Classification of Weil restrictions obtained by $(2, ..., 2)$ coverings of $\mathbb{P}^1$

(An extended summary)

Fumiyuki Momose, Jinhui Chao

Dept. of Mathematics, and Dept. of Information and Sysytem Engineering
Chuo University, Tokyo, Japan

August 1, 2006

Abstract

In this paper, we show a general classification of cryptographically used elliptic and hyperellipti curves which can be attacked by the Weil descent attack and index calculus algorithms. In particular, we classfy all the Weil restriction of these curves obtained by $(2, ..., 2)$ covering. Density analysis of these curves are shown. Explicit defintion equations of such weak curves are also provided.

Contents

1 Introduction **3**

2 Indecomposable cases **6**
2.1 Case $2|d$ 6
2.2 Case $2 \not| d$ 7

3 Classification **8**
3.1 Case $2|d$ 8
3.2 Case $\mathrm{char}(k) \neq 2$ 8

4 Indecomposable and $2|d$ case **9**
4.1 Ordinary cases 10

5 Indecomposable non-ordinary and $d \neq 2^n - 1$ cases **11**
5.1 Defining Equation of C_0 13

6 Indecomposable with $2 \not| d,\ d \neq 2^n - 1$ **13**
6.1 Case char$(k) \neq 2$ 13
6.2 Case char$(k) = 2$ 14
6.2.1 Ordinary cases ($d \leq \frac{2^n-1}{3}$) 14

7 Indecomposable and $d = m = 2^n - 1$ **17**
7.1 Case char$(k) \neq 2$ 17
7.2 Case char$(k) = 2$ 18
7.2.1 Necessary condition 18
7.2.2 Sufficient condition 20
7.2.3 On $g(x)$ 21

8 Decomposable case **24**
8.1 Char$(k) \neq 2$ case 25
8.2 Char$(k) = 2$ case 27

9 Lists of classifications **30**

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 which are supposed to secure for cryptographic applications, i.e. those of genera $g_0 := g(C_0) = 1, 2$ and $g_0 = 3$ hyperelliptic curves.

It is known that at present the most powerful attacks to the cryptosystems based on these curves are the so-called double-large-prime variation by Gaudry-Theriault-Thome and Nagao [12], [20], with complexities $\tilde{O}(q^{2-\frac{2}{g}})$. In particular for $g = 3$, the cost is $\tilde{O}(q^{4/3})$, a little faster than the square-root attacks. Hyperelliptic curves of genera 5 to 9 are attacked by these algorithms more effectively than the square-root attacks.

Recently Diem proposed an attack under which non-hyperelliptic curves of low degrees and genera greater than or equal to 3 are weaker than hyperelliptic curves[6]. In particular, if C is a non-hyperelliptic curve over k of genus $g \geq 3$, such that $\deg C = d$,the complexity of Diem's double-large-prime variation [6] is $\tilde{O}(q^{2-\frac{2}{d-2}})$. When $d = g + 1$, it is $\tilde{O}(q^{2-\frac{2}{g-1}})$. In particular, genus 3 non-hyperelliptic curves over $\mathbb{F}_q$ can be attacked in an expected time $\tilde{O}(q)$.

Another generic attack to algebraic curve-based cryptosystem is the so-called Weil descent attack or cover attack [9] [13][10] [17][5] [15][16] [24][25][7].

To consider the Weil descent attack to C_0/k_d, we assume that there is a covering C/k of C_0/k_d and

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

such that for

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

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

is an isogeny, here $J(C)$ is the Jacobian variety of C and $Re_{k_d/k}J(C_0)$ its Weil restriction. Then $g(C) = dg_0$.

It is an interesting and important question to see what kind and how many curves C_0 have weak coverings or their Weil restrictions can be attacked by the above two index calculus algorithms, even they are designed to be secure over extension fields k_d.

The classification and density analysis of these weak curves seemed to be a nontrivial problem. It is also believed that even if such curves did exist, they must be very special therefore rare.

In [19] a classification and density analysis is provided for odd characteristics and genus 1,2,3 elliptic and hyperelliptic curves for extension degree 2,3,5. It is shown that actually the number of these weak curves could be alarmingly large. e.g. for $g_0 = 1, d = 3$, if you chosen random elliptic curves E defined over k_3 in the Legandre form, then a half of them are weak and can not be used in cryptosystems since a 160-bit systems could only have strength of 107 bits key-length under the proposed attack.

In this paper, we will show a general classification the elliptic and hyperellipti curves which can be attacked by the Weil descent attack and index calculus algorithms. In particular, we classfy all the Weil restriction of these curves obtained by $(2, ..., 2)$ covering. We show that when such coverings exist, these curves can be attacked effectively by Weil descent attack except for the case $(g_0, d) = (1, 2), (1, 3)$ and C is hyperelliptic. Density analysis of these curves are shown. Explicit defintion equations of such weak curves are also provided.

We consider that following curves.

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

such that

$$C_0 \stackrel{2}{\longrightarrow} \mathbb{P}^1(x)/k \tag{5}$$

is a degree 2 covering.

Then we have a tower of extensions of function fields such that $k_d(x, \{^{\sigma^i}y\}_i)/k_d(C_0)$ is a $\overbrace{(2, ..., 2)}^{n}$ type extension.

Correspondingly C/k is a $\overbrace{(2, ..., 2)}^{n}$ covering of $\mathbb{P}^1(x)/k$.

$$\begin{array}{ccc}
k_d(x, \{^{\sigma^i}y\}_i) & & C/k \\
| & & | \\
k_d(C_0) & & C_0/k_d \\
| & & | \\
k_d(x) & & \mathbb{P}^1(x)/k
\end{array}$$

Bellow, we assume

Condition (C):

$$Re(\pi_*): \quad J(C) \longrightarrow Re_{k_d/k}(J(C_0)) \tag{6}$$

is an isogeny over k.

Lemma 1. *The Condition (C) is equivalent to the following statemant.*

$\exists H < cov(C/\mathbb{P}^1)$, a subgroup of index 2 such that the Tate module of $J(C)$ has the following decomposition

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

We will classify all $(2, ..., 2)$ coverings of

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

satisfying the Condition (C).

We will make use of classification of representation of $G(k_d/k)$ on $\mathrm{cov}(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$.

$$G(k_d/k) = <\sigma> \quad \curvearrowright \quad cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n \tag{9}$$

We show that the following cases are subjected to the Weil descent attacks.

