

NEW OPTIMAL FUNCTION FIELD TOWERS OVER FINITE FIELDS OF QUARTIC POWER

CHUANGQIANG HU AND XIUWU ZHU

ABSTRACT. We introduce two new types of towers of Drinfeld modular curves. These towers originate from a specific domain \mathcal{A} and are analogous to the towers of rank-two Drinfeld modular curves over the polynomial ring. Specifically, the domain \mathcal{A} corresponds to the projective line over the finite field \mathbb{F}_q , equipped with an infinite place of degree two. We select an arbitrary non-zero principal \mathcal{A} -ideal I_η of degree two. Notably, the I_η -reduction of the tower of minimal Drinfeld modular curves is asymptotically optimal over the finite field \mathbb{F}_{q^4} .

Keywords: Drinfeld module; Drinfeld modular curve; Isogeny; Ihara quantity

1. INTRODUCTION

1.1. Ihara's quantity. Let \mathbb{F}_q denote the finite field of cardinality q . Let F be a function field over \mathbb{F}_q with genus $g(F)$. Estimating the number of rational places of F is an important topic in number theory and algebraic geometry. The Hasse-Weil bound [34] states that the number of rational places of F satisfies the inequality

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

An improved bound was obtained by Serre [28]:

$$N(F) \leq q + 1 + g(F)\lfloor 2\sqrt{q} \rfloor.$$

A function field F/\mathbb{F}_q that achieves the Hasse-Weil bound is called maximal. For a comprehensive overview, the interested reader is referred to [8, 9, 13, 19, 20, 31] for standard examples, and to [6, 30] for recent progress on maximal curves.

To investigate the asymptotic behavior for function fields over \mathbb{F}_q , Ihara [26] introduced the quantity

$$\text{Ihara}(q) := \limsup_{g(F) \rightarrow \infty} \frac{N(F)}{g(F)},$$

where F ranges over the function fields over \mathbb{F}_q . Due to Serre's lower bound [29] and the Drinfeld-Vladut upper bound [11], it is now well-known that

$$0 < \text{Ihara}(q) \leq \sqrt{q} - 1.$$

In search of lower bounds for $\text{Ihara}(q)$, researchers have invented various constructions of function field towers over \mathbb{F}_q . Roughly speaking, a function field tower \mathcal{F}_* means a sequence of successive inclusions

$$\mathcal{F}_0 \longrightarrow \mathcal{F}_1 \longrightarrow \mathcal{F}_2 \longrightarrow \mathcal{F}_3 \longrightarrow \mathcal{F}_4 \longrightarrow \cdots,$$

of function fields over \mathbb{F}_q with $g(\mathcal{F}_n) \rightarrow \infty$ when $n \rightarrow \infty$.

The limit

$$\lambda(\mathcal{F}_*) = \lim_{n \rightarrow \infty} \frac{N(\mathcal{F}_n)}{g(\mathcal{F}_n)}$$

certainly gives a lower bound of $\text{Ihara}(q)$. A function field tower \mathcal{F}_* is called asymptotically good if $\lambda(\mathcal{F}_*) > 0$ and called asymptotically optimal if $\lambda(\mathcal{F}_*)$ verifies the Drinfeld-Vladut bound. Notice that it is not generally easy to construct good towers.

When q is a square, a sharp lower bound for Ihara's quantity is established independently: $\text{Ihara}(q) \geq \sqrt{q} - 1$ (hence $\text{Ihara}(q) = \sqrt{q} - 1$). Specifically, Ihara [26] used families of Shimura modular curves to derive this result, whereas Tsfasman, Vlăduț, and Zink [32] relied on families of classical modular curves. A key limitation of both approaches, however, is that the modular curves involved are not explicit. To address this lack of explicitness, Garcia and Stichtenoth [14] later constructed an explicit optimal sequence of function fields over \mathbb{F}_{q^2} :

$$\{\mathcal{F}_n := \mathbb{F}_q(x_1, \dots, x_n)\}.$$

This tower is defined by a recursive condition on its variables x_n :

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

In a subsequent work [15], they extended this line of research by introducing a second explicit tower of function fields, governed by the recursive relation:

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

Later, Elkies [12] established a key connection: the function field towers (and their associated curves) constructed by Garcia and Stichtenoth are in fact Drinfeld modular curves. This pattern extends to other settings: well-performing function field constructions have also been shown to arise from modular curves. Motivated by this, Elkies conjectured that all optimal recursive towers must originate from some type of modular curve—though the exact formalization of this claim remains non-trivial to specify. Independently, Gekeler [18] further confirmed the relevance of Drinfeld modular curves by showing that certain families of these curves also achieve the aforementioned lower bound (for Ihara's quantity).

When q is not a square, the exact value of $\text{Ihara}(q)$ remains undetermined. Write $q = p^{2m+1}$ with $m \geq 1$. Bassa, Beelen, Garcia, and Stichtenoth [3] established a key lower bound:

$$\text{Ihara}(q) \geq \frac{2(p^{m+1} - 1)}{p + 1 + (p - 1)/(p^m - 1)}.$$

Notably, this bound is achieved by function field towers derived from Drinfeld modular curves of rank $2m + 1$. Subsequently, the work in [2] and its follow-up [10] built on this foundation. These contributions extended the analysis and provided a precise modular description for each function field in the towers.

1.2. Main results. In [4] and [5], Bassa et al. systematically studied good families of Drinfeld modular curves. Roughly speaking, the points of the curve $X_0(\mathfrak{n})$ parametrize isomorphism classes of pairs consisting of rank-two Drinfeld \mathcal{A} -modules together with an \mathfrak{n} -torsion, where the domain \mathcal{A} is derived from a smooth algebraic curve over \mathbb{F}_q associated with a marked place at infinity. The modular curve $\mathbf{x}_0(\mathfrak{n})$ is defined as any geometric component of $X_0(\mathfrak{n})$. Replacing the full set of Drinfeld modules with normalized modules in the sense of Hayes' notion [22], one can construct the normalized Drinfeld modular curves $\dot{\mathbf{x}}_0(\mathfrak{n})$ in a similar manner. In particular, when $\mathcal{A} = \mathbb{F}_q[t]$, and $\mathfrak{n} = (t^n)$, the resulting Drinfeld modular curves $\mathbf{x}_0(\mathfrak{n})$ and $\dot{\mathbf{x}}_0(\mathfrak{n})$ coincide with the curves considered by Elkies [12] after reduction at $(t - 1)$.

In this paper, we construct the optimal families of Drinfeld modular curves following the framework of Bassa et al. We focus on the domain \mathcal{A} corresponding to the projective line over

the finite field \mathbb{F}_q associated with an infinite place P_ρ of degree two. One may show that the domain \mathcal{A} can be expressed as

$$\mathcal{A} = \mathbb{F}_q[x, y] / \langle y^2 - (\zeta + \zeta^q)xy + \zeta^{q+1}x^2 - x \rangle$$

where ζ is some element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Recall that [24] derived that the complete family of rank-two normalized Drinfeld modules is described by ϕ^λ and its Frobenius twist $\phi^{\sigma;\lambda}$ with independent variable λ . Let $I_\infty = (x, y)$ be an ideal of \mathcal{A} . The main result in this paper is devoted to computing the explicit expressions for the function field towers of modular curves with $\mathfrak{n} = I_\infty^n$.

Theorem A. *Let $H^+ = \mathbb{F}_q(t, \zeta, \nu)$ be the narrow class field of \mathcal{A} with the relation*

$$\nu^{q+1} = -\frac{1}{(t - \zeta)(t^q - \zeta)}.$$

The normalized modular curves $\mathbf{x}_0(I_\infty^i)$ are represented by the function field tower

$$\mathcal{F}_0 \xrightarrow{q+1} \mathcal{F}_1 \xrightarrow{q} \mathcal{F}_2 \xrightarrow{q} \mathcal{F}_3 \xrightarrow{q} \mathcal{F}_4 \xrightarrow{q} \cdots,$$

where the number on the arrow denotes the extension degree. The function field \mathcal{F}_k is generated by the variables $\lambda_0, \dots, \lambda_k$ as follows.

- (1) *For $k = 0$, $\mathcal{F}_0 = H^+(\lambda_0)$.*
- (2) *For $k = 1$, $\mathcal{F}_1 = H^+(\lambda_0, \lambda_1)$, where the defining equation of λ_0 and λ_1 is given by*

$$\lambda_1^{q+1} - \lambda_0^q \lambda_1^q - \frac{\zeta^{1-q} - 1}{\zeta \lambda_0} (t - \zeta^q) \nu \lambda_1 + ((\zeta^{-q} - \zeta^{-1})(t - \zeta^q) + (\zeta^{q-1} - 1)^{q+1}) \nu \lambda_0^{q-1} = 0.$$

- (3) *For $k \geq 2$, we obtain*

$$\mathcal{F}_k = \mathcal{F}_1(\lambda_2, \dots, \lambda_k) = H^+(\lambda_0, \lambda_1, \lambda_2, \dots, \lambda_k),$$

where the variables $\lambda_2, \dots, \lambda_k$ are subject to

$$\sum_{i=0}^{q-1} \left(\frac{\nu^{\sigma^k} (1 - \zeta^{1-q})^{q+1} \lambda_{k-2}^{q-1}}{\lambda_{k-1} - \lambda_{k-2}^q} \right)^i (\lambda_k - \lambda_{k-1}^q)^{q-i} - \nu^{\sigma^{k-1} - \sigma^{k-2}} \frac{\lambda_{k-1} - \lambda_{k-2}^q}{\lambda_{k-2}^{q-1}} \lambda_{k-1}^{q-1} = 0.$$

Similarly, we obtain the modular curves for minimal models.

Theorem B. *Let H be the class field of \mathcal{A} . The minimal modular curves $\mathbf{x}_0(I_\infty^k)$ of Drinfeld \mathcal{A} -modules are represented by the function field tower*

$$\mathcal{G}_0 \xrightarrow{q+1} \mathcal{G}_1 \xrightarrow{q} \mathcal{G}_2 \xrightarrow{q} \mathcal{G}_3 \xrightarrow{q} \mathcal{G}_4 \xrightarrow{q} \cdots.$$

The function field \mathcal{G}_k is generated by j_0 and w_i for $i = 1, \dots, k$ in the following forms:

- (1) *For $k = 0$, $\mathcal{G}_0 = H(j_0)$.*
- (2) *For $k = 1$, $\mathcal{G}_1 = H(j_0, w_1) = H(w_1)$, and the inclusion $\mathcal{G}_0 \rightarrow \mathcal{G}_1$ is represented by*

$$j_0 \mapsto -\frac{1 + \zeta^{-1}(t - \zeta^q)w_1}{w_1^{q+1} + (1 - \zeta^{1-q})^{-1}w_1}.$$

- (3) *For $k \geq 2$, $\mathcal{G}_k = H(w_1, w_2, \dots, w_k)$, where w_i satisfy the relations*

$$\sum_{i=0}^{q-1} (w_{k-1}^\nabla)^i w_2^{q-i} = \frac{w_{k-1}^q}{1 - (\zeta^{q^{k+1}-q^k} - 1)w_{k-1}} \left(w_{k-1}^\nabla (t - \zeta^{q^{k+1}}) \right)^{q-1},$$

and w_{k-1}^∇ is given by

$$w_{k-1}^\nabla = \frac{1}{(\zeta^{q^k - q^{k+1}} - 1)(1 + \zeta^{-q^k}(t - \zeta^{q^{k+1}})w_{k-1})}.$$

Now the optimal family of function field towers over the finite field \mathbb{F}_{q^4} is derived from the reduction of the family in Theorem B.

