FAMILIES OF ALGEBRAIC VARIETIES AND TOWERS OF ALGEBRAIC CURVES OVER FINITE FIELDS

SERGEY RYBAKOV

Abstract. We introduce a new construction of towers of algebraic curves over finite fields and provide a simple example of an optimal tower.

1. Introduction

In this paper we use the following notation. Let $k$ be a field of positive characteristic $p$. Fix an algebraic closure $\bar{k}$ of $k$, and denote by $Y$ the base change $Y \times_{\text{Spec } k} \text{Spec } \bar{k}$ of an algebraic variety $Y$ over $k$. We also fix a prime number $\ell \neq p$.

A tower of algebraic curves over $k$ is an infinite sequence
$$\ldots C_n \to C_{n-1} \to \ldots \to C_0$$
of smooth, projective, and geometrically connected curves and finite morphisms. We assume that the genus $g(C_n)$ is unbounded. If $k = \mathbb{F}_q$ is a finite field, the number of points $|C_n(k)|$ on the curve $C_n$ is defined, and the limit
$$\beta(C) = \lim_{n \to \infty} \frac{|C_n(k)|}{g(C_n)}$$exists. Moreover, by the Drinfeld-Vlăduţ theorem [TsVN07, 3.2.1], $\beta(C) \leq \sqrt{q} - 1$. The tower is called optimal, if $\beta(C) = \sqrt{q} - 1$. It is known that if $q$ is a square, examples of optimal towers over $\mathbb{F}_q$ can be constructed as modular towers (see [TsVZ82], and [I81]), but in other cases all known towers are far from being optimal.

In this paper we introduce a new construction of towers of algebraic curves over finite fields. We begin with a smooth family $f : X \to C$ of algebraic varieties over a projective curve $C$. Assume that $f$ is smooth over an open subset $U \subset C$. The $i$-th derived étale direct image of the constant sheaf $\mathbb{Z}/\ell^n\mathbb{Z}$ corresponds to a local system $V_n$ on $U$. There is a fiberwise projectivisation $P_n(V_n)$ of this local system (see section 2), which is an étale scheme $U_n$ over $U$. Clearly, $U_n$ is a regular scheme of dimension one, and there exists a regular compactification $C_n$ of $U_n$. If $a \in C(\bar{k})$ is a closed point such that the fiber $X_a$ of $X$ over $a$ is smooth, then the set of $\bar{k}$-points on the fiber of $C_n$ over $a$ is canonically isomorphic to the quotient
$$H^i_{\text{ét}}(X_a, \mathbb{Z}/\ell^n\mathbb{Z})/(\mathbb{Z}/\ell^n\mathbb{Z})^*$$by the multiplicative group of the ring $\mathbb{Z}/\ell^n\mathbb{Z}$. In particular, this isomorphism respects Frobenius action if $a \in C(k)$. We prove that under some strong technical conditions on the family $X$ the scheme $C_n$ is a geometrically irreducible algebraic curve. As an example, we construct the Legendre tower starting from the Legendre family of elliptic curves over $\mathbb{F}_{p^2}$, and prove that it is an optimal tower.

1991 Mathematics Subject Classification. 14D05, 14D10, 14G15.

Key words and phrases. optimal tower, finite field.

The research was carried out at the IITP RAS at the expense of the Russian Foundation for Sciences (project N 14-50-00150).
Our construction is related to modular towers as follows. Recall that points on the curve $X_0(ℓ^n)$ correspond to isomorphism classes of elliptic curves $E$ with a cyclic subgroup in $E(\bar{k})$ of order $ℓ^n$. In fact, this curve is defined over $\mathbb{F}_{p^2}$ (and even over $\mathbb{F}_p$), and the family $X_0(ℓ^n)$ is an optimal tower over $\mathbb{F}_{p^2}$. An elliptic curve $E$ over $\bar{k}$ defines a point on $X_0(1)$, and the fiber of $X_0(ℓ^n)$ over this point is isomorphic to the projectivisation $P_n(E)[ℓ^n](\bar{k})$ of the $ℓ^n$–torsion. Let $\mathcal{E} \to \mathbb{P}^1$ be a family of elliptic curves such that its $j$–invariant is a map of degree 1. We expect that for an appropriate family $\mathcal{E}$ our construction gives the modular tower $X_0(ℓ^\bullet)$, and the Legendre tower is a base change of $X_0(ℓ^\bullet)$.

