arXiv:2305.06117v1 [math.AG] 10 May 2023

Gauss sums and Van der Geer–Van der Vlugt curves

Daichi Takeuchi and Takahiro Tsushima

Abstract

我们从分歧理论的角度研究 Van der Geer–Van der Vlugt 曲线。我们给出了这些曲线的 L-多项式的显式公式。由此，我们证明了这些曲线是超奇异的，并给出了这些曲线成为极大曲线或极小曲线的充分条件。

1 Introduction

设 q 为素数 p_0 的一个幂， $\mathbb{F}_q$ 为一个含有 q 个元素的有限域。设 $\mathbb{F}$ 为 $\mathbb{F}_q$ 的一个代数闭包。设 $\mathrm{Fr}_q\colon \mathbb{F} \to \mathbb{F};\ x \mapsto x^{q^{-1}}$ 为几何弗罗贝尼乌斯自同构。设 $\ell \nmid p$ 为一个素数。若光滑射影几何连通曲线 C 在 $\mathbb{F}_q$ 上的 Fr_q 在 $H^1(C_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ 上的所有特征值均为 $q^{1/2}$ 乘以单位根，则称 C 为超奇异曲线。根据泰特定理， C 是超奇异的，当且仅当 C 的雅可比簇在 $\mathbb{F}$ 上与若干条超奇异椭圆曲线的乘积同源。

令 p 为 p_0 的一个幂，并假设 q 是 p的一个幂。令 $R(x) = \sum_{i=0}^{e} a_i x^{p^i} \in \mathbb{F}_q[x]$ 为一个次数为 p^e的加性多项式。令 C_R 为由 $y^p - y = xR(x)$ 在 $\mathbb{A}^2_{\mathbb{F}_q} = \mathrm{Spec}\ \mathbb{F}_q[x, y]$ 中定义的 $\mathbb{F}_q$ 上的仿射曲线。令 $\overline{C}_R$ 表示 C_R的光滑紧化。我们称 $\overline{C}_R$ 为 Van der Geer–Van der Vlugt 曲线。假设。

$$(p_0, e) \neq (2, 0),$$

这保证了 $\overline{C}_R$ 的亏格为正。在 [4], 中，Van der Geer 和 Van der Vlugt 证明了这一族 $\{\overline{C}_R\}_R$ 具有各种有趣的性质。其中，他们证明了当 p 是一个素数时，它们是超奇异的。这是通过构造一种算法来实现的，该算法可以求出 C_R 的显式商。当 p 为偶数时，证明过程较为复杂。当 p 为奇素数时，该定理的详细证明见 [2]。该定理广泛应用于数论和编码理论。

In this paper, by using tools from ℓ-adic cohomology theory, we give another method to describe the L-polynomials of $\overline{C}_R$ which is simple and can be applied regardless of the parity of the characteristic of $\mathbb{F}_q$. We start with observing that C_R admits an action of a certain Heisenberg group. Using this group action, we decompose the cohomology group $H^1(\overline{C}_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ into the direct sum of 1-dimensional representations of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. Then, applying Laumon's product formula for epsilon factors ([5]) to each direct summand, we compute the Frobenius eigenvalues in terms of epsilon factors of characters. It is

关键词：Van der Geer–Van der Vlugt 曲线；超奇异曲线；分歧理论2020 年数学主题分类：主要分类：11G20、11S15、14F20；次要分类：11F85。

classically known that the epsilon factors of characters are calculated by Gauss sums. As a consequence, we can show that $\overline{C}_R$ is supersingular in the case where p is a power of a prime number.

我们更精确地描述结果。设 $E_R(x) := R(x)^{p^e} + \sum_{i=0}^{e}(a_i x)^{p^{e-i}}$ 和

$$H_R := \{(a,b) \in \mathbb{F}^2 \mid E_R(a) = 0,\ b^p - b = aR(a)\}.$$

这个集合自然具有群结构，并作用于曲线 C_R。中心 $Z(H_R)$ 等于 $\{0\} \times \mathbb{F}_p$。设 $A_R \subset H_R$ 为一个极大阿贝尔子群。那么 A_R 包含中心 $\mathbb{F}_p$。对于有限阿贝尔群 A，令 $A^\vee := \mathrm{Hom}(A, \overline{\mathbb{Q}}_\ell^\times)$ 表示其特征群。对于 $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$，令

$$A_\psi^\vee := \{\xi \in A_R^\vee \mid \xi|_{\mathbb{F}_p} = \psi\}.$$

于是 L-多项式

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

具有如下分解。

定理 1.1。假设 $A_R \subset \mathbb{F}_q^2$。对于每个 $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$ 和 $\xi \in A_\psi^\vee$，存在某个数 τ_ξ，它等于 $q^{1/2}$ 乘以一个单位根，使得公式

$$L_{\overline{C}_R/\mathbb{F}_q}(T) = \prod_{\psi \in \mathbb{F}_p^\vee \setminus \{1\}} \prod_{\xi \in A_\psi^\vee} (1 - \tau_\xi T)$$

成立。因此，$\overline{C}_R$ 是超奇异的。

我们将 τ_ξ 视为与 ξ相联系的高斯和。命题 3.1 给出了用局部 ε 因子表示 τ_ξ 的显式公式。在推论 A.9 中，我们给出了另一个不使用 ε 因子的 τ_ξ 显式公式。利用 Grothendieck 迹公式，以及对 C_R 取 H_R的阿贝尔子群之商的机制，我们推导出该公式。

