Towers of function fields and examples of optimal tame towers

Unit 26

Gil Cohen

January 19, 2025

Overview

Towers of function fields

Definition 1

Let q be a prime power. A tower of function fields over $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (\mathrm{F}_0, \mathrm{F}_1, \ldots)$ of function fields $\mathrm{F}_i/\mathbb{F}_q$ s.t.

1. $\forall i \geq 0 \quad \mathrm{F}_i \subsetneq \mathrm{F}_{i+1}$;
2. $\forall i \geq 0 \quad \mathrm{F}_{i+1}/\mathrm{F}_i$ is finite and separable;
3. $g_i \triangleq g(\mathrm{F}_i) \to \infty$ as $i \to \infty$.

Recall that a prime divisor $\mathfrak{p} \in \mathbb{P}(\mathrm{E}/\mathrm{K})$ is rational if

$$\deg \mathfrak{p} \triangleq [\mathrm{E}_{\mathfrak{p}} : \mathrm{K}] = 1.$$

We denote by $n_i \triangleq \mathrm{N}(\mathrm{F}_i)$ the number of rational prime divisors of F_i.

Claim 2

Item 3 follows by items 1,2 and by $g_j \geq 2$ for some $j \geq 0$.

Proof.

By Hurwitz Genus Formula, for all $i \geq 0$,

$$g_{i+1} - 1 \geq [\mathsf{F}_{i+1} : \mathsf{F}_i](g_i - 1)$$

Since $g_j \geq 2$ and $[\mathsf{F}_{i+1} : \mathsf{F}_i] \geq 2$ we have

$$g_{j+1} \geq 2(g_j - 1) + 1 \geq 3,$$
$$g_{j+2} \geq 2(g_{j+1} - 1) + 1 \geq 5.$$

In particular, by induction one can show that $g_{i+1} > g_i$ for $i \geq j$. □

Towers of function fields

Claim 3

Let $\mathcal{F} = (\mathsf{F}_0, \mathsf{F}_1, \ldots)$ be a tower over $\mathbb{F}_q$. Then,

1. The sequence
$$\left(\frac{n_i}{[\mathsf{F}_i : \mathsf{F}_0]} \right)_{i \in \mathbb{N}}$$
is monotonically decreasing and so it is convergent.
2. The sequence
$$\left(\frac{g_i - 1}{[\mathsf{F}_i : \mathsf{F}_0]} \right)_{i \in \mathbb{N}}$$
is monotonically increasing and so it is convergent in $\mathbb{R} \cup \{\infty\}$.
3. Let j be s.t. $g_j \geq 2$. Then the sequence
$$\left(\frac{n_i}{g_i - 1} \right)_{i \geq j}$$
is monotonically decreasing and so it is convergent.

Towers of function fields

Proof.

Fix an extension F_{i+1}/F_i. Under a rational prime divisor $\mathfrak{p}_{i+1}$ of F_{i+1} there is a rational prime divisor $\mathfrak{p}_i$ of F_i. Indeed,

$$\deg \mathfrak{p}_{i+1} = f(\mathfrak{P}_{i+1}/\mathfrak{P}_i) \deg \mathfrak{p}_i$$

and so $\deg \mathfrak{p}_{i+1} \implies \deg \mathfrak{p}_i = 1$.

On the other hand, by the fundamental equality, there are at most $[F_{i+1} : F_i]$ rational prime divisors of F_{i+1} lying over a rational prime divisor of F_i, and so

$$n_{i+1} \leq [F_{i+1} : F_i] \cdot n_i.$$

Thus,

$$\frac{n_{i+1}}{[F_{i+1} : F_0]} \leq \frac{[F_{i+1} : F_i]}{[F_{i+1} : F_0]} \cdot n_i = \frac{n_i}{[F_i : F_0]}.$$

This establishes Item 1.

Towers of function fields

Proof.

Moving on to Item 2, by Hurwitz Genus Formula,

$$g_{i+1} - 1 \geq [\mathsf{F}_{i+1} : \mathsf{F}_i](g_i - 1).$$

Dividing by $[\mathsf{F}_{i+1} : \mathsf{F}_0]$ we get

$$\begin{aligned} \frac{g_{i+1} - 1}{[\mathsf{F}_{i+1} : \mathsf{F}_0]} &\geq \frac{[\mathsf{F}_{i+1} : \mathsf{F}_i]}{[\mathsf{F}_{i+1} : \mathsf{F}_0]}(g_i - 1) \\ &= \frac{g_i - 1}{[\mathsf{F}_i : \mathsf{F}_0]}, \end{aligned}$$

as desired.

Item 3 follows by Items 1,2.

Towers of function fields

Given Claim 3, the following definition makes sense.

Definition 4

Let $\mathcal{F} = (F_0, F_1, \dots)$ be a tower over $\mathbb{F}_q$.

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
$$\lambda(\mathcal{F}) = \lim_{i \to \infty} \frac{n_i}{g_i} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}$$

Towers of function fields

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

Definition 5

A tower $\mathcal{F}$ is asymptotically good if $\lambda(\mathcal{F}) > 0$. Otherwise, $\mathcal{F}$ is asymptotically bad.

Note that

$$\mathcal{F} \text{ is asymptotically good} \iff \nu(\mathcal{F}) > 0 \ \ \& \ \ \gamma(\mathrm{F}) < \infty.$$

Overview

Ihara's constant

How good can a tower over $\mathbb{F}_q$ be? Namely, what is

$$\mathrm{T}(q) = \sup_{\mathcal{F}} \lambda(\mathcal{F}),$$

where the supremum is taken over all towers $\mathcal{F}$ over $\mathbb{F}_q$?

One can ask a more general question. For an integer $g \geq 0$ let

$$\mathsf{N}_q(g) = \max \{\mathsf{N}(\mathsf{F}) \mid \mathsf{F}/\mathbb{F}_q \text{ is a function field with genus } g\}.$$

Serre proved the bound

$$\mathsf{N}_q(g) \leq q + 1 + g\lceil 2\sqrt{q}\rceil$$

(improving upon the Hasse-Weil celebrated bound $q + 1 + 2g\sqrt{q}$), and so $\mathsf{N}_q(g)$ is well-defined.

