Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristic

Fumiyuki Momose†, Jinhui Chao‡

† Department of Mathematics, Chuo University, Tokyo Japan
‡Department of Information and System Engineering,
Chuo University, Tokyo Japan

Abstract

In this paper, we present a classification of elliptic curves defined over a cubic extension of a finite field with odd characteristic which have coverings over the finite field therefore subjected to the GHS attack. The densities of these weak curves, with hyperelliptic and non-hyperelliptic coverings, are then analyzed respectively. In particular, we show, for elliptic curves defined by Legendre forms, at least half of them are weak. We also give an algorithm to determine if an elliptic curve belongs to one of two classes of weak curves.

keywords

Elliptic curves, Hyperelliptic curves, Non-hyperelliptic curves, Index calculus, GHS attack, Cover attack

1 Introduction

Let q be a power of an odd prime. $k := \mathbb{F}_q, k_d := \mathbb{F}_{q^d}$.

Among general attacks to discrete logarithms on an abelian group G with group order $l := \#G$ (known as the key-length of the cryptosystem), the so-called "square-root" attacks such as the Baby-step-giant-step attack or Pollard's rho-method and lambda-method have running time in the order of the square root of the group order, i.e., $\tilde{O}(l^{1/2})$). $(\tilde{O}(x) := O(x \log^m x))$.

Besides the square-root algorithms there are two main attacks on algebraic-curve-based cryptosystems: variations of the index calculus attack [12][9][29][13] [27] and the GHS attack [10][14][11][22][6][18][19][30][31][8][4].

For a hyperelliptic curve cryptosystem, the double-large-prime variation of the index calculus attack by Gaudry-Thériault-Thomé-Diem [13] and Nagao [27] solves discrete logarithms in running time $\tilde{O}(q^{2-\frac{2}{g}})$. In particular for $g = 3$, the running time is $\tilde{O}(q^{4/3}) = \tilde{O}(l^{4/9})$, a little faster than the square-root attacks. However, the hyperelliptic curves of genus from 5 to 9 can be attacked by these algorithms more effectively than by the square-root attacks.

Recently, Gaudry showed a general algorithm for solving discrete logarithms on Abelian varieties of dimension n in running time $\tilde{O}(q^{2-\frac{2}{n}})$ [15]. In particular, for elliptic curves over the cubic extension field $\mathbb{F}_{q^3}$, the running time is $\tilde{O}(q^{4/3})$.

In spite of a common belief that non-hyperelliptic curves should be harder to attack than hyperelliptic ones, Diem recently showed an attack under which non-hyperelliptic curves of low degree and genus at least 3 are actually weaker than hyperelliptic curves [7]. More specifically, when C is a non-hyperelliptic curve of genus $g \geq 3$, one can almost always find a birational transform over k to another curve C'

$$C \overset{birat}{\dashrightarrow} C' \subset \mathbb{P}^2$$

such that $\deg C' = d \geq g+1$. (Notice that when C' is a hyperelliptic curve, one has $\deg C' = d \geq g+2$).) Thus when C' is defined over k, the running time of Diem's double-large-prime variation [7] is $\tilde{O}(q^{2-\frac{2}{d-2}})$. When $d = g+1$, it becomes $\tilde{O}(q^{2-\frac{2}{g-1}})$. In particular, genus 3 non-hyperelliptic curves over $\mathbb{F}_q$ can be attacked in an expected time $\tilde{O}(q) = \tilde{O}(l^{1/3})$.

Recently, Smith showed that a certain fraction of hyperelliptic curves of genus 3 can be transformed to non-hyperelliptic curves [28].

The other main attacks on algebraic-curve-based cryptosystems are GHS and related attacks. It was Frey who introduced the use of Weil descent into elliptic curve cryptosystems [10]. The GHS attack has also been conceptually generalized to the cover attack [6][8]. Let E/k_d be an elliptic curve, $W := Res_{k_d/k}E$ its Weil restriction. Then, since $E(k_d) \simeq W(k)$, if there is a covering curve C/k of E, it may be possible to transfer the discrete logarithms on $E(k_d)$ to the Jacobian of the covering curve $J(C)(k)$. The GHS attack proposed in [14] used the norm-conorm map to transfer the discrete logarithms from $Cl(E/k_d)$ to $Cl(C/k)$.

A natural and important question is then what kind of curves and how many of them are vulnerable to this attack. Until now, certain weak classes of curves have been discovered [8][30][31][23]. However, a complete description of the classes of weak curves and their exact number still remains to be obtained.

In this paper, we first present a classification of elliptic curves defined over the cubic extension of a finite field with odd characteristic which have coverings defined over the finite field and therefore can be attacked by the GHS attacks. We refer to such a curve as a curve with weak covering, or simply a weak curve.

Below, we will follow the formulation in [6] and [4] and refer to them for the details of the GHS attack.

Let C_0 be an algebraic curve over k_d with genus $g_0 := g(C_0) \geq 1$. Assume there exists an algebraic curve C of genus $g := g(C)$ defined over k such that

$$\pi : C \twoheadrightarrow C_0$$

is a covering defined over k_d.

We assume the following isogeny condition: for the induced map

$$\pi_* : \quad J(C) \quad \twoheadrightarrow \quad J(C_0),$$

the restriction of scalars of π_*

$$Res(\pi_*) : J(C) \longrightarrow \operatorname{Res}_{k_d/k}\big(J(C_0)\big)$$

defines an isogeny over k. Therefore, $g = dg_0$.

In order to be able to transfer a discrete logarithm on $J(C_0)$ to $J(C)$, we must have $g \geq dg_0$. Under the isogeny condition, the curves obtained in the previous description are the most favorable for a GHS attack.

Based on the classification of the weak curves, we then present a density analysis of these weak curves or count the number of such curves up to $\mathrm{PGL}_2(k)$-actions and show how to test if a curve has a weak covering so they could be easily avoided for one of the classes of weak curves.

The main results of this paper are summarized in the following theorem.

Theorem 1. *Under the isogeny condition, elliptic curves E over a cubic extension field k_3 which have covering curves $C/\mathbb{P}^1$ are as follows.*

When $C/\mathbb{P}^1$ is a $(2,2,2)$-covering, E has the following form and C is hyperelliptic.

$$\begin{gathered} E/k_3 : \quad y^2 = eg(x)(x-\alpha)(x-\alpha^q) \qquad (1) \\ \alpha \in k_3 \setminus k, \quad e \in k_3^\times, \quad g(x) \in k[x], \quad \deg g(x) = 1 \text{ or } 2. \end{gathered}$$

The number of such E is $q^2 - 2q + 3$.

When $C/\mathbb{P}^1$ is a $(2,2)$-covering, E has one of the following two forms:

$$\begin{aligned} &\textit{Type I:} && E_1: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q) && (2) \\ & && \qquad \alpha, \beta \in k_3 \setminus k, \quad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4 && \\ &\textit{Type II:} && E_2: \quad y^2 = (x-\alpha)\left(x-\alpha^{q^3}\right)(x-\alpha^q)\left(x-\alpha^{q^4}\right) && (3) \\ & && \qquad \alpha \in k_6 \setminus \{k_2 \cup k_3\}, \quad \beta = \alpha^{q^3} && \end{aligned}$$

$E_i, i = 1, 2$ is k_3-isomorphic to a Legendre form:

$$E_i \simeq \quad y^2 = e_i x(x-1)(x-\lambda_i), \quad e_i \in k^\times.$$

If one defines

$$\lambda(\alpha, \beta) := \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)^{q+1}}$$

and for Type II curves, let $\beta = \alpha^{q^3}$, then for Type I curves,

$$e_1 = 1, \qquad \lambda_1 = \lambda(\alpha, \beta).$$

For Type II curves,

$$e_2 = (\alpha - \alpha^{q^3})^{q+1}, \qquad \lambda_2 = -\lambda(\alpha, \beta)$$

and

$$\begin{cases} e_2 \in (k_3^\times)^2 & \Longleftrightarrow \quad q \equiv 3 \bmod 4 \\ e_2 \notin (k_3^\times)^2 & \Longleftrightarrow \quad q \equiv 1 \bmod 4 \end{cases}.$$

Thus only in the first case we can assume that $e_2 = 1$.

The number of λ_1 such that Type I curves have non-hyperelliptic covers is $\frac{1}{2}(q^3 - q^2 - q - 3)$.

The number of λ_2 such that Type II curves have non-hyperelliptic covers is $\frac{1}{2}(q^3 - q^2 + q - 1)$.

Among either Type I or Type II curves, the number of λ_i such that the curves E_i have hyperelliptic covers C equals q^2.

For Type I curves, we show in Lemma 7.2 a fast algorithm to test if an elliptic curve is a Type I curve. Implementation of the GHS attack on these two types of curves is also discussed in [17].

The density analysis is undertaken using some but not all k_3-isomorphisms, so the above numbers of Legendre forms provide lower bounds for the true densities.

Besides, at present we do not know if there is any overlap between Type I and II curves. However, it is conjectured that the overlap is about a half.

The numbers of these weak curves seemed alarmingly large. E.g., if you choose random elliptic curves E defined over k_3 in the Legendre form , then at least half of them are weak and should not be used in cryptosystems since when the order $\#E(k_3)$ are 160-bit prime numbers, their coverings $C(k)$ only have 107-bit key-length under the GHS attack.

The curves over extension fields could often be desirable in practice for fast and low-cost implementation, especially certain extension fields with good properties. An example is to use extension fields which possess a normal basis. Another example is that a fast and cheap way to implement a 160-bit elliptic cryptosystem is to use a 64-bit processor and an elliptic curve defined over the cubic extension of a 64-bit prime field. The above results show that such a setting could be dangerous. Therefore, the threat of Weil descent attacks should not be underestimated.

2 Classification of elliptic curves with $(2, 2, \ldots, 2)$-coverings

Let $k := \mathbb{F}_q, k_d := \mathbb{F}_{q^d}, d \geq 2$. Let C_0 be a hyperelliptic curve defined over k_d with genus $g(C_0) := g_0$ equals to 1, 2 or 3.

Assume that C is an algebraic curve of genus g defined over k such that there is a covering

$$\pi/k_d : C \longrightarrow C_0$$

defined over k_d. In particular, C is an n-tuple $(2, 2, \ldots, 2)$-covering of $\mathbb{P}^1(x)$ with degree 2^n, or $k_d(C)$ is the compositum of $k_d({}^{\sigma^i}C_0), i = 0, \ldots, d-1$ with extension degree 2^n over $k_d(x)$.

The Weil restriction of the Jacobian $J(C_0)$ of C_0 is defined as

$$Res_{k_d/k}J(C_0) := \prod_{i=0}^{d-1} J({}^{\sigma^i}C_0)$$

which is an Abelian variety of dimension dg_0.

Then, the induced map

$$\pi_* : J(C) \longrightarrow J(C_0)$$

has the restriction of scalars

$$Res(\pi_*) : J(C) \longrightarrow \mathrm{Res}_{k_d/k}\big(J(C_0)\big)$$

which we assume to be an isogeny over k. Therefore, $g = dg_0$.

One can prove

Lemma 1.

(1) $\ker Res(\pi_*) \subset J(C)[2^{n-1}]$*;*
(2) If C is hyperelliptic, then the above kernel can be described explicitly.

Similar results for the GHS attack have been proved in [14][18][19].

Hereafter, we assume that C_0 is an elliptic curve E and $d = 3$.

2.1 Classification and defining equations of E with $(2, 2, \ldots, 2)$-coverings

When the degree of the covering $C \to \mathbb{P}^1$ is eight, or $C/\mathbb{P}^1$ is a $(2, 2, 2)$-covering, one can prove under the isogeny condition that C is a hyperelliptic curve over k of genus three.

Lemma 2. *An E/k_3 with a covering C/k which is a $(2, 2, 2)$-covering of $\mathbb{P}^1$ has the following form.*

$$\begin{aligned} E/k_3: \quad y^2 &= eg(x)(x-\alpha)(x-\alpha^q) \qquad (4)\\ \textit{where} \quad &\alpha \in k_3 \setminus k,\\ &g(x) \in k[x], \quad \deg g(x) = 1 \ \textit{or}\ 2,\\ &e \in k_3^\times. \end{aligned}$$

Proof: Let S be the set of ramification points of the covering $C \longrightarrow \mathbb{P}^1$ in $\mathbb{P}^1(x)$, and let R be the set of ramification points in E. Define $R_i := {}^{\sigma^i}R$, which are sets of ramifications points in ${}^{\sigma^i}E, i = 0, 1, 2,$ $R_0 = R$. We have $\#R = \#R_0 = \#R_1 = \#R_2$.

We divide the ramification points of ${}^{\sigma^i}E$ into three parts.

- $T_1 = \{a \in k_3 \setminus k \mid a$ belongs to only one of the $R_i, i = 0, 1, 2$ };

- $T_2 = \{b \in k_3 \setminus k \mid b$ belongs to two of the R_i but not all three};

- $T_3 = \{c \in \cap_{i=0}^{2} R_i\}$, or the sets of ramification points which are σ-invariant (as sets).

By the Riemann-Hurwitz formula,

$$\begin{aligned} 2g(C) - 2 &= \deg(C/\mathbb{P}^1)(2g(\mathbb{P}^1) - 2) + 2^{n-1}\#S, \\ 2g(E) - 2 &= \deg(E/\mathbb{P}^1)(2g(\mathbb{P}^1) - 2) + \#R. \end{aligned}$$

Here all ramification points have index 2, and the number of fibres on C over a ramification point on $\mathbb{P}^1$ is $2^{n-1} = 4$. Therefore, $\#S = 5$ and $\#R = 4$.

This implies

$$\begin{aligned} \#R &= \#T_1 + 2\#T_2 + \#T_3 = 4, \\ \#S &= \# \cup_{i=0}^{2} R_i = 3\#T_1 + 3\#T_2 + \#T_3 = 5. \end{aligned}$$

Thus, one has

$$\#T_1 = 0, \#T_2 = 1, \#T_3 = 2.$$

Denote

$$T_2 = \{\alpha | \alpha \in k_3 \setminus k, \ s.t. \ \{\alpha, \alpha^q\} \subset R\}, \qquad T_3 = \{c, c'\}.$$

We have the defining equation of E as

$$E : y^2 = e(x - c)(x - c')(x - \alpha)(x - \alpha^q) = eg(x)(x - \alpha)(x - \alpha^q), \qquad e \in k_3^{\times}.$$

Now, taking the norm over the field extension k_3/k,

$$N_{k_3/k}(y^2) = N_{k_3/k}(e)g(x)^3 N_{k_3/k}(x - \alpha)^2$$

one obtains the following curve

$$\left(\frac{N_{k_3/k}(y)}{g(x)N_{k_3/k}(x - \alpha)}\right)^2 = N_{k_3/k}(e)g(x)$$

which is isomorphic to $\mathbb{P}^1$ since $\deg g(x) \leq 2$. Therefore, the covering of the curve (4) is indeed a $(2, 2, 2)$-type. □

When the degree of the covering $C \longrightarrow \mathbb{P}^1(x)$ is four, we have

Lemma 3. *An elliptic curve E/k_3 with a covering C/k which is a $(2, 2)$-covering over $\mathbb{P}^1$ is one of the following two types.*

Type I: $$E : \quad y^2 = (x - \alpha)(x - \alpha^q)(x - \beta)(x - \beta^q), \tag{5}$$

$$\alpha, \beta \in k_3 \setminus k, \quad \#\{\alpha, \alpha^q, \beta, \beta^q\} = 4; \tag{6}$$

Type II: $$E : \ y^2 = (x - \alpha)\left(x - \alpha^{q^3}\right)(x - \alpha^q)\left(x - \alpha^{q^4}\right), \tag{7}$$

$$\alpha \in k_6 \setminus \{k_2 \cup k_3\}. \tag{8}$$

In fact, the equation (5) of Type I was already given as Eq.(10) in [8] as an example. The existence of Type II curves with hyperelliptic coverings was also mentioned in [6], footnote 6.

Proof: We use the same notations as in the proof of Lemma 2. By the Riemann-Hurwitz formula,

$$2g(C) - 2 \quad = \quad \deg(C/\mathbb{P}^1)\left(2g(\mathbb{P}^1) - 2\right) + 2^{n-1}\#S.$$

Then, $\#S = 6$ and one has

$$\begin{aligned} \#R = \#T_1 + 2\#T_2 + \#T_3 &= 4, && (9)\\ \#S = 3\#T_1 + 3\#T_2 + \#T_3 &= 6. && (10) \end{aligned}$$

Since $n = 2$, one knows $\#T_1 = 0$. Thus, $\#T_2 = 2, \#T_3 = 0$, and there are two possibilities for ramification points. We call the two cases Type I and Type II hereafter.

In the Type I case:

$$R \quad = \quad \{\alpha, \alpha^q, \beta, \beta^q\}, \qquad \{\alpha, \alpha^q, \alpha^{q^2}\} \cap \{\beta, \beta^q, \beta^{q^2}\} = \emptyset. \qquad (11)$$

In the Type II case:

$$R = \{\alpha^{\sigma^i}, \alpha^{\sigma^{i+1}}, \alpha^{\sigma^j}, \alpha^{\sigma^{j+1}}\}, \qquad \#R = 4.$$

Then, one has the defining equations of Type I and II curves as follows.

$$E : y^2 = e\,(x-\alpha)\,(x-\alpha^q)\,(x-\beta)\,(x-\beta^q)\,, \qquad e \in k_3^\times$$

where $\beta = \alpha^{q^3}$ in the Type II case.

We now take the norm over the field extension k_3/k, then

$$N_{k_3/k}(y)^2 \quad = \quad N_{k_3/k}(e) N_{k_3/k}(x-\alpha)^2 N_{k_3/k}(x-\beta)^2.$$

Since

$$N_{k_3/k}(e) = \left(\frac{N_{k_3/k}(y)}{N_{k_3/k}(x-\alpha)N_{k_3/k}(x-\beta)}\right)^2,$$

one knows that $e \in \left(k_3^\times\right)^2$ can thus be assumed to be 1.