如果一条射影光滑几何连通曲线 C over $\mathbb{F}_q$ 满足 $|C(\mathbb{F}_{q^n})| = q^n + 1 + 2g(C)q^{n/2}$（分别为 $|C(\mathbb{F}_{q^n})| = q^n + 1 - 2g(C)q^{n/2}$），则称其为 $\mathbb{F}_{q^n}$-极大曲线（分别称为 $\mathbb{F}_{q^n}$-极小曲线），其中 $g(C)$ 表示 C 的亏格。换言之，当且仅当 Fr_{q^n} 在 $H^1(C_{\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ 上的作用为标量乘法，其标量为 $-q^{n/2}$（分别为 $q^{n/2}$）时，C 才是 $\mathbb{F}_{q^n}$-极大曲线（分别为 $\mathbb{F}_{q^n}$-极小曲线）。极大曲线在编码理论中具有重要意义。

通过计算高斯和 $\{\tau_\xi\}_\xi$，定理 1.1 得出以下结论。

定理 1.2。假设 $A_R \subset \mathbb{F}_q^2$。

(1) 曲线 $\overline{C}_R$ 是 $\mathbb{F}_{q^{4p_0}}$-极小的。(2) 假设 f 是奇数且 $p_0 \neq 1$ (模 4)。则 $\overline{C}_R$ 是 $\mathbb{F}_{q^{2p_0}}$-极大的。(3) 假设 $p_0 = 2$ 和 $H_R \subset \mathbb{F}_q^2$。则 f 是偶数，且 $\overline{C}_R$ 是 $\mathbb{F}_{q^2}$-极小的。

本研究得到 JSPS KAKENHI GrantNumbers 20K03529/21H00973 以及理化学研究所特别博士后研究员计划的资助。

2 Van der Geer–Van der Vlugt curves

曲线 C_R 具有一个较大的自同构群，其中包含一个海森堡群。我们简要回顾这一事实。设

$$E_R(x) := R(x)^{p^e} + \sum_{i=0}^{e} (a_i x)^{p^{e-i}},$$
$$f_R(x,y) := -\sum_{i=0}^{e-1} \left(\sum_{j=0}^{e-i-1} (a_i x^{p^i} y)^{p^j} + (xR(y))^{p^i} \right) \in \mathbb{F}_q[x,y].$$

We easily check that

$$f_R(x,y)^p - f_R(x,y) = -x^{p^e} E_R(y) + xR(y) + yR(x). \tag{2.1}$$

Let $V_R := \{x \in \mathbb{F} \mid E_R(x) = 0\}$ and $H_R := \{(a,b) \in V_R \times \mathbb{F} \mid b^p - b = aR(a)\}$ be the group whose group law is defined by

$$(a,b) \cdot (a',b') = (a+a', b+b'+f_R(a,a')).$$

We recall some basic properties of H_R.

Lemma 2.1. ([7, Lemma 2.6])

(1) The center $Z(H_R)$ equals $\{0\} \times \mathbb{F}_p$.

(2) The quotient $H_R/Z(H_R)$ is isomorphic to V_R via $(a,b) \mapsto a$.

(3) 映射 $H_R \times H_R \to Z(H_R)$; $(x,y) \mapsto xyx^{-1}y^{-1}$ 诱导出一个非退化辛配对 ω_R: $V_R \times V_R \to \mathbb{F}_p$; $(a,a') \mapsto f_R(a,a') - f_R(a',a)$。

证明。断言（1）和（2）已在 [7, 引理 2.6(1)] 中得到证明。断言（3）则是 [7,引理 2.4] 和 [7, 引理 2.6(2)] 的推论。 □

Lemma 2.2. Let $h \in H_R$. The order of h divides p_0 if p_0 is odd and 4 if $p_0 = 2$.

Proof. We write $h = (a,b)$. Then $h^i = (ia, ib + \binom{i}{2} f_R(a,a))$ for an integer $i \geq 2$. Hence the claim follows. □

The element $H_R \ni (a,b)$ acts on $C_{R,\mathbb{F}} \ni (x,y)$ by

$$(x,y) \cdot (a,b) = (x+a, y + f_R(x,a) + b). \tag{2.2}$$

设 $A_R \subset H_R$ 为一个极大阿贝尔子群：注意，这类子群与 V_R 中关于 ω_R 极大全各向同性的子群一一对应。从现在起，我们始终假设 that

$$(p_0, e) \neq (2,0), \quad A_R \subset \mathbb{F}_q^2. \tag{2.3}$$

存在一个加性多项式 $F_R(x) \in \mathbb{F}_q[x]$，使得 $F_R \mid E_R$，并且 A_R 是 $\{x \in \mathbb{F} \mid F_R(x) = 0\} \subset V_R$ 在 $H_R \to V_R$ 下的逆像。关于 (2.3) 中的后一条件，我们作如下说明。

引理 2.3。假设 $p \neq 2$。条件 $\{x \in \mathbb{F} \mid F_R(x) = 0\} \subset \mathbb{F}_q$ 意味着$A_R \subset \mathbb{F}_q^2$。

证明。设 $a \in \mathbb{F}_q$ 是一个满足 $F_R(a) = 0$的元素。则 $2^{-1}f_R(a,a) \in \mathbb{F}_q$，且 $(2^{-1}f_R(a,a))^p - 2^{-1}f_R(a,a) = aR(a)$。因此，结论得证。 □

In the characteristic two case, the claim in the above lemma does not hold in general (cf. [4, Proposition (3.1)]).