Ihara's constant

$$\begin{aligned} N_q(g) &= \max\{N(F) \mid F/\mathbb{F}_q \text{ is a function field with genus } g\} \\ &\leq q + 1 + g\lceil 2\sqrt{q}\rceil. \end{aligned}$$

Ihara's constant is defined by

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

By Serre's bound,

$$0 \leq A(q) \leq \lceil 2\sqrt{q}\rceil.$$

The Drinfeld-Vladut bound sharpens the upper bound to $\sqrt{q} - 1$.

The quantity $A(q)$ is called Ihara's constant.

Ihara's constant

Ihara's constant is defined by

$$\mathrm{A}(q) = \limsup_{g\to\infty} \frac{\mathsf{N}_q(g)}{g}.$$

By the Drinfeld-Vladut bound,

$$0 \le \mathrm{A}(q) \le \sqrt{q} - 1.$$

Interestingly, the Drinfeld-Vladut bound is tight for every q which is an even power of a prime. This was first proved by Ihara (1981) and by Tsfasman, Vladut and Zink (1982) using modular curves.

Garcia and Stichtenoth gave an alternative, more explicit, proof, establishing in fact that

$$\mathrm{T}(q) \ge \sqrt{q} - 1$$

for such q-s. To the best of my knowledge, for q a non-square, the exact value of $\mathrm{A}(q)$ is unknown, though, $\mathrm{A}(q) = \Omega(\log q)$.

Ihara's constant

Definition 6

A tower $\mathcal{F}$ over $\mathbb{F}_q$ is said to be asymptotically optimal if

$$\lambda(\mathcal{F}) = \mathrm{A}(q) = \sqrt{q} - 1.$$

Personally, I find this terminology confusing as it may be that asymptotically optimal towers do not exist when sticking to the above definition.

Overview

The ramification and splitting loci of a tower

For a function field E/K we let $\mathbb{P}_1(E/K)$ be the set of rational prime divisors of E/K.

Let F/L be a function field extension of E/K. A prime divisor $\mathfrak{p}$ of E/K is said to split completely if there are exactly [F : E] prime divisors of F/L lying over $\mathfrak{p}$.

Recall that by the fundamental equality,

$$[F : E] = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}),$$

there can be at most [F : E] prime divisors lying over $\mathfrak{p}$. Moreover, if $\mathfrak{p}$ splits completely then

$$\forall \mathfrak{P}/\mathfrak{p} \quad e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1.$$

In particular, if $\mathfrak{p}$ is rational then so is $\mathfrak{P}$ as recall

$$\deg \mathfrak{P} = f(\mathfrak{P}/\mathfrak{p}) \cdot \deg \mathfrak{p}.$$

The ramification and splitting loci of a tower

Definition 7

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

$$\mathrm{Split}(\mathcal{F}) = \{\mathfrak{p} \in \mathbb{P}_1(\mathrm{F}_0) \mid \mathfrak{p} \text{ splits completely in all extesnions } \mathrm{F}_i/\mathrm{F}_0\}$$

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 8

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

$$\mathrm{Ram}(\mathcal{F}) = \{\mathfrak{p} \in \mathbb{P}(\mathrm{F}_0) \mid \mathfrak{p} \text{ is ramified in } \mathrm{F}_i/\mathrm{F}_0 \text{ for some } i \geq 1\}$$

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

Note that Split($\mathcal{F}$) is finite (and may be empty). Ram($\mathcal{F}$) may be finite or infinite.

The ramification and splitting loci of a tower

Claim 9

Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$ with $s = |\mathrm{Split}(\mathcal{F})|$. Then,

$$\nu(\mathcal{F}) \geq s.$$

Proof.

Fix $\mathfrak{p} \in \mathrm{Split}(\mathcal{F})$ and $i \geq 0$. In F_i, there are exactly $[\mathrm{F}_i : \mathrm{F}_0]$ rational prime divisors lying over $\mathfrak{p}$. Thus,

$$n_i \geq [\mathrm{F}_i : \mathrm{F}_0] \cdot s$$

and so

$$\nu(\mathcal{F}) = \lim_{i \to \infty} \frac{n_i}{[\mathrm{F}_i : \mathrm{F}_0]} \geq s.$$

□

The ramification and splitting loci of a tower

Claim 10

Let $\mathcal{F}$ be a tower over $\mathbb{F}_q$. Assume that $\mathrm{Ram}(\mathcal{F})$ is finite and that

$$\forall \mathfrak{p} \in \mathrm{Ram}(\mathcal{F}) \quad \exists a_{\mathfrak{p}} \in \mathbb{R} \quad \forall i \geq 0,\ \mathfrak{P} \in \mathbb{P}(\mathrm{F}_i) \qquad d(\mathfrak{P}/\mathfrak{p}) \leq a_{\mathfrak{p}} \cdot e(\mathfrak{P}/\mathfrak{p}).$$

Then,

$$\gamma(\mathcal{F}) \leq g_0 - 1 + \frac{1}{2} \sum_{\mathfrak{p} \in \mathrm{Ram}(\mathcal{F})} a_{\mathfrak{p}} \cdot \deg \mathfrak{p} < \infty.$$

Proof.

