A DRINFELD MODULAR INTERPRETATION OF AN ASYMPTOTICALLY OPTIMAL TOWER OF CURVES OVER FINITE FIELDS

by
TÜRKÜ ÖZLÜM ÇELIK

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
Fall 2014

A DRINFELD MODULAR INTERPRETATION OF AN ASYMPTOTICALLY OPTIMAL TOWER OF CURVES OVER FINITE FIELDS

APPROVED BY:

Assoc. Prof. Dr. Cem Güneri
(Thesis Supervisor)

Asst. Prof. Dr. Kağan Kurşungöz

Prof. Dr. Henning Stichtenoth

Prof. Dr. Alev Topuzoğlu

Assoc. Prof. Dr. Hüsnü Yenigün

DATE OF APPROVAL: 05.01.2015

THE DRINFELD MODULAR INTERPRETATION OF AN ASYMPTOTICALLY OPTIMAL TOWER OF CURVES

Türkü Özlüm Çelik

Mathematics, MSc Thesis, 2014

Thesis Supervisor: Assoc. Prof. Cem Güneri

Abstract

In this thesis, we study a Drinfeld modular interpretation due to Elkies of an asymptotically optimal tower that was constructed by Bezerra and Garcia.

We explain what an asymptotically optimal tower over a finite field $\mathbb{F}_q$ is and give the definition of the asymptotically optimal tower given by Bezerra and Garcia.

We give some basic facts about Drinfeld modules. Additionally, we present the analytical theory of Drinfeld modules using lattices and exponential functions to better understand the analogy with the classical theory.

We exhibit the Drinfeld modular curves that give the tower of Bezerra and Garcia. Hence we see a Drinfeld modular interpretation of this tower.

ASİMTOTİK OLARAK OPTİMAL BİR EĞRİ KULESİNİN DRINFELD MODÜLER YORUMU

Türkü Özlüm Çelik

Matematik, Yüksek Lisans Tezi, 2014

Tez Danışmanı: Assoc. Prof. Cem Güneri

Özet

Bu tezde, Bezerra ve Garcia tarafından verilmiş asimptotik olarak optimal bir $\mathbb{F}_q$-fonksiyon cisim kulesinin Drinfeld moduler eğrilerle inşasını inceledik.

İlk bölümde $\mathbb{F}_q$ üzerinde asimptotik olarak optimal bir fonksiyon cismi kulesinin ne demek olduğunu anlattık. Bölümün sonunda Drinfeld modüler eğrilerle yorumunu göreceğimiz, Bezerra ve Garcia tarafından inşa edilmiş fonksiyon cisim kulesinin tanımını verdik.

İkinci bölümde Drinfeld modülleri hakkında ihtiyacımız olan bilgileri derledik. Ek olarak, Drinfeld modüllerin, klasik teorideki eliptik eğrilerle benzerliğini resmettik.

Son bölümde ise, özel birtakım Drinfeld modüler eğrilerin hesabını yaptık. Bahsi geçen fonksiyon cismi kulesinin Drinfeld modüler eğriler kullanarak inşasının nasıl olacağını anlattık.

Anahtar Kelimeler: asimptotik olarak optimal, fonksiyonel cisim kuleleri, Drinfeld modülleri, modül, modüler eğri.

Table of Contents

CHAPTER 1

Introduction

In this thesis, the main object is an asymptotically optimal tower given by Bezerra–Garcia. The notion of an asymptotically optimal tower will be introduced in this chapter.

Let $\mathbb{F}_q$ be a finite field of characteristic p with q elements. Let F be an algebraic function field over $\mathbb{F}_q$ of one variable. Suppose that the constant field of F is $\mathbb{F}_q$. Let $N(F)$ be the number of rational places of F. The theorem of Hasse–Weil [13] gives the bound

$$N(F) \leq q + 1 + 2\sqrt{q}g \tag{1.1}$$

where g denotes the genus of F. Serre [12] improved this upper bound by replacing $2\sqrt{q}$ by $\lfloor 2\sqrt{q} \rfloor$. Ihara [10] realized that over a fixed finite field $\mathbb{F}_q$, the Hasse–Weil upper bound becomes weak when the genus g of F is large. He introduced the quantity

$$A(q) = \limsup_{g(F)\to\infty} \frac{N(F)}{g(F)}$$

where F runs over all function fields with constant field $\mathbb{F}_q$. By the Hasse–Weil theorem, we have $A(q) \leq 2\sqrt{q}$. Ihara [10] proved that $A(q) \leq \sqrt{2q}$ for any q. This indicates that the Hasse–Weil bound can be improved for large genera, as stated above. The best known upper bound due to Drinfeld and Vlăduţ [4] gives

$$A(q) \leq \sqrt{q} - 1$$

for any prime power q. If q is square then Ihara proved that $A(q) \geq \sqrt{q} - 1$ [10]. Hence $A(q) = \sqrt{q} - 1$ when q is square. For any prime power q, Serre [12] showed that $A(q) > c \log_2(q)$ for some $c > 0$. In particular, $A(q) > 0$ for any q. If $q = p^{3m}$ for a positive integer m then we have

$$A(q) \geq \frac{2(p^{2m} - 1)}{p^m + 2}. \tag{1.2}$$

This lower bound was obtained by Zink [14] in the case where $m = 1$. Bezerra, Garcia and Stichtenoth [3] generalized this lower bound for any m by using recursive towers of function fields.

There are many other lower bounds for $A(p^n)$, with a prime p and an odd power $n > 3$, however they seem not to be particularly strong. One of them [11] is

$$A(q^n) \geq \frac{4q+4}{\lfloor \frac{3+\lfloor 2\sqrt{2q+2} \rfloor}{n-2} \rfloor + \lfloor 2+\sqrt{2q+3} \rfloor}$$

where q is an odd prime power and $n \geq 3$ is prime. This was given by Li and Maharaj.

With the purpose of investigating $A(q)$ Garcia and Stichtenoth introduced the notion of towers of $\mathbb{F}_q$-function fields.

Definition 1.0.1 *A tower of over $\mathbb{F}_q$ is an infinite sequence of function fields F_i over $\mathbb{F}_q$*

$$\mathcal{F} = (F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots \subseteq F_i \subseteq \dots)$$

such that the following hold;

(i) $F_1 \subsetneq \cdots \subsetneq F_i \subsetneq \dots$;

(ii) each extension F_{i+1}/F_i is finite and separable;

(iii) the genera satisfy $g(F_i) \to \infty$ for $i \to \infty$.

By the Hurwitz genus formula the limit

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}$$

exists [6]. Clearly $0 \leq \lambda(\mathcal{F}) \leq A(q)$ for any $\mathbb{F}_q$-tower $\mathcal{F}$. Hence towers are useful to obtain good lower bounds for $A(q)$.

Definition 1.0.2 *A tower $\mathcal{F}$ over $\mathbb{F}_q$ is called asymptotically optimal if $\lambda(\mathcal{F}) = A(q)$.*

Definition 1.0.3 *An $\mathbb{F}_q$-tower of function fields $\mathcal{F} = (F_1 \subseteq F_2 \subseteq \cdots \subseteq F_i \subseteq \dots)$ is recursively defined by $f(X,Y) \in \mathbb{F}_q[X,Y]$ if*

(i) $F_1 = \mathbb{F}_q(x_1)$ is the rational function field

(ii) $F_{i+1} = F_i(x_{i+1})$ with $f(x_i, x_{i+1}) = 0$ for all $i \geq 1$.

According to a result by Garcia and Stichtenoth [6], for $q = p^{2m}$ the $\mathbb{F}_q$-tower of function fields $\mathcal{F}_1$ recursively defined by

$$f(X,Y) = (1 + X^{p^m-1})(Y^{p^m} + Y) - X^{p^m} \tag{1.3}$$

is asymptotically optimal i.e. $\lambda(\mathcal{F}_1) = p^m - 1$.