Then, for Type I curves,

$${}^{\sigma^2}y = \pm\frac{N_{k_3/k}(x-\alpha)N_{k_3/k}(x-\beta)}{y\;{}^{\sigma}y}.$$

For Type II curves,

$${}^{\sigma^2}y = \pm\frac{N_{k_3/k}(x-\alpha)^2}{y\;{}^{\sigma}y}.$$

Thus, one has a $(2,2)$-covering in both cases. □

2.2 Condition for a $(2,2)$-covering curve $C/\mathbb{P}^1$ to be hyperelliptic

Let the defining equation of E be

$$E : y^2 \quad = \quad (x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q), \tag{12}$$

where for Type II curves, $\beta = \alpha^{q^3}$.

Recall that, for a field F, the $\mathrm{PGL}_2(F)$-action on r by a matrix $A \in GL_2(F)$ is defined as

$$\begin{aligned} A &:= \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \\ A \cdot r &:= \frac{ar+b}{cr+d}. \end{aligned}$$

We will prove

Lemma 4. *C is a hyperelliptic curve if and only if there is a matrix $\Theta \in GL_2(k)$ such that $Tr(\Theta) = 0$ and $\beta = \Theta \cdot \alpha$.*

Proof: For the $(2,2)$-covering $C \longrightarrow E \longrightarrow \mathbb{P}^1(x)$, the commutative diagram of curves when C is hyperelliptic is shown below, where Θ is defined by the hyperelliptic involution of $C/\mathbb{P}^1$, which permutes the ramification points α and β of $E/\mathbb{P}^1(s)$.

$$\begin{tikzcd}
& & C \arrow[dl] \arrow[dr] & \\
& E \arrow[dl] \arrow[dr] & & \mathbb{P}^1(u) \arrow[dl] \\
\mathbb{P}^1(x) \arrow[dr] & & \mathbb{P}^1(s) \arrow[dl] & \\
& \mathbb{P}^1(t) & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& C \arrow[dl, "(2,2)"'] \arrow[dr, "2"] & \\
\mathbb{P}^1(x) \arrow[dr, "2"'] & & \mathbb{P}^1(u) \arrow[dl, "(2,2)"] \\
& \mathbb{P}^1(t) &
\end{tikzcd}$$

Now, given such a Θ, we will show explicitly the existence of the curves in the above diagram. Indeed, $\Theta \in Aut(\mathbb{P}^1(x))$ defines a degree-two covering $\theta : \mathbb{P}^1(x) \longrightarrow \mathbb{P}^1(t)$ such that $\mathbb{P}^1(t) = \mathbb{P}^1(x)/\theta$.

In fact, $\Theta \in GL_2(k)$ with zero trace can be classified into the following two forms:

$$\Theta_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Theta_2 = \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix} \qquad e \in k^\times \setminus \left(k^\times\right)^2.$$

We treat the two cases separately below.

1. For Θ_1, one has

$$\Theta_1 \cdot x = -x, \quad \beta = \Theta_1 \cdot \alpha = -\alpha,$$

$$s := x(\Theta_1 \cdot x) = -x^2.$$

The degree-two covering $\theta_1 : \mathbb{P}^1(x) \longrightarrow \mathbb{P}^1(t)$ is defined by

$$x^2 = t.$$

The defining equation of $\mathbb{P}^1(s)$ can be found as follows.
Define a map ζ_1 by

$$\begin{array}{rcl} \zeta_1 : E & \longrightarrow & E, \\ (x, y) & \longmapsto & (-x, -y). \end{array}$$

Then, $\mathbb{P}^1(s)$ is the quotient curve E/ζ_1. Define

$$s := xy,$$

then $\mathbb{P}^1(s)$ is defined by

$$\mathbb{P}^1(s) : s^2 = t(t - \alpha^2)(t - \alpha^{2q}).$$

2. For Θ_2, one has

$$\Theta_2 \cdot x = \frac{e}{x}, \qquad \beta = \Theta_2 \cdot \alpha = \frac{e}{\alpha}.$$

The degree-two covering $\theta_2 : \mathbb{P}^1(x) \longrightarrow \mathbb{P}^1(t)$ is defined by

$$t = x + \Theta_2 \cdot x = x + \frac{e}{x},$$

or

$$x^2 - tx + e = 0.$$

The defining equation of $\mathbb{P}^1(s)$ can be found as follows.
Define a map ζ_2 by

$$\begin{array}{rcl} \zeta_2 : E & \longrightarrow & E, \\ (x, y) & \longmapsto & \left(\frac{e}{x}, -\frac{e}{x^2} y\right). \end{array}$$

Then, $\mathbb{P}^1(s)$ is the quotient curve E/ζ_2. Define

$$s := y + \left(-\frac{e}{x^2} y\right),$$

$\mathbb{P}^1(s)$ is defined by

$$\mathbb{P}^1(s) : s^2 = (t^2 - 4e)\left(t - \left(\alpha + \frac{e}{\alpha}\right)\right)\left(t - \left(\alpha^q + \frac{e}{\alpha^q}\right)\right).$$

Next, we construct explicitly the (2,2)-covering $\mathbb{P}^1(u)/\mathbb{P}^1(t)$, then find the defining equation of C.

Define

$$\gamma := \left\{ \begin{array}{ll} \alpha^2 & \text{for case 1} \\ \alpha + \frac{e}{\alpha} & \text{for case 2} \end{array} \right. ,$$

$$\Phi := \begin{pmatrix} \gamma & b \\ 1 & -\gamma \end{pmatrix}.$$

Denote the determinant of Φ by $D = \det \Phi$; then

$$b \quad = \quad D - \gamma^2.$$

Denote the map induced by Φ by $\phi : \mathbb{P}^1(u) \longrightarrow \mathbb{P}^1(u)$; then the $(2,2)$-covering has the covering group:

$$\begin{aligned} \Gamma \quad &:= \quad cov\left(\mathbb{P}^1(u)/\mathbb{P}^1(t)\right) \\ &= \quad \{1, \phi, {}^{\sigma}\phi, {}^{\sigma^2}\phi\}, \\ {}^{\sigma}\phi \cdot \phi \quad &= \quad \phi \cdot {}^{\sigma}\phi = {}^{\sigma^2}\phi. \end{aligned}$$

Thus, we can show that $\mathbb{P}^1(s) = \mathbb{P}^1(u)/ < {}^{\sigma}\phi >$ and further $\mathbb{P}^1(t) = \mathbb{P}^1(u)/\Gamma$.

In fact,

$$D \quad = \quad (\gamma - \gamma^q)\left(\gamma - \gamma^{q^2}\right).$$

Thus,

$$\begin{aligned} t \quad &= \quad u + \phi(u) + {}^{\sigma}\phi(u) + {}^{\sigma^2}\phi(u) \\ &:= \quad \frac{F(u)}{N_{k_3/k}(u - \gamma)}, \\ F(u) \quad &= \quad t^4 - 2\mathrm{Tr}_{k_3/k}(\gamma^{q+1})t^2 + 8N_{k_3/k}(\gamma)u - 2\mathrm{Tr}_{k_3/k}(\gamma)N_{k_3/k}(\gamma) + \mathrm{Tr}_{k_3/k}(\gamma^{2q+2}). \end{aligned}$$

Define

$$X := u, \qquad Y := N_{k_3/k}(X - \gamma)x,$$

the defining equation of C is then obtained as

$$C: \quad Y^2 = F(X)N_{k_3/k}(X - \gamma)$$

in the first case.

The defining equation of C in the second case is

$$C: \quad Y^2 - F(X)Y + eN_{k_3/k}(X - \gamma)^2 = 0.$$

In fact, the ramification points of C in the second case are the zeros of the discriminant

$$\mathrm{disc} = F(X)^2 - 4eN_{k_3/k}(X - \gamma).$$

□

3 Density of E with $(2,2,2)$-hyperelliptic coverings $C/\mathbb{P}^1$

Lemma 5. *The number of E with $(2,2,2)$-hyperelliptic coverings $C/\mathbb{P}^1$ is*

$$\#\{E\} = q^2 - 2q + 3.$$

Proof: Given an E such that $C/\mathbb{P}^1$ is a $(2,2,2)$-covering, there is an elliptic curve E' which is the quotient of an order 2 element in $\mathrm{cov}(C/E)$. Since the density analysis is independent of the choice of this element, we choose it to be ${}^{\sigma^2}\phi$; then, $E' = C/{}^{\sigma^2}\phi$. Here we also assume $\mathbb{P}^1(t) = \mathbb{P}^1(s)/{}^{\sigma}\phi$.

Thus we have the following diagram with C a $(2,2)$-hyperelliptic covering of $\mathbb{P}^1(x)$, where E' is unique given C/E and when ${}^{\sigma^2}\phi$ is chosen. Then, we can count the number of E by counting the number of E', up to $\mathrm{PGL}_2(k)$ actions.

$$\begin{tikzcd}
 & & C \arrow[dl, "2"'] \arrow[dr, "2"] & \\
 & E' \arrow[dl, "2"'] \arrow[d, "2"] \arrow[dr, "2"] & & \mathbb{P}^1(u) \arrow[dl, "2"] \\
\mathbb{P}^1(x) \arrow[dr, "2"'] & E \arrow[d, "2"] & \mathbb{P}^1(s) \arrow[dl, "2"] & \\
 & \mathbb{P}^1(t) & &
\end{tikzcd}$$

We assume $\mathbb{P}^1(x)$ is defined by

$$\mathbb{P}^1(x): \quad x^2 = at^2 + bt, \quad a \in k, b \in k^\times;$$

since $\mathrm{char}(k) \neq 2$, one can always cancel the cross term xt, and remove the constant term by a $\mathrm{PGL}_2(k)$-action.

Denote

$$\phi = \begin{pmatrix} \gamma & b \\ 1 & -\gamma \end{pmatrix}.$$

Since $\mathbb{P}^1(s) = \mathbb{P}^1(u)/\ {}^{\sigma^2}\phi,\ \mathbb{P}^1(t) = \mathbb{P}^1(s)/\ {}^{\sigma}\phi$,

$$\begin{aligned}
t &= s + {}^{\sigma}\phi(s) \\
s &= u + {}^{\sigma^2}\phi(u) \\
{}^{\sigma}\phi(s) &= \frac{(\gamma^q u + b^q)(u-\gamma) + (u-\gamma^q)(\gamma u + b)}{(u-\gamma^q)(u-\gamma)}.
\end{aligned}$$

Using the relation ${}^{\sigma^2}\phi = \phi \cdot {}^{\sigma}\phi$, one can show that

$$b = \gamma^{q+q^2} - \gamma^{1+q} - \gamma^{1+q^2}.$$

Thus,

$$ {}^{\sigma}\phi(s) \quad = \quad \frac{(\gamma+\gamma^q)s - 4\gamma^{1+q}}{s-(\gamma+\gamma^q)}, $$

or the matrix of ${}^{\sigma}\phi$ on $\mathbb{P}^1(s)$

$$ {}^{\sigma}\phi\Big|_{\mathbb{P}^1(s)} = \begin{pmatrix} \gamma+\gamma^q & -4\gamma^{1+q} \\ 1 & -(\gamma+\gamma^q) \end{pmatrix}. $$

Therefore, one has

$$ t \quad = \quad \frac{s^2 - 4\gamma^{1+q}}{s-(\gamma+\gamma^q)}. $$

Thus, E' is defined by

$$ E' : \quad y^2 = a\left(\frac{s^2 - 4\gamma^{1+q}}{s-(\gamma+\gamma^q)}\right)^2 + b\left(\frac{s^2 - 4\gamma^{1+q}}{s-(\gamma+\gamma^q)}\right). $$

Here $b \neq 0$; otherwise E' is genus zero.
When $a \neq 0$

$$ \begin{aligned} E' : ((s-\gamma-\gamma^q)y)^2 \quad &= \quad a(s^2 - 4\gamma^{1+q})(s^2 - 4\gamma^{1+q} + d(s-\gamma-\gamma^q)) \\ d \quad &:= \quad b/a \in k^\times \end{aligned} $$

Since the action of $\mathrm{PGL}_2(k)$ on $k_3 \setminus k$ is transitive, all $\gamma \in k_3 \setminus k$ belong to one single orbit of the $\mathrm{PGL}_2(k)$-action.

Thus, E' is only determined by the value of (a, d) up to the $\mathrm{PGL}_2(k)$-action. The number of E' equals to $\#\{(a,d) | a \in k^\times, d \in k^\times\} = (q-1)^2$.
When $a = 0$

$$ E' : ((s-\gamma-\gamma^q)y)^2 \quad = \quad b(s^2 - 4\gamma^{1+q})(s-\gamma-\gamma^q) $$

$$ b \in k^\times \equiv \begin{cases} 1 & b \in (k_3^\times)^2 \\ -1 & b \notin (k_3^\times)^2 \end{cases} $$

Again by the transitivity of the $\mathrm{PGL}_2(k)$-action on $k_3 \setminus k$, E' only has two orbits.

Therefore,

$$ \#\{E/PGL_2(k)\} = (q-1)^2 + 2 = q^2 - 2q + 3. $$

□

4 Type I curves

4.1 Legendre form over k_3 of Type I curves

Lemma 6. *A Type I elliptic curve E is k_3-isomorphic to*

$$E \underset{/k_3}{\simeq} \quad y^2 = x(x-1)(x-\lambda), \tag{13}$$

$$\lambda = \tfrac{(\beta-\alpha^q)(\beta^q-\alpha)}{(\beta-\alpha)(\beta^q-\alpha^q)}. \tag{14}$$

Proof:

Define

$$\begin{aligned} A &:= \begin{pmatrix} 1 & -\alpha^q \\ 1 & -\alpha \end{pmatrix}, \\ t &:= A \cdot x = \frac{x-\alpha^q}{x-\alpha}. \end{aligned}$$

Since

$$\begin{aligned} A^{-1} &= \frac{1}{-\alpha+\alpha^q} \begin{pmatrix} -\alpha & \alpha^q \\ -1 & 1 \end{pmatrix} \\ &\equiv \begin{pmatrix} \alpha & -\alpha^q \\ 1 & -1 \end{pmatrix} \bmod k^\times, \end{aligned}$$

one has

$$x = \begin{pmatrix} 1 & -\alpha^q \\ 1 & -\alpha \end{pmatrix}^{-1} \cdot t = \begin{pmatrix} \alpha & -\alpha^q \\ 1 & -1 \end{pmatrix} \cdot t = \frac{\alpha t - \alpha^q}{t-1}.$$

$$\begin{aligned} x-\alpha &= \frac{\alpha-\alpha^q}{t-1}, \\ x-\alpha^q &= \frac{\alpha-\alpha^q}{t-1} t, \\ x-\beta &= \frac{\alpha-\beta}{t-1}\left(t - \frac{\beta-\alpha^q}{\beta-\alpha}\right), \\ x-\beta^q &= \frac{\alpha-\beta^q}{t-1}\left(t - \frac{\beta^q-\alpha^q}{\beta^q-\alpha}\right). \end{aligned}$$

Substituting the above equations into (5), one obtains

$$\left((t-1)^2 y\right)^2 = (\alpha-\alpha^q)^2 (\alpha-\beta)(\alpha-\beta^q)\, t \left(t - \frac{\beta-\alpha^q}{\beta-\alpha}\right)\left(t - \frac{\beta^q-\alpha^q}{\beta^q-\alpha}\right). \tag{15}$$

Now, define

$$u := \frac{\beta^q-\alpha}{\beta^q-\alpha^q}\, t.$$

Then, (15) becomes

$$\left((t-1)^2y\right)^2 = (\alpha-\alpha^q)^2\,(\alpha-\beta)\,(\alpha-\beta^q)\left(\frac{\beta^q-\alpha^q}{\beta^q-\alpha}\right)^3 u(u-1)\left(u-\frac{\beta^q-\alpha}{\beta^q-\alpha^q}\frac{\beta-\alpha^q}{\beta-\alpha}\right),$$

$$\left((t-1)^2y\right)^2 = \frac{(\alpha-\alpha^q)^2\,(\beta-\alpha)\,(\beta^q-\alpha^q)^3}{(\beta^q-\alpha)^2}u(u-1)\left(u-\frac{\beta^q-\alpha}{\beta^q-\alpha^q}\frac{\beta-\alpha^q}{\beta-\alpha}\right).$$

The Legendre form for Type I curves is obtained after defining

$$\begin{aligned} e &:= \frac{(\alpha-\alpha^q)^2\,(\beta-\alpha)\,(\beta^q-\alpha^q)^3}{(\beta^q-\alpha)^2} \\ &= \frac{(\alpha-\alpha^q)^2\,(\beta^q-\alpha^q)^2}{(\beta^q-\alpha)^2}\,(\beta-\alpha)^{1+q} \\ &\equiv 1 \bmod \left(k_3^\times\right)^2, \\ \lambda &:= \frac{\beta^q-\alpha}{\beta^q-\alpha^q}\frac{\beta-\alpha^q}{\beta-\alpha}. \end{aligned}$$

□

4.2 Characteristics of Type I curves

The action of $PGL_2(k)$ on $k_3\setminus k$ induces the following action on the set $\{\alpha,\beta\}$:

$$\{\alpha,\beta\} \quad\longmapsto\quad \{A\cdot\alpha, A\cdot\beta\}, \qquad \forall A\in GL_2(k).$$

This action transforms E in (5) to a new elliptic curve

$$E' : y^2 \quad = \quad (x-A\cdot\alpha)\,(x-A\cdot\alpha^q)\,(x-A\cdot\beta)\,(x-A\cdot\beta^q) \qquad (16)$$

which also has a Legendre form the same as (13) with

$$\lambda' \quad := \quad \frac{(A\cdot\beta-A\cdot\alpha^q)(A\cdot\beta^q-A\cdot\alpha)}{(A\cdot\beta-A\cdot\alpha)(A\cdot\beta^q-A\alpha^q)}. \qquad (17)$$

Then, it is easy to see

$$\lambda=\lambda'$$

or the Legendre forms are invariant under this action.

