

Cubic Function Fields in Characteristic 3

Mark Bauer*

* Joint work with Jonathan Webster

University of Calgary
Department of Mathematics & Statistics
Centre for Information Security and Cryptography

May 12, 2008

Motivation?

Fun things to do with curves and function fields:

- 1 Cryptography.
 - 1 Efficient arithmetic on the Jacobian.
 - 2 Difficulty of the Discrete Log Problem.
- 2 Calculating invariants.
 - 1 Class numbers.
 - 2 Regulators.
 - 3 Genus.

Generic Curves in Characteristic 3

For $A, B, C \in \mathbb{F}_q[x]$, define an affine curve by

$$C : y^3 + Ay^2 + By + C = 0.$$

If $A \neq 0$, we can do a transformation to get:

$$C : y^3 + Ay^2 + C = 0.$$

The polynomial discriminant of this equation is $D = -A^3C$.

Because we hate/love cubes in char. 3, we'll instead deal with:

$$C : y^3 + y^2 + F = 0 \quad F \in \mathbb{F}_q[x].$$

Function Fields

Two perspectives/definitions:

- 1 $\mathbb{F}_q(C) = \text{Hom}_{\mathbb{F}_q}(C, \mathbb{P}_{\mathbb{F}_q}^1)$
- 2 Rational maps (i.e. rational functions in two variables) defined over \mathbb{F}_q from the curve to \mathbb{F}_q .

For our curve:

$$\mathbb{F}_q(C) \cong \mathbb{F}_q(x)[y]/\langle y^3 + y^2 + f \rangle$$

- Curves are really classified by their function fields, not how we write them down.

Ring of Regular Functions

Definition

The Ring of Regular Functions of C is a subring $\mathbb{F}_q(C)$ composed of all function that do not have a pole at any of the (finite) points of C , and is denoted $\mathbb{F}_q[C]$.

$\mathbb{F}_q[C]$ is the integral closure of $\mathbb{F}_q[x]$ in $\mathbb{F}_q(C)$.

Note: It is a Dedekind Domain.

Things we need to know:

- integral basis
- field discriminant (aka ramification)
- ideal decomposition
- ideal arithmetic

Polynomial Discriminant vs. Field Discriminant

Field Discriminant - holds information about ramification in $\mathbb{F}_q[C]$ over $\mathbb{F}_q[x]$ (norm of the different).

- Polynomial Discriminant: $-F$.
- Field Discriminant (of $\mathbb{F}_q(C)/\mathbb{F}_q(x)$): $\Delta \in \mathbb{F}_q[x]$.

How do they relate?

$F = I^2\Delta$ for some polynomial $I \in \mathbb{F}_q[x]$.

So, given F , can we determine I and Δ ?

- Equivalent to knowing about ramification in $\mathbb{F}_q[C]$ over $\mathbb{F}_q[x]$.

Determining Ramification

Integral basis for the ring of regular functions:

$$\mathbb{F}_q[C] = \langle 1, y, \frac{y^2 + y}{I} \rangle = \langle 1, \rho, \omega \rangle .$$

Kummer's Theorem

Look at our defining equation modulo the various irreducibles in $\mathbb{F}_q[x]$ to determine splitting behavior. (sort of)

Note:

$y^3 + y^2 + F$ is NEVER a pure cube!

⇒ There is no total ramification at the finite places (i.e. no wild ramification!).

- Hence Δ is square free, and all we do is write $F = I^2\Delta$, with Δ being squarefree.
- This is why we take $A = 1$.

Prime decomposition

- 1 $u|\Delta$ then $(u) = \mathfrak{p}q^2$.
- 2 $u|I, u \nmid \Delta$:
 - If $\Delta \equiv \square \pmod{u}$ then $(u) = \mathfrak{p}q\mathfrak{r}$.
 - Otherwise $(u) = \mathfrak{p}q$, where q has inertial degree 2.
- 3 $u \nmid F$:
 - $y^3 + y^2 + F$ has one root modulo u , then $(u) = \mathfrak{p}q$ where q has inertial degree 2.
 - $y^3 + y^2 + F$ has three roots modulo u , then $(u) = \mathfrak{p}q\mathfrak{q}$.
 - $y^3 + y^2 + F$ has no roots modulo u , then $(u) = \mathfrak{p}$ where \mathfrak{p} has inertial degree 3.

Note: To determine the splitting behavior of the bad primes ($u|I$), we look at the splitting behavior for the minimal polynomial of ω which is $y^3 + \Delta y + I\Delta$.

Definition

The *signature* of the $\mathbb{F}_q(C)$ over $\mathbb{F}_q(x)$ is $(e_1, f_1, \dots, e_s, f_s)$, where s is the number of places lying above infinity, and e_i is the ramification and f_i the inertial degree of the i^{th} place.

- $\sum e_i f_i = [\mathbb{F}_q(C) : \mathbb{F}_q(x)] = 3.$

Obvious questions:

- 1 How many places lie above infinity?
- 2 What are their ramification/inertial degree?

