splits into different prime factors as $gcd((x+1)^m - 1, m(x+1)^{m-1}) = 1$. Thus, this is a tame cyclic extension and

$$\Lambda_0 = \{\beta \in \overline{\mathbb{F}_q} \mid (\beta+1)^m = 1\}$$

First we note that $\Lambda_0 \subseteq \mathbb{F}_q$. Recall that $Gal(\mathbb{F}_q/\mathbb{F}_\ell) = (Frob_\ell^i)_{i=0}^{r-1}$. Therefore, for $x \in \mathbb{F}_q$

$$Norm_{\mathbb{F}_\ell}(x) = \prod x^{\ell^i} = x^{\sum \ell^i} = x^m.$$

Finally, as $Norm_{\mathbb{F}_\ell} : \mathbb{F}_q^\times \to \mathbb{F}_\ell^\times$ is a group homomorphism there are exactly $m = \frac{q-1}{\ell-1}$ solutions to the equation $Norm(x) = 1$ in $\mathbb{F}_q$, which are all the solutions.
Let $\beta \in \mathbb{F}_q$, then and therefore, $\beta^m = Norm_{\mathbb{F}_\ell}(\beta) \in \mathbb{F}_\ell$ thus, as before, all the solutions to the equation $(\alpha+1)^m = \beta^m + 1$ are in $\mathbb{F}_q = \Lambda$.

Splitting locus for $\mathcal{T}_2$

Let $\mathfrak{p}_\infty \in \mathbb{P}(F_0)$. Similarly to the analysis of $\mathcal{T}_1$ we can not use Kummers theorem as $y \notin \mathcal{O}'_{\mathfrak{p}}$, but we can fix it in a similar manner:

Splitting locus for $\mathcal{T}_2$

Let $\mathfrak{p}_\infty \in \mathbb{P}(F_0)$. Similarly to the analysis of $\mathcal{T}_1$ we can not use Kummers theorem as $y \notin \mathcal{O}'_\mathfrak{p}$, but we can fix it in a similar manner: Consider $\left(\frac{x_1}{x_0+1}\right)^m = 1 - \frac{1}{(x+1)^m}$. Now, $\mathfrak{P}_\infty(1 - \frac{1}{(x+1)^m}) = 1$ and from Kummers theorem, the polynomial $X^m - 1$ splits into m factors in $\mathbb{F}_q$, and thus the place $\mathfrak{p}_\infty$ splits completely, every place $\mathfrak{P}/\mathfrak{p}_\infty$ must also satisfy $\mathfrak{P}(x_1) = -1$ and therefore, we can repeat the argument to get $\mathfrak{p}_\infty \in \mathrm{Split}(\mathcal{T}_2)$.

$\mathcal{T}_2$ is a asymptotically good tower

First, we must show that item 4 holds, i.e. for some i $g_i \geq 2$. Indeed,

$$2g_1 - 2 = [F_1 : F_0](2g_0 - 2) + \deg Diff(F_1/F_2)$$

plug in what we know,

$$2g_1 - 2 \geq -2 \cdot m + (m-1)(m) = (m-3)m \geq m \geq 2$$

if $m > 3$ if $q = 4, \ell = 2$ then we already saw in $\mathcal{T}_1$.

$\mathcal{T}_2$ is a asymptotically good tower

First, we must show that item 4 holds, i.e. for some i $g_i \geq 2$. Indeed,

$$2g_1 - 2 = [F_1 : F_0](2g_0 - 2) + \deg \mathit{Diff}(F_1/F_2)$$

plug in what we know,

$$2g_1 - 2 \geq -2 \cdot m + (m-1)(m) = (m-3)m \geq m \geq 2$$

if $m > 3$ if $q = 4, \ell = 2$ then we already saw in $\mathcal{T}_1$.
Now for $\Lambda(\mathcal{T}_2)$:

$$\lambda(\mathcal{T}_2) \geq \frac{2s}{r-2} \geq \frac{2 \cdot 1}{q-2} > 0$$

which implies that the code is asymptotically good.