Theorem C. Let I_η be a principal \mathcal{A} -ideal generated by z_η with $\deg z_\eta = 2$. Let $\mathbf{x}_0(I_\infty^k)/I_\eta$ ($k \geq 0$) denote the I_η -reduction of the minimal Drinfeld modular curves $\mathbf{x}_0(I_\infty^k)$. Then the genus of $\mathbf{x}_0(I_\infty^k)/I_\eta$ is given by

$$g(\mathbf{x}_0(I_\infty^k)/I_\eta) = -1 + \frac{q^{k-1}(q+1)}{q-1} - \frac{2}{q-1} \cdot (q^{\lfloor k/2 \rfloor} + q^{k-\lfloor k/2 \rfloor-1} - 1).$$

Consider $\mathbf{x}_0(I_\infty^k)/I_\eta$ as defined over the constant field $\mathbb{F}_{\mathbf{q}} = \mathbb{F}_{q^4}$. Then all the supersingular points of these curves are $\mathbb{F}_{\mathbf{q}}$ -rational. Moreover, the function field tower of $\mathbf{x}_0(I_\infty^k)/I_\eta$ is asymptotically optimal.

1.3. Remarks. The approaches adopted in the paper are essentially the same as those in Elkies' paper [12] (see [2, 4, 5, 10] for further reading). We translate the information on primitive I_∞^k -torsions into isogeny relations between the k -th Frobenius twists of Drinfeld modules for $k \geq 0$. However, we shall emphasize that the isogeny formula presents the main difficulty in this work. Our main technique is to describe explicitly the algebraic structure of I_∞ -annihilator $\phi_{I_\infty}^\lambda$, which is particularly studied in [24] with the help of Anderson motives.

It is remarkable that our Drinfeld modular tower also achieves Ihara's quantity. From Goppa's construction [21], good towers yield good linear error-correcting codes. By demonstrating that long linear codes can surpass the Gilbert-Varshamov bound [31, Proposition 8.4.4], the celebrated work of Tsfasman et al. [32] established a crucial connection between coding theory and Ihara's quantity. Recursive good towers play an important role in the study of Ihara's quantity, coding theory, and cryptography [1, 7, 23, 25, 33, 35].

The paper is organized as follows. We introduce some necessary notations and results concerning Drinfeld modules in Section 2. Section 3 is devoted to constructing the tower of normalized Drinfeld module curves. Using this construction, we investigate the tower of minimal Drinfeld modules in Section 4. In Section 5, we compute the genus and rational places of the I_η -reduction of the tower to estimate Ihara's quantity.

2. PRELIMINARIES

2.1. Galois groups and Hilbert fields. We briefly recall the necessary notations that will be used in the remainder of this paper. Let \mathbb{P}^1 be the projective line over \mathbb{F}_q . It is clear that the function field of \mathbb{P}^1 equals $K = \mathbb{F}_q(t)$. Let P_ρ be a degree two place of K corresponding to the monic irreducible polynomial $\rho(t) = (t - \zeta)(t - \zeta^q) \in \mathbb{F}_q[t]$ for some element $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We view P_ρ as the infinity of \mathbb{P}^1 for the remainder of this paper. Denote by \mathcal{A} the Dedekind domain arising from $\mathbb{P}^1 - P_\rho$; that is

$$\mathcal{A} = H^0(\mathbb{P}_{\mathbb{F}_q}^1 - P_\rho, \mathcal{O}_{\mathbb{P}^1}).$$

Notice that the quotient field of \mathcal{A} recovers the function field K . Define the coordinates x, y of \mathcal{A} as

$$x = \frac{1}{\rho(t)}, \quad y = \frac{t}{\rho(t)}.$$

Then we know \mathcal{A} is indeed the \mathbb{F}_q -algebra generated by x, y , that is

$$\mathcal{A} = \mathbb{F}_q[x, y] / \langle y^2 - (\zeta + \zeta^q)xy + \zeta^{q+1}x^2 - x \rangle.$$

From the class field theory for function fields, the Hilbert field of \mathcal{A} is given by

$$H = \mathbb{F}_q(t, \zeta) = \mathbb{F}_{q^2}(T),$$

where $T = \frac{1}{t-\zeta^q} = y - \zeta x$. The Galois group of H/K is isomorphic to $\text{Cl}(\mathcal{A}) = \mathbb{Z}/2$ generated by

$$\sigma : \zeta \mapsto \zeta^q.$$

In particular, σ acts on T by

$$T^\sigma := \frac{1}{t - \sigma(\zeta^q)} = \frac{1}{t - \zeta} = \frac{T}{1 + (\zeta^q - \zeta)T}.$$

Note that we always denote the action of σ by a superscript to simplify the notation. Let $H^+ = \mathbb{F}_q(t, \zeta, \nu) = H(\nu)$, where ν satisfies

$$\nu^{q+1} = -T^{q+\sigma} = \frac{-1}{(t - \zeta)(t^q - \zeta)}.$$

As shown in [24], H^+ is the narrow class field of K with respect to a sign function at P_ρ . The Galois group $\text{Gal}(H^+/K)$ is isomorphic to

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(q+1)\mathbb{Z}$$

with generators σ and M_μ , where

$$\sigma : \zeta \mapsto \zeta^q; \quad \nu \mapsto \nu^\sigma := T^{1-q}\nu^q = -\frac{x}{\nu} \quad (1)$$

and for $\mu^{q+1} = 1$,

$$M_\mu : \zeta \mapsto \zeta; \quad \nu \mapsto \mu\nu.$$

We know the isomorphism $\text{Cl}^+(\mathcal{A}) \cong \text{Gal}(H^+/K)$ is given by the Artin map of H^+/K . One can show that σ is in fact the image of I_∞ . In particular, since $I_\infty^2 = (x)$, we have $\sigma^2 = \text{Id}$.

2.2. Drinfeld \mathcal{A} -modules. For a Dedekind domain \mathcal{A} over \mathbb{F}_q , we define the norm $|a|$ of an element $a \in \mathcal{A}$ to be the cardinality of $\mathcal{A}/\langle a \rangle$. We define the degree of $a \in \mathcal{A}$ to be $\deg(a) := \log_q(|a|)$. Let L be an \mathcal{A} -field, i.e., a field over \mathbb{F}_q equipped with an \mathbb{F}_q -homomorphism $\iota : \mathcal{A} \rightarrow L$. The kernel of ι is called the \mathcal{A} -characteristic of L . Let $L\{\tau\}$ be the non-commutative polynomial ring generated by q -Frobenius endomorphism τ satisfying

$$\tau a = a^q \tau,$$

for all $a \in L$. The non-commutative polynomial ring $L\{\tau\}$ is usually called the twisted polynomial ring over L .

Definition 2.1. We recall that the Drinfeld \mathcal{A} -module of rank $r (\geq 1)$ is defined as the morphism

$$\phi : \mathcal{A} \rightarrow L\{\tau\}$$

of \mathbb{F}_q -algebras such that the image ϕ_a of $a \in \mathcal{A}$ is a twisted polynomial of τ -degree $r \deg(a)$.

In particular, when \mathcal{A} is the Dedekind domain given in Section 2.1, we have $\deg(x) = \deg(y) = 2$. By definition, a rank-two Drinfeld \mathcal{A} -module requires

$$\deg_\tau \phi_x = \deg_\tau \phi_y = 4.$$

Let $\text{LT}_\phi(a)$ be the leading coefficient of ϕ_a . We call ϕ a normalized Drinfeld module (or a Hayes-Drinfeld module) if $\text{LT}_\phi(x) = 1$. It follows directly that $\text{LT}_\phi(y)/\text{LT}_\phi(x)$ equals either ζ or ζ^q . We call ϕ a ζ -type (resp. ζ^q -type) Drinfeld \mathcal{A} -module if $\text{LT}_\phi(y)/\text{LT}_\phi(x)$ equals ζ (resp. ζ^q).

Definition 2.2. Let ϕ and ψ be Drinfeld \mathcal{A} -modules.

(1) We say $\lambda \in L\{\tau\}$ is an isogeny from ϕ to ψ (over L) if the equality

$$\lambda \phi_a = \psi_a \lambda$$

holds for all $a \in \mathcal{A}$.

(2) In particular, if $\lambda \in \bar{L}^*$, we say ϕ is isomorphic to ψ .

Obviously, any Drinfeld \mathcal{A} -module is isomorphic to some normalized Drinfeld \mathcal{A} -module.

2.3. Normalized model. The following theorem is one of the core results in [24], where detailed discussions can be found.

Theorem 2.3. *Let ϕ^λ be the ζ^q -type degree two normalized Drinfeld module parameterized by λ , defined over $H^+(\lambda)$. Its expressions are as follows:*

$$\begin{cases} \phi_x := (\tau^2 + \tilde{\alpha}\tau + \frac{x}{\nu\lambda^{q-1}})(\tau^2 + \alpha\tau + \nu\lambda^{q-1}), \\ \phi_y := \zeta^q(\tau^2 + \tilde{\beta}\tau + \frac{y}{\zeta^q\nu\lambda^{q-1}})(\tau^2 + \alpha\tau + \nu\lambda^{q-1}), \end{cases}$$

where the coefficients satisfy:

$$\begin{aligned} \tilde{\alpha} &= -\frac{\nu T^{\sigma q - (q+\sigma)}}{\zeta \lambda^{q^2}} + \frac{\zeta^q \lambda}{\zeta - \zeta^q}, \\ \tilde{\beta} &= -\frac{\nu T^{\sigma q - (q+\sigma)}}{\zeta \lambda^{q^2}} + \frac{\zeta \lambda}{\zeta - \zeta^q}, \\ \alpha &= \frac{\lambda^{q^2}}{1 - \zeta^{1-q}} + \frac{\nu}{\zeta T \lambda}. \end{aligned}$$

This module ϕ^λ is complete, meaning that any ζ^q -type rank-two normalized Drinfeld module over \bar{L} is isomorphic to ϕ^{λ_0} for some $\lambda_0 \in \bar{L}$.

The isomorphism class of ϕ^λ is determined by the j -invariant, namely

$$j(\phi^\lambda) = \frac{\lambda^{q^2+1}}{\nu}.$$

More precisely, the two Drinfeld modules of ζ^q -type ϕ^{λ_1} and ϕ^{λ_2} are isomorphic if and only if

$$j(\phi^{\lambda_1}) = j(\phi^{\lambda_2}).$$

Applying σ to the coefficients of ϕ^λ yields the ζ -type Drinfeld module $\phi^{\sigma; \lambda'}$ with the formal variable $\lambda' := \lambda^\sigma$. This is in fact the complete family of ζ -type normalized modules of rank two. Moreover, applying σ^k , we have

$$\phi^{\sigma^k; \lambda'} = \begin{cases} \phi^{\sigma; \lambda'}, & \text{when } k \text{ is odd;} \\ \phi^{\lambda'}, & \text{when } k \text{ is even.} \end{cases}$$

Accordingly, the j -invariant of $\phi^{\sigma^k; \lambda'}$ is defined as

$$j(\phi^{\sigma^k; \lambda'}) = \frac{\lambda'^{q^2+1}}{\nu^{\sigma^k}}.$$

2.4. Minimal model. In fact, the isomorphism class of rank-two Drinfeld \mathcal{A} -modules can be represented by the minimal model Φ^j , which is parameterized by the j -invariant and defined over the Hilbert class field of \mathcal{A} . If we choose ℓ to be a root of $\ell^{q-1} = \lambda^q$, then ℓ is essentially an isogeny from Φ^j to ϕ^λ .

Theorem 2.4. *With the notations above, the complete family of ζ^q -type Drinfeld \mathcal{A} -modules of rank two is represented as the minimal model Φ^j (parameterized by j) in the following form:*

$$\begin{aligned} \Phi_x^j &= \ell^{-1} \phi_x^\lambda \ell \\ &= \left(-j^{q(q+1)} T^{(\sigma+q)q} \tau^2 + \left(\frac{T^{\sigma q} j^q}{\zeta} + \frac{j^{q+1} T^{\sigma+q}}{1 - \zeta^{1-q}} \right) \tau + xj \right) \\ &\quad \cdot \left(\tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{1}{\zeta T} \frac{1}{j} \right) \tau + \frac{1}{j} \right), \end{aligned}$$

and

$$\begin{aligned}\Phi_y^j &= \ell^{-1} \phi_y^\lambda \ell \\ &= \left(-j^{q(q+1)} T^{(\sigma+q)q} \zeta^q \tau^2 + \left(\zeta^{q-1} j^q T^{\sigma q} - \frac{\zeta^q T^{\sigma+q} j^{q+1}}{1 - \zeta^{q-1}} \right) \tau + yj \right) \\ &\quad \cdot \left(\tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{1}{\zeta T} \frac{1}{j} \right) \tau + \frac{1}{j} \right).\end{aligned}$$

So any ζ^q -type rank-two Drinfeld \mathcal{A} -module is isomorphic to some Φ^{j_0} .

