Classification of Elliptic/Hyperelliptic Curves with Weak Coverings against the GHS Attack under an Isogeny Condition

Tsutomu Iijima [*] Fumiyuki Momose [†] Jinhui Chao [‡]

Abstract

The GHS attack is known to map the discrete logarithm problem(DLP) in the Jacobian of a curve C_0 defined over the d degree extension k_d of a finite field k to the DLP in the Jacobian of a new curve C over k which is a covering curve of C_0, then solve the DLP of curves C/k by variations of index calculus algorithms. It is therefore important to know which curve C_0/k_d is subjected to the GHS attack, especially those whose covering C/k have the smallest genus $g(C) = dg(C_0)$, which we called satisfying the isogeny condition. Until now, 4 classes of such curves were found by Thériault in [35] and 6 classes by Diem in [3][5]. In this paper, we present a classification i.e. a complete list of all elliptic curves and hyperelliptic curves C_0/k_d of genus 2, 3 which possess $(2, ..., 2)$ covering C/k of $\mathbb{P}^1$ under the isogeny condition (i.e. $g(C) = d \cdot g(C_0)$) in odd characteristic case. In particular, classification of the Galois representation of $\mathrm{Gal}(k_d/k)$ acting on the covering group $\mathrm{cov}(C/\mathbb{P}^1)$ is used together with analysis of ramification points of these coverings. Besides, a general existential condition of a model of C over k is also obtained. As the result, a complete list of all defining equations of curves C_0/k_d with covering C/k are provided explicitly. Besides the 10 classes of C_0/k_d already known, 17 classes are newly found.

Keywords : Weil descent attack, GHS attack, Elliptic curve cryptosystems, Hyperelliptic curve cryptosystems, Galois representation

Contents

[*] Koden Electoronics Co.,Ltd, 2-13-24 Tamagawa, Ota-ku, Tokyo, 146-0095 Japan

[†] Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

[‡] Department of Information and System Engineering, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan

1 Introduction

Let q be a power of an odd prime, $k := \mathbb{F}_q, k_d := \mathbb{F}_{q^d}$. We consider in this paper algebraic curves C_0/k_d used in cryptographic applications, i.e. elliptic and hyperelliptic curves of genera $g_0 := g(C_0) = 1, 2, 3$.

For these algebraic curve-based cryptosystems, the GHS attack was proposed by Gaudry, Hess and Smart[13] based on the idea of Frey[8] to apply Weil descent to elliptic curve cryptosystems. The GHS attack has been then extended and analyzed by many authors [3][10][16][17][18][24][25][26][35][36] and conceptually generalized to the cover attack by Frey and Diem[6]. The GHS attack, in terms of the cover attack, can be described as to map the DLP in the Jacobian of C_0/k_d to the DLP in the Jacobian of a covering curve C/k of C_0/k_d, then apply either the index calculus algorithms [14][30] when C is hyperelliptic or the algorithm in [4] when C is non-hyperelliptic or C is hyperelliptic but has been transformed to a non-hyperelliptic one [33].

A main approach for analysis of the GHS attack until now is to investigate the genus $g(C)$ of the covering curve C as a function of the extension degree d of the definition field k_d of C_0. The genus $g(C)$ of C was calculated on definition finite fields of characteristic 2 for elliptic curves C_0 using Artin-Schreier theory in [13] and generalized to arbitrary Artin-Schreier extensions in [16][17]. In [24][25] and [26], lower bounds of the above $g(C)$ of C were calculated for elliptic curves with prime or composite extension degrees in certain ranges which are cryptographically meaningful. When the lower bound of $g(C)$ is large enough the DLP will be infeasible but when the lower bound is small, the definition field therefore all curves defined on it are recommended to be avoided. In [3], Diem generalized the GHS attack to odd characteristic cases and by genus analysis using Kummer theory, he showed that on definition fields with prime extension degrees d, for all $d \geq 11$, the genus $g(C)$ will be very large when C exists, therefore, attacks to C become impractical.

These results based on genus analysis are very impressive and useful. On the other hand, the problem about when and for which C_0 such covering curves C actually exist still remained open. Besides, the approach using genus analysis show the possible range of the extension degrees d of the definition field k_d when C exists, without telling exactly if or not C_0 has a covering. In fact, even when the extension degree d of the definition field of a curve fallen in the "weak" range, it is still possible that it has no covering curve or every curve on the definition field is without covering so is perfectly secure to use in cryptosystems. In practice, cryptosystems often need to use particular finite fields or curves with certain properties in order to obtain efficient implementation, which however could be shut out by the above false-alarm of the GHS attack.

Thus, both theoretically and practically it is interesting and important to know exactly which curve C_0/k_d possesses covering C/k therefore is subjected to the GHS attack. It should be particularly useful to find all such weak curves so cryptosystem designers have complete information about which curve is weak and which is not.

In fact, after the first proposal of the GHS attack, a major effort has been to find particular classes of curves which have covering so are subjected to the GHS attack[13][10][36] [35][6] [5] [27][28][29]. Among them those C_0/k_d whose covering curve C/k has the genus $g = dg_0$ are particularly interesting.

Indeed, in order to transfer the DLP of $J_{k_d}(C_0)$ to $J_k(C)$, the genus of C is bounded from below: $g(C) \geq d \cdot g_0$. The equality holds when the Jacobians of C_0 and C are isogenous. Then the Jacobian of C has the smallest possible size which is the most favorable situation for attackers, or curves C_0/k_d having such coverings C/k are the weakest ones for cryptographic usage.

For odd characteristic case, Thériault obtained three families of curves whose function fields are Kummer extensions [35]. Among them, there are 4 classes of elliptic and hyperelliptic curves which have the genus $g = dg_0$.

C_0/k_d which possess covering curves C/k for $d = 3, 5, 7$ were obtained in [5][6]. In [5], Diem shown a table of curves C_0/k_d whose covering C have the smallest genera. Among them there are 9 classes whose covering curve C/k have the genus $g = dg_0$, among them 3 classes were contained in Thériault's results.

The existence of C_0/k_d with such a covering C/k or the completeness of results by Thériault and Diem is not clear at all. In fact, it was stated in [13] that "we wish the genus of C is linear in $n(= d$ in this paper), but it is highly unlikely such a curve exists at all".

On the other hand, there could be a large number of the curves satisfying the isogeny condition subjected to the GHS attack. E.g. more than a half of random elliptic curves E defined over k_3 in the Legendre form possess covering curves therefore a 160-bit system only has strength of 107 bits key-length[29].

In this paper, we aim to provide a full answer to these questions by classification of such C_0/k_d with covering C/k. We classified the elliptic and hyperelliptic curves which are subjected to the GHS attack or have covering curves, in particular, $(2, ..., 2)$-covering of C_0/k_d, i.e. those with covering groups of order 2^n for $1 < n \leq d$ in odd characteristic for $g_0 = 1, 2, 3$ and arbitrary d, under the following isogeny condition:

The isogeny condition:
"There is a covering map between C/k and C_0/k_d

$$\pi/k_d : C \twoheadrightarrow C_0 \tag{1}$$

such that for

$$\pi_* : \quad J(C) \twoheadrightarrow J(C_0), \tag{2}$$

$$Re(\pi_*) : \quad J(C) \longrightarrow Re_{k_d/k}J(C_0) \tag{3}$$

defines an isogeny over k, here $J(C)$ is the Jacobian variety of C and $Re_{k_d/k}J(C_0)$ is its Weil restriction with respect to the field extension k_d/k. Therefore $g(C) = d \cdot g_0$."

