Algebraic Geometric Codes

Recitation 13

Tomer Manket

Tel Aviv University

Towers of Function Fields

Definition 1

A *tower over* $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_i)_{i=0}^{\infty}$ of function fields $F_i/\mathbb{F}_q$ such that

1. $F_i \subsetneq F_{i+1}$ for all i.
2. each F_{i+1}/F_i is finite and separable.
3. $g_i := g(F_i) \to \infty$ as $i \to \infty$.

Remark 1

Let $F_0/\mathbb{F}_q$ be a function field and $F_0 \subseteq F_1 \subseteq \ldots$ be a sequence of finite separable field extensions. We saw in class that if

1. $\exists j \geq 0$ *s.t.* $g_j \geq 2$; *and*
2. $\forall i \geq 0$ *there exist* $\mathfrak{p}_i \in \mathbb{P}_{F_i}$ *and* $\mathfrak{P}_i \in \mathbb{P}_{F_{i+1}}$ *s.t.* $\mathfrak{P}_i \mid \mathfrak{p}_i$ *and*

$$e(\mathfrak{P}_i/\mathfrak{p}_i) = [F_{i+1} : F_i] > 1\,,$$

then $\mathcal{F} = (F_i)_{i=0}^{\infty}$ *is a tower over* $\mathbb{F}_q$.

Towers of Function Fields

Let $\mathcal{F} = (F_i)_{i=0}^{\infty}$ be a *tower over* $\mathbb{F}_q$. We denote by $n_i = N(F_i)$ the number of prime divisors of degree one in F_i.

Definition 2

1. The *splitting rate* of $\mathcal{F}$ is defined by
$$\nu(\mathcal{F}) = \lim_{i\to\infty} \frac{n_i}{[F_i : F_0]}.$$
2. The *genus* of $\mathcal{F}$ is defined by
$$\gamma(\mathcal{F}) = \lim_{i\to\infty} \frac{g_i}{[F_i : F_0]}.$$
3. The *limit* of $\mathcal{F}$ is defined by
$$\lambda(\mathcal{F}) = \lim_{i\to\infty} \frac{n_i}{g_i}.$$

The tower is *asymptotically good* if $\lambda(\mathcal{F}) > 0$.

Towers of Function Fields

Remark 2

We saw in class that

$$0 \leq \nu(\mathcal{F}) < \infty,$$
$$0 < \gamma(\mathcal{F}) \leq \infty,$$
$$0 \leq \lambda(\mathcal{F}) = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} < \infty$$

and $\mathcal{F}$ *is asymptotically good* $\iff \nu(\mathcal{F}) > 0$ *and* $\gamma(\mathcal{F}) < \infty$.

Theorem 3 (Drinfeld-Vladut)

Let $\mathcal{F}$ *be a tower over* $\mathbb{F}_q$. *Then*

$$\lambda(\mathcal{F}) \leq \sqrt{q} - 1.$$

An optimal tower over $\mathbb{F}_4$

Example 4

Consider the tower $\mathcal{T}_1 = (F_i)_{i=0}^{\infty}$ in which $F_0 = \mathbb{F}_4(x_0)$ and for each $i \geq 0$,

$$F_{i+1} = F_i(x_{i+1}) \text{ where } x_{i+1}^3 = \frac{{x_i}^3}{x_i^2 + x_i + 1}$$

i.e. the tower over $\mathbb{F}_4$ that is recursively defined by the equation

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

Claim 4.1

$\mathcal{T}_1$ is an optimal tower over $\mathbb{F}_4$, i.e. it is a tower with

$$\lambda(\mathcal{T}_1) = \sqrt{q} - 1 = 2 - 1 = 1.$$

The tower $\mathcal{T}_1$

Let us first show that $\mathcal{T}_1$ is indeed a tower over $\mathbb{F}_q$.

- Let $\mathfrak{p}_\infty \in \mathbb{P}_{F_0}$ be the unique pole of x_0 in $F_0 = \mathbb{F}_4(x_0)$.

