On cohomology and zeta functions of generalized Suzuki curves in characteristic two

Takahiro Tsushima

Abstract

We study cohomology of generalized Suzuki curves in characteristic two as representations of their automorphism groups. We calculate the number of rational points and the zeta functions of the curves.

1 Introduction

Let p be a power of 2. Let $t \geq 1$ be a positive integer and $q := p^{2t-1}$. Let S be the smooth affine curve defined by $y^q - y = x^{p^t}(x^q - x)$ in $\mathbb{A}^2_{\mathbb{F}_q} = \operatorname{Spec} \mathbb{F}_q[x, y]$. The smooth compactification $\overline{S}$ of S is called a Suzuki curve if $p = 2$ and $t \geq 2$. In this paper, we call $\overline{S}$ a generalized Suzuki curve in characteristic two. The Suzuki curve has been studied in so many aspects (cf. [BC, Introduction]).

Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. A structure of the automorphism group Q of $\overline{S}_{\mathbb{F}}$ is known. First, Q consists of $\mathbb{F}_q$-automorphisms. The group is isomorphic to the Suzuki group whose order is $q^2(q-1)(q^2+1)$ if $p = 2$. If $p > 2$, the structure of Q is determined in [BC, Theorem 1.3 and Introduction]. The group is a 3-step solvable group of order $q^2(q-1)$.

Let $\ell \neq 2$ be a prime number. We consider the first ℓ-adic étale cohomology group of $\overline{S}_{\mathbb{F}}$ which is denoted by $H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$. Let $G_{\mathbb{F}_q}$ denote the Galois group of the extension $\mathbb{F}/\mathbb{F}_q$. In this paper, we explicitly study $H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ as a $Q \times G_{\mathbb{F}_q}$-representation. Further, we explicitly determine the L-polynomial and the numbers of the rational points of $\overline{S}$. Counting rational points on an algebraic curve over a finite field is an interesting and important problem in number theory and coding theory (cf. [Se3]). In general, it can be so difficult to calculate them exactly. Maximal curves are often used in coding theory. We give a criterion whether $\overline{S}$ is maximal over a finite extension of $\mathbb{F}_q$.

Let $n \geq 1$ be a positive integer. Let $C(\mathbb{F}_{q^n})$ denote the set of the $\mathbb{F}_{q^n}$-rational points on an algebraic curve C over $\mathbb{F}_q$. A projective smooth geometrically connected curve C is said to be $\mathbb{F}_{q^n}$-maximal (resp. $\mathbb{F}_{q^n}$-minimal) if and only if $|C(\mathbb{F}_{q^n})| = q^n + 1 + 2g(C)q^{n/2}$ (resp. $|C(\mathbb{F}_{q^n})| = q^n + 1 - 2g(C)q^{n/2}$), where $g(C)$ denotes the genus of C.

We state two main theorems in this paper. We note $g(\overline{S}) = p^t(q-1)/2$.

Theorem 1.1. We write $p = 2^f$ with an integer $f \geq 1$.

(1) Assume $2 \nmid f$. We have

$$|\overline{S}(\mathbb{F}_{q^n})| = q^n + 1 - \frac{2g(\overline{S})q^{n/2}}{p}\left(\frac{p}{2}\left((-1)^n + 1\right) + \sqrt{\frac{p}{2}}\left((-1)^n - 1\right)\right)\cos\frac{\pi n}{4}.$$

In particular, $\overline{S}$ is $\mathbb{F}_{q^n}$-maximal (resp. $\mathbb{F}_{q^n}$-minimal) if and only if $n \equiv 4 \pmod 8$ (resp. $8 \mid n$).

Keywords: generalized Suzuki curve; number of rational points; zeta function
2020 *Mathematics Subject Classification.* Primary: 14G05, 11M38, 11G20, 14F20; Secondary: 14H37.

(2) Assume $2 \mid f$. We have

$$|\overline{S}(\mathbb{F}_{q^n})| = q^n + 1 - \frac{2g(\overline{S})q^{n/2}}{p}\left(\frac{p}{4}(1+(-1)^n+i^n+(-i)^n) + \frac{\sqrt{p}}{2}((-1)^n-1)\right).$$

In particular, $\overline{S}$ is $\mathbb{F}_{q^n}$-minimal if and only if $4 \mid n$. Moreover, $\overline{S}$ is not $\mathbb{F}_{q^n}$-maximal for any $n \geq 1$.

For a projective smooth geometrically connected curve C over $\mathbb{F}_q$, we define

$$L_{C/\mathbb{F}_q}(T) := \det(1 - \mathrm{Fr}_q^* T; H^1(C_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)),$$

where Fr_q is the Frobenius endomorphism of $C_{\mathbb{F}}$ (cf. Notation). This rational polynomial is called the L-polynomial of C. We show the following theorem.

Theorem 1.2. (1) Assume $2 \nmid f$. We have

$$L_{\overline{S}/\mathbb{F}_q}(T) = \left((1+\sqrt{2q}T+qT^2)^{k_1}(1-\sqrt{2q}T+qT^2)^{k_2}\right)^{p^{t-1}(q-1)},$$

where

$$k_1 = \frac{1}{2}\left(\frac{p}{2}+\sqrt{\frac{p}{2}}\right), \quad k_2 = \frac{1}{2}\left(\frac{p}{2}-\sqrt{\frac{p}{2}}\right).$$

(2) Assume $2 \mid f$. We have

$$L_{\overline{S}/\mathbb{F}_q}(T) = \left((1-\sqrt{q}T)^{l_1}(1+\sqrt{q}T)^{l_2}(1+qT^2)^{l_3}\right)^{p^{t-1}(q-1)},$$

where

$$l_1 = \frac{p}{4} - \frac{\sqrt{p}}{2}, \quad l_2 = \frac{p}{4} + \frac{\sqrt{p}}{2}, \quad l_3 = \frac{p}{4}.$$

If $f = 1$, these theorems are shown in [Ha, Proposition 4.3] and [Se3, 5.4.1]. Our proofs of these theorems restricted to $f = 1$ are different from the ones there.

For $g \in \mathbb{Z}_{>0}$, let $N_q(g)$ denote the maximum number of $\mathbb{F}_q$-rational points on a curve of genus g over $\mathbb{F}_q$. This quantity has been studied in many aspects (cf. [GV2] and [Se3]).

Let $1 \leq i \leq f(2t-1)$ be a positive integer and $g_i := p^t(2^i-1)/2$. Assume that f is odd and $n \equiv 4 \pmod 8$. As an application of Theorem 1.1, we show

$$N_{q^n}(g_i) = q^n + 1 + 2g_i q^{n/2}.$$

We briefly describe the structure of $H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ as a $Q \times G_{\mathbb{F}_q}$-representation. Let $\mathrm{Frob}_q \in G_{\mathbb{F}_q}$ be the geometric Frobenius automorphism defined by $\mathrm{Frob}_q(x) = x^{q^{-1}}$ for $x \in \mathbb{F}$.

For a finite abelian group A, let $A^\vee := \mathrm{Hom}_{\mathbb{Z}}(A, \overline{\mathbb{Q}}_\ell^\times)$. Let $Z = \mathbb{F}_p \times \mathbb{F}_p$ be the abelian group defined by $(b,c)\cdot(b',c') = (b+b', c+c'+bb')$. Let $Z^\vee_{\mathrm{prim}} := \{\psi \in Z^\vee \mid \psi|_{\{0\}\times\mathbb{F}_p} \neq 1\}$. We define an action of $\mathbb{F}_p^\times \ni a$ on $Z^\vee_{\mathrm{prim}} \ni \psi$ by $(a\psi)(b,c) = \psi(ab, a^2c)$ for $(b,c) \in Z$. Let $\mathscr{Z} := Z^\vee_{\mathrm{prim}}/\mathbb{F}_p^\times$. Let ξ_ψ be the character of $G_{\mathbb{F}_q}$ which sends Frob_q to the character sum

$$x_\psi := -p^{t-1}\sum_{b \in \mathbb{F}_p} \psi(b,0),$$

which depends only on the class $[\psi] \in \mathscr{Z}$. We define distinct irreducible Q-representations $\{\rho_\psi\}_{[\psi]\in\mathscr{Z}}$ of dimension $p^{t-1}(q-1)$ (cf. Definition 3.11).