The char$(k) \neq 2$ cases:

d	n	Hyper/Nonhyper	g_0	$\#C_0$	
2	3	Hyper		$O(q^{2g_0})$	
3	2			$O(q^{3g_0})$?	$g_0 = 1$ OK
		Hyper	1	$O(q^2)$	
$2^n - 1$	≥ 3	Nonhyper		$O(q^{d\ell-3})$?(*)	
5		Nonhyper	1	$O(q^2)$	

(*) ℓ $s.t.$ $g_0 + 1 = 2^{n-2}\ell$

Note: Here "?" means a conjectured density.

For char$(k) = 2$ case:

d	n	Hyper?	g_0	Ordin?	$\#C_0$
2	2	Hyper			$O(q^{2g_0})$
4	3	Hyper			$O(q^{2g_0+1})$
$2^n - 1$					$O(q^{(n+1)(g_0+1)-3})$
		Hyper	1	Ordin	$O(q^n)$?
	e.g. 2				$O(q^2)$
$(2^{n_1}-1)(2^{n_2}-1)$ $2 \leq n_1, n_2$ $(2^{n_1}-1, 2^{n_2}-1) = 1$		Nonhyper	1	Ordin	$O(q^{n_1+n_2-1})$?

Note: Here "?" means a conjectured density.

2 Indecomposable cases

2.1 Case $2|d$

Then $d = 2^r$ and since σ is indecomposable, it is in a form of irreducible Jordan cell

$$\sigma = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 0 \\ 0 & 1 & 1 & \cdots & \\ 0 & 0 & 1 & 1 & \cdots \\ \vdots & \cdots & \cdots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \tag{10}$$

Then we know that

$$2^{r-1} < n \leq 2^r = d \tag{11}$$

Indeed,

$$(\sigma + I)^n = 0. \tag{12}$$

On the other hand, $d = 2^r$ is the first integer s.t.

$$\mathrm{ord}(\sigma) = d = 2^r \qquad \sigma^{2^r} = I \tag{13}$$

Thus, $d = 2^r$ is also the first integer s.t.

$$(\sigma^{2^r} + I)^{2^r} = \sigma^{2^r} + I = 2I = 0 \tag{14}$$

$$2^{r-1} < n \leq 2^r \tag{15}$$

the first inequality is due to that $(\sigma + I)^{2^{r-1}} \neq 0$.

2.2 Case $2 \not| d$

$$d | \, 2^n - 1, \quad d \not| \, 2^l - 1, \quad (1 \leq \forall l \leq n-1) \tag{16}$$

Let $\zeta = \zeta_d$ be a primitive d-th root of 1 in $\overline{\mathbb{F}}_2$.

Let the minimal polynomial of ζ over $\mathbb{F}_2$ as

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i, \quad a_0 = 1, \; a_i \in \mathbb{F}_2 \tag{17}$$

Then

$$\zeta^n = \sum_{i=0}^{n-1} a_i \zeta^i \tag{18}$$

One can take a representation of $G(k_d/k)$ acting on $cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n$

$$\forall v \in cov(C/\mathbb{P}^1), \quad {}^{\sigma^n} v = \sum_{i=0}^{n-1} a_i \; {}^{\sigma^i} v \tag{19}$$

The number of irreducible representations of such action is

$$\frac{\varphi(d)}{n} \tag{20}$$

In the case $d = 2^n - 1 =: m$, define a k-linear map L of $k_m(C)$

$$L: \quad k_m(C) \longrightarrow k_m(C) \tag{21}$$

$$\forall h \in k_m(C), \qquad L(h) :={}^{\sigma^n} h + \sum_{i=0}^{n-1} a_i \; {}^{\sigma^i} h \tag{22}$$

Define a sequence $\{b_i \in \mathbb{F}_2, i = 0, m-1\}$ as

$$b_0 = b_1 = ... = b_{n-1} = 1, \quad a_n = 1, \tag{23}$$

$$b_{n+l} = \sum_{i=0}^{n-1} a_{n-i} b_{l+i}. \qquad l = 0, 1, ..., m-1-n \tag{24}$$

Then a homomorphism M of $k_m(x)^\times$ is defined as

$$M: \quad k_m(x)^\times \longrightarrow k_m(x)^\times \tag{25}$$

$$\forall h \in k_m(x)^\times, \qquad M(h) := \prod_{i=0}^{m-1} ({}^{\sigma^i} h)^{b_i} \tag{26}$$

3 Classification

3.1 Case $2|d$

We show that in this case, C is a hyperellpitic curves

In fact,

$$\sigma = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 0 \\ 0 & 1 & 1 & \cdots & \\ 0 & 0 & 1 & 1 & \cdots \\ \vdots & \cdots & \cdots & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \tag{27}$$

Then for the $\phi \in cov(C/\mathbb{P}^1)$

$$\phi/k = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}^T \tag{28}$$

$$^{\sigma}\phi = \phi \tag{29}$$

If we consider the degree two covering over k

$$C \xrightarrow{2} C/\phi \tag{30}$$

By the Condition (C),

$$C/\phi = \mathbb{P}^1 \tag{31}$$

3.2 Case char$(k) \neq 2$

When char$(k) \neq 2$,

$$n = d = 2 \tag{32}$$

Indeed, by RH,

$$2dg_0 - 2 = 2^n(-2) + 2^{n-1}S \tag{33}$$

here S is the number of fixed points on $\mathbb{P}^1$, then

$$S = 4 + \frac{dg_0 - 1}{2^{n-2}} \tag{34}$$

Since $2|d$, $n = 2$, which means $d = 2$ and $S = 2g_0 + 3$.

The C_0 is defined by

$$C_0 : \quad y^2 = (x - \alpha)g(x) \tag{35}$$

$$\alpha \in k_2 \setminus k, \quad g(x) \in k[x] \tag{36}$$

4 Indecomposable and $2|d$ case

By 3.1, we can assume that $\mathrm{char}(k) = 2$. Then

$$d = 2^r, \quad s.t. \quad 2^{r-1} < n \leq 2^r \tag{37}$$

We will use the ramification theory of Galois extension of a complete field with a discrete valuation.

Assume the characteristic equals $p > 0$. Consider a Galois extension K_2/K_1 such that $G(K_2/K_1)$ is of p-power order. Denote t the uniformizer of K_2 and x of K_1. ν: the valuation on K_2.