  Suppose $\mathfrak{P}_\infty \in \mathbb{P}_{F_1}$ lies above $\mathfrak{p}_\infty$. Then

$$3 \cdot \nu_{\mathfrak{P}_\infty}(x_1) = \nu_{\mathfrak{P}_\infty}(x_1^3) = \nu_{\mathfrak{P}_\infty}\left(\frac{x_0^3}{x_0^2+x_0+1}\right)$$
$$= e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) \cdot \underbrace{\nu_\infty\left(\frac{x_0^3}{x_0^2+x_0+1}\right)}_{=-1} = -e(\mathfrak{P}_\infty/\mathfrak{p}_\infty)$$

  Since $1 \leq e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) \leq [F_1 : F_0] \leq 3$ we conclude that

$$e(\mathfrak{P}_\infty/\mathfrak{p}_\infty) = [F_1 : F_0] = 3 \quad \text{and} \quad \nu_{\mathfrak{P}_\infty}(x_1) = -1,$$

  i.e. $\mathfrak{p}_\infty$ is totally ramified in F_1/F_0 and $\mathfrak{P}_\infty$ is the unique prime divisor lying above it in F_1.

The tower $\mathcal{T}_1$

Moreover, $F_1 = F_0(x_1)$ where $x_1^n = u$ for $n = 3$ and $u = \frac{x_0^3}{x_0^2+x_0+1} \in F_0$,

- $n = 3$ is coprime to $\mathrm{char}(\mathbb{F}_4) = 2$
- $\mathbb{F}_4$ contains a primitive 3^{rd} root of unity ($\delta \in \mathbb{F}_4 \setminus \{0, 1\}$).
- $u \neq w^3$ for all $w \in F_0$ (as $3 \nmid \nu_\infty(u) = -1$).

Therefore F_1/F_0 is a Kummer extension, so it is Galois and in particular finite and separable.

Note that since $\nu_{\mathfrak{P}_\infty}(x_1) = -1 = \nu_\infty(x_0)$, we can reiterate this argument to get that for all $i \in \mathbb{N}$, the extension F_{i+1}/F_i is finite and separable, and there exist $\mathfrak{p}_i \in \mathbb{P}_{F_i}$ and $\mathfrak{P}_i \in \mathbb{P}_{F_{i+1}}$ s.t. $\mathfrak{P}_i \mid \mathfrak{p}_i$ and

$$e(\mathfrak{P}_i/\mathfrak{p}_i) = [F_{i+1} : F_i] = 3.$$

This part of Remark 1 implies that the constant field of each F_i is $\mathbb{F}_4$. It remains to show that $g_j \geq 2$ for some $j \geq 0$. This is indeed the case, as we will see later.

Rational prime divisors in $\mathcal{T}_1$

As $F_0 = \mathbb{F}_4(x_0)$ is a rational function field, the rational (i.e. degree one) prime divisors in F_0 are $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\delta$, $\mathfrak{p}_{1+\delta}$ and $\mathfrak{p}_\infty$ (where $\delta^2 + \delta + 1 = 0$).

Each rational prime divisor in F_1 lies above one of them, so let us explore the prime divisors above them in F_1.

- $\mathfrak{p}_\infty$: We already showed that $\mathfrak{p}_\infty$ is totally ramified in F_1/F_0. Since F_0 and F_1 have the same constant field $\mathbb{F}_4$, we get that

$$\deg \mathfrak{P}_\infty = f(\mathfrak{P}_\infty/\mathfrak{p}_\infty) = 1.$$

- $\mathfrak{p}_1$: The min. poly. of x_1 over F_0 is $\varphi(Y) = Y^3 - \frac{x_0^3}{x_0^2+x_0+1} \in F_0[Y]$, and

$$\varphi_1(Y) := Y^3 - \frac{1^3}{1^2+1+1} = Y^3 - 1 = (Y-1)(Y^2+Y+1) = (Y-1)(Y-\delta)(Y-(1+\delta)).$$

  By Kummer theorem, $\mathfrak{p}_1$ splits completely in F_1/F_0 to $\mathfrak{P}_{1,1}, \mathfrak{P}_{1,\delta}$ and $\mathfrak{P}_{1,1+\delta}$, all of degree 1.