By the Hurwitz Genus Formula,

$$\begin{aligned} 2g_i - 2 &= [\mathrm{F}_i : \mathrm{F}_0](2g_0 - 2) + \deg \mathrm{Diff}(\mathrm{F}_i/\mathrm{F}_0) \\ &= [\mathrm{F}_i : \mathrm{F}_0](2g_0 - 2) + \sum_{\mathfrak{p} \in \mathbb{P}(\mathrm{F}_0)} \sum_{\mathfrak{P}/\mathfrak{p}} d(\mathfrak{P}/\mathfrak{p}) \cdot \deg \mathfrak{P} \\ &\leq [\mathrm{F}_i : \mathrm{F}_0](2g_0 - 2) + \sum_{\mathfrak{p} \in \mathbb{P}(\mathrm{F}_0)} \sum_{\mathfrak{P}/\mathfrak{p}} a_{\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{p}. \end{aligned}$$

The ramification and splitting loci of a tower

Proof.

$$2g_i - 2 \leq [F_i : F_0](2g_0 - 2) + \sum_{\mathfrak{p} \in \mathbb{P}(F_0)} \sum_{\mathfrak{P}/\mathfrak{p}} a_{\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{p}$$

$$= [F_i : F_0](2g_0 - 2) + \sum_{\mathfrak{p} \in \mathbb{P}(F_0)} a_{\mathfrak{p}} \deg \mathfrak{p} \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}).$$

Using the fundamental equality we get

$$2g_i - 2 \leq [F_i : F_0] \left(2g_0 - 2 + \sum_{\mathfrak{p} \in \mathbb{P}(F_0)} a_{\mathfrak{p}} \deg \mathfrak{p} \right),$$

and so

$$\frac{g_i}{[F_i : F_0]} \leq g_0 - 1 + \frac{1}{2} \sum_{\mathfrak{p} \in \mathbb{P}(F_0)} a_{\mathfrak{p}} \deg \mathfrak{p} + \frac{1}{[F_i : F_0]}.$$

The proof follows by taking the limit and using that $[F_i : F_0] \to \infty$.

The ramification and splitting loci of a tower

Corollary 11

Let $\mathcal{F}$ be a tower as in Claim 10. Assume that $s = |\mathrm{Split}(\mathcal{F})| > 0$. Then, $\mathcal{F}$ is asymptotically good, and we have

$$\lambda(\mathcal{F}) \geq \frac{2s}{2g_0 - 2 + \sum_{\mathfrak{p} \in \mathrm{Ram}(\mathcal{F})} a_{\mathfrak{p}} \deg \mathfrak{p}}.$$

Proof.

The proof readily follows by Claim 9, Claim 10 and since

$$\lambda(\mathcal{F}) = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}.$$

□

The ramification and splitting loci of a tower

Definition 12

A tower $\mathcal{F}$ over $\mathbb{F}_q$ is celled tame if all ramification indices $e(\mathfrak{P}/\mathfrak{p})$, $\mathfrak{p} \in \mathbb{P}(\mathsf{F}_0)$, $\mathfrak{P} \in \mathbb{P}(\mathsf{F}_i)$ are coprime to q (equivalently, to the $p = \operatorname{char} \mathbb{F}_q$.)

Corollary 13

Let $\mathcal{F}$ be a tame tower with $\mathsf{F}_0 = \mathbb{F}_q(x)$ and

$$s = |\mathrm{Split}(\mathcal{F})| > 0 \qquad r = \sum_{\mathfrak{p} \in \mathrm{Ram}(\mathcal{F})} \deg \mathfrak{p}.$$

Then,

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

Proof.

The proof readily follows by Corollary 11 and by Dedekind's Different Theorem which states that $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$ for tame towers.

Tower properties via ramification

Claim 14

Let $\mathsf{F}_0 \subseteq \mathsf{F}_1 \subseteq \cdots$ be a sequence of finite separable field extensions. Assume $\mathsf{F}_0/\mathbb{F}_q$ is a function field, and denote the constant field of F_i by K_i. Suppose that

$$\forall i \geq 0 \quad \exists \mathfrak{p}_i \in \mathbb{P}(\mathsf{F}_i), \mathfrak{P}_i \in \mathbb{P}(\mathsf{F}_{i+1}) \quad s.t. \quad \mathfrak{P}_i/\mathfrak{p}_i \text{ and } e(\mathfrak{P}_i/\mathfrak{p}_i) > 1.$$

Then, $\mathsf{F}_i \neq \mathsf{F}_{i+1}$.

Moreover, if in the above notation $e(\mathfrak{P}_i/\mathfrak{p}_i) = [\mathsf{F}_{i+1} : \mathsf{F}_i]$ for all i then $\mathsf{K}_i = \mathbb{F}_q$.

Proof.

By the fundamental equality, $e(\mathfrak{P}_i/\mathfrak{p}_i) \leq [\mathsf{F}_{i+1} : \mathsf{F}_i]$ and so

$$e(\mathfrak{P}_i/\mathfrak{p}_i) > 1 \quad \Longrightarrow \quad \mathsf{F}_{i+1} \neq \mathsf{F}_i.$$

We move to the moreover part.

Tower properties via ramification

Proof.

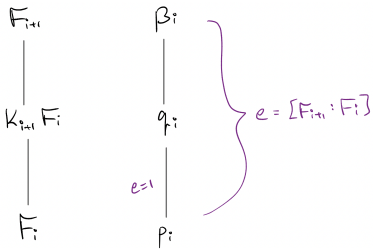
Consider the constant field extension $K_{i+1}F_i/K_{i+1}$. We have that

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

Let $\mathfrak{q}_i \in \mathbb{P}(K_{i+1}F_i)$ be the prime divisor lying under $\mathfrak{P}_i$. Then,

$$e(\mathfrak{P}_i/\mathfrak{p}_i) = e(\mathfrak{P}_i/\mathfrak{q}_i) \cdot e(\mathfrak{q}_i/\mathfrak{p}_i) = e(\mathfrak{P}_i/\mathfrak{q}_i),$$

where the last equality holds as ramification does not occur in constant field extensions.



Tower properties via ramification

Proof.