To obtain the curves in his table, Diem used invariance of ramification points of C_0/k_d. But since it still seemed to be difficult to exhaust all isogeny cases for arbitrary d, we used a representational approach or to classify the Galois representation of $\mathrm{Gal}(k_d/k)$ acting on the covering group $\mathrm{cov}(C/\mathbb{P}^1)$ besides the analysis of ramification points.

Furthermore, existence of a model of C over k is another interesting and practically important issue. It was proved by Diem in [3] that it is true for odd d in odd characteristic case for hyperelliptic curves. In this paper, we show more general existential conditions of a model of C over k.

As a result, a complete list of these weak curves C_0/k_d with explicit defining equations is obtained and contained in the section 7.

This classification list contains 27 classes of curves C_0/k_d including 17 new classes besides the 10 classes discovered by Thériault and Diem. Firstly, 4 classes of new patterns of ramification points besides the known 10 classes are included for $(g_0, n, d) = (1, 3, 7), (3, 3, 7), (3, 4, 15)$. Furthermore, 9 new classes are also shown explicitly when the x-coordinates of ramification points are not in k_d but certain extension fields of k_d for $(g_0, n, d) = (1, 2, 3)$, $(2, 2, 3), (3, 2, 3), (3, 3, 7)$. Besides, to use the generalized conditions for existence of k-model of C, we obtained the following 4 new classes in the cases of $(g_0, n, d) = (1, 2, 2), (1, 3, 3), (2, 2, 2), (3, 2, 2)$, where the definition equation of C_0/k_d are not monic in x but $y^2 = cf(x)$ where c is a non-square in k_d.

2 The GHS and cover attack

We suppose that the Frobenius automorphism $\sigma_{k_d/k}$ extends to an automorphism σ in the separable closure of $k_d(x)$. It is showed by Diem[3] that $\sigma_{k_d/k}$ can extend to an automorphism of order d on the Galois closure of $k_d(C_0)/k(x)$ when C_0 is a hyperelliptic curve and d is odd in the odd characteristic case. In the section 6, we will show a generalization of the result.

Under the assumption that σ has order d, the Galois closure of $k_d(C_0)/k(x)$ is $K := k_d(C_0)\cdot\sigma(k_d(C_0))\cdots\sigma^{d-1}(k_d(C_0))$ and the fixed field of K by the automorphism σ is $K' := \{\zeta \in K \mid \sigma(\zeta) = \zeta\}$. The original GHS attack maps the DLP in $Cl^0(k_d(C_0)) \cong J(C_0)(k_d)$ to the DLP in $Cl^0(K') \cong J(C)(k)$ using the following composition of conorm and norm maps

$$N_{K/K'} \circ Con_{K/k_d(C_0)} : Cl^0(k_d(C_0)) \longrightarrow Cl^0(K')$$

for elliptic curves in characteristic 2 case [13]. This attack has been extended to various classes of curves. It is also conceptually generalized to the cover attack by Frey and Diem[6] as described briefly as follows. When there exist an algebraic curve C/k and a covering $\pi/k_d : C \longrightarrow C_0$, the DLP in $J(C_0)(k_d)$ can be mapped to the DLP in $J(C)(k)$ by a pullback-norm map, as in the following diagram.

$$\begin{tikzcd}
J(C)(k_d) \arrow[d, "N"'] & J(C_0)(k_d) \arrow[l, "\pi^*"'] \arrow[dl, "N\circ\pi^*"] \\
J(C)(k) &
\end{tikzcd}$$

Unless otherwise noted, we consider the following hyperelliptic curves with $g(C_0) \in \{1, 2, 3\}$ given by

$$C_0/k_d \quad : \quad y^2 = c \cdot f(x) \tag{4}$$

where $c \in k_d^\times$ and $f(x)$ is a monic polynomial in $k_d[x]$ such that

$$C_0 \xrightarrow{2} \mathbb{P}^1(x) \tag{5}$$

is a degree 2 covering over k_d . Then, we have a $\overbrace{(2,\ldots,2)}^{n}$ covering or a covering $\pi/k_d : C \longrightarrow \mathbb{P}^1$ such that $\mathrm{cov}(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$, here $n \leq d$,

$$\mathrm{cov}(C/\mathbb{P}^1) := \mathrm{Gal}(k_d(C)/k_d(x)). \tag{6}$$

In language of function fields, it can be described by a tower of extensions of function fields such that $k_d(x, y, {}^{\sigma^1}y, \ldots, {}^{\sigma^{n-1}}y) \simeq k_d(C)$ is a $\overbrace{(2,...,2)}^{n}$ type extension.

Lemma 2.1. *The isogeny condition is equivalent to the each of following two statements.*
(A)

$${}^{\forall}I \subset \mathrm{cov}(C/\mathbb{P}^1),\ [\mathrm{cov}(C/\mathbb{P}^1) : I] = 2,$$

$$g(C/I) = \begin{cases} 0 & I \neq {}^{\sigma^i}H, {}^{\forall}i \\ g_0 & I \simeq {}^{\sigma^i}H, {}^{\exists}i \end{cases} \quad \text{or} \ \ C^I = C/I = \begin{cases} \mathbb{P}^1 & I \neq {}^{\sigma^i}H, {}^{\forall}i \\ {}^{\sigma^i}C_0 & I \simeq {}^{\sigma^i}H, {}^{\exists}i \end{cases}$$

here $C/H = C_0$.

(B) There is a subgroup H of index 2 in $\mathrm{cov}(C/\mathbb{P}^1)$ *such that the Tate module of $J(C)$ has the following decomposition*

$$V_l(J(C)) = \oplus_{i=0}^{d-1} \quad V_l(J(C))^{{}^{\sigma^i}H}. \tag{7}$$

3 Galois representation

We will classify all n-tuple $(2, ..., 2)$ coverings $C/\mathbb{P}^1$ with the degree 2 subcovering $C_0/\mathbb{P}^1$ as below.

$$\overbrace{C \longrightarrow \underbrace{C_0 \longrightarrow \mathbb{P}^1(x)}_{2}}^{\overbrace{(2,\cdots,2)}^{n}} \tag{8}$$

In order to do that, we consider and classify the representation of $\mathrm{Gal}(k_d/k)$ on $\mathrm{cov}(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$. For simplicity, we denote hereafter $\sigma_{k_d/k}$ as σ.

$$\begin{array}{rcl} \mathrm{Gal}(k_d/k) \times \mathrm{cov}(C/\mathbb{P}^1) & \longrightarrow & \mathrm{cov}(C/\mathbb{P}^1) \qquad (9) \\ (\sigma^i, \phi) & \longmapsto & {}^{\sigma^i}\phi := \sigma^i \phi \sigma^{-i} \qquad (10) \end{array}$$

Here, one has a map into $\mathrm{Aut}(\mathrm{cov}(C/\mathbb{P}^1))$.

$$\mathrm{Gal}(k_d/k) \hookrightarrow \mathrm{Aut}(\mathrm{cov}(C/\mathbb{P}^1)) \simeq GL_n(\mathbb{F}_2) \tag{11}$$

The representation of σ for given n, d has the following form in general. (We use the same notation for σ and its representation in the rest of this paper):

$$\sigma = \begin{pmatrix} \Delta_1 & O & \cdots & O \\ O & \Delta_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \Delta_s \end{pmatrix} \begin{matrix} \}n_1 \\ \}n_2 \\ \\ \}n_s \end{matrix}, \quad n = \sum_{i=1}^{s} n_i \tag{12}$$

where O stands for the zero matrix. The indecomposable subrepresentations

$$\Delta_i := \begin{pmatrix} \Omega_i & \Omega_i & \hat{O} & \cdots \\ \hat{O} & \Omega_i & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega_i \\ \hat{O} & \cdots & \hat{O} & \Omega_i \end{pmatrix} \begin{matrix} \}n_i/l_i \\ \}n_i/l_i \\ \vdots \\ \}n_i/l_i \end{matrix} \tag{13}$$

is an $n_i \times n_i$ matrix which has a form of an $l_i \times l_i$ block matrix. The sub-block Ω_i is an $n_i/l_i \times n_i/l_i$ matrix and $\hat{O}$ also the zero matrix. Here, we denote the characteristic polynomial of Ω_i as $f_i(x)$, the characteristic polynomial of Δ_i is $F_i(x) := f_i(x)^{l_i}$, $F(x) := LCM\{F_i(x)\}$ is the minimal polynomial of σ. Denoting d_i :=ord(Δ_i), one has $d = LCM\{d_i\}$.