One of the conditions on the family is connected with supersingularuty of the smooth fibers. We say that a smooth variety $Y$ over $k$ is strongly supersingular in degree $i$ if the Frobenius action on $H^i_{\text{ét}}(\overline{Y}, \mathbb{Z}_ℓ)$ is the multiplication by $q^{i/2}$ or $-q^{i/2}$. Clearly, if $Y$ is strongly supersingular, then it is supersingular in the usual sense. Moreover, we show that if the fiber $X_a$ over $a \in C(k)$ is strongly supersingular, then the fiber of $C_n$ over $a$ is split for all $n$.

We hope that our construction will help to find towers with good asymptotic properties over $\mathbb{F}_p$. Note that the eigenvalue $±p^{i/2}$ of the Frobenius action on $H^i_{\text{ét}}(\overline{Y}, \mathbb{Z}_ℓ)$ is integral only if $i$ is even. In particular, if $Y$ is strongly supersingular in degree $i$ over $\mathbb{F}_p$, then $i$ is even. This observation force us to study families of algebraic varieties of dimension at least two.

We discuss here the case $i = 2$, and $\dim X = 3$, i.e., $f : X \to \mathbb{C}$ is a family of algebraic surfaces. One of the most important restrictions on the family comes from the monodromy representation. Namely, the monodromy group has to be infinite. It follows that families of rational surfaces do not lead to interesting towers, because the image of the fundamental group in the automorphism group of the Neron–Severi group of a surface is finite. On the other hand, the example of Legendre family shows that towers assigned to families of abelian varieties are closely related to known modular towers, and these towers are non-optimal over $\mathbb{F}_p$. Therefore it is natural to consider algebraic surfaces that are far from being rational or abelian. This will be the object of our future research.

2. The construction

2.1. Fix a prime number $ℓ \neq p$, and denote the ring $\mathbb{Z}/ℓ^n\mathbb{Z}$ by $Λ_n$. Let $V$ be a finitely generated $Λ_n$–module. The set

$$V^* = \{v \in V|ℓ^{n-1}v \neq 0\}$$

has the natural action of the group of invertible elements $Λ_n^\times$. We say that the set

$$P_n(V) = V^*/Λ_n^\times$$

is the projectivisation of $V$. For example, $P_1$ is the usual projectivisation of an $\mathbb{F}_ℓ$–vector space. Recall that the cardinality of the set $P_1(Λ_1^b)$ is equal to

$$c_ℓ(b) = \frac{ℓ^b - 1}{ℓ - 1}.$$ 

Lemma. Suppose that $V_n$ is a $Λ_n$–module, and $V_{n-1}$ is a $Λ_{n-1}$–module. The group $V_{n-1}$ is a $Λ_n$–module in an obvious way. Let $ϕ : V_n \to V_{n-1}$ be a homomorphism such that $ℓ \ker ϕ = 0$. Then there is an induced map

$$P(ϕ) : P_n(V_n) \to P_{n-1}(V_{n-1}).$$

Proof. Let $v \in V_n^*$. Since $ℓ \ker ϕ = 0$, we have $ℓ^{n-2}ϕ(v) \neq 0$. This gives a morphism $ϕ^* : V_n^* \to V_{n-1}^*$ which is compatible with the actions of multiplicative groups. □

For example, the natural projection $Λ_n^b \to Λ_{n-1}^b$ induces a morphism

$$P_n(Λ_n^b) \to P_{n-1}(Λ_{n-1}^b)$$

of degree $ℓ^{b-1}$. It follows that the cardinality of $P_n(Λ_n^b)$ is $c_ℓ(b)ℓ^{(b-1)(n-1)}$. 