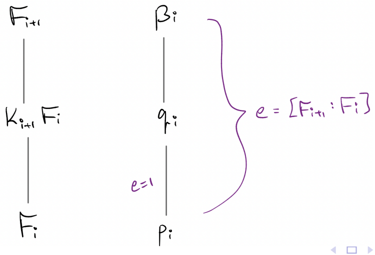
$$e(\mathfrak{P}_i/\mathfrak{q}_i) = [\mathsf{F}_{i+1} : \mathsf{K}_{i+1}\mathsf{F}_i] \cdot [\mathsf{K}_{i+1}\mathsf{F}_i : \mathsf{F}_i].$$

But by the fundamental equality,

$$e(\mathfrak{P}_i/\mathfrak{q}_i) \leq [\mathsf{F}_{i+1} : \mathsf{K}_{i+1}\mathsf{F}_i],$$

and so

$$\mathsf{K}_{i+1}\mathsf{F}_i = \mathsf{F}_i \quad \Longrightarrow \quad \mathsf{K}_{i+1} = \mathsf{K}_i$$



Overview

Recursive towers

Let K be a field. We define the degree of an element

$$f(T) = \frac{g(T)}{h(T)} \in \mathrm{K}(T)$$

with $g(T), h(T) \in \mathrm{K}[T]$ coprime by

$$\deg(f) = \max(\deg(g), \deg(h)).$$

Note that this is well-defined as $\mathrm{K}[T]$ is a UFD.

Note that $f(T)$ is constant $(f(T) \in \mathrm{K})$ iff $\deg(f) = 0$.

Recursive towers

Definition 15

Let $f(Y) \in \mathbb{F}_q(Y)$, $h(X) \in \mathbb{F}_q(X)$ be non-constant rational functions, and let $\mathcal{F} = (\mathrm{F}_0, \mathrm{F}_1, \ldots)$ be a sequence of function fields over $\mathbb{F}_q$.

Suppose that $\forall i \in \mathbb{N}\ \exists x_i \in \mathrm{F}_i$ s.t.

1. $\mathrm{F}_0 = \mathbb{F}_q(x_0)$ is a rational function field (namely, x_0 is transcendental over $\mathbb{F}_q$);
2. $\mathrm{F}_i = \mathbb{F}_q(x_0, x_1, \ldots, x_i)$;
3. $f(x_{i+1}) = h(x_i)$; and
4. $[\mathrm{F}_1 : \mathrm{F}_0] = \deg(f)$.

Then, we say that $\mathcal{F}$ is recursively defined over $\mathbb{F}_q$ by the equation

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

We call the function field $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ with $f(y) = h(x)$ the basic function field of the tower.

Recursive towers

Note that in a recursive tower,

$$\forall i \in \mathbb{N} \quad [\mathrm{F}_{i+1} : \mathrm{F}_i] \leq \deg(f).$$

Indeed, write $f(T) = f_1(T)/f_2(T)$ where $f_1(T), f_2(T) \in \mathbb{F}_q[T]$ are coprime. By Item 2,

$$\mathrm{F}_{i+1} = \mathrm{F}_i(x_{i+1}),$$

and by Item 3, x_{i+1} is a root of

$$g(T) = f_1(T) - h(x_i)f_2(T) \in \mathrm{F}_i[T]$$

whose degree is

$$\deg(g) \leq \max(\deg(f_1), \deg(f_2)) = \deg(f).$$

Thus,

$$[\mathrm{F}_{i+1} : \mathrm{F}_i] \leq \deg(g) \leq \deg(f).$$

Overview

Example

Let q be a power of an odd prime. We will show that the sequence $\mathcal{F} = (\mathrm{F}_0, \mathrm{F}_1, \dots)$ that is recursively defined by

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

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

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

As

$$\mathrm{F}_{i+1} = \mathrm{F}_i(x_{i+1}) \quad \text{and} \quad x_{i+1}^2 = \frac{x_i^2 + 1}{2x_i},$$

we have that $[\mathrm{F}_{i+1} : \mathrm{F}_i] \leq 2$. As q is odd, by the theory of Kummer extensions, $\mathrm{F}_{i+1}/\mathrm{F}_i$ is separable. This establishes Item 2.

Example

To prove Items 1,3 using Claim 14 we will find, for each $i \in \mathbb{N}$

$$\mathfrak{p}_i \in \mathbb{P}(\mathsf{F}_i),\, \mathfrak{P}_i \in \mathbb{P}(\mathsf{F}_{i+1}) \quad \text{s.t.} \quad \mathfrak{P}_i/\mathfrak{p}_i \quad \text{and} \quad e(\mathfrak{P}_i/\mathfrak{p}_i) = 2.$$

Let $\mathfrak{p}_0$ be the unique pole of x_0 in $\mathsf{F}_0 = \mathbb{F}_q(x_0)$. Let $\mathfrak{P}_0/\mathfrak{p}_0$ in $\mathbb{P}(\mathsf{F}_1)$. We have that

$$2 \cdot \upsilon_{\mathfrak{P}_0}(x_1) = \upsilon_{\mathfrak{P}_0}(x_1^2) = e(\mathfrak{P}_0/\mathfrak{p}_0) \cdot \upsilon_{\mathfrak{p}_0}\left(\frac{x_0^2+1}{2x_0}\right) = -e(\mathfrak{P}_0/\mathfrak{p}_0).$$

Thus, using also the fundamental equality, $e(\mathfrak{P}_0/\mathfrak{p}_0) = 2$ as desired.

Moreover, note that $\upsilon_{\mathfrak{P}_0}(x_1) = -1$ and so we can iterate this argument for all $i \in \mathbb{N}$.

Example

It remains to prove Item 4. By the result on tame cyclic extensions, the only prime divisors of F_0 that ramify are

- $\mathfrak{p}_0$ - the zero of x_0 in F_0.
- $\mathfrak{p}_\infty$ - the unique pole of x_0 in F_0 as

  $$d = \gcd\left(n, \sum_{i=1}^{s} n_i \deg p_i(x)\right) = \gcd(2, 2-1) = \gcd(2, 1+1-1) = 1;$$

  and
- either the prime divisor corresponding to $x_0^2 + 1$ in case it is irreducible in $\mathbb{F}_q[x_0]$ or the two prime divisors that correspond to its two distinct irreducible factors $x + i, x - i$.

Assume that $x_0^2 + 1$ is irreducible in $\mathbb{F}_q[x_0]$ (the other case is treated similarly and gives the same result).

Example

By a result we proved, the three prime divisors totally ramify, namely have ramification index $e = 2$.