Now define the minimal polynomial of σ as $F(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$. Then $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$. The Galois action of $\mathrm{Gal}(k_d/k)$ on y induces the following action:

$$^{\sigma^n}y \equiv \prod_{j=0}^{n-1} \left(^{\sigma^j}y\right)^{a_j} \mod k_d(x)^\times .$$

Therefore

$$^{\sigma^n}y^2 \equiv \prod_{j=0}^{n-1} \left(^{\sigma^j}y^2\right)^{a_j} \mod \left(k_d(x)^\times\right)^2 .$$

As a result, we obtain the following necessary and sufficient condition for existence of a model of C over k_d given n, d, σ :

C has a model over k_d if and only if

$$\begin{aligned} ^{F(\sigma)}y^2 &\equiv 1 \mod (k_d(x)^\times)^2 \quad \text{and} \\ ^{G(\sigma)}y^2 &\not\equiv 1 \mod (k_d(x)^\times)^2 \text{ for } {}^\forall G(x) \mid F(x), G(x) \neq F(x). \end{aligned} \tag{14}$$

4 Classification of C_0/k_d with covering C/k

Hereafter, let S be the set of the ramification points in $\mathbb{P}^1$ of the covering $C/\mathbb{P}^1$. Then according to the Riemann-Hurwitz genus formula,

$$2g(C) - 2 \quad = \quad 2^n(0-2) + \#S \cdot 2^{n-1}(2-1) \cdot 1. \tag{15}$$

Here ramification indices equal 2, and the number of fibres on C over a ramification point on $\mathbb{P}^1$ is 2^{n-1}, since the ramification group is cyclic for $\gcd(\mathrm{char}(k), 2) = 1$.

Therefore,

$$\#S = \frac{2g(C) - 2 + 2^{n+1}}{2^{n-1}} = 4 + \frac{d \cdot g_0 - 1}{2^{n-2}}. \tag{16}$$

These coverings can be classified to the following four cases.

4.1 The case when σ is indecomposable

We will treat the cases when d is even and odd separately.

4.1.1 When d is even

Assume $d = 2^r \cdot d'$ $(2 \nmid d')$. Representation of an indecomposable σ is in the form of the following block matrix:

$$\sigma = \left.\begin{pmatrix} \Omega & \Omega & \hat{O} & \cdots \\ \hat{O} & \Omega & \ddots & \ddots \\ \vdots & \ddots & \ddots & \Omega \\ \hat{O} & \cdots & \hat{O} & \Omega \end{pmatrix}\right\} n \tag{17}$$

Here $n = l \cdot m$, Ω is in $M_m(\mathbb{F}_2)$ such that $\Omega^{d'} = I$, and

$$\sigma^{2^r} = \begin{array}{cc} \begin{pmatrix} \tilde{\Omega} & \hat{O} & \hat{O} & \cdots \\ \hat{O} & \tilde{\Omega} & \ddots & \ddots \\ \vdots & \ddots & \ddots & \hat{O} \\ \hat{O} & \cdots & \hat{O} & \tilde{\Omega} \end{pmatrix} & \begin{array}{c} 1 \\ \\ \vdots \\ \\ l \end{array} \end{array} \quad , \sigma^d = (\sigma^{2^r})^{d'} = \begin{pmatrix} I & \hat{O} & \hat{O} & \cdots \\ \hat{O} & I & \ddots & \ddots \\ \vdots & \ddots & \ddots & \hat{O} \\ \hat{O} & \cdots & \hat{O} & I \end{pmatrix}. \tag{18}$$

Then, we have $2^{r-1} < l \le 2^r$ and $\Omega \in M_m(\mathbb{F}_2)$, $\Omega \notin M_{m'}(\mathbb{F}_2)$ for $1 \le {}^{\forall}m' \le m-1$. Here $M_m(\mathbb{F}_2)$ stands for $m \times m$ binary matrices. Since the minimal polynomial of Ω is in the form of $x^m + \tilde{a}_{m-1}x^{m-1} + \cdots + \tilde{a}_1 x + \tilde{a}_0$, we have

$$d' | (2^m - 1), \;\; d' \nmid (2^{m'} - 1), 1 \le m' \le m-1. \tag{19}$$

As we showed in the previous section, the number of the ramification points of $C/\mathbb{P}^1$ is $\#S = 4 + \frac{d \cdot g_0 - 1}{2^{n-2}}$. The numerator $d \cdot g_0 - 1$ of the fraction part in $\#S$ is odd since d is even. Then the denominator 2^{n-2} must be 1 since $\#S \in \mathbb{N}$. Therefore $n = 2$.

Now from $n = 2$ and $l > 1$, one has $m = 1, l = n = 2$. By (19), $d' = 1$ and $d = 2^r$. Since $2^{r-1} < 2 \leq 2^r = d$ and $r = 1$, therefore $d = 2$. Thus we know that $(d, n) = (2, 2)$ is the only possibility.

In fact, the general form of σ only appear in cases when the isogeny condition does not hold, which will be reported elsewhere.

4.1.2 When d is odd

(a) $d = 2^n - 1$

By the Riemann-Hurwitz genus formula, $2dg_0 - 2 = 2^n(-2) + 2^{n-1} \cdot \#S$. Therefore

$$\#S = \frac{2d(g_0 + 1)}{2^{n-1}} = \frac{d(g_0 + 1)}{2^{n-2}}. \tag{20}$$

Now, since d is odd, there exists a natural number $t \in \mathbb{N}$ such that $g_0 + 1 = t \cdot 2^{n-2}$. Then $\#S = d \cdot t$. Below we consider cases in which g_0 has different values:

- $g_0 = 1$
  In this case, $t = \frac{2}{2^{n-2}} \in \mathbb{N}$. It is obvious that only $n = 2, 3$ are possible. Therefore we have $(n, d) = (2, 3), (3, 7)$ since $d = 2^n - 1$.

- $g_0 = 2$
  In the similar manner, $t = \frac{3}{2^{n-2}} \in \mathbb{N}$ therefore $(n, d) = (2, 3)$.

- $g_0 = 3$
  $t = \frac{4}{2^{n-2}} \in \mathbb{N}$ therefore $(n, d) = (2, 3), (3, 7), (4, 15)$.

In the above cases, the representations of σ are $n \times n$ matrices whose orders are d. Then we have the following minimal polynomial $F(x)$ as a degree n irreducible factor of $x^d + 1$ for each σ:

- $(n, d) = (2, 3)$
  Since $x^3 + 1 = (x + 1)(x^2 + x + 1)$, we obtain $F(x) = x^2 + x + 1$.