Obviously, the smallest field of definition of Φ^j is $H(j) = \mathbb{F}_q(T, \zeta, j)$. One may also obtain the minimal model of ζ -type rank-two Drinfeld module $\Phi^{\sigma:j'}$ parameterized by the formal variable j' by applying the σ -action on the coefficients of Φ^j . In the same manner, we adopt the symbol $\Phi^{\sigma^k:j'}$ for the k -th σ -action of Φ^j .

2.5. Torsions. Let ϕ be a rank r Drinfeld \mathcal{A} -module over the \mathcal{A} -field L . Let I be an ideal of \mathcal{A} . Denote by $\phi[I]$ the I -torsion of ϕ , i.e., the intersection of all kernels $\ker \phi_f$ for all $f \in I$. Through the Drinfeld module ϕ , the I -torsion admits a natural \mathcal{A} -module structure. If the \mathcal{A} -characteristic of L is disjoint with I , then the \mathcal{A} -module structure on $\phi[I]$ is isomorphic to $(\mathcal{A}/I)^{\oplus r}$.

Definition 2.5. A primitive \mathfrak{n} -torsion of ϕ is an \mathcal{A} -submodule of $\phi[\mathfrak{n}]$ which is isomorphic to \mathcal{A}/\mathfrak{n} . We denote by $\text{Prim}_{\mathfrak{n}}(\phi)$ the set collecting all the primitive \mathfrak{n} -torsion of ϕ .

Definition 2.6. The maximal common monic right-divisor $\phi_I \in \bar{L}\{\tau\}$ of each ϕ_f for $f \in I$ is called the annihilator of the ideal I .

It is trivial to check that the kernel of ϕ_I coincides with $\phi[I]$. Let $I_\infty = (x, y)$ and $I_0 = (x - \zeta^{-q-1}, y)$. Note that the twisted polynomial $\tau^2 + \alpha\tau + \nu\lambda^{q-1}$ is the common right-divisor of both ϕ_x^λ and ϕ_y^λ , we conclude that

$$\phi_{I_\infty}^\lambda = \tau^2 + \alpha\tau + \nu\lambda^{q-1}. \quad (2)$$

Lemma 2.7 (Equation (48) of [24]). *Let ϕ^λ be the ζ^q -type normalized Drinfeld module introduced above. Then the annihilator $\phi_{I_\infty}^\lambda$ verifies the equality:*

$$\phi_{I_\infty}^\lambda = \frac{\tau + A(\lambda)}{C(\lambda)} \phi_y^\lambda - \frac{\zeta\tau + B(\lambda)}{C(\lambda)} \phi_x^\lambda$$

where

$$A(\lambda) = \frac{\zeta}{\zeta - \zeta^q} \lambda^q, \quad B(\lambda) = \frac{\zeta^2}{\zeta - \zeta^q} \lambda^q, \quad C(\lambda) = \frac{T}{1 - \zeta^{q-1}} \frac{\lambda^q}{\delta}.$$

Moreover, the annihilator $\phi_{I_0}^\lambda$ for the ideal I_0 is also determined in [24]:

$$\phi_{I_0}^\lambda = \phi_{I_\infty}^\lambda + \frac{(1 - \zeta^{q-1})\nu}{\zeta^q T \lambda} \tau + \frac{\nu\lambda^{q-1}}{\zeta^q T}.$$

We remark that the explicit formula of ϕ^λ is indeed deduced from the expressions of $\phi_{I_\infty}^\lambda$ and $\phi_{I_0}^\lambda$ through technical computations. For the minimal model Φ^j , one may show that

$$\Phi_{I_\infty}^j = \tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{1}{\zeta T} \frac{1}{j} \right) \tau + \frac{1}{j}$$

and

$$\Phi_{I_0}^j = \tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{1}{\zeta^q T j} \right) \tau + \left(\frac{1}{\zeta^q T} + 1 \right) \frac{1}{j}.$$

2.6. Modular curves. Let \mathcal{A} temporarily be a Dedekind domain with quotient field K . For a congruence subgroup Γ of $\mathrm{GL}_2(\mathcal{A})$, the quotient of the Drinfeld upper plane by Γ classifies isomorphism classes of Drinfeld modules equipped with some "level structure". These quotients are the analogs of various modular curves classifying elliptic curves.

For a nonzero ideal $\mathfrak{n} \in \mathcal{A}$, Gekeler investigates in [16] (among other things) the Drinfeld modular curve $Y_0(\mathfrak{n})$, defined as the Drinfeld upper space modulo the arithmetic subgroup

$$\Gamma_0(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{A}) \mid c \equiv 0 \pmod{\mathfrak{n}} \right\}.$$

The points on the curve $Y_0(\mathfrak{n})$ parametrize isomorphism classes of pairs of Drinfeld \mathcal{A} -modules of rank two together with a primitive \mathfrak{n} -torsion.

Adding so-called cusps to $Y_0(\mathfrak{n})$ gives a projective algebraic curve $X_0(\mathfrak{n})$ defined over K that in general however will not be absolutely irreducible. Indeed, the irreducible components are in one-to-one correspondence with the class group $\mathrm{Cl}(\mathcal{A})$ of \mathcal{A} . It is straightforward to see that the absolutely irreducible components of $X_0(\mathfrak{n})$ are mutually isomorphic by considering the action of $\mathrm{Cl}(\mathcal{A})$. We will denote by $\mathbf{x}_0(\mathfrak{n})$ an absolutely irreducible component of $X_0(\mathfrak{n})$. The cusps are distributed equally among the absolutely irreducible components of $X_0(\mathfrak{n})$. In particular, there exist exactly $|\mathrm{Cl}(\mathcal{A})|$ cusps on the modular curve $\mathbf{x}_0(1)$.

To simplify notation, we use the informal definition of the absolutely irreducible component of $X_0(\mathfrak{n})$ as follows.

Definition 2.8. Let G and H be corresponding \mathfrak{n} -torsion of Drinfeld modules ϕ and ψ respectively. We say that the pair (ϕ, G) is equivalent to (ψ, H) , if there exists an isogeny $\lambda \in \bar{L}\{\tau\}$ from ϕ to ψ such that $\lambda G = H$.

Definition 2.9 (Minimal Modular Curve). We formally define the $(\zeta^q\text{-type})$ modular curve $\mathbf{x}_0(\mathfrak{n})$ as the algebraic curve that parametrizes the pairs (ϕ, G) modulo the equivalence in Definition 2.8, where ϕ denotes the $\zeta^q\text{-type}$ Drinfeld \mathcal{A} -modules and G denotes a primitive \mathfrak{n} -torsion of ϕ .

Analogously, we restrict the Drinfeld modules to be normalized, then we obtain the similar concept of modular curve:

Definition 2.10 (Normalized modular curve). The $(\zeta^q\text{-type})$ normalized modular curve $\dot{\mathbf{x}}_0(\mathfrak{n})$ is an algebraic curve parametrizing the pairs (ϕ, G) , where ϕ denotes a $\zeta^q\text{-type}$ normalized Drinfeld \mathcal{A} -modules and G denotes a primitive \mathfrak{n} -torsion of ϕ .

In particular, we choose \mathfrak{n} to be of the form I_∞^k with $k \geq 1$. Then there are exactly

$$|\mathrm{Prim}_{\mathfrak{n}}(\phi)| = (q+1)q^{k-1} \tag{3}$$

distinct choices of primitive I_∞^k -torsion of ϕ . For a primitive I_∞^{k+1} -torsion G of ϕ , we know

$$I_\infty \cdot G := \{\phi_z(\mu) \mid \mu \in G, z \in I_\infty\}$$

forms a primitive I_∞^k -torsion. Since a geometric point of $\mathbf{x}_0(I_\infty^{k+1})$ is represented by the pair (ϕ, G) , the map $(\phi, G) \mapsto (\phi, I_\infty \cdot G)$ induces a covering morphism from $\mathbf{x}_0(I_\infty^{k+1})$ to $\mathbf{x}_0(I_\infty^k)$. So the covering degree of $\mathbf{x}_0(I_\infty^{k+1})$ over $\mathbf{x}_0(I_\infty^k)$ is given by

$$[\mathbf{x}_0(I_\infty^{k+1}) : \mathbf{x}_0(I_\infty^k)] = \frac{|\mathrm{Prim}_{I_\infty^{k+1}}(\phi)|}{|\mathrm{Prim}_{I_\infty^k}(\phi)|} = \begin{cases} q+1, & \text{when } k=0; \\ q, & \text{when } k \geq 1. \end{cases}$$

This formula coincides with degrees displayed in Theorem B.

3. NORMALIZED DRINFELD MODULAR TOWER

We wish to construct the normalized Drinfeld modular tower in this section. We begin with the construction of isogeny

$$\tau - u_1 : \phi^{\lambda_0} \rightarrow \phi^{\sigma; \lambda_1}$$

for the normalized Drinfeld \mathcal{A} -modules.

3.1. Isogeny formula. Suppose that $\mu_1 \in \phi^{\lambda_0}[I_\infty]$, namely

$$\phi_x^{\lambda_0}(\mu_1) = 0 \quad \text{and} \quad \phi_y^{\lambda_0}(\mu_1) = 0.$$

Since the twisted polynomial $\phi_{I_\infty}^{\lambda_0}$ (see Equation (2)) is the annihilator of I_∞ , we have

$$\phi_{I_\infty}^{\lambda_0}(\mu_1) = (\tau^2 + \alpha\tau + \nu\lambda_0^{q-1})(\mu_1) = 0.$$

Let $u_1 = \mu_1^{q-1}$. Then u_1 satisfies the equality

$$\xi^{\lambda_0}(u_1) := u_1^{q+1} + \left(\frac{\lambda_0^q}{1 - \zeta^{1-q}} + \frac{\nu}{\zeta T \lambda_0} \right) u_1 + \nu \lambda_0^{q-1} = 0. \quad (4)$$

Since $\tau - u_1$ is a right-divisor of $\phi_x^{\lambda_0}$ and $\phi_y^{\lambda_0}$, we know that $\tau - u_1$ is an isogeny from ϕ^{λ_0} to some Drinfeld module of ζ -type, say $\phi^{\sigma; \lambda_1}$. That is

$$(\tau - u_1)\phi_a^{\lambda_0} = \phi_a^{\sigma; \lambda_1}(\tau - u_1)$$

for all $a \in \mathcal{A}$. The following lemma determines the value of λ_1 .

Lemma 3.1. *Let ϕ^{λ_0} and $\phi^{\sigma; \lambda_1} : \mathcal{A} \rightarrow L\{\tau\}$ denote the normalized Drinfeld \mathcal{A} -modules of ζ^q -type and ζ -type respectively. Suppose that $\xi^{\lambda_0}(u_1) = 0$. Then $\tau - u_1$ is an isogeny from ϕ^{λ_0} to $\phi^{\sigma; \lambda_1}$, where*

$$\lambda_1 = \lambda_0^q - (\zeta^{q-1} - 1)u_1. \quad (5)$$

Proof. Without loss of generality, we may assume that L is a perfect field extension over $\mathbb{F}_q(t, \zeta)$ containing both λ_0 and λ_1 . We define

$$V = \{(a, b) \in L\{\tau\}^2 \mid \deg_\tau(a\phi_y^{\lambda_0} + b\phi_x^{\lambda_0}) \leq 3, \deg_\tau(a) \leq 2, \deg_\tau(b) \leq 2\}.$$

It is clear that V is a three-dimensional L -vector space and contains the following three vectors by Lemma 2.7:

$$\begin{aligned} \mathbf{e}_1 &= (1, -\zeta^q), \\ \mathbf{e}_2 &= \left(\frac{\tau + A(\lambda_0)}{C(\lambda_0)}, -\frac{\zeta\tau + B(\lambda_0)}{C(\lambda_0)} \right), \\ \mathbf{e}_3 &= \tau \left(\frac{\tau + A(\lambda_0)}{C(\lambda_0)}, -\frac{\zeta\tau + B(\lambda_0)}{C(\lambda_0)} \right). \end{aligned}$$

Since $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ are linearly independent, they form an L -basis of V .