2.2. Let $U$ be a smooth curve over $k$, and let $\mathcal{V}_n$ be a projective system of locally constant sheaves $\mathcal{V}_n$ of free $\Lambda_n$-modules on the small étale site of $U$. We assume that the rank $b$ of $\mathcal{V}_n$ does not depend on $n$. By [Mil80, V.1.1], $\mathcal{V}_n$ is representable by a finite étale scheme over $U$ with a free action of the group $\Lambda_n^*$. Thus the quotient by this action represents the sheaf $\tilde{U}_n = P_n(\mathcal{V}_n)$.

**Theorem.** The sheaf $\tilde{U}_n = P_n(\mathcal{V}_n)$ is representable by a finite étale scheme $U$ over $U$.

Let $C_0$ be a smooth projectivisation of $U$, and let $C_n$ be a regular projectivisation of $U_n$. Note that every connected component $Y$ of $C_n$ is a smooth algebraic curve over the algebraic closure of $k$ in $k(Y)$.

**Lemma.** The fiber of $C_n$ over $\bar{a} \in U(\bar{k})$ is naturally isomorphic to $P_n((\mathcal{V}_n)_{\bar{a}})$.

**Proof.** By [Mil80, V.1.7(c)], the scheme $U_n$ represents the sheaf $g^*\mathcal{V}_n$, where $g$ is the tautological morphism from the big étale site to the small étale site of $U$. Untwisting the definitions we get the lemma. $\square$

**Corollary.** The degree of $C_1$ over $C_0$ is equal to $c_1(b)$. If $n > 1$, then the natural projection $\mathcal{V}_n \rightarrow \mathcal{V}_{n-1}$ induces a morphism $C_n \rightarrow C_{n-1}$ of degree $t^{b-1}$.

2.3. Let $f : X \rightarrow C$ be a family of algebraic varieties. We assume that $f$ is smooth over $U \subset C$, and denote by $f_U : X_U \rightarrow U$ the corresponding smooth family. By [Mil80 VI.4.2], we have a locally constant finite sheaf of $\Lambda_n$-modules on $U$:

$$\mathcal{V}_n = R^\ell f_U^*(\Lambda_n),$$

where the direct image is taken with respect to the small étale site of $U$.

A point $\bar{a} \in U(\bar{k})$ corresponds to a morphism $\text{Spec } \bar{k} \rightarrow U$. By [Mil80 VI.2.5], the stalk $(\mathcal{V}_n)_{\bar{a}}$ of $\mathcal{V}_n$ is isomorphic to $H^\ell_\text{et}(X_{\bar{a}}, \Lambda_n)$. In what follows we assume that the module $H^\ell_\text{et}(X_{\bar{a}}, \mathbb{Z}_\ell)$ if free, and denote by $b$ the corresponding Betti number.

By Section 2.2, we construct a tower of schemes $C_n$ starting from $\mathcal{V}_n$. We are going to discuss under what conditions on the family $f$ the tower $C_n$ is a tower of (geometrically connected) algebraic curves.

2.4. **The fundamental group of $U$.** Recall some basic properties of the fundamental group of a $k$-scheme $Z$ [Mil80 I.5]. Let $K$ be a separably closed field. Suppose that there is a morphism $\bar{a} : \text{Spec } K \rightarrow Z$. The fundamental group $\pi_1(Z, \bar{a})$ is the automorphism group of the functor from finite étale $Z$-schemes to sets

$$T \mapsto \text{Hom}_Z(\text{Spec } K, T).$$

This is a profinite group, and for any other point $\bar{a}'$ there exists an isomorphism of profinite groups $i_{\bar{a}\bar{a}'} : \pi_1(Z, \bar{a}) \rightarrow \pi_1(Z, \bar{a}')$. This isomorphism is unique up to inner automorphism of $\pi_1(Z, \bar{a})$.

