A modular interpretation of various cubic towers

Anbar Meidl, Nurdagül; Bassa, Alp; Beelen, Peter

Published in:
Journal of Number Theory

Link to article, DOI:
10.1016/j.jnt.2016.07.025

Publication date:
2017

Document Version
Peer reviewed version

A modular interpretation of various cubic towers

Nurdagül Anbar*, Alp Bassa† and Peter Beelen‡

Abstract

In this article we give a Drinfeld modular interpretation for various towers of function fields meeting Zink's bound.

1 Introduction

Let p be a prime number and n a positive integer. In the past years, several developments have taken place concerning Ihara's constant $A(p^n)$. This fundamental constant gives a measure on how many rational places families of function fields of increasing genus with full constant field $\mathbb{F}_{p^n}$ can have. More precisely, given a function field F with full constant field $\mathbb{F}_{p^n}$, we denote by $g(F)$, (resp. $N(F)$) the genus (resp. the number of rational places) of F. Then for a given finite field $\mathbb{F}_{p^n}$, Ihara's constant is defined as follows:

$$A(p^n) := \limsup_{g(F)\to\infty} \frac{N(F)}{g(F)},$$

where the limit is over all function fields with full constant field $\mathbb{F}_{p^n}$. It is known that $0 < A(p^n) \leq \sqrt{p^n} - 1$, the first inequality being due to Serre [13], while the second inequality is known as the Drinfeld–Vladut bound [14]. Combining the work of Ihara [11] and the Drinfeld–Vladut bound, one sees that $A(p^n) = \sqrt{p^n} - 1$ if n is even. For odd values of n the true value of $A(p^n)$ is currently unknown.

To obtain lower bound for $A(q)$, with $q = p^n$, one can use a *tower (of function fields) over* $\mathbb{F}_q$,

$$\mathcal{F} = (F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_i \subseteq \ldots).$$

It is required that all function fields F_i have full constant field $\mathbb{F}_q$, and $g(F_n) \to \infty$ as $n \to \infty$. Also all extensions F_{i+1}/F_i are assumed to be separable. These assumptions imply that the following limit exists:

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

which is called the limit of the tower $\lambda(\mathcal{F})$. One then obtains the lower bound for Ihara's constant: $A(q) \geq \lambda(\mathcal{F})$. Using this method it was shown in [2] that

$$A(p^n) \geq 2\left(\frac{1}{p^{\lceil \frac{n}{2} \rceil} - 1} + \frac{1}{p^{\lfloor \frac{n}{2} \rfloor} - 1}\right)^{-1}, \tag{1}$$

*Nurdagül Anbar is supported by H.C. Ørsted COFUND Post-doc for the project "Algebraic curves with many rational points" and by The Danish Council for Independent Research (Grant No. DFF–4002-00367)

†Alp Bassa is supported by Tübitak Proj. No. 112T233.

‡Peter Beelen is supported by The Danish Council for Independent Research (Grant No. DFF–4002-00367).

where $\lceil\ \rceil$, resp. $\lfloor\ \rfloor$, denotes the ceiling, resp. floor, of a real number.

As mentioned above, the case where n is even has been settled by work of Ihara. For cubic finite fields, i.e., if n is divisible by 3, the following results are known: In [15] it was announced that

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}.$$

Note Equation (1) specializes to the same if $n = 3$. For $p = 2$, this was obtained in [8], while this result was generalized in [5] to

$$A(q^3) \geq \frac{2(q^2-1)}{q+2},$$

with $q = p^m$ for any positive integer m. The generalization was achieved by explicitly constructing a tower of function fields over $\mathbb{F}_{q^3}$ (which we will call a *cubic* tower) with limit $\lambda(\mathcal{F}) \geq 2(q^2-1)/(q+2)$. Since then several other papers have appeared in which other towers or alternative descriptions of previously known towers were formulated, giving rise to various cubic towers with the same limit [12, 6, 2]. While the towers in [2] were explained using the theory of Drinfeld modules, the towers in [5, 12, 6] have no such modular explanation. The goal of this article is to fill this gap in our knowledge.

2 Modular setup and first equations

We start by giving a brief introduction to Drinfeld modules, since these will be needed in the remainder of the paper. See [10] for a more thorough and general overview.

2.1 Drinfeld modules over $\mathbb{F}_q[T]$

Let L be a field and $\overline{L}$ a fixed algebraic closure. Moreover, assume that $\iota : \mathbb{F}_q[T] \to L$ is a $\mathbb{F}_q$-algebra homomorphism. The kernel of ι is called the *characteristic* of L. From now on, we will always assume that this characteristic is given by $\langle T-1\rangle \subset \mathbb{F}_q[T]$ and by slight abuse of language also call the polynomial $T-1$ the characteristic of L. Note that this assumption implies that for any $P(T) \in \mathbb{F}_q[T]$ we have $\iota(P(T)) = P(1)$, the evaluation of the polynomial $P(T)$ in 1. Now let $L\{\tau\}$ be the *non-commutative polynomial ring* generated by the Frobenius endomorphism τ satisfying $\tau r = r^q\tau$ for all $r \in L$. Then an $\mathbb{F}_q[T]$-*Drinfeld module* over L of *rank* 3 is a homomorphism

$$\begin{aligned} \varphi : \mathbb{F}_q[T] &\to L\{\tau\} \\ P(T) &\mapsto \varphi_{P(T)} \end{aligned}$$

such that for all $P(T) \in \mathbb{F}_q[T]\backslash\{0\}$, we have $\deg_\tau \varphi_{P(T)} = 3\deg P(T)$, and the constant term of $\varphi_{P(T)}$ is equal to $\iota(P(T))$, i.e., equal to $P(1)$. This gives $\bar{L}$ the structure of an $\mathbb{F}_q[T]$-module. Since φ is a homomorphism, it is already fully determined by φ_T. Therefore by slight above of language, we will talk about the Drinfeld module φ_T. Using that the rank of φ is three, we see that

$$\varphi_T = \Delta\tau^3 + g\tau^2 + h\tau + 1,$$

for certain $\Delta, g, h \in L$ and $\Delta \neq 0$.