By the ζ -type version of Lemma 2.7, we have

$$\phi_{I_\infty}^{\sigma; \lambda_1} = \left(\frac{\tau + A(\lambda_1)}{C(\lambda_1)} \right)^\sigma \phi_y^{\sigma; \lambda_1} - \left(\frac{\zeta\tau + B(\lambda_1)}{C(\lambda_1)} \right)^\sigma \phi_x^{\sigma; \lambda_1}.$$

By assumption, $\tau - u_1$ is an isogeny, we have

$$\begin{aligned} \phi_{I_\infty}^{\sigma; \lambda_1}(\tau - u_1) &= \left(\frac{\tau + A(\lambda_1)}{C(\lambda_1)} \right)^\sigma \phi_y^{\sigma; \lambda_1}(\tau - u_1) - \left(\frac{\zeta\tau + B(\lambda_1)}{C(\lambda_1)} \right)^\sigma \phi_x^{\sigma; \lambda_1}(\tau - u_1) \\ &= \left(\frac{\tau + A(\lambda_1)}{C(\lambda_1)} \right)^\sigma (\tau - u_1)\phi_y^{\lambda_0} - \left(\frac{\zeta\tau + B(\lambda_1)}{C(\lambda_1)} \right)^\sigma (\tau - u_1)\phi_x^{\lambda_0} \end{aligned}$$

$$=:v_1\phi_y^{\lambda_0} + v_2\phi_x^{\lambda_0}.$$

It yields that the pair $\mathbf{v} = (v_1, v_2) \in L\{\tau\}^2$ satisfies the required condition of V . Then there exist some coefficients $t_1, t_2, t_3 \in L$, such that

$$\mathbf{v} = t_1\mathbf{e}_1 + t_2\mathbf{e}_2 + t_3\mathbf{e}_3,$$

namely,

$$\begin{aligned} & \left(\left(\frac{\tau + A(\lambda_1)}{C(\lambda_1)} \right)^\sigma (\tau - u_1), - \left(\frac{\zeta\tau + B(\lambda_1)}{C(\lambda_1)} \right)^\sigma (\tau - u_1) \right) \\ &= \left(t_1 + (t_2 + t_3\tau) \frac{\tau + A(\lambda_0)}{C(\lambda_0)}, -\zeta^q t_1 - (t_2 + t_3\tau) \frac{\zeta\tau + B(\lambda_0)}{C(\lambda_0)} \right). \end{aligned} \quad (6)$$

We now compare the coefficients of τ^i -terms for $i = 0, 1, 2$ in the above equation, proceeding as follows.

- (1) By comparing the τ^2 -terms of (6), we have

$$\left(\frac{1}{C(\lambda_1)^\sigma}, \frac{\zeta^\sigma}{C(\lambda_1)^\sigma} \right) = (t_3 C(\lambda_0)^{-q}, t_3 \zeta^q C(\lambda_0)^{-q}).$$

This is equivalent to

$$t_3 = C(\lambda_0)^q C(\lambda_1)^{-\sigma}.$$

- (2) Coefficients of the τ -terms in (6) yield that

$$\begin{aligned} & \left(-\frac{u_1^q}{C(\lambda_1)^\sigma} + \frac{A(\lambda_1)^\sigma}{C(\lambda_1)^\sigma}, \zeta^\sigma \frac{u_1^q}{C(\lambda_1)^\sigma} - \frac{B(\lambda_1)^\sigma}{C(\lambda_1)^\sigma} \right) \\ &= \left(\frac{t_2}{C(\lambda_0)} + \frac{t_3 A(\lambda_0)^q}{C(\lambda_0)^q}, -\frac{t_2 \zeta}{C(\lambda_0)} - \frac{t_3 B(\lambda_0)^q}{C(\lambda_0)^q} \right). \end{aligned}$$

Substituting $t_3 = \frac{C(\lambda_0)^q}{C(\lambda_1)^\sigma}$ into the above equality, equating the first coordinates yields

$$t_2 = \frac{C(\lambda_0)}{C(\lambda_1)^\sigma} (A(\lambda_1)^\sigma - u_1^q - A(\lambda_0)^q),$$

while equating the second coordinates yields

$$t_2 = \frac{C(\lambda_0)}{\zeta C(\lambda_1)^\sigma} (-B(\lambda_0)^q - \zeta^\sigma u_1^q + B(\lambda_1)^\sigma).$$

Equating these two expressions for t_2 implies

$$\zeta (A(\lambda_1)^\sigma - u_1^q - A(\lambda_0)^q) = -B(\lambda_0)^q - \zeta^\sigma u_1^q + B(\lambda_1)^\sigma,$$

or equivalently,

$$\lambda_1^q = \lambda_0^{q^2} - (\zeta^{1-q} - 1)u_1^q.$$

Since L is perfect, taking the q -th root of both sides gives

$$\lambda_1 = \lambda_0^q - (\zeta^{q-1} - 1)u_1.$$

- (3) From the constant terms of (6), it follows

$$\left(-\frac{A(\lambda_1)^\sigma u_1}{C(\lambda_1)^\sigma}, \frac{B(\lambda_1)^\sigma u_1}{C(\lambda_1)^\sigma} \right) = \left(t_1 + t_2 \frac{A(\lambda_0)}{C(\lambda_0)}, -\zeta^q t_1 - t_2 \frac{B(\lambda_0)}{C(\lambda_0)} \right).$$

Equating the first coordinates, we obtain

$$t_1 = -\frac{A(\lambda_1)^\sigma u_1}{C(\lambda_1)^\sigma} - t_2 \frac{A(\lambda_0)}{C(\lambda_0)}$$

$$= \frac{1}{C(\lambda_1)^\sigma} (-A(\lambda_1)^\sigma u_1 - A(\lambda_0)A(\lambda_1)^\sigma + A(\lambda_0)u_1^q + A(\lambda_0)^{q+1}).$$

Equating the second coordinates, we obtain

$$\begin{aligned} t_1 &= -\frac{B(\lambda_1)^\sigma u_1}{\zeta^q C(\lambda_1)^\sigma} - t_2 \frac{B(\lambda_0)}{C(\lambda_0)} \\ &= \frac{1}{\zeta C(\lambda_1)^\sigma} (-\zeta^{1-q} B(\lambda_1)^\sigma u_1 + B(\lambda_0)^{q+1} + \zeta^\sigma B(\lambda_0)u_1^q - B(\lambda_0)B(\lambda_1)^\sigma). \end{aligned}$$

Hence, we get

$$t_2 = 0, \quad t_1 = -\frac{A(\lambda_1)^\sigma u_1}{C(\lambda_1)^\sigma}.$$

In conclusion, the isogeny relation between ϕ^{λ_0} and $\phi^{\sigma; \lambda_1}$ is

$$\lambda_1 = \lambda_0^q - (\zeta^{q-1} - 1)u_1.$$

□

3.2. Description of the primitive torsions. We recall the useful lemma in [27, Lemma 3.1.5].

Lemma 3.2. *Let W be an n -dimensional \mathbb{F}_q -vector space of \bar{K} , then there exists a unique monic twisted polynomial ω of τ -degree n such that $W = \ker \omega$.*

If W is identical to a I_∞^n -torsion G_n of Drinfeld module ϕ , we obtain a stronger form for ω .

Lemma 3.3. *Given a primitive I_∞^n -torsion G_n of Drinfeld module ϕ , there is a sequence of nonzero elements u_1, u_2, \dots, u_n in \bar{K} such that G_n is represented as the kernel of the twisted polynomial*

$$\omega_n = (\tau - u_n) \cdots (\tau - u_2)(\tau - u_1). \quad (7)$$

Proof. Fix an integer $n \geq 0$, and set $G_i = I_\infty^{n-i} G_n$ for $i = 0, 1, \dots, n$. We obtain the sequence

$$0 = G_0 \subseteq G_1 \subseteq G_2 \subseteq G_3 \subseteq \cdots \subseteq G_n.$$

Since G_n is primitive, there is no doubt that G_i is a primitive I_∞^i -torsion of ϕ . We know from Lemma 3.2 that G_i is given by the kernel of some twisted polynomial ω_i . In particular, $\omega_0 = 1$. Since $G_i \subsetneq G_{i+1}$, we know ω_i is a right-divisor of ω_{i+1} , i.e.,

$$\omega_{i+1} = (\tau - u_{i+1})\omega_i.$$

Therefore, we have the expression (7). □

Indeed, the variables u_1, \dots, u_n can be expressed by the basis of G_n . Let us fix the primitive I_∞^n -torsion G_n of a Drinfeld \mathcal{A} -module ϕ . By Lemma 3.3, we know there exist u_1, \dots, u_n , such that

$$G_n = \ker \omega_n = \ker(\tau - u_n) \cdots (\tau - u_2)(\tau - u_1). \quad (8)$$

Suppose that $\alpha_1, \dots, \alpha_n$ is the basis of G_n such that α_i is contained in $G_i \setminus G_{i-1}$. Then α_i satisfies

$$\omega_i(\alpha_i) = (\tau - u_i)\omega_{i-1}(\alpha_i) = 0$$

and

$$\omega_{i-1}(\alpha_i) \neq 0.$$

This implies that

$$u_i = \omega_{i-1}(\alpha_i)^{q-1}. \quad (9)$$

3.3. Iterative formula of isogeny. Let u_i, α_i, ω_i be defined as above associated to the primitive I_∞ -torsion G_n of the ζ^q -type normalized Drinfeld module ϕ^{λ_0} .

Lemma 3.4. *Maintain the notations above. Suppose that λ_k with $1 \leq k \leq n$ is defined by the iterative formula*

$$\lambda_k = \lambda_{k-1}^q - (\zeta^{q^k - q^{k-1}} - 1)u_k. \quad (10)$$

Then

$$\phi_{I_\infty}^{\sigma^{k-1}; \lambda_{k-1}}(\omega_{k-1}(\alpha_k)) = 0, \quad (11)$$

or equivalently, u_k and λ_{k-1} satisfy

$$\xi^{\sigma^{k-1}; \lambda_{k-1}}(u_k) := u_k^{q+1} + \left(\frac{\lambda_{k-1}^{q^2}}{1 - \zeta^{q^{k-1} - q^k}} + \frac{\nu^{\sigma^{k-1}}}{\zeta^{q^{k-1}} T^{\sigma^{k-1}} \lambda_{k-1}} \right) u_k + \nu^{\sigma^{k-1}} \lambda_{k-1}^{q-1} = 0. \quad (12)$$

Moreover, the twisted polynomial ω_k represents an isogeny from ϕ^{λ_0} to $\phi^{\sigma^k; \lambda_k}$, namely,

$$\omega_k \phi^{\lambda_0} = \phi^{\sigma^k; \lambda_k} \omega_k. \quad (13)$$

Proof. For the case $k = 1$, the equality (11) just says that α_1 is contained in G_1 , which has been investigated in Section 3.1. Since $u_1 = \omega_0(\alpha_1)^{q-1} = \alpha_1^{q-1}$, we know from Section 3.1 that u_1 and λ_0 automatically satisfy Equation (4), i.e., $\xi^{\lambda_0}(u_1) = 0$. Equation (13) with $k = 1$ has been shown in Lemma 3.1.

Moreover, we can deduce the equivalence of (11) and (12) by the equality (9) for each $k \leq n$.