When $q = p^{3m}$ one can use the polynomial

$$f(X,Y) = Y^{p^m}(X^{p^m} + X + 1) - X(1-Y) \in \mathbb{F}_q[X,Y]$$

to obtain a tower $\mathcal{F}_2$ with

$$\lambda(\mathcal{F}) \geq 2(p^{2m}-1)/(p^m+2).$$

This is how Inequality (1.2) is proved. The case $q = 2$ reduces to a tower that was introduced by van der Geer and van der Vlugt [8].

On the other hand, a lower bound given by Bassa, Beelen, Garcia and Stichtenoth [1] is rather close to the Drinfeld–Vlăduţ upper bound $A(p^n)$ for large n and small p. It is obtained by using recursive towers given by explicit polynomials $f(X, Y) \in \mathbb{F}[X, Y]$. The lower bound they obtain is

$$A(p^n) \geq \frac{2(p^{m+1}-1)}{p+1+\epsilon} \quad \text{where} \quad \epsilon = \frac{p-1}{p^m-1}$$

for a prime number p and an odd integer $n = 2m + 1 \geq 3$.

In my thesis, I study a Drinfeld modular interpretation of a tower that is constructed by Bezerra and Garcia [2]. The tower is defined over quadratic finite fields $\mathbb{F}_{q^2}$. It is defined as follow;

Definition 1.0.4 *Let the tower $\mathcal{F}$ be defined recursively by $F_1 := \mathbb{F}_{q^2}(x_1)$. For each $n \geq 1$, we have that $F_{n+1} := F_n(x_{n+1})$ with*

$$\frac{x_{n+1}-1}{x_{n+1}^q} = \frac{x_n^q - 1}{x_n}. \tag{1.4}$$

This tower over $\mathbb{F}_{q^2}$ attains the Drinfeld–Vlăduţ bound [2] i.e.

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

In the second chapter, I introduce Drinfeld modules. I present an important example of Drinfeld modules, which is the Carlitz module. At the end of that chapter, I briefly describe the analogy between Drinfeld modules and elliptic curves over complex numbers. In the third chapter, I compute the Drinfeld modular curves that form the tower in Definition 1.0.4. For this computation, I first compute another Drinfeld modular tower, from which I obtain the tower (1.4) by using Drinfeld modular curves.

CHAPTER 2

Drinfeld Modules

2.1 Additive Polynomials

Let k be a field of positive characteristic p. Let $\bar{k}$ be a fixed algebraic closure.

Definition 2.1.1 *We say that $P(X) \in k[X]$ is additive over k if*

$$P(\alpha + \beta) = P(\alpha) + P(\beta)$$

for all α, $\beta \in k$. We say that $P(X)$ is absolutely additive if $P(X)$ is additive over $\bar{k}$.

Example 2.1.1 *The polynomial $\tau_p(X) := X^p$ is absolutely additive.*

Proposition 2.1.1 *Let $P(X)$, $Q(X)$ be additive polynomials over k. Then*

1. *$P(X) + Q(X)$ is additive over k,*
2. *For all $\alpha \in k$, $\alpha P(X)$ is additive over k,*
3. *$P(Q(X))$ is additive over k.*

Proof: This follows immediately from the definitions. □

Remark: Let $\tau_p^i(X) := X^{p^i}$ for $i \in \mathbb{N}$. Any element of the set of polynomials generated by $\{X^{p^i} : i \in \mathbb{N}\}$ over k is absolutely additive by Proposition 2.1.1.

Definition 2.1.2 *We define $k\{\tau_p\}$ as the k vector space that is generated $\{X^{p^i} : i \in \mathbb{N}\}$.*

The vector space $k\{\tau_p\}$ is a ring under usual addition and composition. If $k \neq \mathbb{F}_p$ then $k\{\tau_p\}$ is noncommutative. Note that, $\tau_p \alpha = \alpha^p \tau_p$ for all $\alpha \in k$.

Example 2.1.2 *Let $k = \mathbb{F}_5$ and*

$$P(X) = X + (X^5 - X)^2 = X^{10} + 3X^3 + X^2 + X.$$

So $P(\alpha) = \alpha$ for all $\alpha \in k$. $P(X)$ is additive over k. But $P(X) \notin k\{\tau_p\}$.

Proposition 2.1.2 *Suppose that k is an infinite field. A polynomial $P(X) \in k[X]$ is additive over k if and only if $P(X) \in k\{\tau_p\}$.*

Proof: Firstly, by Example 2.1.1 and Proposition 2.1.1 we have seen that if $P(X) \in k\{\tau_p\}$ then $P(X)$ is additive. For the converse, take $\alpha \in k$. Then

$$Q_\alpha(x) := P(x+\alpha) - P(x) - P(\alpha) = 0$$

for all $x \in k$. Since k is infinite, $Q_\alpha(X)$ is identically zero. Also

$$P'(\alpha) = \frac{d}{dx}P(x+\alpha)\Big|_{x=0} = \frac{d}{dx}(P(x)+P(\alpha))\Big|_{x=0} = P'(0).$$

Again by the infinitude of k,

$$P'(X) \equiv P'(0) \equiv c$$

for some $c \in k$. This means that

$$P(X) = cX + \sum_{i=2}^{k} a_i X^{n_i}$$

where $a_i \in k$ and $n_i \equiv 0 (\mathrm{mod} p)$ for all $i \in \{2, \ldots, k\}$. Now we write

$$P(X) = P_0(X) + P_1(X)$$

where $P_0(X) = cX +$terms with n_i's that are powers of p
and $P_1(X) =$ terms with n_i's that are divisible by a prime $\neq p$. We will show that $P_1(X) \equiv 0$.

Now, since $P_0(X) \in k\{\tau_p\}$, $P_1(X) = P(X) - P_0(X)$ is additive. It is sufficient to show that $P_1(X) \equiv 0$ in $\overline{k}[X]$. We know that $\tau_p : \overline{k} \to \overline{k}$ is an automorphism of $\overline{k}$. Let p^e be the largest power of p dividing all powers n_i's of terms of $P_1(X)$. Set $P_2(X) := P_1(X)^{1/p^e} \in \overline{k}[X]$. The mapping $\alpha \mapsto \alpha^{1/p^e}$ from k to $\overline{k}$ is additive (although it is not polynomial). Then $P_2(X)$ is also additive. Similarly as above, we see that $P_2'(X)$ is identically zero by using additivity of $P_2(X)$ on k. Because of the definition of $P_2(X)$, this means that $P_2(X)$ is identically zero. Hence $P_1(X) \equiv 0$. □

Corollary 2.1.3 *$k\{\tau_p\}$ is the set of absolutely additive polynomials over k.*

Proof: The algebraic closure of any field is infinite. □

Suppose that $q := p^m$ for a natural number m. Take any extension L of k. Let $L\{\tau\}$ be the ring of polynomials in τ by setting $\tau := \tau_p^m$. Now, $L\{\tau\}$ is a k-algebra of k-linear polynomials. Any element $f = l_0 + l_1\tau + \cdots + l_d\tau^d$ represents a k-linear endomorphism of L which is

$$x \mapsto l_0 x + l_1 x^q + \cdots + l_d x^{q^d}$$

2.2 Drinfeld Modules

2.2.1 The General Definition of a Drinfeld Module

The theory of Drinfeld modules was developed to use the ideas coming from lattices and their exponential functions in the function field setting in positive characteristic. This theory is an extension of Carlitz module to higher rank lattices. The Carlitz module behaves as the analogue of the multiplicative group $\mathbb{G}_m$ over $\mathbb{C}$. In more detail, Drinfeld modules come from A-lattices of rank r where A is the ring of functions on a curve over a finite field with poles at most at a fixed place, denoted ∞. (This is parallel to the fact that $\mathbb{Z}$-lattices of rank 2 give rise to elliptic curves over $\mathbb{C}$ in the classical theory.) In analogy to classical modular curves, which are parametrizing elliptic curves (together with some additional structure), one can consider Drinfeld modular curves, parametrizing analogous objects, namely Drinfeld modules.