Definition 1.

$$G \ni \sigma \neq 1, \quad \iota(\sigma) \; := \nu({}^{\sigma}t - t) \tag{38}$$

$$\iota(1) \; = \infty \tag{39}$$

Since $G(K_2/K_1)$ has an order of p-power, we know $\iota(\sigma) \geq 2$.

$$\mathbb{R} \ni u \geq -1, \quad G_u \; := \; \{ \; \sigma \in G(K_2/K_1) \quad | \quad \iota(\sigma) \geq u+1 \; \} \tag{40}$$

$$\gamma_u \; := \; \#G_u \tag{41}$$

Then we know

$$G \; \triangleright \; G_u \tag{42}$$

$$G \; = \; G_0 \triangleright G_1 \triangleright G_2 \cdots \tag{43}$$

Now we define the function $\psi(u), u \geq 1$

$$l \in \mathbb{N}, \qquad l \leq u < l+1 \tag{44}$$

$$\psi(u) \; := \; \frac{1}{\gamma_1} \left\{ \sum_{i=1}^{l} \gamma_i + (u-l)\gamma_{l+1} \right\} \tag{45}$$

and

$$G_u := G^{\psi(u)} \tag{46}$$

It is known that

Theorem 1. *[22]*

$$\forall H \lhd G, \quad \forall u, \quad (G/H)^u = G^u H \big/ H \tag{47}$$

Theorem 2. *(Hasse-Arf)[22]*
If G is an abelian group, then

$$G_u \neq G_{u+1} \Longrightarrow \psi(u) \in \mathbb{Z} \tag{48}$$

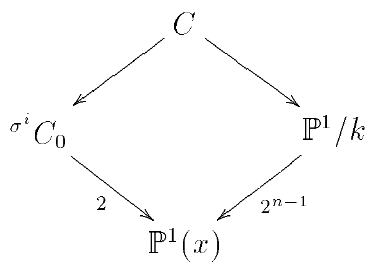
We will apply these results to the case when $p = 2$ and $G(K_2/K_1)$ is $(2, 2, ..., 2)$ type.

4.1 Ordinary cases

$$C_0: \quad y^2 + g(x)y = f(x) \tag{49}$$
$$\deg g(x) = g_0 + 1, \quad \deg f(x) = 2g_0 + 2 \tag{50}$$

By the section 2, we know that C is hyperelliptic.
Since C is ordinary,

$$\forall \phi \in cov(C/\mathbb{P}^1), \ \ \forall P \in C, \quad \phi(P) = P \tag{51}$$
$$\Longrightarrow \qquad \nu_P(\phi) = 2 \tag{52}$$



The number of ramification points of ${}^{\sigma^i}C_0/\mathbb{P}^1(x)$ is $g_0 + 1$, while the ramification point of $\mathbb{P}^1/k/\mathbb{P}^1(x)$ is 0 alone. Therefore, $g(x) \in k[x]$.
Apply the Riemann-Hurwitz to the degree two covering $C \longrightarrow \mathbb{P}^1$

$$2dg_0 - 2 = 2(-2) + S \tag{53}$$
$$S = 2(dg_0 + 1) \tag{54}$$

On the other hand,

$$S = 2^{n-1} \times 2g_0 \tag{55}$$
$$or = 2^{n-1} \times 2g_0 + 2 \tag{56}$$

therefore

$$(2^{n-1} - d)g_0 \leq 1, \qquad (n \geq 2) \tag{57}$$
$$d = 2^{n-1} \tag{58}$$

Hence by $2^{n-2} < n \leq 2^{n-1}$,

$$n = 2,3 \tag{59}$$
$$d = 2,4 \tag{60}$$

5 Indecomposable non-ordinary and $d \neq 2^n - 1$ cases

$$\exists H < cov(C/\mathbb{P}^1), \text{ of index 2}, \ s.t. \ C/H = \mathbb{P}^1 \tag{61}$$

First, notice that for the degree two covering with P, Q as ramification points

$$\mathbb{P}^1 \longrightarrow \mathbb{P}^1(x) \tag{62}$$
$$P \longrightarrow P_0 \tag{63}$$
$$\nu_P(\phi) = 2 \tag{64}$$

and for the degree two covering

$$^{\sigma^i}C_0 \longrightarrow \mathbb{P}^1(x) \tag{65}$$
$$Q \longrightarrow Q_0 \tag{66}$$
$$\exists Q \quad s.t. \quad \nu_Q(\phi) \geq 3 \tag{67}$$

due to non-ordinary assumption.

$$I := < \{\phi \in cov(C/\mathbb{P}^1) : \exists P \in \mathbb{P}^1(x), \nu_P(\phi) \geq 3\} > \subsetneq cov(C/\mathbb{P}^1) \tag{68}$$

Then

$$\forall H < cov(C/\mathbb{P}^1), \qquad \text{of index } 2 \tag{69}$$
$$C/H = \mathbb{P}^1 \iff I \subset H \tag{70}$$

Assume that

$$\#I = 2^a, \qquad (1 \leq a \leq n-1) \tag{71}$$

then

$$\begin{aligned} \#\{H < cov(C/\mathbb{P}^1), \ \text{of index } 2, \ g(C/H) = g_0\} &= d \\ \Longrightarrow \ \#\{H < cov(C/\mathbb{P}^1), \ \text{of index } 2, \ C/H = \mathbb{P}^1\} &= 2^n - 1 - d \end{aligned}$$

But

$$\#\{H < cov(C/\mathbb{P}^1), \ \text{of index } 2, \ C/H = \mathbb{P}^1\} \tag{72}$$
$$= \#\{H < cov(C/\mathbb{P}^1), \ \text{of index } 2, \ H \supset I\} = 2^a - 1 \tag{73}$$

Thus

$$2^n = d + 2^a, \qquad (1 \leq a \leq n-1) \tag{74}$$
$$d = 2^{n-1}, \quad a = n-1 \tag{75}$$
$$\Longrightarrow \quad n = 2, 3 \tag{76}$$