Two Drinfeld modules φ and ψ with the same characteristic are called *isogenous* if there exists $\lambda \in L\{\tau\}$ different from zero such that

$$\lambda \circ \varphi_{P(T)} = \psi_{P(T)} \circ \lambda \tag{2}$$

for all $P(T) \in \mathbb{F}_q[T]$. The element λ is called an *isogeny* from φ to ψ. Since we are considering $\mathbb{F}_q[T]$-Drinfeld modules, it is sufficient to require that $\lambda \circ \varphi_T = \psi_T \circ \lambda$ for λ to be an isogeny. It is easy to see that $\varphi_{P(T)}$ is an isogeny from φ to itself for any $P(T) \in \mathbb{F}_q[T]$. This isogeny is called the *multiplication by $P(T)$ map*. The Drinfeld modules φ and ψ are called *isomorphic (over $\overline{L}$)* if λ can be chosen from $\overline{L}\backslash\{0\}$.

An isogeny $\lambda \in L\{\tau\}$ corresponds to a linearized polynomial by identifying τ^i and X^{q^i}. This makes it possible to evaluate λ in elements of $\overline{L}$. In particular we define the kernel of an isogeny λ as follows:

$$\ker \lambda := \{x \in \bar{L} | \lambda(x) = 0\}.$$

From Equation (2) it follows that $\ker \lambda = \{x \in \bar{L} | \lambda(x) = 0\}$ is an $\mathbb{F}_q[T]$-submodule of $\bar{L}$ under the $\mathbb{F}_q[T]$-action given by φ. For $P(T) \in \mathbb{F}_q[T]$, we write $\varphi[P(T)] := \ker \varphi_{P(T)}$. This set is called the set of $P(T)$-*torsion points* of the Drinfeld module φ. If $P(T)$ is coprime with the characteristic $T-1$, then $\varphi[P(T)] \cong (\mathbb{F}_q[T]/\langle P(T)\rangle)^3$ as an $\mathbb{F}_q[T]$-module, i.e., it is a free $\mathbb{F}_q[T]/\langle P(T)\rangle$-module of rank 3.

An isogeny λ is called a $P(T)$-*isogeny* if $\ker \lambda$ is a free $\mathbb{F}_q[T]/\langle P(T)\rangle$-submodule of $\varphi[P(T)]$. The *rank of* λ is defined to be the rank of its kernel as a $\mathbb{F}_q[T]/\langle P(T)\rangle$-module. Unlike in the classical case of elliptic curves, nontrivial isogenies can have rank 1 or 2. For a separable $P(T)$-isogeny λ one can find $\mu \in L\{\tau\}$ such that $\varphi_{P(T)} = \mu \circ \lambda$.

In case $P(T) = T - 1$, we have $\varphi_{T-1} = \Delta\tau^3 + g\tau^2 + h\tau$ and therefore $\varphi[T-1]$ is isomorphic to a free $\mathbb{F}_q[T]/\langle T-1\rangle$-module of rank at most 2. Classically, the Drinfeld module is called *supersingular* (in characteristic $T-1$), if the rank of $\varphi[T-1]$ is zero, i.e., if the multiplication by $T-1$ map φ_{T-1} is purely inseparable. This is the case if and only if $g = h = 0$. We will call a Drinfeld module φ *weakly supersingular* (in characteristic $T-1$), if $T-1$-torsion points $\varphi[T-1]$ form a free module of rank at most one. In this case the multiplication by $T-1$ map has inseparability degree $\geq q^2$ and $h = 0$. Comparing the inseparability degrees of ϕ_{T-1} and ψ_{T-1} by Equation (2), we see that the property of being (weakly) supersingular is preserved under isogenies and in particular under isomorphisms. From now on we will restrict ourselves to weakly supersingular Drinfeld modules and their isogenies.

For weakly supersingular $\mathbb{F}_q[T]$-Drinfeld modules of rank 3 given by $\varphi_T = \Delta\tau^3 + g\tau^2 + 1$, we define the following J-invariant:

$$J(\varphi) := \frac{g^{q^2+q+1}}{\Delta^{q+1}}.$$

Two Drinfeld modules $\varphi_T = \Delta_1\tau^3 + g_1\tau^2 + 1$ and $\psi_T = \Delta_2\tau^3 + g_2\tau^2 + 1$, are isomorphic if and only if $J(\varphi) = J(\psi)$. Indeed, if $c\varphi = \psi c$ for some nonzero constant $c \in \overline{L}$, then $c^{q^3-1}\Delta_2 = \Delta_1$ and $c^{q^2-1}g_2 = g_1$, implying that $J(\varphi) = J(\psi)$. Conversely, if $J(\varphi) = J(\psi)$, then $(\Delta_1/\Delta_2)^{q+1} = (g_1/g_2)^{q^2+q+1}$. We can find $c \in \overline{L}$ such that $c^{q^3-1} = \Delta_1/\Delta_2$ and from the previous we see that $c^{(q^2-1)(q^2+q+1)} = (g_1/g_2)^{q^2+q+1}$. Therefore we can choose α satisfying $\alpha^{q^2+q+1} = 1$ such that $c' := \alpha c$ satisfies both $(c')^{q^3-1} = \Delta_1/\Delta_2$ and $(c')^{q^2-1} = g_1/g_2$. The desired isomorphism between φ and ψ is then given by c'. Note that the supersingular Drinfeld modules of rank three form one isomorphism class determined by $J(\varphi) = 0$. In fact any supersingular Drinfeld module φ and all isogenies from φ to ψ can be defined over $\mathbb{F}_{q^3}$ (see [9]).

2.2 Normalized Drinfeld modules

Since the expression for the J-invariant is somewhat cumbersome, rather than working with isomorphism classes directly, we will use normalized Drinfeld modules. An $\mathbb{F}_q[T]$-Drinfeld module of rank three is said to be normalized if $\Delta = -1$. This is a direct generalization of a similar notion used in [7] for rank two Drinfeld modules. Any isomorphism class of Drinfeld modules

contains a normalized one, but two distinct normalized Drinfeld modules can be isomorphic. The J-invariant of the normalized weakly supersingular Drinfeld module $\varphi_T = -\tau^3 + g_1\tau^2 + 1$ is given by:

$$J(\varphi) = g_1^{q^2+q+1}. \tag{3}$$

Since we will be working with normalized Drinfeld modules or isomorphism classes thereof, we will take all isogenies to be monic.