- $\mathfrak{p}_\delta$: Suppose $\mathfrak{P}_\delta \in \mathbb{P}_{F_1}$ lies above $\mathfrak{p}_\delta$. Since

$$\nu_\delta\left(\frac{x_0^3}{x_0^2+x_0+1}\right) = 3\cdot\nu_\delta(x_0) - \nu_\delta(x_0^2+x_0+1) = 0-1 = -1$$

  we can proceed as in the analysis of $\mathfrak{p}_\infty$ to get $e(\mathfrak{P}_\delta/\mathfrak{p}_\delta) = 3$. Hence $\mathfrak{p}_\delta$ is also totally ramified in F_1/F_0, $\mathfrak{P}_\delta$ is unique, has degree one, and

$$\nu_{\mathfrak{P}_\delta}(x_1) = -1.$$

- $\mathfrak{p}_{1+\delta}$: Suppose $\mathfrak{P}_{1+\delta} \in \mathbb{P}_{F_1}$ lies above $\mathfrak{p}_{1+\delta}$. Since

$$\nu_{1+\delta}\left(\frac{x_0^3}{x_0^2+x_0+1}\right) = 3\cdot\nu_{1+\delta}(x_0) - \nu_{1+\delta}(x_0^2+x_0+1) = 0-1 = -1$$

  this case is also similar.

- $\mathfrak{p}_0$: In this case

$$\varphi_0(Y) = Y^3 - \frac{0^3}{0^2 + 0 + 1} = Y^3$$

so we cannot apply Kummer theorem for the element $x_1 \in F_1$. However, if we consider the element $z = \frac{x_1}{x_0} \in F_1$, then $z^3 = \frac{1}{x_0^2 + x_0 + 1}$, its minimal polynomial is $\tilde{\varphi}(Z) = Z^3 - \frac{1}{x_0^2 + x_0 + 1} \in F_0[Z]$ and

$$\tilde{\varphi}_0(Z) = Z^3 - 1 = (Z - 1)(Z - \delta)(Z - (1 + \delta)).$$

Hence by Kummer theorem, $\mathfrak{p}_0$ splits completely in F_1/F_0 to $\mathfrak{P}_{0,z-1}$, $\mathfrak{P}_{0,z-\delta}$ and $\mathfrak{P}_{0,z-(1+\delta)}$, all of degree 1. Clearly, for each $\mathfrak{P} \mid \mathfrak{p}_0$,

$$3 \cdot \nu_{\mathfrak{P}}(x_1) = \nu_{\mathfrak{P}}(x_1^3) = e(\mathfrak{P}/\mathfrak{p}_0) \cdot \nu_0 \left(\frac{x_0^3}{x_0^2 + x_0 + 1} \right) = 1 \cdot 3 = 3$$

so that $\nu_{\mathfrak{P}}(x_1) = 1 = \nu_0(x_0)$.

Rational prime divisors in F_1/F_0

In summary, we have 3 rational prime divisors in F_0 that ramify in F_1/F_0:

$$\begin{array}{ccc} \mathfrak{P}_{\infty}^{(1)} & \mathfrak{P}_{\delta,\infty} & \mathfrak{P}_{1+\delta,\infty} \\ \Big| \, e=3 & \Big| \, e=3 & \Big| \, e=3 \\ \mathfrak{p}_{\infty} & \mathfrak{p}_{\delta} & \mathfrak{p}_{1+\delta} \end{array}$$

and 2 rational prime divisors in F_0 that split completely in F_1/F_0:

$$\begin{array}{ccc} \mathfrak{P}_{0,z-1} & \mathfrak{P}_{0,z-\delta} & \mathfrak{P}_{0,z-(1+\delta)} \\ \searrow & \Big| & \swarrow \\ & \mathfrak{p}_0 & \end{array} \qquad \begin{array}{ccc} \mathfrak{P}_{1,1} & \mathfrak{P}_{1,\delta} & \mathfrak{P}_{1,1+\delta} \\ \searrow & \Big| & \swarrow \\ & \mathfrak{p}_1 & \end{array}$$

