Explicit Towers of Drinfeld Modular Curves

Explicit towers of Drinfeld modular curves

Noam D. Elkies

Abstract. We give explicit equations for the simplest towers of Drinfeld modular curves over any finite field, and observe that they coincide with the asymptotically optimal towers of curves constructed by Garcia and Stichtenoth.

1. Introduction

Fix a finite field k_1 of size q_1. It has been known for almost twenty years (see [16, 18, 17]) that any curve C/k_1 of genus $g = g(C)$ has at most $(q_1^{1/2} - 1 + o(1))g$ points rational over k_1 as $g \to \infty$ (the *Drinfeld-Vlăduţ bound* [1]), and that if q_1 is a square then there are various families of classical, Shimura, or Drinfeld modular curves C/k_1 of genus $g \to \infty$ with $\#(C(k_1)) \geq (q_1^{1/2} - 1)(g - 1)$. Thus such curves are "asymptotically optimal": they attain the lim sup of $\#(C(k_1))/g(C)$. Moreover, asymptotically optimal curves yield excellent linear error-correcting codes over k_1 [12, 17].

To actually construct and use these Goppa codes one needs explicit equations for asymptotically optimal C. Now the definitions of modular curves are in principle constructive, but it is usually not feasible to actually exhibit a given modular curve. For certain Drinfeld modular curves, [17, pp.453ff.] gives explicit, albeit unpleasant, models as plane curves with two complicated singularities. Garcia and Stichtenoth gave nice formulas for asymptotically optimal families of curves in [6] for $q_1 = 4, 9$ (see also [7]), and in [4] for all square prime powers q_1. In each case they construct a sequence of curves $C_1, C_2, C_3, \ldots$ forming what we'll call a *recursive tower*. A "tower" $\{C_n\}$ is a sequence of curves in which each C_n is given as a low-degree cover of C_{n-1}. We shall call a tower "recursive" if C_2 is given as a curve in $C_1 \times C_1$, and C_n is the curve in C_1^n consisting of n-tuples $(P_1, \ldots, P_n)$ of points in C_1 such that $(P_j, P_{j+1}) \in C_2$ for each $j = 1, 2, \ldots, n-1$. That is, C_n is obtained by iterating $n-1$ times the correspondence from C_1 to itself given by C_2. In each of the cases discovered by Garcia and Stichtenoth, analysis of this correspondence yields the genus of each C_n and enough k_1-rational points on C_n to prove that $\#(C_n(k_1)) \geq (q_1^{1/2} - 1)g(C_n)$. The genus grows exponentially with n, yet only $O(n)$ equations of bounded degree are needed to exhibit C_n.

Now while equations for most modular curves cannot be reasonably exhibited, modular curves whose conductors are products of small primes form towers, and modular curves with a single repeated factor even form recursive towers. For instance, for any integers $N_0 \geq 1$ and $l > 1$, the classical modular curves $X_0(N_0 l^n)$ $(n = 1, 2, 3, \dots)$ form a recursive tower of curves related by maps of degree l. There are analogous towers of Shimura and Drinfeld modular curves. We observed in [3] that this can be used to exhibit asymptotically optimal towers, and carried out the computation of explicit equations for eight such towers, six of classical modular curves and two of Shimura curves. Moreover, we showed that the towers of classical modular curves $\mathrm{X}_0(2^n)$ and $\mathrm{X}_0(3^n)$ in characteristics 3 and 2 respectively are the same as the towers constructed in [6].

In the same paper we noted that similar methods can be used to exhibit towers of Drinfeld modular curves, and announced that one such tower recovers the curves constructed in [4] for arbitrary square q_1. In the present paper we specify this tower and perform the computations that determine its equations and thus identify it with the Garcia-Stichtenoth tower. We do the same for a closely related tower obtained by Garcia and Stichtenoth in [5].

In the next section we recall basic definitions of Drinfeld modules, isogenies, and supersingularity. The following section describes certain Drinfeld modular curves. In both sections we simplify the exposition by describing only the modules and curves that arise in the interpretation of the Garcia-Stichtenoth towers; for a thorough treatment of the general case we refer to [9]. In the final section we give explicit equations for several of the simplest towers of Drinfeld modular curves and observe that two of them coincide with asymptotically optimal towers obtained by Garcia and Stichtenoth.