We consider the finite Galois étale morphism

$$\phi\colon C_R \to \mathbb{A}^1_{\mathbb{F}_q};\ (x,y) \mapsto F_R(x),$$

其伽罗瓦群为 A_R。令 $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$ 和 $A_\psi^\vee := \{\xi \in A_R^\vee \mid \xi|_{\mathbb{F}_p} = \psi\}$。对于 $\xi \in A_\psi^\vee$，令 $\mathscr{Q}_\xi$ 表示由 ξ 和 ϕ定义在 $\mathbb{A}^1_{\mathbb{F}_q}$ 上的光滑层。

令 $\mathscr{L}_\psi(s)$ 表示由 $a^p - a = s$ 和 $\psi \in \mathbb{F}_p^\vee$ 定义在 $\mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}\ \mathbb{F}_q[s]$ 上的 Artin–Schreier 层。对于概形态射 $f\colon X \to \mathbb{A}^1_{\mathbb{F}_q}$，令 $\mathscr{L}_\psi(f)$ 表示 $\mathscr{L}_\psi(s)$ 沿 f 的拉回。我们用 $\mathbb{A}^1$ 表示 $\mathbb{F}$ 上的仿射直线。

Lemma 2.4. (1) We have isomorphisms

$$H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{\psi \in \mathbb{F}_p^\vee \setminus \{1\}} H^1_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi(xR(x))),$$

$$H^1_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi(xR(x))) \simeq \bigoplus_{\xi \in A_\psi^\vee} H^1_{\mathrm{c}}(\mathbb{A}^1, \mathscr{Q}_\xi) \quad \text{for } \psi \in \mathbb{F}_p^\vee \setminus \{1\}.$$

Moreover, we have $\dim H^i_{\mathrm{c}}(\mathbb{A}^1, \mathscr{Q}_\xi) = 0$ if $i \neq 1$ and $= 1$ if $i = 1$. We have $\deg \mathrm{Sw}_\infty(\mathscr{Q}_\xi) = 2$.

(2) The canonical map $H^1_{\mathrm{c}}(C_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \to H^1(\overline{C}_{R,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ is an isomorphism.

Proof. We show (1). Let

$$\phi_1\colon C_R \to \mathbb{A}^1_{\mathbb{F}_q};\ (x,y) \mapsto x, \quad \phi_2\colon \mathbb{A}^1_{\mathbb{F}_q} \to \mathbb{A}^1_{\mathbb{F}_q};\ x \mapsto F_R(x).$$

于是 $\phi = \phi_2 \circ \phi_1$。我们有 $\phi_{1*}\overline{\mathbb{Q}}_\ell \simeq \bigoplus_{\psi \in \mathbb{F}_p^\vee} \mathscr{L}_\psi(xR(x))$ 和 $\phi_{2*}\mathscr{L}_\psi(xR(x)) \simeq \bigoplus_{\xi \in A_\psi^\vee} \mathscr{Q}_\xi$。因此，(1) 中的同构关系得证。

根据 Grothendieck–Ogg–Shafarevich 公式，我们很容易验证，对于 $i \neq 1$，$H^i_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi(xR(x))) = 0$，且 $\dim H^1_{\mathrm{c}}(\mathbb{A}^1, \mathscr{L}_\psi(xR(x))) = p^e$。因此，根据 $|A_\psi^\vee| = p^e$，对于 $i \neq 1$，$H^i_{\mathrm{c}}(\mathbb{A}^1, \mathscr{Q}_\xi) = 0$，且 $\dim H^1_{\mathrm{c}}(\mathbb{A}^1, \mathscr{Q}_\xi) = 1$。再次利用 Grothendieck–Ogg–Shafarevich 公式，即可得到最后一个结论。

Since the covering $\phi_1\colon C_R \to \mathbb{A}^1_{\mathbb{F}_q}$ is totally ramified, $\overline{C}_R \setminus C_R$ consists of one point. Hence (2) follows. □

如果多项式 $f(x) \in \mathbb{F}_q[x]$是约化的，则称其为约化多项式，当且仅当 $\mathbb{F}_q[x]/(f(x))$ 是约化的。设$\delta(y) := \sum_{i=0}^d b_i y^{p_0^i} \in \mathbb{F}_q[y] \setminus \{0\}$ 是一个根包含于 $\mathbb{F}_p$中的约化加性多项式。我们可以将其写为 $y^p - y = \delta(\nu(y))$，其中 $\nu(y)$ 是一个加性多项式。令$V_\delta := \{y \in \mathbb{F} \mid \delta(y) = 0\}$。我们有一个满射同态 $\mathbb{F}_p \to V_\delta;\ \ x \mapsto \nu(y)$。这诱导出一个单射 $V_\delta^\vee \hookrightarrow \mathbb{F}_p^\vee$。令 C_δ 表示由 $\delta(y) = xR(x)$ 在 $\mathbb{F}_q$ 上定义的光滑仿射曲线。

Corollary 2.5. Let τ_ξ be the eigenvalue of Fr_q on $H^1_c(\mathbb{A}^1, \mathscr{Q}_\xi)$. Then we have

$$L_{\overline{C}_\delta/\mathbb{F}_q}(T) = \prod_{\psi \in V_\delta^\vee \setminus \{1\}} \prod_{\xi \in A_\psi^\vee} (1 - \tau_\xi T).$$

证明。与引理 2.4(1) 类似，我们有 $H^1_c(C_{\delta,\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \simeq \bigoplus_{\psi \in V_\delta^\vee \setminus \{1\}} H^1_c(\mathbb{A}^1, \mathscr{L}_\psi(xR(x)))$。我们有一列有限态射 $C_R \to C_\delta \to \mathbb{A}^1_{\mathbb{F}_q}$，其复合映射由 $\phi_1 \colon (x, y) \mapsto x$ 给出。这延拓为紧化 $\overline{C}_R \to \overline{C}_\delta \to \mathbb{P}^1_{\mathbb{F}_q}$ 之间的映射。由于 $\overline{C}_R \setminus C_R$ 由一个 $\mathbb{F}_q$-有理点构成，C_δ 也同样如此。因此，自然映射 $H^1_c(C_{\delta,\mathbb{F}}, \overline{\mathbb{Q}}_\ell) \to H^1(\overline{C}_{\delta,\mathbb{F}}, \overline{\mathbb{Q}}_\ell)$ 是一个同构。

□

We analyze τ_ξ in the next section.