According to the above lemma and the transitivity of the action of $PGL_2(k)$ on $k_3\setminus k$, we can assume that there is an $A\in GL_2(k)$ and an $\epsilon\in k_3\setminus k$ such that $\alpha=A\cdot\epsilon$. Therefore, the first element in the pair $\{\alpha,\beta\}$ can be fixed to be some $\epsilon\in k_3\setminus k$. Hereafter we consider only the pairs $\{\epsilon,\beta\}$ and the corresponding values of λ.

From now on we assume Type I curves to be

$$E: \quad y^2 = (x-\epsilon)\,(x-\epsilon^q)\,(x-\beta)\,(x-\beta^q)\,, \tag{18}$$

$$\epsilon, \beta \in k_3 \setminus k, \quad \#\{\epsilon, \epsilon^q, \beta, \beta^q\} = 4, \tag{19}$$

$$\lambda = \tfrac{\beta-\epsilon^q}{\beta-\epsilon} \cdot \tfrac{\beta^q-\epsilon}{\beta^q-\epsilon^q}. \tag{20}$$

Now, we define

$$\mu := \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \cdot \lambda; \tag{21}$$

then, since $\lambda \neq 0, 1, \infty$, we have $\mu \neq \epsilon, \epsilon^q, \infty$.

Define here two matrices A and B,

$$A =: \begin{pmatrix} -\mu + \epsilon + \epsilon^q & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix}, \tag{22}$$

$$B :=^{\sigma^2}\! A \ {}^{\sigma}\! A \ A. \tag{23}$$

Then, we have

Lemma 7.

1. *Given λ, there exists some β such that* (20) *holds if and only if*

$$A \cdot \beta = \beta^q. \tag{24}$$

2. *The above condition is equivalent to*

$$B \cdot \beta = \beta. \tag{25}$$

Then, one can find β from λ as the solutions of the quadratic equation obtained from (25)*.*

3. *When such a β exists, B is not upper triangular:*

$$B \ \not\equiv \ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \bmod k_3^\times \tag{26}$$

since $\mu \neq \epsilon, \epsilon^q$.

Thus, the quadratic equation in 2. does not degenerate to a linear equation, or there are always two β's given one λ.

4. *Denote the discriminant of the quadratic equation in 2. by*

$$\Delta \ := \ (\mathit{Tr}B)^2 - 4(\det B) \quad \in k, \tag{27}$$

$$\Delta \ = \ N(\varepsilon - \varepsilon^q)^2 N\left(\frac{1}{\lambda - 1}\right)^2 \{[\mathit{Tr}(\lambda) - 1]^2 - 4N(\lambda)\}. \tag{28}$$

Given λ, there exists some β satisfying (20) *if and only if $\Delta \in k^2$.*

5.

$$\Delta = 0 \Longrightarrow \begin{cases} \exists G \in GL_2(k), \quad G^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod} k^\times) \\ \beta = G \cdot \epsilon \end{cases} \tag{29}$$

The number of β when $\Delta = 0$ is q^2.

Remark 1. *Given a random elliptic curve E in Legendre form, one can easily test if it is of Type I by solving the quadratic equation defined by* (25)*.*

Proof of Lemma 7.1:

From (20),

$$\lambda = \frac{\beta - \epsilon^q}{\beta - \epsilon} \cdot \frac{\beta^q - \epsilon}{\beta^q - \epsilon^q},$$

one has

$$0 \quad = \quad (1-\lambda)\beta^{1+q} + (\lambda\epsilon - \epsilon^q)\beta^q + (\lambda\epsilon^q - \epsilon)\beta + (1-\lambda)\epsilon^{1+q}.$$

Since $\lambda \neq 0, 1, \infty$,

$$0 \quad = \quad \beta^{1+q} - \frac{\lambda\epsilon - \epsilon^q}{\lambda - 1}\beta^q - \frac{\lambda\epsilon^q - \epsilon}{\lambda - 1}\beta + \epsilon^{1+q}.$$

Define

$$\mu \quad := \quad \begin{pmatrix} \epsilon & -\epsilon^q \\ 1 & -1 \end{pmatrix} \cdot \lambda, \tag{30}$$

$$\nu \quad := \quad \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \cdot \lambda. \tag{31}$$

Then, one has from (30)

$$\begin{aligned} 0 &= \beta^{1+q} - \mu\beta^q - \nu\beta + \epsilon^{1+q} \\ &= \beta^q(\beta - \mu) - \nu\beta + \epsilon^{1+q}, \\ \beta^q &= \frac{\nu\beta - \epsilon^{1+q}}{\beta - \mu} \\ &= \begin{pmatrix} \nu & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix} \cdot \beta. \end{aligned}$$

On the other hand, from the definitions of μ and ν,

$$\begin{aligned} \nu &= \begin{pmatrix} \epsilon^q & -\epsilon \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -\epsilon^q \\ 1 & -\epsilon \end{pmatrix} \cdot \mu \\ &= -\mu + \epsilon + \epsilon^q. \end{aligned}$$

Therefore, if one defines

$$A \quad := \quad \begin{pmatrix} -\mu + \epsilon + \epsilon^q & -\epsilon^{1+q} \\ 1 & -\mu \end{pmatrix},$$

then, given λ, there is a β such that (20) holds if and only if

$$\beta^q = A \cdot \beta.$$

Proof of Lemma 7.2:
(25)$\Longleftarrow$ (24): Easy.
(25)$\Longrightarrow$ (24):

Assume the two solutions of (25) are β and γ.

$$B \cdot \beta = \beta, \qquad B \cdot \gamma = \gamma. \tag{32}$$

Since

$$\begin{aligned} ({}^{\sigma^2}A\ {}^{\sigma}A\ A) \cdot \beta &= \beta, \\ (A\ {}^{\sigma^2}A\ {}^{\sigma}A) \cdot \beta^q &= \beta^q, \\ ({}^{\sigma^2}A\ {}^{\sigma}A) \cdot \beta^q &= A^{-1} \cdot \beta^q, \\ ({}^{\sigma^2}A\ {}^{\sigma}A\ A)(A^{-1} \cdot \beta^q) &= A^{-1} \cdot \beta^q, \\ B \cdot (A^{-1} \cdot \beta^q) &= A^{-1} \cdot \beta^q. \end{aligned}$$

Therefore, either

$$A^{-1} \cdot \beta^q = \beta \qquad \textit{i.e.} \qquad A \cdot \beta = \beta^q, \tag{33}$$

or

$$A^{-1} \cdot \beta^q = \gamma \qquad \textit{i.e.} \qquad A \cdot \gamma = \beta^q. \tag{34}$$

The latter case is when the action of A interchanges the two solutions; i.e.,

$$A \cdot \gamma = \beta^q, \qquad A \cdot \beta = \gamma^q. \tag{35}$$

Then,

$$({}^{\sigma}A\ A) \cdot \beta = {}^{\sigma}A \cdot \gamma^q = (A \cdot \gamma)^q = \beta^{q^2}, \tag{36}$$

$$({}^{\sigma^2}A\ {}^{\sigma}A\ A) \cdot \beta = {}^{\sigma^2}A \cdot \beta^{q^2} = (A \cdot \beta)^{q^2} = \gamma. \tag{37}$$

This means

$$B \cdot \beta = \gamma, \qquad \textit{i.e.} \qquad \beta = \gamma. \tag{38}$$

Proof of Lemma 7.3: See Appendix 1.

Proof of Lemma 7.4:

Denote

$$B := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad c \neq 0,$$

then, values of β are solutions of

$$cx^2 + (d - a)x - b = 0.$$

Hence, given λ, there exist at most two β satisfying $B \cdot \beta = \beta$.

Denote the discriminant of the above quadratic equation by

$$\Delta := (\mathrm{Tr} B)^2 - 4(\det B) \quad (\in k).$$

Then,

$$\begin{aligned} \#\{\beta\} = 2 \quad &\text{iff} \quad \Delta \in (k^\times)^2, && (39)\\ \#\{\beta\} = 1 \quad &\text{iff} \quad \Delta = 0, && (40)\\ \#\{\beta\} = 0 \quad &\text{iff} \quad \Delta \notin (k^\times)^2. && (41) \end{aligned}$$

The explicit formula (28) for Δ is obtained in Appendix 2.

Proof of Lemma 7.5:

Define the matrix mapping β to ϵ to be $G \in GL_2(k)$, which is unique modulo $k^\times$. Denote the image of ϵ under G by γ, i.e.:

$$\exists!\ G \in PGL_2(k), \quad s.t. \quad G \cdot \beta = \epsilon, \quad G \cdot \epsilon =: \gamma. \tag{42}$$

Then,

$$\begin{aligned} G \cdot \beta^q &= (G \cdot \beta)^q = \epsilon^q, && (43)\\ G \cdot \epsilon^q &= (G \cdot \epsilon)^q = \gamma^q. && (44) \end{aligned}$$

Thus, under the action of G, one obtains another elliptic curve E'' which is isomorphic to E:

$$E'' : y^2 = (x - \epsilon)(x - \epsilon^q)(x - \gamma)(x - \gamma^q), \tag{45}$$

which has the same λ as E due to the invariance of λ under the $\mathrm{PGL}_2(k)$-action.

When $\Delta = 0$, there is only one β so one has $\gamma = \beta$.

Thus,

$$\begin{aligned} G \cdot \beta &= \epsilon, \qquad G \cdot \epsilon = \beta, && (46)\\ G^2 \cdot \beta &= \beta. && (47) \end{aligned}$$

Since $\beta \in k_3 \setminus k$,

$$G^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod k^\times, \tag{48}$$

but $G \not\equiv I \bmod k^\times$, thus $\mathrm{Tr}(G) = 0$.

Denote

$$G = \left(\begin{array}{cc} a & b \\ c & -a \end{array} \right).$$

When $c = 0$, one can assume $a = 1$, thus the number of $\beta = G \cdot \epsilon = -\epsilon - b$ equals $\#\{b \in k\} = q$.

When $c \neq 0$, the number of

$$\beta = G \cdot \epsilon = \frac{a\epsilon + b}{\epsilon - a} \tag{49}$$

equals $\#\{(a, b) \in k^2 | a^2 + b \neq 0\} = q(q - 1)$.

Thus, the number of β when $\Delta = 0$ is q^2. □

5 Classification of the $\mathbf{PGL}_2(k)$-actions on Type I curves

Recall that for Type I curves,

$$E \underset{/k_3}{\simeq} \quad y^2 = x(x-1)(x-\lambda), \tag{50}$$

$$\lambda \quad = \quad \lambda(\alpha, \beta) = \frac{\beta^q - \alpha}{\beta^q - \alpha^q}\frac{\beta - \alpha^q}{\beta - \alpha}, \qquad \beta \in k_3 \setminus k, \ \beta \neq \alpha, \alpha^q, \alpha^{q^2}. \tag{51}$$

Since the action of $\mathrm{PGL}_2(k)$ on k_3 is transitive and fixed-point free, one can fix $\alpha = \varepsilon \in k_3 \setminus k$, then,

$$\lambda = \lambda(\varepsilon, \beta) = \frac{(\beta^q - \varepsilon)(\beta - \varepsilon^q)}{(\beta - \varepsilon)^{q+1}}, \qquad \beta \in k_3 \setminus k, \ \beta \neq \varepsilon, \varepsilon^q, \varepsilon^{q^2}.$$

As shown before, λ is $\mathrm{PGL}_2(k)$-invariant:

$$\forall A \in PGL_2(k), \qquad \lambda(A\alpha, A\beta) = \lambda(\alpha, \beta). \tag{52}$$

We now define a double-sided action on $A \in GL_2(k)$ as follows.

$$PGL_2(k) \curvearrowright GL_2(k) \curvearrowleft PGL_2(k).$$

In particular,

$$T \cdot \beta := TAT^{-1}T\varepsilon, \quad T \in GL_2(k).$$

It can be shown that an $A \in GL_2(k)$ under the above action has three representatives as follows:

1.
$$A_1 = \left(\begin{array}{cc} a & 0 \\ 0 & 1 \end{array} \right), \qquad a \neq 0, 1;$$

2.

$$A_2 = \left(\begin{array}{cc} a & e \\ 1 & a \end{array} \right), \qquad \eta^2 = e \in k^\times \setminus (k^\times)^2;$$

3.

$$A_3 = \left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right).$$

6 Density of Type I curves with hyperelliptic coverings

First, we consider the matrix Θ in Lemma 4 under the double-sided $\mathrm{PGL}_2(k)$-action. In fact, Θ can be represented by the following matrices under the double-sided $\mathrm{PGL}_2(k)$-action.

$$\begin{array}{rrcl} (i) & \Theta_1 & = & \left(\begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right), \\ (ii) & \Theta_2 & = & \left(\begin{array}{cc} 0 & e \\ 1 & 0 \end{array} \right), \qquad \exists \eta \in k_2,\ \eta^2 = e \in k^\times \setminus \left(k^\times\right)^2. \end{array}$$

Since

$$\lambda = \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)^{1+q}} \neq 0, 1, \qquad \beta \in k_3 \setminus k,\ \ \beta \neq \alpha, \alpha^q, \alpha^{q^2},$$

one has β_1 and β_2 corresponding to the two representatives Θ_1 and Θ_2.

$$\begin{aligned} \beta_1 &= \Theta_1 \cdot \alpha = -\alpha, & (53) \\ \lambda_1 &= \frac{(\alpha + \alpha^q)^2}{4\alpha^{1+q}}, & (54) \\ \beta_2 &= \Theta_2 \cdot \alpha = \frac{e}{\alpha}, & (55) \\ \lambda_2 &= \frac{(e - \alpha^{1+q})^2}{(e - \alpha^2)^{1+q}}. & (56) \end{aligned}$$

Lemma 8. *The covering curve C/k of a Type I elliptic curve E is hyperelliptic if and only if the discriminant Δ in* (27) *of Lemma 7 equals zero.*

Proof:

By Lemma 7.5 and Lemma 4 one knows that $\Delta = 0$ implies C/k is a hyperelliptic covering curve of E.

Now, we prove the other direction. According to Lemma 4 and Appendix 3, we know that λ is either λ_1 in (54) or λ_2 in (56) when C/k is hyperelliptic.

Substituting λ_i into (28), one finds that $\Delta(\lambda_i) = 0, i = 1, 2$. □

Remark 2. *Using the formula for Δ in* (28)*, values of λ such that C is a hyperelliptic covering of E can be calculated by solving the equation $\Delta = 0$.*

Lemma 9. *For λ in the Legendre forms of Type I curves,*

$$\#\{\lambda \mid C/\mathbb{P}^1 : \textit{hyperelliptic}\} = q^2.$$

Proof: According to Lemma 8, λ defines a Type I curve E such that C/k is hyperelliptic if and only if $\Delta = 0$.

On the other hand, by Lemma 7.4, the correspondence between β and λ is one to one in the hyperelliptic covering case, and by Lemma 7.5, the number of β such that $D = 0$ equals q^2. Thus, we know that this is also the number of λ defining hyperelliptic C. □

7 Density of Type I curves with non-hyperelliptic coverings

Since $\beta \in k_3 \setminus k$, $\beta \neq \alpha, \alpha^q, \alpha^{q^2}$, one knows that

$$\#\{\beta\} = q^3 - q - 3.$$

In fact, there is a symmetry between ε and β:

$$\lambda(\varepsilon, \beta) = \lambda(\beta, \varepsilon).$$

When C is non-hyperelliptic, the correspondence between β and λ is two to one. When C is hyperelliptic, by Lemma 8, $\Delta = 0$; then β and λ are one to one. By Lemma 9, the number of such λ is q^2.