Rational prime divisors in F_2/F_1

We can use similar arguments to analyze the behavior of these prime divisors in the second floor of the tower, i.e. F_2/F_1. For the ramified places we obtain

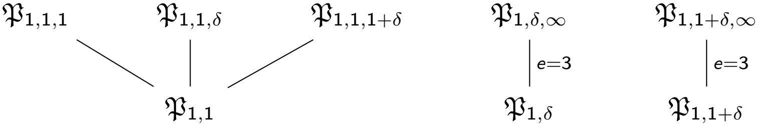
$$\begin{array}{ccc} \mathfrak{P}_{\infty}^{(2)} & \mathfrak{P}_{\delta,\infty,\infty} & \mathfrak{P}_{1+\delta,\infty,\infty} \\ \Big|\, e=3 & \Big|\, e=3 & \Big|\, e=3 \\ \mathfrak{P}_{\infty}^{(1)} & \mathfrak{P}_{\delta,\infty} & \mathfrak{P}_{1+\delta,\infty} \end{array}$$

The prime divisors above $\mathfrak{p}_0$ splits completely. For example, for $\mathfrak{P}_{0,z-1}$, denoting $w = \frac{x_2}{x_1} \in F_2$, we get

$$\begin{array}{ccc} \mathfrak{P}_{0,z-1,w-1} & \mathfrak{P}_{0,z-1,w-\delta} & \mathfrak{P}_{0,z-1,w-(1+\delta)} \\ \diagdown & | & \diagup \\ & \mathfrak{P}_{0,z-1} & \end{array}$$

Rational prime divisors in F_2/F_1

Finally, for the prime divisors above $\mathfrak{p}_1$ in F_1, we get that two of them are totally ramified in F_2/F_1 while $\mathfrak{P}_{1,1}$ splits completely there:



and we can continue in the same manner to the next levels of the tower.

In particular, since each prime divisor lying above $\mathfrak{p}_0$ in F_i/F_0 splits completely, we get that

$$n_i = N(F_i) \geq 3^i. \tag{1}$$

To conclude, we need to find the genera g_i.

To conclude, we need to find the genera g_i.

Since each F_{i+1}/F_i is finite and separable (and both have the same constant field $\mathbb{F}_q$), we get by Hurwitz Genus Formula that

$$2g_{i+1} - 2 = [F_{i+1} : F_i] \cdot (2g_i - 2) + \deg \mathrm{Diff}(F_{i+1}/F_i). \qquad (2)$$

Note that $[F_{i+1} : F_i] = 3$ and this extension is Galois, so each ramification index is either 1 or 3, and above each ramified $\mathfrak{p} \in \mathbb{P}_{F_i}$ there is a unique $\mathfrak{P} \in \mathbb{P}_{F_{i+1}}$ with $\deg \mathfrak{P} = 1$. Hence

$$\deg \mathrm{Diff}(F_{i+1}/F_i) = \sum_{\mathfrak{p} \in \mathbb{P}_{F_i}} \sum_{\substack{\mathfrak{P} \in \mathbb{P}_{F_{i+1}} \\ \mathfrak{p} | \mathfrak{P}}} (e(\mathfrak{P}/\mathfrak{p}) - 1) \deg \mathfrak{P} = 2R_i$$

where R_i is the number of $\mathfrak{p} \in \mathbb{P}_{F_i}$ which are ramified in F_{i+1}/F_i. Let us assume that every such $\mathfrak{p}$ lies above a *rational* prime divisor in $F_0 = \mathbb{F}_4(x_0)$ (we will be justify this later). By the previous analysis of the rational prime divisors in F_0 and their extensions in the tower, we obtain