Let k be a finite field with q elements of characteristic p. Let L be any extension of k. We fix an algebraic closure $\overline{L}$ of L. Set $A := k[T]$. Fix a k-algebra homomorphism $\iota : A \to L$. We call $\ker \iota$ the *characteristic* of L. Since L is a field, $\ker \iota$ is a prime ideal. We say that L has *generic characteristic* if $\ker \iota = (0)$ i.e. if ι is injective. Otherwise we say that $\ker \iota$ is *finite* and L has finite characteristic.

Let $D : L\{\tau\} \to L$ be the k-algebra homomorphism that is given by

$$D\left(\sum_{i=0}^{n} l_i \tau^i\right) = l_0$$

Definition 2.2.1 *A Drinfeld A-module over L is a k-algebra homomorphism*

$$\phi : A \to L\{\tau\}$$

with the following properties,

i. $D \circ \phi = \iota$,

ii. $\phi(a) \neq \iota(a)\tau^0$ *for some* $a \in A$.

First, we will use ϕ_a instead of $\phi(a)$.

Note that, since ϕ is a k-algebra homomorphism, it is determined by ϕ_T. Also, because of (i) the constant term of ϕ_a in τ is $\iota(a)$ for all $a \in A$.

We get an A-module structure on L by using ϕ. The action of A on L is given by

$$a.l = \phi_a(l)$$

for any $a \in A$, $l \in L$. We denote this module by $\phi(L)$. Similarly, we get another A-module structure on L by ι. The action is given as follows:

$$a.l := \iota(a)l.$$

Definition 2.2.1 (i) requires that this second action agrees with the lowest term of the action defined by ϕ. Definition 2.2.1 means (ii) that these two actions above are not the same. So the action defined by ϕ is a nontrivial deformation of the A-action on L given by the homomorphism ι.

Definition 2.2.2 *If $P{:=}a_0 + a_1\tau + \cdots + a_n\tau^n \in L\{\tau\}$ then the degree of P is defined as the largest exponent of τ appearing in P. It is denoted by* $\deg P$.

Definition 2.2.3 *If P is an additive polynomial over L then the kernel of P is defined as follows;*

$$\ker P = \{l \in \overline{L} : P(l) = 0\}.$$

Definition 2.2.4 *Let ϕ be a Drinfeld module over L as above. Since A is a principal ideal domain, if ι is not injective then* $\ker \iota = Aa_0$ *for some $a_0 \in A$. We say that ϕ is supersingular if*

$$\ker \phi_{a_0} = \{0\},$$

and ordinary otherwise.

Definition 2.2.5 *Let ϕ and ψ be two Drinfeld modules over L. A morphism from ϕ to ψ over L is an element $u \in L\{\tau\}$ with*

$$u \circ \phi_a = \psi_a \circ u \tag{2.1}$$

for all $a \in A$.

A nonzero morphism is called an isogeny.

Note that, since a Drinfeld module is a k-algebra homomorphism, $u \circ \phi_a = \psi_a \circ u$ holds for all $a \in A$ if and only if it holds for $a = T$.

Definition 2.2.6 *We say that ϕ and ψ are isomorphic over $\overline{L}$ if there exists $\lambda \in \overline{L}^\times$ such that (2.1) holds for $u = \lambda$.*

To define a special isogeny from a Drinfeld module ϕ, we need the following proposition:

Proposition 2.2.1 *Let $a' \in A$. Then $\phi_{a'}$ is an isogeny from ϕ to itself.*

Proof: Since ϕ is a k-algebra homomorphism,

$$\phi_{a'} \circ \phi_T = \phi_{a'T} = \phi_{Ta'} = \phi_T \circ \phi_{a'}.$$

Hence the result follows. □

Definition 2.2.7 *This isogeny in the Proposition 2.2.7 is called the multiplication by a' map. The elements of* $\ker \phi_{a'}$ *are called a'-torsion points (a'-division points) of the Drinfeld module ϕ.*

2.2.2 An Example of a Drinfeld Module

Let $K = k(T)$ and K_∞ be the ∞-adic completion of K. Let $\overline{K}_\infty$ be a fixed algebraic closure of K_∞ equipped with the canonical extension of the ∞-adic valuation. However, it is not complete. Let C_∞ be the completion of $\overline{K}_\infty$. The Carlitz module was defined by Leonard Carlitz. It is a k-algebra homomorphism

$$C : A \to C_\infty\{\tau\}$$

which is defined by $C_T := T + \tau$. So the Carlitz module is a Drinfeld module over C_∞ of rank 1. Also the ι map from A to C_∞ is just the inclusion map. It sends T to T.

The Carlitz module is the simplest of all Drinfeld modules. The Carlitz module can be understood in an elemantary way. At the same time, many ideas about Drinfeld modules already appear in theory of the Carlitz module. So the Carlitz module is perfect to understand the general theory. It also plays a central role for the class field theory of the rational function field K.

2.2.3 The Drinfeld Module Associated to a Lattice

At the beginning of this section, I have mentioned the analogy between the classical theory of elliptic curves and Drinfeld modules. To better understand the analogy with the classical theory, I try to present the analytical theory of Drinfeld modules using lattices and exponential functions in a concise and somewhat sketchy form. In that analytical part, proofs are sketched and references are given. The aim of this section is to present the similarities of the two theories.

Let k be a finite field of characteristic p with $q = p^m$ elements. We set $A := k[T]$. Let $K := k(T)$. Put K_∞ be the ∞-adic completion of K. Let $|\cdot|_\infty$ denote the absolute value on K_∞ that comes from the ∞-adic valuation. Fix an algebraic closure of K_∞, say $\overline{K}_\infty$. Let C_∞ be the completion of $\overline{K}_\infty$ with respect to the unique extension of the absolute value $|\cdot|_\infty$ to $\overline{K}_\infty$, which we will also denote by $|\cdot|_\infty$.

Definition 2.2.8 *An A-submodule Λ of C_∞ is called A-lattice if Λ is a discrete, finitely generated, torsion-free submodule of C_∞. The rank of Λ is its rank as a finitely generated torsion-free submodule of C_∞.*

Definition 2.2.9 *Let Λ be an A-lattice of C_∞. We define the associated lattice exponential function as follows:*

$$\exp_\Lambda(z) := z \prod_{0 \neq \lambda \in \Lambda} \Big(1 - \frac{z}{\lambda}\Big).$$

The discreteness of Λ guarantees the convergence of $\exp_\Lambda(z)$ for all $z \in C_\infty$. By considering partial products of $\exp_\Lambda(z)$ one can see that the Drinfeld exponential function

has an expansion of the form

$$\exp_\Lambda(z) = z + \sum_{i\geq 1} a_i z^{q^i} \quad \text{for} \quad a_i \in A.$$

So we have that

$$\exp_\Lambda(z_1 + cz_2) = \exp_\Lambda(z_1) + c\exp_\Lambda(z_2)$$

for all $c \in \mathbb{F}_q$. In addition,

$$\exp_{c\Lambda}(cz) = c\exp_\Lambda(z).$$

Moreover, $\exp_\Lambda$ is a group homomorphism from C_∞ onto itself. The kernel of $\exp_\Lambda$ is just Λ. Since the function $\exp_\Lambda$ is nonconstant and entire, it is surjective onto C_∞. Thus $\exp_\Lambda$ gives rise to an isomorphism from C_∞/Λ onto C_∞. Now take any two A-lattices $\Lambda_1 \subseteq \Lambda_2$ of the same rank. Then Λ_2/Λ_1 is a finite dimensional $\mathbb{F}_q$-vector space. Choose a set of coset representatives $\{\lambda_0 = 0, \lambda_1, \ldots, \lambda_{d-1}\}$ and set

$$P_{[\Lambda_2:\Lambda_1]}(z) := z\prod_{i=1}^{d-1}\left(1 - \frac{z}{\exp_{\Lambda_1}(\lambda_i)}\right).$$

Then $P_{[\Lambda_2:\Lambda_1]}(z)$ is an $\mathbb{F}_q$-linear polynomial in z and z is the lowest term of it. Since $\exp_{\Lambda_2}(z)$ and $P_{[\Lambda_2:\Lambda_1]}(z)$ have the same zeroes and the same derivative, they are equal.