**Example 2.4.1.** By [Mil80 I.5.2(a)], if $Z = \text{Spec } L$ is the spectrum of a field, then it has only one point $x$, and $\pi_1(Z, \bar{x})$ is the Galois group $\text{Gal}(L)$ of a separable closure $L^{\text{sep}}$ of $L$. The functors $L' \mapsto \text{Hom}_L(L', L^{\text{sep}})$ and

$$S \mapsto \left( \prod_{s \in S} L^{\text{sep}} \right)^{\text{Gal}(L)}$$

establish an equivalence between the category of étale extensions of $\text{Spec } L$ and the category of finite $\text{Gal}(L)$-sets. Moreover, finite extensions of $L$ correspond to transitive actions of $\text{Gal}(L)$ on finite sets.
Any morphism of $k$-schemes $\varphi : Z \to Y$ induces a homomorphism of fundamental groups

$$\pi_1(Z, \bar{a}) \to \pi_1(Y, \varphi(\bar{a})).$$

For example, let $a$ be a closed point on $U$; in other words we have a morphism $a : \text{Spec } k(a) \to U$. Choose an embedding $k(a) \to k(a)_{\mathrm{sep}}$ to a separable closure of $k(a)$. This embedding defines a morphism $\bar{a} : \text{Spec } k(a)_{\mathrm{sep}} \to U$. It follows that there is a homomorphism $\pi_1(U, \bar{a}) \to \text{Gal}(k)$. If $k$ is a finite field, then $\text{Gal}(k) \cong \hat{\mathbb{Z}}$ is topologically generated by Frobenius. In this case we have an exact sequence of profinite groups

$$1 \to G^{\mathrm{geom}} \to \pi_1(U, \bar{a}) \to \hat{\mathbb{Z}} \to 1,$$

where $G^{\mathrm{geom}} = \pi_1(U, \bar{a})$ is the geometric part of the fundamental group.

Let $\eta = \text{Spec } k(C)$ be the generic point of $C$. Then there is a surjective homomorphism $\text{Gal}(k(U)) \to \pi_1(U, \bar{\eta})$ [Mil80, 1.5.2(b)].

**Lemma.** If the action of $\pi_1(U, \bar{a})$ is transitive on $P_n((\mathcal{V}_n)_{\bar{a}})$, then $C_n$ is a connected scheme.

**Proof.** The group $\pi_1(U, \bar{a})$ is isomorphic to the quotient of the Galois group $\text{Gal}(k(U))$. By 2.4.1 finite field extensions of $k(U)$ correspond to transitive actions of $\text{Gal}(k(U))$ on finite sets. Since the action on $P_n((\mathcal{V}_n)_{\bar{a}})$ is transitive, the generic point of $C_n$ is the spectrum of a field; thus $C_n$ is connected.

**Corollary.** We use notation of the section 2.3. If the natural action of $\pi_1(U, \bar{a})$ is transitive on $P_n(H^i_{\text{ét}}(\bar{X}_a, \Lambda_n))$, then $C_n$ is a connected scheme.

### 2.5. The Frobenius action

Assume that $k$ is finite. Let $a \in U(k)$. The fiber $(\mathcal{V}_n)_{\bar{a}}$ is representable by an abelian object of the small étale site of $\text{Spec } k$. By Example 2.4.1 this is an abelian group endowed with a continuous action of $\text{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$. This group is topologically generated by the Frobenius automorphism $F$, thus $(\mathcal{V}_n)_{\bar{a}}$ is simply a finite abelian group plus an action of Frobenius. The following assumption plays a crucial role in this paper:

$(F_a, n)$ The Frobenius action on $(\mathcal{V}_n)_{\bar{a}}$ is the multiplication by a constant.