Thus, defining the number of Type I curves with non-hyperelliptic coverings as

$$\nu := \#\{\lambda \ s.t.\ C/\mathbb{P}^1 : \text{ non-hyperelliptic}\},$$

one has

$$\#\{\beta\} = 2\nu + q^2 = q^3 - q - 3.$$

Therefore,

$$\nu = \#\{\lambda\} = \frac{1}{2}(\#\{\beta\} - q^2) = \frac{1}{2}(q^3 - q^2 - q - 3).$$

8 Type II curves

8.1 Legendre form over k_3 of Type II curves

Lemma 10. *For a Type II elliptic curve E/k_3,*

$$E/k_3 : \quad y^2 = (x - \alpha)\left(x - \alpha^{q^3}\right)(x - \alpha^q)\left(x - \alpha^{q^4}\right),$$
$$\alpha \in k_6 \setminus \{k_2 \cup k_3\},$$

there is a k_6-isomorphism φ_0 mapping E/k_3 to E_0/k_3:

$$\varphi_0 : \ E/k_3 \ \underset{/k_6}{\xrightarrow{\simeq}} \ E_0/k_3 : \qquad y^2 = \epsilon x(x-1)(x-\mu), \tag{57}$$

$$\begin{cases} \mu = \left(\frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^3}}\right)^{1+q^3} = N_{k_6/k_3}\left(\frac{\alpha^q-\alpha}{\alpha^q-\alpha^{q^3}}\right), \\ \epsilon \equiv N_{k_6/k_3}\left(\alpha-\alpha^{q^4}\right) \bmod \left(k_6^\times\right)^2 \\ \quad \equiv 1 \bmod \left(k_6^\times\right)^2. \end{cases} \tag{58}$$

Furthermore, there is another k_6-isomorphism φ_1 mapping E/k_3 to E_1/k_3:

$$\varphi_1 : \ E/k_3 \ \underset{\simeq}{\xrightarrow{/k_6}} \ E_1/k_3 : \quad v^2 \quad = \quad u(u-1)(u-\mu). \tag{59}$$

Proof: Let

$$A := \begin{pmatrix} 1 & -\alpha^{q^3} \\ 1 & -\alpha \end{pmatrix}$$

and

$$t := A \cdot x = \frac{x-\alpha^{q^3}}{x-\alpha},$$

then

$$x = A^{-1}\cdot t = \begin{pmatrix} \alpha & -\alpha^{q^3} \\ 1 & -1 \end{pmatrix} \cdot t = \frac{\alpha t - \alpha^{q^3}}{t-1}.$$

The factors on the RHS in the equation of the Type II curve E become

$$\begin{aligned} x-\alpha &= \frac{\alpha-\alpha^{q^3}}{t-1}, \\ x-\alpha^{q^3} &= \frac{\alpha-\alpha^{q^3}}{t-1}t, \\ x-\alpha^q &= \frac{\alpha-\alpha^q}{t-1}\left(t-\frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\right), \\ x-\alpha^{q^4} &= \frac{\alpha-\alpha^{q^4}}{t-1}\left(t-\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\right). \end{aligned}$$

Then, E becomes

$$y^2 \quad = \quad \frac{(\alpha-\alpha^{q^3})^2(\alpha-\alpha^q)(\alpha-\alpha^{q^4})}{(t-1)^4}\, t\left(t-\frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\right)\left(t-\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\right).$$

Let

$$t := \frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\, u, \tag{60}$$

then

$$\left((t-1)^2 y\right)^2 \quad = \quad \frac{(\alpha-\alpha^{q^3})^2(\alpha-\alpha^{q^4})\left(\alpha^{q^3}-\alpha^q\right)^3}{\left(\alpha-\alpha^q\right)^2} u\left(u-1\right)\left(u-\mu\right).$$

Define

$$\begin{aligned} \mu &:= \frac{(\alpha-\alpha^q)}{(\beta-\alpha^q)}\frac{(\beta-\beta^q)}{(\alpha-\beta^q)} \\ &= N_{k_6/k_3}\left(\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right) \in k_3, \end{aligned}$$

$$\epsilon \;:\equiv\; N_{k_6/k_3}(\alpha-\alpha^{q^4}) \bmod \left(k_6^{\times}\right)^2,$$

and replace $(t-1)^2 y$ by y, u by x; then one has E_0/k_3 in (57).

Next, define

$$\begin{aligned} v &:= \frac{(t-1)^2}{\sqrt{e}}y && (61)\\ &= \frac{(t-1)^2\,(\alpha-\alpha^q)}{(\alpha-\alpha^{q^3})\left(\alpha^{q^3}-\alpha^q\right)(\alpha-\alpha^{q^4})^{\frac{1+q^3}{2}}}y, && (62) \end{aligned}$$

then one obtains

$$E_1/k_3: \qquad v^2 \;=\; u(u-1)(u-\mu). \qquad (63)$$

□

Lemma 11.

$$E \overset{/k_3}{\simeq} E_0 \overset{/k_3}{\simeq} E_2$$

where

$$\begin{aligned} E_0/k_3: \quad y^2 &= N_{k_6/k_3}(\alpha-\beta^q)x(x-1)(x-\mu), && (64)\\ E_2/k_3: \quad y^2 &= (\alpha-\beta)^{q+1}x(x-1)(x-\lambda), && (65)\\ \lambda &:= \frac{1}{1-\mu} = \frac{(\beta-\alpha^q)(\beta^q-\alpha)}{(\beta-\alpha)^{q+1}}, \qquad \beta=\alpha^{q^3}. && (66) \end{aligned}$$

$$\textit{Here} \quad \begin{cases} (\alpha-\beta)^{q+1} \in (k_3^{\times})^2 & \textit{when } q \not\equiv 1 \bmod 4 \\ (\alpha-\beta)^{q+1} \notin (k_3^{\times})^2 & \textit{when } q \equiv 1 \bmod 4. \end{cases}$$

Proof:

We prove that E_0 is isomorphic to E_2 as follows. Define

$$x := \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \cdot s = 1 - \frac{1}{s}.$$

Then,

$$\begin{aligned} y^2 &= N_{k_6/k_3}(\alpha-\beta^q)x(x-1)(x-\mu) \\ &= (\alpha-\beta)^{q+1}\frac{1}{s^4}s\,(s-1)\left(s-\frac{1}{1-\mu}\right). \end{aligned}$$

Here we have used

$$\mu = \frac{(\alpha^q-\alpha)(\beta^q-\beta)}{(\alpha^q-\beta)(\beta^q-\alpha)}, \qquad \mu - 1 = \frac{(\alpha-\beta)^{q+1}}{(\alpha^q-\beta)(\beta^q-\alpha)}.$$

Now, replace s^2 by y, s by x; one has

$$E_0 \simeq E_2 : y^2 = (\alpha-\beta)^{q+1} x\,(x-1)\left(x - \frac{1}{1-\mu}\right).$$

Since $(\alpha-\beta)^{q+1} \in k_3^{\times}$,

$$\begin{aligned} e^{\frac{q^3-1}{2}} &= \left((\alpha-\beta)^{q+1}\right)^{\frac{q^3-1}{2}} \quad (67)\\ &= (-1)^{\frac{q+1}{2}} \quad (68)\\ &= \begin{cases} +1 & \Longleftrightarrow \quad q \equiv 3 \bmod 4 \\ -1 & \Longleftrightarrow \quad q \equiv 1 \bmod 4, \end{cases} \quad (69) \end{aligned}$$

we know that $e \in (k_3^{\times})^2$ if and only if $q \equiv 3 \bmod 4$. □

8.2 k_3-isomorphism of Type II curves

Here we further consider k_3-isomorphisms of Type II curves and show E is k_3-isomorphic to E_1. For simplicity $\sigma_3 := (\cdot)^{q^3}$.

Let φ_1 be the k_6-isomorphism of E onto E_1:

$$E/k_3 \xrightarrow{\phi_1/k_6} E_1/k_3 = {}^{\sigma_3}E_1, \tag{70}$$

then we have an k_6-isomorphism of E_1:

$$\psi :={}^{\sigma_3} \varphi_1 \circ \varphi_1^{-1} \ /k_6 : \quad E_1 \xrightarrow{\simeq} E_1.$$

$$\begin{tikzcd} & E \arrow[dl, "\varphi_1"'] \arrow[dr, "{}^{\sigma_3}\varphi_1"] & \\ E_1 \arrow[rr, "\psi={}^{\sigma_3}\varphi_1\circ\varphi_1^{-1}"'] & & {}^{\sigma_3}E_1 \end{tikzcd}$$

8.2.1 $\psi^*(\omega) = -\varepsilon(\omega),\ \varepsilon = \pm 1$

We first consider the k_6/k_3-conjugate ${}^{\sigma^3}E_1$ of E_1 under the action of $\sigma_3 = (\cdot)^{q^3}$.

The variable changes under ϕ_1 :

$$u \longmapsto t = \frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\, u \longmapsto x = A \cdot t = \begin{pmatrix} \alpha & -\alpha^{q^3} \\ 1 & -1 \end{pmatrix} \cdot \frac{\alpha^{q^3}-\alpha^q}{\alpha-\alpha^q}\, u \tag{71}$$

have the Galois conjugates below, where $u' :=^{\sigma_3} u$:

$$u' \longmapsto^{\sigma_3} t = \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u \longmapsto x =^{\sigma_3} A \cdot\ ^{\sigma_3}t = \begin{pmatrix} \alpha^{q^3} & -\alpha \\ 1 & -1 \end{pmatrix} \cdot \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u'. \quad (72)$$

From (71) and (72),

$$x = \begin{pmatrix} \alpha^{q^3} & -\alpha \\ 1 & -1 \end{pmatrix} \cdot \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u', \quad (73)$$

$$\begin{aligned} \frac{\alpha - \alpha^{q^4}}{\alpha^{q^3} - \alpha^{q^4}}\ u' &= \begin{pmatrix} \alpha^{q^3} & -\alpha \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha & -\alpha^{q^3} \\ 1 & -1 \end{pmatrix} \cdot \frac{\alpha^{q^3} - \alpha^{q}}{\alpha - \alpha^{q}}\ u && (74) \\ &= \frac{\alpha - \alpha^{q}}{\left(\alpha^{q^3} - \alpha^{q}\right) u}, && (75) \end{aligned}$$

$$u' = \frac{\alpha^{q^3} - \alpha^{q^4}}{\alpha - \alpha^{q^4}} \frac{\alpha - \alpha^{q}}{\alpha^{q^3} - \alpha^{q}} \frac{1}{u} = \frac{\lambda}{u}. \quad (76)$$

The conjugate of E_1 is

$$\begin{aligned} ^{\sigma_3}E_1 : \quad (v')^2 &= u'(u'-1)(u'-\lambda) && (77) \\ &= \frac{\lambda^2}{u^4}\ u\,(u-1)\,(u-\lambda) && (78) \end{aligned}$$

or

$$\left(\frac{u^2}{\lambda} v'\right)^2 = u\,(u-1)\,(u-\lambda)\,. \quad (79)$$

Comparing with E_1, we have

$$\frac{u^2}{\lambda} v' = \pm v, \quad (80)$$

$$v' = \pm \frac{\lambda}{u^2} v = \varepsilon \frac{\lambda}{u^2} v, \quad (81)$$

$$\varepsilon := \pm 1. \quad (82)$$

Consider the differential form on E_1

$$\omega = \frac{du}{v}, \quad (83)$$

then

$$\psi : E_1 \quad \longrightarrow \quad ^{\sigma_3}E_1 \quad (84)$$

induces

$$\begin{aligned} \psi^*(\omega) &= \omega' && (85) \\ &= -\frac{\frac{\lambda}{u^2}}{\varepsilon \frac{\lambda}{u^2} v} du && (86) \\ &= -\varepsilon\omega = \pm\omega. && (87) \end{aligned}$$

8.2.2 Exact expression for ε

Recall that a rational map f over a field K from a group variety G with the group unit e to an Abelian variety A is a homomorphism up to a translation. I.e., there is a homomorphism $f_0 : G \longrightarrow A$ over K such that $f(P) = f_0(P) + f(e)$. Then,

$$f^* \quad = \quad f_0^*,$$

and $f^* = f_0^* = 1$ means

$$f_0 = 1 \quad \textit{or} \quad f(P) = P + Q, \quad Q = f(e).$$

Now, one has

$$\begin{array}{rcl} \psi : E_1 & \overset{\simeq}{\longrightarrow} & {}^{\sigma_3}E_1 \\ P & \longmapsto & \pm P + Q, \qquad Q = \psi(\mathcal{O}) \in E_1(k_3), \\ \omega & \longmapsto & \psi^*(\omega) = -\varepsilon\omega. \end{array}$$

In order to find an exact expression for ε, define

$$y_1 \quad := \quad (t-1)^2 y; \tag{88}$$

then

$$v \quad = \quad \frac{(t-1)^2}{\sqrt{e}} y = \frac{1}{\sqrt{e}} y_1 \tag{89}$$

by the definition of v. Here

$$\frac{1}{\sqrt{e}} \quad = \quad \frac{(\alpha - \alpha^q)}{(\alpha - \alpha^{q^3})\left(\alpha^{q^3} - \alpha^q\right)(\alpha - \alpha^{q^4})^{\frac{1+q^3}{2}}}. \tag{90}$$

From (60), one has

$$t - 1 \quad = \quad \frac{\alpha^{q^3} - \alpha^q}{\alpha - \alpha^q}\left(u - \frac{\alpha - \alpha^p}{\alpha^{q^3} - \alpha^q}\right), \tag{91}$$

$$\frac{(t-1)^2}{\sqrt{e}} \quad = \quad \frac{(\alpha^{q^3} - \alpha^q)\left(u - \frac{\alpha - \alpha^q}{\alpha^{q^3} - \alpha^q}\right)^2}{(\alpha - \alpha^q)(\alpha - \alpha^{q^3})(\alpha - \alpha^{q^4})^{\frac{1+q^3}{2}}}.$$

By (89)

$$y \quad = \quad \frac{\sqrt{e}v}{(t-1)^2} = \frac{(\alpha - \alpha^q)(\alpha - \alpha^{q^3})(\alpha - \alpha^{q^4})^{\frac{1+q^3}{2}}}{(\alpha^{q^3} - \alpha^q)\left(u - \frac{\alpha - \alpha^q}{\alpha^{q^3} - \alpha^q}\right)^2} v. \tag{92}$$

Meanwhile,

$$
\begin{aligned}
y &= {}^{\sigma_3}y && (93)\\
&= \frac{(\alpha^{q^3}-\alpha^{q^4})(\alpha^{q^3}-\alpha)(\alpha^{q^3}-\alpha^q)^{\frac{1+q^3}{2}}}{(\alpha-\alpha^{q^4})\left(u'-\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\right)^2}\,v'. && (94)
\end{aligned}
$$

The second factor in the denominator of (94) can be further calculated using $u' = \lambda/u$ as

$$
\begin{aligned}
u' - \frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}} &= \lambda/u - \frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\\
&= -\frac{\alpha^{q^3}-\alpha^{q^4}}{\alpha-\alpha^{q^4}}\left(1-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\,\frac{1}{u}\right).
\end{aligned}
$$

Substituting this into (94), one obtains

$$
y = \frac{(\alpha-\alpha^{q^4})(\alpha^{q^3}-\alpha)(\alpha^{q^3}-\alpha^q)^{\frac{1+q^3}{2}}}{(\alpha^{q^3}-\alpha^{q^4})}\,\frac{u^2}{\left(u-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right)^2}\,v'. \qquad (95)
$$

Thus,

$$
v' = \frac{(\alpha^{q^3}-\alpha^{q^4})}{(\alpha-\alpha^{q^4})(\alpha^{q^3}-\alpha)(\alpha^{q^3}-\alpha^q)^{\frac{1+q^3}{2}}}\,\frac{\left(u-\frac{\alpha-\alpha^q}{\alpha^{q^3}-\alpha^q}\right)^2}{u^2}\,y. \qquad (96)
$$

Now, substitute y in (92) into the above equation,

$$
\begin{aligned}
v' &= -\frac{(\alpha-\alpha^q)(\alpha^{q^3}-\alpha^{q^4})}{(\alpha^{q^3}-\alpha^q)^{\frac{3+q^3}{2}}}(\alpha-\alpha^{q^4})^{\frac{q^3-1}{2}}\,\frac{v}{u^2}\\
&:= \varepsilon_1\frac{v}{u^2}.
\end{aligned}
$$

The exact value of ε_1 can be obtained as follows.

$$
\varepsilon_1 = -\lambda\left(\frac{\alpha-\alpha^{q^4}}{\alpha^{q^3}-\alpha^q}\right)^{\frac{q^3+1}{2}}.
$$

Therefore,

$$
\begin{aligned}
v' &= \varepsilon_1\frac{v}{u^2}\\
&= -\left(\frac{\alpha-\alpha^{q^4}}{\alpha^{q^3}-\alpha^q}\right)^{\frac{q^3+1}{2}}\frac{\lambda v}{u^2}\\
&= \varepsilon\frac{\lambda v}{u^2}
\end{aligned}
$$

by the definition $v' = \varepsilon\lambda v/u^2$.

Thus,

$$\begin{aligned}
\varepsilon &= -\left(\frac{\alpha-\alpha^{q^4}}{\alpha^{q^3}-\alpha^{q}}\right)^{\frac{q^3+1}{2}} \\
&= -\left(\alpha^{q^3}-\alpha^{q}\right)^{\frac{q^6-1}{2}} \\
&= \pm 1.
\end{aligned}$$

8.2.3 When $\varepsilon = 1,\ \psi^* = -1$

We know already that E is k_6-isomorphic to

$$E_1/k_3: \quad y^2 = x(x-1)(x-\lambda),$$

and

$$\begin{aligned}
\psi^*(\omega) &= -\varepsilon\omega, \\
\varepsilon &= N_{k_6/k_3}(\alpha^{q^4}-\alpha)^{(q^3-1)/2} = \pm 1,
\end{aligned}$$

ψ sends a point P to $-\varepsilon P + Q$, where Q is the point $(0,0)$ of E_1.

First we treat the case where $\varepsilon = 1, \psi^* = -1$. Denote the k_6/k_3-twist E_1' of E_1 by

$$\begin{aligned}
E_1': \ y^2 &= \kappa x(x-1)(x-\lambda), \\
\kappa \in k_3^{\times}, \qquad & \kappa^{\frac{q^3-1}{2}} = -1.
\end{aligned}$$

Define the k_6/k_3-twisting map τ as

$$\begin{aligned}
\tau : E_1 &\overset{\simeq}{\longrightarrow} E_1' \\
(x,y) &\longmapsto (x, \sqrt{\kappa}y), \\
\tau^*(\omega) &= \tau^*\left(\frac{dx}{y}\right) = \frac{dx}{\sqrt{\kappa}y} = \frac{1}{\sqrt{\kappa}}\omega.
\end{aligned}$$

Moreover,

$$\begin{aligned}
{}^{\sigma^3}\tau \circ \tau^{-1}(x,y) &= {}^{\sigma^3}\tau\left(x, \frac{y}{\sqrt{\kappa}}\right) \\
&= \left(x, \kappa^{\frac{q^3-1}{2}} y\right) = (x,-y),
\end{aligned}$$

or

$$\left({}^{\sigma^3}\tau \circ \tau^{-1}(x,y)\right)^* = -1.$$

Then,

$$\begin{array}{rcl} \psi' : E_1' & \longrightarrow & E_1' \\ \psi' & = & {}^{\sigma_3}\tau \circ \psi \circ \tau^{-1} \\ (\psi')^* & = & (\ {}^{\sigma_3}\tau)^* \circ \psi^* \circ \tau^{-*} \\ & = & -(\ {}^{\sigma_3}\tau)^* \circ \tau^{-*} = (-1)^2 = -1. \end{array}$$

Thus, when $\varepsilon = 1, \psi^* = -1$, we can always use E_1' and ψ' instead of E_1 and ψ so that $(\psi')^* = 1$.