When Λ_1, Λ_2 are two A-lattices of the same rank,

$$\exp_{\Lambda_2}(z) = P_{[\Lambda_2:c\Lambda_1]}(\exp_{c\Lambda_1}(cz)) = P_{[\Lambda_2:c\Lambda_1]}(c\exp_{\Lambda_1}(z))$$

as both sides have the same zeros and have the same derivatives. In particular, if we take $\Lambda_1 = \Lambda_2 = \Lambda$ and $a \in A$ then we can write

$$\exp_\Lambda(az) = \phi_\Lambda(a)exp_\Lambda(z) \quad \text{for} \quad \phi_\Lambda(a)(z) = P_{[\Lambda:a\Lambda]}(z)$$

where $\phi_\Lambda(a) = a\tau^0 + \text{higher order terms in } \tau \text{ lies in} C_\infty\{\tau\}$. Thus we have a function that is defined from A to C_∞,

$$\phi_\Lambda : A \to C_\infty\{\tau\}.$$

We have that,

$$\phi_\Lambda(a)\phi_\Lambda(b)\exp_\Lambda(z) = \exp_\Lambda(abz) = \phi_\Lambda(ab)\exp_\Lambda(z)$$

for a, $b \in A$. Also $a \mapsto \phi_\lambda(a)$ is additive. So ϕ_Λ is a ring homorphism. Therefore, we have an A-module structure on C_∞ by using ϕ_Λ. In addition we know that the degree of $\phi_\Lambda(a)(z)$ in z is $[\Lambda : a\Lambda] = q^{r\deg a}$. So the degree of ϕ_Λ in τ is r. Thus ϕ_Λ is a Drinfeld A-module of rank r.

Now we we see isogenies between Drinfeld modules in this context.

Definition 2.2.10 *Let Λ_1 and Λ_2 be two A-lattices of the same rank. A morphism from Λ_1 to Λ_2 is an element c of C_∞ with $c\Lambda_1 = \Lambda_2$. If the ranks of Λ_1 and Λ_2 are different, then we can allow $0 \in C_\infty$ to be a morphism.*

Proposition 2.2.2 *Let ϕ and ψ be two Drinfeld modules associated to lattices Λ_1 and Λ_2, respectively, of the same rank. Let $c \in C_\infty$ be a morphism from Λ_1 to Λ_2. Then via the isomorphisms*

$$\exp_{\Lambda_1} : C_\infty/\Lambda_1 \to \mathbb{C}_\infty \quad \textit{and} \quad \exp_{\Lambda_2} : C_\infty/\Lambda_2 \to C_\infty$$

the element $c \in C_\infty$ corresponds to a polynomial $P(\tau) := P_c(\tau) \in C_\infty$ with

$$P \circ \phi_{\Lambda_1}(a) = \psi_{\Lambda_2}(a) \circ P$$

for all $a \in A$.

Proof: We have that $c\Lambda_1 \subseteq \Lambda_2$. Then $c^{-1}\Lambda_2$ contains Λ_1. We know that $\exp_{\Lambda_2}(cz)$ is zero on $c^{-1}\Lambda_2$. Since $c^{-1}\Lambda_2$ and Λ_1 have the same rank, we get that $c^{-1}\Lambda_2/\Lambda_1$ is finite. Now set

$$P(z) := P_c(z) = cP_{[c^{-1}\Lambda_2:\Lambda_1]}(z).$$

$P(z)$ is $\mathbb{F}_q$-linear. In addition, the function $P(\exp_{\Lambda_1}(z))$ has a simple zero at each point of $c^{-1}\Lambda_2$ with derivative c. Therefore

$$P(\exp_{\Lambda_1}(z)) = \exp_{\Lambda_2}(cz).$$

□

Remark: Let Λ be a lattice that is associated to a Drinfeld module ϕ. The action of $a \in A$ via ϕ_a can be expressed by the commutative diagram

$$\begin{array}{ccc} C_\infty/\Lambda & \xrightarrow{a} & C_\infty/\Lambda \\ {\scriptstyle \exp_\Lambda}\downarrow & & \downarrow{\scriptstyle \exp_\Lambda} \\ C_\infty & \xrightarrow{\phi_{\Lambda(a)}} & C_\infty \end{array}$$

Similarly, if Λ_1 and Λ_1 are lattices with Drinfeld modules ϕ and ψ respectively and if $c \in C_\infty$ is a morphism from Λ_1 to Λ_2 then the morphism from ϕ to ψ associated to c is expressed by the following commutative diagram

$$\begin{array}{ccc} C_\infty/\Lambda_1 & \xrightarrow{c} & C_\infty/\Lambda_1 \\ {\scriptstyle \exp_{\Lambda_1}}\downarrow & & \downarrow{\scriptstyle \exp_{\Lambda_2}} \\ C_\infty & \xrightarrow{P_c} & C_\infty \end{array}$$

Theorem 2.2.3 *(Drinfeld's Uniformization Theorem) Suppose that ϕ is an A-Drinfeld module over C_∞ of rank r. If ι map of ϕ is inclusion then there is a unique A-lattice Λ such that such that $\phi_\Lambda = \phi$. Moreover,* $\mathrm{rk}_A\, \Lambda = r$

Proof: See [9]. □

CHAPTER 3

Explicit Towers of Drinfeld Modules

3.1 Some Basic Definitions for Drinfeld Modular Curves

In this section k is a finite field of size q and $\overline{k}$ is a fixed algebraic closure of k. Let k_1 be the unique quadratic extension of k in $\overline{k}$. Let L be any algebraically closed field that contains $\overline{k}$. We will consider Drinfeld Modules over L of rank 2. Let $A = k[T]$.

Let ϕ be a Drinfeld Module over L of rank 2. We know that ϕ is determined by ϕ_T. Let

$$\phi_T = l_0 + g\tau + \Delta\tau^2 \text{ with } \Delta \neq 0$$

Note that $l_0 = \iota(T)$, so l_0 is determined by ι. We say that ϕ is *normalized* if $\Delta = -1$.

Definition 3.1.1 *We define the J-invariant of ϕ as*

$$J(\phi) = \frac{g^{q+1}}{\Delta}.$$

Proposition 3.1.1 *Suppose that ρ and ψ are two Drinfeld modules of rank 2 with the same ι. They are isomorphic over L if and only if their J-invariants are equal. Moreover, every Drinfeld module ρ is isomorphic to a normalized one.*

Proof: Let us set ρ and ψ as follows,

$$\rho_T = \iota(T) + g_1\tau + \Delta_1\tau^2 \text{ and } \psi_T = \iota(T) + g_2\tau + \Delta_2\tau^2$$

where $\Delta_1, \Delta_2 \neq 0$.

Firstly, suppose that ρ and ψ are isomorphic. By Definition 2.2.6, there exist an element $\lambda \in L^\times$ such that $\rho_T \circ \lambda = \lambda \circ \psi_T$. So

$$\iota(T)\lambda + g_1\lambda^q\tau + \Delta_1\lambda^{q^2}\tau^2 = \lambda\iota(T) + \lambda g_2\tau + \lambda\Delta_2\tau^2.$$

This equality gives that,

$$g_1\lambda^q = \lambda g_2 \quad (*) \text{ and } \Delta_1\lambda^{q^2} = \lambda\Delta_2 \quad (**)$$

By taking $(q+1)$-st power of the both sides of the equality (*) and by looking at the ratio of (*) and (**), one can see that their J-invariants are the same.