3 Evaluations of τ_ξ

3.1 Formulae for τ_ξ in terms of local epsilon factors

For a non-archimedean local field F, let $\mathcal{O}_F$ be its ring of integers and $\mathfrak{m}_F$ denote its maximal ideal. Let $U_F^i := 1 + \mathfrak{m}_F^i$ for $i \geq 1$.

设 $K := \mathbb{F}_q((t))$。令 $\mathrm{res} \colon \Omega^1_K \to \mathbb{F}_q$ 表示剩余映射。对于有限域扩张 E/F，令 $\mathrm{Tr}^{E/F}$ 表示从 E 到 F 的迹映射。我们固定 $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$。令 $\psi_{\mathbb{F}_q} := \psi \circ \mathrm{Tr}^{\mathbb{F}_q/\mathbb{F}_p}$ 并

$$\Psi \colon K \to \overline{\mathbb{Q}}_\ell^\times;\ x \mapsto \psi_{\mathbb{F}_q}(\mathrm{res}(x dt)).$$

我们取 $\overline{K}$ 的一个可分闭包 K，并用 W_K 表示 $\overline{K}/K$ 的魏尔群。令 $j \colon \mathbb{A}^1_{\mathbb{F}_q} \to \mathbb{P}^1_{\mathbb{F}_q}$ 为典范嵌入，并令 x 为 $\mathbb{A}^1_{\mathbb{F}_q}$ 上的标准参数。通过设定 $t = 1/x$，我们将 $\mathbb{P}^1_{\mathbb{F}_q}$ 在 ∞ 处的局部域与 K 等同。令 $\xi \in A_\psi^\vee$ 为 ψ 的一个扩张。于是，$\mathscr{Q}_\xi$ 诱导出 W_K 的一个光滑特征，我们将其记为 ξ。根据引理 2.4(1)，我们有 $\deg \mathrm{Sw}(\xi) = 2$。

Let $c \in \mathfrak{m}_K^{-3} \setminus \mathfrak{m}_K^{-2}$. We consider the Gauss sum

$$\tau(\xi, \Psi) := q^{-1} \sum_{x \in \mathcal{O}_K^\times / U_K^3} \xi^{-1}(cx) \Psi(cx).$$

Note that the sum is independent of a choice of c.

The second assertion of the following proposition is a consequence of Laumon's product formula.

Proposition 3.1. (1) We have $\xi(t) = 1$.

(2) We have $\tau_\xi = -\tau(\xi, \Psi)$.

˜证明。（1）设 $F := \mathbb{F}_q(x)$，$\mathbb{A}_F^\times$ 为 F 的幂等元群。令 ξ 表示与 $\mathscr{Q}_\xi$ 对应的特征标 $\mathbb{A}_F^\times / F^\times \to \overline{\mathbb{Q}}_\ell^\times$。根据阿廷互反律，我们有以下等式

$$\tilde{\xi}(x_0)\xi(1/t) = 1,$$

其中，x_0 表示 $\mathbb{A}_F^\times$ 中的一个幺位，其各分量定义如下：在由 $0 \in \mathbb{A}^1_{\mathbb{F}_q}$ 定义的地方，它为 x；在其他地方，均为1。由于在0处的茎 $\mathscr{Q}_{\xi,\,0}$ 是

˜同构于 $\mathscr{L}_\psi(xR(x))$，在该对象上 Fr_q 的作用为恒等映射，我们有 $\xi(x_0) = 1$。断言得证。

(2) By Lemma 2.4(1) and [5, Théorème (3.2.1.1)], we have

$$\det(-\mathrm{Fr}_q; H^1_c(\mathbb{A}^1, \mathscr{Q}_\xi)) = q \cdot \varepsilon_\psi(\mathbb{P}^1_{\mathbb{F}_q,(\infty)}, j_!\mathscr{Q}_\xi, -dx).$$

Let $t = x^{-1}$, which is a uniformizer at ∞. We have

$$\begin{aligned}\varepsilon_\psi(\mathbb{P}^1_{\mathbb{F}_q,(\infty)}, j_!\mathscr{Q}_\xi, -dx) &= \varepsilon_\psi(\mathbb{P}^1_{\mathbb{F}_q,(\infty)}, j_!\mathscr{Q}_\xi, t^{-2}dt)\\ &= \xi(t)^{-2}q^{-2}\varepsilon_\psi(\mathbb{P}^1_{\mathbb{F}_q,(\infty)}, j_!\mathscr{Q}_\xi, dt).\end{aligned}$$

By [3, (5.8.2)], we have

$$\varepsilon_\psi(\mathbb{P}^1_{\mathbb{F}_q,(\infty)}, j_!\mathscr{Q}_\xi, dt) = q \cdot \tau(\xi, \Psi).$$

Then the assertion follows as $\xi(t) = 1$ by (1). □

3.2 Evaluation of Gauss sums

Let

$$G_\psi := \sum_{x\in\mathbb{F}_q} \psi_{\mathbb{F}_q}(x^2).$$

A similar result to the following lemma is found in [1, Proposition 8.7(ii)].

Lemma 3.2. Assume that $p \neq 2$. Let $(\cdot,\cdot)_K$ denote the quadratic Hilbert symbol over K. Let $\gamma \in K^\times/U_K^2$ be the unique element satisfying

$$\xi\left(1 + x + \frac{x^2}{2}\right) = \Psi(\gamma x) \quad \text{for } x \in \mathfrak{m}_K.$$

Then we have $\tau(\xi, \Psi) = \xi^{-1}(\gamma)\Psi(\gamma)(2\gamma, t)_K G_\psi$.