- $(n, d) = (3, 7)$
  $F(x) = x^3 + x + 1$ or $F(x) = x^3 + x^2 + 1$ since $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

- $(n, d) = (4, 15)$
  $F(x) = x^4 + x + 1$ or $F(x) = x^4 + x^3 + 1$ since $x^{15} + 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

(b) $d \neq 2^n - 1$
For given n and d, we know that

$$\sigma \in M_n(\mathbb{F}_2),\ \sigma \notin M_l(\mathbb{F}_2) \text{ for } \ 1 \leq {}^{\forall} l \leq n-1. \tag{21}$$

Since $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$, we have

$$d|(2^n - 1),\ d \nmid (2^l - 1). \tag{22}$$

Then $3d \leq 2^n - 1$. Obviously, $n \geq 4$. From the Riemann-Hurwitz formula,

$$\#S = 4 + \frac{dg_0 - 1}{2^{n-2}}. \tag{23}$$

Therefore, g_0 is odd, which means that $g_0 = 1$ or 3. On the one hand, we have

$$\begin{aligned} \#S = 4 + \frac{dg_0 - 1}{2^{n-2}} &\geq 2g_0 + 3 && (24)\\ dg_0 - 1 &\geq 2^{n-1}(2g_0 - 1) && (25)\\ 2^{n-2} - 1 &\geq 2^{n-1}g_0 - dg_0 = (2^{n-1} - d)g_0. && (26)\end{aligned}$$

From now, we consider the two cases when $g_0 = 1$ and $g_0 = 3$:

- $g_0 = 1$
Since $\#S = 4 + \frac{d-1}{2^{n-2}} \in \mathbb{N}$, there exists a natural number $t \in \mathbb{N}$ such that $d = 1 + 2^{n-2}t$. We have already known that $2^n - 1 \geq 3d$, which does not hold if $t \geq 2$. Therefore, only $t = 1$ is possible. Now, as $d|(2^n - 1)$, we have

$$d = (1 + 2^{n-2})|(2^n - 1). \tag{27}$$

Then $d \mid \{4(2^{n-2} + 1) - 5\}$ since $2^n - 1 = 4(2^{n-2} + 1) - 5$. Therefore, $(n, d) = (4, 5)$ is the only possibility. In this case, σ is a 4×4 matrix whose order is 5 and the minimal polynomial $F(x)$ is $x^4+x^3+x^2+x+1$.

- $g_0 = 3$
We have $2^{n-2} - 1 \geq (2^{n-1} - d)3 = 3 \cdot 2^{n-1} - 3d$.
Furthermore,

$$3d \geq 3 \cdot 2^{n-2} - 2^{n-2} + 1 = 2^n + 2^{n-2} + 1, \tag{28}$$

which is against

$$2^n - 1 \geq 3d, \tag{29}$$

so this case does not exist.

4.2 The case when σ is decomposable

As a $\mathrm{Gal}(k_d/k)$-module, the representation of σ is a direct sum of indecomposable subrepresentations A_i.

$$\mathrm{cov}(C/\mathbb{P}^1) = A_1 \oplus \cdots \oplus A_r,\ r \geq 2,\ \#A_i = 2^{n_i} \tag{30}$$

Define

$$A'_i := \bigoplus_{j \neq i} A_j. \tag{31}$$

Under the isogeny condition, we know that

$$A_j \cap {}^{\sigma^i}H = \{0\} \text{ and } A_j \not\subset {}^{\sigma^i}H \text{ for } i = 0, ..., n-1. \tag{32}$$

Therefore, it follows that

$$g(C/A_j) = 0 \text{ for } j = 1, ..., r. \tag{33}$$

A similar argument also apply to A'_i, therefore we have

$$C/A_j = C/A'_i = \mathbb{P}^1 \text{ for } i, j = 1, ..., r. \tag{34}$$

If $r \geq 3$,

$$C/(A'_i \cap A'_j) = C/(\oplus_{l \neq i,j} A_l) = \mathbb{P}^1 \text{ for } {}^{\forall}i, j. \tag{35}$$

Thus, one obtains the following covering.

$$\begin{tikzcd}
 & & C/\bigcap_{l\neq i} A'_l \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
C/A'_1 \arrow[drr, dash] & \cdots C/A'_{i-1} \arrow[dr, dash] & & C/A'_{i+1} \cdots \arrow[dl, dash] & C/A'_r \arrow[dll, dash] \\
 & & \mathbb{P}^1 & &
\end{tikzcd}$$

Since $C/\bigcap_{l\neq i} A'_l = \mathbb{P}^1$, this implies one has a (2,..,2)-covering $\mathbb{P}^1/\mathbb{P}^1$ of degree $2^{\sum_{l\neq i} n_l}$. Now we consider a $\overbrace{(2, ..., 2)}^{\nu}$-covering $\mathbb{P}^1 \longrightarrow \mathbb{P}^1$. By the Riemann-Hurwitz genus formula, when $\mathrm{char}(k) \neq 2$, the number of the ramification points of this covering is $4 - \frac{1}{2^{\nu-2}}$. It follows that $\nu \leq 2$.

Therefore, we obtain $\sum_{l\neq i} n_l \leq 2$ for ${}^{\forall}i$. Thus, $r = 2$. Consequently, the only possibility is $n = n_1 + n_2 = 1 + 2 = 3, d = 3, g_0 = 1$ when σ is decomposable. This means that σ decomposes into a tensor product of 1 and a 2×2 matrix whose order is 3 :

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{36}$$

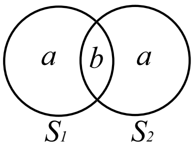
5 Defining equations of C_0/k_d for $c = 1$ or a square

Now we wish to determine the defining equations of C_0/k_d for given n, d. Hereafter, we assume that C is a model over k_d. In this section, we also assume that $c = 1$ (i.e. $c \in (k_d^\times)^2$) in (4). Then, it is sufficient to find a monic $f(x)$ in (4) such that C has a model over k_d (i.e. ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$). For $d = 2, 3$, it is possible to find $f(x)$ by using the Venn diagram to describe the sets of ramification points of ${}^{\sigma^{i-1}}C_0/\mathbb{P}^1$. In the section 6, we will treat explicit conditions for $c \in k_d^\times$ such that the curve C has a model over k, then determine the defining equations with a non-square c.

5.1 σ : indecomposable

5.1.1 d : even

From the section 4.1.1, the only possibility here is $d = 2, n = 2$. Thus, $\#S = 2g_0 + 3$. Let S_i be the set of ramification points of ${}^{\sigma^{i-1}}C_0/\mathbb{P}^1$ for $i = 1, 2$. Then $S = S_1 \cup S_2$. For $d = 2, n = 2$, the ramification points of ${}^{\sigma^{i-1}}C_0/k_2$ for $i = 1, 2$ and C/k on $\mathbb{P}^1$ can be represented by the following Venn diagram.



Here, $b := \#(S_1 \cap S_2)$, $a := \#S_1 - b = \#S_2 - b$. As a result, we obtain the following simultaneous equations :

$$\begin{cases} a + b = 2g_0 + 2 \\ 2a + b = \#S. \end{cases} \tag{37}$$

From the Riemann-Hurwitz genus formula, $\#S = 5, 7, 9$ for $g_0 = 1, 2, 3$. By solving the above simultaneous equations, one obtains $(a, b) = (1, 3), (1, 5), (1, 7)$ for $g_0 = 1, 2, 3$ respectively. Consequently, the defining equations C_0/k_2 are

$$y^2 = (x - \alpha)h(x) \tag{38}$$

where $h(x) \in k[x]$, $\alpha \in k_2 \setminus k$, $\deg h(x) = 2, \cdots, 7$. These three classes $(g_0, n, d) = (1, 2, 2), (2, 2, 2), (3, 2, 2)$ were obtained in [35] and [29].