As q is odd, Dedekind different theorem implies that the different exponent is $d = e - 1 = 1$.

Moreover, by the fundamental equality, each of the three prime divisors have a unique prime divisor lying above it and the corresponding residual degree $f = 1$. Thus,

$$\deg \mathrm{Diff}(\mathsf{F}_1/\mathsf{F}_0) = \sum_{\mathfrak{p} \in \mathbb{P}(\mathsf{F}_0)} \sum_{\mathfrak{P}/\mathfrak{p} \in \mathbb{P}(\mathsf{F}_1)} d(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{P}$$
$$= 1 \cdot 2 + 1 \cdot 1 + 1 \cdot 1 = 4.$$

Note that in the case that $x_0^2 + 1$ is reducible the answer is also 4.

Example

Recall Hurwitz Genus Formula for an extension F/L over E/K

$$2g_{\mathsf{F}} - 2 = \frac{[\mathsf{F} : \mathsf{E}]}{[\mathsf{L} : \mathsf{K}]} \cdot (2g_{\mathsf{E}} - 2) + \deg \mathrm{Diff}(\mathsf{F}/\mathsf{E}).$$

In our case,

$$2g_1 - 2 = \frac{2}{1} \cdot (2 \cdot 0 - 2) + 4 = 0,$$

and so $g_1 = 1$.

Example

Recall Hurwitz Genus Formula for an extension F/L over E/K

$$2g_{\mathsf{F}} - 2 = \frac{[\mathsf{F} : \mathsf{E}]}{[\mathsf{L} : \mathsf{K}]} \cdot (2g_{\mathsf{E}} - 2) + \deg \mathrm{Diff}(\mathsf{F}/\mathsf{E}),$$

and that $g_1 = 1$. Thus,

$$2g_2 - 2 = \frac{2}{1} \cdot (2g_1 - 2) + \deg \mathrm{Diff}(\mathsf{F}_2/\mathsf{F}_1) = \deg \mathrm{Diff}(\mathsf{F}_2/\mathsf{F}_1).$$

We proved that the prime divisor $\mathfrak{P}_0$ of F_1 lying above $\mathfrak{p}_0$ totally ramifies. In particular, $\deg \mathrm{Diff}(\mathsf{F}_2/\mathsf{F}_1) \geq 1$ and so

$$2g_2 - 2 \geq 1,$$

which implies $g_2 \geq 2$, concluding the proof of Item 4.

Overview

Splitting locus in recursive towers

Claim 16

Let $\mathcal{F} = (\mathsf{F}_0, \mathsf{F}_1, \ldots)$ be a recursive tower over $\mathbb{F}_q$ which is defined by the equation

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

and let $\mathsf{F} = \mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ be the basic function field of the tower.

Assume that

$$\exists \emptyset \neq \Sigma \subseteq \mathbb{F}_q \cup \{\infty\} \quad \text{s.t.} \quad \forall \alpha \in \Sigma,$$

1. $\mathfrak{p}_{x-\alpha}$ splits completely in F.
2. $\forall \mathfrak{P} \in \mathbb{P}(\mathsf{F})$ that lies over $\mathfrak{p}_{x-\alpha}$ it holds that $y(\mathfrak{P}) \in \Sigma$.

Then,

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

In particular,

$$\nu(\mathcal{F}) \geq |\Sigma|.$$

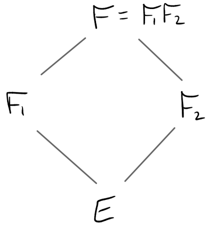
Splitting locus in recursive towers

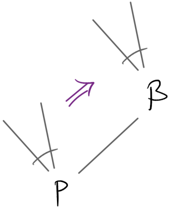
For the proof we will need the following result which, for lack of time, I am forced to omit (see Stichtenoth; Proposition 3.9.6). We will cover the result in the seminar part of the course.

Lemma 17

Let F/K *be a finite separable extension of* E/K. *Assume that* $\mathsf{F} = \mathsf{F}_1\mathsf{F}_2$ *where* $\mathsf{E} \subseteq \mathsf{F}_1, \mathsf{F}_2$.

Suppose that $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$ *splits completely in* F_1/E. *Then, every* $\mathfrak{P} \in \mathbb{P}(\mathsf{F}_2)$ *that lies over* $\mathfrak{p}$ *splits completely in* F/F_2.





Proof. (Proof of Claim 16)

Fix $\alpha \in \Sigma$. We show by induction on i that $\mathfrak{p}_{x_0-\alpha}$ splits completely in $\mathsf{F}_i/\mathsf{F}_0$.

The base case $i = 1$ follows per our assumption and since

$$\begin{aligned} \mathsf{F}_1/\mathsf{F}_0 &= \mathbb{F}_q(x_0, x_1)/\mathbb{F}_q(x_0) \\ &\cong \mathbb{F}_q(x, y)/\mathbb{F}_q(x). \end{aligned}$$

For the induction step, it suffices to prove that every $\mathfrak{P} \in \mathbb{P}(\mathsf{F}_i)$ that lies over $\mathfrak{p}_{x_0-\alpha}$ splits completely in $\mathsf{F}_{i+1}/\mathsf{F}_i$.

By an iterative application of Item 2,

$$\beta \triangleq x_i(\mathfrak{P}) \in \Sigma.$$

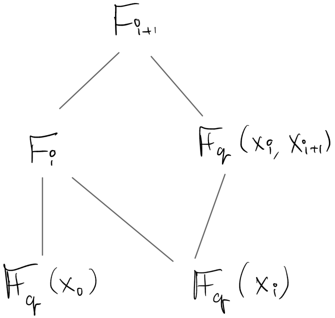
Splitting locus in recursive towers

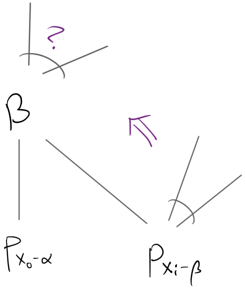
Proof.

$$\beta \triangleq x_i(\mathfrak{P}) \in \Sigma.$$

Thus, by Item 1, $\mathfrak{p}_{x_i-\beta}$ splits completely in $\mathbb{F}_q(x_i, x_{i+1})/\mathbb{F}_q(x_i)$.