Next, we assume by induction that the lemma is valid for $1 \leq k \leq i$. It suffices to prove the case $k = i + 1$. By definition, G_{i+1} is a primitive I_∞^{i+1} -torsion of ϕ^{λ_0} . For $z \in I_\infty$, we have

$$\phi_z^{\lambda_0} G_{i+1} \subseteq G_i. \quad (14)$$

From Equation (8), it yields that $\phi_z^{\lambda_0}(\alpha_{i+1})$ is always annihilated by ω_i . Equation (13) with $k = i$ implies that

$$0 = \omega_i(\phi_z^{\lambda_0}(\alpha_{i+1})) = \phi_z^{\sigma^i; \lambda_i}(\omega_i \alpha_{i+1}) \quad \text{for all } z \in I_\infty. \quad (15)$$

Note that ϕ_{I_∞} is the annihilator of ideal I_∞ . Thus, (15) is equivalent to

$$\phi_{I_\infty}^{\sigma^i; \lambda_i}(\omega_i \alpha_{i+1}) = 0.$$

This verifies the Equation (11) with $k = i + 1$.

On the other hand, applying the k -th σ -action in Lemma 3.1, the relation of λ_i and λ_{i+1} gives that

$$(\tau - u_{i+1}) \phi^{\sigma^i; \lambda_i} = \phi^{\sigma^{i+1}; \lambda_{i+1}}(\tau - u_{i+1}). \quad (16)$$

Therefore,

$$\begin{aligned} \omega_{i+1} \phi^{\lambda_0} &= (\tau - u_{i+1}) \omega_i \phi^{\lambda_0} \\ &= (\tau - u_{i+1}) \phi^{\sigma^i; \lambda_i} \omega_i \\ &= \phi^{\sigma^{i+1}; \lambda_{i+1}}(\tau - u_{i+1}) \omega_i \quad \text{By (16)} \\ &= \phi^{\sigma^{i+1}; \lambda_{i+1}} \omega_{i+1}. \end{aligned}$$

The equality holds for $k = i + 1$. □

3.4. Restrictions on primitive I_∞^{i+1} -torsion. Next, we need to derive the restriction on the variables u_{i+1} from the information on G_n , a primitive I_∞^{i+1} -torsion of ϕ^{λ_0} . In our assumption, G_{i+1} shall be a primitive I_∞^{i+1} -torsion. It splits into two conditions:

- (1) For $z \in I_\infty$, $\phi_z^{\lambda_0}(G_{i+1})$ is contained in G_i , i.e., Equation (15) holds;
- (2) $\phi_z^{\lambda_0}(G_{i+1})$ is not always contained in G_{i-1} .

From the proof of lemma 3.4, we know the first condition is equivalent to

$$\xi^{\sigma^i; \lambda_i}(u_{i+1}) = 0.$$

The second condition requires that $\phi_z^{\lambda_0}(\alpha_{i+1})$ is not always annihilated by ω_{i-1} . Equivalently,

$$\phi_{I_\infty}^{\sigma^{i-1}; \lambda_{i-1}} \omega_{i-1}(\alpha_{i+1}) \neq 0. \quad (17)$$

The equality (11) with $k = i - 1$ says that $\omega_{i-1}(\alpha_i)$ is annihilated by $\phi_{I_\infty}^{\sigma^{i-1}; \lambda_{i-1}}$. This yields that $(\tau - u_i)$ is a right-divisor of $\phi_{I_\infty}^{\sigma^{i-1}; \lambda_{i-1}}$. In fact, we obtain the decomposition

$$\phi_{I_\infty}^{\sigma^{i-1}; \lambda_{i-1}} = (\tau - u_i^\nabla) (\tau - u_i),$$

where $u_i^\nabla := \frac{\nu^{\sigma^{i-1}} \lambda_{i-1}^{q-1}}{u_i}$. Thus, the left hand side of (17) equals

$$\begin{aligned} \phi_{I_\infty}^{\sigma^{i-1}; \lambda_{i-1}} \omega_{i-1}(\alpha_{i+1}) &= (\tau - u_i^\nabla) (\tau - u_i) (\omega_{i-1}(\alpha_{i+1})) \\ &= (\tau - u_i^\nabla) (\omega_i(\alpha_{i+1})) \\ &= \omega_i(\alpha_{i+1}) \cdot (u_{i+1} - u_i^\nabla). \end{aligned}$$

Since $\omega_i(\alpha_{i+1}) \neq 0$, Equation (17) is the same as $u_{i+1} \neq u_i^\nabla$. From the argument above, we see that $u_{i+1} = u_i^\nabla$ must be a root of $\xi^{\sigma^i; \lambda_i}(u_{i+1})$.

Indeed, it is straightforward to check that polynomial $\xi^{\sigma^i; \lambda_i}(u_{i+1})$ admits a decomposition

$$\xi^{\sigma^i; \lambda_i}(u_{i+1}) = \xi_{\nabla}^{\sigma^i; \lambda_i}(u_{i+1}) \cdot (u_{i+1} - u_i^\nabla),$$

where

$$\begin{aligned} \xi_{\nabla}^{\sigma^i; \lambda_i}(u_{i+1}) &= \frac{\lambda_i^{q^2}}{1 - \zeta^{(1-q)q^i}} + \frac{\nu^{\sigma^i}}{T^{\sigma^i} \lambda_i \zeta^{q^i}} + \sum_{s=0}^q (u_i^\nabla)^s u_{i+1}^{q-s} \\ &= -\lambda_i^{q-1} \frac{\nu^{\sigma^i} u_i}{\nu^{\sigma^{i-1}} \lambda_{i-1}^{q-1}} + \sum_{s=0}^{q-1} (u_i^\nabla)^s u_{i+1}^{q-s}. \end{aligned} \quad (18)$$

In conclusion, the two conditions on G_{i+1} together are equivalent to

$$\xi_{\nabla}^{\sigma^i; \lambda_i}(u_{i+1}) = 0.$$

3.5. Proof of Theorem A. Now we are able to state the proof of Theorem A.

Proof of Theorem A. For the case $k = 0$, the theorem just says that λ_0 represents the complete family of ζ^q -type normalized \mathcal{A} -Drinfeld module, which has been investigated in Theorem 2.3.

For $k \geq 1$, from the definition of Drinfeld modular curves, it suffices to show that $\lambda_0, \dots, \lambda_k$ is in one-to-one correspondence with primitive I_∞^k -torsions of ϕ^{λ_0} .

The case $k = 1$ can be easily checked that (λ_0, u_1) corresponds to the primitive I_∞ -torsion

$$G_1 = \ker(\tau - u_1)$$

where u_1 verifies $\xi^{\lambda_0}(u_1) = 0$. Indicated by Equation (5), we choose transformation:

$$u_1 := \frac{\lambda_0^q - \lambda_1}{\zeta^{q-1} - 1}.$$

Substituting u_1 into ξ^{λ_0} it yields that

$$\xi^{\lambda_0} \left(\frac{\lambda_0^q - \lambda_1}{\zeta^{q-1} - 1} \right) = 0,$$

i.e.,

$$\lambda_1^{q+1} - \lambda_0^q \lambda_1^q - \frac{\zeta^{1-q} - 1}{\zeta T \lambda_0} \nu \lambda_1 + \left(\frac{\zeta^{1-q} - 1}{\zeta T} + (\zeta^{q-1} - 1)^{q+1} \right) \nu \lambda_0^{q-1} = 0.$$

So (λ_0, λ_1) is in one-to-one correspondence with primitive I_∞ -torsion.

Next, we assume that $k \geq 2$. Given the primitive I_∞^k -torsion G_k , we construct u_i, λ_i as above. In Section 3.4, we have realized that it is equivalent to

$$\xi_{\nabla}^{\sigma^i; \lambda_i}(u_{i+1}) = 0, \quad (19)$$

for $i = 0, \dots, k-1$. It follows from the equality (10) of Lemma 3.4 that

$$u_{i+1} := \frac{\lambda_i^q - \lambda_{i+1}}{\zeta^{q^{i+1}-q^i} - 1}$$

and

$$u_i := \frac{\lambda_{i-1}^q - \lambda_i}{\zeta^{q^i - q^{i-1}} - 1}.$$

Combining these with Equation (19), we have

$$\begin{aligned} \xi_{\nabla}^{\sigma^i; \lambda_i}(u_{i+1}) &= -\lambda_i^{q-1} \frac{\nu^{\sigma^i} (\lambda_i - \lambda_{i-1}^q)}{\nu^{\sigma^{i-1}} \lambda_{i-1}^{q-1}} \\ &\quad + \sum_{s=0}^{q-1} \left(\frac{\nu^{\sigma^{i-1}} \lambda_{i-1}^{q-1} (1 - \zeta^{1-q})^{q+1}}{\lambda_i - \lambda_{i-1}^q} \right)^s (\lambda_{i+1} - \lambda_i^q)^{q-s} = 0. \end{aligned} \quad (20)$$

Conversely, we can reconstruct the I_∞^i -primitive torsions G_i through λ_i as follows:

$$\begin{aligned} G_i &= \ker(\omega_i) \\ &= \ker \left(\tau - \frac{\lambda_i - \lambda_{i-1}^q}{1 - \zeta^{(1-q)q^{i-2}}} \right) \left(\tau - \frac{\lambda_{i-1} - \lambda_{i-2}^q}{1 - \zeta^{(1-q)q^{i-3}}} \right) \cdots \left(\tau - \frac{\lambda_1 - \lambda_0^q}{1 - \zeta^{(1-q)q^{-1}}} \right) \end{aligned}$$

where $\lambda_0, \dots, \lambda_i$ verifies the recursive condition (20). \square

4. MINIMAL DRINFELD MODULAR TOWER

4.1. The modular curve $\mathbf{x}_0(I_\infty)$. We start with a minimal Drinfeld module Φ^{j_0} parameterized by the j -invariant j_0 . We know from Section 2.4 that a $(q-1)$ -th root of λ_0^q gives an isogeny from Φ^{j_0} to ϕ^{λ_0} , where λ_0 satisfies

$$j_0 = \frac{\lambda_0^{q^2+1}}{\nu}. \quad (21)$$

Suppose that $\beta_1 \neq 0$ is contained in $\Phi^{j_0}[I_\infty]$, i.e., $\Phi_{I_\infty}^{j_0}(\beta_1) = 0$. Then the space $G_1 := \mathbb{F}_q \beta_1$ is a primitive I_∞ -torsion of Φ^{j_0} . From the isogeny ℓ_0 , we find that the element $\alpha_1 := \ell_0 \beta_1$ is annihilated by ϕ_{I_∞} , and hence

$$\Phi_{I_\infty}^{j_0} = \ell_0^{-q^2} \phi_{I_\infty}^{\lambda_0} \ell_0. \quad (22)$$

Substituting the expression (2), we obtain

$$\Phi_{I_\infty}^{j_0} = \tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{1}{\zeta T} \frac{1}{j_0} \right) \tau + \frac{1}{j_0}. \quad (23)$$

This equality can also be deduced from the expression of Φ^{j_0} , as $\Phi_{I_\infty}^{j_0}$ is exactly the right-divisor of both $\Phi_x^{j_0}$ and $\Phi_y^{j_0}$.

Take $w_1 = \beta_1^{q-1}$. Then applying (23) yields that

$$\Xi^{j_0}(w_1) := w_1^{q+1} + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{1}{\zeta T j_0} \right) w_1 + \frac{1}{j_0} = \frac{1}{\beta_1} \Phi_{I_\infty}^{j_0}(\beta_1) = 0. \quad (24)$$

Since G_1 can be expressed as $\ker(\tau - w_1)$, we find that the function field of the modular curve $\mathbf{x}_0(I_\infty)$ is $H(j_0, w_1)$, where j_0, w_1 are subject to (24). Furthermore, from the equation (24), the j -invariant of Φ^{j_0} is determined by w_1 of the form

$$j_0 = \frac{-(1 + \zeta^{-1} T^{-1} \beta_1^{q-1})}{\beta_1^{q^2-1} + (1 - \zeta^{1-q})^{-1} \beta_1^{q-1}} = \frac{(\zeta^{1-q} - 1)(1 + \zeta^{-1} T^{-1} w_1)}{w_1 (1 + (1 - \zeta^{1-q}) w_1^q)}. \quad (25)$$

Thus the function field of the modular curve $\mathbf{x}_0(I_\infty)$ is rational and is generated by w_1 .