5.1.2 d : odd

(a) $d = 2^n - 1$

In this case, all possibilities for (n, d) are $(2, 3)(3, 7)(4, 15)$ from the section 4.1.2. Recall that $F(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{F}_2[x]$ is the minimal polynomial of σ. Then $\sigma^n = a_{n-1}\sigma^{n-1} + \cdots + a_1\sigma + a_0$. Here, we define a homomorphism L of $k_d(x)^\times$ as follows:

$$\begin{aligned} L : k_d(x)^\times &\longrightarrow k_d(x)^\times && (39) \\ \mu &\longmapsto \prod_{i=0}^{d-1} \left({}^{\sigma^i}\mu\right)^{b_i}. && (40) \end{aligned}$$

Here, the sequence $\{b_i \in \mathbb{F}_2 | i = 0, \ldots, d-1\}$ is defined as follows:

$$\begin{aligned} b_0 = b_1 = \cdots = b_{n-1} = 1, && (41) \\ b_{n+j} := \sum_{i=0}^{n-1} a_{n-i}b_{n+i} \text{ for } \ j = 0, 1, \ldots, d-1-n. && (42) \end{aligned}$$

Then one can verify that

$$ {}^{F(\sigma)}\left\{ \prod_{i=0}^{d-1} \left({}^{\sigma^i}\mu\right)^{b_i} \right\} \equiv 1 \mod \left(k_d(x)^\times\right)^2. \tag{43}$$

Consequently, we have the following defining equation of C_0/k_d. Recall that $\#S = d \cdot t$. Assume t is decomposed into $t := t_1 + t_2 + \cdots + t_r$, $\alpha_i \in k_{d\cdot t_i}$, $k_d(\alpha_i) = k_{d\cdot t_i}$, $\left\{{}^{\sigma^\iota}\alpha_i\right\}_\iota \cap \left\{{}^{\sigma^\iota}\alpha_j\right\}_\iota = \emptyset$ $(i \neq j)$. Then we have

$$f(x) = \prod_{i=1}^{r} N_{k_{d\cdot t_i}/k_d}\left(L(x-\alpha_i)\right) = \prod_{i=1}^{r} N_{k_{d\cdot t_i}/k_d}\left(\prod_{j=0}^{d-1} {}^{\sigma^j}(x-\alpha_i)^{b_j} \right). \tag{44}$$

Recall the following minimal polynomial $F(x)$ for each (n, d):

- $(n, d) = (2, 3)$: $F(x) = x^2 + x + 1$
- $(n, d) = (3, 7)$: $F(x) = x^3 + x + 1$ or $F(x) = x^3 + x^2 + 1$
- $(n, d) = (4, 15)$: $F(x) = x^4 + x + 1$ or $F(x) = x^4 + x^3 + 1$.

Then one obtains the defining equations C_0/k_3 as follows:

- $g_0 = 1, d = 3, n = 2$
  $\#S = d \cdot t = 3 \cdot 2$, $F(x) = x^2 + x + 1$
  Then we have the following two cases.

  1. $t = t_1 + t_2 = 1 + 1$
     $\alpha_1, \alpha_2 \in k_3, \{\alpha_1, \alpha_1^q, \alpha_1^{q^2}\} \cap \{\alpha_2, \alpha_2^q, \alpha_2^{q^2}\} = \emptyset$
     $f(x) = \prod_{i=0}^{2}\left({}^{\sigma^i}(x-\alpha_1)^{b_i}\right) \prod_{j=0}^{2}\left({}^{\sigma^j}(x-\alpha_2)^{b_j}\right)$
     Since $b_1 = b_2 = 1, a_0 = a_1 = a_2 = 1, b_2 = a_2b_0 + a_1b_1 = 0$,
     $C_0/k_3 : y^2 = (x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$

2. $t = t_1 = 2$
   $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), k(\alpha_1) = k_6$
   $C_0/k_3 : y^2 = N_{k_6/k_3}\left(\prod_{i=0}^{2} {}^{\sigma^i}(x-\alpha_1)^{b_i}\right)$
   $\qquad = (x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^3})(x-\alpha_1^{q^4})$

   Here the case 1 was the equation (10) in [5] and referred as the Type I in [29]. The existence when $\alpha \in k_3 \setminus k$ was mentioned in the footnote 6 [3]. The general case including $\alpha \in k_6 \setminus (k_2 \cup k_3)$ was shown and referred as Type II in [29].

- $g_0 = 1, d = 7, n = 3$
  Since $\#S = d \cdot t = 7 \cdot 1 = 7$, then $t = t_1$.
  $\alpha \in k_7, k(\alpha) = k_7$

$$\begin{aligned} C_0/k_7 : y^2 &= L(x-\alpha) = \prod_{i=0}^{6}({}^{\sigma^i}(x-\alpha))^{b_i} \\ &= \begin{cases} (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4}) & \text{if } F(x) = x^3+x+1 \\ (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^5}) & \text{if } F(x) = x^3+x^2+1 \end{cases} \end{aligned}$$

Here, the first case was contained in [5], while the second case is newly found.

The two classes for $(g_0, n, d) = (3, 4, 15)$ are also unknown until now.

Lists of all defining equations for $g_0 = 2, 3$ are given in the classification list in the section 7. In fact, a new class of $(g_0, n, d) = (3, 3, 7)$ is also shown in the list.

(b) $d \neq 2^n - 1$

Since $x^5 + 1 = (x+1)(x^4+x^3+x^2+x+1)$, when $(n, d) = (4, 5)$, σ has the minimal polynomial $F(x) = x^4+x^3+x^2+x+1$. Recall that we need ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$ in order that C is a model over k_d. If this condition is satisfied, $f(x)$ has the following three possibilities for $\alpha \in k_5 \setminus k$:

$$\begin{aligned} (x-\alpha)(x-\alpha^q) &\mid f(x) \quad \text{or} \\ (x-\alpha)(x-\alpha^{q^2}) &\mid f(x) \quad \text{or} \\ (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3}) &\mid f(x). \end{aligned}$$

For $g_0 = 1$ and $\#S = 4 + 1 = 5$, it follows that

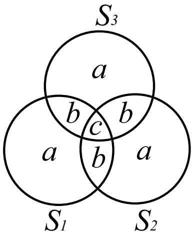
$$C_0/k_5 : y^2 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3}). \tag{45}$$

This class of curves was contained in the table in [5].

5.2 σ : decomposable

Recall that there exists only one case in which $g_0 = 1, n = 3, d = 3$ when σ is decomposable and $\#S$ is the number of ramification points of $C/\mathbb{P}^1$. By the Riemann-Hurwitz genus formula, $\#S = 4 + \frac{dg_0 - 1}{2^{n-2}} = 5$. Let S_i be the set of ramification points of ${}^{\sigma^{i-1}}C/\mathbb{P}^1$. Then, $\#S = \#(S_1 \cup S_2 \cup S_3)$. Now, $\#S_1 = \#S_2 = \#S_3 = 2g_0 + 2 = 4$ since $g_0 = 1$. Here, we define a, b, c as follows:

$$\begin{aligned}
c &:= \#(S_1 \cap S_2 \cap S_3), \\
b &:= \#(S_1 \cap S_2) - c = \#(S_2 \cap S_3) - c = \#(S_3 \cap S_1) - c, \\
a &:= \#S_1 - (2b + c) = \#S_2 - (2b + c) = \#S_3 - (2b + c).
\end{aligned}$$



Then we obtain the simultaneous equations as follows :

$$\begin{cases} a + 2b + c = 2g_0 + 2 \\ 3a + 3b + c = \#S. \end{cases} \tag{46}$$

In the case of $g_0 = 1, n = 3, d = 3, \#S = 5$, the solution of the equation is $a = 0, b = 1, c = 2$. Thus the defining equation is

$$C_0/k_3 : y^2 = (x - \alpha)(x - \alpha^q)h(x) \tag{47}$$

where $\alpha \in k_3 \setminus k$, $h(x) \in k[x], \deg h(x) = 2$ or 1. In fact, C is a hyperelliptic curve (see [29]). Notice that there do not exist other cases besides $g_0 = 1, n = 3, d = 3$ when σ is decomposable.