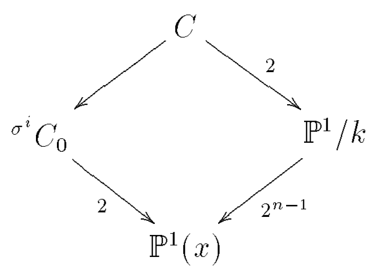
Next, we show that $g(x) \in k[x]$.
Assume

$$g(x) = x^a g_1(x), \qquad g_1(0) \neq 0, \quad (a \geq 1) \tag{77}$$

Then we have

$$^{\sigma^i}g(x) = x^a \ ^{\sigma^i}g_1(x) \tag{78}$$

From



we have

$$^{\sigma^i}g_1(x) = g_1(x) \tag{79}$$

5.1 Defining Equation of C_0

$$\begin{aligned} C_0 : \quad y^2 + g(x)y &= f(x) && (80) \\ {}^{\sigma} f(x) &= f(x) + g^2(x)l(x) && (81) \\ \deg l(x) &= 1, 2 && (82) \\ \text{and } \deg(l(x) +^{\sigma} l(x)) &= 1, 2 \quad \text{if } n = 3 && (83) \end{aligned}$$

6 Indecomposable with $2 \not| d,\ d \neq 2^n - 1$

In this case, we have

$$d|(2^n - 1), \qquad (d \not| (2^l - 1), \ \ 1 \leq l \leq n-1, \ \ n \geq 4) \tag{84}$$

6.1 Case char$(k) \neq 2$

By RH, denote by S again the number of fixed points over $C_0/\mathbb{P}^1(x)$

$$\begin{aligned} 2dg_0 - 2 &= 2^n(-2) + 2^{n-1}S && (85) \\ \Longrightarrow S &= 4 + \frac{dg_0 - 1}{2^{n-2}} && (86) \end{aligned}$$

Since $n \geq 4$, g_0 is an odd integer, thus

$$S \geq 2g_0 + 3 \tag{87}$$

Then

$$\begin{aligned} (2^{n-1} - d)g_0 &\leq 2^{n-2} - 1 && (88) \\ \Longrightarrow \quad g_0 &\leq \frac{2^{n-2} - 1}{2^{n-1} - d} \leq \frac{2^{n-2} - 1}{2^{n-1} - \frac{2^n - 1}{3}} = \frac{2^{n-1} + 2^{n-2} - 3}{2^{n-1} + 1} < 2 && (89) \end{aligned}$$

Therefore

$$\begin{aligned} g_0 &= 1 && (90) \\ d &= 1 + l \times 2^{n-2} \qquad (\leq \frac{2^n - 1}{3}) && (91) \\ \Longrightarrow \quad d &= 1 + 2^{n-2} && (92) \end{aligned}$$

since $l = 1$.

$$(1+2^{n-2})\big|(2^n-1) = 2(2^{n-2}+1)-5 \tag{93}$$
$$1+2^{n-2}\big|5 \qquad (n \geq 4) \tag{94}$$

Therefore

$$n=4, \text{ and } d=5, \quad S=5 \tag{95}$$

The defintion equation of C_0 is

$$C_0: \quad y^2 = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3}) \tag{96}$$
$$\alpha \in k_5 \setminus k \tag{97}$$

6.2 Case char$(k)=2$

6.2.1 Ordinary cases ($d \leq \frac{2^n-1}{3}$)

By Riemann-Hurwitz,

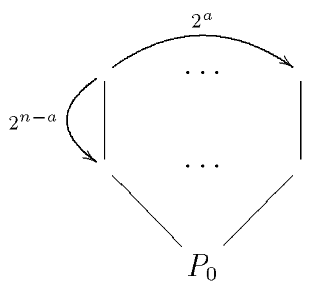
$$2dg_0 - 2 = 2^n(-2)+S \tag{98}$$
$$S = 2(dg_0 + 2^n - 1) \tag{99}$$
$$\geq 2^n(g_0+1+\epsilon) \tag{100}$$
$$\Longrightarrow \quad (2^{n-1}-d)g_0 \leq 2^{n-1}(1-\epsilon)-1 \tag{101}$$

Therefore

$$\epsilon = 0, \quad i.e. \quad g(x) \in k[x] \tag{102}$$

In fact, locally a ramification point P_0 has 2^a fibres and each fibre with 2^{n-a} points. Thus

$$2 \times (2^{n-a}-1) \times 2^a = 2(2^a - 2^a) \geq 2^n \tag{103}$$

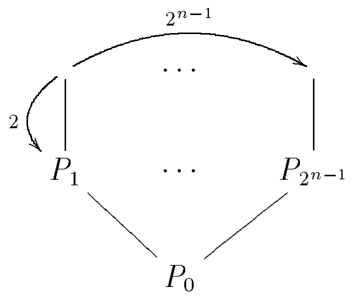


We now consider two cases:

Case 1

Assume that there exsits a P_0 such that the points $P_i, i = 1, ..., 2^{n-1}$ over it is fixed by ϕ:

$$
\begin{aligned}
\phi(P_1) &= P_1 && (104)\\
\Longrightarrow \quad \phi(P_i) &= P_i \quad \forall i && (105)
\end{aligned}
$$



$$
H = <\phi> \qquad \simeq \mathbb{Z}/2\mathbb{Z} \tag{106}
$$

Then in the covering

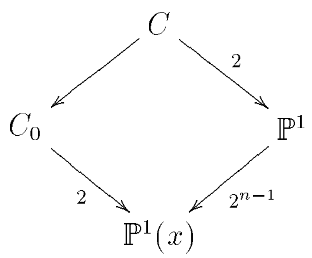
$$
C \xrightarrow{2} C/H \longrightarrow \mathbb{P}^1(x) \tag{107}
$$

P_0 is unramified over $C/H \longrightarrow \mathbb{P}^1(x)$.

Since $g(x) \in k[x]$, we have

$$
C/H = \mathbb{P}^1 \tag{108}
$$

Then in the following covering diagram,



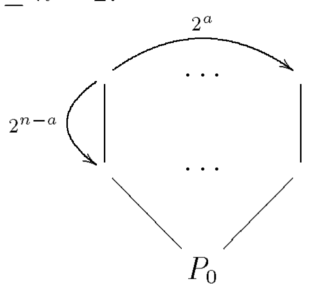
$C_0/\mathbb{P}^1(x)$ has g_0+1 ramification points.
By Riemann-Hurwitz, $C/\mathbb{P}^1$ is degree two and for $C/\mathbb{P}^1(x)$

$$\begin{aligned} 2dg_0 - 2 &= 2(-2) + S && (109)\\ S &= 2(dg_0+1) && (110)\\ &= 2^{n-1}\times 2g_0 + 2 && (111)\\ \Longrightarrow \quad d &= 2^{n-1} && (112) \end{aligned}$$

So such a case does not exists.