4.2. Isogeny formula for minimal Drinfeld modules. In the rest, we always assume that w_1 and j_0 satisfy the equality (25). We have seen that the isogeny relation

$$(\tau - u_1) \phi^{\lambda_0} = \phi^{\sigma; \lambda_1} (\tau - u_1) \quad (26)$$

is essential in the construction of normalized Drinfeld modular tower. We now derive the analogous relation for Φ^{j_0} .

Lemma 4.1. *Suppose that w_1 is a root of the equation $\Xi^{j_0}(w_1) = 0$. Let δ_1 be a $(q-1)$ -th root of the constant $(1 - (\zeta^{1-q} - 1)w_1^q)^{-1}$. Then the twisted polynomial*

$$\Omega_1 := \delta_1(\tau - w_1)$$

represents an isogeny from Φ^{j_0} to $\Phi^{\sigma; j_1}$, where j_1 is determined by

$$j_1 = T^{q-1} j_0^q (1 + (1 - \zeta^{q-1}) w_1)^{q^2+1} \quad (27)$$

$$= T^{-1} (\zeta^{q-1} - 1) (1 + (1 - \zeta^{q-1}) w_1) (T^q w_1^{-q} + \zeta^{-q}). \quad (28)$$

Proof. Let ϕ^{λ_0} and $\phi^{\sigma; \lambda_1}$ be the same notation as in Equation (26). Let ℓ_0 be a $(q-1)$ -th root of λ_0^q ; and ℓ_1 a $(q-1)$ -th root of λ_1^q . Let j_1 be the j -invariant of $\phi^{\sigma; \lambda_1}$, i.e.,

$$j_1 = \frac{\lambda_1^{q^2+1}}{\nu^\sigma}.$$

We obtain the diagram of square consisting of isogenies:

$$\begin{array}{ccc} \phi^{\lambda_0} & \xrightarrow{\tau - u_1} & \phi^{\sigma; \lambda_1} \\ \ell_0 \uparrow & & \ell_1 \uparrow \\ \Phi^{j_0} & \longrightarrow & \Phi^{\sigma; j_1} \end{array} \quad (29)$$

As in Section 4.1, we choose β_1 to be a $(q-1)$ -th root of w_1 . Note that $\beta_1 \in \Phi^{j_0}[I_\infty]$, and $\alpha_1 := \ell_0 \beta_1$ is then contained in the I_∞ -torsion of ϕ^{λ_0} . By the assumption $u_1 = \alpha_1^{q-1}$ and $w_1 = \beta_1^{q-1}$, we obtain

$$w_1 \ell_0^{q-1} = u_1.$$

From the diagram (29), the isogeny from Φ^{j_0} to $\Phi^{\sigma; j_1}$ can be written as

$$\Omega_1 := \ell_1^{-1} (\tau - u_1) \ell_0 = \ell_1^{-1} \ell_0^q (\tau - w_1) = \delta_1 (\tau - w_1),$$

where $\delta_1 = \ell_1^{-1} \ell_0^q$. Indeed, this can be checked directly:

$$\delta_1 (\tau - w_1) \Phi^{j_0} = \ell_1^{-1} (\tau - u_1) \phi^{\lambda_0} \ell_0 \quad \text{By (22)}$$

$$\begin{aligned}
&= \ell_1^{-1} \phi^{\sigma; \lambda_1}(\tau - u_1) \ell_0 \quad \text{By (26)} \\
&= \Phi^{\sigma; j_1} \ell_1^{-1}(\tau - u_1) \ell_0 \quad \text{Analogous to (22)} \\
&= \Phi^{\sigma; j_1} \ell_1^{-1} \ell_0^q(\tau - w_1) \\
&= \Phi^{\sigma; j_1} \delta_1(\tau - w_1).
\end{aligned}$$

Next, we need to compute δ_1 and j_1 . From the relation

$$\lambda_1 = \lambda_0^q - (\zeta^{q-1} - 1)u_1 = \lambda_0^q (1 - (\zeta^{q-1} - 1)w_1)$$

we have

$$\delta_1^{q-1} = (\ell_0^q \ell_1^{-1})^{q-1} = \lambda_0^{q^2} \lambda_1^{-q} = \frac{1}{1 + (1 - \zeta^{1-q})w_1^q}. \quad (30)$$

It follows from the expression ν^σ in (1) that

$$\begin{aligned}
j_1 &= \frac{\lambda_1^{q^2+1}}{\nu^\sigma} = \frac{1}{\nu^\sigma} (\lambda_0^q (1 + (1 - \zeta^{q-1})w_1))^{q^2+1} \\
&= \frac{T^{q-1} \lambda_0^{q(q^2+1)}}{\nu^q} ((1 + (1 - \zeta^{q-1})w_1))^{q^2+1} \\
&= T^{q-1} j_0^q ((1 + (1 - \zeta^{q-1})w_1))^{q^2+1},
\end{aligned}$$

where we apply Equation (21) in the last equality. So the equality (27) is valid.

Set $w_1^\nabla := (\zeta^{1-q} - 1)^{-1} (1 + \zeta^{-1} T^{-1} w_1)^{-1}$. From Equation (25), we have

$$\frac{\delta_1^{q-1}}{w_1^\nabla w_1} = \frac{1}{(1 + (1 - \zeta^{1-q})w_1^q) w_1 \cdot w_1^\nabla} = j_0.$$

Substituting this into the expression (27), we have

$$\begin{aligned}
j_1 &= T^{q-1} j_0^q (1 + (1 - \zeta^{q-1})w_1)^{q^2+1} \\
&= T^{q-1} \frac{(1 + (1 - \zeta^{q-1})w_1^q)^2 (1 + (1 - \zeta^{q-1})w_1)}{1 + (1 - \zeta^{q-1})w_1^q} \left(\frac{1}{w_1 w_1^\nabla} \right)^q \\
&= \frac{T^{q-1} (1 + (1 - \zeta^{q-1})w_1)}{(w_1 w_1^\nabla)^q} \\
&= T^{-1} (\zeta^{q-1} - 1) (1 + (1 - \zeta^{q-1})w_1) (T^q w_1^{-q} + \zeta^{-q}).
\end{aligned}$$

This is exactly the equality (28). \square

4.3. Restrictions on primitive I_∞^n -torsion. To show the case $n \geq 2$ of Theorem B, it is essential to choose coordinates w_1, \dots, w_n to parametrize the primitive I_∞^n -torsions of Φ^{j_0} . Suppose that the elements $\beta_1, \beta_2, \dots, \beta_n$ span a primitive I_∞^n -torsion of Φ^{j_0} . Without loss of generality, we assume that $\beta_k \in \Phi^{j_0}[I_\infty^k] \setminus \Phi^{j_0}[I_\infty^{k-1}]$ for $1 \leq k \leq n$. We define recursively the twisted polynomial Ω_k , with $0 \leq k \leq n$ as follows. We set $\Omega_0 = 1$ and

$$\Omega_k = \delta_k(\tau - w_k) \Omega_{k-1} \quad (31)$$

where

$$w_k := \Omega_{k-1}(\beta_k)^{q-1}, \quad (32)$$

and δ_k is a $(q-1)$ -th root of

$$(1 + (1 - \zeta^{q^{k-1}-q^k})w_k^q)^{-1}.$$

It is straightforward to show that

$$\Omega_k = \delta_k(\tau - w_k) \cdots \delta_2(\tau - w_2) \delta_1(\tau - w_1) \quad (33)$$

$$= \delta_1 \delta_2 \cdots \delta_k ((\delta_1 \delta_2 \cdots \delta_{k-1})^{q-1} \tau - w_k) \cdots ((\delta_2 \delta_1)^{q-1} \tau - w_3) (\delta_1^{q-1} \tau - w_2) (\tau - w_1). \quad (34)$$

Adopting a similar proof as in Lemma 3.4, we have the following lemma.

Lemma 4.2. *Maintain the notations above. Then*

- (1) *The elements $\beta_1, \beta_2, \dots, \beta_k$ are annihilated by Ω_k .*
- (2) *The element $\Omega_{k-1}(\beta_k)$ is annihilated by $\Phi_{I_\infty}^{\sigma^{k-1}; j_{k-1}}$, and thus*

$$\Phi_{I_\infty}^{\sigma^{k-1}; j_{k-1}} = \left(\tau - \frac{1}{w_k j_{k-1}} \right) (\tau - w_k). \quad (35)$$

- (3) *The twisted polynomial $\delta_k(\tau - w_k)$ is an isogeny from $\Phi^{\sigma^k; j_k}$ to $\Phi^{\sigma^{k+1}; j_{k+1}}$, where j_k are recursively defined as*

$$j_k = j_k(w_k) = T^{-\sigma^{k-1}} (\zeta^{q^k - q^{k-1}} - 1) \left(1 + (1 - \zeta^{q^k - q^{k-1}}) w_k \right) (T^{q\sigma^{k-1}} w_k^{-q} + \zeta^{-q^k}). \quad (36)$$

- (4) *The twisted polynomial Ω_k is indeed an isogeny from Φ^{j_0} to $\Phi^{\sigma^k; j_k}$.*

For $1 \leq k \leq n-1$, the restriction on β_{k+1} is that for $z \in I_\infty$,

$$\Phi_z^{j_0}(\beta_{k+1}) \in \langle \beta_1, \dots, \beta_k \rangle \quad (37)$$

and there exists some z_0 such that

$$\Phi_{z_0}^{j_0}(\beta_{k+1}) \notin \langle \beta_1, \dots, \beta_{k-1} \rangle. \quad (38)$$

From Lemma 4.2, the condition (37) is equivalent to

$$0 = \Omega_k \Phi_z^{j_0}(\beta_{k+1}) = \Phi_z^{\sigma^k; j_k}(\Omega_k(\beta_{k+1})) \quad (39)$$

for all $z \in I_\infty$. Applying σ^k to (23), we know the annihilator of the ideal I_∞ is given by

$$\Phi_{I_\infty}^{\sigma^k; j_k} = \tau^2 + \left(\frac{1}{1 - \zeta^{q^k - q^{k+1}}} + \frac{1}{\zeta^{q^k} T^{\sigma^k}} \frac{1}{j_k} \right) \tau + \frac{1}{j_k}.$$

Define the polynomial $\Xi^{\sigma^k; j_k}(w_{k+1})$ in the variable w_{k+1} as

$$\Xi^{\sigma^k; j_k}(w_{k+1}) := w_{k+1}^{q+1} + \left(\frac{1}{1 - \zeta^{q^k - q^{k+1}}} + \frac{1}{\zeta^{q^k} T^{\sigma^k}} \frac{1}{j_k} \right) w_{k+1} + \frac{1}{j_k}$$

where j_k is subject to Equation (36). Recall that $w_{k+1} = \Omega_k(\beta_{k+1})^{q-1}$, we derive that (39) (resp. (37)) is equivalent to

$$\Xi^{\sigma^k; j_k}(w_{k+1}) = \frac{\Phi_{I_\infty}^{\sigma^k; j_k}(\Omega_k(\beta_{k+1}))}{\Omega_k(\beta_{k+1})} = 0.$$

On the other hand, Lemma 4.2 and the condition (38) yield that for $z \in I_\infty$,

$$\Omega_{k-1} \Phi_z^{j_0}(\beta_{k+1}) = \Phi_z^{\sigma^{k-1}; j_{k-1}}(\Omega_{k-1}(\beta_{k+1}))$$

does not always vanish. Thus, we derive the inequality

$$0 \neq \Phi_{I_\infty}^{\sigma^{k-1}; j_{k-1}}(\Omega_{k-1}(\beta_{k+1})). \quad (40)$$