This class of C_0 was obtained in [35] and [29].

6 Existence of a model of C over k and defining equations of C_0

6.1 Existential condition of a model of C over k

Finally, we discuss conditions for existence of a model of C over k. One knows that a model of C over k exists if and only if the extension σ of the Frobenius automorphism $\sigma_{k_d/k}$ is an automorphism of order d on $k_d(C)$ in the separable closure of $k_d(x)$. In this section, we define $\hat{F}(x) \in \mathbb{F}_2[x]$ as the polynomial such that $x^d + 1 = F(x)\hat{F}(x) \in \mathbb{F}_2[x]$.

Lemma 6.1. *Assume that* ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$. *When* $\hat{F}(1) = 0$, *if c is a square element in* $(k_d^\times)^2$ *then C has a model over k. When* $\hat{F}(1) = 1$, *if σ does not have order d, there is a* $\phi \in \mathrm{cov}(C/\mathbb{P}^1)$ *such that $\sigma\phi$ has order d so we can adopt $\sigma\phi$ instead of σ. Therefore C always has a model over k when* $\hat{F}(1) = 1$.

Proof: Let $Q := \{\frac{b(x)}{a(x)} | k_d[x] \ni a(x), b(x) : \text{monic}\}$.
Since ${}^{F(\sigma)}f(x) \equiv 1 \mod (k_d(x)^\times)^2$, we have

$$\begin{aligned} {}^{F(\sigma)}y^2 &\equiv {}^{F(\sigma)}c = c^{F(q)} \mod (k_d(x)^\times)^2 & (48)\\ {}^{F(\sigma)}y &\equiv \epsilon c^{\frac{F(q)}{2}} \mod Q, \qquad \text{here } \epsilon = \pm 1 & (49)\\ {}^{\hat{F}(\sigma)F(\sigma)}y &\equiv {}^{\hat{F}(\sigma)}\epsilon c^{\frac{\hat{F}(q)F(q)}{2}} & (50)\\ {}^{\sigma^d+1}y &\equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d+1}{2}} & (51)\\ {}^{\sigma^d}y &\equiv \epsilon^{\hat{F}(1)} c^{\frac{q^d-1}{2}} y & (52) \end{aligned}$$

We first consider two possibilities of $F(1) = 1$ and $F(1) = 0$ respectively.

- Case $F(1) = 1$:
  We notice $\hat{F}(1) = 0$ in this case. Now, ${}^{\sigma^d}y \equiv c^{\frac{q^d-1}{2}} y$. In order that σ has order d (i.e. ${}^{\sigma^d}y \equiv y$), c needs to be a square $c \in (k_d^\times)^2$.

- Case $F(1) = 0$:
  Here, we consider further two possibilities of $\hat{F}(1) = 0$ and $\hat{F}(1) = 1$.
  (a) $\hat{F}(1) = 0$
  Similarly, ${}^{\sigma^d}y \equiv c^{\frac{q^d-1}{2}} y$. c should be a square element in $k_d^\times$.
  (b) $\hat{F}(1) = 1$
  Then ${}^{\sigma^d}y \equiv \epsilon c^{\frac{q^d-1}{2}} y$.
  If $\epsilon = +1$ and $c \in (k_d^\times)^2$, then σ has order d (i.e. ${}^{\sigma^d}y = y$).
  If $\epsilon = -1$ or $c \notin (k_d^\times)^2$, then σ has order $2d$.
  However, we can show that in this case there is a $\phi \in \mathrm{cov}(C/\mathbb{P}^1)$ such that $(\sigma\phi)^d = 1$.
  Indeed, suppose $d = 2^r \cdot d'$ $(2 \nmid d')$. Since ${}^{\sigma}\phi := \sigma\phi\sigma^{-1}$, we have

$$\begin{aligned} (\sigma\phi)^d &= \sigma\phi\sigma^{-1} \cdot \sigma^2\phi\sigma^{-2} \cdots \sigma^d\phi\sigma^{-d} \cdot \sigma^d & (53)\\ &= {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^d}\phi\ \sigma^d & (54)\\ &= {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r d'}}\phi\ \sigma^d. & (55) \end{aligned}$$

Now, we choose $\phi := {}^t(\overbrace{0, 0, \ldots, 1}^{m}, 0, \ldots, 0) \in \mathrm{cov}(C/\mathbb{P}^1)$. Define

$$I \text{ as the identity matrix, } J := \left.\begin{pmatrix} 0 & 1 & & O \\ \vdots & \ddots & \ddots & \\ \vdots & O & \ddots & 1 \\ 0 & \ldots & \ldots & 0 \end{pmatrix}\right\} m \leq 2^r .$$

Then $J^m = O$. We notice that the representation of σ is

$$\begin{pmatrix} \Delta & O \\ O & * \end{pmatrix} \text{ where } \Delta := I + J. \tag{56}$$

Here, ${}^{\sigma^i}\phi$ corresponds to $(I + J)^i \cdot {}^t(\overbrace{0, \ldots 0, 1}^{m})$. Now, since ${}^{\sigma^{2^r}}\phi = \phi$, $(\sigma\phi)^d = (\phi\ {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi)^{d'}\ \sigma^d$. Furthermore, since

$$I+(I+J)+\cdots+(I+J)^{2^r-1} = \begin{cases} O & \text{if } m < 2^r \\ \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 0 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & 0 \end{pmatrix} & \text{if } m = 2^r, \end{cases} \tag{57}$$

where O is the zero matrix, it follows that

$$\phi\ {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi = \begin{cases} {}^t(0, 0, \ldots, 0) & \text{if } m < 2^r \\ \psi := {}^t(1, 0, \ldots, 0) & \text{if } m = 2^r. \end{cases} \tag{58}$$

On the one hand, define K as the Galois closure of $k_d(C_0)/k(x)$, σ^d is an element in the center of $\mathrm{Gal}(K/k(x))$, i.e., $\sigma^d \in Z(\mathrm{Gal}(K/k(x))) = \{1, \psi\}$. When $\mathrm{ord}(\sigma) = 2d$, $\sigma^d = \psi$. Furthermore, notice that $m = 2^r$ in the case of (b). Thus, in the multiplicative notation,

$$(\sigma\phi)^d = (\phi\ {}^{\sigma}\phi\ {}^{\sigma^2}\phi \cdots {}^{\sigma^{2^r-1}}\phi)^{d'}\ \sigma^d = \psi^{d'} \cdot \psi = 1 \tag{59}$$

As a result, we can adopt the above $\sigma\phi$ instead of σ.

□

Consequently, we can determine defining equations of all classes of $C_0/k_d : y^2 = c \cdot f(x)$ whose covering curves C has a model over k under the isogeny condition. When $\hat{F}(1) = 0$, c has to be a square in k_d or can be regarded as 1, which has been treated in previous section.