Now, suppose that they have the same J-invariants. i.e.

$$\frac{g_1^{q+1}}{\Delta_1} = \frac{g_2^{q+1}}{\Delta_2}.$$

We try to find an element $\lambda \in L^\times$ such that

$$g_1\lambda^q = \lambda g_2 \text{ and } \Delta_1\lambda^{q^2} = \lambda\Delta_2.$$

Choose $\lambda \in L^\times$ such that $\lambda^{q-1} = g_2/g_1$. Then by using the equality for the J-invariants, one can see that $\lambda^{q^2-1} = \Delta_2/\Delta_1$. Therefore ρ and ψ are isomorphic.

For the final part, we will show that we can find a normalized Drinfeld module ψ of rank 2 with the same ι that is isomorphic to ρ. By the first part of the proposition, this means that we try to find a normalized Drinfeld module ψ such that the J-invariants of ψ and ρ are the same. Since L is algebraically closed, we can choose g_2 such that

$$\frac{g_1^{q+1}}{\Delta_1} = \frac{g_2^{q+1}}{-1}.$$

Proposition 3.1.2 *For any $j \in L$, there exists a normalized Drinfeld module ρ of rank 2 such that $J(\rho) = j$.*

Proof: Since L is algebraically closed, one can choose $g \in L$ and $\Delta \in L$ such that $\frac{g^{q+1}}{\Delta} = j$. Now, take

$$\rho : A \to L\{\tau\}$$

that is defined by $\rho_T = \Delta\tau^2 + g\tau + \iota(T)$. Then this Drinfeld module is the required one. □

Note that there is a normalized Drinfeld module in each of these isomorphism classes by Proposition 3.1.2. In fact all isomorphism classes contain exactly $q+1$ normalized Drinfeld modules, except the class containing the Drinfeld module $\tau^2 + g\tau + 1$ with $g = 0$, which contains only one normalized one.

Working with isomorphism classes is very cumbersome, so most of the time we will work with normalized Drinfeld modules.

From now on, we use Drinfeld modules that send T to $-\tau^2 + g\tau + 1$. Note that ι is defined by $\iota(T) = 1$.

Proposition 3.1.3 *Suppose that ϕ is a normalized Drinfeld module such that*

$$\phi_T = -\tau^2 + g\tau + \iota(T).$$

where $\iota(T) = 1$. Then

$$\ker \iota = \langle T - 1 \rangle.$$

Proof: Firstly; since $\iota(T) = 1$,

$$\iota(T-1) = \iota(T) - \iota(1) = 0.$$

Also, $\iota((T-1)P(T)) = 0$ for any $P(T) \in A$ because ι is a k-algebra homomorphism. Hence $\ker \iota = \langle T-1 \rangle$ □

Therefore, our Drinfeld modules have finite characteristic $T-1$.

3.2 Some Important Drinfeld Modular Curves

In this section we define some classical Drinfeld modular curves and exhibit equations for them. These curves will apriori be defined over the field L (so the function fields will have constant field L), but in all cases, they can already be defined over k.

3.2.1 $\mathbf{X(1)}$:

We have seen that isomorphism classes of Drinfeld modules are determined precisely by the J-invariant and that every $j \in L$ occurs as the J-invariant of an isomorphism class. We can think of these $j \in L$ as points on an affine line over L. So we have a line with coordinate given as j and each point corresponds to an isomorphism class of Drinfeld modules. The function field of this line will be given by $L(j)$. This affine line paramterizing isomorphism classes of Drinfeld modules is usually denoted by $Y(1)$. As is done customary, one adds a point at infinity to get a projective curve $X(1)$. The point at infinity does not really correspond to an isomorphism class, but can be interpreted as corresponding to some distorted object.

Definition 3.2.1 $X(1) := L \cup \{\infty\}$.

It turns out that there is natural way to identify isomorphism classes of Drinfeld modules of rank 2 with points on an algebraic curve. $X(1)$ turns out to be a line. The function field that is associated to $X(1)$ is $k(j)$ where j is transcendental over k. In analogy with the classical theory of elliptic curves over $\mathbb{C}$, the isomorphism class of an elliptic curve is uniquely determined by the j-invariant of that elliptic curve. The function field of $X(1)$ is given by $\mathbb{C}(j)$ where j is transcendental over $\mathbb{C}$.

3.2.2 $\dot{\mathbf{X}}\mathbf{(1)}$:

The curve $\dot{X}(1)$ parametrizes normalized Drinfeld module. A normalized Drinfeld module is uniquely determined by $\phi_T = -\tau + g\tau + 1$, hence can be determined by specifying the value of g. Each g corresponds to a unique normalized drinfeld module. So we can think of an affine line, with coordinate g, that parametrizes normalized

Drinfeld modules (each point on the affine line will correspond to a specific value of g and hence to a particular normalized Drinfeld module). The function field of $\dot{X}(1)$ is given by $k(g)$. Since the normalized Drinfeld module ϕ, with $\phi_T = -\tau^2 + g\tau + 1$ has J-invariant $g^{q+1}/(-1)$, we see that $k(g)$ is a degree $(q+1)$-Kummer extension of $k(j)$ given by $g^{q+1} = j$.

3.2.3 $\dot{\mathbf{X}}_\mathbf{1}(\mathbf{T})$ and its equation:

$\dot{X}_1(T)$ parametrizes normalized Drinfeld modules of rank 2 together with a T-torsion point of the Drinfeld module.

If x be a T-torsion point of ϕ then

$$\phi_T(x) = x + gx^q - x^{q^2} = 0.$$

So

$$g = \frac{x^{q^2} - x}{x^q}.$$

Here g determines the Drinfeld module ϕ and g can be written in terms of the T-torsion point x. So g and hence the normalized Drinfeld module is uniquely determined by the T-torsion point x, i.e. there is a unique normalized Drinfeld module that admits x as a T-torsion point. Hence,

$$\{(x, g) : -\tau^2 + g\tau + 1 \text{ is a Drinfeld module with } T\text{-torsion point } x\}$$

gives a plane model for the Drinfeld modular curve $\dot{X}_1(T)$. Here x and g satisfy the relation $g = (x^{q^2} - x)/x^q$. Since x already determines g the function field of $\dot{X}_1(T)$ is $k(x)$.

Now, we need a definition before continuing with other Drinfeld modular curves. For understanding the information that is given by the parametrization of the Drinfeld modular curve, we need to know the definition of a T^n-isogeny from a Drinfeld module to another. In this manner, we firstly give a proposition.

Proposition 3.2.1 *If $i \in L\{\tau\}$ is an isogeny from ϕ to ψ then* $\ker i$ *is an A-submodule of L under the A-module structure given by the Drinfeld module ϕ.*

Proof: Let $a \in A$. Since i is an isogeny from ϕ to ψ, we have $i \circ \phi_a = \psi_a \circ i$. If $x \in \ker i$ i.e. $i(x) = 0$ then

$$i(a.x) = i(\phi_a(x)) = i \circ \phi_a(x) = \psi_a \circ i(x) = \psi_a(0) = 0$$

So $\phi_a(x) \in \ker i$. Hence $\ker i$ is a submodule under the A-module structure given by ϕ. □

Proposition 3.2.2 *For each $n \in \mathbb{N}$,* $\ker \phi_{T^n}$ *is a free $A/\langle T^n \rangle$ module of rank 2.*

Proof: Suppose that $n = 2$. The idea of the proof in the general case is similar with this case.

Firstly, by Propostion 2.2.1 the additive polynomial ϕ_{T^2} is an isogeny from ϕ to itself. So by Propostion 3.2.1, its kernel is an A-submodule of L under the A-module structure of ϕ. Since all elements of $\ker \phi_{T^2}$ are annihilated by T^2, the kernel of ϕ_{T^2} becomes an $A/\langle T^2\rangle$-module. The module action is naturally defined as follows,

$$(a + \langle T^2\rangle).x := \phi_a(x)$$

for any $x \in \ker \phi_{T^2}$ and $a \in A$. Since ϕ_{T^2} is an isogeny from ϕ to itself, this action is well-defined. Indeed,

$$T^2.\phi_a(x) = \phi_{T^2}(\phi_a(x)) = (\phi_a(\phi_{T^2}(x)) = \phi_a(x) = 0.$$

for any $x \in \ker \phi_{T^2}$ and $a \in A$. Note that since A is a principal ideal domain, any ideal of $A/\langle T^2\rangle$ is generated by one element. So $A/\langle T^2\rangle$ is principal ideal ring.