Now let $\lambda : \varphi \to \psi$ be a separable monic T-isogeny of rank 1. Then $\lambda = \tau - u_1$ with

$$\lambda \circ \varphi_T = \psi_T \circ \lambda$$

and there exists $\mu \in L\{\tau\}$ such that

$$\varphi_T = \mu \circ \lambda.$$

These imply that $\psi_T = \lambda \circ \mu$. From

$$\mu \circ \lambda = \varphi_T = -\tau^3 + g_1\tau^2 + 1$$

it follows that

$$\mu = -\tau^2 - \frac{1}{u_1^{q+1}}\tau - \frac{1}{u_1}, \text{ with } g_1 = \frac{u_1^{q^2+q+1} - 1}{u_1^{q+1}} \tag{4}$$

and

$$\psi_T = -\tau^3 + g_2\tau^2 + 1, \text{ with } g_2 = \frac{u_1^{q^2+q+1} - 1}{u_1^{q^2+q}}. \tag{5}$$

The following lemma follows which will be useful later:

Lemma 2.1 *With the relations as above, we have*

$$\mathbb{F}_q(g_1, g_2) = \mathbb{F}_q(u_1) \text{ and } \mathbb{F}_q(g_1^{q^2+q+1}, g_2^{q^2+q+1}) = \mathbb{F}_q(u_1^{q^2+q+1}).$$

Proof. First observe that in the extension $\mathbb{F}_q(u_1)/\mathbb{F}_q(g_1/g_2)$ only tame ramification occurs, since $g_1/g_2 = u_1^{q^2-1}$. In particular, the same holds for the extension $\mathbb{F}_q(u_1)/\mathbb{F}_q(g_1, g_2)$. On the other hand there exists a place of $\mathbb{F}_q(u_1)$ lying above the pole of g_1 in $\mathbb{F}_q(g_1)$ which has ramification index q^2. Since all ramification in $\mathbb{F}_q(u_1)/\mathbb{F}_q(g_1, g_2)$ is tame, we conclude that the extension degree $[\mathbb{F}_q(g_1, g_2) : \mathbb{F}_q(g_1)]$ is at least q^2. However, $[\mathbb{F}_q(g_1, g_2) : \mathbb{F}_q(g_1)]$ also divides $[\mathbb{F}_q(u_1) : \mathbb{F}_q(g_1)] = q^2 + q + 1$, implying that $\mathbb{F}_q(g_1, g_2) = \mathbb{F}_q(u_1)$ as desired. The second part of the lemma can be shown similarly considering the (q^2+q+1)-st powers of all variables involved. ■

By Equation (3) the quantity $g_1^{q^2+q+1}$ (resp. $g_2^{q^2+q+1}$) is the J-invariant of the normalized supersingular Drinfeld module $\varphi_T = -\tau^3 + g_1\tau^2 + 1$ (resp. $\psi_T = -\tau^3 + g_2\tau^2 + 1$). The above lemma is useful, since it implies that if two such Drinfeld modules are isogenous by an isogeny $\lambda = \tau - u_1$, then $u_1^{q^2+q+1}$ can be used as a parameter to describe isomorphism classes of the data $\lambda : \varphi \to \psi$ with $\lambda = \tau - u_1$.

3 Composition of T-isogenies

Next we will study composites of T-isogenies between normalized Drinfeld modules of rank 3. The various possibilities of their structure will later on be the main ingredient in our explanation of the cubic towers in [5, 12, 6] from a modular point of view.

3.1 Composition of two T-isogenies

Let $\varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)}$ be Drinfeld modules with $\varphi_T^{(i)} = -\tau^3 + g_i\tau^2 + 1$, and $\lambda_1 : \varphi^{(1)} \to \varphi^{(2)}$ and $\lambda_2 : \varphi^{(2)} \to \varphi^{(3)}$ be T-isogenies of rank 1 with $\lambda_i = \tau - u_i$. Since λ_1 and λ_2 are separable T-isogenies, there exist μ_1 and μ_2 such that $\varphi_T^{(1)} = \mu_1 \circ \lambda_1$ and $\varphi_T^{(2)} = \lambda_1 \circ \mu_1 = \mu_2 \circ \lambda_2$. We wish to find an algebraic relation between u_1 and u_2. Combining Equation (4) applied to $\varphi^{(2)}$ and λ_2 with Equation (5) applied to $\varphi^{(1)}$ and λ_1, we see that

$$\frac{u_2^{q^2+q+1} - 1}{u_2^{q+1}} = g_2 = \frac{u_1^{q^2+q+1} - 1}{u_1^{q^2+q}}. \tag{6}$$

Clearing denominators we have

$$\begin{aligned} 0 = (u_2^{q^2+q+1} - 1)u_1^{q^2+q} - u_2^{q+1}(u_1^{q^2+q+1} - 1) \\ = \left(u_1^{q+1}u_2^{q+1} + u_2 + u_1^q\right)\left(u_2 \cdot \left(u_1^{q+1}u_2^{q+1} + u_2 + u_1^q\right)^{q-1} - u_1^{q^2}\right). \end{aligned}$$

We will now recover these two factors in Equations (7) and (8) using the modular theory, thus giving them a modular interpretation. The composite $\lambda_2 \circ \lambda_1$ will be an isogeny from $\varphi^{(1)}$ to $\varphi^{(3)}$, with

$$\ker \lambda_2 \circ \lambda_1 \subseteq \varphi^{(1)}[T^2].$$

Since $\lambda_2 \circ \lambda_1$ defines a separable map of degree q^2, under the $\phi^{(1)}$-action $\ker \lambda_2 \circ \lambda_1$ is an $\mathbb{F}_q[T]/\langle T^2\rangle$-module with q^2 elements. Hence it will be isomorphic to $\langle T\rangle/\langle T^2\rangle \bigoplus \langle T\rangle/\langle T^2\rangle$ or $\mathbb{F}_q[T]/\langle T^2\rangle$ as an $\mathbb{F}_q[T]/\langle T^2\rangle$-module. In the first case $\ker \lambda_2 \circ \lambda_1$ is annihilated by $\varphi_T^{(1)}$, so $\lambda_2 \circ \lambda_1$ is a T-isogeny of $\varphi^{(1)}$ of rank 2. In the second case $\ker \lambda_2 \circ \lambda_1$ is a free $\mathbb{F}_q[T]/\langle T^2\rangle$-submodule of $\varphi^{(1)}[T^2]$, so $\lambda_2 \circ \lambda_1$ is a T^2-isogeny of rank 1. We will consider these two cases separately in detail.