Acknowledgements. I thank Bjorn Poonen for introducing me to Drinfeld modules, and Henning Stichtenoth for information on his and Garcia's asymptotically optimal towers. Thanks also to E.-U. Gekeler, D. Goss, B.H. Gross, B. Poonen, and M. Zieve for much enlightening communication concerning Drinfeld modules and modular curves.

This work was made possible in part by funding from the Packard Foundation.

2. Drinfeld modules and isogenies

Fix a finite field k of size q. (In our application, k_1 will be the quadratic extension of k, so $q_1 = q^2$; the use of "k" instead of "$\mathbf{F}_q$" is our only divergence from the notations of [9]). For any field $L \supseteq k$, we denote by $L\{\tau\}$ the non-commutative L-algebra generated by τ and satisfying the relation $\tau a = a^q \tau$ for all $a \in L$. Equivalently, $L\{\tau\}$ is the ring of endomorphisms of $\mathbf{G}_a$ defined over L and linear over k. Explicitly, the polynomial $\sum_{i=0}^{n} l_i \tau^i$ acts on $\mathbf{G}_a$ as the endomorphism taking any X to the q-linearized polynomial $\sum_{i=0}^{n} l_i X^{q^i}$.

We only consider Drinfeld modules of rank 2, and usually only ones associated to a function field of genus 0 with a place at infinity of degree 1. Let then $K = k(T)$ and $A = k[T]$. (See [9] for the general case, in which A is the ring of functions on a curve over k with poles at most at a fixed place ∞ of the curve.) In general, a Drinfeld module is defined as a k-algebra homomorphism $\phi : a \mapsto \phi_a$ from A to $L\{\tau\}$ satisfying certain technical conditions. In our case, $A = k[T]$, so specifying ϕ is equivalent to choosing ϕ_T. The rank of the resulting Drinfeld module is then simply the degree of ϕ_T as a polynomial in τ. Thus for us

$$\phi_T = l_0 + l_1\tau + l_2\tau^2 = l_0 + g\tau + \Delta\tau^2, \tag{1}$$

with nonzero *discriminant* $\Delta = \Delta(\phi)$. In general the map $\gamma : A \to L$ taking any $a \in A$ to the "constant term" (τ^0 coefficient) of ϕ_a is a ring homomorphism; in our case γ is determined by $\gamma(T) = l_0$.

If ϕ, ψ are two Drinfeld modules, an *isogeny* from ϕ to ψ is a $u \in \bar{L}\{\tau\}$ such that

$$u \circ \phi_a = \psi_a \circ u \tag{2}$$

for all $a \in A$. For our A, (2) holds for all $a \in A$ if and only if it holds for $a = T$. The *kernel* of the isogeny is[1]

$$\ker(u) := \{x \in \bar{L} : \phi_u(x) = 0\}. \tag{3}$$

This is a k-vector subspace of $\bar{L}$, which is of finite dimension unless $u = 0$. By (2), $\phi_a(x) \in \ker(u)$ for all $x \in \ker(u)$, so $\ker(u)$ in fact has the structure of an A-module. Conversely, for every finite $G \subset \bar{L}$ which is an A-submodule of $\bar{L}$ for the ϕ-action of A on $\bar{L}$, one may define $u \in \bar{L}\{\tau\}$ of degree $\dim_k G$ by

$$u(X) = \prod_{x \in G} (X - x), \tag{4}$$

and then u is an isogeny with kernel G from ϕ to some Drinfeld module ψ_a. In particular, if $u = \phi_{a_1}$ then (2) holds with $\psi = \phi$ for any $a_1 \in A$; thus ϕ_{a_1} is an isogeny from ϕ to itself, called *multiplication by* a_1. If $\gamma(a_1) \neq 0$, the kernel of this isogeny is isomorphic with $(A/a_1A)^2$ as an A-module [9, Prop. I.1.6]. Elements of $\ker(\phi_{a_1})$ are called a_1-*division points* or a_1-*torsion points* of the Drinfeld module ϕ. In particular, the T-torsion points are the roots in $x \in \bar{L}$ of

$$\phi_T(X) = \gamma(T)X + gX^q + \Delta X^{q^2}. \tag{5}$$

If γ is not injective then $\ker\gamma = Aa_0$ for some irreducible $a_0 \in A$. Then the a_0-torsion points of ϕ constitute a vector space of dimension 1 or 0 over the field A/a_0A. The Drinfeld module ϕ is then said to be *supersingular* if $\ker(\phi_{a_0}) = \{0\}$, *ordinary* otherwise. We shall use the case $\deg(a_0) = 1$, when $\phi_{a_0} = g\tau + \Delta\tau^2$ and thus ϕ is supersingular if and only if $g = 0$. Note that a_0 is of degree 1 if and only