Therefore, we need only to discuss the case $\varepsilon = -1$ and $\psi^* = 1$.

8.2.4 Construction of the k_3-isomorphism $\rho/k_3 \colon E \longrightarrow E_1$

Assume $\varepsilon = -1$. Then,

$$\begin{array}{rcl} \psi(P) & = & P + Q, \\ {}^{\sigma^3}\varphi_1 \circ \varphi_1^{-1}(P) & = & P + Q. \end{array}$$

Let

$$\begin{array}{rcl} R & := & \varphi_1^{-1}(P), \\ P & = & \varphi_1(R), \end{array}$$

i.e.,

$$\begin{array}{rcl} {}^{\sigma^3}\varphi_1(R) & = & \varphi_1(R) + Q. \end{array}$$

Lemma 12. *For $Q \in E_1(k_3)$, there exists an*

$$S \in E_1(\overline{k}) \qquad \textit{such that} \qquad S - \ {}^{\sigma^3}S = Q.$$

Proof: This is due to the following short exact sequence:

$$0 \longrightarrow E_1(k_3) \longrightarrow E_1(\overline{k}) \overset{\sigma^3-1}{\longrightarrow} E_1(\overline{k}) \longrightarrow 0$$

or the surjectivity of $\sigma^3 - 1$ and the fact that $E_1(\overline{k})$ is a divisible group. □

Remark 3. *In fact, such an S is unique up to translations by $E_1(k_3)$. Indeed, if one defines*

$$S_1 \quad := \quad S + T \qquad \forall T \in E_1(k_3),$$

then

$$\begin{array}{rcl} {}^{\sigma^3}S_1 & = & {}^{\sigma^3}S +^{\sigma^3} T = S - Q + T \\ & = & S_1 - Q. \end{array}$$

Lemma 13. *Define a map ρ by*

$$\begin{aligned} \rho : E &\overset{\sim}{\longrightarrow} E_1 && (97)\\ P &\longmapsto \rho(P) := \varphi_1(P) + S. && (98) \end{aligned}$$

Then, ρ is an isomorphism of E to E_1 defined over k_3.

Proof: Since

$$\begin{aligned} {}^{\sigma^3}\rho(P) &= {}^{\sigma^3}\varphi_1(P) +^{\sigma^3} S \\ &= \varphi_1(P) + (Q +^{\sigma^3} S) \\ &= \varphi_1(P) + S \\ &= \rho(P), \end{aligned}$$

which means ρ is defined over k_3. □

9 Density of Type II curves

We first notice that the action

$$PGL_2(k_2) \curvearrowright k_6/k_2 \qquad (99)$$

is also transitive and fixed-point free. The proof is obtained by replacing k with k_2 in the proof for $PGL_2(k) \curvearrowright k_3 \setminus k$.

Then, for any $\alpha \in k_6 \setminus k_2$, one can find an $\varepsilon \in k_3 \setminus k$ and a $V \in PGL_2(k_2)$ such that α is the image of ε under the action of V. In fact,

$$\begin{aligned} \exists\varepsilon \in k_3 \setminus k & \qquad \exists V \in GL_2(k_2) \setminus k_2^{\times} GL_2(k) \\ s.t. \qquad \alpha &= V \cdot \varepsilon \\ \beta &= {}^{\sigma}V \cdot \varepsilon. \end{aligned}$$

We know that $\lambda(\alpha)$ is invariant under the left-action of $\mathrm{PGL}_2(k)$:

$$\forall U \in GL_2(k), \qquad U \cdot \alpha = UV \cdot \varepsilon \in k_6 \setminus k_2,$$

$$\lambda(UV \cdot \varepsilon) = \lambda(V \cdot \varepsilon).$$

Now, we consider also the action on the other side or the right-action on V:

$$\begin{aligned} \forall W &\in GL_2(k), \qquad \exists\varepsilon' \in k_3 \setminus k \\ s.t. \qquad \varepsilon &= W\varepsilon'. \end{aligned}$$

Then,

$$\lambda(V \cdot \varepsilon) = \lambda(VW \cdot \varepsilon'),$$

i.e., λ is also invariant under this action.

Now, we have two actions from both the left and the right sides on V. We then consider the double-sided action and the double cosets

$$k_2^\times GL_2(k) \Big\backslash\ GL_2(k_2)\ \Big/ k_2^\times GL_2(k) \tag{100}$$

defined by the above left and right actions on V such that

$$\lambda(V \cdot \varepsilon) \quad = \quad \lambda(UVW \cdot \varepsilon').$$

In order to obtain the number of Type II curves E, we will count $\#\lambda$ in their Legendre forms which are invariant under the action.

Lemma 14. *$V \in GL_2(k_2)\backslash GL_2(k)$ under the double-sided action can be classified to the following three cases: (Assume $r, s, t \in k, \eta \in k_2,\ e = \eta^2 \in k^\times \backslash (k^\times)^2$)*

$$(i) \qquad V_1 \quad = \quad \begin{pmatrix} r+\eta & 0 \\ 0 & 1 \end{pmatrix}; \tag{101}$$

$$(ii) \qquad V_2 \quad = \quad \begin{pmatrix} s+t\eta & e \\ 1 & s+t\eta \end{pmatrix}, \quad t \neq 0, \quad (s,t) \neq (0, \pm 1); \tag{102}$$

$$(iii) \qquad V_3 \quad = \quad \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}. \tag{103}$$

Proof:

One can always choose an $\eta \in k_2$ such that $\eta^2 = e \in k^\times \setminus (k^\times)^2$; then

$$\forall V \in GL_2(k_2) \setminus GL_2(k), \qquad V = V' + \eta V'', \qquad V', V'' \in M_2(k).$$

First, we assume V' is a regular matrix.

Then, under the double-sided action, V' can be transformed into the identity matrix I_2 while the ε' remains inside $k_3 \setminus k$. (Here V'' is used again.)

$$V = I_2 + \eta V'' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \eta V'', \qquad V'' \in M_2(k)$$

Under the double-sided action, V'' can be expressed in the following three forms:

$$(i) \qquad V_1'' \quad = \quad \begin{pmatrix} r & 0 \\ 0 & s \end{pmatrix}, r \neq s, \quad r, s \in k; \tag{104}$$

$$(ii) \qquad V_2'' \quad = \quad \begin{pmatrix} 0 & re \\ r & 0 \end{pmatrix} = r \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix}, \qquad r \in k^\times; \tag{105}$$

$$(iii) \qquad V_3'' \quad = \quad \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}, \qquad r \in k^\times. \tag{106}$$

Then, V becomes one of the following three forms under the double-sided action:

$$(i) \qquad V_1' = \begin{pmatrix} 1+r\eta & 0 \\ 0 & 1+s\eta \end{pmatrix}, \ r \neq s, \quad r,s \in k; \tag{107}$$

$$(ii) \qquad V_2' = \begin{pmatrix} 1 & re\eta \\ r\eta & 1 \end{pmatrix} = I_2 + r\eta \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix}, \qquad r \in k^\times; \tag{108}$$

$$(iii) \qquad V_3' = \begin{pmatrix} 1 & r\eta \\ 0 & 1 \end{pmatrix}, \qquad r \in k^\times. \tag{109}$$

V_1' can be transformed into V_1 in the Lemma as follows.

Assume $\frac{1+r\eta}{1+s\eta} = \frac{(1+r\eta)(1-s\eta)}{1-s^2e} = a + b\eta, a, b \in k$; one can use the following two actions, $\frac{1}{1+s\eta} \in k_2^\times$ and $\begin{pmatrix} \frac{1}{b} & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(k)$ on V_1' such that

$$\frac{1}{1+s\eta} \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+r\eta & 0 \\ 0 & 1+s\eta \end{pmatrix} = \begin{pmatrix} r+\eta & 0 \\ 0 & 1 \end{pmatrix};$$

here $b \neq 0$ since $V_1' \in GL_2(k_2) \setminus GL_2(k)$.

V_2' can be transformed into V_2 in the Lemma using a scaling by $\frac{1}{r\eta} = s + t\eta \in k_2^\times$.

Here, if $t = 0$ then $V_2 \in GL_2(k)$ which was excluded previously.

Besides, when V_2 is a singular matrix, $\det V_2 = (s+t\eta)^2 - e = s^2 + 2st\eta + (t^2-1)e = 0$, i.e., $s^2 + (t^2-1)e = 0$ and $st = 0$. Since $t \neq 0$ for $V_2 \notin GL_2(k)$, this means $s = 0, t^2 = 1$. Therefore, the cases $t = 0, (s,t) = (0, \pm 1)$ should be excluded.

V_3' can be transformed by the following double-sided $GL_2(k)$-action into V_3 in the Lemma as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & r\eta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{r} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & \eta \\ 0 & \frac{1}{r} \end{pmatrix} = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}.$$

Next, we consider the case when V' is singular. (Here $V' \neq O_2$; otherwise $V \in GL_2(k) \bmod k_2^\times$).

Then, under the double-sided action, one can assume

$$V' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Therefore,

$$V = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \eta V''.$$

Now, if V'' is regular, then one can change this case to the regular V' cases by the following left $GL_2(k)$-action mod$k_2^\times$: (Notice here $1/\eta = \eta/e$.)

$$\frac{1}{\eta}(V'')^{-1}V = I_2 + \eta V''', \qquad V''' := \frac{1}{e}(V'')^{-1}V'.$$

Now, assume V'' is singular,

$$V'' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \det V'' = ad - bc = 0.$$

Here we treat the cases of $b \neq 0$ and $b = 0$ separately.

First, in the $b \neq 0$ case, V'' can be transformed by a right $GL_2(k)$-action which preserves the form of $V' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$:

$$V'' \begin{pmatrix} b & 0 \\ -a & 1 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix}.$$

Thus, we can assume that

$$V = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \eta \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & b\eta \\ 0 & d\eta \end{pmatrix}.$$

Below, we show that this case can be reduced to case (i) of the regular V' cases.

Indeed, since $V \in GL_2(k_2), d \neq 0$, dividing V by $d\eta$ one has

$$\frac{1}{d\eta} V = \frac{1}{d\eta} \begin{pmatrix} 1 & b\eta \\ 0 & d\eta \end{pmatrix} = \begin{pmatrix} l\eta & h \\ 0 & 1 \end{pmatrix} \quad \bmod k_2^\times .$$

Now, by another left $GL_2(k)$-action:

$$\begin{pmatrix} 1 & -h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} l\eta & h \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} l\eta & 0 \\ 0 & 1 \end{pmatrix},$$

but it becomes a special case of (i) in the regular V' cases if one scales it by $1 + \eta$:

$$(1{+}\eta)V = (1{+}\eta) \begin{pmatrix} l\eta & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} le + l\eta & 0 \\ 0 & 1+\eta \end{pmatrix} = \begin{pmatrix} le & 0 \\ 0 & 1 \end{pmatrix} + \eta \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus, the case when V'' is singular with $b \neq 0$ is contained in case (i) of the regular V' cases.

In the remaining case, $b = 0$, first let $d \neq 0$; then $a = 0$ and

$$V = \begin{pmatrix} 1 & 0 \\ c\eta & d\eta \end{pmatrix}$$

which is the transpose of the $b \neq 0$ case.

If $d = 0$ in the $b = 0$ case, then

$$V = \begin{pmatrix} 1 + a\eta & 0 \\ c\eta & 0 \end{pmatrix} \notin GL_2(k_2),$$

which should be excluded. □

Lemma 15. *Elliptic curves of Type II can be classified to the following cases according to the classification of V under the double-sided action in Lemma 14. λ in each case has a representative as follows:*

$$\begin{aligned}
(i) \qquad \lambda_1 &= \frac{r^2-e}{4e}\,\frac{(\varepsilon-\varepsilon^q)^2}{\varepsilon^{q+1}}; && (110)\\
(ii) \qquad \lambda_2 &= \frac{N_{k_2/k}((s+t\eta)^2-e)}{4et^2}\,\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{q+1}} && (111)\\
&= \frac{N_{k_2/k}(\det V_2)}{4et^2}\,\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{q+1}}; && (112)\\
(iii) \qquad \lambda_3 &= \frac{1}{4e}(\varepsilon-\varepsilon^q)^2. && (113)
\end{aligned}$$

Proof:
(i) Define

$$\alpha_1 = V_1\cdot\varepsilon = (r+\eta)\varepsilon \qquad \in k_6\setminus(k_2\cup k_3).$$

Then,

$$\beta_1 = \alpha_1^{q^3} = (r-\eta)\varepsilon.$$

This is because $\varepsilon \in k_3\setminus k$, $\varepsilon^{q^3}=\varepsilon$ and $\eta^{2q}=e^q=e$, $\eta^q=-\eta$. Now,

$$\begin{aligned}
\beta_1-\alpha_1 &= -2\eta\varepsilon,\\
(\beta_1-\alpha_1)^{1+q} &= 4e\varepsilon^{1+q},\\
\beta_1-\alpha_1^q &= (r-\eta)(\varepsilon-\varepsilon^q),\\
\beta_1^q-\alpha_1 &= -(r+\eta)(\varepsilon-\varepsilon^q),\\
(\beta_1-\alpha_1^q)(\beta_1^q-\alpha_1) &= -(r^2-e)(\varepsilon-\varepsilon^q).
\end{aligned}$$

Thus, one has

$$\lambda_1 = -\frac{(r^2-e)}{4e}\frac{(\varepsilon-\varepsilon^q)}{\varepsilon^{1+q}}.$$

(ii) Define

$$\begin{aligned}
\alpha_2 &= V_2\cdot\varepsilon\\
&= \frac{(s+t\eta)\varepsilon+e}{\varepsilon+s+t\eta}.
\end{aligned}$$

Then,

$$\beta_2 = \frac{(s-t\eta)\varepsilon+e}{\varepsilon+s-t\eta}$$

and

$$\begin{aligned}\beta_2-\alpha_2 &= \frac{(s-t\eta)\varepsilon+e}{\varepsilon+s-t\eta}-\frac{(s+t\eta)\varepsilon+e}{\varepsilon+s+t\eta}\\ &= -\frac{2t\eta(\varepsilon^2-e)}{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)},\end{aligned}$$

$$(\beta_2-\alpha_2)^{1+q} = \frac{4et^2(\varepsilon^2-e)^{1+q}}{\{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)\}^{1+q}},$$

$$\begin{aligned}\beta_2-\alpha_2^q &= \frac{((s-t\eta)\varepsilon+e)(\varepsilon^q+s-t\eta)-((s-t\eta)\varepsilon^q+e)(\varepsilon+s-t\eta)}{(\varepsilon+s-t\eta)(\varepsilon^q+s-t\eta)}\\ &= \frac{((s-t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon+s-t\eta)(\varepsilon^q+s-t\eta)}=\frac{((s-t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)^q},\end{aligned}$$

$$\begin{aligned}\beta_2^q-\alpha_2 &= \frac{((s+t\eta)\varepsilon^q+e)(\varepsilon+s+t\eta)-((s+t\eta)\varepsilon+e)(\varepsilon^q+s+t\eta)}{(\varepsilon^q+s+t\eta)(\varepsilon+s+t\eta)}\\ &= -\frac{((s+t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon^q+s+t\eta)(\varepsilon+s+t\eta)}=-\frac{((s+t\eta)^2-e)(\varepsilon-\varepsilon^q)}{(\varepsilon+s-t\eta)^q(\varepsilon+s+t\eta)},\end{aligned}$$

$$(\beta_2-\alpha_2^q)(\beta_2^q-\alpha_2) = -\frac{((s-t\eta)^2-e)((s+t\eta)^2-e)(\varepsilon-\varepsilon^q)^2}{\{(\varepsilon+s-t\eta)(\varepsilon+s+t\eta)\}^{1+q}}.$$

Thus, one obtains

$$\begin{aligned}\lambda_2 &= \frac{((s-t\eta)^2-e)((s+t\eta)^2-e)}{4et^2}\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}}\\ &= \frac{N_{k_2/k}(((s+t\eta)^2-e)}{4et^2}\frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}}.\end{aligned}$$

(iii) Define

$$\begin{aligned}\alpha_3 &= V_3\cdot\varepsilon\\ &= \varepsilon+\eta.\end{aligned}$$

Then,

$$\begin{aligned}\beta_3 &= \alpha_3^{q^3}\\ &= \varepsilon-\eta\end{aligned}$$

and

$$\begin{aligned}
\beta_3 - \alpha_3 &= -2\eta, \\
(\beta_3 - \alpha_3)^{1+q} &= -4e, \\
\beta_3 - \alpha_3^q &= \varepsilon - \varepsilon^q, \\
\beta_3^q - \alpha_3 &= -(\varepsilon - \varepsilon^q), \\
(\beta_3 - \alpha_3^q)(\beta_3^q - \alpha_3) &= -(\varepsilon - \varepsilon^q)^2.
\end{aligned}$$

Thus, one obtains

$$\lambda_3 = \frac{1}{4e}(\varepsilon - \varepsilon^q)^2.$$

□

Lemma 16. *The three cases in Lemma 14 are pairwise disjoint.*

Proof: We will show the orbits of V under the double-sided action are disjoint in the following three steps.