- In the first case where $\lambda_2 \circ \lambda_1$ is a right factor of $\varphi_T^{(1)} = \mu_1 \circ \lambda_1$, we have that λ_2 is a right factor of μ_1 already. Let x_2 be a nonzero T-torsion point in the kernel of λ_2, i.e., $x_2^{q-1} = u_2$. Then, using Equation (4):

  $$\mu_1(x_2) = -x_2^{q^2} - \frac{1}{u_1^{q+1}}x_2^q - \frac{1}{u_1}x_2 = 0.$$

  Dividing by x_2 we obtain

  $$-(x_2^{q-1})^{q+1} - \frac{1}{u_1^{q+1}}x_2^{q-1} - \frac{1}{u_1} = -u_2^{q+1} - \frac{1}{u_1^{q+1}}u_2 - \frac{1}{u_1} = 0.$$

  After clearing denominators, we obtain

  $$u_1^{q+1}u_2^{q+1} + u_2 + u_1^q = 0. \tag{7}$$

- In the second case where λ_2 is a right factor of $\varphi_T^{(2)} = \lambda_1 \circ \mu_1$, but not a right factor of μ_1, the kernel of $\lambda_2 \circ \lambda_1$ is annihilated by T^2 but not by T. So $\lambda_2 \circ \lambda_1$ is a T^2-isogeny of rank 1. As before, let x_2 be a nonzero T-torsion point in the kernel of λ_2. Then, since $\varphi_T^{(2)} = \lambda_1 \circ \mu_1$, the quantity

  $$\mu_1(x_2) = -x_2^{q^2} - \frac{1}{u_1^{q+1}}x_2^q - \frac{1}{u_1}x_2$$

is a nonzero element of the kernel of $\lambda_1 = \tau - u_1$, i.e., a root of $T^{q-1} - u_1$. So we have

$$\begin{aligned}
&\left(-x_2^{q^2} - \frac{1}{u_1^{q+1}} x_2^q - \frac{1}{u_1} x_2\right)^{q-1} - u_1 \\
&= x_2^{q-1} \cdot \left(-(x_2^{q-1})^{q+1} - \frac{1}{u_1^{q+1}} x_2^{q-1} - \frac{1}{u_1}\right)^{q-1} - u_1 \\
&= u_2 \cdot \left(-u_2^{q+1} - \frac{1}{u_1^{q+1}} u_2 - \frac{1}{u_1}\right)^{q-1} - u_1 = 0.
\end{aligned}$$

After clearing denominators, we obtain

$$u_2 \cdot (u_1^{q+1} u_2^{q+1} + u_2 + u_1^q)^{q-1} - u_1^{q^2} = 0. \tag{8}$$

This behaviour also occurs when working with isomorphism classes. From Lemma 2.1 we see that the quantities $z_1 := u_1^{q^2+q+1}$ and $z_2 := u_2^{q^2+q+1}$ can be used to describe isomorphism classes. By raising both sides in Equation (6) to the $q^2 + q + 1$-st power, we see that

$$\frac{(z_2 - 1)^{q^2+q+1}}{z_2^{q+1}} = g_2^{q^2+q+1} = \frac{(z_1 - 1)^{q^2+q+1}}{z_1^{q^2+q}} \ . \tag{9}$$

The analogues of the factors described in Equations (7) and (8) can be given below in Equations (10) and (11).

$$0 = z_2^{q+1}(z_1 - 1)^{q^2+q+1} - (z_2 - 1)^{q^2+q+1} z_1^{q^2+q} = F_1 \cdot F_2 \ ,$$

where

$$z_2(z_1 - 1)^{q+1} + (z_1 - 1) z_1^q (z_2 - 1)^q + z_1^{q+1}(z_2 - 1)^{q+1} = 0. \tag{10}$$

$$(z_1 - 1) z_2 \cdot \left(z_2(z_1 - 1)^{q+1} + (z_1 - 1) z_1^q (z_2 - 1)^q + z_1^{q+1}(z_2 - 1)^{q+1}\right)^{q-1} - z_1^{q^2}(z_2 - 1)^{q^2} = 0. \tag{11}$$

3.2 Composition of three T-isogenies

The factor of degree $q+1$ found in Equation (7) corresponded to the situation of two T-isogenies $\lambda_1 : \varphi^{(1)} \to \varphi^{(2)}$ and $\lambda_2 : \varphi^{(2)} \to \varphi^{(3)}$ whose composition $\lambda_2 \circ \lambda_1$ is a T-isogeny of rank 2. Now consider a third T-isogeny $\lambda_3 : \varphi^{(3)} \to \varphi^{(4)}$ and assume that $\lambda_3 \circ \lambda_2$ is a T-isogeny of rank 2 as well. Writing $\lambda_3 = \tau - u_3$, we see that

$$u_1^{q+1} u_2^{q+1} + u_2 + u_1^q = 0 \text{ and } u_2^{q+1} u_3^{q+1} + u_3 + u_2^q = 0.$$

However,

$$0 = u_2^{q+1} u_3^{q+1} + u_3 + u_2^q = \left(u_2 u_3 - \frac{1}{u_1}\right)\left(u_2 u_3 \left(u_2 u_3 - \frac{1}{u_1}\right)^{q-1} - u_1 u_2^q\right). \tag{12}$$

These factors can be explained and obtained using modular theory (see Equation (13) and (16)).

- If $\lambda_3 \circ \lambda_2 \circ \lambda_1 = (\tau - u_3)(\tau - u_2)(\tau - u_1)$ is a T-isogeny of rank 3, then $\varphi_T^{(1)} = -(\tau - u_3)(\tau - u_2)(\tau - u_1)$, implying that $u_3 u_2 u_1 = 1$, or equivalently

$$u_2 u_3 - \frac{1}{u_1} = 0. \tag{13}$$

- Assume that $\lambda_3 \circ \lambda_2 \circ \lambda_1$ is not a T-isogeny. Since $\lambda_2 \circ \lambda_1 : \varphi^{(1)} \to \varphi^{(3)}$ (resp. $\lambda_3 \circ \lambda_2 : \varphi^{(2)} \to \varphi^{(4)}$) is a T-isogeny, it is a right factor of $\varphi_T^{(1)}$ (resp. $\varphi_T^{(2)}$). This implies that

$$\varphi_T^{(1)} = \left(-\tau + \frac{1}{u_1 u_2}\right)(\tau - u_2)(\tau - u_1) \text{ and } \varphi_T^{(2)} = \left(-\tau + \frac{1}{u_2 u_3}\right)(\tau - u_3)(\tau - u_2). \quad (14)$$

Since furthermore $(\tau - u_1)\varphi_T^{(1)} = \varphi_T^{(2)}(\tau - u_1)$, we see after canceling common factors that

$$(\tau - u_1)\left(-\tau + \frac{1}{u_1 u_2}\right) = \left(-\tau + \frac{1}{u_2 u_3}\right)(\tau - u_3). \quad (15)$$