[1] When u is not separable, i.e. has τ^0 coefficient zero, it is for many purposes better to consider $\ker(u)$ not as a subgroup of $\bar{L}$ but as a group subscheme of $\mathbf{G}_a$. We shall not need this refinement here. Note that the condition $\gamma(a) \neq 0$ occurring later in this paragraph is equivalent to the separability of ϕ_a.

if $\gamma(T) \in k$, and that Drinfeld modules over $\bar{k}$ with $\gamma(T) \in k$ may arise as the "reduction mod $(T - \gamma(T))$" of Drinfeld modules over $\bar{k}(T)$ with $\gamma(T) = T$.

3. Drinfeld modular curves

An *isomorphism* between Drinfeld modules is an invertible isogeny, i.e. some $u \in \bar{L}^*$ satisfying (2). This isomorphism multiplies each coefficient l_i in (1) by u^{1-q^i}. We define the *J-invariant* of a Drinfeld module ϕ given by (1) as follows:[2]

$$J(\phi) = \frac{g^{q+1}}{\Delta}. \tag{6}$$

Two Drinfeld modules with the same γ are isomorphic (over $\bar{L}$) if and only if their J-invariants are equal. Thus, in analogy with the case of the classical modular curves parametrizing elliptic curves, we refer to the J-line as the *Drinfeld modular curve* $\mathrm{X}(1)$ for Drinfeld modules with a given γ. Likewise, for $N \in A$ such that $\gamma(N) \neq 0$, we have Drinfeld modular curves $\mathrm{X}_0(N)$, $\mathrm{X}_1(N)$, $\mathrm{X}(N)$ parametrizing Drinfeld modules with a given γ and a choice of torsion subgroup $G \cong A/NA$, or such a subgroup G together with a generator of G as an A-module, or an identification of the group of N-torsion points with $(A/NA)^2$. These are finite separable covers of $\mathrm{X}(1)$, all of which except $\mathrm{X}(N)$ ($N \notin k^*$) are geometrically irreducible; $\mathrm{X}(N)$ is a normal cover of $\mathrm{X}(1)$ with Galois group $\mathrm{GL}_2(A/NA)$, and $\mathrm{X}_1(N)$ is an abelian normal cover of $\mathrm{X}_0(N)$ with Galois group $(A/NA)^*$. Note that, unlike $\mathrm{X}(1)$, these curves $\mathrm{X}_0(N)$, $\mathrm{X}_1(N)$, $\mathrm{X}(N)$ generally depend on the choice of γ. If $\gamma(T) \in k$, we may regard the curves $\mathrm{X}(1), \mathrm{X}_0(N), \mathrm{X}_1(N), \mathrm{X}(N)$ as the "reduction mod $(T-\gamma(T))$" of the corresponding modular curves for $\gamma(T) = T$. More generally, reducing the $\gamma(T) = T$ curves modulo any irreducible $a_0 \in A$ yields the curves parametrizing Drinfeld modules for which $\gamma(T)$ is a root of a_0.

If γ is not injective, we say that a point on a Drinfeld modular curve is *ordinary* or *supersingular* according as the Drinfeld modules it parametrizes are ordinary or supersingular. It is known that in this case the supersingular points constitute a nonempty finite set. For instance, we have seen in effect that if $\gamma(T) \in k$ then $\mathrm{X}(1)$ has the unique supersingular point $J = 0$. The supersingular points on $\mathrm{X}_0(N)$, $\mathrm{X}_1(N)$ and $\mathrm{X}(N)$ are then the preimages of $J = 0$ under the natural maps from those Drinfeld modular curves to $\mathrm{X}(1)$. It is known that each supersingular point on $\mathrm{X}_0(N)$ is defined over the quadratic extension k_1 of k, and that the same is true for certain twists of $\mathrm{X}_1(N)$ and of each component of $\mathrm{X}(N)$.