Proof. The sum $q\tau(\xi, \Psi) = \sum_{x\in\mathcal{O}_K^\times/U_K^3} \xi^{-1}(\gamma x)\Psi(\gamma x)$ can be computed as follows:

$$\begin{aligned}\sum_{x\in\mathcal{O}_K^\times/U_K^3} \xi^{-1}(\gamma x)\Psi(\gamma x) &= \sum_{\zeta\in\mathbb{F}_q^\times, z\in\mathfrak{m}_K/\mathfrak{m}_K^3} \xi^{-1}(\gamma\zeta(1+z))\Psi(\gamma\zeta(1+z))\\ &= \sum_{\zeta\in\mathbb{F}_q^\times} \xi^{-1}(\gamma\zeta)\Psi(\gamma\zeta) \sum_{z\in\mathfrak{m}_K/\mathfrak{m}_K^3} \xi^{-1}(1+z)\xi\left(1 + \zeta z + \frac{(\zeta z)^2}{2}\right).\end{aligned}$$

和式 $\sum_{z\in\mathfrak{m}_K/\mathfrak{m}_K^3} \xi^{-1}(1+z)\xi(1+\zeta z+{(\zeta z)_2}^2)$ 可以写成

$$\begin{aligned}&\sum_{y\in\mathfrak{m}_K/\mathfrak{m}_K^2, z\in\mathfrak{m}_K^2/\mathfrak{m}_K^3} \xi^{-1}(1+y)\xi^{-1}(1+z)\xi\left(1+\zeta y+\frac{(\zeta y)^2}{2}\right)\xi(1+\zeta z)\\ &= \sum_{y\in\mathfrak{m}_K/\mathfrak{m}_K^2} \xi^{-1}(1+y)\xi\left(1+\zeta y+\frac{(\zeta y)^2}{2}\right) \sum_{z\in\mathfrak{m}_K^2/\mathfrak{m}_K^3} \xi(1+(\zeta-1)z).\end{aligned}$$

最后一部分 $\sum_z$ 除非满足 $\zeta = 1$，否则为零。因此，我们可以计算

$$q\tau(\xi,\Psi) = q\xi^{-1}(\gamma)\Psi(\gamma) \sum_{y\in\mathfrak{m}_K/\mathfrak{m}_K^2} \xi^{-1}(1+y)\xi\left(1+y+\frac{y^2}{2}\right)$$
$$= q\xi^{-1}(\gamma)\Psi(\gamma) \sum_{y\in\mathfrak{m}_K/\mathfrak{m}_K^2} \Psi\left(\frac{\gamma y^2}{2}\right) = q\xi^{-1}(\gamma)\Psi(\gamma)(2\gamma,t)_K G_\psi.$$

Hence the assertion follows. □

The following is shown in an elementary way.

Lemma 3.3. Let $\tau \in \mathbb{Z}[i]$. Assume that $|\tau|^2 = 2^n$ with an integer $n \geq 1$. We have

$$\frac{\tau}{2^{n/2}} \in \begin{cases} \left\{e^{\pm\frac{\pi i}{4}}, e^{\pm\frac{3\pi i}{4}}\right\} & \text{if } n \text{ is odd,} \\ \{\pm 1, \pm i\} & \text{if } n \text{ is even.} \end{cases}$$

证明。环 $\mathbb{Z}[i]$ 有唯一的素理想 $(1+i)$，它位于 $\mathbb{Z}$ 的理想 (2) 之上。因此，我们可以写成 $\tau = \zeta(1+i)^n$，其中 $\zeta = \pm 1, \pm i.$。由于 $\frac{1+i}{\sqrt{2}}$ 是一个本原 8 次单位根，结论得证。

□

Let $\mu_n := \{x \in \overline{\mathbb{Q}}_\ell \mid x^n = 1\}$ for an integer $n \geq 1$.

Lemma 3.4. Assume that p is even. We have $\tau_\xi \in \mathbb{Z}[\mu_4]$.

证明。根据引理 2.2，ξ 的像包含于 μ_4 中。因此，对 $\tau_\xi = \mathrm{Tr}(\mathrm{Fr}_q; H_c^1(\mathbb{A}^1, \mathscr{L}_\xi))$ 应用 Grothendieck 的迹公式，即可得到所述结论。 □

Corollary 3.5. We write $q = p_0^f$ with a prime number p_0.

(1) 我们有 $\tau_\xi \in \mu_{4p_0} q^{1/2}$.(2) 假设 f 为奇数，且 $p_0 \not\equiv 1$ (模 4)。那么我们有 $\tau(\xi, \Psi)^{2p_0} = -q^{p_0}$。

证明。假设 $p_0 \neq 2$。引理 2.2 表明 $\xi^{-1}(c) \in \mu_{p_0}$。引理 3.2 表明 $\tau_\xi^{2p_0} = (-1)^{f(p_0-1)/2} q^{p_0}$。因此，在这种情况下，结论 (1) 和 (2) 成立。

假设 $p_0 = 2$。根据命题 3.1、引理 3.3 和引理 3.4，我们知道 $\tau_\xi/q^{1/2} \in \mu_8$，并且当 $2 \nmid f$ 时，这个值是一个本原 8 次单位根。 □

3.3 Conclusion

Now, we give a generalization of [4, Theorems (9.4) and (13.7)] (cf. [2, Proposition 8.5]).

Theorem 3.6. We write $q = p_0^f$ with a prime number p_0.