Denote by x_3 a nonzero element in $\ker \lambda_3$, so that $x_3^{q-1} = u_3$. Then x_3 is in the kernel of the righthand side in Equation (15). However, x_3 is not in the kernel of $(-\tau + 1/(u_1 u_2))$, since this would give $\lambda_3 = (\tau - 1/(u_1 u_2))$ and hence that $\lambda_3 \circ \lambda_2 \circ \lambda_1 = -\varphi_T^{(1)}$ would be a T-isogeny. Therefore, using Equation (15), we see that $-x_3^q + x_3/(u_1 u_2)$ is a nonzero element of $\ker \lambda_1$, which implies that

$$0 = \left(-x_3^q + \frac{x_3}{u_1 u_2}\right)^{q-1} - u_1 = x_3^{q-1}\left(-x_3^{q-1} + \frac{1}{u_1 u_2}\right)^{q-1} - u_1 = u_3\left(-u_3 + \frac{1}{u_1 u_2}\right)^{q-1} - u_1$$

or alternatively

$$u_2 u_3 \left(u_2 u_3 - \frac{1}{u_1}\right)^{q-1} - u_1 u_2^q = 0. \quad (16)$$

When passing to isomorphism classes, similar phenomena occur. First of all Equation (7) is replaced by Equation (10). Given that

$$z_2(z_1 - 1)^{q+1} + (z_1 - 1)z_1^q(z_2 - 1)^q + z_1^{q+1}(z_2 - 1)^{q+1} = 0,$$

one then obtains by direct verification that

$$\begin{aligned} 0 &= z_3(z_2 - 1)^{q+1} + (z_2 - 1)z_2^q(z_3 - 1)^q + z_2^{q+1}(z_3 - 1)^{q+1} \\ &= \left(z_2 z_3 - \frac{1}{z_1}\right)\left((z_2 z_3 - 1)\left(z_2 z_3 - \frac{1}{z_1}\right)^{q-1} - \frac{(z_2 - 1)^q}{z_2} - \frac{(z_1 - 1)^q}{z_1^q}\right). \end{aligned}$$

The analogues of Equations (13) and (16) when working with isomorphism classes are therefore given by

$$z_2 z_3 - \frac{1}{z_1} = 0 \quad (17)$$

and

$$(z_2 z_3 - 1)\left(z_2 z_3 - \frac{1}{z_1}\right)^{q-1} - \frac{(z_2 - 1)^q}{z_2} - \frac{(z_1 - 1)^q}{z_1^q} = 0. \quad (18)$$

3.3 Composition of more than three isogenies

We finish this section by giving some information on the composite of more than three T-isogenies. As before let $\phi^{(i)}$ be Drinfeld modules given by $\phi_T^{(i)} = -\tau^3 + g_i\tau + 1$ and let $\lambda_i : \phi^{(i)} \mapsto \phi^{(i+1)}$ be T-isogenies of rank 1 with $\lambda_i = \tau - u_i$ for nonzero element $u_i \in L$. In this subsection we always assume that the composite of two T-isogenies $\lambda_i \circ \lambda_{i+1} : \phi^{(i)} \mapsto \phi^{(i+2)}$ is a T-isogeny of rank 2, but that the composite of three T-isogenies $\lambda_i \circ \lambda_{i+1} \circ \lambda_{i+2} : \phi^{(i)} \mapsto \phi^{(i+3)}$ is not a T-isogeny. These assumptions correspond to the case in the previous subsections leading to Equations (10) and (18). Using this we show the following theorem.

Theorem 3.1 *Assume that for any $i \geq 1$, the composite of two T-isogenies $\lambda_i \circ \lambda_{i+1}$ is a T-isogeny of rank 2, but that the composite of three T-isogenies $\lambda_{i+2} \circ \lambda_{i+1} \circ \lambda_i$ is not a T-isogeny. Then the composite of $2k$ many T-isogenies $\lambda_{i+2k-1} \circ \cdots \circ \lambda_i$ is a T^k-isogeny of rank 2.*

Proof. First note that similarly as in Equation (14), the assumption that the composite of two T-isogenies $\lambda_i \circ \lambda_{i+1}$ is a T-isogeny of rank 2, implies that:

$$\phi_T^{(i)} = \eta_i \circ \lambda_{i+1} \circ \lambda_i \ , \quad \phi_T^{(i+1)} = \lambda_i \circ \eta_i \circ \lambda_{i+1} \quad \text{and} \quad \phi_T^{(i+2)} = \lambda_{i+1} \circ \lambda_i \circ \eta_i \ , \tag{19}$$

where $\eta_i = -(\tau - 1/(u_{i+1}u_i))$. We firstly prove that for any integers $i, k \geq 1$ we have

$$\phi_{T^k}^{(i)} = \eta_i \circ \eta_{i+2} \circ \cdots \circ \eta_{i+2k-2} \circ \lambda_{i+2k-1} \circ \lambda_{i+2k-2} \circ \cdots \circ \lambda_{i+1} \circ \lambda_i \ .$$

The proof is induction on k. By our assumption, the argument is trivially true for $k = 1$. Now suppose that it is true for $k = n$. Then by using Equation (19) we obtain the following equalities, which concludes the desired argument.

$$\begin{aligned}
\phi_{T^{n+1}}^{(i)} &= \phi_{T^n}^{(i)} \circ \phi_T^{(i)} \\
&= (\eta_i \circ \eta_{i+2} \circ \cdots \circ \eta_{i+2n-2} \circ \lambda_{i+2n-1} \circ \lambda_{i+2n-2} \circ \cdots \circ \lambda_{i+1} \circ \lambda_i) \circ (\eta_i \circ \lambda_{i+1} \circ \lambda_i) \\
&= (\eta_i \circ \eta_{i+2} \circ \cdots \circ \eta_{i+2n-2} \circ \lambda_{i+2n-1} \circ \lambda_{i+2n-2} \circ \cdots \circ \lambda_{i+1}) \circ (\lambda_i \circ \eta_i \circ \lambda_{i+1}) \circ \lambda_i \\
&= (\eta_i \circ \eta_{i+2} \circ \cdots \circ \eta_{i+2n-2} \circ \lambda_{i+2n-1} \circ \lambda_{i+2n-2} \circ \cdots \circ \lambda_{i+1}) \circ \phi_T^{(i+1)} \circ \lambda_i \\
&= (\eta_i \circ \eta_{i+2} \circ \cdots \circ \eta_{i+2n-2} \circ \lambda_{i+2n-1} \circ \lambda_{i+2n-2} \circ \cdots \circ \lambda_{i+1}) \circ (\eta_{i+1} \circ \lambda_{i+2} \circ \lambda_{i+1}) \circ \lambda_i \\
&\ \ \vdots \\
&= \eta_i \circ \eta_{i+2} \circ \cdots \circ \eta_{i+2n} \circ \lambda_{i+2n+1} \circ \lambda_{i+2n} \circ \cdots \circ \lambda_{i+1} \circ \lambda_i \, .
\end{aligned}$$