For a representation ρ_i of a group G_i for $i = 1, 2$, let $\rho_1 \boxtimes \rho_2$ denote the tensor product representation of $G_1 \times G_2$.

We give an irreducible decomposition of $H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ as a $Q \times G_{\mathbb{F}_q}$-representation in the following.

Theorem 1.3. (Theorem 3.13) We have an isomorphism

$$H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{[\psi]\in\mathcal{Z}} (\rho_\psi \boxtimes \xi_\psi)$$

as $Q \times G_{\mathbb{F}_q}$-representations.

The exponent $p^{t-1}(q-1)$ in $L_{\overline{S}/\mathbb{F}_q}(T)$ is regarded as the dimension of ρ_ψ.

Our main results in this paper are Theorems 1.1–1.3. First we show Theorem 1.3 in a cohomological and representation-theoretic manner. Using this theorem, we show Theorems 1.1 and 1.2. We describe the strategy roughly. We identify $\overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$. Then we can prove

$$\frac{x_\psi}{\sqrt{q}} \in \begin{cases} \{e^{\pm\frac{\pi i}{4}}, e^{\pm\frac{3\pi i}{4}}\} & \text{if } f \text{ is odd,} \\ \{\pm 1, \pm i\} & \text{if } f \text{ is even.} \end{cases}$$

Computing the values $\sum_{[\psi]\in\mathcal{Z}} x_\psi$ and $\sum_{[\psi]\in\mathcal{Z}} x_\psi^2$, we can determine the set of the Frobenius eigenvalues: $\{x_\psi \mid [\psi] \in \mathcal{Z}\}$ (cf. Lemma 3.18). Theorems 1.1 and 1.2 follow from this.

We study the curve $\overline{S}$ in the case where p is a power of an odd prime number in [T2].

This work was supported by JSPS KAKENHI Grant Numbers 20K03529/21H00973.

Notation

For a scheme X over a field k and a field extension l/k, let X_l denote the base change of X to l.

For a scheme X over $\mathbb{F}_q$, let $F\colon X \to X$ be the q-th power Frobenius endomorphism. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. Let $\mathrm{Fr}_q\colon X_{\mathbb{F}} \to X_{\mathbb{F}}$ denote the base change of F to $\mathbb{F}$. Let $\ell \nmid q$ be a prime number. For a variety X over $\mathbb{F}_q$ and an integer $i \geq 0$, let $H^i_{\mathrm{c}}(X_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ denote the i-th ℓ-adic étale cohomology group of $X_{\mathbb{F}}$ with compact support. For a proper morphism between $\mathbb{F}_q$-varieties $f\colon Y \to X$ and an integer $i \geq 0$, let $f^*\colon H^i_{\mathrm{c}}(X_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \to H^i_{\mathrm{c}}(Y_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ denote the pull-back. We refer to the Grothendieck trace formula (cf. [De, (1.9.1) and Remarque 1.9.4 in Sommes trig.]) as the trace formula.

Let $\overline{C}$ denote the smooth compactification of an algebraic curve C over $\mathbb{F}_q$.

For a vector space V over a field k and a k-endomorphism $f\colon V \to V$, let $\mathrm{Tr}(f; V) \in k$ denote the trace of f.

For a group G, Let $Z(G)$ denote its center.

For a finite field extension $\mathbb{F}_{p^r}/\mathbb{F}_{p^s}$, let $\mathrm{Tr}_{p^r/p^s}\colon \mathbb{F}_{p^r} \to \mathbb{F}_{p^s}$ and $\mathrm{Nr}_{p^r/p^s}\colon \mathbb{F}_{p^r} \to \mathbb{F}_{p^s}$ denote the trace map and the norm map, respectively.

For a representation M of a finite abelian group A and a character $\chi \in A^\vee$, let $M[\chi]$ denote the χ-isotypic part of M.

2 Review on generalized Suzuki curve

In this section, we build notation and collect fundamental facts on S used in the proceeding section. Let D be the affine curve defined by $w^p + w = x^{p^{t-1}+1} + x^{p^t+1}$. We relate the cohomology of S to the one of D (cf. Proposition 2.15). The curve D is regarded as a quotient of S.

2.1 Generalized Suzuki curve and its automorphisms

Definition 2.1. (1) Let $Q = \mathbb{F}_q^\times \times \mathbb{F}_q \times \mathbb{F}_q$ be the group defined by

$$(a, b, c) \cdot (a', b', c') = \left(aa', b + a^{-1}b', c + a^{-(p^t+1)}(c' + abb'^{p^t})\right).$$

(2) Let Q act on S by $(x,y)\cdot(a,b,c) = \left(a(x+b), a^{p^t+1}(y+b^{p^t}x+c)\right)$ for $(x,y)\in S$ and $(a,b,c)\in Q$.

(3) We define $Q_p := \{(a,b,c)\in Q \mid a\in \mathbb{F}_p^\times\}$, which is a normal subgroup of Q.

All automorphisms of $\overline{S}_{\mathbb{F}}$ are $\mathbb{F}_q$-rational. The automorphism group of $\overline{S}_{\mathbb{F}}$ is isomorphic to Q as in [BC, Introduction and Theorem 1.3] if $f>1$. This result is independent of the parity of p. If $p=2$, the group Q is regarded as a Borel subgroup of the Suzuki group.

We simply write (b,c) for $(1,b,c)\in Q$ and write a for $(a,0,0)\in Q$. Then

$$(b,c)a = (a,b,c), \quad a^{-1}(b,c)a = (ab, a^{p^t+1}c) \quad \text{for } a\in\mathbb{F}_q^\times \text{ and } (b,c)\in Q. \tag{2.1}$$

2.2 Quotient of Q_p and certain representations

Definition 2.2. (1) Let

$$R(x) := x^{p^{t-1}} + x^{p^t} \in \mathbb{F}[x], \quad f(x,y) := x^{p^{t-1}}y + \sum_{i=0}^{t-1}(xR(y))^{p^i} \in \mathbb{F}_p[x,y].$$

(2) Let $Q_R := \{(a,b,c)\in \mathbb{F}_p^\times\times\mathbb{F}_q^2 \mid c^p+c=bR(b)\}$ be the group defined by

$$(a,b,c)\cdot(a',b',c') = \left(aa', b+a^{-1}b', c+a^{-2}(c'+f(ab,b'))\right).$$

Let $P_R := \{(1,b,c)\in Q_R\} \lhd Q_R$.

We note that $f(x,y)$ is bilinear form in a natural sense. We write (b,c) and a for $(1,b,c)\in P_R$ and $(a,0,0)\in Q_R$ respectively. Then

$$(b,c)a = (a,b,c), \quad a^{-1}(b,c)a = (ab, a^2c) \quad \text{for } a\in\mathbb{F}_p^\times \text{ and } (b,c)\in P_R. \tag{2.2}$$

We have $|Q_R| = pq(p-1)$.

Lemma 2.3. We have the surjective group homomorphism

$$\phi\colon Q_p\to Q_R;\ (a,b,c)\mapsto \left(a, b, \mathrm{Tr}_{q/p}(c) + \sum_{i=0}^{t-1} b^{p^i(p^{t-1}+1)}\right).$$

Proof. By $b^{p^{2t-1}} = b$ for $b\in\mathbb{F}_q$, one knows that ϕ is well-defined. Surjectivity of ϕ follows from $|\operatorname{Ker}\phi| = p^{2t-2}$. □

2.2.1 Representations of P_R

For elements g,g' of a group G, let $[g,g'] := gg'g^{-1}g'^{-1}$.

Lemma 2.4. (1) For $g=(b,c)$ and $g'=(b',c')\in P_R$, we have $[g,g'] = (0, f(b,b')+f(b',b))$. Moreover, we have $f(b,b')+f(b',b) = \mathrm{Tr}_{q/p}(b'b^{p^t}+bb'^{p^t})$.

(2) We have $Z(P_R) = \{(b,c)\mid b,c\in\mathbb{F}_p\}$, which is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^f$ with $p=2^f$.

(3) We identify $\{(0,c)\mid c\in\mathbb{F}_p\}\xrightarrow{\sim}\mathbb{F}_p;\ (0,c)\mapsto c$. The pairing

$$\omega\colon (P_R/Z(P_R))\times(P_R/Z(P_R))\to\mathbb{F}_p;\ (g,g')\mapsto[g,g']$$

is a non-degenerate symmetric form.

Proof. We have $(b,c)^{-1} = (b, c + f(b,b))$. Then (1) is easily verified.