(1) 曲线 $\overline{C}_R$ 是 $\mathbb{F}_{q^{4p_0}}$-极小的。特别地，$\overline{C}_R$ 是超奇异的。(2) 假设 f 是奇数，且 $p_0 \not\equiv 1 \pmod 4$。那么 $\overline{C}_R$ 是 $\mathbb{F}_{q^{2p_0}}$-极大的。

Proof. The claims follow from Lemma 2.4, Proposition 3.1 and Corollary 3.5. □

例 3.7。我们给出一个符合定理 3.6(2) 中情形的例子。假设 $q = p$ 是一个满足 $p \neq 1 \pmod 4$ 的素数。令 $R(x) = x^p - x$。我们考虑曲线 $\overline{C}_R$。容易验证 $\mathbb{F}_p \subset V_R$。$\mathbb{F}_p$-子空间 $\mathbb{F}_p \subset V_R$ 是全各向同性的。于是 $A_R = \mathbb{F}_p^2$。显然，(2.3) 得到满足。

Corollary 3.8. Assume that $p_0 = 2$ and $H_R \subset \mathbb{F}_q^2$. Write $q = p_0^f$. Then f is even and $\overline{C}_R$ is $\mathbb{F}_{q^2}$-minimal.

证明。沿用推论 3.5 的证明中的记号。由引理 3.3 可知，若 f 为奇数，则 $\tau_\xi/q^{1/2}$ 是一个本原 8 次单位根。因此，只需证明 $\tau_\xi/q^{1/2} \in \{\pm 1\}$。反设结论不成立。设 π_ψ 为 H_R 的唯一一个中心特征标等于 ψ 的不可约表示。那么 $\dim \pi_\psi = p^e$。因此，我们有一个同构 $H_c^1(\mathbb{A}^1, \mathscr{L}_\psi(xR(x))) \simeq \pi_\psi$，作为 H_R-表示。根据 $H_R \subset \mathbb{F}_q^2$，Schur 引理表明，$\mathrm{Fr}_q$ 在 $H_c^1(\mathbb{A}^1, \mathscr{L}_\psi(xR(x)))$ 上的作用为数乘：

$$a_\psi := \mathrm{Tr}(\mathrm{Fr}_q; H_c^1(\mathbb{A}^1, \mathscr{L}_\psi(xR(x)))) = p^e \tau_\xi.$$

根据 a ssumption，我们知道 $a_\psi \notin \mathbb{Z}$。Grothendieck 迹公式表明 tha t

$$\mathrm{Tr}(\mathrm{Fr}_q; H_c^1(\mathbb{A}^1, \mathscr{L}_\psi(xR(x)))) = -\sum_{x \in \mathbb{F}_q} \psi_{\mathbb{F}_q}(xR(x)).$$

由于 ψ 的像是 $\{\pm 1\}$，因此我们有 $a_\psi \in \mathbb{Z}$，这就产生了矛盾。因此，结论得证。□

注 3.9. 假设 $p_0 = 2$。在引理 3.4 的证明中，我们只使用了 Grothendieck 迹公式。因此，在这种情况下，无需使用劳蒙乘积公式，我们便可得到推论 3.5、定理 3.6 和推论 3.8。

附录 A τξ 的另一种计算

在本附录中，我们不借助局部类域论，直接计算 $p_0 \neq 2$ 情形下 τ_ξ 的精确值。

A.1 Taking quotients of C_R

Let $(a, b) \in H_R$ be an element such that

$$a \neq 0, \quad b = \frac{f_R(a, a)}{2}. \tag{A.4}$$

以下引理在 [4, Propositions (9.1) and (13.5)], [2, Proposition 7.2]and [7, Lemma 4.9] 中给出，适用于 p为素数的情形。该引理给出了一种算法，用于计算 C_R 在 H_R中的某些阿贝尔子群作用下的商。

Lemma A.1. Assume $e \geq 1$.

(1) 设

$$\Delta_0(x) := -\frac{x}{a}\left(\frac{b}{a}x - f_R(x, a)\right)$$

and

$$u := x^p - a^{p-1}x, \quad v := y - \Delta_0(x). \tag{A.5}$$

那么存在一个次数为 p^{e-1} 、满足$v^p - v = uR_1(u)$ 的加性多项式 $R_1(u) \in \mathbb{F}[u]$。 $R_1(u)$ 的首项系数是

$$\begin{cases} -\dfrac{a_e}{a^{p-1}} & \text{if } e > 1, \\ -\dfrac{a_e}{2a^{p-1}} & \text{if } e = 1. \end{cases}$$

(2) Let $U_a := \{(\xi a, \xi^2 b) \in H_R \mid \xi \in \mathbb{F}_p\}$. The quotient C_R/U_a is isomorphic to C_{R_1}.

Proof. We show the claims in just the same way as [7, Lemma 4.9]. □

By Lemma A.1(1),

$$xR(x) = uR_1(u) + \Delta_0(x)^p - \Delta_0(x). \tag{A.6}$$

We write $u(x)$ for u.

设 $(a', b') \in H_R$是满足 (A.4) 的元素。假设 $\omega_R(a, a') = 0$。由引理 2.1(3)，(a, b) 与 (a', b') 交换。因此，(a', b') 的作用诱导出 $C_{R_1} \simeq C_R/U_a$ 的自同构。

Lemma A.2. Let $\pi(a', b') := (u(a')\ 2^{-1}f_{R_1}(u(a')\ u(a'))) \in \mathbb{F}^2$.

(1) We have

$$\Delta_0(x + a') + f_{R_1}(u(x), u(a')) = \Delta_0(x) + \Delta_0(a') + f_R(x, a'). \tag{A.7}$$

(2) We have $\pi(a', b') \in H_{R_1}$.

(3) The action of (a', b') on C_R induces the automorphism $\pi(a', b')$ on C_{R_1}.