We shall relate the Garcia-Stichtenoth curves to certain Drinfeld modular curves with $N = T^n$ and $\gamma(T) = 1$. We shall find that in some cases the modules

[2] Usually a lower-case j is used for this. We use a capital J to forestall confusion with the integer variable j appearing in the next section. For elliptic curves one sometimes sees $J = j/12^3$; in the Drinfeld modular setting, no factor analogous to 12^3 is needed, so we might plausibly claim that the invariant of a Drinfeld module corresponds to J as well as j in the classical theory of modular invariants of elliptic curves ...

parametrized by these curves must satisfy the additional condition $\Delta = -1$, i.e.

$$\phi_T = 1 + g\tau - \tau^2. \tag{7}$$

We call such Drinfeld modules *normalized*. A Drinfeld module ϕ with $\gamma(T) = 1$ is isomorphic to a normalized one if and only $-\Delta(\phi)$ is a (q^2-1)-st power. This condition is invariant under isogeny. One thus expects that there would be an equivalent condition in terms of the torsion structure of ϕ. Such a condition cannot be given in completely elementary terms, because $\mathrm{GL}_2(A)$ does not have a large enough cyclic quotient. But[3] one can give an equivalent condition in terms of $\wedge^2\phi$. For a general Drinfeld module ϕ given by (1), "$\wedge^2\phi$" is the rank-1 module $T \mapsto l_0 - l_2\tau$, whose Tate modules are the discriminants of those of ϕ [14, Thm.4.1]. Thus ϕ is normalized if and only if $\wedge^2\phi$ takes T to $1-\tau$.

In terms of the coordinate J on $X(1)$, the condition that ϕ be equivalent to a normalized module is that $-J(\phi)$ be a $(q+1)$-st power. Thus normalized modules, or normalized modules with suitable level-N structure, are parametrized by curves we shall call $\dot{\mathrm{X}}(1)$, $\dot{\mathrm{X}}_0(N)$, $\dot{\mathrm{X}}_1(N)$, $\dot{\mathrm{X}}(N)$, whose function fields are obtained from those of $\mathrm{X}(1), \mathrm{X}_0(N), \mathrm{X}_1(N), \mathrm{X}(N)$ by adjoining a $(q+1)$-st root of $(-J)$.

Now by analogy with the case of classical and Shimura curves, one might expect that the curves $\mathrm{X}_0(N)$ are asymptotically optimal over k_1, and that the same is true of the twists mentioned earlier of $\mathrm{X}_1(N)$ and of the components of $\mathrm{X}(N)$, with supersingular points already providing $(q-1+o(1))g$ rational points in each case. One might even hope that the same is true with X_0, X_1, X replaced by $\dot{\mathrm{X}}_0$, $\dot{\mathrm{X}}_1$, $\dot{\mathrm{X}}$. It would be enough to prove this for $\dot{\mathrm{X}}(N)$, since all the other curves listed are quotients of $\dot{\mathrm{X}}(N)$ by subgroups of $\mathrm{GL}_2(A/NA)$. This is stated explicitly in the literature only for components of $\mathrm{X}(N)$ in the case that N is an irreducible polynomial of odd degree (see for instance [17, pp.449ff.]). We expect that the same is true for $\dot{\mathrm{X}}(N)$ and arbitrary N, and indeed even for modular curves for Drinfeld modules over rings other than $k[T]$. In each case the supersingular points are readily enumerated, and the main technical challenge is computing the genus of the curve, since the covering maps to $\mathrm{X}(1)$ are highly and wildly ramified above the "cusp" $J = \infty$. [This was also the most difficult part of Garcia and Stichtenoth's direct construction in [4].]