Applying the decomposition (35) we get

$$\begin{aligned} \Phi_{I_\infty}^{\sigma^{k-1}; j_{k-1}}(\Omega_{k-1}(\beta_{k+1})) &= \left(\tau - \frac{1}{j_{k-1} w_k} \right) (\tau - w_k) (\Omega_{k-1}(\beta_{k+1})) \\ &= \delta_k^{-q} \left(\tau - \frac{\delta_k^{q-1}}{j_{k-1} w_k} \right) \delta_k(\tau - w_k) (\Omega_{k-1}(\beta_{k+1})) \end{aligned}$$

$$\begin{aligned}
&= \delta_k^{-q} \left(\tau - \frac{\delta_k^{q-1}}{j_{k-1} w_k} \right) (\Omega_k(\beta_{k+1})) \\
&= (\Omega_k(\beta_{k+1})) \delta_k^{-q} \left(w_{k+1} - \frac{\delta_k^{q-1}}{j_{k-1} w_k} \right).
\end{aligned}$$

The inequality (40) yields that $w_{k+1} \neq w_k^\nabla$, where

$$w_k^\nabla = \frac{\delta_k^{q-1}}{j_{k-1} w_k}.$$

From the equality

$$\Xi^{\sigma^{k-1}; j_{k-1}}(w_k) = w_k^{q+1} + \left(\frac{1}{1 - \zeta^{q^{k-1}-q^k}} + \frac{1}{\zeta^{q^{k-1}} T^{\sigma^{k-1}}} \frac{1}{j_{k-1}} \right) w_k + \frac{1}{j_{k-1}} = 0,$$

we get

$$j_{k-1} = \frac{(\zeta^{q^{k-1}-q^k} - 1)(w_k \zeta^{-q^{k-1}} T^{-\sigma^{k-1}} + 1)}{(1 - \zeta^{q^{k-1}-q^k}) w_k^{q+1} + w_k}.$$

So

$$w_k^\nabla = \frac{\delta_k^{q-1}}{j_{k-1} w_k} = \frac{1}{(\zeta^{q^{k-1}-q^k} - 1)(w_k \zeta^{-q^{k-1}} T^{-\sigma^{k-1}} + 1)}.$$

Remember that $w_{k+1} = w_k^\nabla$ must be a special root of $\Xi^{\sigma^k; j_k}(w_{k+1}) = 0$. There must be a decomposition

$$\Xi^{\sigma^k; j_k}(w_{k+1}) = \Xi_{\nabla}^{\sigma^k; j_k}(w_{k+1})(w_{k+1} - w_k^\nabla)$$

for some polynomial $\Xi_{\nabla}^{\sigma^k; j_k}(w_{k+1})$. It is straightforward to show that

$$\Xi_{\nabla}^{\sigma^k; j_k}(w_{k+1}) = -\frac{w_k^q}{1 - (\zeta^{q^k-q^{k-1}} - 1)w_k} \left(\frac{w_k^\nabla}{T^{\sigma^{k-1}}} \right)^{q-1} + \sum_{i=0}^{q-1} (w_k^\nabla)^i w_{k+1}^{q-i}.$$

In conclusion, we understand that the restrictions (37) and (38) on β_{k+1} reduce to the equality

$$\Xi_{\nabla}^{\sigma^k; j_k}(w_{k+1}) = 0.$$

4.4. Proof of Theorem B. The case $n = 0$ of Theorem B is the restatement of 2.4. In Section 4.1, we have proved the case $n = 1$.

Proof of Theorem B. Assume that a primitive I_∞^n -torsion of Φ^{j_0} is spanned by β_1, \dots, β_n . Let w_1, \dots, w_n be the variables associated to β_1, \dots, β_n as in Equation (32). We conclude from Section 4.1 that w_1 satisfies the equation

$$\Xi^{j_0}(w_1) = 0.$$

For $k = 2, \dots, n-1$, Section 4.3 implies that w_k satisfies

$$\Xi_{\nabla}^{\sigma^{k-1}; j_{k-1}}(w_k) = 0.$$

Conversely, given w_1, \dots, w_n , the corresponding primitive I_∞^n -torsion of Φ^{j_0} is written as

$$\ker \Omega_k = \ker((\delta_1 \delta_2 \cdots \delta_{k-1})^{q-1} \tau - w_k) \cdots ((\delta_2 \delta_1)^{q-1} \tau - w_3) (\delta_1^{q-1} \tau - w_2) (\tau - w_1),$$

where

$$\delta_k^{q-1} = \frac{1}{1 + (1 - \zeta^{q^{k-1}-q^k}) w_k^q}.$$

This establishes the one-to-one correspondence between the parameters w_i and the set of primitive I_∞^n -torsions of Φ^{j_0} . \square

5. REDUCTION OF MODULAR CURVES

5.1. Genus formula. In this section, we briefly recall the genus formula established by Bassa-Beelen-Nguyen [5] based on the results of [17]. For this aim we temporarily reset \mathcal{A} to be a Dedekind domain arising from a general smooth curve over \mathbb{F}_q associated with a unique infinity. Let δ be the degree of the infinity.

Notation 5.1. Let $\mathfrak{n} \subseteq \mathcal{A}$ be an ideal and suppose that $\mathfrak{n} = \mathfrak{p}^{r_1} \cdots \mathfrak{p}^{r_s}$ for prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ and positive integers r_1, \dots, r_s . Writing $q_i := |\mathfrak{p}_i|$, we define

$$\epsilon(\mathfrak{n}) = \prod_{i=1}^s q_i^{r_i-1} (q_i + 1)$$

and

$$\kappa(\mathfrak{n}) = \prod_{i=1}^s \left(q_i^{\lfloor r_i/2 \rfloor} + q_i^{r_i - \lfloor r_i/2 \rfloor - 1} \right),$$

where $\lfloor r \rfloor$ denotes the integral part of a real number r .

Theorem 5.2 (Theorem 3.1 of [5]). *Let $\mathcal{A}, \mathfrak{n}$ be as in Notation 5.1. Let $\mathbf{x}_0(\mathfrak{n})$ be the minimal modular curve associated with \mathcal{A} . Denote by $P_K(t)$ the L -polynomial of the quotient field K of \mathcal{A} . Then the genus of $\mathbf{x}_0(\mathfrak{n})$ is given by*

$$g(\mathbf{x}_0(\mathfrak{n})) = 1 + \frac{(q^\delta - 1)\epsilon(\mathfrak{n})P_K(q)}{(q^2 - 1)(q - 1)} - \frac{P_K(1)\delta}{q - 1} \cdot (\kappa(\mathfrak{n}) + 2^{s-1}(q - 2)) + \Delta,$$

where $\Delta = -P_K(-1)2^{s-1}q/(q + 1)$ if δ is odd and all prime divisors of \mathfrak{n} are of even degree; and $\Delta = 0$ otherwise.

We now return to our main setting on \mathcal{A} and choose $\mathfrak{n} = I_\infty^k$. Then the degree of infinity equals $\delta = \deg P_\rho = 2$. It is obvious that $P_K = 1$ since K is rational. From Notation 5.1, we have $s = 1$, $|I_\infty| = q$,

$$\epsilon(\mathfrak{n}) = q^{k-1}(q + 1)$$

and

$$\kappa(\mathfrak{n}) = q^{\lfloor k/2 \rfloor} + q^{k - \lfloor k/2 \rfloor - 1}.$$

Substituting these quantities into Theorem 5.2, we have

$$\begin{aligned} g(\mathbf{x}_0(\mathfrak{n})) &= 1 + \frac{\epsilon(\mathfrak{n})}{q - 1} - \frac{2}{q - 1} \cdot (\kappa(\mathfrak{n}) + q - 2) \\ &= -1 + \frac{q^{k-1}(q + 1)}{q - 1} - \frac{2}{q - 1} \cdot (q^{\lfloor k/2 \rfloor} + q^{k - \lfloor k/2 \rfloor - 1} - 1). \end{aligned} \quad (41)$$

In particular, for $k = 1$, we have $g(\mathbf{x}_0(\mathfrak{n})) = 0$. This coincides with the fact that $\mathbf{x}_0(I_\infty)$ is rational.

5.2. Supersingular points. For $\eta \in \mathbb{F}_{q^2} \setminus (\{\zeta, \zeta^q\} \cup \mathbb{F}_q)$, we define

$$\begin{aligned} z_\eta &= \frac{(t - \eta)(t - \eta^q)}{(t - \zeta)(t - \zeta^q)} \\ &= \frac{-(\eta + \eta^q - \zeta - \zeta^q)t + \eta^{q+1} - \zeta^{q+1}}{(t - \zeta)(t - \zeta^q)} + 1 \\ &= (\eta^{q+1} - \zeta^{q+1})x - (\eta + \eta^q - \zeta - \zeta^q)y + 1. \end{aligned}$$

It is clear that z_η is an element of \mathcal{A} of degree two. Denote by I_η the ideal of \mathcal{A} generated by z_η . The Drinfeld \mathcal{A} -module Φ^j has a good reduction at I_η . Let us denote the I_η -reduction of Φ^j by $\bar{\Phi}^j$. More precisely, the \mathbb{F}_q -homomorphism

$$\mathcal{A} \rightarrow \mathbb{F}_{q^2} : x \mapsto \frac{1}{(\eta - \zeta)(\eta - \zeta^q)}, y \mapsto \frac{\eta}{(\eta - \zeta)(\eta - \zeta^q)}$$

defines an \mathcal{A} -field with characteristic I_η . Substituting $t = \eta$ into both Φ_x^j and Φ_y^j , we obtain the Drinfeld \mathcal{A} -module $\bar{\Phi}^j$ over \mathbb{F}_{q^2} with expressions

$$\begin{aligned} \bar{\Phi}_x^j &= \left(\frac{-j^{q(q+1)}}{(\eta^q - \zeta^q)(\eta - \zeta^q)} \tau^2 + \left(\frac{j^q}{\zeta(\eta^q - \zeta^q)} + \frac{j^{q+1}}{(1 - \zeta^{1-q})(\eta^q - \zeta)(\eta - \zeta)} \right) \tau + \frac{j}{(\eta - \zeta)(\eta - \zeta^q)} \right) \\ &\quad \cdot \left(\tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{\eta - \zeta^q}{\zeta} \frac{1}{j} \right) \tau + \frac{1}{j} \right), \end{aligned}$$

and

$$\begin{aligned} \bar{\Phi}_y^j &= \left(\frac{-j^{q(q+1)} \zeta^q}{(\eta^q - \zeta^q)(\eta - \zeta^q)} \tau^2 + \left(\frac{j^q \zeta^q}{\zeta(\eta^q - \zeta^q)} - \frac{\zeta^q j^{q+1}}{(1 - \zeta^{q-1})(\eta^q - \zeta)(\eta - \zeta)} \right) \tau + \frac{j\eta}{(\eta - \zeta)(\eta - \zeta^q)} \right) \\ &\quad \cdot \left(\tau^2 + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{\eta - \zeta^q}{\zeta} \frac{1}{j} \right) \tau + \frac{1}{j} \right). \end{aligned}$$

We determine the supersingular condition for $\bar{\Phi}^j$ in the following lemma.

Lemma 5.3. *The ζ^q -type Drinfeld \mathcal{A} -module $\bar{\Phi}^j$ over \mathbb{F}_{q^2} is supersingular, if and only if j is contained in \mathbb{F}_{q^2} and satisfies*

$$\left(j + \frac{\eta - \zeta}{\zeta - \zeta^{1-q}} \right)^{q+1} + \frac{\eta - \eta^q}{\zeta - \zeta^q} = 0. \quad (42)$$

Proof. It is straightforward to check that

$$\begin{aligned} \bar{\Phi}_{z_\eta}^j &= (\eta^{q+1} - \zeta^{q+1}) \bar{\Phi}_x^j - (\eta + \eta^q - \zeta - \zeta^q) \bar{\Phi}_y^j + 1 \\ &= -j^{q(q+1)} \tau^4 + \frac{j^q}{1 - \zeta^{1-q}} (-j^{q^2} + j) \tau^3 \\ &\quad + \left(\left(\frac{j}{1 - \zeta^{1-q}} + \eta \zeta^{-1} - 1 \right)^{q+1} + (\zeta^{-1} - \zeta^{-q})(\eta - \eta^q) \right) \tau^2. \end{aligned}$$

This implies that $\bar{\Phi}^j$ is supersingular if and only if

$$\left(\frac{j}{1 - \zeta^{1-q}} + \eta \zeta^{-1} - 1 \right)^{q+1} + (\zeta^{-1} - \zeta^{-q})(\eta - \eta^q) = 0.$$

The last equality can be simplified to (42). Moreover, all such j are contained in \mathbb{F}_{q^2} . \square

In a similar manner, we define $\mathbf{x}_0(I_\infty^k)/I_\eta$ to be the I_η -reduction of the modular curve $\mathbf{x}_0(I_\infty^k)$ for each $k \geq 0$. The following result is a consequence of Theorem B.