Let $x \in \ker \phi_{T^2}$ be nonzero. Suppose that $(a + \langle T^2\rangle).x = 0$ for some $a \in A$. If a is relatively prime with T^2, then by the Euclidean algorithm, we can find elements $a_1, a_2 \in A$ such that

$$a_1T^2 + a_2a = 1.$$

Then we obtain

$$x = 1.x = \phi_1(x) = \phi_{a_1T^2+a_2a}(x) = \phi_{a_1}(\phi_{T^2}(x)) + \phi_{a_2}(\phi_a(x)) = \phi_{a_1}(0) + \phi_{a_2}(0) = 0.$$

So the only element in the kernel of ϕ_{T^2}, that is annihilated by an element $a \in A$ relatively prime to T^2 is the zero element. This means that $\ker \phi_{T^2}$ is torsion free. By the structure theorem of modules over principal ideal rings, $\ker \phi_{T^2}$ is free.

Now, if we think of ϕ_{T^2} as a linearized polynomial, then its degree is q^4. Also, since $\iota(T) = 1$ i.e. $\ker \iota = \langle T-1\rangle$, this polynomial is separable. This means it has q^4 distinct roots. So $\ker \phi_{T^2}$ has q^4 elements. Again by using the structure theorem for modules over principal ideal rings, we see that

$$\ker \phi_{T^2} \cong A/\langle T^2\rangle \times A/\langle T^2\rangle$$

as $A/\langle T^2\rangle$-module, because it is torsion free. □

Now, we give the following definition.

Definition 3.2.2 *We say that the isogeny i is a T^n-isogeny, if* $\ker i$ *is a free $A/\langle T^n\rangle$-submodule of* $\ker \phi_{T^n}$ *of rank* 1.

3.2.4 $\dot{\mathbf{X}}_0(\mathbf{T})$ and its equation:

$\dot{X}_0(T)$ parametrizes normalized Drinfeld modules of rank 2 with a T-isogeny, i.e. an A-submodule that is generated by T-torsion point x.

Again, let ϕ be a normalized Drinfeld module with $\iota(T) = 1$ given by

$$\phi_T := -\tau^2 + g\tau + 1.$$

A-submodule which is generated by a nonzero T-torsion point x under the action of ϕ is

$$\{P(T).x | P(T) \in A\} = \{\phi_{P(T)}(x) | P(T) \in k\}.$$

Since x is annihilated by T,

$$\{\phi_{P(T)}(x) | P(T) \in A\} = \{\phi_a(x) | a \in k\}.$$

Since ϕ is an k-algebra homomorpism,

$$\{\phi_a(x) | a \in k\} = \{ax | a \in k\}. \tag{3.1}$$

We identify the set in the equation (3.1) with the polynomial whose roots are exactly all elements of the set in Equation (3.1)

$$\prod_{a \in k}(T - ax). \tag{3.2}$$

Lemma 3.2.3

$$\prod_{a \in k}(T - ax) = T^q - x^{q-1}T.$$

Proof: Firstly,

$$\prod_{a \in k}(T - ax) = x^q \prod_{a \in k}(T/x - a).$$

Say $S := T/x$. We know that

$$\prod_{a \in k}(S - a) = S^q - S.$$

Then

$$x^q \prod_{a \in k}(T/x - a) = x^q \prod_{a \in k}(S - a) = x^q(S^q - S) = x^q(T^q/x^q - T/x) = T^q - x^{q-1}T.$$

Hence,

$$\prod_{a \in k}(T - ax) = T^q - x^{q-1}T \tag{3.3}$$

□

Proposition 3.2.4 *If we set $u := x^{q-1}$ for the coefficient of the polynomial in (3.3) then $\tau - u$ is a T-isogeny of ϕ. i.e. there exists a Drinfeld module ψ of rank 2 such that $\tau - u$ is an isogeny between ϕ and ψ with*

$$\ker(\tau - u) \subseteq \ker \phi_T. \tag{3.4}$$

Proof: If we consider the Drinfeld module ψ that is defined by

$$\psi_T = -\tau^2 + (u - \frac{1}{u^q})\tau + 1$$

then we see that $\tau - u$ is an isogeny between ϕ and ψ. In fact,

$$\phi_T = (-\tau - \frac{1}{u}) \circ (\tau - u)$$

and

$$\psi_T = (\tau - u)(-\tau - \frac{1}{u}).$$

Then

$$(\tau - u) \circ \phi_T = (\tau - u) \circ (-\tau - \frac{1}{u}) \circ (\tau - u) = \psi_T \circ (\tau - u).$$

Note that $\tau - u$ is the right linear factor of ϕ_T. So $\ker(\tau - u) \subseteq \ker \phi_T$. □

If x is a T-torsion point, then the set in (3.1) corresponds to x^{q-1} because of the stated identification and Lemma 3.2.3. Explicitly, the polynomial in (3.2) correponds to the set in (3.1) and x^{q-1} comes from the polynomial in (3.2) as a coefficient. In fact it uniquely determines the polynomial . So the function field of $X_0(T)$ is $k(x^{q-1})$.

Hence we have the following picture,

$$\begin{array}{ccc} k(x) & \dot{X}_1(T) & \ni (\phi, x) \ \text{ where } \ x \in \ker \phi_T \\ \downarrow & \downarrow & \\ k(x^{q-1}) & \dot{X}_0(T) & \ni (\phi, k.x) \\ \downarrow & \downarrow & \\ k(g) & \dot{X}(1) & \ni \phi \end{array}$$

3.2.5 $\dot{\mathbf{X}}_\mathbf{0}(\mathbf{T^2})$ and its equations :

$\dot{X}_0(T^2)$ parametrizes normalized Drinfeld modules of rank 2 together with a T^2-isogeny from the Drinfeld module.

Let $\phi^{(i)}$ be a normalized Drinfeld module of rank 2 defined by

$$\phi_T^{(i)} = -\tau^2 + g_i\tau + 1$$

for $i \in \{1, 2, 3\}$.

Proposition 3.2.5 *If i_1 and i_2 are T-isogenies from $\phi^{(1)}$ to $\phi^{(2)}$ and from $\phi^{(2)}$ to $\phi^{(3)}$ respectively, then $i_2 \circ i_1$ is a an isogeny from $\phi^{(1)}$ to $\phi^{(3)}$ with the property that*

$$\ker i_2 \circ i_1 \subseteq \ker \phi^{(1)}_{T^2}.$$

Proof: Since i_1 is an isogeny from $\phi^{(1)}$ to $\phi^{(2)}$ and i_2 is an isogeny from $\phi^{(2)}$ to $\phi^{(3)}$,

$$i_2 \circ i_1 \circ \phi^{(1)}_T = i_2 \circ \phi^{(2)}_T \circ i_1 = \phi^{(3)}_T \circ i_2 \circ i_1.$$

This means that $i_2 \circ i_1$ is an isogeny from $\phi^{(1)}$ to $\phi^{(3)}$.