Case 2:

Assume that all ramification points $\forall P_0$ has a ramification graph as below where $0 \le a \le n-2$.



Then by Riemann-Hurwitz,

$$\begin{aligned} 2dg_0 - 2 &= 2^n(-2) + S && (113)\\ S &= 2(dg_0 + 2^{n-1}) && (114)\\ &\ge (g_0+1)(2^n - 2^{n-2})\times 2 && (115)\\ \Longrightarrow &\quad (2^n - 2^{n-2} - d)g_0 \le 2^{n-2} - 1 && (116)\\ d &\le \frac{2^n-1}{3} && (117) \end{aligned}$$

which also does not exists.

7 Indecomposable and $d = m = 2^n - 1$

We use the notation in Section 2.2,

$$C_0 \quad : \quad y^2 + g(x)y = f(x) \tag{118}$$

$$\zeta \quad = \quad \zeta_m \in \overline{\mathbb{F}}_2 \tag{119}$$

$$\zeta^n \quad = \quad \sum_{i=0}^{n-1} a_i \zeta^i \tag{120}$$

and L defined in Eq.(21) and M in Eq.(26)

7.1 Case char$(k) \neq 2$

(i)

$$C_0 : \quad y^2 \quad = \quad f(x) \tag{121}$$

$$\forall \alpha \quad = \quad (\epsilon_0, \epsilon_1, \cdots, \epsilon_{n-1}) \in \mathbb{F}_2^n \setminus (0, 0, \cdots, 0) \tag{122}$$

$$y^\alpha \quad := \quad \prod_{i=0}^{n-1} \left({}^{\sigma^i} y \right)^{\epsilon_i} \tag{123}$$

Since $d = 2^n - 1$,

$$\forall H < cov(C/\mathbb{P}^1), \qquad \text{of index } 2 \tag{124}$$

$$g(C/H) \quad = \quad g_0 \tag{125}$$

Now consider the action of cov$(C/\mathbb{P}^1)$ on $\{y^\alpha\}_\alpha$

$$\forall i, \quad \exists \alpha \in \mathbb{F}_2^n \setminus (0, 0, \cdots, 0) \tag{126}$$

$$s.t. \quad {}^{\sigma^i} y \equiv y^\alpha \mod k_m(x)^\times, \tag{127}$$

Therefore

$$G(k_m/k) \curvearrowright \{y^\alpha\} \bmod k_m(x)^\times \tag{128}$$

$$\Longrightarrow \quad {}^{\sigma^n} y \equiv \prod_{i=0}^{n-1} \left({}^{\sigma^i} y \right)^{a_i} \bmod k_m(x)^\times \tag{129}$$

$$\Longrightarrow \quad {}^{\sigma^n} f \equiv \prod_{i=0}^{n-1} \left({}^{\sigma^i} f \right)^{a_i} \bmod \left(k_m(x)^\times \right)^2 \tag{130}$$

(ii) By Riemann-Hurwitz,

$$\begin{aligned} 2mg_0 - 2 &= 2^n(-2) + 2^{n-1}S & (131) \\ S &= \frac{m(g_0+1)}{2^{n-2}} & (132) \end{aligned}$$

Then

$$\begin{aligned} g_0 + 1 &= l \times 2^{n-2} & (133) \\ S &= ml & (134) \end{aligned}$$

(iii) The definition equation of C_0:
Assume the decomposition of l is

$$\begin{aligned} l &:= l_1 + l_2 + \cdots + l_r \qquad (l_i \geq 1) & (135) \\ \alpha_i &\in k_{ml_i}, \quad k(\alpha_i) = k_{ml_i} & (136) \\ \left\{{}^{\sigma^l}\alpha_i\right\}_l &\cap \left\{{}^{\sigma^l}\alpha_j\right\}_l = \emptyset, \quad i \neq j & (137) \end{aligned}$$

Then

$$C_0 : \quad y^2 = \prod_{i=0}^{r} N_{k_{ml_i}/k_m}(M(x - \alpha_i)) \tag{138}$$

7.2 Case char$(k) = 2$

$$\begin{aligned} C_0 : \quad y^2 + g(x)y &= f(x) & (139) \\ \deg g(x) &= g_0 + 1, \quad \deg f(x) = 2g_0 + 2 & (140) \\ \hat{g}(x) &:= LCM\left\{{}^{\sigma^i}g(x)\right\} \in k[x] & (141) \end{aligned}$$

7.2.1 Necessary condition

From $d = 2^n - 1$,

$$\forall H < cov(C/\mathbb{P}^1), \qquad g(C/H) = g_0 \tag{142}$$

Define

$$\begin{aligned} Z &:= \frac{\hat{g}(x)}{g(x)}y & (143) \\ h(x) &:= \left(\frac{\hat{g}(x)}{g(x)}\right)^2 f & (144) \end{aligned}$$

Then

$$C_0: \quad Z^2 + \hat{g}(x)Z = h(x) \tag{145}$$

Let $V = \oplus_{i=0}^{n-1} \mathbb{F}_2 \ {}^{\sigma^i}Z$.

Since $\forall v \in V$, the subgroup of $cov(C/\mathbb{P}^1)$ fixing v has index 2,

$$\begin{aligned} \Longrightarrow \quad {}^{\sigma^l}Z &\equiv \sum_{i=0}^{n-1} c_i \ {}^{\sigma^i}Z \mod k_m[x], \quad \exists c_i \in \mathbb{F}_2 & (146) \\ \Longrightarrow \quad {}^{\sigma^n}Z &= \sum_{i=0}^{n-1} a_i \ {}^{\sigma^i}Z + l(x), \quad l(x) \in k_m[x] & (147) \\ \Longrightarrow \quad l^2(x) + \hat{g}(x)l(x) &= L(h) \in k_m[x] & (148) \end{aligned}$$

Therefore,

$$l(x) \in k_m[x], \text{ and } \deg l(x) \leq \deg \left(\frac{\hat{g}(x)}{g(x)} \right) + g_0 + 1 \tag{149}$$