$$R_i = 3 + 2i$$

Substituting in Equation (2), we get

$$\begin{aligned} 2g_{i+1} - 2 &= [F_{i+1} : F_i] \cdot (2g_i - 2) + \deg \mathrm{Diff}(F_{i+1}/F_i) \\ &= 3 \cdot (2g_i - 2) + 2R_i \end{aligned}$$

which implies

$$g_{i+1} - 1 = 3 \cdot (g_i - 1) + R_i = 3g_i - 3 + 3 + 2i$$

which gives $g_{i+1} = 3g_i + 2i + 1$. Since $g_0 = 0$, we can solve to get

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

Note that in particular $g_2 = 6 \geq 2$ so it is indeed a tower (this is also clear as $g_i \to \infty$ as $i \to \infty$).

The limit of $\mathcal{T}_1$

Finally, we can see that

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

But by the Drinfeld-Vladut bound,

$$\lambda(\mathcal{T}_1) \leq \sqrt{q} - 1 = \sqrt{4} - 1 = 1$$

hence $\lambda(\mathcal{T}_1) = 1$ and this tower is optimal over $\mathbb{F}_4$.

The limit of $\mathcal{T}_1$

Finally, we can see that

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

But by the Drinfeld-Vladut bound,

$$\lambda(\mathcal{T}_1) \leq \sqrt{q} - 1 = \sqrt{4} - 1 = 1$$

hence $\lambda(\mathcal{T}_1) = 1$ and this tower is optimal over $\mathbb{F}_4$.

We are almost done - we still need to show that all the ramification in the tower occur above *rational* prime divisors in F_0.

The ramification locus of $\mathcal{T}_1$

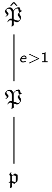
Definition 5

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

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

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

Suppose that $\mathfrak{P} \in \mathbb{P}_{F_i}$ is ramified in F_{i+1}/F_i, i.e. there exists $\hat{\mathfrak{P}} \in \mathbb{P}_{F_{i+1}}$ s.t. $\hat{\mathfrak{P}} \mid \mathfrak{P}$ and $e(\hat{\mathfrak{P}}/\mathfrak{P}) > 1$. Let $\mathfrak{p} \in \mathbb{P}_{F_0}$ be the prime divisor below $\mathfrak{P}$.



Then clearly $\mathfrak{p} \in \mathrm{Ram}(\mathcal{F})$, as

$$e(\hat{\mathfrak{P}}/\mathfrak{p}) = \underbrace{e(\hat{\mathfrak{P}}/\mathfrak{P})}_{>1} \cdot e(\mathfrak{P}/\mathfrak{p}) > 1.$$

Thus, it suffices to show that $\mathrm{Ram}(\mathcal{T}_1) \subseteq \mathbb{P}^1_{F_0}$. Fortunately, we have

Theorem 6

Let $\mathcal{F} = (F_i)_{i=0}^{\infty}$ be a recursive tower over $\mathbb{F}_q$ defined by the equation

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

with a basic function field F, i.e. $F = \mathbb{F}_q(x, y)$ where $f(y) = h(x)$. Assume that every prime divisor of $\mathbb{F}_q(x)$ that ramifies in $F/\mathbb{F}_q(x)$ is rational. In particular,

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

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

1. $\Lambda_0 \subseteq \Lambda$*; and*
2. *if $\beta \in \Lambda$ and $\alpha \in \overline{\mathbb{F}_q} \cup \{\infty\}$ satisfy the equation $f(\beta) = h(\alpha)$, then $\alpha \in \Lambda$.*

Then, the ramification locus is finite and

$$\mathrm{Ram}(\mathcal{F}) \subseteq \{\mathfrak{p} \in \mathbb{P}^1_{F_0} \mid x_0(\mathfrak{p}) \in \Lambda\}.$$

Let us apply this theorem to the tower $\mathcal{T}_1$.