In our main example from Section 2.3 we have $\mathcal{V}_n = R^i_{\text{ét}f_U^*}(\Lambda_n)$, and $(\mathcal{V}_n)_{\bar{a}} \cong H^i_{\text{ét}}(\bar{X}_a, \Lambda_n)$. By the Weil conjectures proved by Deligne, $(F_a, n)$ for all $n$ is equivalent to the strong supersingularity of $X_a$ in degree $i$.

**Lemma.** Assume that there exists a point $a \in U(k)$ such that the condition $(F_a, n)$ is satisfied.

1. The fiber of the morphism $C_n \to C_0$ over $a$ is split.
2. The scheme $C_n$ is a smooth curve over $k$.
3. If $C_n$ is connected, then $C_n$ is a geometrically irreducible curve over $k$.

**Proof.** By Lemma 2.2 the fiber is isomorphic to $P_n((\mathcal{V}_n)_{\bar{a}})$ as sets with Frobenius action. The condition $(F_a, n)$ means that for any point $x \in C_n(k)$ of the fiber we have $F(x) = x$, where $F$ denotes Frobenius action. Thus $x \in C_n(k)$ is a closed point, and the fiber is split. Moreover, the algebraic closure of $k$ in $k(C_n)$ is equal to $\bar{k}$; in other words, $C_n$ is a $k$–variety. This proves part (2). If $C_n$ is a connected $k$–scheme, then $k(C_n)$ is a field such that $\bar{k} \cap k(C_n) = k$ as subfields of an algebraic closure of $k(C_n)$. We see that the composit of $\bar{k}$ and $k(C_n)$ is isomorphic to $\bar{k}(C_n)$, i.e., $k(C_n)$ is a field, and $C_n$ is geometrically irreducible.

**Corollary.** We use notation of the section 2.3. Assume that $C_n$ is connected, and there exists $a \in U(k)$ such that $X_a$ is strongly supersingular in degree $i$. Then $C_n$ is a smooth, geometrically irreducible curve over $k$, and the fiber of the morphism $C_n \to C_0$ over $a$ is split.
2.6. The monodromy representation. Let $a \in \overline{U}(k)$ be a closed point. The action of $G_{\mathrm{geom}}$ on $(\mathcal{V}_n)_a$ induces homomorphisms

$$
\rho_n : G_{\mathrm{geom}} \to \GL_b(\mathbb{Z}/\ell^n\mathbb{Z}),
\rho : G_{\mathrm{geom}} \to \GL_b(\mathbb{Z}_\ell).
$$

By definition, the induced action on $P_n((\mathcal{V}_n)_a)$ is isomorphic to the action on the fiber of the morphism $\overline{\mathcal{C}}_n \to \overline{\mathcal{C}}_0$ over $a$.

We can describe the fundamental group locally. Let $A = \overline{k}[[t]]$ be the ring of formal power series, and let $K = \overline{k}((t))$ be its fraction field. The scheme $\Spec A$ has the only closed point $\alpha$, and the generic point $\eta : \Spec K \to \Spec A$ given by the inclusion $A \to K$. The fundamental group $G_\eta = \pi_1(\Spec K, \eta)$ is isomorphic to $\Gal(K^{\mathrm{sep}}/K)$. Thus there is an exact sequence:

$$
1 \to G_\eta^{\mathrm{wild}} \to G_\eta \to G_\eta^{\mathrm{tame}} \to 1,
$$

where $G_\eta^{\mathrm{wild}}$ is a $p$-group, and

$$
G_\eta^{\mathrm{tame}} \cong \prod_{\ell \neq p} \mathbb{Z}_\ell
$$

is the Galois group of the extension of $K$ generated by $\sqrt[n]{\ell}$ for all $n$ coprime to $p$. The group $G_\eta^{\mathrm{tame}}$ has a topological generator $\xi$ such that the action on $\sqrt[n]{\ell}$ is the multiplication by a primitive $n$-th root of unity.