(i) and (ii) have no overlap

Assume case (i) and case (ii) have an intersection so there is an

$$\begin{aligned}
A &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), && (114) \\
\mu &:= A \cdot \varepsilon = \frac{a\varepsilon + b}{c\varepsilon + d} && (115) \\
\text{such that} \qquad \lambda_1(\mu) &= \lambda_2(\varepsilon). && (116)
\end{aligned}$$

Then, notice the scaling constants in (110) and (112) are in k and independent of ε, so one has the following equation up to $k^\times$-scaling.

$$\frac{(\mu - \mu^q)^2}{\mu^{1+q}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{1+q}} \bmod k^\times. \qquad (117)$$

Since

$$\begin{aligned}
\mu - \mu^q &= \frac{(a\varepsilon + b)(c\varepsilon^q + d) - (a\varepsilon^q + b)(c\varepsilon + d)}{(c\varepsilon + d)(c\varepsilon^q + d)} \\
&= \frac{(ad - bc)(\varepsilon - \varepsilon^q)}{(c\varepsilon + d)^{1+q}}, \qquad (118)
\end{aligned}$$

one has

$$\begin{aligned}
LHS(117) &= \frac{(\mu - \mu^q)^2}{\mu^{1+q}} \\
&= \frac{(ad - bc)^2(\varepsilon - \varepsilon^q)^2}{\{(c\varepsilon + d)(a\varepsilon + b)\}^{1+q}}.
\end{aligned}$$

Thus, from (117),

$$\frac{(ad-bc)^2(\varepsilon-\varepsilon^q)^2}{\{(c\varepsilon+d)(a\varepsilon+b)\}^{1+q}} \quad \equiv \quad \frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}} \bmod k^\times,$$

one has

$$\{(c\varepsilon+d)(a\varepsilon+b)\}^{1+q} \equiv (\varepsilon^2-e)^{1+q} \bmod k^\times.$$

Denote this equation by

$$L^{1+q} \equiv R^{1+q} \bmod k^\times \text{ or } \left(\frac{L}{R}\right)^{1+q} \equiv 1 \bmod k^\times.$$

Since

$$\left(\frac{L}{R}\right)^{q^2-1} \equiv 1, \quad \left(\frac{L}{R}\right)^{q^3-1} \equiv 1,$$

then $L/R \in k^\times$ since $(q^2-1, q^3-1) = q-1$.

Therefore,

$$(c\varepsilon+d)(a\varepsilon+b) = l(\varepsilon^2-e), \qquad \exists l \in k^\times.$$

This means

$$\begin{aligned} ac &= l(\neq 0), \\ ad+bc &= 0, \\ bd &= -le(\neq 0), \end{aligned}$$

which implies

$$c \neq 0.$$

Now, we normalize A with $c=1$, then

$$a = l, \quad b = -ad = -ld, \quad bd = -ld^2 = -le,$$

thus,

$$d^2 = e.$$

But since $e \in k^\times \setminus (k^\times)^2$, such a d does not exist. Thus, the presumed intersection does not exist.

(i) and (iii) have empty overlap

Now, assume case (i) and case (iii) have an intersection such that under the action of (114), (115),

$$\lambda_1(\mu) \quad = \quad \lambda_3(\varepsilon). \tag{119}$$

From (110), (113), one has the following equation up to $k^\times$-scaling:

$$\frac{(\mu-\mu^q)^2}{\mu^{1+q}} \equiv (\varepsilon-\varepsilon^q)^2 \bmod k^\times. \tag{120}$$

From (119),

$$\frac{(\varepsilon-\varepsilon^q)^2}{\{(c\varepsilon+d)(a\varepsilon+b)\}^{1+q}} \equiv (\varepsilon-\varepsilon^q)^2 \bmod k^\times.$$

Then,

$$\{(c\varepsilon+d)(a\varepsilon+b)\}^{1+q} \equiv 1 \bmod k^\times.$$

For the same reason as before,

$$(c\varepsilon+d)(a\varepsilon+b) = l, \quad \exists l \in k^\times.$$

This means

$$\begin{aligned} ac &= 0, \\ ad+bc &= 0, \\ bd &= l \quad (\neq 0). \end{aligned}$$

We divide the conditions into two subcases: $c=0$ and $c \neq 0$.

When $c=0$, normalize A so that $d=1$; then $a=0$,

$$A = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix} \notin GL_2(k)$$

which is contrary to the assumption on A.

When $c \neq 0$, we can normalize A so that $c=1$. Then, $a=b=0$,

$$A = \begin{pmatrix} 0 & 0 \\ 1 & d \end{pmatrix} \notin GL_2(k)$$

which is again contrary to the assumption on A; thus the presumed intersection does not exist.

(ii) and (iii) have empty overlap

Assume case (iii) and case (ii) have an intersection such that under the action of (114), (115),

$$\lambda_3(\mu) = \lambda_2(\varepsilon).$$

From (113) and (112), one has the following equation up to $k^\times$-scaling:

$$(\mu-\mu^q)^2 \equiv \frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}} \bmod k^\times. \tag{121}$$

From (118)

$$\frac{(\varepsilon-\varepsilon^q)^2}{(c\varepsilon+d)^{2+2q}} \equiv \frac{(\varepsilon-\varepsilon^q)^2}{(\varepsilon^2-e)^{1+q}} \bmod k^\times.$$

Then,

$$(c\varepsilon+d)^{2+2q} \equiv (\varepsilon^2-e)^{1+q}.$$

Using the same reasoning as before again,

$$(c\varepsilon+d)^2 = l(\varepsilon^2-e) \qquad \exists l \in k^\times.$$

Therefore,

$$\begin{aligned} c^2 &= l \quad (\neq 0),\\ 2cd &= 0,\\ d^2 &= -le \quad (\neq 0). \end{aligned}$$

Thus,

$$d=0, \qquad 0=-le$$

which is impossible since $l, e \in k^\times$. Thus, the presumed intersection does not exist. □

Lemma 17. *The numbers of Type II curves in the three cases of Lemma 14 are as follows.*

$$\begin{aligned} (i) \qquad \#\{\lambda_1\} &= \frac{1}{4}q(q+1)^2; && (122)\\ (ii) \qquad \#\{\lambda_2\} &= \frac{1}{4}q(q-1)^2; && (123)\\ (iii) \qquad \#\{\lambda_3\} &= \frac{1}{2}(q^2-1). && (124) \end{aligned}$$

The total number of Type II curves is

$$\frac{1}{2}(q^3+q^2+q-1).$$

Proof:
(i) From (110), one can observe that λ_1 in case (i) is a product of two factors f_1, f_2:

$$\lambda_1 = f_1 f_2, \qquad f_1 := \frac{r^2-e}{4e}, \quad f_2 := \frac{(\varepsilon-\varepsilon^q)^2}{\varepsilon^{q+1}}.$$

We will count the two factors separately.

First, look at the factor f_2 which contains ε. Recall that $\varepsilon \in k_3 \setminus k$.

In order to count the orbits of f_2 under the $GL_2(k)$-action, we first consider

$$\begin{array}{rcl} A & = & \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in GL_2(k), \\ \mu & := & A \cdot \varepsilon \\ \text{such that} \qquad f_2(\mu) & \equiv & f_2(\varepsilon) \bmod k^\times, \end{array}$$

or

$$\frac{(\mu - \mu^q)^2}{\mu^{q+1}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{\varepsilon^{q+1}} \quad \bmod k^\times.$$

We wish to count the number of such μ or equivalently such matrices A. From

$$\frac{(ad - bc)^2(\varepsilon - \varepsilon^q)^2}{\{(a\varepsilon + b)(c\varepsilon + d)\}^{q+1}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{\varepsilon^{q+1}} \quad \bmod k^\times,$$

one has

$$(a\varepsilon + b)(c\varepsilon + d) = l\varepsilon, \qquad \exists l \in k^\times.$$

Therefore,

$$\begin{array}{rcl} ac & = & 0, \\ ad + bc & = & l \quad (\neq 0), \\ bd & = & 0. \end{array}$$

When $c = 0$, normalize A so that $d = 1$; then

$$a = l \neq 0, \quad b = 0, \qquad A = \left(\begin{array}{cc} a & 0 \\ 0 & 1 \end{array} \right).$$

Thus, the number of A in this case is

$$\#\{A\} = \#\{a\} = \#k^\times = q - 1.$$

When $c \neq 0$, one can normalize A so that $c = 1$; then

$$a = 0,\ b = l \neq 0,\ d = 0, \qquad A = \left(\begin{array}{cc} 0 & l \\ 1 & 0 \end{array} \right).$$

Therefore, the number of A in this case is

$$\#\{A\} = \#\{l\} = \#k^\times = q - 1.$$

The total number of A in these two cases is

$$\#\{A\} = 2(q - 1).$$

The number of f_2 is

$$\#\{f_2\} = \frac{\#\{\varepsilon \bmod k_3 \setminus k\}}{\#\{A\}} = \frac{q^3 - q}{2(q-1)} = \frac{1}{2}q(q+1).$$

Now, we count the factor $f_1 = \frac{r^2-e}{4e}$ in λ_1, where e is fixed:

$$\#\{f_1\} = \#\left\{\frac{r^2-e}{4e}, \quad r \in k\right\} = \#k^2 = \#(k^\times)^2 + \#\{0\} = \frac{q-1}{2} + 1 = \frac{q+1}{2}.$$

Thus,

$$\#\{\lambda_1\} = \#\{f_1\}\#\{f_2\} = \frac{1}{2}q(q+1) \times \frac{q+1}{2} = \frac{1}{4}q(q+1)^2.$$

(ii) By (112), λ_2 in case (ii) is a product of two factors g_1, g_2:

$$\lambda_2 = g_1 g_2, \qquad g_1 := \frac{N_{k_2/k}(\det V)}{4et^2}, \qquad g_2 := \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2)^{q+1}}. \tag{125}$$

Therefore, we will also count the two factors separately.

First, we count the factor g_2 which contains ε.

In order to count the orbits of g_2 under the $GL_2(k)$-action, consider

$$\begin{array}{rrcl} & A & = & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k), \\ & \mu & := & A \cdot \varepsilon \\ \text{such that} & g_2(\mu) & \equiv & g_2(\varepsilon) \bmod k^\times, \end{array}$$

or

$$\frac{(\mu - \mu^q)^2}{(\mu^2 - e)^{q+1}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{q+1}} \quad \bmod k^\times. \tag{126}$$

We wish to count the number of such μ or equivalently such matrices A. By (118),

$$\begin{array}{rrcl} & (\mu - \mu^q)^2 & = & \dfrac{(ad-bc)^2(\varepsilon - \varepsilon^q)^2}{(c\varepsilon + d)^{2q+2}} \\ \text{and} & \mu^2 - e & = & \dfrac{(a\varepsilon + b)^2 - e(c\varepsilon + d)^2}{(c\varepsilon + d)^2}. \end{array}$$

Then, (126) becomes

$$\frac{(\varepsilon - \varepsilon^q)^2}{\{(a\varepsilon + b)^2 - e(c\varepsilon + d)^2\}^{q+1}} \equiv \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{q+1}} \quad \bmod k^\times.$$

Thus, $\{(a\varepsilon + b)^2 - e(c\varepsilon + d)^2\}^{q+1} \equiv (\varepsilon^2 - e)^{q+1} \bmod k^\times$,

$$(a\varepsilon + b)^2 - e(c\varepsilon + d)^2 = l(\varepsilon^2 - e), \quad \exists l \in k^\times.$$

Now, one has

$$\begin{aligned} a^2 - ec^2 &= l, \\ 2(ab - ecd) &= 0, \\ b^2 - ed^2 &= -el. \end{aligned}$$

When $c = 0$,

$$\begin{aligned} a^2 = l & \quad (\neq 0), \\ ab = 0, & \quad b = 0, \\ d^2 = l, & \qquad d = \pm a. \end{aligned}$$

Therefore,

$$A = a \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix};$$

i.e., there are two such A mod $k^\times$ in this case.

When $c \neq 0$, one can normalize A so that $c = 1$; then

$$\begin{aligned} a^2 - e &= l, \\ ab = ed, \qquad d &= \frac{ab}{e}, \\ b^2 - ed^2 = -el, \qquad b^2 - e\left(\frac{ab}{e}\right)^2 &= -e(a^2 - e), \\ \frac{b^2}{e}(e - a^2) &= e(e - a^2), \\ b^2 = e^2, \qquad b = \pm e, \qquad d &= \frac{b}{e}a = \pm a, \end{aligned}$$

therefore

$$A = \begin{pmatrix} a & \pm e \\ 1 & \pm a \end{pmatrix}$$

since $e \notin (k^\times)^2$, $\det A \neq 0$.

The number of such A is

$$2\#\{a \in k\} = 2q.$$

Adding up the above two cases,

$$\#\{A\} = \#(c = 0) + \#(c = 1) = 2q + 2.$$

The number of orbits of g_2 under the $\mathrm{GL}_2(k)$-action becomes

$$\#\{g_2\} = \frac{\#\{\varepsilon\}}{\#\{A\}} = \frac{q^3 - q}{2(q+1)} = \frac{q(q-1)}{2}.$$

Now, we count the number of $g_1 = \frac{N_{k_2/k}((s+t\eta)^2 - e)}{4et^2}$. Define

$$\begin{aligned} \rho \quad &:= \quad \frac{N_{k_2/k}((s+t\eta)^2 - e)}{t^2} && (127) \\ &= \quad \frac{1}{t^2}((s^2 + e(t^2 - 1))^2 - 4es^2t^2). && (128) \end{aligned}$$

Recall $e \in k^\times \setminus (k^\times)^2$. Obviously $t \neq 0, (s,t) \neq (0, \pm 1)$ if and only if $\rho \neq 0, \infty$.

To count $\#\{\rho\}$, notice there is a ρ if and only if the following plane curve has nontrivial k-rational points $\{(s^2, t^2)\}$:

$$(s^2 + e(t^2 - 1))^2 - 4es^2t^2 = \rho t^2.$$

Redefine $X := s^2, Y := t^2$; then one has a conic curve

$$C_1 : (X + e(Y - 1))^2 - 4eXY = \rho Y \tag{129}$$

which has $(X, Y) = (e, 0)$ as a k-rational point corresponding to $\rho = \infty$.

Now, we draw a straight line through $(e, 0)$:

$$X = e + hY$$

whose intersection with the conic C_1 is determined by

$$(h - e)^2 Y^2 = (4e^2 + \rho)Y.$$

When $h = e$, i.e., $\rho = -4e^2$:

Then, the straight line becomes

$$X = e(1 + Y).$$

Since $X = s^2, Y = t^2$, one has a conic

$$C_2 : \; s^2 - et^2 = e \tag{130}$$

which is nonsingular. This is because

$$(\partial_s, \partial_t) = (2s, -2et) = (0, 0)$$

means $(s, t) = (0, 0)$ which however is not contained in $C_2(\bar{k})$.

Therefore, its set of rational points $C_3(k)$ is isomorphic to $\mathbb{P}^1(k)$.

Thus, in this case there is one value of $\rho = -4e^2$ to be counted.

When $h \neq e$, i.e., $\rho \neq -4e^2$:

Assume $h \neq e$; then one has a linear equation in Y:

$$(h - e)^2 Y = 4e^2 + \rho \tag{131}$$

Thus, for any ρ there is a k-rational point (X, Y) on the above curve C_1.

$$Y = \frac{4e^2 + \rho}{(h - e)^2} \qquad \neq 0, \tag{132}$$

$$X = \frac{e(h - e)^2 + h(4e^2 + \rho)}{(h - e)^2}. \tag{133}$$

Define

$$f := (h-e)t,$$

one has

$$f^2 = 4e^2 + \rho \qquad \exists f \in k. \tag{134}$$

Since $\rho \neq 0$, $f \neq \pm 2e$. Thus, the correspondence between f and ρ is 2-1 when $f \neq 0, \pm 2e$.

So we will consider the existence of (s,t) when $f \neq 0, \pm 2e$.

Define

$$v \quad := \quad (h-e)s. \tag{135}$$

From (133), one obtains a new conic curve in v, h with f fixed:

$$C_3 : \ v^2 \quad = \quad e(h-e)^2 + f^2 h. \tag{136}$$

We are to count the number of such C_3 with non-empty k_2-rational points. In order to do that, we show that the curve is a nonsingular conic.

Indeed, assume

$$\partial_v = 2v = 0, \quad \partial_h = 2e(h-e) + f^2 = 0 \qquad (h \neq e);$$

one obtains

$$0 = e(h-e)^2 + f^2 h, \quad 2e(h-e) + f^2 = 0, \quad 2eh(h-e) + f^2 h = 0,$$

thus,

$$2eh(h-e) = -f^2 h = e(h-e)^2, \quad 2h = h - e, \quad h = -e,$$

but since $f^2 = -2e(h-e) = 4e^2, f = \pm 2e$ which is excluded already. Thus, the affine curve is nonsingular.

Now consider its projective version:

$$\frac{v^2}{w^2} = e\left(\frac{h}{w} - e\right)^2 + f^2 \frac{h}{w},$$

$$v^2 = e(h - ew) + f^2 w.$$

Assume again

$$\partial_v = 2v = 0, \quad \partial_h = 2e(h - ew) + f^2 w = 0, \quad \partial_w = -2e^2(h - ew) + f^2 h = 0.$$

Then, one has to check only the point at infinity: $w = 0$. But

$$eh = 0, \quad -2e^2 h + f^2 h = 0$$

means $v = h = w = 0$, which is absurd. Thus, C_3 is a nonsingular projective conic.

Besides, it has a rational point $(v, h) = (0, -e(h-e)^2/f^2)$. Thus, $C_3(k) \simeq \mathbb{P}^1(k)$.