Hence, by Lemma 17, using that $\mathrm{F}_{i+1} = \mathbb{F}_q(x_{i+1})\mathrm{F}_i$, we have that $\mathfrak{P}$ splits completely in $\mathrm{F}_{i+1}/\mathrm{F}_i$. □





Splitting locus in recursive towers

Corollary 18

Let $\mathcal{F} = (\mathsf{F}_0, \mathsf{F}_1, \ldots)$ *be a recursive tower over* $\mathbb{F}_q$ *that is defined by*

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

Let $m = \deg f(Y)$*. Assume that* $\Sigma \subseteq \mathbb{F}_q$ *satisfies the following:* $\forall \alpha \in \Sigma$

1. $h(\alpha) \neq \infty$ *(equivalently,* $v_{\mathfrak{p}_{x-\alpha}}(h(x)) \geq 0$*); and*
2. $f(t) = h(\alpha)$ *has* m *distinct solutions (for* t*) in* Σ*.*

Then,

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

Splitting locus in recursive towers

Proof.

Let $\mathsf{F} = \mathbb{F}_q(x, y)$ be the basic function field of the tower, namely,

$$f(y) = h(x).$$

Fix $\alpha \in \Sigma$ and let $\mathfrak{p} = \mathfrak{p}_{x-\alpha} \in \mathbb{P}(\mathbb{F}_q(x))$.

Write

$$f(Y) = \frac{f_1(Y)}{f_2(Y)} = \frac{a_m Y^m + \cdots + a_0}{b_m Y^m + \cdots + b_0},$$

with $f_1(Y), f_2(Y) \in \mathbb{F}_q[Y]$ coprime. As $\deg f(Y) = m$, not both $a_m, b_m = 0$.

Splitting locus in recursive towers

Proof.

As $f(y) = h(x)$, y is a root of the polynomial

$$g(Y) = f_1(Y) - h(x)f_2(Y) \in \mathbb{F}_q(x)[Y].$$

Per our assumption, $h(\alpha) \neq \infty$ and the polynomial

$$g_\alpha(Y) = f_1(Y) - h(\alpha)f_2(Y) \in \mathbb{F}_q[Y]$$

has m distinct roots. Thus, $\deg g_\alpha = m$ and so the leading coefficient of $g_\alpha(Y)$,

$$a_m - h(\alpha)b_m \neq 0.$$

Thus,

$$a_m - h(x)b_m \in \mathcal{O}_{\mathfrak{p}}^\times.$$

Splitting locus in recursive towers

Proof.

$$a_m - h(x)b_m \in \mathcal{O}_{\mathfrak{p}}^{\times},$$

and so

$$\frac{g(Y)}{a_m - h(x)b_m} \in \mathcal{O}_{\mathfrak{p}}[Y]$$

is a monic polynomial, establishing that $\alpha \in \mathcal{O}'_{\mathfrak{p}}$.

If we denote the distinct roots of $g_\alpha(Y)$ by $\beta_1, \ldots, \beta_m$, where recall

$$g_\alpha(Y) = \text{ the reduction of } g(Y) \text{ modulo } \mathfrak{m}_{\mathfrak{p}},$$

then, Kummer's Theorem implies that in F, above $\mathfrak{p}$ there are m distinct prime divisors $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ s.t. $y(\mathfrak{P}_i) = \beta_i$.

Per our assumption $\beta_1, \ldots, \beta_m \in \Sigma$ and the proof follows by Claim 16. □

Example continued

Consider again the recursive tower over $\mathbb{F}_9 = \mathbb{F}_3(\delta)$, $\delta^2 = -1$, that is given by

$$f(Y) = Y^2 = \frac{X^2+1}{2x} = h(X).$$

It can be verified that

$$\Sigma = \{a + b\delta \mid a, b \in \{1,2\}\}$$

satisfies the condition of Corollary 18. Indeed, take for example $1+\delta$.

$$(1+\delta)^2 = 2\delta, \qquad \frac{1}{2+2\delta} = 1+2\delta.$$

Hence,

$$h(1+\delta) = \frac{(1+\delta)^2+1}{2(1+\delta)} = (2\delta+1)(1+2\delta) = \delta,$$

and the solutions to $t^2 = \delta$ are $1+2\delta$, $2+\delta$, both are in Σ.

Thus, by Corollary 18, $\nu(\mathcal{F}) \geq |\Sigma| = 4$.

Overview

Ramification in recursive towers

Lemma 19

Let $\mathcal{F} = (\mathsf{F}_0, \mathsf{F}_1, \ldots)$ *be a recursive tower over* $\mathbb{F}_q$ *defined by the equation*

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

with a basic function field F*. Assume that every prime divisor of* $\mathbb{F}_q(x)$ *that ramifies is rational, in particular,*

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

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

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

Ramification in recursive towers

We make a small remark before proving Lemma 19.

Say F/L is an extension of E/K. Take $\mathfrak{P} \in \mathbb{P}(F)$ that lies over $\mathfrak{p} \in \mathbb{P}(E)$.

Take $x \in \mathcal{O}_{\mathfrak{p}}$. Then $x \in \mathcal{O}_{\mathfrak{P}}$ and

$$x(\mathfrak{P}) = x(\mathfrak{p}).$$

Indeed,

$$x(\mathfrak{p}) = x + \mathfrak{m}_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}} \Big/ \mathfrak{m}_{\mathfrak{p}} \hookrightarrow \mathcal{O}_{\mathfrak{P}} \Big/ \mathfrak{m}_{\mathfrak{P}},$$
$$x(\mathfrak{P}) = x + \mathfrak{m}_{\mathfrak{P}} \in \mathcal{O}_{\mathfrak{P}} \Big/ \mathfrak{m}_{\mathfrak{P}},$$

where the embedding maps $x + \mathfrak{m}_{\mathfrak{p}} \mapsto x + \mathfrak{m}_{\mathfrak{P}}$.