We show (2). The former claim follows from (1) and $\mathbb{F}_{p^{2t}} \cap \mathbb{F}_q = \mathbb{F}_p$. We take a basis $b_1, \ldots, b_f$ of $\mathbb{F}_p$ over $\mathbb{F}_2$. Then we set $x_i := (b_i, 0) \in Z(P_R)$. By $f(b_i, b_i) = b_i^2$, we have $x_i^2 = (0, b_i^2)$. We can easily check that the homomorphism

$$(\mathbb{Z}/4\mathbb{Z})^f \to Z(P_R);\ (i_1, \ldots, i_f) \mapsto x_1^{i_1} \cdots x_f^{i_f}$$

is surjective. Hence this is injective. Thus we obtain the claim.

We show (3). We identify $P_R/Z(P_R) \xrightarrow{\sim} \mathbb{F}_q/\mathbb{F}_p;\ (b,c) \mapsto \bar{b}$. Then ω is given by $(\bar{b}, \bar{b}') \mapsto \mathrm{Tr}_{q/p}(b' b^{p^t} + b b'^{p^t})$. The claim follows from $\mathbb{F}_{p^{2t}} \cap \mathbb{F}_q = \mathbb{F}_p$. $\square$

The above lemma implies the following.

Lemma 2.5. ([Bu, Exercise 4.1.8: The Stone–Von Neumann Theorem]) Let $\psi \in Z(P_R)^\vee \setminus \{1\}$. There exists a unique irreducible representation τ_ψ of P_R containing ψ restricted to $Z(P_R)$. Moreover, we have an isomorphism $\tau_\psi|_{Z(P_R)} \simeq \psi^{\oplus p^{t-1}}$.

2.3 Quotients of S and first analysis of cohomology

Let $\alpha \in \mathbb{F}_q^\times$ and let C_α be the affine curve defined by $z^p + z = \alpha x^{p^t}(x^q + x)$ over $\mathbb{F}_q$.

Lemma 2.6. We have the isomorphism $C_\alpha \xrightarrow{\sim} C_1;\ (x,z) \mapsto \big(\alpha^{\frac{p^t-1}{p-1}} x, \mathrm{Nr}_{q/p}(\alpha) z\big)$.

Proof. The claim is checked using $\mathrm{Nr}_{q/p}(\alpha)\alpha = \mathrm{Nr}_{q/p}(\alpha)^p \alpha = \alpha^{\frac{p^{2t}-1}{p-1}}$. $\square$

The curve C_α appears as a quotient of S naturally as follows. We have the finite Galois étale morphism

$$\pi_\alpha \colon S \to C_\alpha;\ (x,y) \mapsto \left(x, \sum_{i=0}^{2t-2} (\alpha y)^{p^i}\right),$$

whose Galois group is the kernel of the homomorphism $\mathrm{Tr}_\alpha \colon \mathbb{F}_q \to \mathbb{F}_p;\ y \mapsto \mathrm{Tr}_{q/p}(\alpha y)$.

The cohomology group of S is understood via the ones of $\{C_\alpha\}_{\alpha \in \mathbb{F}_q^\times}$.

Lemma 2.7. Let $\ell \neq 2$ be a prime number. For $\alpha \in \mathbb{F}_q^\times$, let $W_\alpha := \pi_\alpha^*(H_c^1(C_{\alpha,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)) \subset V := H_c^1(S_\mathbb{F}, \overline{\mathbb{Q}}_\ell)$.

(1) The subspace W_α depends only on the class $\alpha\mathbb{F}_p^\times \in \mathbb{F}_q^\times/\mathbb{F}_p^\times$.

(2) We have $V = \sum_{\alpha\mathbb{F}_p^\times \in \mathbb{F}_q^\times/\mathbb{F}_p^\times} W_\alpha$.

Proof. For $\alpha, \alpha' \in \mathbb{F}_q^\times$,

$$\alpha\mathbb{F}_p^\times = \alpha'\mathbb{F}_p^\times \in \mathbb{F}_q^\times/\mathbb{F}_p^\times \Longrightarrow \mathrm{Ker}\,\mathrm{Tr}_\alpha = \mathrm{Ker}\,\mathrm{Tr}_{\alpha'}.$$

If a finite group G acts on a vector space V, let V^G denote its G-fixed part. Since the Galois group of the finite Galois étale morphism π_α is isomorphic to $\mathrm{Ker}\,\mathrm{Tr}_\alpha$, we know $W_\alpha = V^{\mathrm{Ker}\,\mathrm{Tr}_\alpha}$. Thus W_α depends only on the class $\alpha\mathbb{F}_p^\times$.

We show (2). We take $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$. For $\alpha \in \mathbb{F}_q^\times$, we define $\psi_\alpha \in \mathbb{F}_q^\vee \setminus \{1\}$ by $\psi_\alpha(x) = \psi(\mathrm{Tr}_\alpha(x))$ for $x \in \mathbb{F}_q$. Then $V = \bigoplus_{\psi' \in \mathbb{F}_q^\vee \setminus \{1\}} V[\psi'] = \bigoplus_{\alpha \in \mathbb{F}_q^\times} V[\psi_\alpha]$. Thus the claim follows from $V[\psi_\alpha] \subset V^{\mathrm{Ker}\,\mathrm{Tr}_\alpha} = W_\alpha$ and (1). $\square$

Lemma 2.8. (1) We regard $\mathbb{F}_q^\times$ as a subgroup of Q by $a \mapsto (a, 0, 0)$. For $a \in \mathbb{F}_q^\times \subset Q$, we have the commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\ a\ } & S \\ {\scriptstyle \pi_{a^{p^t+1}}}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ C_{a^{p^t+1}} & \xrightarrow[f_a]{\simeq} & C_1, \end{array}$$

where f_a is given by $(x, z) \mapsto (ax, z)$.

(2) Let the notation be as in Lemma 2.7. Then the subgroup $\mathbb{F}_q^\times \subset Q$ permutes the subspaces $\{W_\alpha\}_{\alpha\mathbb{F}_p^\times \in \mathbb{F}_q^\times/\mathbb{F}_p^\times}$ in V transitively.

Proof. The assertion (1) is directly checked. We show (2). For $a \in \mathbb{F}_q^\times$, we have $a^*(W_1) = W_{a^{p^t+1}}$ by (1). Since $\gcd(p^t+1, q-1) = 1$ by $2 \mid p$, the map $\mathbb{F}_q^\times \to \mathbb{F}_q^\times;\ a \mapsto a^{p^t+1}$ is a bijection. Thus the claim follows. □

Definition 2.9. (1) Let D be the affine curve defined by $w^p + w = xR(x)$ over $\mathbb{F}_q$.

(2) Let $Q_R \ni (a, b, c)$ act on $D \ni (x, w)$ by

$$(x, w) \cdot (a, b, c) = \big(a(x + b), a^2(w + c + f(x, b))\big).$$

Curves like D have been studied in [GV] in detail if $p = 2$. Now, we relate C_α to D.

Lemma 2.10. We have the isomorphism $\pi_R \colon C_1 \xrightarrow{\sim} D;\ (x, z) \mapsto \big(x, z + \sum_{i=0}^{t-1} x^{p^i(p^{t-1}+1)}\big)$. Moreover, we have $C_\alpha \xrightarrow{\sim} D$.

Proof. The first claim is directly checked. Then the latter claim follows from Lemma 2.6. □

Lemma 2.11. Let ϕ be as in Lemma 2.3. Let $\pi := \pi_R \circ \pi_1$. For $(a, b, c) \in Q_p$, we have the commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{(a,b,c)} & S \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ D & \xrightarrow{\phi(a,b,c)} & D. \end{array}$$

Proof. The claim is reduced to the equality

$$f(x, b) = \sum_{i=0}^{2t-2} (xb^{p^t})^{p^i} + \sum_{i=0}^{t-1} (x^{p^{t-1}} b + xb^{p^{t-1}})^{p^i} \quad \text{for } b \in \mathbb{F}_q.$$

This equality follows from $\sum_{i=0}^{2t-2} (xb^{p^t})^{p^i} = \sum_{i=0}^{t-1} (xb^{p^t})^{p^i} + \sum_{i=1}^{t-1} (xb^{p^{t-1}})^{p^i}$ by $b^{p^{2t-1}} = b$. □

In the following, all isomorphisms between cohomology groups are supposed to be isomorphisms as $G_{\mathbb{F}_q}$-representations. For a separated scheme X over $\mathbb{F}$, we often write $H_c^i(X)$ for $H_c^i(X, \overline{\mathbb{Q}}_\ell)$ in proofs.