For any point $y \in C(\overline{k})$ there is a morphism $\varphi_y : \Spec A \to C$ such that $\varphi_y(\alpha) = y$, and there is a commutative diagram

$$
\begin{array}{ccc}
\Spec K & \xrightarrow{\varphi_y} & U \\
\downarrow \eta & & \downarrow \\
\Spec A & \xrightarrow{\varphi_y} & C
\end{array}
$$

Let $\rho_y : G_\eta \to \GL_b(\mathbb{Z}_\ell)$ be the composition of $\rho$ with the induced homomorphism $G_\eta \to G$. The representation $\rho$ is called unramified in $y$ if $\varphi_y(G_\eta) = 1$, and $\rho$ is called tame in $y$ if $\rho_y(G_\eta^{\mathrm{wild}}) = 1$. In the tame case $\rho_y$ is uniquely determined by $M = \rho_y(\xi)$. We say that $M$ is the monodromy operator. We denote by $G_\eta(y)$ the image of $G_\eta$ in $G$.

Lemma. If $y \in U(\overline{k})$, then $\rho$ is unramified in $y$.

Proof. The morphism $\varphi_y$ factors through $\Spec A$; thus $\rho_y$ factors through $\pi_1(\Spec A, \alpha)$. By [Mil80 I.5.2(b)], the last group is trivial.

2.7. Let $y \in C(\overline{k})$ be a point such that the fiber $X_y$ is not smooth. Assume that $\rho$ is tame in $y$. Fix a point $\bar{a} \in U(\overline{k})$. We are going to compute ramification of $\overline{\mathcal{C}}_n$ over $y$ in terms of the monodromy operator $M$.

Proposition. There is a bijection between orbits of the action of $G_y$ on $P_n((\mathcal{V}_n)_a)$ and points $x \in C_n(\overline{k})$ over $y$. The ramification index of $x$ is equal to the cardinality of the corresponding orbit.

Proof. An orbit $S$ of the action of $G_y$ on $P_n((\mathcal{V}_n)_a)$ corresponds to a finite extension $K_S$ of $K$. Moreover, since the representation is tame, $K_S \cong K[\sqrt{r}]$, where $r = |S|$. Let $A_S$ be the normalization of $A$ in $K_S$. Then there is a morphism $\varphi_S : \Spec A_S \to C_n$ such that the diagram

$$
\begin{array}{ccc}
\Spec A_S & \xrightarrow{\varphi_S} & C_n \\
\downarrow & & \downarrow \\
\Spec A & \xrightarrow{\varphi_a} & C_0
\end{array}
$$
is commutative. It follows that the unique point $\alpha_S \in \text{Spec } A_S$ over $\alpha \in \text{Spec } A$ goes to a point $x$ of $C_n$ over $y$ with ramification index $r$. \hfill \square

3. Families of elliptic curves

3.1. In this section we assume that $k = \mathbb{F}_q$ is a finite field of odd characteristic $p$. Let $E$ be an elliptic curve over $k$. Denote by $E_m$ the kernel of the multiplication by $\ell^m$ in $E(\bar{k})$. The $\ell$-th Tate module of $A$ is defined by the formula:

$$T_\ell(E) = \lim_{\leftarrow} E_m.$$  

The module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2. The Frobenius endomorphism $F$ of $E$ acts on the Tate module by a semisimple linear transformation, which we also denote by $F$. The characteristic polynomial $f_E(t) = \det(t - F|T_\ell(E))$ is called the Weil polynomial of $E$. It is a monic polynomial of degree 2 with rational integer coefficients independent of the choice of the prime $\ell$.

The Tate module $T_\ell(E)$ is isomorphic to $\text{Hom}_{\mathbb{Z}_\ell}(H^1_{\text{ét}}(E, \mathbb{Z}_\ell), \mathbb{Z}_\ell)$. Therefore, $E$ is strongly supersingular in degree 1 if and only if $f_E(t) = (t \pm \sqrt{q})^2$.