Ramification in recursive towers

We will need the following lemma which will be covered in the seminar part of the course.

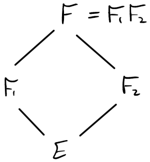
Lemma 20 (Abhyankar's Lemma)

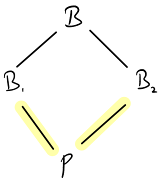
Let F/L *be a finite separable extension of* E/K. *Let* $\mathsf{F}_1/\mathsf{L}_1$, $\mathsf{F}_2/\mathsf{L}_2$ *be extensions of* E/K *s.t.* $\mathsf{F} = \mathsf{F}_1\mathsf{F}_2$.

Let $\mathfrak{P} \in \mathbb{P}(\mathsf{F})$ *a prime divisor lying over* $\mathfrak{p} \in \mathbb{P}(\mathsf{E})$. *Let* $\mathfrak{P}_1, \mathfrak{P}_2$ *be the prime divisors lying under* $\mathfrak{P}$ *in* $\mathbb{P}(\mathsf{F}_1), \mathbb{P}(\mathsf{F}_2)$, *respectively.*

If one of $\mathfrak{P}_1/\mathfrak{p}$, $\mathfrak{P}_2/\mathfrak{p}$ *is tame then*

$$e(\mathfrak{P}/\mathfrak{p}) = \mathrm{lcm}\left(e(\mathfrak{P}_1/\mathfrak{p}), e(\mathfrak{P}_2/\mathfrak{p})\right).$$



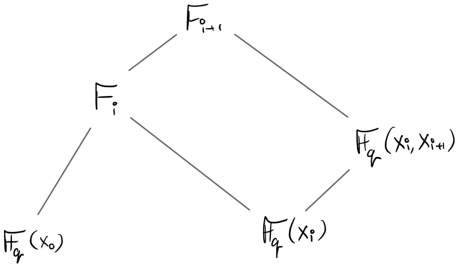


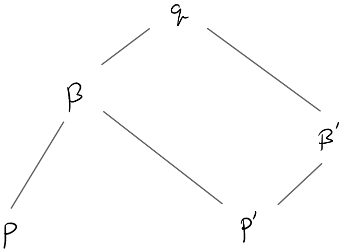
Ramification in recursive towers

Proof. (Proof of Lemma 19)

Take $\mathfrak{p} \in \mathbb{P}(\mathbb{F}_q(x_0))$ which ramifies in $\mathcal{F}$. We wish to prove $x_0(\mathfrak{p}) \in \Lambda$.

Let $i \geq 0$ and $\mathfrak{P} \in \mathbb{P}(\mathrm{F}_i)$ be a prime divisor lying over $\mathfrak{p}$ which ramifies in $\mathrm{F}_{i+1}/\mathrm{F}_i$.





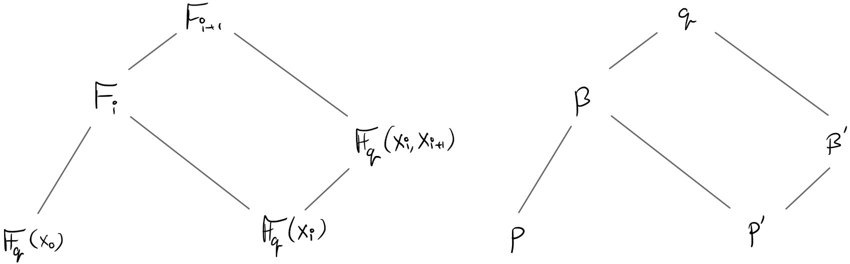
Ramification in recursive towers

Proof.

By Abhyankar's Lemma, $\mathfrak{p}'$ ramifies in $\mathbb{F}_q(x_i, x_{i+1})/\mathbb{F}_q(x_i)$. Indeed, otherwise $e(\mathfrak{P}'/\mathfrak{p}') = 1$ and so we can apply the lemma and get

$$e(\mathfrak{q}/\mathfrak{p}') = \text{lcm}\left(e(\mathfrak{P}/\mathfrak{p}'), e(\mathfrak{P}'/\mathfrak{p}')\right) = e(\mathfrak{P}/\mathfrak{p}')$$

which contradicts $e(\mathfrak{q}/\mathfrak{P}) > 1$.



Ramification in recursive towers

Proof.

As $\mathfrak{p}'$ ramifies in $\mathbb{F}_q(x_i, x_{i+1})/\mathbb{F}_q(x_i)$,

$$\beta_i \triangleq x_i(\mathfrak{p}') \in \Lambda_0.$$

By the remark, $\beta_i = x_i(\mathfrak{P})$. Thus, if we denote

$$\beta_j \triangleq x_j(\mathfrak{P}) \qquad j = i, \dots, 0$$

then

$$f(\beta_j) = f(x_j(\mathfrak{P})) = h(x_{j-1}(\mathfrak{P})) = h(\beta_{j-1}),$$

and so, per our assumption on Λ,

$$\beta_i \in \Lambda_0 \subseteq \Lambda \quad \Longrightarrow \quad \beta_{i-1} \in \Lambda \quad \Longrightarrow \quad \cdots \quad \Longrightarrow \quad \beta_0 \in \Lambda.$$

The proof then follows since

$$\beta_0 = x_0(\mathfrak{P}) = x_0(\mathfrak{p}).$$

Overview

Example continued

Consider again the recursive tower over $\mathbb{F}_9 = \mathbb{F}_3(\delta)$, $\delta^2 = -1$, that is given by

$$f(Y) = Y^2 = \frac{X^2+1}{2X} = \frac{(X-\delta)(X+\delta)}{2X} = h(X).$$

As this is a Kummer extension, the only prime divisors that ramify are those that correspond to

$$\Lambda_0 = \{0, \pm\delta, \infty\}.$$

We claim that, with the notation of Lemma 19,

$$\Lambda = \Lambda_0 \cup \{\pm 1\}.$$

Indeed, consider first $\beta = 0$. The solutions to

$$0 = f(0) = f(\beta) = h(\alpha) = \frac{(\alpha-\delta)(\alpha+\delta)}{2\alpha}$$

are $\pm\delta \in \Lambda$.