Lemma 2.12. (1) We have $g(\overline{D}) = p^t(p-1)/2$ and

$$H_c^0(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) = 0, \quad H_c^2(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}}_\ell(-1), \quad \dim H_c^1(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) = p^t(p-1).$$

(2) The forgetful map $H_c^1(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \to H^1(\overline{D}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ is an isomorphism.

Proof. The claims are well-known. For example, see [T1, Lemma 3.28]. □

Lemma 2.13. (1) We have $g(\overline{S}) = p^t(q-1)/2$ and

$$H_c^0(S_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) = 0, \quad H_c^2(S_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}}_\ell(-1), \quad \dim H_c^1(S_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) = p^t(q-1).$$

(2) The forgetful map $H_c^1(S_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \to H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ is an isomorphism.

Proof. As in the proof of Lemma 2.7(2), we have $V = \bigoplus_{\alpha \in \mathbb{F}_q^\times} V[\psi_\alpha]$. Then $V[\psi_\alpha] \simeq H_c^1(C_{\alpha,\mathbb{F}})[\psi]$. We will show that the natural map $H_c^1(S_{\mathbb{F}}) \to H^1(S_{\mathbb{F}})$ is an isomorphism. For each $\alpha \in \mathbb{F}_q^\times$, we have the commutative diagram

$$\begin{array}{ccc} H_c^1(S_{\mathbb{F}})[\psi_\alpha] & \xrightarrow{\sim} & H_c^1(C_{\alpha,\mathbb{F}})[\psi] \\ \downarrow \iota & & \downarrow \\ H^1(S_{\mathbb{F}})[\psi_\alpha] & \xrightarrow{\sim} & H^1(C_{\alpha,\mathbb{F}})[\psi]. \end{array}$$

From Lemma 2.10 and Lemma 2.12(2), the right vertical map is an isomorphism. Thus ι is an isomorphism. Hence the claim follows. This implies that $\overline{S} \setminus S$ consists of one point and (2) (cf. [T1, Lemma 3.27]). For each $\alpha \in \mathbb{F}_q^\times$, we have $\dim H_c^1(C_{\alpha,\mathbb{F}})[\psi] = p^t$ by Lemma 2.10 (cf. [T1, Remark 3.29]). Hence (1) follows. □

Remark 2.14. One can directly check that $\overline{S} \setminus S$ consists of one point. Thus Lemma 2.13(2) follows. To deduce $\dim H_c^1(S_{\mathbb{F}}) = 2g(\overline{S}) = p^t(q-1)$, one may apply [GS, Proposition 4.1].

Proposition 2.15. We have an isomorphism

$$H_c^1(S_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \mathrm{Ind}_{Q_p}^{Q} H_c^1(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$$

as Q-representations.

Proof. Let the notation be as in Lemma 2.7. We have $\dim W_\alpha = p^{t-1}(p-1)$ and $\dim V = p^{t-1}(q-1)$ by Lemmas 2.10, 2.12 and 2.13. Thus $V = \bigoplus_{\alpha \mathbb{F}_p^\times \in \mathbb{F}_q^\times/\mathbb{F}_p^\times} W_\alpha$ by Lemma 2.7(2).

Let H be the stabilizer of W_1 in Q. By [Se2, Proposition 19 in Chapter 7] and Lemma 2.8(2), we have $V \simeq \mathrm{Ind}_H^Q W_1$. Hence $[Q : H] = (q-1)/(p-1)$. We identify $\pi^* \colon H_c^1(D_{\mathbb{F}}) \xrightarrow{\sim} W_1$. Lemma 2.11 implies that $Q_p \subset H$. By $[Q : Q_p] = [Q : H]$, we have $Q_p = H$. Hence the claim follows. □

3 Cohomology of S

It suffices to study D to show Theorems 1.1 and 1.2 by Proposition 2.15.

3.1 Cohomology of D

3.1.1 Computing dimension

In the following, we compute the dimension of $H_c^1(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ for $\psi \in Z(P_R)^\vee$.

Let

$$D \to \mathbb{A}_{\mathbb{F}_q}^1;\ (x, w) \mapsto x^p + x, \tag{3.3}$$

which is a finite Galois étale morphism whose Galois group is $Z(P_R)$. In the following, we will study the ramification of this covering at ∞.

Let $F := \mathbb{F}_q((t))$, which is regarded as a local field with t-adic valuation. We regard $\mathbb{A}_{\mathbb{F}_q}^1$ as an open subscheme of $\mathbb{P}_{\mathbb{F}_q}^1$ naturally. We regard the ring of integers $\mathbb{F}_q[[t]]$ of F as the completion of $\mathbb{P}_{\mathbb{F}_q}^1$ at ∞.

We take a separable closure $\overline{F}$ of F. Let $x, w \in \overline{F}$ be elements satisfying $x^p + x = t^{-1}$ and $w^p + w = x^{p^{t-1}+1} + x^{p^t+1}$. We define

$$F \subset E_1 := F(x) \subset E_2 := E_1(w).$$

This extension comes from the pull-back of (3.3) via the natural morphism $\operatorname{Spec} F \to \mathbb{A}^1_{\mathbb{F}_q}$.

For a finite Galois extension L/K of local fields, let $G := \mathrm{Gal}(L/K)$ denote its Galois group. let $\varphi_{L/K}$ denote the inverse of the Herbrand function of L/K and $\{G^i\}_{i \geq -1}$ (resp. $\{G_i\}_{i \geq -1}$) denote the upper (resp. lower) numbering ramification subgroups of G (cf. [Se1, IV§3]).

Lemma 3.1. (1) We have

$$\varphi_{E_1/F}(u) = \begin{cases} u & \text{if } u \leq 1, \\ p^{-1}(u + p - 1) & \text{otherwise,} \end{cases}$$

$$\varphi_{E_2/E_1}(u) = \begin{cases} u & \text{if } u \leq p^t + 1, \\ p^{-1}(u + (p-1)(p^t + 1)) & \text{otherwise,} \end{cases}$$

$$\varphi_{E_2/F}(u) = \begin{cases} u & \text{if } u \leq 1, \\ p^{-1}(u + p - 1) & \text{if } 1 < u \leq p^t + 1, \\ p^{-2}(u + (p-1)(p^t + p + 1)) & \text{otherwise.} \end{cases}$$

(2) We have

$$\mathrm{Gal}(E_2/F)^i = \begin{cases} \mathrm{Gal}(E_2/F) & \text{if } i \leq 1, \\ \mathrm{Gal}(E_2/E_1) & \text{if } 1 < i \leq p^{t-1} + 1, \\ \{1\} & \text{otherwise.} \end{cases}$$

Proof. We show (1). We note that x^{-1} is a uniformizer of E_1. The extension E_2/E_1 is totally ramified. Let $\varpi_{E_2} := w^{-1}x^{p^{t-1}}$, which is a uniformizer of E_2 by $w^p + w = x^{p^{t-1}+1} + x^{p^t+1}$. Let $v_{E_2}(\cdot)$ denote the normalized valuation of E_2. Let $\sigma \in \mathrm{Gal}(E_2/E_1) \setminus \{1\}$. Then $\sigma(w) - w \in \mathbb{F}_p^{\times}$ and $v_{E_2}(\sigma(\varpi_{E_2}) - \varpi_{E_2}) = p^t + 2$ by $v_{E_2}(w^{-1}) = p^t + 1$. This implies that

$$\mathrm{Gal}(E_2/E_1)_i = \begin{cases} \mathrm{Gal}(E_2/E_1) & \text{if } i \leq p^t + 1, \\ \{1\} & \text{otherwise.} \end{cases}$$

Hence we obtain the claim on φ_{E_2/E_1}. The claim on $\varphi_{E_1/F}$ is checked more easily. Thus the last claim follows from $\varphi_{E_2/F} = \varphi_{E_1/F} \circ \varphi_{E_2/E_1}$.