Even though explicit statements of asymptotic optimality have not been made, the genera of $\mathrm{X}_0(N)$, $\mathrm{X}_1(N)$, and the components of $\mathrm{X}(N)$ are known. They were computed in [13, Thm.4.4] for $\mathrm{X}(N)$, and also in Gekeler's thesis [8, Satz 3.4.8], which also deals with the case of $\mathrm{X}_0(N)$ (Satz 3.4.18). The curves $\mathrm{X}_1(N)$ were treated in [11]. These results, combined with the enumeration of supersingular points, should yield the asymptotic optimality of all these curves over k_1. Alternatively, M. Zieve suggests, and Gekeler confirms by e-mail, that one may be able to entirely avoid the genus computation and the enumeration of supersingular points by adapting an earlier proof by Ihara [15, pp.292–3] that a classical modular curve

[3] Thanks to Bjorn Poonen for pointing this out, and to David Goss for the reference to Hamahata.

of genus g has at least $(p-1)(g-1)$ points rational over the field of p^2 elements. That argument uses the reduction mod p of certain Hecke correspondences on the curve, such as $\mathrm{X}_0(Np)$ considered as a correspondence on $\mathrm{X}_0(N)$ via its map to $\mathrm{X}_0(N) \times \mathrm{X}_0(N)$ (when $\gcd(p, N) = 1$); similar correspondences are available in the Drinfeld modular setting. We are not aware of a published analysis along the same lines of the curves $\dot{\mathrm{X}}_0(N)$ etc.; but as Gekeler points out it should be straightforward to obtain their genera from those of $\mathrm{X}_0(N)$ etc., of which they are cyclic covers of degree prime to q. At any rate the results of the next section, together with the genus calculations in [4, 5], show at least that the curves $\dot{\mathrm{X}}_0(T^n)$ are asymptotically optimal.

4. Some Drinfeld modular curves of conductor T^n

If x_1 is a nonzero torsion point of ϕ then we can solve for g by setting (5) equal to zero, obtaining

$$0 = T(x_1) = x_1 + g x_1^q - x_1^{q^2}, \quad \text{i.e.} \quad g = x_1^{-q}(x_1^{q^2} - x_1). \tag{8}$$

Thus x_1 may be regarded as a coordinate for the rational curve $\dot{\mathrm{X}}_1(T)$ parametrizing normalized Drinfeld modules ϕ with a T-torsion point. For any nonzero $x \in \bar{L}$ we let t_x be the corresponding linearized polynomial

$$t_x(X) := X + \frac{x^{q^2} - x}{x^q} X^q - X^{q^2}. \tag{9}$$

The supersingular x_1 are those for which the X^q coefficient of t_{x_1} vanishes, i.e. the units of the quadratic extension k_1 of k. (The points $x_1 = 0, \infty$ are the cusps of $\dot{\mathrm{X}}_1(T)$.) We next construct the curves we shall call $\dot{\mathrm{X}}'_0(T^n)$, parametrizing ϕ with such a torsion point x_1 as well as a torsion group $G_n \cong A_0[T]/T^n$ containing x_1, and find the supersingular points on these curves. Note that $\dot{\mathrm{X}}'_0(T) = \dot{\mathrm{X}}_1(T)$, but for $n \geqslant 2$ the curve $\dot{\mathrm{X}}'_0(T^n)$ is only a quotient of $\dot{\mathrm{X}}_1(T^n)$, because, as in the case of elliptic curves, we demand not that each point of G_n be rational, only that G_n be permuted by Galois.

For $j \leqslant n$ let G_j be the group $T^{n-j}G_n$ of T^j-torsion points in G_n. Of course $G_1 = kx_1$. For any $x \neq 0$ let P_x be the linearized polynomial

$$P_x(X) = x^{q-1}X - X^q \tag{10}$$

vanishing on kx. Since t_x vanishes on kx we expect it to factor through P_x (see for instance [2, Prop.3]), and indeed we find

$$t_x(X) = Q_x(P_x(X)) \tag{11}$$

where Q_x is the linearized polynomial

$$Q_x(X) = x^{1-q}X + X^q. \tag{12}$$

Let $t'_x(X)$ be the reverse composition $P_x \circ Q_x$, given by

$$t'_x(X) := P_x(Q_x(X)) = X + (x^{q-1} - x^{q-q^2})X^q - X^{q^2}. \tag{13}$$

Note that t'_x again gives a normalized Drinfeld module of rank 2, namely the module T-isogenous[4] to ϕ obtained as the quotient of ϕ by G_1. Now suppose y_2 is a generator of G_2 such that $t_{x_1}(y_2) = x_1$. There are q such y_2, all differing by multiples of x_1, so $x_2 := P_{x_1}(y_2)$ does not depend on the choice of t_2; conversely x_2 determines G_2. Since $t_{x_1} = Q_{x_1} \circ P_{x_1}$, the condition $t_{x_1}(y_2) = x_1$ is equivalent to $Q_{x_1}(x_2) = x_1$. Recalling the definition (12) and multiplying by x_1^q we find