Therefore,

$$\#\{\rho \neq -4e^2, 0\} = \frac{\#\{f \neq 0, \pm 2e\}}{2} = \frac{q-3}{2}, \tag{137}$$

$$\#\{g_1\} = \#\{\rho\} = \frac{\#\{f \neq 0, \pm 2e\}}{2} + \#\{f = 0\} = \frac{q-3}{2} + 1 = \frac{q-1}{2}. \tag{138}$$

Finally,

$$\#\{\lambda_2\} = \#\{g_1\} \times \#\{g_2\} = \frac{q-1}{2} \times \frac{q(q-1)}{2} = \frac{q(q-1)^2}{2}. \tag{139}$$

(iii) We now count the number of λ_3 under the $\mathrm{GL}_2(k)$-action. Recall

$$\lambda_3(\varepsilon) = \frac{(\varepsilon - \varepsilon^q)^2}{4e}.$$

Consider the action by $A \in GL_2(k)$ such that

$$\mu := A \cdot \varepsilon \quad \text{and} \quad \lambda_3(\mu) = \lambda_3(\varepsilon).$$

Then, one has

$$\begin{aligned} (\mu - \mu^q)^2 &= (\varepsilon - \varepsilon^q)^2, \\ \mu - \mu^q &= \pm(\varepsilon - \varepsilon^q), \\ \mu \pm \varepsilon &= \mu^q \pm \varepsilon^q = (\mu \pm \varepsilon)^q, \\ (\mu \pm \varepsilon)^{q-1} &= 1, \quad \mu \pm \varepsilon =: l \in k, \\ \mu &= \pm\varepsilon + l \qquad \exists l \in k. \end{aligned}$$

Thus, the number of A such that $\lambda_3(\mu) = \lambda_3(\varepsilon)$ is

$$2\#\{l\} = 2\#k = 2q.$$

The number of orbits of λ_3 is

$$\frac{q^3 - q}{2q} = \frac{q^2 - 1}{2}.$$

Now, we add up the cases (i), (ii), and (iii) to obtain the total number of Type II curves:

$$\#\{\lambda\} = \frac{q(q+1)^2}{4} + \frac{q(q-1)^2}{4} + \frac{q^2-1}{2} = \frac{q^3 + q^2 + q - 1}{2}. \tag{140}$$

□

10 Density of Type II curves with hyperelliptic coverings

Lemma 18. *A Type II curve E has a hyperelliptic covering C/k if and only if there is a $V \in GL_2(k_2), \Theta \in GL_2(k)$ such that $\Theta =^\sigma VV^{-1}$, $Tr(\Theta) = 0$, $\beta = \Theta \cdot \alpha$.*

Proof: For $\varepsilon \in k_3 \setminus k$, there is a unique $V \in G_2(k_2)$ such that $\alpha = V \cdot \varepsilon \in k_6$. Then,

$$\beta = \alpha^{q^3} = (V \cdot \varepsilon)^{q^3} =^\sigma V \cdot \varepsilon =^\sigma VV^{-1} \cdot \alpha.$$

Define $\Theta =^\sigma VV^{-1}$. If $\mathrm{Tr}(\Theta) = 0$, then C/k is hyperelliptic and vice versa. □

Lemma 19. *The numbers of hyperelliptic covering curves in the three cases of Type II curves are*

$$\begin{array}{lrcl} (i) & \#\{\textit{hyperelliptic covers}\} & = & \frac{1}{2}q(q+1); \\ (ii) & \#\{\textit{hyperelliptic covers}\} & = & \frac{1}{2}q(q-1); \\ (iii) & \#\{\textit{hyperelliptic covers}\} & = & 0. \end{array}$$

Thus, the total number of Type II curves with hyperelliptic coverings is

$$\#\{\textit{Type II hyperelliptic covers}\} = q^2.$$

Proof: We consider again representatives under the double-sided action in Lemma 14 and count each orbit of Θ with zero trace.

(i) From (101),

$$V_1 = \begin{pmatrix} r+\eta & 0 \\ 0 & 1 \end{pmatrix},$$

$$\begin{aligned} \Theta_1 &= {}^\sigma V_1 V_1^{-1} \sim \begin{pmatrix} r-\eta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & r+\eta \end{pmatrix} \\ &= \begin{pmatrix} r-\eta & 0 \\ 0 & r+\eta \end{pmatrix}. \end{aligned}$$

Assume $\mathrm{Tr}(\Theta_1) = 2r = 0$, then $r = 0$,

$$V_1 = \begin{pmatrix} -\eta & 0 \\ 0 & +\eta \end{pmatrix} \equiv \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix} \bmod k^\times.$$

From Lemma 15,

$$\lambda_1 = -\frac{1}{4}\,\frac{(\varepsilon - \varepsilon^q)^2}{\varepsilon^{q+1}}$$

which is f_2 in the proof of (i) Lemma 17. Hence we have

$$\#\{\lambda_1\} = \frac{1}{2}q(q+1).$$

(ii) From (102),

$$V_2 = \begin{pmatrix} s+t\eta & e \\ 1 & s+t\eta \end{pmatrix}, \qquad t \neq 0, \quad (s,t) \neq (0, \pm 1),$$

one has

$$\begin{array}{rcl} \Theta_2 & = & {}^{\sigma}V_2 V_2^{-1} \\ & \sim & \begin{pmatrix} s-t\eta & e \\ 1 & s-t\eta \end{pmatrix} \begin{pmatrix} s+t\eta & -e \\ -1 & s+t\eta \end{pmatrix} \\ & = & \begin{pmatrix} s^2-e(t^2+1) & 2te\eta \\ 2t\eta & s^2-e(t^2+1) \end{pmatrix}. \end{array}$$

Assuming

$$\mathrm{Tr}(\Theta_2) = 0,$$

one obtains a conic

$$s^2 = e(t^2+1)$$

which is nonsingular. Therefore, its k-rational points are bijective to those of $\mathbb{P}^1(k)$. Therefore,

$$\#\{\lambda_2\} = \frac{\#\{\alpha \in k_3 \setminus k\}}{\# V_2} = \frac{q(q^2-1)}{q+1} = \frac{q(q-1)}{2}.$$

Or, since

$$\lambda_2 = -e \frac{(\varepsilon - \varepsilon^q)^2}{(\varepsilon^2 - e)^{q+1}}$$

equals the factor g_2 in the proof of Lemma 17 (ii), which has cardinality $\frac{q(q-1)}{2}$.

(iii) From (103),

$$V_3 = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix},$$

one has

$$\begin{array}{rcl} \Theta_3 & = & {}^{\sigma}V_3 V_3^{-1} \\ & = & \begin{pmatrix} 1 & -2\eta \\ 0 & 1 \end{pmatrix}. \end{array}$$

Then, $\mathrm{Tr}(\Theta_3) \neq 0$, or there is no hyperelliptic covering in this case.

□

11 Conclusion

In this paper, we presented an analysis of the GHS attack on elliptic curves E defined over the cubic extension k_3 of a finite field k of odd characteristic. Analysis of the GHS attack in general seems to be a difficult task. In this paper we restricted ourselves to the most favorable situation for the GHS attack. In fact, we assumed the isogeny condition which means that the covering curve C/k has the smallest possible size. Therefore the genus of C is $d = 3$.

We classified those curves which have covering curves C defined over k, therefore the discrete logarithm on E can be mapped to the Jacobian of C so the GHS attack is applicable. In particular, the double-large-prime index calculus algorithm and Gaudry's low dimension Abelian varieties algorithm on E over cubic fields have running time $\tilde{O}(q^{4/3})$. On the other hand, discrete logarithms on these E with a genus 3 non-hyperelliptic covering C under the GHS attack can be solved in $\tilde{O}(q)$.

When $C/\mathbb{P}^1$ is a $(2,2,2)$-covering, C is hyperelliptic. When $C/\mathbb{P}^1$ is a $(2,2)$-covering, E has forms of either Type I or Type II. The numbers of both the Type I and Type II curves with non-hyperelliptic covering C are $\frac{1}{2}q^3 + O(q^2)$. This is the same as the order of the total isogeny classes of elliptic curves over the cubic field k_3. On the other hand, E with hyperelliptic coverings C are much less common. In fact, the numbers of E with hyperelliptic covering C for both $(2,2,2)$ case and $(2,2)$ Type I or Type II cases are $q^2 + O(q)$.

As for how to test if an elliptic curve is weak, we presented a simple algorithm for the Type I case by solving a quadratic equation. It would be desirable to be able to test for the Type II case. Further researches also include classification of general cases of both odd and even characteristics [25], curves with weak coverings without isogeny condition [20][21], and explicit construction of covering curves [6], [17].

References

[1] L. Adleman, J. De Marrais and M. Huang, "A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields," Algorithmic Number Theory, Springer-Verlag, LNCS 877, pp.28–40, 1994.

[2] S. Arita, K. Matsuo, K. Nagao, M. Shimura "A Weil descent attack against elliptic curve cryptosystems over quartic extension field I", Proceedings of SCIS2004, IEICE Japan 2004.

[3] I.F. Black, G. Seroussi and N. Smart, "Advances in elliptic curve cryptography", Cambridge University Press 2005.

[4] H. Cohen, G. Frey, "Handbook of elliptic and hyperelliptic curve cryptography", Chapman & Hall, 2006

[5] J. Chao, “Elliptic and hyperelliptic curves with weak coverings against Weil descent attack,” Talk at the 11th Elliptic Curve Cryptography Workshop, 2007.

[6] C. Diem, “The GHS attack in odd characteristic,” J. Ramanujan Math. Soc., vol.18 no.1, pp.1–32, 2003.

[7] C. Diem, “Index calculus in class groups of plane curves of small degree”, Proceedings of ANTS VII, 2006. Available from http://www.math.uni-leipzig.de/˜diem/preprints/small-degree.ps

[8] C. Diem, J. Scholten, “Cover attacks, a report for the AREHCC project”, preprint Oct. 2003.

[9] A. Enge and P. Gaudry, “A general framework for subexponential discrete logarithm algorithms,” Acta Arith., vol.102, pp.83–103, 2002.

[10] G. Frey, “How to disguise an elliptic curve,” Talk at the 2nd Elliptic Curve Cryptology Workshop, 1998.

[11] S.D. Galbraith, “Weil descent of Jacobians,” Discrete Applied Mathematics, vol.128 no.1, pp.165–180, 2003.

[12] P. Gaudry, “An Algorithm for solving the discrete logarithm problem on hyperelliptic curves,” Advances in cryptology EUROCRYPTO 2000, Springer-Verlag, LNCS 1807, pp.19–34, 2000.

[13] P. Gaudry, N. Thériault, E. Thomé, C. Diem “A double large prime variation for small genus hyperelliptic index calculus” Math. Comp. 76 (2007), pp.475–492.

[14] P. Gaudry, F. Hess and N. Smart, “Constructive and destructive facets of Weil descent on elliptic curves,” J. Cryptol, 15, pp.19–46, 2002.

[15] P. Gaudry, “Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem”, *Journal of Symbolic Computation*, Elsevier, 44, 12, pp.1690–1702, 2009.

[16] M. Gonda, K. Matsuo, K. Aoki, J. Chao and S. Tsujii, “Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation”, IEICE Transactions on Fundamentals, E88-A(1), pp.89–96, 2005.

[17] N.Hashizume, F.Momose and J.Chao, “On Implementation of GHS Attack against Elliptic Curve Cryptosystems over Cubic Extension Fields of Odd Characteristics” Available from http://eprint.iacr.org/2008/215

[18] F. Hess, “The GHS attack revisited,” Advances in cryptology EUROCRYPTO 2003, Springer-Verlag, LNCS 2656, pp.374–387, 2003.

[19] F. Hess, “Generalizing the GHS Attack on the Elliptic Curve Discrete Logarithm,” LMS J. Comput. Math. vol.7, pp.167–192, 2004.

[20] T. Iijima, F. Momose, J. Chao, "Classification of Weil Restrictions Obtained by $(2, \ldots, 2)$ Coverings of $\mathbb{P}^1$ without Isogeny Condition in Small Genus Cases" Proceedings of SCIS 2009, 2009.

[21] T. Iijima, F. Momose, J. Chao, "Classification of Elliptic/hyperelliptic Curves with Weak Coverings against GHS Attack without Isogeny Condition" preprint, 2009. Available from http://eprint.iacr.org/2009/613

[22] A. Menezes and M. Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart," Topics in Cryptology CT-RSA 2001, Springer-Verlag, LNCS 2020, pp.308–318, 2001.

[23] A. Menezes, E. Teske and A. Weng, "Weak Fields for ECC". Topics in Cryptology CT-RSA 2004, Springer-Verlag, LNCS 2964, pp.366–386, 2004.

[24] F. Momose, J. Chao, M. Shimura, "On Weil descent of elliptic curves over quadratic extensions" Proceedings of SCIS2005, pp.787–792, 2005

[25] F. Momose and J. Chao, "Classification of Weil restrictions obtained by $(2, \ldots, 2)$ coverings of $\mathbb{P}^1$," preprint, 2006. Available from http://eprint.iacr.org/2006/347

[26] F. Momose and J. Chao, "Scholten Forms and Elliptic/Hyperelliptic Curves with Weak Weil Restrictions," preprint, 2005. Available from http://eprint.iacr.org/2005/277

[27] K. Nagao, "Improvement of Theriault algorithm of index calculus of Jacobian of hyperelliptic curves of small genus", preprint 2004.

[28] B.Smith, "Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves". Journal of Cryptology 22, 4, 505–529, 2009

[29] N. Thériault, "Index calculus attack for hyperelliptic curves of small genus", Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Computer Science, 2894, 75–92, 2003

[30] N. Thériault, "Weil descent attack for Kummer extensions," J. Ramanujan Math. Soc, vol.18, pp.281–312, 2003.

[31] N. Thériault, "Weil descent attack for Artin-Schreier curves," preprint, 2003, available at http://www.math.toronto.edu/ganita/papers/wdasc.pdf

12 Appendix 1: Proof of Lemma 7.3: B is not upper triangular

Since

$$A = \begin{pmatrix} \nu & -\varepsilon^{1+q} \\ 1 & -\mu \end{pmatrix}, \qquad B = {}^{\sigma^2}\!A \ {}^{\sigma}\!A\ A,$$

we have

$$ {}^{\sigma}\!A\ A \ = \ \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & * \\ \nu - \mu^q & * \end{pmatrix}. \tag{141}$$

On the other hand,

$$\begin{aligned} {}^{\sigma^2}\!A \ &= \ \begin{pmatrix} \nu^{q^2} & -\varepsilon^{1+q^2} \\ 1 & -\mu^{q^2} \end{pmatrix}, && (142)\\ \widetilde{{}^{\sigma^2}\!A} \ &= \ \frac{-1}{\det {}^{\sigma^2}\!A} \begin{pmatrix} \mu^{q^2} & -\varepsilon^{1+q^2} \\ 1 & -\nu^{q^2} \end{pmatrix} && (143)\\ &= \ \frac{-1}{\det {}^{\sigma^2}\!A} \begin{pmatrix} \mu^{q^2} & * \\ 1 & * \end{pmatrix}. && (144) \end{aligned}$$

Assume B is upper triangular, then

$$ {}^{\sigma}\!A\ A \equiv \widetilde{{}^{\sigma^2}\!A} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod k_3^\times. \tag{145}$$

By (141), (144)

$$\begin{aligned} \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & * \\ \nu - \mu^q & * \end{pmatrix} \ &\equiv \ \begin{pmatrix} \mu^{q^2} & * \\ 1 & * \end{pmatrix} \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod k_3^\times && (146)\\ &= \ \begin{pmatrix} \mu^{q^2} & * \\ 1 & * \end{pmatrix} \bmod k_3^\times. && (147) \end{aligned}$$

In the above equation of 2×2 matrices, taking the ratios of $(1,1)$ entries over $(1,2)$ entries of both sides, we obtain the following equation:

$$\nu^{1+q} - \varepsilon^{q+q^2} = \mu^{q^2}(\nu - \mu^q). \tag{148}$$

Since this equation contains μ, ν and ε at the same time, we will try to represent μ, ν in terms of ε.

Now, substitute $\nu = -\mu + \varepsilon + \varepsilon^q$ into the equation (148),

$$\begin{aligned} (-\mu + \varepsilon + \varepsilon^q)\left(-\mu^q + \varepsilon^q + \varepsilon^{q^2}\right) - \varepsilon^{q+q^2} &= \mu^{q^2}\left(-\mu - \mu^q + \varepsilon + \varepsilon^q\right) \\ &= -\mu^{1+q^2} - \mu^{q+q^2} + (\varepsilon + \varepsilon^q)\,\mu^{q^2}, \\ \mu^{1+q} - \left(\varepsilon^q + \varepsilon^{q^2}\right)\mu - (\varepsilon + \varepsilon^q)\,\mu^q + \varepsilon^{1+q} + \varepsilon^{1+q^2} + \varepsilon^{2q} & \\ &= -\mu^{1+q^2} - \mu^{q+q^2} + (\varepsilon + \varepsilon^q)\,\mu^{q^2}. \end{aligned}$$

Then, we have

$$\mathrm{Tr}_{k_3/k}(\mu^{1+q}) - \mathrm{Tr}_{k_3/k}(\left(\varepsilon^q + \varepsilon^{q^2}\right)\mu) + \mathrm{Tr}_{k_3/k}(\varepsilon^{1+q}) + \left(\varepsilon^{q^2} - \varepsilon^q\right)\mu^q + \varepsilon^q(\varepsilon^q - \varepsilon^{q^2}) = 0.$$

Since $\mathrm{Tr}_{k_3/k} \in k$,

$$\left(\varepsilon^q - \varepsilon^{q^2}\right)\mu^q - \varepsilon^q(\varepsilon^q - \varepsilon^{q^2}) = \tau \in k,$$

$$\begin{aligned} \mu^q &= \varepsilon^q + \frac{\tau}{\left(\varepsilon^q - \varepsilon^{q^2}\right)}, && (149) \\ \mu &= \varepsilon + \frac{\tau}{\left(\varepsilon - \varepsilon^q\right)}, && (150) \end{aligned}$$

$$\nu = -\mu + \varepsilon + \varepsilon^q = \varepsilon^q - \frac{\tau}{\left(\varepsilon - \varepsilon^q\right)}. \qquad (151)$$

Therefore, we can represent μ, ν in terms of $\varepsilon, \tau \in k$.