By (1) and [Se1, Proposition 12 in IV§3],

$$\mathrm{Gal}(E_2/F)_i = \begin{cases} \mathrm{Gal}(E_2/F) & \text{if } i \leq 1, \\ \mathrm{Gal}(E_2/E_1) & \text{if } 1 < i \leq p^t + 1, \\ \{1\} & \text{otherwise.} \end{cases}$$

Hence (2) follows from $G^{\varphi_{E_2/F}(i)} = G_i$. □

Definition 3.2. (1) Let $Z^{\vee}_{\mathrm{prim}} := \{\chi \in Z(P_R)^{\vee} \mid \chi|_{\{0\} \times \mathbb{F}_p} \neq 1\}$.

(2) We define an action of $\mathbb{F}_p^{\times}$ on $Z^{\vee}_{\mathrm{prim}}$ by $(a\psi)(b, c) := \psi(ab, a^2c)$ for $a \in \mathbb{F}_p^{\times}$, $(b, c) \in Z(P_R)$ and $\psi \in Z^{\vee}_{\mathrm{prim}}$. Let

$$\mathcal{Z} := Z^{\vee}_{\mathrm{prim}}/\mathbb{F}_p^{\times}.$$

We have $|Z^{\vee}_{\mathrm{prim}}| = p(p-1)$ and $|\mathcal{Z}| = p$.

Lemma 3.3. Let $\psi \in Z^\vee_{\mathrm{prim}}$. We have $[\psi] \neq [\psi^{-1}]$ in $\mathcal{Z}$.

Proof. Assume $[\psi] = [\psi^{-1}]$. There exists $a \in \mathbb{F}_p^\times$ such that $\psi^{-1} = a\psi$. Since p is even, $\psi|_{\mathbb{F}_p}$ is a quadratic character. Hence $\psi(0,c) = \psi^{-1}(0,c) = \psi(0,a^2c)$. This implies that $a = 1$ by $\psi|_{\mathbb{F}_p} \neq 1$. Thus $\psi^2 = 1$. This contradicts to $\psi \in Z^\vee_{\mathrm{prim}}$. □

Proposition 3.4. Let $\psi \in Z^\vee_{\mathrm{prim}}$. Let $\mathscr{L}_\psi$ denote the smooth $\overline{\mathbb{Q}}_\ell$-sheaf on $\mathbb{A}^1_{\mathbb{F}_q}$ defined by φ in (3.3) and ψ in [De, Définition 1.7 in Sommes trig.]. Let τ_ψ be as in Lemma 2.5.

(1) We have $\dim H^1_{\mathrm{c}}(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi] = p^{t-1}$.

(2) We have an isomorphism $H^1_{\mathrm{c}}(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{\psi \in Z^\vee_{\mathrm{prim}}} \tau_\psi$ as P_R-representations.

Proof. We show (1). Let $\mathbb{A}^1 := \mathbb{A}^1_{\mathbb{F}}$. For any integer i, $H^i_{\mathrm{c}}(D_{\mathbb{F}})[\psi] = H^i_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi)$. Let $\mathrm{Sw}(\mathscr{L}_\psi)$ denote the Swan divisor of $\mathscr{L}_\psi$. We have $\deg \mathrm{Sw}(\mathscr{L}_\psi) = p^{t-1} + 1$ by Lemma 3.1(2) and $\psi \in Z^\vee_{\mathrm{prim}}$. We have $\chi_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi) - \chi_{\mathrm{c}}(\mathbb{A}^1, \overline{\mathbb{Q}}_\ell) = -\deg \mathrm{Sw}(\mathscr{L}_\psi)$ by the Grothendieck–Ogg–Shafarevich formula in [De, (3.2.1) in Sommes trig.]. Hence the claim follows from $H^i_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi) = 0$ for $i \neq 1$.

From (1) and Lemma 2.5, it results that $H^1_{\mathrm{c}}(D_{\mathbb{F}})[\psi] \simeq \tau_\psi$ for $\psi \in Z^\vee_{\mathrm{prim}}$. Hence (2) follows from Lemma 2.12(1) and $|Z^\vee_{\mathrm{prim}}| = p(p-1)$. □

3.1.2 Frobenius eigenvalues and proof of Theorem 1.3

For $\psi \in Z^\vee_{\mathrm{prim}}$, we determine the Frobenius eigenvalues on $H^1_{\mathrm{c}}(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]$ and show Theorem 1.3. For an $\mathbb{F}$-endomorphism T of a scheme X over $\mathbb{F}$, let X^T denote the fixed point subscheme of T. If X^T is finite over $\mathbb{F}$, let $|X^T|$ denote the degree of $X^T \to \mathbb{F}$.

Lemma 3.5. Let $(b,c) \in Z(P_R)$. We have

$$\left|D^{\mathrm{Fr}_q \circ (b,c)}\right| = \begin{cases} pq & \text{if } c = b^2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $(x,w) \in D$. Assume $x^q = x + b$. Then we compute

$$\begin{aligned} w^q + w &= \sum_{i=0}^{2t-2} (w^p + w)^{p^i} = \sum_{i=0}^{2t-2} \left(x^{p^i(p^{t-1}+1)} + x^{p^i(p^t+1)} \right) \\ &= \sum_{i=0}^{t-1} x^{p^i(p^{t-1}+1)} + \sum_{i=0}^{t-2} x^{p^{i+t}(p^{t-1}+1)} + \sum_{i=0}^{t-2} x^{p^i(p^t+1)} + \sum_{i=0}^{t-1} x^{p^{i+t-1}(p^t+1)} \\ &= \sum_{i=0}^{t-1} x^{p^i(p^{t-1}+1)} + \sum_{i=0}^{t-2} (x^{p^t}(x+b))^{p^i} + \sum_{i=0}^{t-2} x^{p^i(p^t+1)} + \sum_{i=0}^{t-1} (x^{p^{t-1}}(x+b))^{p^i} = bx^{p^{t-1}}, \end{aligned}$$

where we substitute $w^p + w = x^{p^{t-1}+1} + x^{p^t+1}$ at the second equality and use $x^q = x + b$ at the fourth one. The endomorphism $\mathrm{Fr}_q \circ (b,c)$ of D is given by $(x,w) \mapsto (x^q + b, (w + bx^{p^{t-1}} + c)^q)$. Thus

$$\begin{aligned} D^{\mathrm{Fr}_q \circ (b,c)} &= \left\{ (x,w) \in D \mid x^q = x + b,\ (w + bx^{p^{t-1}} + c)^q = w \right\} \\ &= \left\{ (x,w) \in D \mid x^q = x + b,\ w^q + w = bx^{p^{t-1}} + b^2 + c \right\} \\ &= \{ (x,w) \in D \mid x^q = x + b,\ b^2 + c = 0 \}. \end{aligned}$$

Hence we obtain the claim. □

Lemma 3.6. For $\psi \in Z^\vee_{\mathrm{prim}}$, we have

$$\operatorname{Tr}(\mathrm{Fr}_q^*; H^1_{\mathrm{c}}(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)) = -q(p-1), \quad \operatorname{Tr}(\mathrm{Fr}_q^*; H^1_{\mathrm{c}}(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)[\psi]) = -\frac{q}{p} \sum_{b \in \mathbb{F}_p} \psi(b,0).$$

Proof. The former equality follows from Lemma 3.5 for $(b,c) = (0,0)$ and the trace formula. We show the latter equality. By the trace formula (cf. [DL, the proof of Proposition 3.3]),

$$-\operatorname{Tr}((\mathrm{Fr}_q \circ (b,c))^*; H^1_{\mathrm{c}}(D_{\mathbb{F}})) + q = \left| D^{\mathrm{Fr}_q \circ (b,c)} \right|.$$

We note $(b,c)^{-1} = (b, c+b^2)$. By Lemma 3.5, we obtain

$$\begin{aligned}
\operatorname{Tr}(\mathrm{Fr}_q^*; H^1_{\mathrm{c}}(D_{\mathbb{F}})[\psi]) &= \frac{1}{p^2} \sum_{(b,c) \in Z(P_R)} \psi((b,c)^{-1}) \operatorname{Tr}((\mathrm{Fr}_q \circ (b,c))^*; H^1_{\mathrm{c}}(D_{\mathbb{F}})) \\
&= \frac{1}{p^2} \left(-\sum_{b \in \mathbb{F}_p} \psi(b,0) q(p-1) + \sum_{(b,c) \in \mathbb{F}_p \times \mathbb{F}_p^\times} \psi(b,c) q \right) = -\frac{q}{p} \sum_{b \in \mathbb{F}_p} \psi(b,0).
\end{aligned}$$

□

Definition 3.7. For $\psi \in Z^\vee_{\mathrm{prim}}$, let ξ_ψ be the character of $G_{\mathbb{F}_q}$ which sends Frob_q to the character sum

$$x_\psi := -p^{t-1} \sum_{b \in \mathbb{F}_p} \psi(b,0),$$

which depends only on the class $[\psi] \in \mathcal{Z}$.