In particular, $E$ is supersingular, and $q$ is a square.

**Proposition 3.2.** Assume that $q = p^2$, and an elliptic curve $E$ is supersingular. Then the Weil polynomial of $E$ is equal to $f(t) = (t \pm p)^2$ if one of the following conditions is satisfied:

1. $p \equiv -1 \pmod{12}$;
2. $E$ is defined over $\mathbb{F}_p$, and $p \neq 3$;
3. $E[2](k) \cong (\mathbb{Z}/2\mathbb{Z})^2$, in other words, 2-torsion is defined over $k$.

**Proof.** We use the Deuring-Waterhouse classification of Weil polynomials [Wa69, Theorem 4.1]. Statement (1) is easy, and (2) follows from the observation that the Weil polynomial of a supersingular elliptic curve over $\mathbb{F}_p$ is equal to $t^2 + p$. Conditions of (3) imply that the Weil polynomial $f(t)$ is congruent to $t^2 + 1$ modulo 2. Thus either $f(t) = (t \pm p)^2$, or $f(t) = t^2 + p^2$. But in the second case the number of points on the curve $f(1) = 1 + p^2 \equiv 2 \pmod{4}$ is not divisible by 4. \hfill \square

3.3. Example: Legendre family. In this section we prove that for large $\ell$ the Legendre family gives an optimal tower of algebraic curves over $k = \mathbb{F}_{p^2}$, where $p > 3$.

Let $C = \mathbb{P}^1$, and $X \to C$ be the desingularisation of the Legendre family given in affine coordinates by the equation

$$y^2 = x(x - 1)(x - a),$$

where $a$ is a coordinate on $\mathbb{A}^1 \subset \mathbb{P}^1$. This family has three degenerate fibers of Kodaira type $I_2$ (see [Sil94, IV.9]) over 0, 1 and infinity. The monodromy matrix for such degenerations is equal to

$$M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$  

We call the corresponding tower $C_n$ the Legendre tower. The $j$-invariant is not constant for the Legendre family and, by [S68, IV.3.2], for large $\ell$ the natural morphism $\pi_1(U, \tilde{a}) \to \text{Aut}(T_\ell(X_\tilde{a}))$ is surjective. By Corollary 2.4 the schemes $C_n$ are connected.
A smooth fiber over a point \( a \in \mathbb{A}^1(k) \) is supersingular if and only if \( a \) is a root of the Hasse polynomial
\[
H(t) = \sum_{i=1}^{\frac{p-1}{2}} \left( \frac{p-1}{2i} \right)^2 t^i.
\]
It is known that \( H(t) \) is separable, and all roots of \( H(t) \) belong to \( k - \{0, 1\} \). Moreover, \( 2 \)-torsion of a smooth fiber over a point \( a \) is the zero of the group law, and three points with coordinates \( y = 0, \) and \( x \in \{0, 1, a\} \). By Proposition 3.2(3), if \( H(a) = 0 \), this fiber is a strongly supersingular elliptic curve. Since \( H(t) \) is separable, there are exactly \( \frac{p-1}{2} \) such fibers. It follows from Corollary 2.5 that \( C_n \) are geometrically irreducible curves over \( k \). By Lemma 2.3(1), all fibers over roots of \( H \) are split; therefore,
\[
|C_n(k)| \geq \frac{p-1}{2}(\ell + 1)\ell^{n-1}.
\]
If \( \ell \) is large, the monodromy representation is tame for all points \( a \in C_0(\bar{k}) \). We compute the ramification of \( C_n \) over \( C_0 \) using Proposition 2.7.