Now set $\mathbf{K}_n := \ker(\lambda_{i+2n-1} \circ \cdots \circ \lambda_i)$ for $n \geq 1$. From above equalities we see that $\mathbf{K}_{n+1}$ is annihilated by $\phi_{T^{n+1}}^{(i)}$, and hence $\mathbf{K}_{n+1}$ is an $\mathbb{F}[T]/\langle T^{n+1} \rangle$ module of cardinality q^{2n+2}. We consider the map $m_T : \mathbf{K}_{n+1} \to \mathbf{K}_n$ defined by $m_T(a) = \phi_T^{(i)}(a)$ for $a \in \mathbf{K}_{n+1}$. Note that since $\mathbf{K}_{n+1}$ is annihilated by $\phi_{T^{n+1}}^{(i)}$, the map m_T is well-defined homomorphism. It is clear that $\ker(\lambda_{i+1} \circ \lambda_i)$ lies in the set $\ker(m_T)$, and hence the cardinality of $\ker(m_T)$ is at least q^2. On the other hand, $\ker(m_T)$ contain at most q^3 elements since $\ker(m_T)$ lies in $\phi^{(i)}[T]$.

Now we prove that the cardinality of $\ker(m_T)$ is equal to q^2. Suppose our claim is not true. Then $\phi^{(i)}[T] \subseteq \mathbf{K}_{n+1}$ and this implies that

$$\lambda_{i+2n+1} \circ \cdots \circ \lambda_i = \psi_i \circ \phi_T^{(i)} = \psi_i \circ \eta_i \circ \lambda_{i+1} \circ \lambda_i \ ,$$

for some $\psi_i \in L\{\tau\}$. In other words, $\lambda_{i+2n+1} \circ \cdots \circ \lambda_{i+2} = \psi_i \circ \eta_i$, where as before $\eta_i = -(\tau - 1/(u_{i+1}u_i))$. Let $1/(x_{i+1}x_i)$ be a nonzero torsion point of η_i. Since by assumption $\lambda_{i+2} \circ \lambda_{i+1} \circ \lambda_i$ is not a T-isogeny, there exists an integer j with $2 < j \leq 2n+1$ such that $1/(x_{i+1}x_i)$ is a nonzero torsion point of $\lambda_{i+j} \circ \cdots \circ \lambda_{i+2}$ but it is not a torsion point of $\lambda_{i+j-1} \circ \cdots \circ \lambda_{i+2}$. Hence the polynomial $f(T) = (T^q - u_{i+j-1}T) \circ \cdots \circ (T^q - u_{i+2}T)$ evaluated at $1/(x_{i+1}x_i)$ is a nonzero torsion point of λ_{i+j}.This means that $(f\,(1/(x_{i+1}x_i)))^{q-1} = u_{i+j}$. Note that

$$f(T) = T^{q^{j-2}} + a_{j-3}T^{q^{j-3}} + \cdots + a_1T^q + a_0T \, ,$$

where the a_ℓ's are polynomials in $\mathbb{Z}[u_{i+j-1}, \ldots, u_{i+2}]$. As a result,

$$\begin{aligned}
u_{i+j} &= f\left(\frac{1}{x_{i+1}x_i}\right)^{q-1} \qquad (20) \\
&= \left(\frac{1}{x_{i+1}x_i}\right)^{q-1} \left(\left(\frac{1}{x_{i+1}x_i}\right)^{q^{j-2}-1} + a_{j-3}\left(\frac{1}{x_{i+1}x_i}\right)^{q^{j-3}-1} + \cdots + a_1\left(\frac{1}{x_{i+1}x_i}\right)^{q-1} + a_0\right)^{q-1} .
\end{aligned}$$

Since $1/(x_{i+1}x_i)$ is a nonzero torsion point of η_i, we have $(1/(x_{i+1}x_i))^{q-1} = 1/(u_{i+1}u_i)$. By Equation (20), we can express u_{i+j} as a rational function of $u_{i+j-1}, \ldots, u_{i+2}, u_{i+1}, u_i$ with coefficients in the prime field. Then we have the following figure:

$$\begin{array}{ccc} \mathbb{F}(u_1,\ldots,u_{i+j-1}) & \xrightarrow[\deg=1]{} & \mathbb{F}(u_1,\ldots,u_{i+j}) \\ \Big| & \Longrightarrow \quad \text{tame extensions} \quad \Longleftarrow & \Big| \\ \mathbb{F}(z_1,\ldots,z_{i+j-1}) & \xrightarrow[\deg=q]{} & \mathbb{F}(z_1,\ldots,z_{i+j}) \end{array}$$

Since $z_i = u_i^{q^2+q+1}$ for all values of i, the extensions $\mathbb{F}_{q^3}(u_1,\ldots,u_{i+j})/\mathbb{F}_{q^3}(z_1,\ldots,z_{i+j})$ and $\mathbb{F}_{q^3}(u_1,\ldots,u_{i+j-1})/\mathbb{F}_{q^3}(z_1,\ldots,z_{i+j-1})$ are tame. Moreover, as shown in [1, Sec.2.1], the extension degree of $\mathbb{F}_{q^3}(z_1,\ldots,z_{i+j})/\mathbb{F}_{q^3}(z_1,\ldots,z_{i+j-1})$, equals q. Therefore we obtain a contradiction. Hence $\ker(m_T)$ has q^2 elements.