Corollary 3.8. For $\psi \in Z^\vee_{\mathrm{prim}}$, let τ_ψ be as in Lemma 2.5.

(1) We have isomorphisms

$$H^1(\overline{D}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \xleftarrow{\sim} H^1_{\mathrm{c}}(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{\psi \in Z^\vee_{\mathrm{prim}}} (\tau_\psi \boxtimes \xi_\psi)$$

as $P_R \times G_{\mathbb{F}_q}$-representations.

(2) The isomorphism class of the induced representation $\operatorname{Ind}_{P_R}^{Q_R} \tau_\psi$ depends only on the class $[\psi] \in \mathcal{Z}$. Furthermore, we have an isomorphism $H^1(\overline{D}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{[\psi] \in \mathcal{Z}} \left((\operatorname{Ind}_{P_R}^{Q_R} \tau_\psi) \boxtimes \xi_\psi \right)$ as $Q_R \times G_{\mathbb{F}_q}$-representations.

Proof. We show (1). The first isomorphism follows from Lemma 2.12(2) and the second one follows from Schur's lemma, Proposition 3.4 and the latter equality in Lemma 3.6.

We show (2). Let $W_\psi := H^1_{\mathrm{c}}(D_{\mathbb{F}})[\psi]$ for $\psi \in Z^\vee_{\mathrm{prim}}$. We have $H^1_{\mathrm{c}}(D_{\mathbb{F}}) = \bigoplus_{\psi \in Z^\vee_{\mathrm{prim}}} W_\psi$ and an isomorphism $W_\psi \simeq \tau_\psi$ as P_R-representations by Lemma 2.5. An automorphism $a \in \mathbb{F}_p^\times \subset Q_R$ sends $W_{a\psi}$ to W_ψ by (2.2), where $a\psi$ is defined in Definition 3.2(2). Hence we obtain the former claim and an isomorphism

$$\bigoplus_{\psi \in Z^\vee_{\mathrm{prim}}} W_\psi \simeq \bigoplus_{[\psi] \in \mathcal{Z}} \operatorname{Ind}_{P_R}^{Q_R} \tau_\psi$$

as Q_R-representations. Thus the latter claim follows from this and (1). □

Corollary 3.9. We have $L_{\overline{D}/\mathbb{F}_q}(T) = \left(\prod_{[\psi] \in \mathcal{Z}} (1 - x_\psi T) \right)^{p^{t-1}(p-1)}$.

Proof. The claim follows from $\dim \tau_\psi = p^{t-1}$, $[Q_R : P_R] = p-1$ and Corollary 3.8(2). □

Corollary 3.10. We have

(1) $\mathrm{Tr}(\mathrm{Fr}_{q^n}^*; H_c^1(D_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)) = p^{t-1}(p-1) \sum_{[\psi]\in\mathcal{Z}} x_\psi^n = \frac{2g(\overline{D})}{p} \sum_{[\psi]\in\mathcal{Z}} x_\psi^n.$

(2) $|\overline{D}(\mathbb{F}_{q^n})| = q^n + 1 - \frac{2g(\overline{D})}{p} \sum_{[\psi]\in\mathcal{Z}} x_\psi^n.$

Proof. The claim (1) follows from Corollary 3.8(2). The claim (2) follows from (1), Lemma 2.12(2) and the trace formula. □

Definition 3.11. Let $\psi \in Z_{\mathrm{prim}}^\vee$. We regard $\mathrm{Ind}_{P_R}^{Q_R} \tau_\psi$ as a Q_p-representation via ϕ in Lemma 2.3 and consider the inflation of it to Q, for which we write ρ_ψ. The isomorphism class of ρ_ψ depends only on $[\psi] \in \mathcal{Z}$ by Corollary 3.8(2).

Lemma 3.12. (1) Let $\psi \in Z_{\mathrm{prim}}^\vee$. The Q_R-representation $\mathrm{Ind}_{P_R}^{Q_R} \tau_\psi$ is irreducible.

(2) The Q-representations $\{\rho_\psi\}_{[\psi]\in\mathcal{Z}}$ are irreducible and distinct.

Proof. We show (1). Let $a \in \mathbb{F}_p^\times \subset Q_R$ and let τ_ψ^a denote the conjugate of τ_ψ by a. Lemma 2.5 implies that

$$\tau_\psi^a \simeq \tau_{a\psi} \tag{3.4}$$

and hence $\tau_\psi \not\simeq \tau_\psi^a$ for $a \in \mathbb{F}_p^\times \setminus \{1\}$. Since the P_R-representation τ_ψ is irreducible, (1) follows from Mackey's irreducibility criterion in [Se2, §7.4].

We show (2). We show the former claim. Let $\widetilde{\tau}_\psi$ denote the inflation of $\mathrm{Ind}_{P_R}^{Q_R} \tau_\psi$ via $\phi\colon Q_p \to Q_R$ in Lemma 2.3. By definition, $\rho_\psi = \mathrm{Ind}_{Q_p}^{Q} \widetilde{\tau}_\psi$. We set $\psi_{\mathbb{F}_p} := \psi|_{\{0\}\times\mathbb{F}_p} \in \mathbb{F}_p^\vee \setminus \{1\}$. For $x \in \mathbb{F}_q$, we define $\psi_x \in \mathbb{F}_q^\vee$ by $\psi_x(y) := \psi_{\mathbb{F}_p}(\mathrm{Tr}_{q/p}(xy))$ for $y \in \mathbb{F}_q$. Let $a \in \mathbb{F}_q^\times \subset Q$. Let $\widetilde{\tau}_\psi^a$ denote the conjugate of $\widetilde{\tau}_\psi$ by a. Recall that $a^{-1}(1,0,c)a = (1,0,a^{p^t+1}c)$ in Q for $c \in \mathbb{F}_q$ by (2.1). We identify the subgroup $\{(1,0,c) \mid c \in \mathbb{F}_q\} \subset Q$ with $\mathbb{F}_q$. By Mackey's formula and Lemma 2.5, we have isomorphisms

$$\widetilde{\tau}_\psi|_{\mathbb{F}_q} \simeq \bigoplus_{x\in\mathbb{F}_p^\times} \psi_x^{\oplus p^{t-1}}, \quad \widetilde{\tau}_\psi^a|_{\mathbb{F}_q} \simeq \bigoplus_{x\in\mathbb{F}_p^\times} \psi_{a^{p^t+1}x}^{\oplus p^{t-1}}. \tag{3.5}$$

Hence $\widetilde{\tau}_\psi \simeq \widetilde{\tau}_\psi^a \iff a \in \mathbb{F}_p^\times$. Similarly as (1), the former claim follows.

Let $a \in \mathbb{F}_p^\times$. By Frobenius reciprocity and (3.4),

$$\mathrm{Hom}_{Q_R}(\mathrm{Ind}_{P_R}^{Q_R} \tau_\psi, \mathrm{Ind}_{P_R}^{Q_R} \tau_{\psi'}^a) = \bigoplus_{x\in\mathbb{F}_p^\times} \mathrm{Hom}_{P_R}(\tau_\psi, \tau_{ax\psi'}) \neq \{0\} \iff [\psi] = [\psi'] \in \mathcal{Z}. \tag{3.6}$$

Let $b \in \mathbb{F}_q^\times$ and $\psi' \in Z_{\mathrm{prim}}^\vee$. We will show that

$$\mathrm{Hom}_{Q_p}(\widetilde{\tau}_\psi, \widetilde{\tau}_{\psi'}^b) \neq \{0\} \iff b \in \mathbb{F}_p^\times,\ [\psi] = [\psi'].$$

Assume that $\mathrm{Hom}_{Q_p}(\widetilde{\tau}_\psi, \widetilde{\tau}_{\psi'}^b) \neq \{0\}$. By (3.5), $\psi_1 = \psi'_{b^{p^t+1}y}$ with some $y \in \mathbb{F}_p^\times$. We take $c \in \mathbb{F}_p^\times$ such that $\psi'_{\mathbb{F}_p}(x) = \psi_{\mathbb{F}_p}(cx)$ for $x \in \mathbb{F}_p$. Hence $1 = b^{p^t+1}yc$. Thus $b \in \mathbb{F}_p^\times$. This and (3.6) imply that $[\psi] = [\psi']$. We can show the converse using (3.4) and (3.6).