$$x_2 = x_1^{-1} z_2 \quad \text{where} \quad z_2^q + z_2 = x_1^{q+1}. \tag{14}$$

Thus the curve $\dot{\mathrm{X}}'_0(T^2)$ is just $z_2^q + z_2 = x_1^{q+1}$, which is known to be k_1-isomorphic with the Fermat curve of degree $q+1$ (a.k.a. the "Hermitian curve" over k_1). Note that G_2 is the k-vector space of zeros of the linearized polynomial $P_{x_2} \circ P_{x_1}$. Moreover,

$$0 = P_{x_1}(Q_{x_1}(x_2)) = t'_{x_1}(x_2). \tag{15}$$

That is, x_2 is a T-torsion point on our T-isogenous module. It follows that $t'_{x_1} = t_{x_2}$. By induction we can now determine the tower of curves $\dot{\mathrm{X}}'_0(T^n)$ explicitly: the function field of $\dot{\mathrm{X}}'_0(T^n)$ is generated by $x_1, x_2, \ldots, x_{n-1}$ with relations $Q_{x_{j-1}}(x_j) = x_{j-1}$, or equivalently

$$x_j = x_{j-1}^{-1} z_j \quad \text{where} \quad z_j^q + z_j = x_{j-1}^{q+1} \tag{16}$$

$(1 < j < n)$; the point $(x_1, x_2, \ldots, x_{n-1})$ parametrizes the Drinfeld module with $\phi_T = t_{x_1}$, with T^n-torsion subgroup generated by any of the q^{n-1} solutions of

$$(P_{x_{n-1}} \circ P_{x_{n-2}} \circ \cdots \circ P_{x_2} \circ P_{x_1})(y_n) = x_n. \tag{17}$$

This works because by applying

$$Q_{x_j} \circ P_{x_j} = T_{x_j} = P_{x_{j-1}} \circ Q_{x_{j-1}} \tag{18}$$

$(n-2)$ times we find

$$\begin{aligned} x_{n-1} = Q_{x_{n-1}}(x_n) &= (Q_{x_{n-1}} \circ P_{x_{n-1}} \circ P_{x_{n-2}} \circ \cdots \circ P_{x_1})(y_n) \\ &= (P_{x_{n-2}} \circ Q_{x_{n-2}} \circ P_{x_{n-2}} \circ \cdots \circ P_{x_1})(y_n) \\ = \cdots &= (P_{x_{n-2}} \circ \cdots \circ P_{x_2} \circ Q_{x_1} \circ P_{x_1})(y_n) \\ &= (P_{x_{n-2}} \circ \cdots \circ P_{x_2} \circ P_{x_1} \circ T_{x_1})(y_n) \\ &= (P_{x_{n-2}} \circ \cdots \circ P_{x_2} \circ P_{x_1})(T_{x_1}(y_n)), \end{aligned} \tag{19}$$

i.e. $T_{x_1}(y_n)$ satisfies the equation for y_{n-1}. As with G_2 we see that G_n is the k-vector space of zeros of the linearized polynomial

$$P_{x_n} \circ P_{x_{n-1}} \circ \cdots \circ P_{x_2} \circ P_{x_1}. \tag{20}$$

[4] i.e. with an isogeny (here P_x or Q_x) whose kernel is isomorphic with A/TA as an A-module.