Combining the structure theorem for finitely generated modules over a principal ideal domain with the fact that $\ker(m_T)$ has q^2 elements, we may conclude that $\mathbf{K}_{n+1}$ is isomorphic to a direct sum of exactly two cyclic submodules, i.e.:

$$\mathbf{K}_{n+1} \cong \langle T^{\ell_1}\rangle/\langle T^{n+1}\rangle \bigoplus \langle T^{\ell_2}\rangle/\langle T^{n+1}\rangle\,.$$

Further, since the cardinality of $\mathbf{K}_{n+1}$ is q^{2n+2}, we obtain that $\ell_1 = \ell_2 = 0$. In other words, $\lambda_{i+2n+1} \circ \cdots \circ \lambda_i$ is a T^{n+1}-isogeny of rank 2. ■

4 Two cubic, recursive towers of function fields

A sequence of function fields $\mathcal{F} = (F_1 \subseteq F_2 \subseteq \ldots)$ over $\mathbb{F}_q$ is called recursive if there exists $f(X,Y) \in \mathbb{F}_q[X,Y]$ such that

(i) there exists $x_1 \in F_1$ transcendental over $\mathbb{F}_q$, such that $F_1 = \mathbb{F}_q(x_1)$, and

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

The polynomial $f(X,Y)$ may not determine the sequence $\mathcal{F}$ uniquely, since it may happen that the polynomial $f(x_i,T) \in F_i[T]$ is reducible for some i. In such cases, there may exist distinct sequences of function fields satisfying the same recursion. Put into another way: the polynomial $f(X,Y)$ may give rise to several recursive sequences of function fields as given in Remark 4.2.

A recursive sequence of function fields $\mathcal{F}$ is called a recursive tower with constant field $\mathbb{F}_q$, if

(i) for all $i \geq 1$, the finite field $\mathbb{F}_q$ is the full constant field of F_1, and

(ii) $\lim_{i\to\infty} g(F_i) = \infty$.

Recursive towers of function fields have been used to achieve excellent lower bounds on Ihara's constant $A(q)$, see [2]. Cubic, recursive towers (whose field of definition we will denote by $\mathbb{F}_{q^3}$) can be obtained from the modular setting in a natural way. For $i \geq 1$, let $\varphi^{(i)}$ be normalized weakly supersingular Drinfeld modules given by $\varphi_T^{(i)} = -\tau^3 + g_i\tau^2 + 1$ and let $\lambda^{(i)} : \varphi^{(i)} \to \varphi^{(i+1)}$ be T-isogenies of the form $\lambda^{(i)} = \tau - u_i$. In the previous section we have seen that the variables g_i and u_j are related to each other in an algebraic way. These relations give rise to several recursive towers of function fields.

As Lemma 2.1 suggests, it is natural to pass to the variables $z_i := u_i^{q^2+q+1}$. We then find two cubic, recursive sequences of function fields:

Definition 4.1 *We denote by* $\mathcal{D} = (D_1 \subset D_2 \subset \cdots)$ *a recursive sequence of function fields satisfying* $D_1 = \mathbb{F}_{q^3}(z_1)$ *and* $D_{i+1} = D_i(z_{i+1})$*, with*

$$z_2(z_1-1)^{q+1} + (z_1-1)z_1^q(z_2-1)^q + z_1^{q+1}(z_2-1)^{q+1} = 0$$

and

$$(z_iz_{i+1}-1)\left(z_iz_{i+1} - \frac{1}{z_{i-1}}\right)^{q-1} - \frac{(z_i-1)^q}{z_i} - \frac{(z_{i-1}-1)^q}{z_{i-1}^q} = 0 \text{ for } i \geq 2.$$

Further we denote by $\mathcal{E} = (E_1 \subset E_2 \subset \cdots)$ *a recursive sequence of function fields satisfying* $E_1 = \mathbb{F}_{q^3}(z_1)$ *and* $E_{i+1} = E_i(z_{i+1})$*, with*

$$(z_i-1)z_{i+1}\cdot\left(z_{i+1}(z_i-1)^{q+1} + (z_i-1)z_i^q(z_{i+1}-1)^q + z_i^{q+1}(z_{i+1}-1)^{q+1}\right)^{q-1} - z_i^{q^2}(z_{i+1}-1)^{q^2} = 0$$

for $i \geq 1$*.*

Remark 4.2 *By definition, sequence* $\mathcal{E}$ *satisfies the recursion*

$$(X-1)Y\cdot\left(Y(X-1)^{q+1} + (X-1)X^q(Y-1)^q + X^{q+1}(Y-1)^{q+1}\right)^{q-1} - X^{q^2}(Y-1)^{q^2} = 0.$$

Comparing the definition of sequence $\mathcal{D}$ *with Equations* (10) *and* (18)*, we see that sequence* $\mathcal{D}$ *satisfies the recursion*

$$Y(X-1)^{q+1} + (X-1)X^q(z_2-1)^q + X^{q+1}(Y-1)^{q+1} = 0.$$

Since Equations (10) *and* (11) *arise as factors of the same function given in Equation* (9)*, we conclude that both sequences* $\mathcal{D}$ *and* $\mathcal{E}$ *satisfy the same recursion, namely*

$$Y^{q+1}(X-1)^{q^2+q+1} - (Y-1)^{q^2+q+1}X^{q^2+q} = 0.$$

Remark 4.3 *In [1] (see the proof of Lemma 2.6 there) it is shown that the sequence* $\mathcal{D}$ *is in fact a tower with full constant field* $\mathbb{F}_{q^3}$*. More precisely, it is shown there that for the tower* $\mathcal{D}$ *it holds that* $[D_2 : D_1] = q+1$ *and* $[D_{i+1} : D_i] = q$ *if* $i > 1$*. Moreover, it is shown that*

$$z_1 = (\alpha_1+1)/\alpha_1^{q+1} \qquad \text{and} \qquad z_2 = \alpha_1^{q+1} + \alpha_1\ ,$$

where $\alpha_1 := (z_1z_2-1)/(z_1+1)$*. This shows in particular that the second function field* D_2 *is rational. If for* $i \geq 1$ *we define* $C_i := D_{i+1}$ *and* $\alpha_i := (z_iz_{i+1}-1)/(z_i+1)$*, we obtain a tower* $\mathcal{C} = (C_1 \subset C_2 \subset \cdots)$ *with variables* $\alpha_1, \alpha_2, \ldots$ *satisfying the recursion*

$$\frac{\alpha_{i+1}+1}{\alpha_{i+1}^{q+1}} = \alpha_i^{q+1} + \alpha_i\,. \tag{21}$$

Remark 4.4 *Tower* $\mathcal{E}$ *is in fact (up to a change of variables) the same as the particular case* $n = 3$*,* $j = 2$ *and* $k = 1$ *of the tower* $\mathcal{H}$ *studied in [2].*

5 Relation to previously known cubic towers

In this section we give an overview of several previously studied, cubic, recursive towers for which no modular interpretation was known. These towers all have limit at least $2(q^2-1)/(q+2)$, which is Zink's bound for $A(q^3)$. We will also see that they essentially all are equal to tower $\mathcal{D}$. Since the defining equations of tower $\mathcal{D}$ are explained by the theory of Drinfeld modules, we will then have obtained our goal.