From Frobenius reciprocity, it results that

$$\mathrm{Hom}_Q(\rho_\psi, \rho_{\psi'}) \simeq \bigoplus_{b\mathbb{F}_p^\times \in \mathbb{F}_q^\times/\mathbb{F}_p^\times} \mathrm{Hom}_{Q_p}(\widetilde{\tau}_\psi, \widetilde{\tau}_{\psi'}^b) \neq \{0\} \iff [\psi] = [\psi'].$$

Thus the required claim follows. □

Theorem 3.13. We have an irreducible decomposition

$$H^1(\overline{S}_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \xleftarrow{\sim} H^1_{\mathrm{c}}(S_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{[\psi]\in\mathcal{Z}} (\rho_\psi \boxtimes \xi_\psi)$$

as $Q \times G_{\mathbb{F}_q}$-representations.

Proof. The claim follows from Proposition 2.15 and Corollary 3.8(2). □

3.1.3 Explicit determination of L-polynomial of $\overline{D}$

Our aim in the following is to show Theorems 3.19 and 3.20. We write $p = 2^f$ as before.

Lemma 3.14. Assume that $x, y \in \mathbb{Z}$ satisfy $x^2 + y^2 = p$. Then we have

$$\frac{x+iy}{\sqrt{p}} \in \begin{cases} \{e^{\pm\frac{\pi i}{4}}, e^{\pm\frac{3\pi i}{4}}\} & \text{if } f \text{ is odd,} \\ \{\pm 1, \pm i\} & \text{if } f \text{ is even.} \end{cases}$$

Proof. Assume $2 \nmid f$. Then $x \neq 0,\ y \neq 0$. We write $x = 2^r x_1$ and $y = 2^s y_1$ with $r \leq s$, $2 \nmid x_1, y_1$. Then $x_1^2 + 2^{2(s-r)} y_1^2 = 2^{f-2r}$. If $s > r$, $2 \nmid f$ implies that $2 \mid x_1$. Hence $s = r$. This implies that $x_1^2 + y_1^2 = 2^{f-2r}$. By $x_1^2 + y_1^2 \equiv 2 \pmod 4$, we must have $f = 2r + 1$. Thus $x_1^2 = y_1^2 = 1$.

Assume that $2 \mid f$ and $x \neq 0,\ y \neq 0$. We write $x = 2^r x_1$ and $y = 2^s y_1$ with $r \leq s$, $2 \nmid x_1, y_1$. Then $x_1^2 + 2^{2(s-r)} y_1^2 = 2^{f-2r}$. If $s > r$, we have $f = 2r$ by $2 \nmid x_1$. This implies $x_1^2 + 2^{2(s-r)} y_1^2 = 1$. This is a contradiction. Hence $s = r$ and $x_1^2 + y_1^2 = 2^{f-2r}$. This is a contradiction by $2 \mid f$, since $x_1^2 + y_1^2 \equiv 2 \pmod 4$. Hence $x = 0$ or $y = 0$. □

We take an isomorphism $\overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$.

Corollary 3.15. Let $\psi \in Z^\vee_{\mathrm{prim}}$. Then we have

$$\frac{1}{\sqrt{p}} \sum_{b\in\mathbb{F}_p} \psi(b, 0) \in \begin{cases} \{e^{\pm\frac{\pi i}{4}}, e^{\pm\frac{3\pi i}{4}}\} & \text{if } f \text{ is odd,} \\ \{\pm 1, \pm i\} & \text{if } f \text{ is even.} \end{cases}$$

Proof. Lemma 2.4(2) implies that $\sum_{b\in\mathbb{F}_p} \psi(b,0) \in \mathbb{Z}[i]$. By the Weil conjecture for curves, $\left|\sum_{b\in\mathbb{F}_p} \psi(b,0)\right| = \sqrt{p}$. Hence the claim follows from Lemma 3.14. □

Lemma 3.16. We have $\sum_{[\psi]\in\mathcal{Z}} x_\psi = -p^t$ and $\sum_{[\psi]\in\mathcal{Z}} x_\psi^2 = 0$.

Proof. The former equality follows from $H^1_{\mathrm{c}}(D_{\mathbb{F}}) = \bigoplus_{[\psi]\in\mathcal{Z}} H^1_{\mathrm{c}}(D_{\mathbb{F}})[\psi]$ and Lemma 3.6.

We show the latter equality. Let $y_\psi := \sum_{b\in\mathbb{F}_p} \psi(b,0)$ for $\psi \in Z(P_R)^\vee$. Then we compute

$$\sum_{\psi\in Z(P_R)^\vee} y_\psi^2 = \sum_{b,b'\in\mathbb{F}_p} \sum_{\psi\in Z(P_R)^\vee} \psi((b,0)(b',0)) = p^2, \tag{3.7}$$

where we use $(b,0)(b',0) = (0,0) \iff b = b' = 0$ at the second equality. Let $g \colon Z(P_R) \to \mathbb{F}_p;\ (b,c) \mapsto b$. By g, we regard $\mathbb{F}_p^\vee$ as a subgroup of $Z(P_R)^\vee$. Then

$$\sum_{\psi\in\mathbb{F}_p^\vee} y_\psi^2 = \sum_{b,b'\in\mathbb{F}_p} \sum_{\psi\in\mathbb{F}_p^\vee} \psi(b+b') = p^2. \tag{3.8}$$

We obtain $\sum_{\psi\in Z^\vee_{\mathrm{prim}}} y_\psi^2 = 0$ by (3.7), (3.8) and $Z^\vee_{\mathrm{prim}} = Z(P_R)^\vee \backslash \mathbb{F}_p^\vee$. Hence $(p-1)\sum_{[\psi]\in\mathcal{Z}} x_\psi^2 = \sum_{\psi\in Z^\vee_{\mathrm{prim}}} x_\psi^2 = p^{2t-2} \sum_{\psi\in Z^\vee_{\mathrm{prim}}} y_\psi^2 = 0$. □

Definition 3.17. Let $\psi \in Z_{\mathrm{prim}}^{\vee}$. We define

$$k_1 := \left|\{[\psi] \in \mathcal{Z} \mid x_\psi = \sqrt{q}e^{\frac{3\pi i}{4}}\}\right|, \quad k_2 := \left|\{[\psi] \in \mathcal{Z} \mid x_\psi = \sqrt{q}e^{\frac{\pi i}{4}}\}\right|$$

if f is odd and

$$\begin{aligned} l_1 &:= |\{[\psi] \in \mathcal{Z} \mid x_\psi = \sqrt{q}\}|, \quad l_2 := |\{[\psi] \in \mathcal{Z} \mid x_\psi = -\sqrt{q}\}|, \\ l_3 &:= |\{[\psi] \in \mathcal{Z} \mid x_\psi = i\sqrt{q}\}| \end{aligned}$$

if f is even.

Lemma 3.18. We have

$$\begin{cases} k_1 = \frac{1}{2}\left(\frac{p}{2} + \sqrt{\frac{p}{2}}\right), \quad k_2 = \frac{1}{2}\left(\frac{p}{2} - \sqrt{\frac{p}{2}}\right) & \text{if } 2 \nmid f, \\ l_1 = \frac{p}{4} - \frac{\sqrt{p}}{2}, \quad l_2 = \frac{p}{4} + \frac{\sqrt{p}}{2}, \quad l_3 = \frac{p}{4} & \text{if } 2 \mid f. \end{cases}$$

Proof. Assume $2 \nmid f$. We have $k_1 + k_2 = p/2$ by Lemma 3.3 and Corollary 3.15. Lemma 3.16 implies that $-k_1 + k_2 = -\sqrt{p/2}$. Hence the claim follows.