Now take any element $x \in \ker i_2 \circ i_1$. Then $i_2(i_1(x)) = 0$. But $i_1(x) \in \ker i_2$. Since i_2 is a T-isogeny from $\phi^{(2)}$ to $\phi^{(3)}$,

$$\ker i_2 \subseteq \ker \phi^{(2)}_T,$$

so $i_1(x) \in \ker \phi^{(2)}_T$. Then we get

$$0 = \phi^{(2)}_T \circ i_1(x) = i_1 \circ \phi^{(1)}_T(x).$$

So $\phi^{(1)}_T(x) \in \ker i_1$. We know that

$$\ker i_1 \subseteq \ker \phi^{(1)}_T.$$

because i_1 is a T-isogeny. So $\phi^{(1)}_T(x) \in \ker \phi^{(1)}_T$. Then we get that

$$\phi^{(1)}_{T^2} = \phi^{(1)}_T \circ \phi^{(1)}_T(x) = 0.$$

Therefore,

$$\ker i_2 \circ i_1 \subseteq \ker \phi^{(1)}_{T^2}.$$

Hence $i_2 \circ i_1$ is an isogeny from $\phi^{(1)}$ to $\phi^{(3)}$ whose kernel is annihilated by the multiplication by T^2 map given by $\phi^{(1)}$. □

Remark: Note that $i_2 \circ i_1$ is not necessarily a T^2-isogeny, since its kernel might not be a $A/\langle T^2 \rangle$-module of rank 1. In fact, since i_1 is a T-isogeny from $\phi^{(1)}$, we know that there is an additive polynomial i_1' such that $i_1' \circ i_1 = \phi^{(1)}_T$. Now it can be seen that i_1' is an isogeny from $\phi^{(2)}$ to a Drinfeld module, which is isomorphic to $\phi^{(1)}$. Exactly in the case that $i_2 = i_1'$ we would have that $i_2 \circ i_1$ is just the multiplication by T map given by $\phi^{(1)}$ and hence has kernel, which is a free $A/\langle T^2 \rangle$-module of rank 2. It can be shown that in all other cases (i.e. if $i_2 \neq i_1'$) we have that $i_2 \circ i_1$ is a T^2-isogeny (so $\ker i_2 \circ i_1$ is a free $A/\langle T^2 \rangle$-module of rank 1).

Now we calculate the equation of $\dot{X}_0(T^2)$.

If x_1 is a T-torsion point of ϕ, then we know that

$$g_1 = \frac{x_1^{q^2} - x_1}{x_1^q} = \frac{x_1^{q^2-1} - 1}{x_1^{q-1}} = \frac{(x_1^{q-1})^{q+1} - 1}{x_1^{q-1}}.$$

By setting $u_1 := x_1^{q-1}$ we obtain

$$g_1 = \frac{u_1^{q+1} - 1}{u_1}.$$

By Propostion 3.2.4, $\tau - u_1$ is a T-isogeny between $\phi^{(1)}$ and $\phi^{(2)}$ where $\phi^{(2)}$ is a normalized Drinfeld module of rank 2 with

$$\phi_T^{(2)} = -\tau + g_2\tau + 1 = -\tau^2 + (u_1 - \frac{1}{u_1^q})\tau + 1. \tag{3.5}$$

On the other hand, if we take a T-torsion point x_2 of $\phi^{(2)}$ then

$$g_2 = \frac{x_2^{q^2} - x_2}{x_2^q} = \frac{u_2^{q+1} - 1}{u_2} \tag{3.6}$$

by setting $u_2 := x_2^{q-1}$. By using the equations (3.5) and (3.6), we get that

$$\frac{u_1^{q+1} - 1}{u_1^q} = g_2 = \frac{u_2^{q+1} - 1}{u_2}. \tag{3.7}$$

However as we have seen above, we need that the isogenies $\tau - u_2$ and $\tau - u_1$ need to come together in a proper way in order to form a T^2-isogeny (i.e. their composite should not give the multiplication by T-map)

By Equation (3.7), we see that u_2 satisties

$$P(T) := T^{q+1} - 1 - \frac{u_1^{q+1} - 1}{u_1^q} T \in k(u_1)[T]. \tag{3.8}$$

If we substitute $\frac{-1}{u_1}$ for u_2 in the expression for g_2 then we see that

$$\frac{u_2^{q+1} - 1}{u_2} = \frac{(\frac{-1}{u_1})^{q+1} - 1}{\frac{-1}{u_1}} = \frac{1 - u_1^{q+1}}{-u_1^q} = \frac{u_1^{q+1} - 1}{u_1^q}$$

This means that $\frac{-1}{u_1}$ is a root of $P(T)$. Note that this choice of root corresponds exactly to the situation where $(\tau - u_2) \circ (\tau - u_1)$ is the multiplication by T-map, since $(\tau - u_2) \circ (\tau - u_1) = (\tau - (-1/u_1)) \circ (\tau - u_1) = -(-\tau^2 + g_1\tau + 1)$. Hence for u_2 we should take any root of $P(T)$ but this one. By dividing $P(T)$ by $T + \frac{1}{u_1}$, we obtain

$$P(T) = (T + \frac{1}{u_1})(\sum_{i=1}^{q} (-1)^{i+1} \frac{T^i}{u_1^{q-i}} - u_1).$$

Since u_2 is a root of $P(T)$ we have,

$$\sum_{i=1}^{q} (-1)^{i+1} \frac{u_2^i}{u_1^{q-i}} - u_1 = 0 \tag{3.9}$$

So $\dot{X}_0(T^2)$ has a plane model given by

$$\{(u_1, u_2) | \sum_{i=1}^{q} (-1)^{i+1} \frac{u_2^i}{u_1^{q-i}} - u_1 = 0\}$$

The function field of $\dot{X}_0(T^2)$ is given by $k(u_1, u_2)$ with u_1, u_2 satisfying Equation (3.9).

If one can take

$$g(X,Y) := \sum_{i=1}^{q} (-1)^{i+1} \frac{Y^i}{X^{q-i}} - X \tag{3.10}$$

to recursively define the following tower $\dot{X}_0(T^n)$.

3.2.6 The tower $\dot{\mathbf{X}}_0(\mathbf{T^n})$:

We have seen above that by composing two T-isogenies we obtain an isogeny with kernel contained in the kernel of the multiplication by T^2-map and that we need to impose another condition, to ensure that the composition is a T^2-isogeny. Similarly by composing n many numbers of T-sogenies and requiring that any two consequtive ones don't form together a multiplication by T map, we can obtain T^n-isogenies. Conversely any T^n-isogeny is obtained in this way. More precisely we have the following,

Remark: Let $\phi^{(1)}, \ldots, \phi^{(n+1)}$ be Drinfeld modules with T-isogenies

$$i_m : \phi^{(m)} \to \phi^{(m+1)}$$

such that the composition of any two consequtive isogenies

$$i_{m+1} \circ i_m : \phi^{(m)} \to \phi^{(m+2)}$$

is a T^2-isogeny for $m = 1, \ldots, n-2$. Then

$$i_n \circ \cdots \circ i_1 : \phi^{(1)} \to \phi^{(n)}$$

is a T^n-isogeny. Conversely any T^n-isogeny can be written as a composition of T-isogenies so that the composite of any two consecutive ones is a T^2-isogeny.

Now we see the tower $\dot{X}_0(T^n)$ is exactly the tower given by $g(X,Y)$ in Equation (3.10).

Let $m \in \{1, \ldots, n\}$. Set

$$\phi_T^{(m)} := -\tau^2 + g_m \tau + 1$$

If x_m is a T-torsion point of $\phi^{(m)}$, then we know that

$$g_m = \frac{x_m^{q^2} - x_m}{x_m^q} = \frac{x_m^{q^2-1} - 1}{x_m^{q-1}} = \frac{(x_m^{q-1})^{q+1} - 1}{x_m^{q-1}}.$$

By setting $u_m := x_m^{q-1}$ we obtain

$$g_m = \frac{u_m^{q+1} - 1}{u_m}.$$

By Propostion 3.2.4, $\tau - u_m$ is a T-isogeny between $\phi^{(m)}$ and $\phi^{(m+1)}$ where $\phi^{(m+1)}$ is a normalized Drinfeld module of rank 2 with

$$\phi_T^{(m+1)} = -\tau^2 + g_{m+1}\tau + 1 = -\tau^2 + (u_m - \frac{1}{u_m^q})\tau + 1. \tag{3.11}$$