Now, substitute (150), (151) into (148),

$$LHS = -\left(\frac{\varepsilon^{q^2}}{\left(\varepsilon - \varepsilon^q\right)} + \frac{\varepsilon^q}{\left(\varepsilon - \varepsilon^q\right)^q}\right)\tau + \frac{\tau^2}{\left(\varepsilon - \varepsilon^q\right)^{1+q}},$$

$$RHS = -\left(\frac{\varepsilon^{q^2}}{\left(\varepsilon - \varepsilon^q\right)} + \frac{\varepsilon^{q^2}}{\left(\varepsilon - \varepsilon^q\right)^q}\right)\tau - \left(\frac{1}{\left(\varepsilon - \varepsilon^q\right)^{1+q^2}} + \frac{1}{\left(\varepsilon - \varepsilon^q\right)^{q+q^2}}\right)\tau^2.$$

Then, (148) becomes

$$\frac{\varepsilon^{q^2} - \varepsilon^q}{\left(\varepsilon - \varepsilon^q\right)^q}\tau + \mathrm{Tr}_{k_3/k}\left(\frac{1}{\left(\varepsilon - \varepsilon^q\right)^{1+q^2}}\right)\tau^2 = 0. \qquad (152)$$

Since

$$\begin{aligned} \frac{\varepsilon^{q^2} - \varepsilon^q}{\left(\varepsilon - \varepsilon^q\right)^q} &= \frac{\left(\varepsilon^q - \varepsilon\right)^q}{\left(\varepsilon - \varepsilon^q\right)^q} = -1, \\ \mathrm{Tr}_{k_3/k}\left(\frac{1}{\left(\varepsilon - \varepsilon^q\right)^{1+q^2}}\right) &= \frac{1}{\left(\varepsilon - \varepsilon^q\right)^{1+q^2}} + \frac{1}{\left(\varepsilon - \varepsilon^q\right)^{q+1}} + \frac{1}{\left(\varepsilon - \varepsilon^q\right)^{q+q^2}} \\ &= \frac{\left(\varepsilon - \varepsilon^q\right)^q + \left(\varepsilon - \varepsilon^q\right)^{q^2} + \varepsilon - \varepsilon^q}{N_{k_3/k}\left(\varepsilon - \varepsilon^q\right)} \\ &= \frac{\varepsilon^q - \varepsilon^{q^2} + \varepsilon^{q^2} - \varepsilon + \varepsilon - \varepsilon^q}{N_{k_3/k}\left(\varepsilon - \varepsilon^q\right)} = 0, \end{aligned}$$

(152) becomes

$$\tau = 0\Gamma \implies \mu = \varepsilon, \qquad (153)$$

which is contrary to the assumption that $\mu \neq \varepsilon$.

Thus, B is not upper triangular.

13 Appendix 2: Type I curves with hyperelliptic coverings: Explicit formula for the discriminant Δ

First, we review notations used here.

$$A = \begin{pmatrix} \nu & -\varepsilon^{1+q} \\ 1 & -\mu \end{pmatrix}, \qquad B =^{\sigma^2} A \ \ ^{\sigma}A \ \ A, \tag{154}$$

$$\mu = \begin{pmatrix} \varepsilon & -\varepsilon^q \\ 1 & -1 \end{pmatrix} \cdot \lambda, \qquad \lambda \neq 0, 1, \infty, \tag{155}$$

$$\nu = \begin{pmatrix} \varepsilon^q & -\varepsilon \\ 1 & -1 \end{pmatrix} \cdot \lambda, \tag{156}$$

$$\rho = \frac{1}{\lambda - 1}.$$

Next, we show the detailed form of the matrix B as follows. Since

$$\mu = \varepsilon + \alpha, \qquad \alpha = (\varepsilon - \varepsilon^q)\rho, \qquad \nu = \varepsilon^q - \alpha,$$

$$\begin{aligned} ^{\sigma}A \ \ A &= \begin{pmatrix} \nu^q & -\varepsilon^{q+q^2} \\ 1 & -\mu^q \end{pmatrix} \begin{pmatrix} \nu & -\varepsilon^{1+q} \\ 1 & -\mu \end{pmatrix} && (157) \\ &= \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & -\varepsilon^{1+q}\nu^q + \varepsilon^{q+q^2}\mu \\ \nu - \mu^q & -\varepsilon^{1+q} + \mu^{1+q} \end{pmatrix}. && (158) \end{aligned}$$

One has

$$\begin{aligned} B &= \ ^{\sigma^2}A \ \ (^{\sigma}A \ \ A) && (159) \\ &= \begin{pmatrix} \nu^{q^2} & -\varepsilon^{1+q^2} \\ 1 & -\mu^{q^2} \end{pmatrix} \begin{pmatrix} \nu^{1+q} - \varepsilon^{q+q^2} & -\varepsilon^{1+q}\nu^q + \varepsilon^{q+q^2}\mu \\ \nu - \mu^q & -\varepsilon^{1+q} + \mu^{1+q} \end{pmatrix} && (160) \\ &=: \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}, && (161) \end{aligned}$$

$$\begin{aligned} B_{11} &= N(\nu) - \varepsilon^{q+q^2}\nu^{q^2} - \varepsilon^{1+q^2}(\nu - \mu^q), && (162) \\ B_{22} &= -\varepsilon^{1+q}\nu^q + \varepsilon^{q+q^2}\mu + \varepsilon^{1+q}\mu^{q^2} - N(\mu). && (163) \end{aligned}$$

Now, we continue further to find Δ. Since

$$\begin{aligned} N(\nu) &= (\varepsilon^q - \alpha)(\varepsilon^{q^2} - \alpha^q)(\varepsilon - \alpha^{q^2}) \\ &= N(\varepsilon) - \varepsilon^{q+q^2}\alpha^{q^2} - \varepsilon^{1+q}\alpha^q - \varepsilon^{1+q^2}\alpha + \varepsilon^q\alpha^{q+q^2} + \varepsilon^{q^2}\alpha^{1+q^2} + \varepsilon\alpha^{1+q} - N(\alpha), \end{aligned}$$

$$-\varepsilon^{q+q^2}\nu^{q^2} = -\varepsilon^{q+q^2}(\varepsilon - \alpha^{q^2}) = -N(\varepsilon) + \varepsilon^{q+q^2}\alpha^{q^2},$$

$$-\varepsilon^{1+q^2}\nu \quad = \quad -\varepsilon^{1+q^2}(\varepsilon^q - \alpha) = -N(\varepsilon) + \varepsilon^{1+q^2}\alpha,$$

$$\varepsilon^{1+q^2}\mu^q \quad = \quad \varepsilon^{1+q^2}(\varepsilon^q + \alpha^q) = N(\varepsilon) + \varepsilon^{1+q^2}\alpha^q,$$

$$-\varepsilon^{1+q}\nu^q \quad = \quad -\varepsilon^{1+q}(\varepsilon^{q^2} - \alpha^q) = -N(\varepsilon) + \varepsilon^{1+q}\alpha^q,$$

$$\varepsilon^{q+q^2}\mu \quad = \quad \varepsilon^{q+q^2}(\varepsilon + \alpha) = N(\varepsilon) + \varepsilon^{q+q^2}\alpha,$$

$$\varepsilon^{1+q}\mu^{q^2} \quad = \quad \varepsilon^{1+q}(\varepsilon^{q^2} + \alpha^{q^2}) = N(\varepsilon) + \varepsilon^{1+q}\alpha^{q^2},$$

$$\begin{aligned} -N(\mu) &= -(\varepsilon + \alpha)(\varepsilon^q + \alpha^q)(\varepsilon^{q^2} + \alpha^{q^2}) \\ &= -N(\varepsilon) - \varepsilon^{1+q}\alpha^{q^2} - \varepsilon^{q+q^2}\alpha - \varepsilon^{1+q}\alpha^q - \varepsilon\alpha^{q+q^2} - \varepsilon^q\alpha^{1+q^2} - \varepsilon^{q^2}\alpha^{1+q} - N(\alpha). \end{aligned}$$

One can find

$$\begin{aligned} \mathrm{Tr}(B) &= \varepsilon^q\alpha^{q+q^2} + \varepsilon^{q^2}\alpha^{1+q^2} + \varepsilon\alpha^{1+q} - N(\alpha) - \varepsilon\alpha^{q+q^2} - \varepsilon^q\alpha^{1+q^2} - \varepsilon^{q^2}\alpha^{1+q} - N(\alpha) \\ &= N(\varepsilon - \varepsilon^q)\mathrm{Tr}(\rho^{1+q}) - 2N(\varepsilon - \varepsilon^q)N(\rho) \\ &= N(\varepsilon - \varepsilon^q)\{\mathrm{Tr}(\rho^{1+q}) + 2N(\rho)\}, \end{aligned}$$

and

$$\begin{aligned} \det B &= N(-\nu\mu + \varepsilon^{1+q}), \\ -\nu\mu + \varepsilon^{1+q} &= -(\varepsilon^q - \alpha)(\varepsilon - \alpha) + \varepsilon^{1+q} \\ &= (\varepsilon - \varepsilon^q)^2(\rho + \rho^2), \end{aligned}$$

$$\det B \quad = \quad N(\varepsilon - \varepsilon^q)^2 N(\rho + \rho^2).$$

Thus, finally

$$\begin{aligned} \Delta &= (\mathrm{Tr}B)^2 - 4\det B & (164) \\ &= N(\varepsilon - \varepsilon^q)^2\{[\mathrm{Tr}(\rho^{1+q}) + 2N(\rho)]^2 - 4N(\rho)N(\rho + 1)\}. & (165) \end{aligned}$$

Substituting $\rho = 1/(\lambda - 1)$ into it, one has

$$\Delta = N(\varepsilon - \varepsilon^q)^2 N\left(\frac{1}{\lambda - 1}\right)^2\{[\mathrm{Tr}(\lambda) - 1]^2 - 4N(\lambda)\}.$$

14 Appendix 3: Density of Type I curves with hyperelliptic coverings

We give a more detailed analysis of Type I curves with hyperelliptic coverings here.

Recall that the matrix Θ under double-sided $\mathrm{PGL}_2(k)$-action can be represented by the following matrices:

$$(i) \quad \Theta_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad (ii) \quad \Theta_2 = \begin{pmatrix} 0 & e \\ 1 & 0 \end{pmatrix} \qquad \exists \eta \in k_2, \eta^2 = e \in k^\times \setminus \left(k^\times\right)^2.$$

Since

$$\lambda = \frac{(\beta - \alpha^q)(\beta^q - \alpha)}{(\beta - \alpha)^{1+q}} \neq 0, 1, \qquad \beta \in k_3 \setminus k, \quad \beta \neq \alpha, \alpha^q, \alpha^{q^2},$$

one has β_1 and β_2 corresponding to the two representatives of Θ_1 and Θ_2.

$$\beta_1 = \Theta_1 \cdot \alpha = -\alpha, \tag{166}$$

$$\lambda_1(\alpha) = \frac{(\alpha + \alpha^q)^2}{4\alpha^{1+q}}, \tag{167}$$

$$\beta_2 = \Theta_2 \cdot \alpha = \frac{e}{\alpha}, \tag{168}$$

$$\lambda_2(\alpha) = \frac{(e - \alpha^{1+q})^2}{(e - \alpha^2)^{1+q}}. \tag{169}$$

Cases (i) and (ii) do not overlap

Assume there is a λ in the intersection of cases (i) and (ii). Then,

$$\lambda_1(\gamma) = \frac{(\gamma + \gamma^q)^2}{4\gamma^{1+q}} = \frac{(e - \alpha^{1+q})^2}{(e - \alpha^2)^{1+q}} = \lambda_2(\alpha) =: \lambda, \qquad \exists \gamma, \alpha \in k_3 \setminus k. \tag{170}$$

Thus, the left half of (170) becomes

$$\gamma^{q-1} + 2 + \frac{1}{\gamma^{q-1}} = 4\lambda. \tag{171}$$

Then,

$$\gamma^{2(q-1)} + 2(1 - 2\lambda)\gamma^{q-1} + 1 = 0.$$

Denote $X := \gamma^{q-1}$; one has a quadratic equation

$$X^2 + 2(1 - 2\lambda)X + 1 = 0, \tag{172}$$

of which the discriminant is

$$D = 4(1 - 2\lambda)^2 - 4 = 4(1 - 4\lambda + 4\lambda^2 - 1) = 16\lambda(\lambda - 1) \neq 0$$

since $\lambda \neq 0, 1$.

Now, we use the right half of (170) to substitute for λ as λ_2:

$$\lambda - 1 \quad = \quad e\frac{(\alpha - \alpha^q)^2}{(e - \alpha^2)^{1+q}}, \tag{173}$$

$$D = 16\lambda(\lambda - 1) = 16\lambda\frac{(\alpha - \alpha^q)^2}{(e - \alpha^2)^{1+q}}e.$$

From (170), one knows that λ is a square or in $(k_3^\times)^2$. Also $\lambda - 1$ is a square. Thus, D is not a square or not in $(k_3^\times)^2$. This means that there is no solution to the equation (172). Therefore the intersection of cases (i) and (ii) is empty. □

The density of case (i)

We first find the cardinality of each orbit of λ_1 under the $\mathrm{PGL}_2(k)$-action.

Assume there are a γ and an α belonging to the same orbit under the $\mathrm{PGL}_2(k)$-action. From (170) and (171), one has

$$\gamma^{q-1} + \gamma^{1-q} = \alpha^{q-1} + \alpha^{1-q} = 4\lambda_1 - 2.$$

Define

$$X := \alpha^{q-1},\ Y := \gamma^{q-1}.$$

Then, the above equation becomes

$$(Y - X)(XY - 1) = 0.$$

Thus, we know

$$\text{either } Y = X \text{ or } Y = \frac{1}{X},$$

or

$$\gamma = l\alpha^{\pm 1} \qquad \exists l \in k^\times.$$

Therefore, fix an α such that $\alpha \in k_3 \setminus k, \alpha \neq \pm 1$; the number of γ which have the same orbit as either α or α^{-1} equals

$$\#\{\gamma | \lambda_1(\gamma) = \lambda_1\} = \#\{l \in k^\times\} \times 2 = 2(q - 1).$$

Thus,

$$\#\{\lambda_1\} = \frac{q^3 - q}{2(q - 1)} = \frac{q(q + 1)}{2}.$$

A lower bound for the density of case (ii)

To count the number of α corresponding to the same λ_2, we replace α in the following formula of λ_2 by the variable X:

$$\frac{(e - X^{1+q})^2}{(2 - X^2)^{1+q}} = \lambda_2 \neq 0, 1.$$

Then, one has the following equation in X:

$$\lambda_2(2 - X^2)^{1+q} = (e - X^{1+q})^2.$$

One can expand the above equation in the order of decreasing powers of X:

$$0 = (\lambda_2 - 1)X^{2+2q} + \cdots . \tag{174}$$

Since $\lambda_2 - 1 \neq 0$, we know that for a λ_2 there could be no more than $2(1+q)$ solutions (i.e., for α). Thus,

$$\#\{\alpha \mid \lambda_2(\alpha) = \lambda_2\} \leq 2(1+q).$$

Therefore, we have a lower bound for the number of $\mathrm{PGL}_2(k)$-orbits of λ_2 in case (ii):

$$\#\{\lambda_2\} \geq \frac{\#\{\forall \alpha \in k_3 \setminus k\}}{\#O(\lambda)} = \frac{q^3 - q}{2(1+q)} = \frac{q(q-1)}{2}.$$

Now, from Lemma 9, one knows that the summation of densities of cases (i) and (ii) equals q^2. Therefore, the above lower bound is the exact density of case (ii):

$$\#\{\lambda_2\} = q^2 - \#\{\lambda_1\} = q^2 - \frac{q(q+1)}{2} = \frac{q(q-1)}{2}.$$

15 Appendix 4: Classification of Type I curves with non-hyperelliptic coverings

Here, we give a more detailed classification for Type I curves with non-hyperelliptic coverings.

We have the following three classes of Type I curves with non-hyperelliptic coverings, where A under the double-sided action has three representatives:

1. $$A_1 = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \qquad a \neq 0, 1,$$

   i.e., $\beta = a\varepsilon$.

   In this case, C is hyperelliptic if and only if $a = -1$.

   Denote the number of λ corresponding to $\beta = \varepsilon^{q^i}$ in this case by δ_1,

   $$\delta_1 = \begin{cases} 1 & q \equiv 1 \bmod 3 \\ 0 & q \not\equiv 1 \bmod 3 \end{cases}.$$

   The number of λ_1 or, equivalently, of Type I curves with non-hyperelliptic coverings, is

   $$\#\{\lambda_1\} = \frac{1}{4}(q^3 - 2q^2 - 3q) - \delta_1.$$

2. $$A_2 = \begin{pmatrix} a & e \\ 1 & a \end{pmatrix}, \qquad \eta^2 = e \in k^\times \setminus (k^\times)^2.$$

   In this case, C is hyperelliptic if and only $a = 0$.

   Denote the number of λ corresponding to $\beta = \varepsilon^{q^i}$ in this case as δ_2,

   $$\delta_2 = \begin{cases} 1 & q \equiv 2 \bmod 3 \\ 0 & q \not\equiv 2 \bmod 3 \end{cases}.$$

   The number of λ_2 or, equivalently, of Type I curves with non-hyperelliptic coverings, is

   $$\#\{\lambda_2\} = \frac{q(q-1)^2}{4} - \delta_2.$$

3. $$A_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then, $\beta = \varepsilon + 1$.

In this case, no C is hyperelliptic.

Denote the number of λ corresponding to $\beta = \varepsilon^{q^i}$ in this case as δ_3,

$$\delta_3 = \begin{cases} 1 & char(k) = 3 \\ 0 & char(k) \neq 3 \end{cases}.$$

The number of λ_3 or, equivalently, of Type I curves with non-hyperelliptic coverings, is

$$\#\{\lambda_3\} = \frac{q(q^2-1)}{2q} - \delta_3.$$

Since

$$\sum_{i=1}^{3} \delta_i = 1,$$

the total number of Type I curves which have non-hyperelliptic coverings is

$$\sum_{i=1}^{3} \#\{\lambda_i\} \quad = \quad \frac{q^3-q^2-q-3}{2}. \tag{175}$$