In [4] Garcia and Stichtenoth obtained many k_1-rational points on these curves as follows. For each of the q^2-1 points on $\dot{\mathrm{X}}_0'(T)$ with $x_1 \in k_1^*$ we have $x_1^{q+1} \in k_1^*$, so the q solutions z_2 of (14) are just the q elements of k_1 whose trace to k is x_1^{q+1}. Clearly none of these z_2 vanish, so $x_2 = x_1 z_2$ is again in k_1^*. Inductively we see that x_1 lies under q^{n-1} rational points of $\dot{\mathrm{X}}_0'(T^n)$ defined over k_1. Garcia and Stichtenoth use the resulting $(q^2-1)q^{n-1}$ rational points to confirm that the $\dot{\mathrm{X}}_0'(T^n)$ form an asymptotically optimal tower over k_1. From the Drinfeld modular viewpoint we recognize $x_1 \in k_1^*$ as the condition that a point on $\dot{\mathrm{X}}_0'(T^n)$ be supersingular. Thus the $(q^2-1)q^{n-1}$ points of $\dot{\mathrm{X}}_0'(T^n)$ lying above k_1^* are precisely the supersingular points on $\dot{\mathrm{X}}_0'(T^n)$.

The group k_1^* acts on $\dot{\mathrm{X}}_0'(T^n)$ by

$$c(x_1, \dots, x_n) = (cx_1, \bar{c}x_2, cx_3, \bar{c}x_4, \dots, c^{q^{n-1}}x_n) \quad (c \in k_1^*, \bar{c} := c^q). \tag{21}$$

If $c \in k^*$ then the automorphism (21) preserves ϕ (see (8)) and each G_j, but changes the generator x_1 of G_1 to cx_1. Thus we recover $\dot{\mathrm{X}}_0(T^n)$ as the quotient of $\dot{\mathrm{X}}_0'(T^n)$ by the action of k^*. The tower of curves $\dot{\mathrm{X}}_0(T^n)$ was obtained in this way (again without mention or use of Drinfeld modules) in [5]. For arbitrary $c \in k_1^*$, the automorphism (21) multiplies g by the $(q+1)$-st root of unity $c/\bar{c}$. This takes ϕ to a Drinfeld module ϕ_c with the same J-invariant but a different choice of $(-J)^{1/(q+1)}$. The isomorphism c from ϕ to ϕ_c respects our choice of subgroups G_j. Thus the quotient of $\dot{\mathrm{X}}_0(T^n)$ by k_1^*/k^*, or equivalently of $\dot{\mathrm{X}}_0'(T^n)$ by $k)1^*$, is the Drinfeld modular curve $\mathrm{X}_0(T^n)$.

We next obtain an explicit description of $\{\mathrm{X}_0(T^n)\}$ as a recursive tower. As with several of the examples in [3], it will be convenient to start the tower at $n = 2$. [To start at $n = 1$ we would have to use $x_j^{q^2-1}$ as the j-th coordinate, and then all the supersingular points would be on the normalization of the highly singular point $(x_1^{q^2-1}, \dots, x_n^{q^2-1}) = (1, \dots, 1)$ on the resulting curve.] The curve $\mathrm{X}_0(T)$ is the quotient of the x_1-line $\dot{\mathrm{X}}_0'(T)$ by k_1^*, so has genus zero and coordinate $x_1^{q^2-1}$. To obtain $\mathrm{X}_0(T^2)$, raise both sides of the equation (14) for $\dot{\mathrm{X}}_0'(T^2)$ to the power $q-1$ to obtain

$$Z_2(1+Z_2)^{q-1} = x_1^{q^2-1}, \quad \text{where } Z_2 := z_2^{q-1} = (x_1 x_2)^{q-1}. \tag{22}$$

Now Z_2 is invariant under k_1^*, and (22) shows that the Z_2-line is a degree-q cover of the $x_1^{q^2-1}$-line $\mathrm{X}_0(T)$; since the cover $\mathrm{X}_0(T^2)/\mathrm{X}_0(T)$ is also of degree q, we conclude that Z_2 generates the function field of $\mathrm{X}_0(T^2)$.