From (147),

$$\begin{aligned} {}^{\sigma^n}Z &= \sum_{i=0}^{n-1} a_i \ {}^{\sigma^i}Z + l(x), \quad l(x) \in k_m(x) & (150) \\ {}^{\sigma^{n+1}}Z &= \sum_{i=0}^{n-1} a'_i \ {}^{\sigma^i}Z +^{\sigma} l(x) + a_{n-1}l(x) & (151) \\ &\cdots & (152) \\ {}^{\sigma^m}Z = Z &= Z +^{\sigma^{m-n}} l(x) + a_{n-1} \ {}^{\sigma^{m-n-1}}l(x) + \cdots & (153) \\ \Longrightarrow \quad 0 &= {}^{\sigma^{m-n}}l(x) + a_{n-1} \ {}^{\sigma^{m-n-1}}l(x) + \cdots & (154) \end{aligned}$$

Therefore, we define a k-linear map

$$\begin{aligned} \hat{L}: \quad k_m[x] &\longrightarrow k_m[x] & (155) \\ l(x) &\longmapsto {}^{\sigma^{m-n}}l(x) + a_{n-1} \ {}^{\sigma^{m-n-1}}l(x) + \cdots & (156) \end{aligned}$$

Then

$$\ker(\hat{L}) = L(k_m[x]) \tag{157}$$

Indeed, recall that

$$L(l(x)) =^{\sigma^n} l(x) + a_{n-1} {}^{\sigma^{n-1}} l(x) + \cdots \tag{158}$$

consider the coefficients of every terms in

$$\hat{L} \cdot L = 0 \tag{159}$$

one has

$$\#\{\alpha : \hat{L}(\alpha) = 0\} \leq q^{m-n} \tag{160}$$

While from the defintion of L,

$$\# \ker(L) = q^n \tag{161}$$

Therefore

$$L(k_m) = \ker \left(\hat{L}\big|_{k_m} \right) \tag{162}$$

□

Thus,

$$l(x) = L(\ell(x)), \quad \exists \ell(x) \in k_m[x], \quad \deg \ell(x) \leq \deg \left(\frac{\hat{g}(x)}{g(x)} \right) + g_0 + 1 \tag{163}$$

From this

$$L(h + \ell^2 + \hat{g}\ell) = 0 \tag{164}$$

$$i.e. \quad L\left(\left(\frac{\hat{g}}{g} \right)^2 f + \ell^2 + \hat{g}\ell \right) = 0 \quad \deg \ell \leq \deg \left(\frac{\hat{g}}{g} \right) + g_0 + 1 \tag{165}$$

7.2.2 Sufficient condition

Now we assume at first that

$$L(h + \ell^2 + \hat{g}\ell) = 0 \tag{166}$$

Then

$$0 = L(Z^2 + \hat{g}Z + \ell^2 + \hat{g}\ell) \tag{167}$$

$$= L(Z + \ell)^2 + \hat{g}L(Z + \ell) \tag{168}$$

From this

$$\Longrightarrow \quad L(Z+\ell) = \begin{cases} 0 \\ \hat{g} \end{cases} \tag{169}$$

Assume $L(Z+\ell) = \hat{g}$, then since

$$\#\{a_i = 1\} = 2^{n-1} \tag{170}$$

$$L(\hat{g}) = \hat{g} \tag{171}$$

$$Z \longmapsto Z + \hat{g} = \frac{\hat{g}}{g} y + \hat{g} = \frac{\hat{g}}{g}(y+g) \tag{172}$$

Thus we could assume that $L(Z+\ell) = 0$.
Therefore

$${}^{\sigma^n}Z \equiv \sum_{i=0}^{n-1} a_i \, {}^{\sigma^i}Z \mod k_m[x] \tag{173}$$

Next, define a surjective homomorphism

$$h: \quad cov(C/\mathbb{P}^1) \simeq \mathbb{F}_2^n \twoheadrightarrow \sum_{i=0}^{n-1} \mathbb{F}_2 \, {}^{\sigma^i}Z \mod k_m[x] \tag{174}$$

Since the action of $G(k_m/k)$ on W is irreducible, either h is an isomorphism or $Z \in k_m[x]$.

In the later case,

$$y \in k_m[x] \text{ and} \tag{175}$$

$$C_0: \quad y^2 + g(x)y = f(x) \tag{176}$$

which is the singular case.

7.2.3 On $g(x)$

(i) Ordinary case

$$g_1(x) := GCD\left\{ {}^{\sigma^i}g(x) \right\} \in k[x] \tag{177}$$

$$g_2(x) := \frac{g(x)}{g_1(x)} \tag{178}$$

(1)

$$\deg g(x)+1 = \deg g_1(x)+\sum_{i=1}^{n-1}\sum_{d|m,\frac{m}{d}|(2^{n-r}-1)}(2^n-2^r)\frac{d}{m}\times b_{i,d} \quad (179)$$

$$\exists b_{i,d}\in\mathbb{Z}_{\geq 0} \quad (180)$$

The points with x-coordinates as the roots of the common factor $g_1(x)$ are totally ramified. On the other hand, for points with x-coordinates as the roots of $g_2(x)$ are not totally ramified.

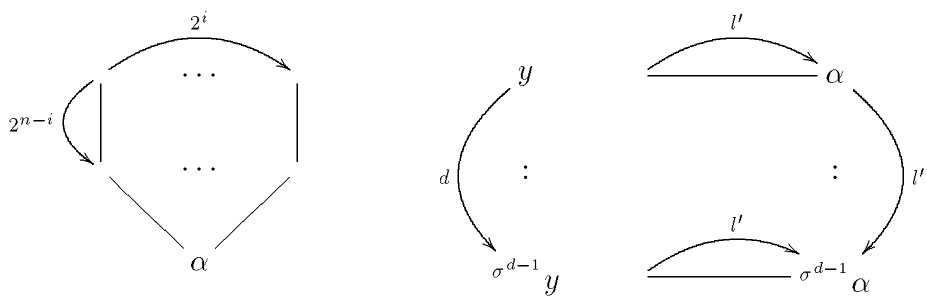
Assume

$$g_2(\alpha) = 0 \quad (181)$$

$$l' := \#\left\{i \mid 0\leq i\leq m-1,\ g_2(\alpha^{q^i})=0\right\} \quad (182)$$

Then

$$\#\left\{H < cov(C/\mathbb{P}^1) \text{ of index } 2,\ s.t.\ \alpha \text{ ramifies in } C/H \xrightarrow{2} \mathbb{P}^1(x)\right\}$$
$$= (2^n-1)-(2^r-1), \qquad (1\leq^{\exists} r\leq n-1)$$



On the other hand, this order is equals to $l'\times\frac{m}{d}$. Thus

$$l'\times\frac{m}{d}=2^n-2^r \quad (183)$$

(2) As to the factor $g_\alpha(x)$ corresponding to each α,
(a) When $d=m, r=n-1,\ l=2^{n-1}$

$$R := \{i : 0 \le i \le m-1, \quad s.t. \;\; b_i = 1\} \tag{184}$$
$$\#R = 2^{n-1} \tag{185}$$
$$\exists j, \quad g_\alpha(x) = \prod_{i \in {}^{\sigma^j}R} (x - \alpha^{q^i}) \tag{186}$$

We now check the points such that $k_m[x, {}^{\sigma^i}y, {}^{\sigma^j}y]$ is not normal.