Proof. All the claims are shown in the same way as [7, Lemma 4.10 and (4.10)]. □

推论 A.3. 设记号同引理 A.1。设 $A \subset V_R$ 是关于 ω_R的一个维数为 d的全各向同性子空间。设 $a_1, \ldots, a_d$是 A在$\mathbb{F}_p$上的一组基。假设 $a = a_d$。那么 $A' := \sum_{i=1}^{d-1} \mathbb{F}_p u(a_i) \subset V_{R_1}$ 是关于 ω_{R_1}的一个维数为 $d-1$ 的全各向同性子空间。

证明。假设 $\sum_{i=1}^{d-1} x_i u(a_i) = 0$，且 $x_i \in \mathbb{F}_p$。那么 $u(\sum_{i=1}^{d-1} x_i a_i) = 0$。因此 $\sum_{i=1}^{d-1} x_i a_i \in \mathbb{F}_p a$。这意味着，对于每个 $1 \le i \le d-1$，都有 $x_i = 0$。故 $\dim_{\mathbb{F}_p} A' = d-1$。令 $1 \le i \ne j \le d-1$。由 (A.7) 和 $\omega_R(a_i, a_j) = 0$，可得 $\omega_{R_1}(u(a_i)\ u(a_j)) = 0$。因此结论成立。

□

设 $A \subset V_R$ 是关于 ω_R 的一个极大全各向同性子空间。我们通过群同态 $A \hookrightarrow H_R$ 将 A 识别为 H_R 的一个阿贝尔子群； $a \mapsto (a, 2^{-1}f_R(a, a))$。下面的结果是将 [2, 定理 7.4] 推广到 p 为素数幂的情形。

Proposition A.4. Let

$$c_A := \begin{cases} (-1)^e \dfrac{a_e}{2} \displaystyle\prod_{\alpha \in A \setminus \{0\}} \alpha^{-1} & \text{if } e \geq 1, \\ a_0 & \text{if } e = 0. \end{cases}$$

The quotient C_R/A is isomorphic to the curve defined by $y^p - y = c_A x^2$.

证明。注意到 $\dim_{\mathbb{F}_p} A = e$。取 A 在 $\mathbb{F}_p$ 上的一组基 $\{a_1, \ldots, a_e\}$。令 $a := a_e$。由引理 A.1 可知，有限 ´étale 态射 $C_R \to C_{R_1}$。令 $a'_i := u(a_i) \in A' = \sum_{i=1}^{e-1} \mathbb{F}_p a'_i \subset V_{R_1}$，根据推论 A.3，该对象关于 ω_{R_1} 是全各向同性的。取 a'_{e-1} 作为 a，并应用引理 A.1，得到一个态射 $C_{R_1} \to C_{R_2}$。继续这一过程。因此，我们得到一个次数为 p^e 的有限 ´étale 态射 $\phi\colon C_R \to C_{R_e}$。由引理 A.1(1)，曲线 C_{R_e} 由 $y^p - y = c_A x^2$ 定义。由引理 A.2(3)，态射 ϕ 可分解为经过 $C_R \to C_R/A \xrightarrow{\phi'} C_{R_e}$ 的态射。由于 $C_R \to C_R/A$ 的次数为 p^e，因此 ϕ' 是一个同构。 □

Lemma A.5. We write $F_R(x) = \sum_{i=0}^{e} b_i x^{p^i}$. Then we have $c_A = (-1)^{e+1}(a_e b_e)/(2b_0)$ if $e \geq 1$.

Proof. By $\prod_{\alpha \in A \setminus \{0\}} \alpha = -b_0/b_e$, the assertion follows from Proposition A.4. □

A.2 Value of τ_ξ

Let $A := \{x \in \mathbb{F} \mid F_R(x) = 0\}$, which is a totally isotropic subspace of V_R with respect to ω_R in Lemma 2.1(3). Assume (2.3). In particular,

$$A \subset \mathbb{F}_q \cap V_R. \tag{A.8}$$

因此，存在一个加性多项式 $a(x) \in \mathbb{F}_q[x]$ 使得 $x^q - x = a(F_R(x))$。我们记为 $q = p^s$。对于 $t \in \mathbb{F}_q$，我们取满足 $F_R(x) = t$ 的 $x \in \mathbb{F}$，并令

$$b(x,t) := \sum_{i=0}^{s-1} (xR(x))^{p^i} - f_R(x, x^q - x). \tag{A.9}$$

Lemma A.6. The value $b(x,t)$ is independent of the choice of x, for which we write $b(t)$. Furthermore, $(a(t)\ b(t)) \in A_R$.

证明。首先注意到 $F_R(a(x)) = x^q - x$，因此由 $t \in \mathbb{F}_q$ 可得 $a(t) \in A$。令 $y \in A$。由于 A 是全各向同性的，因此 $\omega_R(a(t)\ y) = 0$。我们将 $\mathrm{Tr}^{\mathbb{F}_q/\mathbb{F}_p}$ 简记为 Tr。我们有 $\mathrm{Tr}(yR(y)) = 2^{-1}\mathrm{Tr}(2yR(y)) = 2^{-1}\mathrm{Tr}(f_R(y,y)^p - f_R(y,y)) = 0$，这里使用了 (2.1) 和 $y \in \mathbb{F}_q$。令 $x' := x + y$。由 (A.8)，可得 $y \in \mathbb{F}_q \cap V_R$。由 $F_R(x) = t$，$x^q - x = a(t)$。利用 (2.1)，我们计算得到

$$\begin{aligned} b(x',t) - b(x,t) &= \sum_{i=0}^{s-1} (yR(x) + xR(y))^{p^i} + \mathrm{Tr}(yR(y)) - f_R(y, a(t)) \\ &= \sum_{i=0}^{s-1} (f_R(x,y)^p - f_R(x,y))^{p^i} - f_R(y, a(t)) \\ &= f_R(x^q, y) - f_R(x,y) - f_R(y, a(t)) = \omega_R(a(t), y) = 0. \end{aligned}$$