6.2 Defining equations of C_0 with a non-square c

In this section, we will treat only classes of C_0/k_d having a non-monic defining equations with a non-square scalar c. These classes are therefore unknown until now. The defining equations of all classes of C_0/k_d can be found in the classification list in the section 7.

6.2.1 σ : indecomposable

- $g_0 = 1, n = 2, d = 2$

Here, $x^2 + 1 = (x + 1)^2$, thus $F(x) = (x + 1)^2, \hat{F}(x) = 1$.
Since $\hat{F}(x) = 1$, $\hat{F}(1) = 1$. From Lemma 6.1, c can be an arbitrary element in $k_2^\times$ in order that the curve C has a model over k. Extending the result of the section 5, we obtain

$$C_0/k_2 : y^2 = \eta(x - \alpha)h(x) \tag{60}$$

where $h(x) \in k[x]$, $\alpha \in k_2 \setminus k$, $\deg h(x) = 3$ or 2, $\eta =$ either 1 (i.e. a square) or a non-square element in k_2.

In the same manner, we can determine c also for $g_0 = 2, 3$ as follows.

- $g_0 = 2, n = 2, d = 2$

$$C_0/k_2 : y^2 = \eta(x - \alpha)h(x) \tag{61}$$

where $h(x) \in k[x]$, $\alpha \in k_2 \setminus k$, $\deg h(x) = 5$ or 4, $\eta =$ either 1 (i.e. a square) or a non-square element in k_2.

- $g_0 = 3, n = 2, d = 2$

$$C_0/k_2 : y^2 = \eta(x - \alpha)h(x) \tag{62}$$

where $\deg h(x) = 7$ or 6.

Thus the curves (60)(61)(62) contain (38) as a subcase.

6.2.2 σ : decomposable

Here, there exists only the case of $g_0 = 1, n = 3, d = 3$. Since $x^3 + 1 = (x + 1)(x^2 + x + 1), F(x) = x^3 + 1, \hat{F}(x) = 1$, then $\hat{F}(1) = 1$. Therefore c is either 1 or a non-square element in k_3. Then we obtain the defining equation of C_0/k_3 as

$$C_0/k_3 : y^2 = \eta(x - \alpha)(x - \alpha^q)h(x) \tag{63}$$

where $\eta =$ either 1 or a non-square element in k_3, $\alpha \in k_3 \setminus k$, $h(x) \in k[x], \deg h(x) = 2$ or 1. Notice that the curves (63) extends the class of (47).

7 Classification list of C_0/k_d with (2,...,2)-covering C/k

Curves in the following classification list are all classes of hyperelliptic curves C_0/k_d for $g(C_0) \in \{1, 2, 3\}$ which possess $(2, ..., 2)$ covering C/k of $\mathbb{P}^1$ under the isogeny condition. Here, $C_0/k_d : y^2 = c \cdot h_d(x)h(x)$, $h_d(x) \in k_d[x] \setminus k_u[x]$, $u||d$, $h(x) \in k[x]$, $\alpha \in k_d \setminus k_v, v||d$ (here $a||b$ means $a|b$ and $a \neq b$), η = either 1 or a non-square element in k_d.

Classification List

$C_0/k_d : y^2 = c \cdot h_d(x)h(x)$

g_0	n, d	c	$h_d(x)$	$\deg(h(x))$
1	$2, 2$	η	$x - \alpha$	3 or 2
	$2, 3$	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)$ Either $\alpha_1, \alpha_2 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}$ C:Hyper $\iff$ $^\exists A \in GL_2(k), \alpha_2 = A \cdot \alpha_1, Tr(A) = 0$ [29]	0
	$3, 3$	η	$(x-\alpha)(x-\alpha^q)$	2 or 1
	$4, 5$	1	$(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	0
	$3, 7$	1	(1) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^4})$ (2) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^5})$	0
2	$2, 2$	η	$x - \alpha$	5 or 4
	$2, 3$	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ Either $\alpha_1, \alpha_2, \alpha_3 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3 \in k_3 \setminus k$ or $\alpha_1 \in k_9 \setminus k_3, \alpha_2 = \alpha_1^{q^3}, \alpha 3 = \alpha_1^{q^6}$	0
3	$2, 2$	η	$x - \alpha$	7 or 6
	$2, 3$	1	$(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_3)(x-\alpha_3^q)$ $\times(x-\alpha_4)(x-\alpha_4^q)$ Either $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3, \alpha_4 \in k_3 \setminus k$ or $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3 \in k_6 \setminus (k_2 \cup k_3), \alpha_4 = \alpha_3^{q^3}$ or $\alpha_1 \in k_9 \setminus k_3, \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}, \alpha_4 \in k_3 \setminus k$ or $\alpha_1 \in k_{12} \setminus (k_6 \cup k_4), \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}, \alpha_4 = \alpha_1^{q^9}$	0
	$3, 7$	1	(1) $(x-\alpha_1)(x-\alpha_1^q)(x-\alpha_1^{q^2})(x-\alpha_1^{q^4})$ $\times(x-\alpha_2)(x-\alpha_2^q)(x-\alpha_2^{q^2})(x-\alpha_2^{q^4})$ (2) $(x-\alpha_1)(x-\alpha_1^{q^2})(x-\alpha_1^{q^3})(x-\alpha_1^{q^4})$ $\times(x-\alpha_2)(x-\alpha_2^{q^2})(x-\alpha_2^{q^3})(x-\alpha_2^{q^4})$ Either $\alpha_1, \alpha_2 \in k_7 \setminus k$ or $\alpha_1 \in k_{14} \setminus (k_2 \cup k_7), \alpha_2 = \alpha_1^{q^7}$	0
	$4, 15$	1	(1) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $\times(x-\alpha^{q^7})(x-\alpha^{q^{10}})(x-\alpha^{q^{11}})(x-\alpha^{q^{13}})$ (2) $(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $\times(x-\alpha^{q^5})(x-\alpha^{q^7})(x-\alpha^{q^8})(x-\alpha^{q^{11}})$ $\alpha \in k_{15} \setminus (k_3 \cup k_5)$	0

8 Discussion about the classification list

Here we discuss in more details of the classification list in the section 7 comparing with results obtained until now.

In fact, Thériault in [35] obtained 4 classes of C_0/k_d with covering C_k such that $g(C) = dg_0$. These 4 classes are $(g_0, n, d) = (1, 2, 2), (2, 2, 2), (3, 2, 2), (1, 3, 3)$, where in the notation of the classification list, these classes are with $\eta = 1$.

The table by Diem in [5] contained the following 9 classes of the curve C_0/k_d having covering curves C/k with different patterns of ramification points, which contained the 3 classes$(g_0, n, d) = (1, 2, 2), (2, 2, 2), (3, 2, 2)$ in [35] and 6 new classes as follows: $(g_0, n, d) = (1, 2, 3), (1, 4, 5), (1, 3, 7), (2, 2, 3), (3, 2, 3), (3, 3, 7)$, where $(1, 2, 3), (2, 2, 3), (3, 2, 3), (3, 3, 7)$ in the notation of the classification list has the x-coordinates α_i of the ramification points in $k_d \setminus k$. In both the $(1, 3, 7), (3, 3, 7)$ cases only one class was shown in [5] among the two classes in our list as explained below.

In the classification list which listed up all C_0/k_d which have isogenous covering curve C/k, the following classes are newly obtained.

In the first place, the following 4 classes with new patterns of ramification points are included. i.e.

(a) The $(g_0, n, d) = (1, 3, 7)$ case which contains a new class besides the class (1110100) (in Diem's symbol) already obtained in [5] and denoted in our list as (1). The new class is denoted as (2) which by Diem's symbol is (1110010).