Thus for $n \geq 2$ the function field of $\mathrm{X}_0(T^n)$ is generated by

$$Z_j := z_j^{q-1} \quad (2 \leq j \leq n). \tag{23}$$

For each $j = 2, \ldots, n-1$, we have $Z_{j+1}(1+Z_{j+1})^{q-1} = x_j^{q^2-1}$ as in (22), which in turn equals

$$(z_j/x_{j-1})^{q^2-1} = Z_j^{q+1}/x_{j-1}^{q^2-1} = Z_j^q/(1+Z_j)^{q-1}. \tag{24}$$

Thus

$$Z_{j+1}(1+Z_{j+1})^{q-1} = Z_j^q/(1+Z_j)^{q-1}. \tag{25}$$

This gives Z_{j+1} as an algebraic function of degree q in Z_j (and vice versa). Thus the relations (25) for $j = 2, \ldots, n-1$ determine the function field of $\mathrm{X}_0(T^n)$. From our description of the supersingular points on $\dot{\mathrm{X}}_0'(T^n)$ we see that the q^{n-1} supersingular points on $\mathrm{X}_0(T^n)$ are the points for which each Z_j is in

$$\begin{aligned} & \{Z \in k_1 : Z^{q+1} = 1, Z \neq -1\} \\ = \; & \{Z \in k_1 : Z(1+Z)^{q-1} = 1\} \qquad (26) \\ = \; & \{Z \in k_1 : Z^q = (1+Z)^{q-1}\}. \end{aligned}$$

(27)

References

[1] Drinfeld, V.G., Vlăduţ, S.G.: The number of points of an algebraic curve. *Functional Anal. Appl.* **17** (1983), #1, 53–54 (translated from the Russian paper in *Funktsional. Anal. i Prilozhen*).

[2] Elkies, N.D.: Linearized algebra and finite groups of Lie type, I: Linear and symplectic groups. Pages 77–108 in *Applications of Curves over Finite Fields* (1997 AMS-IMS-SIAM Joint Summer Research Conference, July 1997, Washington, Seattle; M.Fried, ed.; Providence: AMS, 1999) = *Contemp. Math.* **245**.

[3] Elkies, N.D.: Explicit modular towers. Pages 23–32 in *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing* (1997, T. Basar, A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign 1998.

[4] Garcia, A., Stichtenoth, H.: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Invent. Math.* **121** (1995), #1, 211–233.

[5] Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory* **61** (1996), #2, 248–273.

[6] Garcia, A., Stichtenoth, H.: Asymptotically good towers of function fields over finite fields. *C. R. Acad. Sci. Paris I* **322** (1996), #11, 1067–1070.

[7] Garcia, A., Stichtenoth, H., Thomas, Michael: On towers and composita of towers of function fields over finite fields. *Finite Fields and their Appl.* **3** (1997), #3, 257–274.

[8] Gekeler, E.-U.: *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern.* Bonner Math. Schriften 119, 1980.

[9] Gekeler, E.-U.: *Drinfeld Modular Curves.* Berlin: Springer, 1980 (Lecture Notes in Math. 1231).

[10] Gekeler, E.-U.: Über Drinfeld'sche Modulkurven vom Hecke-Typ. *Compositio Math.* **57** (1986), #2, 219–236.

[11] Gekeler, E.-U., Nonnengardt, U.: Fundamental domains of some arithmetic groups over function fields. *International J. Math.* **6** (1995), #5, 689–708.

[12] Goppa, V.D.: Codes on algebraic curves. *Soviet Math. Dokl.* **24** (1981), #1, 170–172.

[13] Goss, D.: π-adic Eisenstein series for function fields. *Compositio Math.* **41** (1980), #1, 3–38.

[14] Hamahata, Y.: Tensor products of Drinfeld modules and v-adic representations. *Manusc. Math.* **79** (1993), #3–4, 307–327.

[15] Ihara, Y.: Congruence relations and Shimura curves. Pages 291–311 of *Automorphic Forms, Representations, and L-functions* (A. Borel and W. Casselman, eds.; Providence: AMS, 1979; Part 2 of Vol.33 of Proceedings of Symposia in Pure Mathematics).

[16] Ihara, Y.: Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo* **28** (1981), #3, 721–724.

[17] Tsfasman, M.A., Vlăduţ, S.G.: *Algebraic-Geometric Codes.* Dordrecht: Kluwer, 1991.

[18] Tsfasman, M.A., Vlăduţ, S.G., Zink, T.: Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound. *Math. Nachr.* **109** (1982), 21–28.

Department of Mathematics,
Harvard University,
Cambridge, MA 02138 USA

E-mail address: elkies@math.harvard.edu