First, the basic function field $F = \mathbb{F}_4(x, y)$ where $y^3 = \frac{x^3}{x^2+x+1}$ is a Kummer extension of $\mathbb{F}_4(x)$ (with $n = 3$ and $u = \frac{x^3}{x^2+x+1}$). By Kummer theory, if $\mathfrak{P} \in \mathbb{P}_F$ lies above $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_4(x)}$, then

$$e(\mathfrak{P}/\mathfrak{p}) = \frac{n}{r_\mathfrak{p}} = \frac{n}{\gcd(n, \nu_\mathfrak{p}(u))} = \frac{3}{\gcd(3, \nu_\mathfrak{p}(u))}.$$

Since $u = \frac{x^3}{(x-\delta)(x-(1+\delta))}$, we have

$$\nu_\mathfrak{p}(u) = \begin{cases} 3 & \mathfrak{p} = \mathfrak{p}_0 \\ -1 & \mathfrak{p} \in \{\mathfrak{p}_\delta, \mathfrak{p}_{1+\delta}, \mathfrak{p}_\infty\} \\ 0 & \text{otherwise} \end{cases}$$

Thus, the only prime divisors in $\mathbb{P}_{\mathbb{F}_4(x)}$ which are ramified in $F/\mathbb{F}_4(x)$ are $\mathfrak{p}_\delta$, $\mathfrak{p}_{1+\delta}$ and $\mathfrak{p}_\infty$, and so

$$\Lambda_0 = \{\delta, 1 + \delta, \infty\}.$$

To conclude, we claim that $\Lambda := \Lambda_0 \cup \{1\} = \{1, \delta, 1+\delta, \infty\}$ satisfies the required conditions.

1. Clearly $\Lambda_0 \subseteq \Lambda$.
2. Let $\beta \in \Lambda$ and suppose $\beta^3 = \frac{\alpha^3}{\alpha^2+\alpha+1}$.

   If $\beta = \infty$ then either $\alpha = \infty$, or $\alpha^2 + \alpha + 1 = 0$, i.e. $\alpha \in \{\delta, 1+\delta\}$. In any case, $\alpha \in \Lambda$.

   Otherwise, $\beta \in \mathbb{F}_4^\times$ so that $\beta^3 = 1$ and hence $\frac{\alpha^3}{\alpha^2+\alpha+1} = 1$. Therefore $\alpha^3 = \alpha^2 + \alpha + 1$. Since the characteristic is 2, we get

   $$(\alpha + 1)^3 = \alpha^3 + \alpha^2 + \alpha + 1 = 0$$

   and therefore $\alpha = 1 \in \Lambda$.

Thus,

$$\mathrm{Ram}(\mathcal{T}_1) \subseteq \{\mathfrak{p} \in \mathbb{P}^1_{F_0} \mid x_0(\mathfrak{p}) \in \Lambda\} = \{\mathfrak{p}_1, \mathfrak{p}_\delta, \mathfrak{p}_{1+\delta}, \mathfrak{p}_\infty\}.$$

In fact, by the previous analysis, this holds with equality.

A simpler calculation

Let us give an immediate proof, using another theorem from class. First, recall

Definition 7

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

$$\mathrm{Split}(\mathcal{F}) = \left\{\mathfrak{p} \in \mathbb{P}^1_{F_0} \mid \mathfrak{p} \text{ splits completely in all extensions } F_i/F_0\right\}$$

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

A simpler calculation

Let us give an immediate proof, using another theorem from class. First, recall

Definition 7

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

$$\mathrm{Split}(\mathcal{F}) = \left\{\mathfrak{p} \in \mathbb{P}^1_{F_0} \mid \mathfrak{p} \text{ splits completely in all extensions } F_i/F_0\right\}$$

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

In our case, we saw that $\mathrm{Split}(\mathcal{T}_1) = \{\mathfrak{p}_0\}$.

In fact, we can show that $\{\mathfrak{p}_0\} \subseteq \mathrm{Split}(\mathcal{T}_1)$ using an analogue theorem for the splitting locus.