Corollary 5.4. *The function field $\bar{\mathcal{G}}_k$ of $\mathbf{x}_0(I_\infty^k)/I_\eta$ is given by $\mathbb{F}_{q^2}(j_0, w_1, \dots, w_k)$, where j_0, w_1, \dots, w_k are subject to*

$$w_1^{q+1} + \left(\frac{1}{1 - \zeta^{1-q}} + \frac{\eta - \zeta^q}{\zeta} \frac{1}{j_0} \right) w_1 + \frac{1}{j_0} = 0, \quad (43)$$

and

$$\sum_{i=0}^{q-1} (w_{k-1}^\nabla)^i w_k^{q-i} = \frac{w_{k-1}^q}{1 - (\zeta^{q^{k+1}-q^k} - 1)w_{k-1}} \left(w_{k-1}^\nabla (\eta - \zeta^{q^{k+1}}) \right)^{q-1}. \quad (44)$$

Notice that here w_{k-1}^∇ is given by

$$w_{k-1}^\nabla = \frac{1}{(\zeta^{q^k - q^{k+1}} - 1)(1 + \zeta^{-q^k}(\eta - \zeta^{q^{k+1}})w_{k-1})}.$$

In particular, the function field $\bar{\mathcal{G}}_0$ of $\mathbf{x}_0(1)/I_\eta$ is $\mathbb{F}_{q^2}[j]$. We already know that the supersingular points of $\mathbf{x}_0(1)/I_\eta$ are precisely \mathbb{F}_{q^2} -rational and satisfy the equality (42) by Lemma 5.3. From Lemma 4.1, we know $\delta_1(\tau - w_1)$ is an isogeny from $\bar{\Phi}^{j_0}$ to another ζ -type Drinfeld module $\bar{\Phi}^{\sigma; j_1}$, where j_1 is the j -invariant satisfies

$$j_1 = j_0^q \frac{\eta - \zeta}{\eta^q - \zeta} \cdot (1 + (1 - \zeta^{q-1})w_1)^{q^2+1}. \quad (45)$$

It is clear that $\bar{\Phi}^{\sigma; j_1}$ is also supersingular. Applying the same argument as in Lemma 5.3 to $\bar{\Phi}^{\sigma; j_1}$ yields that j_1 is also contained in \mathbb{F}_{q^2} . It follows from (45) that

$$(1 + (1 - \zeta^{q-1})w_1)^{q^4-1} = \left(\frac{j_1}{j_0^q} \frac{\eta^q - \zeta}{\eta - \zeta} \right)^{q^2-1} = 1.$$

This implies that $(1 + (1 - \zeta^{q-1})w_1)$ lies in \mathbb{F}_{q^4} , and so does w_1 . Therefore, we understand that when j_0 verifies (42), all the solutions w_1 of (43) for are contained in \mathbb{F}_{q^4} and are distinct. Proceeding with the same procedure, we find that for given coordinates $j_0, w_1, \dots, w_{k-1} \in \mathbb{F}_{q^4}$, the solutions w_k of (44) form a subset of \mathbb{F}_{q^4} with cardinality q . Hence following lemma follows.

Lemma 5.5. *The supersingular points of the modular curves $\mathbf{x}_0(I_\infty^k)/I_\eta$ are \mathbb{F}_{q^4} -rational and their cardinality is $(q+1)^2 q^{k-1}$.*

5.3. Proof of Theorem C. The proof of Theorem C relies on Lemma 5.5 and the equality given in (41). We elaborate on the details below.

Proof. Let $\mathbb{F}_{q^4}\bar{\mathcal{G}}_k$ denote the function field of $\mathbf{x}_0(I_\infty^k)/I_\eta$ over the finite field \mathbb{F}_{q^4} . We know the genus of a curve is invariant under taking reduction and constant field extension. So the genus $g(\mathbb{F}_{q^4}\bar{\mathcal{G}}_k)$ of $\mathbb{F}_{q^4}\bar{\mathcal{G}}_k$ is given by (41). From Lemma 5.5, the cardinality $N(\mathbb{F}_{q^4}\bar{\mathcal{G}}_k)$ of the \mathbb{F}_{q^4} -rational points on $\mathbf{x}_0(I_\infty^k)/I_\eta$ is greater than $(q+1)^2 q^{k-1}$.

We obtain that

$$\lambda(\mathbb{F}_{q^4}\bar{\mathcal{G}}_k) = \lim_{k \rightarrow \infty} \frac{N(\mathbb{F}_{q^4}\bar{\mathcal{G}}_k)}{g(\mathbb{F}_{q^4}\bar{\mathcal{G}}_k)} \geq q^2 - 1. \quad (46)$$

Since the upper bound of Ihara's quantity over \mathbb{F}_{q^4} is $(q^2 - 1)$, we know that the equality of (46) holds. In other words, the function field tower $\{\mathbb{F}_{q^4}\bar{\mathcal{G}}_k\}$ is optimal. \square

REFERENCES

- [1] Ilia Aleshnikov, Vinay Deolalikar, P. Vijay Kumar, and Henning Stichtenoth, *Towards a basis for the space of regular functions in a tower of function fields meeting the Drinfeld-Vladut bound*, Finite fields and applications (Augsburg, 1999), 2001, pp. 14–24. MR1849075
- [2] Nurdagül Anbar, Alp Bassa, and Peter Beelen, *A modular interpretation of various cubic towers*, J. Number Theory **171** (2017), 341–357. MR3556689
- [3] Alp Bassa, Peter Beelen, Arnaldo Garcia, and Henning Stichtenoth, *Towers of function fields over non-prime finite fields*, Mosc. Math. J. **15** (2015), no. 1, 1–29, 181. MR3427409
- [4] Alp Bassa, Peter Beelen, and Nhut Nguyen, *Good towers of function fields*, Algebraic curves and finite fields, 2014, pp. 23–40. MR3287681
- [5] ———, *Good families of Drinfeld modular curves*, LMS J. Comput. Math. **18** (2015), no. 1, 699–712. MR3433893
- [6] Peter Beelen and Maria Montanucci, *A new family of maximal curves*, J. Lond. Math. Soc. (2) **98** (2018), no. 3, 573–592. MR3893192
- [7] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing, *Torsion limits and Riemann-Roch systems for function fields and applications*, IEEE Trans. Inform. Theory **60** (2014), no. 7, 3871–3888. MR3225937

- [8] Emrah Çakçak and Ferruh Özbudak, *Subfields of the function field of the Deligne-Lusztig curve of Ree type*, Acta Arith. **115** (2004), no. 2, 133–180. MR2099835
- [9] ———, *Number of rational places of subfields of the function field of the Deligne-Lusztig curve of Ree type*, Acta Arith. **120** (2005), no. 1, 79–106. MR2189720
- [10] Rui Chen, Zhuo Chen, and Chuangqiang Hu, *A modular interpretation of BBGS towers*, J. Number Theory **221** (2021), 143–173. MR4203564
- [11] Vladimir Gershonovich Drinfeld and Sergei G. Vlăduț, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 1, 68–69. MR695100 (85b:14028)
- [12] Noam D. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics, Vol. II (Barcelona, 2000), 2001, pp. 189–198. MR1905359
- [13] Arnaldo Garcia, Cem Güneri, and Henning Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. **10** (2010), no. 3, 427–434. MR2660419
- [14] Arnaldo Garcia and Henning Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduț bound*, Invent. Math. **121** (1995), 211–222.
- [15] Arnaldo García and Henning Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C.R. Acad. Sci. Paris Sér. **322** (1996), 1067–1070.
- [16] Ernst-Ulrich Gekeler, *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern*, Bonner Mathematische Schriften [Bonn Mathematical Publications], vol. 119, Universität Bonn, Mathematisches Institut, Bonn, 1980. Dissertation, Rheinische Friedrich-Wilhelms-Universität, Bonn, 1979. MR594434
- [17] ———, *Drinfeld modular curves*, Lecture Notes in Mathematics, 1231. Springer-Verlag, Berlin, 1986.
- [18] ———, *Asymptotically optimal towers of curves over finite fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 325–336. MR2037099
- [19] Massimo Giulietti and Gábor Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), no. 1, 229–245. MR2448446
- [20] Massimo Giulietti, Gábor Korchmáros, and Fernando Torres, *Quotient curves of the Suzuki curve*, Acta Arith. **122** (2006), no. 3, 245–274. MR2239917
- [21] V. D. Goppa, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR **259** (1981), no. 6, 1289–1290. MR628795
- [22] David R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, 1979, pp. 173–217. MR535766
- [23] Chuangqiang Hu, *Explicit construction of AG codes from a curve in the tower of Bassa-Beelen-Garcia-Stichtenoth*, IEEE Trans. Inform. Theory **63** (2017), no. 11, 7237–7246. MR3724425
- [24] Chuangqiang Hu and Xiao-Min Huang, *Drinfeld module and Weil pairing over Dedekind domain of class number two*, Finite Fields Appl. **100** (2024), Paper No. 102516, 52. MR4808031
- [25] Chuangqiang Hu and Chang-An Zhao, *Multi-point codes from generalized Hermitian curves*, IEEE Trans. Inform. Theory **62** (2016), no. 5, 2726–2736. MR3493874
- [26] Yasutaka Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, In Journal of the Faculty of Science, the University of Tokyo, Sect. 1 A, Mathematics **28** (1981), 721–724, 1982. MR0656048
- [27] Mihran Papikian, *Drinfeld modules*, Graduate Texts in Mathematics, vol. 296, Springer, Cham, [2023] ©2023. MR4592575
- [28] Jean-Pierre Serre, *Résumé des cours de 1983-1984*, in Annuaire College de France **128** (1984), 79–83.
- [29] ———, *Sur le nombre des points rationnels d’une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris **296** (1984), 397–402.
- [30] Dane C. Skabelund, *New maximal curves as ray class fields over deligne-lusztig curves*, Proc. Amer. Math. Soc. **146** (2018), no. 2, 525–540. MR3731688
- [31] Henning Stichtenoth, *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941
- [32] M. A. Tsfasman, S. G. Vlăduț, and Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28. MR705893
- [33] Conny Voss and Tom Høholdt, *An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduț-Zink bound: the first steps*, IEEE Trans. Inform. Theory **43** (1997), no. 1, 128–135. MR1426240
- [34] André Weil, *Variétés abéliennes et courbes algébriques*, Publications de l’Institut de Mathématiques de l’Université de Strasbourg [Publications of the Mathematical Institute of the University of Strasbourg], vol. 8 (1946), Hermann & Cie, Paris, 1948. Actualités Scientifiques et Industrielles, No. 1064. [Current Scientific and Industrial Topics]. MR29522
- [35] Shudi Yang and Chuangqiang Hu, *Weierstrass semigroups on the third function field in a tower attaining the Drinfeld-Vlăduț bound*, Adv. Math. Commun. **18** (2024), no. 4, 1051–1083. MR4762483

SUN YAT-SEN UNIVERSITY, SCHOOL OF MATHEMATICAL, GUANGZHOU, CHINA

Email address: huchq@mail2.sysu.edu.cn

BEIJING INSTITUTE OF MATHEMATICAL SCIENCES AND APPLICATIONS, BEIJING, CHINA

Email address: xwzhu@bimsa.cn