**Lemma.** Assume \( n \) is even. There are three types of orbits of the action of \( G_a \) on \( P_n((\mathbb{Z}/\ell^n\mathbb{Z})^2) \), where \( a \in \{0,1,\infty\} \):

1. one orbit of length \( \ell^n \);
2. for each \( i \in \{1, \ldots, n/2\} \) there are \( (\ell - 1)\ell^{i-1} \) orbits of length \( \ell^{n-2i} \);
3. \( \ell^{n/2} \) orbits of length one.

**Proof.** Let \( v_0, v_1 \) be a basis of \((\mathbb{Z}/\ell^n\mathbb{Z})^2\) such that \( Mv_0 = v_0 \), and \( Mv_1 = v_1 + 2v_0 \). We denote the class of a vector \( v \in (\mathbb{Z}/\ell^n\mathbb{Z})^2 \) in \( P_n((\mathbb{Z}/\ell^n\mathbb{Z})^2) \) by \([v]\). The orbit of type (1) is formed by classes
\[
[v_1 + \lambda v_0], \quad \text{where} \quad \lambda \in (\mathbb{Z}/\ell^n\mathbb{Z}).
\]
Let \( i \geq 1 \), and let \( \lambda \in (\mathbb{Z}/\ell^{n-i}\mathbb{Z})^* \). Put
\[
v_{\lambda,i} = v_0 + \ell^i\lambda v_1.
\]
We claim that \([v_{\lambda,1}]\) and \([v_{\lambda,2}]\) are in one orbit if and only if \( \lambda_1 \equiv \lambda_2 \mod \ell^i \). If \( n \geq 2i \), we say that an orbit of type (2) is formed by classes of vectors
\[
v_{\lambda,i} + \ell^{2i}\mu v_1,
\]
where \( \mu \in \mathbb{Z}/\ell^{n-2i}\mathbb{Z} \). If \( n < 2i \), then we define an orbit of type (3) as the class of \( v_{\lambda,i} \). Additionally, \([v_0]\) is also of type (3).

To prove the claim choose a natural number \( s \) such that
\[
2\lambda^2 s \equiv -1 \mod \ell^{n-2i}.
\]
It is straightforward to check that
\[
M^s[v_{\lambda,i}] = [v_{\lambda+s,i}].
\]
The lemma is proved. \( \square \)

By the Hurwitz formula
\[
g(C_n) = 1 - \ell^n + \frac{3}{2}(\ell^n - 1) + \frac{3}{2} \sum_{i=0}^{n/2-1} (\ell - 1)\ell^i(\ell^{n-2i-2} - 1) = 1 + \frac{1}{2}(\ell^{n-1}(\ell + 1) - 2\ell^{n/2}).
\]
We finally obtain
\[
\beta(C_*) \geq p - 1.
\]
By the Drinfeld-Vlăduţ bound, the Legendre tower is optimal.
References

[I81] Ihara Y., Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Tokyo vol. 28, 721–724, 1981

[Mil80] Milne J., Etale cohomology. Princeton Mathematical Series 33, Princeton University Press. 1980, 344 pp.

[S68] Serre J.P., Abelian ℓ—adic representations and elliptic curves. Bull. Amer. Math. Soc. Volume 22, Number 1 (1990), 214-218.

[Sil94] Silverman J. H., Advanced topics in the arithmetic of elliptic curves. GTM 151, 1994.

[TsVN07] Tsfasman M., Vlăduţ S., Nogin D., Algebraic geometric codes: basic notions, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI, 2007.

[TsVZ82] Tsfasman M., Vlăduţ S., Zink T. Modular curves, Shimura curves, and Goppa codes, better than Varshamov–Gilbert bound. Math. Nachr., vol. 109, pp. 21–28, 1982.

[Wa69] Waterhouse W., Abelian varieties over finite fields, Ann. scient. Éc. Norm. Sup., 1969, 4 serie 2, 521-560.

Institute for information transmission problems of the Russian Academy of Sciences

E-mail address: rybakov@mccme.ru, rybakov.sergey@gmail.com