(b) The $(g_0, n, d) = (3, 3, 7)$ case which also contains a new class besides the class (1110100)(1110100) contained in the table of [5], which is denoted in our list as (1). The new class is denoted as (2) which by Diem's symbol is (1011100)(1011100).

(c) The $(g_0, n, d) = (3, 4, 15)$ case where two new classes are found and denoted in our list as (1) and (2). In the Diem's symbol they are

$$(1)\quad (111100010011010) \tag{64}$$

$$(2)\quad (111101011001000) \tag{65}$$

In the second places, 9 new classes are explicitly shown when the x-coordinates of ramification points are not in k_d but certain extension fields of k_d. E.g. the curve shown in the eq.(10) in [5] had the x-coordinates a_i of the ramification points in $k_d \setminus k$. The curves with the same ramification pattern appeared also in $(g_0, n, d) = (1, 2, 3), (2, 2, 3), (3, 2, 3), (3, 3, 7)$. In the classification list, for $(g_0, n, d) = (1, 2, 3)$, besides the case $\alpha_1, \alpha_2 \in k_3 \setminus k$ which was contained in the table in [5], the case $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}$ is also included.

For $(g_0, n, d) = (2, 2, 3)$, besides the case $\alpha_1, \alpha_2 \in k_3 \setminus k$ which was contained in the table of [5], 2 new cases: $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3 \in$

$k_3 \setminus k$ and $\alpha_1 \in k_9 \setminus k_3, \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}$ are also included.

For $(g_0, n, d) = (3, 2, 3)$, besides the case $\alpha_i \in k_3 \setminus k$ which was contained in the table of [5], 4 new cases:

(i) $\alpha_1 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_3, \alpha_4 \in k_3 \setminus k$;

(ii) $\alpha_1, \alpha_3 \in k_6 \setminus (k_2 \cup k_3), \alpha_2 = \alpha_1^{q^3}, \alpha_4 = \alpha_3^{q^3}$;

(iii) $\alpha_1 \in k_9 \setminus k_3, \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}, \alpha_4 \in k_3 \setminus k$;

(iv) $\alpha_1 \in k_{12} \setminus (k_6 \cup k_4), \alpha_2 = \alpha_1^{q^3}, \alpha_3 = \alpha_1^{q^6}, \alpha_4 = \alpha_1^{q^9}$ are also included.

Besides, for $(g_0, n, d) = (3, 3, 7)$, while the curve (1) in the classification list in the case $\alpha_1, \alpha_2 \in k_7 \setminus k$, was contained in [5], the new case of $\alpha_1 \in k_{14} \setminus (k_2 \cup k_7), \alpha_2 = \alpha_1^{q^7}$ is added here. The similar new case is included also to the curve (2) in the classification list.

In the third place, due to the generalization of the conditions for existence of k-model of C, we have the following 4 new classes in the cases of $(g_0, n, d) = (1, 2, 2), (1, 3, 3), (2, 2, 2), (3, 2, 2)$, where the definition equation of C_0/k_d are not monic but $y^2 = cf(x)$ where $c = \eta$ is a non-square in k_d.

References

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

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

[4] C. Diem, “Index calculus in class groups of plane curves of small degree,” an extensive preprint from ANTS VII, 2005. Available from http://www.math.uni-leipzig.de/ diem/preprints/small-degree.ps

[5] C. Diem and J. Sholten, “cover attack,” preprint, 2003. Available from http://www.math.uni-leipzig.de/ diem/preprints/english.html

[6] C. Diem, “A study on theoretical and practical aspects of Weil-restrictions of varieties,” dissertation, 2001.

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

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

[9] G. Fujisaki, “Fields and Galois theory,” Iwanami, 1991, in Japanese.

[10] S. Galbraith, “Weil descent of jacobians,” Discrete Applied Mathematics, 128 no.1, pp.165–180, 2003.

[11] P. Gaudry, “An algorithm for solving the discrete logarithm problem on hyperelliptic curves,” Advances is Cryptology-EUROCRYPTO 2000, Springer-Verlag, LNCS 1807, pp.19–34, 2000.

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

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

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

[15] N. Hashizume, F. Momose and J. Chao, “On implementation of GHS attack against elliptic curve cryptosystems over cubic extension fields of odd characteristics ,” preprint, 2008. Available from http://eprint.iacr.org/2008/215

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

[17] F. Hess, “Generalizing the GHS attack on the elliptic curve discrete logarithm,” LMS J. Comput. Math.7 , pp.167–192, 2004.

[18] T. Iijima, M. Shimura, J. Chao, and S. Tsujii, “An extension of GHS Weil descent attack,” IEICE Trans. vol.E88-A, no.1,pp97–104 ,2005.

[19] T. Iijima, F. Momose, and J. Chao, “On certain classes of elliptic/hyperelliptic curves with weak coverings against GHS attack,” Proc. of SCIS2008, IEICE Japan, 2008.

[20] T. Iijima, F. Momose, and J. Chao, “Classification of Weil restrictions obtained by $(2, \ldots, 2)$ coverings of $\mathbb{P}^1$ without isogeny condition in small genus cases,” Proc. of SCIS2009, IEICE Japan, 2009.

[21] T. Iijima, F. Momose, and J. Chao, “Classification of elliptic/hyperelliptic curves with weak coverings against GHS attack without isogeny condition,” Proc. of SCIS2010, IEICE Japan, 2010.

[22] T. Iijima, F. Momose, and 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.

[23] S. Lang, “Algebra (Revised Third Edition),” Graduate Text in Mathematics, no.211, Springer-Verlag, 2002.

[24] M. Maurer, A. Menezes, and E. Teske, “Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree,” LMS J. Comput. Math.5 , pp.127–174, 2002.

[25] 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.

[26] A. Menezes, E. Teske, and A. Weng, “Weak fields for ECC,” Topics in Cryptology CT-RSA 2004, Springer-Verlag, LNCS2964 , pp.366–386, 2004.

[27] 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

[28] 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

[29] F. Momose and J. Chao, “Elliptic curves with weak coverings over cubic extensions of finite fields with odd characteristics,” J. Ramanujan Math.Soc, 28 no.3, pp.299–357, 2013.

[30] K. Nagao, “Improvement of Thériault algorithm of index calculus for jacobian of hyperelliptic curves of small genus,” preprint, 2004. Available from http://eprint.iacr.org/2004/161

[31] M. Shimura, F. Momose, and J. Chao, “Elliptic curves with weak coverings over cubic extensions of finite fields with even characteristic,” Proc. of SCIS2010, IEICE Japan, 2010.

[32] M. Shimura, F. Momose, and J. Chao, “Elliptic curves with weak coverings over cubic extensions of finite fields with even characteristic II,” Proc. of SCIS2011, IEICE Japan, 2011.

[33] B. Smith, “Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves,” Advances in Cryptology-EUROCRYPTO 2008, Springer-Verlag, LNCS 4965, pp.163–180, 2008.

[34] H. Stichtenoth, “Algebraic function fields and codes,” Universitext, Springer-Verlag, 1993.

[35] N.Thériault, “Weil descent attack for Kummer extensions,” J. Ramanujan Math. Soc, 18, pp.281–312, 2003.

[36] N.Thériault, “Weil descent attack for Artin-Schreier curves,” preprint, 2003. Available from http://homepage.mac.com/ntheriau/weildescent.pdf

[37] N.Thériault, “Index calculus attack for hyperelliptic curves of small genus,” Advances in Cryptology-ASIACRYPT 2003, LNCS 2894, pp.75–92, 2003