Define

$$T := \left\{ i : g_2(\alpha^{q^i}) = 0 \right\} \tag{187}$$
$$\#T = 2^{n-1} \tag{188}$$
$$\epsilon := (\epsilon_0, \cdots, \epsilon_{m-1}) \in \mathbb{F}_2^m \tag{189}$$
$$\epsilon_i := \begin{cases} 1 & i \in T \\ 0 & i \notin T \end{cases} \tag{190}$$

and

$$Z^i + Z^j =: Z^s \tag{191}$$

Then

$$\left({}^{\sigma^i}T \cup {}^{\sigma^j}T \right) \setminus \left({}^{\sigma^i}T \cap {}^{\sigma^j}T \right) = {}^{\sigma^s}T \tag{192}$$

Therefore

$${}^{\sigma^i}\epsilon + {}^{\sigma^j}\epsilon = {}^{\sigma^s}\epsilon \tag{193}$$

Thus, since the action of $G(k_m/k)$ is an isomorphism

$$\rho := (\rho_0, \rho_1, \cdots, \rho_{m-1}) \in \mathbb{F}_2^m \tag{194}$$
$$\epsilon = {}^{\sigma^i}\rho, \quad \exists i \tag{195}$$

(b) Conjecture: When $d = m, r = n - l, \; (l \ge 2)$

$$W := \cup_{j=1}^{l} {}^{\sigma^{i_j}}R \tag{196}$$

Then the factor of α is

$$g_\alpha(x) = \prod_{i \in W} (x - \alpha^{q^i}) \tag{197}$$

(c) Conjecture : When $d \neq m-1$, $d|2^n-1$.

Take l_m as

$$l_m := \max_l \left\{ \left. \frac{m}{d} \right| \left(2^{n-l}-1\right) \right\} \tag{198}$$

Then this case can be treated similarly as the case (b), with l replaced by l_m and

$$W \ := \ \cup_{j=0}^{\frac{m}{d}-1} {}^{\sigma^{i_j}} R \tag{199}$$

(ii) Non-ordinary case

This case can be treated in a similar way as the case (i). In particular, we investigated the cases when $n=4, d=5, \frac{m}{d}=3$.

Notice that in these cases, $d \not| (2^l-1), 1 \leq^{\forall} l \leq n-1$.

8 Decomposable case

Assume that as a $G(k_d/k)$-module, the representation of σ is a direct sum of indecomposable subrepresentations H_v.

$$cov(C/\mathbb{P}^1(x)) \ = \ H_1 \oplus \cdots \oplus H_r, \tag{200}$$
$$r \geq 2, \qquad \# H_i = 2^{n_i}, \tag{201}$$

Define

$$H'_i \ := \ \oplus_{j \neq i} H_j \tag{202}$$

By the condiction (C),

$$C/H_i = C/H'_i = \mathbb{P}^1 \quad \forall i \tag{203}$$

If $r \geq 3$,

$$C/(H'_i \cap H'_j) = C \Big/ (\oplus_{l \neq i,j} H_l) = \mathbb{P}^1 \tag{204}$$

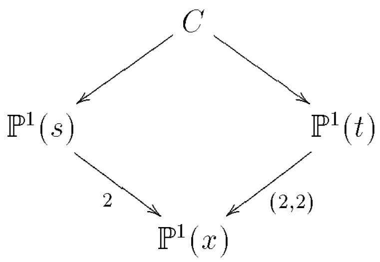
8.1 Char$(k) \neq 2$ case

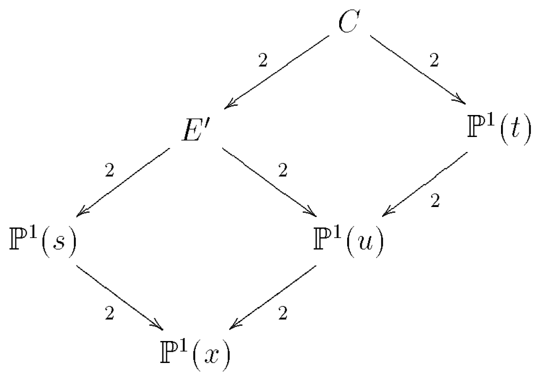
When char$(k) \neq 2$, by (204)

$$\sum_{l \neq i} n_l \leq 2, \qquad \forall i \tag{205}$$

$$\Longrightarrow \quad r = 2, n_1 = 1, n_2 = 2, d = 3, g_0 = 1 \tag{206}$$

We have then a covering as follows.





Then $\mathbb{P}^1(t) = C/\iota$ where ι is the hyperelliptic involution,

$$cov(\mathbb{P}^1(t)/\mathbb{P}^1(x) \ni^{\exists} \phi = \begin{pmatrix} \beta & b \\ 1 & -\beta \end{pmatrix} \tag{207}$$

$$b = D - \beta^2 \tag{208}$$

$$D = (\beta - \beta^q)(\beta - \beta^{q^2}) \tag{209}$$

and ${}^{\sigma^2}\phi \sim \phi \circ {}^{\sigma}\phi \sim {}^{\sigma}\phi \circ \phi$.

$$x = t + \phi(t) +^{\sigma} \phi(t) +^{\sigma^2} \phi(t) \tag{210}$$

Now consider $\mathbb{P}^1(u) = C/ < {}^{\sigma}\phi >$ defined by

$$u = t +^{\sigma} \phi(t) \tag{211}$$

Since under ${}^{\sigma}\phi$

$$\beta \pm \sqrt{D} \longmapsto 2\beta \tag{212}$$

$$\beta^q \pm \sqrt{D^q} \longmapsto 2(\beta^q \pm \sqrt{D^q}) \tag{213}$$

$$\beta^{q^2} \pm \sqrt{D^{q^2}} \longmapsto 2\beta^{q^2} \tag{214}$$

Denote

$$\phi\Big|_{\mathbb{P}^1(u)} := \begin{pmatrix} a & c \\ 1 & -a \end{pmatrix} \tag{215}$$