Hence $b(x,t)$ is independent of x. Again by (2.1), (A.8) and $x^q - x = a(t)$, we obtain

$$b(t)^p - b(t) = (xR(x))^q - xR(x) - xR(a(t)) - a(t)R(x) = a(t)R(a(t)).$$

□

Lemma A.7. Let $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$ and $\xi \in A_\psi^\vee$. Then we have

$$\tau_\xi = -\sum_{t\in\mathbb{F}_q} \xi(a(t), b(t)).$$

证明。令 $t \in \mathbb{F}_q$。我们取 $(x,y) \in C_R$ 使得 $F_R(x) = t$。回顾 $x^q - x = a(t)$。显然，$y^q - y = \sum_{i=0}^{s-1}(y^p - y)^{p^i} = \sum_{i=0}^{s-1}(xR(x))^{p^i}$。因此 $y^q = y + f_R(x, a(t)) + b(t)$。因此，根据 (2.2)，$(x^q, y^q) = (x,y)\cdot(a(t)\ b(t))$。将 Grothendieck 迹公式应用于 $\tau_\xi = \mathrm{Tr}(\mathrm{Fr}_q;\ H_c^1(\mathbb{A}^1, \mathscr{Q}_\xi))$，结论即得。□

By Proposition A.4, the curve C_R/A is defined by $y^p - y = c_A x^2$. We consider the quotient morphism

$$\pi\colon C_R \to C_R/A;\ (x,y) \mapsto (F_R(x), y - \Delta(x)).$$

Then

$$\begin{aligned} xR(x) &= c_A F_R(x)^2 + \Delta(x)^p - \Delta(x), \\ f_R(x,a) + \frac{f_R(a,a)}{2} &= \Delta(x+a) - \Delta(x) \quad \text{for } a \in A, \end{aligned} \tag{A.10}$$

where the second equality follows from $\pi((x,y)\cdot(a, 2^{-1}f_R(a,a))) = \pi(x,y)$ and (2.2).

Proposition A.8. We have

$$b(t) - \frac{f_R(a(t), a(t))}{2} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c_A t^2)$$

Proof. Using (A.10), $\Delta(x) \in \mathbb{F}_q[x]$ and $x^q - x = a(t)$, we compute

$$\begin{aligned} b(t) - \frac{f_R(a(t), a(t))}{2} &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c_A t^2) + \Delta(x^q) - \Delta(x) - (\Delta(x + a(t)) - \Delta(x)) \\ &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(c_A t^2). \end{aligned}$$

□

We consider the character

$$\xi'\colon \mathbb{F}_q \to \overline{\mathbb{Q}}_\ell^\times;\ t \mapsto \xi\left(a(t), \frac{f_R(a(t), a(t))}{2}\right).$$

Let $\eta \in \mathbb{F}_q^\times$ be the element such that $\xi'(t) = \psi_{\mathbb{F}_q}(\eta t)$ for $t \in \mathbb{F}_q$.

推论 A.9. 设 $\psi \in \mathbb{F}_p^\vee \setminus \{1\}$ 和 $\xi \in A_\psi^\vee$。设 $\left(\frac{x}{q}\right) = x^{\frac{q-1}{2}}$，其中 $x \in \mathbb{F}_q^\times$。则我们有

$$\tau_\xi = -\psi_{\mathbb{F}_q}\left(-\frac{\eta^2}{4c_A}\right)\cdot\left(\frac{c_A}{q}\right) G_\psi.$$

证明。引理 A.7 和命题 A.8 蕴含

$$\tau_\xi = -\sum_{t\in\mathbb{F}_q} \psi_{\mathbb{F}_q}(c_A t^2 + \eta t) = -\psi_{\mathbb{F}_q}\left(-\frac{\eta^2}{4c_A}\right)\cdot\left(\frac{c_A}{q}\right) G_\psi.$$

□

参考文献

[1] A. Abbes 和 T. Saito，《局部傅里叶变换与 ε 因子》，Compos. Math. 146，第 6 期（2010），1507–1551。

[2] I. Bouw、W. Ho、B. Malmskog、R. Scheidler、P. Srinivasan 和 C. Vincent，《具有大量自同构的 Artin–Schreier 曲线类的 ζ 函数》，《数论研究方向》，87–124 页，数学女性协会丛书，第 3 卷，Springer，2016 年。

[3] P. Deligne，《L 函数泛函方程的常数》，《单变量模函数》第二卷（1972 年，安特卫普大学国际暑期学校论文集），第 501–597 页。数学讲义，第 349 卷，施普林格出版社，柏林，1973 年。

[4] G. van der Geer 和 M. van der Vlugt，《Reed-Muller 码与超奇异曲线 I》，Compositio Mathematica，84 卷第 3 期（1992 年），333–367 页。

[5] G. Laumon，《傅里叶变换、函数方程的常数与韦伊猜想》，高等科学研究所数学出版物，第65期（1987年），131–210页。

[6] J. P. Serre，《局部域》，第二版，Hermann，巴黎，1968年。

[7] T. Tsushima，与加性多项式相关的局部伽罗瓦表示，预印本。

Daichi Takeuchi
日本埼玉县和光市广泽2-1，邮编351-0198，理化学研究所（RIKEN）先进智能项目中心（AIP）数学科学团队 daichi.takeuchi@riken.jp

Takahiro Tsushima 千叶大学理学院数学与信息学系，日本千叶县千叶市稻毛区弥生町1-33，邮编263-8522 tsushima@math.s.chiba-u.ac.jp