Assume $2 \mid f$. From Lemma 3.3 and Corollary 3.15, it results that $l_1 + l_2 + 2l_3 = p$. From Lemma 3.16, it results that $l_1 - l_2 = -\sqrt{p}$ and $l_1 + l_2 - 2l_3 = 0$. Thus the claim follows. □

Theorem 3.19. (1) Assume $2 \nmid f$. We have

$$|\overline{D}(\mathbb{F}_{q^n})| = q^n + 1 - \frac{2g(\overline{D})q^{n/2}}{p}\left(\frac{p}{2}((-1)^n + 1) + \sqrt{\frac{p}{2}}((-1)^n - 1)\right)\cos\frac{\pi n}{4}.$$

In particular, $\overline{D}$ is $\mathbb{F}_{q^n}$-maximal if and only if $n \equiv 4 \pmod 8$.

(2) Assume $2 \mid f$. We have

$$|\overline{D}(\mathbb{F}_{q^n})| = q^n + 1 - \frac{2g(\overline{D})q^{n/2}}{p}\left(\frac{p}{4}(1 + (-1)^n + i^n + (-i)^n) + \frac{\sqrt{p}}{2}((-1)^n - 1)\right).$$

In particular, $\overline{D}$ is $\mathbb{F}_{q^n}$-minimal if and only if $4 \mid n$.

Proof. We show (1). Assume that f is odd. By Lemma 3.18,

$$\sum_{[\psi]\in\mathcal{Z}} x_\psi^n = q^{n/2}\left(2k_1\cos\frac{3\pi n}{4} + 2k_2\cos\frac{\pi n}{4}\right) = q^{n/2}\left(\frac{p}{2}((-1)^n + 1) + \sqrt{\frac{p}{2}}((-1)^n - 1)\right).$$

The claim follows from Corollary 3.10(2). The claim (2) is shown in the same manner. □

Theorem 3.20. We have

$$L_{\overline{D}/\mathbb{F}_q}(T) = \begin{cases} \left((1 + \sqrt{2q}T + qT^2)^{k_1}(1 - \sqrt{2q}T + qT^2)^{k_2}\right)^{p^{t-1}(p-1)} & \text{if } 2 \nmid f, \\ \left((1 - \sqrt{q}T)^{l_1}(1 + \sqrt{q}T)^{l_2}(1 + qT^2)^{l_3}\right)^{p^{t-1}(p-1)} & \text{if } 2 \mid f. \end{cases}$$

Proof. The assertions follow from Corollary 3.9. □

3.2 Proof of Theorems 1.1 and 1.2

For an integer $n \geq 1$, we have

$$q^n + 1 - |\overline{S}(\mathbb{F}_{q^n})| = \frac{q-1}{p-1}(q^n + 1 - |\overline{D}(\mathbb{F}_{q^n})|), \quad L_{\overline{S}/\mathbb{F}_q}(T) = L_{\overline{D}/\mathbb{F}_q}(T)^{\frac{q-1}{p-1}}$$

by Lemmas 2.12, 2.13 and Proposition 2.15. Hence the theorems follow from $g(\overline{S}) = p^t(q-1)/2$ in Lemma 2.13(1), Theorems 3.19 and 3.20.

3.3 Application

Let $A(T) \in \mathbb{F}_q[T]$ be an additive polynomial all whose roots are contained in $\mathbb{F}_q$. Let C_A be the affine smooth curve over $\mathbb{F}_q$ defined by $A(y) = x^{p^t}(x^q - x)$.

Proposition 3.21. Assume that f is odd and $n \equiv 4 \pmod 8$. The curve $\overline{C}_A$ is $\mathbb{F}_{q^n}$-maximal with genus $p^t(\deg A - 1)/2$.

Proof. By the assumption on $A(T)$, we can write $T^q - T = A(B(T))$ with an additive polynomial $B(T) \in \mathbb{F}_q[T]$. The finite étale morphism $\pi\colon S \to C_A;\ (x, y) \mapsto (x, B(y))$ extends to a non-constant morphism $\overline{\pi}\colon \overline{S} \to \overline{C}_A$. Then $\mathbb{F}_{q^n}$-maximality follows from Theorem 1.1(1) and [Se3, Theorem 5.2.1].

We consider the commutative diagram

$$\begin{array}{ccc} H^1_{\mathrm{c}}(C_{A,\mathbb{F}}) & \xrightarrow{\nu} & H^1(\overline{C}_{A,\mathbb{F}}) \\ \downarrow{\scriptstyle \pi^*} & & \downarrow{\scriptstyle \overline{\pi}^*} \\ H^1_{\mathrm{c}}(S_{\mathbb{F}}) & \xrightarrow{\simeq} & H^1(\overline{S}_{\mathbb{F}}), \end{array}$$

where the bottom horizontal isomorphism follows from Lemma 2.13(2). Since π^* is injective, so is ν. Since ν is surjective, this is bijective. To compute the genus of $\overline{C}_A$, it suffices to show $\dim H^1_{\mathrm{c}}(C_{A,\mathbb{F}}) = p^t(\deg A - 1)$. Let $B\colon \mathbb{F}_q \to \mathbb{F}_q;\ x \mapsto B(x)$ and $\mathbb{F}_B^\vee := \{\psi \in \mathbb{F}_q^\vee \mid \psi(\operatorname{Ker} B) = 1\}$. We have $H^1_{\mathrm{c}}(C_{A,\mathbb{F}}) \xrightarrow{\sim} H^1_{\mathrm{c}}(S_{\mathbb{F}})^{\operatorname{Ker} B} = \bigoplus_{\psi \in \mathbb{F}_B^\vee \setminus \{1\}} H^1_{\mathrm{c}}(S_{\mathbb{F}})[\psi]$. Hence we obtain the claim by $\dim H^1_{\mathrm{c}}(S_{\mathbb{F}})[\psi] = p^t$ in the proof of Lemma 2.13(1). □

Recall that $N_q(g)$ is the maximum number of $\mathbb{F}_q$-rational points on a curve of genus g over $\mathbb{F}_q$. The following result give new entries in [GV2].

Corollary 3.22. Let t be a positive integer, $p = 2^f$ and $q = p^{2t-1}$. Let $1 \leq i \leq f(2t-1)$ be a positive integer and $g_i := p^t(2^i - 1)/2$. Assume that f is odd and $n \equiv 4 \pmod 8$. Then we have

$$N_{q^n}(g_i) = q^n + 1 + 2g_i q^{n/2}.$$

Proof. We take an $\mathbb{F}_2$-vector subspace $V \subset \mathbb{F}_q$ of dimension i and take an additive polynomial $A(T) \in \mathbb{F}_q[T]$ of degree 2^i such that $V = \{x \in \mathbb{F}_q \mid A(x) = 0\}$. Then the claim follows from Proposition 3.21. □

References

[BC] H. Borges and M. Coutinho, On the zeta function and the automorphism group of the generalized Suzuki curve, *Trans. Am. Math. Soc.* 374, No. 3, (2021) 1899–1917.

[Bu] D. Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics. 55, 1997.

[De] P. Deligne, *Cohomologie étale*, Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2. Lect. Notes Math., 569. Berlin: Springer-Verlag, 1977.

[DL] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields *Ann. Math.* (2) 103, (1976) 103–161.

[GS] A. Garcia and H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, *Manuscr. Math.* 72, No. 1, (1991) 67–79.

[GV] G. van der Geer and M. van der Vlugt, Reed-Muller codes and supersingular curves. I, *Compositio Math.* 84, no. 3, (1992) 333–367.

[GV2] G. van der Geer et al., *Tables of curves with many points*, http://www.manypoints.org, 2009.

[Ha] J. P. Hansen, *Deligne-Lusztig varieties and group codes*, Coding theory and algebraic geometry, Proc. Int. Workshop, Luminy/Fr. 1991, Lect. Notes Math. 1518, (1992) 63–81.

[Se1] J. P. Serre, *Corps locaux*, Troisième édition, Hermann, Paris, 1968.

[Se2] J. P. Serre, *Linear representations of finite groups*, GTM 42. Springer-Verlag, 1977.

[Se3] J.-P. Serre, *Rational points on curves over finite fields*, With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler. Edited by Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler and René Schoof. Documents Mathématiques 18. Société Mathématique de France, 2020.

[T1] T. Tsushima, Good reduction of affinoids in the Lubin-Tate curve in even equal characteristic. I, *J. Number Theory* 214, (2020) 414–439.

[T2] T. Tsushima, On cohomology of generalized Suzuki curves and exponential sums, preprint (2023).

Takahiro Tsushima
Department of Mathematics and Informatics, Faculty of Science, Chiba University
1-33 Yayoi-cho, Inage, Chiba, 263-8522, Japan
tsushima@math.s.chiba-u.ac.jp