On the other hand, if we take a T-torsion point x_{m+1} of $\phi^{(m+1)}$ then

$$g_{m+1} = \frac{x_{m+1}^{q^2} - x_{m+1}}{x_{m+1}^q} = \frac{u_{m+1}^{q+1} - 1}{u_{m+1}} \tag{3.12}$$

by setting $u_{m+1} := x_{m+1}^{q-1}$. By using the equations (3.11) and (3.12), we get that

$$\frac{u_m^{q+1} - 1}{u_m^q} = g_{m+1} = \frac{u_{m+1}^{q+1} - 1}{u_{m+1}}. \tag{3.13}$$

However as we have seen above, we need that the isogenies $(\tau - u_{m+1})$ and $(\tau - u_m)$ need to come together in a proper way in order to form a T^2-isogeny (i.e. their composite should not give the multiplication by T-map)

By Equation (3.13), we see that u_{m+1} satisties

$$P(T) := T^{q+1} - 1 - \frac{u_m^{q+1} - 1}{u_m^q} T \in k(u_m)[T]. \tag{3.14}$$

If we substitute $\frac{-1}{u_m}$ for u_{m+1} in the expression for g_{m+1} then we see that

$$\frac{u_{m+1}^{q+1} - 1}{u_{m+1}} = \frac{(\frac{-1}{u_m})^{q+1} - 1}{\frac{-1}{u_m}} = \frac{1 - u_m^{q+1}}{-u_m^q} = \frac{u_m^{q+1} - 1}{u_m^q}$$

This means that $\frac{-1}{u_m}$ is a root of $P(T)$. Note that this choice of root corresponds exactly to the situation where $(\tau - u_{m+1}) \circ (\tau - u_m)$ is the multiplication by T-map, since $(\tau - u_{m+1}) \circ (\tau - u_m) = (\tau - (-1/u_m)) \circ (\tau - u_m) = -(-\tau^2 + g_m\tau + 1)$. Hence for u_{m+1} we should take any root of $P(T)$ but this one. By dividing $P(T)$ by $T + \frac{1}{u_m}$, we obtain

$$P(T) = (T + \frac{1}{u_m})(\sum_{i=1}^{q} (-1)^{i+1} \frac{T^i}{u_m^{q-i}} - u_m).$$

Since u_2 is a root of $P(T)$ we have,

$$\sum_{i=1}^{q} (-1)^{i+1} \frac{u_{m+1}^i}{u_m^{q-i}} - u_m = 0 \tag{3.15}$$

Hence the function field of the Drinfeld modular curve $\dot{X}_0(T^m)$ over k is

$$k(u_1, \ldots, u_m)(u_{m+1})$$

where $g(u_m, u_{m+1}) = 0$.

3.3 $\mathbf{X_0(T^n)}$ and the tower of Bezerra–Garcia

Alternatively, we can parametrize isomorphism classes rather than working normalized Drinfeld modules. Propostion 3.1.1 gives that two normalized Drinfeld modules ϕ and ψ

$$\phi_T = -\tau^2 + g_1\tau + 1$$

and

$$\psi_T = -\tau^2 + g_2\tau + 1$$

are isomorphic if and only if

$$g_1^{q+1} = g_2^{q+1}.$$

When we have tried to find the equation of $\dot{X}_0(T^2)$, we have obtained that

$$\frac{u_1^{q+1}-1}{u_1^q} = g_2 = \frac{u_2^{q+1}-1}{u_2}.$$

Since we study with the isomorphism classes now, we have

$$\frac{(u_1^{q+1}-1)^{q+1}}{(u_1^{q+1})^q} = \left(\frac{u_1^{q+1}-1}{u_1^q}\right)^{q+1} = g_2^{q+1} = \left(\frac{u_2^{q+1}-1}{u_2}\right)^{q+1} = \frac{(u_2^{q+1}-1)^{q+1}}{u_2^{q+1}}.$$

By denoting u_i^{q+1} by U_i for $i = 1, 2$, we obtain

$$\frac{(U_1-1)^{q+1}}{U_1^q} = \frac{(U_2-1)^{q+1}}{U_2}.$$

where U_1 and U_2 generate the functions field of $X_0(T^2)$. After some computaions we get that,

$$\frac{(U_1-1)^{q+1}}{U_1^q} - \frac{(U_2-1)^{q+1}}{U_2} = \left(U_1 - \frac{1}{U_2}\right)\left(1 - \frac{1}{U_1^q} - \left(U_2 - \frac{1}{U_1}\right)^{q-1}\left(\frac{U_2}{U_1} - \frac{1}{U_1}\right)\right).$$

So

$$\left(U_1 - \frac{1}{U_2}\right)\left(1 - \frac{1}{U_1^q} - \left(U_2 - \frac{1}{U_1}\right)^{q-1}\left(\frac{U_2}{U_1} - \frac{1}{U_1}\right)\right) = 0 \tag{3.16}$$

Note that the first factor corresponds to the undesired case where the two isogenies get together to form a multiplication by T-map.

Now, Equation (3.10) can rewritten as

$$\frac{U_1-1}{U_2-1} = \left(\frac{U_1U_2-1}{U_1-1}\right)^{q-1}.$$

If we define V_1 as

$$V_1 := \frac{U_1U_2-1}{U_1-1}$$

then we see that

$$U_1 = V_1^{q-1}(V_1-1) \text{ and } U_2 = \frac{(V_1-1)^q}{V_1^{q-1}}.$$

Therefore V_1 is a generator of the function field of $X_0(T^2)$.

If we define

$$\xi_1 := V_1$$

then U_1 and U_2 can be written in terms of ξ_1

$$U_1 = \frac{1-\xi_1}{\xi_1^q} \quad \text{and} \quad U_2 = \frac{(1-\xi_1)^q}{\xi_1}.$$

If we use the generator V_2 of the function field $k(U_2, U_3)$ where U_3 coming from the isomorphism class of the third Drinfeld module then by similar calculations we get that

$$U_2 = \frac{1-\xi_2}{\xi_2^q}$$

with $V_2 := 1/\xi_2$. Therefore,

$$\frac{1-\xi_1^q}{\xi_1} = U_2 = \frac{1-\xi_2}{\xi_2^q}.$$

If we define the polynomial $F(X, Y)$

$$F(X,Y) := \frac{1-X^q}{X} - \frac{1-Y}{Y^q}$$

then $F(X, Y)$ defines recursively the tower of Bezerra–Garcia that attains the Drinfel–Vlăduţ bound.

Bibliography

[1] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, *Towers of Function Fields over Non-Prime Finite Fields*, to appear in Moscow Mathematical Journal.

[2] J. Bezerra, A. Garcia, *A Tower with non-Galois steps which attains the Drinfeld–Vlăduţ bound* , J. Number Theory 106 (2004), (142-154).

[3] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589** (2005), 159-199.

[4] V.G.Drinfeld and S.G.Vladut, *The number of points of an algebraic curve*, Funktsional Anal. i Prilozhen 17, 68-69 (1983).

[5] N. D. Elkies, *Explicit towers of Drinfeld modular curves*, in European Congress of Mathematics, vol. II (Barcelona 2000), ed. C. Casacuberta, R. M. Miró–Roig, J. Verdera, S. Xambó–Descamps, Progr. Math. **202**, Birkhäuser (2001), 189-198.

[6] A.Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J.Number Theory 61, 248-273 (1996).

[7] A. Garcia, H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211-222.

[8] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. 34, 291-300 (2002).

[9] D. Goss, "Basic Structures of Function Field Arithmetic", Springer Verlag, Berlin-Heidelberg- New York (1998).

[10] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo 28, 721-724 (1981).

[11] W.-C.W. Li and H.Maharaj, *Coverings of curves with asymptotically many rational points*, J. Number Theory 96, 232-256 (2002).

[12] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini*, C.R. Acad. Sc. Paris 296, 397-402 (1983).

[13] H. Stichtenoth, "Algebraic Function Fields and Codes", Graduate Texts in Mathematics, 197-198 (2008-2).

[14] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Fundamentals of Computation Theory (ed. L.Budach), Lecture Notes Comp. Sc. LNCS 199, 503-511 (1985).