The splitting locus

Theorem 8

Let $\mathcal{F} = (F_i)_{i=0}^{\infty}$ be a recursive tower over $\mathbb{F}_q$ defined by the equation

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

and let F be the basic function field of the tower. Assume that there exists $\emptyset \neq \Sigma \subseteq \mathbb{F}_q \cup \{\infty\}$ s.t. for all $\alpha \in \Sigma$:

1. *$\mathfrak{p}_{x-\alpha}$ splits completely in F; and*
2. *for all $\mathfrak{P} \in \mathbb{P}_F$ s.t. $\mathfrak{P} \mid \mathfrak{p}_{x-\alpha}$, it holds that $y(\mathfrak{P}) \in \Sigma$.*

Then,

$$\{\mathfrak{p}_{x_0-\alpha} \mid \alpha \in \Sigma\} \subseteq \mathrm{Split}(\mathcal{F}).$$

In our case, we can apply this theorem with $\Sigma = \{0\}$. The same arguments used for F_1/F_0 shows that $\mathfrak{p}_{x-0}$ splits completely in F, and for every $\mathfrak{P} \in \mathbb{P}_F$ s.t. $\mathfrak{P} \mid \mathfrak{p}_{x-0}$ it holds that $\nu_{\mathfrak{P}}(y) = 1$, hence $y(\mathfrak{P}) = 0 \in \Sigma$ as desired.

To conclude, recall

Definition 9

A tower $\mathcal{F} = (F_i)_{i=0}^{\infty}$ over $\mathbb{F}_q$ is called *tame* if all ramification indices $e(\mathfrak{P}/\mathfrak{p})$ (where $\mathfrak{p} \in \mathbb{P}_{F_0}$ and $\mathfrak{P} \in \mathbb{P}_{F_i}$) are coprime to char $\mathbb{F}_q$.

Theorem 10

Let $\mathcal{F} = (F_i)_{i=0}^{\infty}$ be a tame tower over $\mathbb{F}_q$ with $F_0 = \mathbb{F}_q(x_0)$ and

$$s = |\mathrm{Split}(\mathcal{F})| \quad \text{and} \quad r = \sum_{\mathfrak{p} \in \mathrm{Ram}(\mathcal{F})} \deg \mathfrak{p}.$$

Then

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

Since the tower $\mathcal{T}_1$ is a tame tower over $\mathbb{F}_4$ with $s \geq 1$ (in fact $s = 1$) and $r = |\mathrm{Ram}(\mathcal{T}_1)| = 4$, we obtain

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

Transformation of Variables

So far we considered the recursive tower $\mathcal{T}_1$ over $\mathbb{F}_4$ defined by the equation

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

Consider the variable transformation $z_i := \frac{1}{x_i}$. Clearly $F_i = F_{i-1}(z_i)$ and

$$\begin{aligned} z_{i+1}^3 = \frac{1}{x_{i+1}^3} = \frac{x_i^2 + x_i + 1}{x_i^3} &= \frac{1}{x_i} + \frac{1}{x_i^2} + \frac{1}{x_i^3} \\ &= z_i + z_i^2 + z_i^3 = (z_i + 1)^3 - 1. \end{aligned}$$

Thus, $\mathcal{T}_1$ is recursively defined (with $F_0 = \mathbb{F}_4(z_0)$ and $F_i = F_{i-1}(z_i)$) by the nicer equation

$$Y^3 = (X + 1)^3 - 1.$$

In fact, this is a particular case of a more general result.

An asymptotically good tower over non-prime fields

Theorem 11

Let ℓ be a prime power and let $q = \ell^r$, where $2 \leq r \in \mathbb{N}$. Let

$$m = \frac{q-1}{\ell-1} = 1 + \ell + \ldots + \ell^{r-1}.$$

Then the equation

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

defines a recursive tower $\mathcal{T}$ over $\mathbb{F}_q$ with

$$\lambda(\mathcal{T}) \geq \frac{2}{q-2} > 0.$$

The tower $\mathcal{T}_1$ over $\mathbb{F}_4$ is obtained by taking $\ell = r = 2$.