Note: If we can find one place with ramification or inertial degree greater than 1, everything is determined. We also either have inertia or ramification, but NOT both.

Behavior at Infinity

To figure out the splitting at infinity, we look at the completion of $\mathbb{F}_q(x)$ at the infinite place: $\mathbb{F}_q \langle x^{-1} \rangle$.

- # of roots of $y^3 + y^2 + F$ in $\mathbb{F}_q \langle x^{-1} \rangle$ corresponds to # of places of degree 1.
- # of roots of $y^3 + y^2 + F$ in $\mathbb{F}_{q^2} \langle x^{-1} \rangle$ corresponds to # of places of degree 2 (excluding the roots found above).
- # of roots of $y^3 + y^2 + F$ in $\mathbb{F}_{q^3} \langle x^{-1} \rangle$ corresponds to # of places of degree 3 (excluding the roots found above).

Approach: low-tech. Write out a generic Laurent series for y and see if you can solve for the coefficients.

$$y = \sum_{i=n}^{-\infty} a_i x^i$$

Corollary

If $3 \nmid \deg F$, we have total (wild) ramification at infinity.

To NOT have total (wild) ramification, we need:

- $3 \mid \deg F$.
- Top $1/3$ of coefficients of F to be 0 unless the exponent is divisible by 3.
- A miracle to occur between the $2/3$ mark and $1/2$ (i.e. $1/6$ of the coefficients)

$$6 \mid \deg F$$

- Total ramification.
- Complete splitting.
- Full inertia.
- Partial splitting with inertia.

$$6 \nmid \deg F$$

- Total ramification.
- Partial splitting with ramification.

Consequence of Behavior at Infinity

Two things that are greatly affected by the behavior at infinity:

- Unit rank of $\mathbb{F}_q[C]$.
 - Unit rank of $\mathbb{F}_q[C]$ is given by $s - 1$ where s is the number of places at infinity.
- Genus of C .
 - Calculate using Hurwitz genus formula

$$2g - 2 = [\mathbb{F}_q(C) : \mathbb{F}_q(x)](-2) + \deg \text{Diff}(F' : F).$$

- Determine the degree of the different using ramification information.

Two objects of interest:

- 1 $Pic_{\mathbb{F}_q}^0(C)$ “is” the Jacobian of C .
- 2 $Cl(\mathbb{F}_q[C])$ is the ideal class group of $\mathbb{F}_q[C]$.

We almost always have total ramification - meaning we have unit rank 0.

In this case, we get a nice isomorphism:

$$Pic_{\mathbb{F}_q}^0(C) \cong Cl(\mathbb{F}_q[C])$$

Doing computations on the Jacobian becomes equivalent to performing ideal arithmetic.

CONTENT OMITTED FOR YOUR SANITY

Goal: Determine $\deg \text{Diff}(\mathbb{F}_q(C)/\mathbb{F}_q(x))$

Easy Case: No wild ramification.

- \mathcal{P} has ramification degree e , then it contributes $(e - 1) \deg \mathcal{P}$ to $\deg \text{Diff}(\mathbb{F}_q(C)/\mathbb{F}_q(x))$.

Corollary

The finite places contribute $\deg \Delta$. The infinite place contributes 0 or 1 to $\deg \text{Diff}(\mathbb{F}_q(C)/\mathbb{F}_q(x))$.

$\deg F \equiv 0 \pmod{3}$ and not totally ramified at infinity

$\deg F \equiv 0 \pmod{2}$:

$$g = \frac{\deg \Delta - 4}{2}$$

$$g = \frac{\deg \Delta}{2} - 2$$

$\deg F \equiv 1 \pmod{2}$:

$$g = \frac{\deg \Delta + 1 - 4}{2}$$

$$g = \frac{\deg \Delta + 1}{2} - 2$$

Goal: Determine $\deg \text{Diff}(\mathbb{F}_q(C)/\mathbb{F}_q(x))$

Hard Case: Wild ramification.

- \mathcal{P} has ramification degree 3, then it contributes $d_{\mathcal{P}} \deg \mathcal{P}$ to $\deg \text{Diff}(\mathbb{F}_q(C)/\mathbb{F}_q(x))$.
- $d_{\mathcal{P}}$ is some “random” number.

Lemma

The finite places contribute $\deg \Delta$ and the infinite place contributes $\deg F + 2$ (when $\deg F \not\equiv 0 \pmod{3}$) or $\deg F$ (otherwise) to $\deg \text{Diff}(\mathbb{F}_q(C)/\mathbb{F}_q(x))$.

Infinity wildly ramified

$\deg F \not\equiv 0 \pmod{3}$:

$$g = \frac{\deg \Delta + \deg F + 2 - 4}{2}$$

$$g = \deg \Delta + \deg l - 1$$

$\deg F \equiv 0 \pmod{3}$ *:

$$g = \frac{\deg \Delta + \deg f - 4}{2}$$

$$g = \deg \Delta + \deg l - 2$$

- Remove the $*$ from the previous page.
- Implementation.
- Consider more general curves in characteristic 3.
- Arithmetic for unit rank larger than 0.