Example continued

$$f(Y) = Y^2 = \frac{X^2+1}{2X} = \frac{(X-\delta)(X+\delta)}{2X} = h(X).$$

$$\Lambda_0 = \{0, \pm\delta, \infty\} \qquad \Lambda = \Lambda_0 \cup \{\pm 1\}.$$

For $\beta = \pm\delta$, the solution to

$$-1 = (\pm\delta)^2 = f(\beta) = h(\alpha) = \frac{\alpha^2+1}{2\alpha},$$

namely to

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

is $-1 \in \Lambda$.

Example continued

$$f(Y) = Y^2 = \frac{X^2+1}{2X} = \frac{(X-\delta)(X+\delta)}{2X} = h(X).$$

$$\Lambda_0 = \{0, \pm\delta, \infty\} \qquad \Lambda = \Lambda_0 \cup \{\pm 1\}.$$

Similarly, for $\beta = \pm 1$, the solution to

$$1 = (\pm 1)^2 = f(\beta) = h(\alpha) = \frac{\alpha^2+1}{2\alpha},$$

namely, to

$$\alpha^2 - 2\alpha + 1 = (\alpha - 1)^2$$

is $1 \in \Lambda$.

Example continued

$$f(Y) = Y^2 = \frac{X^2+1}{2X} = \frac{(X-\delta)(X+\delta)}{2X} = h(X).$$

$$\Lambda_0 = \{0, \pm\delta, \infty\} \qquad \Lambda = \Lambda_0 \cup \{\pm 1\}.$$

Lastly is $\beta = \infty$ (recall the arithmetic rules involving ∞) the solution to

$$\infty = \infty^2 = f(\infty) = h(\alpha) = \frac{\alpha^2+1}{2\alpha},$$

are

$$\alpha = 0, \infty.$$

Both are in Λ.

Example continued

Recall Corollary 13 which states that in a tame tower $\mathcal{F}$ with $\mathsf{F}_0 = \mathbb{F}_q(x)$, with

$$s = |\mathsf{Split}(\mathcal{F})| \qquad r = \sum_{\mathfrak{p} \in \mathsf{Ram}(\mathcal{F})} \deg \mathfrak{p},$$

it holds that

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

By Lemma 19,

$$\mathsf{Ram}(\mathcal{F}) \subseteq \{0, \infty, \pm\delta, \pm 1\}$$

and so $r \leq 6$.

By a previous calculation we did, $s \geq 4$, and so

$$\lambda(\mathcal{F}) \geq \frac{2 \cdot 4}{6-2} = 2 = \sqrt{9} - 1 = \mathrm{A}(9),$$

and so this is an optimal tower over $\mathbb{F}_9$.

Example continued

In fact, the recursive tower that is given by

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

is optimal over any field $\mathbb{F}_q$ with q an even power of an odd prime.

The analysis we did for the ramification locus remains as is. Indeed, note that as $q = p^2$, where p is a power of an odd prime,

$$|\mathbb{F}_q^\times| = p^2 - 1 = (p+1)(p-1) \quad \Longrightarrow \quad 4 \mid |\mathbb{F}_q^\times|,$$

and so there is an element δ of order 4 in $\mathbb{F}_q$, namely, $\delta^2 = -1$.

Therefore $r \leq 6$ and so

$$\lambda(\mathcal{F}) \geq \frac{2s}{6-2} = \frac{s}{2}.$$

Example continued

The difficult part is to show that

$$s = |\mathrm{Split}(\mathcal{F})| = 2(p-1).$$

This will establish that $\mathcal{F}$ is optimal since then

$$\lambda(\mathcal{F}) \geq \frac{s}{2} = p - 1 = \sqrt{q} - 1 = \mathrm{A}(q).$$

The key to achieve this is to consider the Deuring polynomial

$$H_p(X) = \sum_{m=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{m}^2 \cdot X^m.$$

E.g.,

$$H_3(X) = 1 + X,$$
$$H_5(X) = 1 + 4X + X^2,$$
$$H_7(X) = 1 + 9X + 9X^2 + X^3.$$

Example continued

$$H_p(X) = \sum_{m=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{m}^2 \cdot X^m.$$

As it turns out, the Deuring polynomial satisfies

$$H_p(X^4) = X^{p-1} \cdot H_p\left(\left(\frac{X^2+1}{2X}\right)^2\right).$$

E.g.,

$$\begin{aligned} X^2 \cdot H_3\left(\left(\frac{X^2+1}{2X}\right)^2\right) &= X^2 \cdot \left(1 + \left(\frac{X^2+1}{2X}\right)^2\right) \\ &= X^2 + \frac{1}{4} \cdot (X^4 + 2X^2 + 1) \\ &= 1 + X^4 \\ &= H_3(X^4). \end{aligned}$$

Example continued

$$H_p(X) = \sum_{m=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{m}^2 \cdot X^m.$$

As it turns out, the Deuring polynomial satisfies

$$H_p(X^4) = X^{p-1} \cdot H_p\left(\left(\frac{X^2+1}{2X}\right)^2\right).$$

Using the above equation it can be checked that

$$\Lambda_0 = \{\alpha \in \overline{\mathbb{F}_p} \mid H_p(\alpha^4) = 0\} \subseteq \mathbb{F}_{p^2},$$

and that Λ_0 satisfies Lemma 19 and, moreover that H_p is separable. Hence,

$$|\Lambda_0| = 4 \cdot \frac{p-1}{2} = 2(p-1).$$

Example continued

To prove the equation

$$H_p(X^4) = X^{p-1} \cdot H_p\left(\left(\frac{X^2+1}{2X}\right)^2\right)$$

one uses Gauss's hypergeometric differential equation which is outside the scope of this course. See, e.g., the paper "Asymptotically good towers and differential equations" by Beelen and Bouw.