The first explicit tower known to achieve Zink's bound was given in [8]. This tower is defined recursively over the field $\mathbb{F}_8$ by the equation

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

In [5] this tower was generalized for any q. The tower found in [5] is recursively defined by the equation

$$\frac{Y^q}{1-Y} = \frac{X}{X^q + X - 1},$$

or equivalently, after the change of variables $x = 1/X$ and $y = 1/Y$, by

$$y^q - y^{q-1} = \frac{1}{x^{q-1}} + 1 - x. \tag{22}$$

We denote the tower recursively defined by Equation (22) by $\mathcal{A} = (A_1 \subset A_2 \subset \cdots)$ and the variables by $x_1, x_2, \ldots$. Given in this form, it is clear that for $q = 2$, the tower $\mathcal{A}$ reduces to the tower in [8].

In [12, 6] it was shown that the tower in [5] also can be defined by the reducible equation

$$v^{q+1} + v = \frac{u+1}{u^{q+1}}. \tag{23}$$

More precisely, the observations in [12] imply that the quantities $U = x^q - x^{q-1}$ and $V = 1/x^{q-1} + 1 - x$ satisfy the equation

$$\frac{-V^q}{(1-V)^{q+1}} = \frac{U-1}{U^{q+1}}.$$

After the substitution of variables $u = -1 + 1/U$ and $v = -1 + 1/V$, Equation (23) follows. Note that the polynomial $v^{q+1} + v - (u+1)/u^{q+1} \in \mathbb{F}_{q^3}(u)[v]$ is the product of $v + (u+1)/u$ and an irreducible factor of degree q given by the left-hand-side of the equation:

$$1 + \sum_{i=0}^{q} v^i \left(-\frac{u+1}{u}\right)^{q-i} = 0. \tag{24}$$

This equation is used to define a tower $\mathcal{B} = (B_1 \subset B_2 \subset \cdots)$ with constant field $\mathbb{F}_{q^3}$. Note that since u and v generate the rational function field $\mathbb{F}_{q^3}(x)$ (since $1/x = u(v+1)$), the towers $\mathcal{A}$ and $\mathcal{B}$ recursively defined by Equations (22) and (24) are essentially the same. To be precise, for $i \geq 1$ we have $A_i = B_{i+1}$ or in other words: if one deletes the first function field of the tower defined by Equation (24), one obtains the tower defined by (22). The towers therefore have the same limit. This limit was computed in [4] (using results from [3] and [5]) to be equal to $2(q^2-1)/(q+2)$.

Given a recursive tower $\mathcal{F}$ satisfying the recursion $F(x, y) = 0$, we define the dual tower of $\mathcal{F}$ to be the recursive tower satisfying the recursion $F(y, x) = 0$. Essentially, the order of the

variables is interchanged. In particular, this means that reversing the order of the variables, gives an isomorphism between the i-th function fields of tower and its dual. Comparing Remark 4.3 and Equation (23), we conclude that the towers $\mathcal{C}$ and $\mathcal{A}$ are duals of each other. In particular that $C_i \cong A_i$ for all $i \geq 1$. In particular, the towers $\mathcal{A}$ and $\mathcal{B}$ can be obtained and explained using the theory of normalized Drinfeld modules of rank 3.

Concluding, an overview of the relation between towers $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ is as in the following figure:

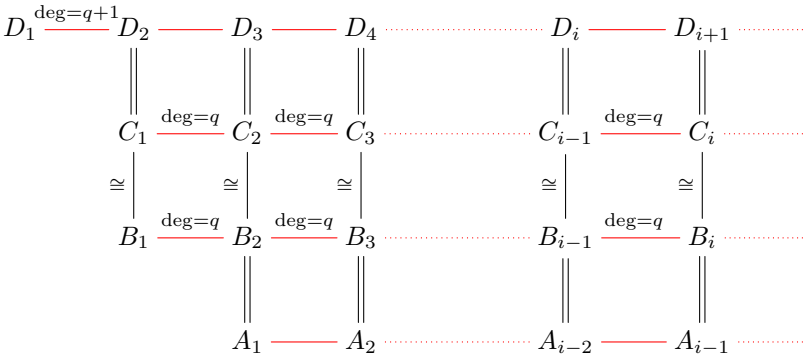

Figure 1: Relationship between towers $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ and $\mathcal{D}$.

References

[1] N. Anbar, P. Beelen, N. Nguyen, "The exact limit of some cubic towers", to appear in the proceedings of AGCT-15.

[2] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, "Towers of function fields over non-prime finite fields", Moscow Mathematical Journal, pp. 1–29, 2015.

[3] P. Beelen, "Graphs and recursively defined towers of function fields", Journal of number theory **108**, 217–240 (2004).

[4] P. Beelen, A. Garcia and H. Stichtenoth, "On towers of function fields over finite fields", Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr. **11**, 1–20 (2005).

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

[6] N. Caro and A. Garcia, "On a tower of Ihara and its limit", Acta Arith. **151**, 191–200 (2012).

[7] N.D. Elkies, "Explicit Towers of Drinfeld Modular Curves", Progress In Mathematics **202**, 189–198 (2001).

[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] E.-U. Gekeler, "On finite Drinfeld modules", J. Algebra **141**, 187–203 (1991).

[10] D. Goss, "Basic structures of function field arithmetic", Springer Berlin Heidelberg, 1996.

[11] Y. Ihara, "Some remarks on the number of rational points of algebratic curves over finite fields", J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28(3)**, 721-724 (1982).

[12] Y. Ihara, "Some remarks on the BGS tower over finite cubic fields", Proceedings of the workshop Arithmetic Geometry, Related Areas and Applications, Chuo University (2007), 127-131.

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

[14] S.G. Vladut and V.G. Drinfel'd, "Number of points of an algebraic curve", Functional analysis and its applications **17(1)** , 53–54 (1983).

[15] Th. Zink, "Degeneration of Shimura surfaces and a problem in coding theory", In: Fundamentals of computation theory (Cottbus, 1985), Lecture Notes in Comput. Sci. **199**, 503–511 (1985).