The fixed points of $\phi\Big|_{\mathbb{P}^1(u)}$ is the solutions of

$$X^2 - 2aX - c = 0 \tag{216}$$

Then one has

$$2a = 2(\beta + \beta^{q^2}) \tag{217}$$

$$-c = 4\beta^{1+q^2} \tag{218}$$

or

$$\phi\Big|_{\mathbb{P}^1(u)} = \begin{pmatrix} \beta + \beta^{q^2} & 4\beta^{1+q^2} \\ 1 & -(\beta + \beta^{q^2}) \end{pmatrix} \tag{219}$$

$$C_0 : (y(u - \phi(u))^2 = y^2\left((u + \phi(u))^2 - 4u\phi(u)\right) \tag{220}$$

$$= y^2(x^2 - 2u\phi(u)) \tag{221}$$

$$x = u + \phi(u) = \frac{u^2 - 4\beta^{1+q^2}}{u - 2(\beta + \beta^{q^2}} \tag{222}$$

$$u\phi(u) = \frac{2(\beta + \beta^{q^2})u^2 - 4\beta^{1+q^2}}{u - 2(\beta + \beta^{q^2})} \tag{223}$$

$$= 2(\beta + \beta^{q^2})x - 4\beta^{1+q^2} \tag{224}$$

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

$$\mathbb{P}^1(s): \quad s^2 = ax^2 + bx + c, \qquad a, b, c \in k \tag{225}$$

One has

$$C_0 : \quad y^2 = (ax^2 + bx + c)(x - 4(\beta + \beta^{q^2})x + 16\beta^{1+q^2}) \tag{226}$$

$$= (ax^2 + bx + c)(x - 4\beta)(x - 4\beta^{q^2}) \tag{227}$$

Therefore, we can assume that C_0 has the form ($\alpha^q = 4\beta$)

$$C_0 : \quad y^2 = (ax^2 + bx + c)(x - \alpha)(x - \alpha^q) \tag{228}$$

When $(g_0, d) = (1, 3)$, this curve corresponds to the cases

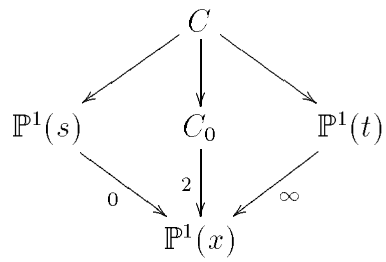
$$y^2 = (x - \alpha)(x - \alpha^q)(x - \beta)(x - \beta^q) \tag{229}$$

$$\beta = A\alpha, \quad \exists A \in GL_2(k), \quad Tr(A) = 0 \tag{230}$$

8.2 Char$(k) = 2$ case

When Char$(k) = 2$, by the Theorem 1, we know that C is ordinary.

Let $r \geq 3$, then ∞ is the only ramification point of the covering $C \longrightarrow \mathbb{P}^1(x)$. Thus $r = 2$ and $g_0 = 1$. We have now a covering diagram as follows.



Now we show the explicit equations of C and C_0. Denote $L_i, i = 1, 2$ as two k-linear map defined in (21).

$$\lambda_i : \quad L_i(\lambda_i) = 0, \qquad i = 1, 2 \tag{231}$$

$$G_i = < \left\{ {}^{\sigma^l}\lambda_i \right\}_l > \tag{232}$$

$$H_i = < \left\{ {}^{\sigma^l}\lambda_i \right\}_{1 \leq l \leq n-1} > \tag{233}$$

$$[G_i : H_i] = 2 \tag{234}$$

$$u_i = \prod_{\mu \in H_i} (s_i + \mu) \tag{235}$$

$$\rho_i = \prod_{\mu \in H_i} (\lambda_i + \mu) \tag{236}$$

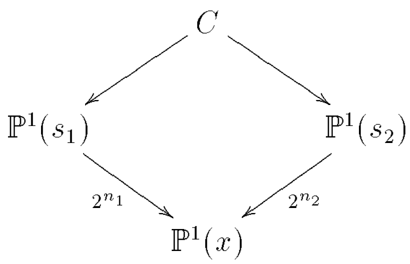
then two degree two covering $\mathbb{P}^1(u_i)/\mathbb{P}^1(x), i = 1,2$ are defined as

$$b \in k, \quad x + b = u_1(u_1 + \rho_1) \quad (= \prod_{\mu \in G_1} (s_1 + \mu)), \tag{237}$$

$$\frac{1}{x} = u_2(u_2 + \rho_2) \quad (= \prod_{\mu \in G_2} (s_2 + \mu)) \tag{238}$$

C is then defined by

$$C: \quad \prod_{\mu \in G_2} (s_2 + \mu) \left(\prod_{\mu \in G_1} (s_1 + \mu) + b \right) = 1 \tag{239}$$



Now, redefine

$$v_1 = u_1(u_1 + \rho_1) \tag{240}$$

$$v_2 = u_2(u_2 + \rho_2) \tag{241}$$

$$\Longrightarrow \quad 1 + bv_1 = v_1 v_2 \tag{242}$$

Let

$$w := \frac{u_1}{\rho_1} + \frac{u_2}{\rho_2} \tag{243}$$

$$\Longrightarrow \quad w^2 + w = \frac{v_1}{\rho_1^2} + \frac{1}{\rho_2^2}\left(\frac{1}{v_1} + b\right) \tag{244}$$

$$(v_1 w)^2 + v_1(v_1 w) = \frac{v_1^3}{\rho_1^2} + \frac{b}{\rho_2^2} v_1^2 + \frac{1}{\rho_2^2} v_1 \tag{245}$$

Denote

$$y := \frac{v_1 w}{\rho_1^2} \tag{246}$$

$$x := \frac{v_1}{\rho_1^2} \tag{247}$$

The definition equation of C_0 is

$$C_0: \quad y^2 + xy = x^3 + \frac{b}{\rho_2^2} x^2 + \left(\frac{1}{\rho_1\rho_2}\right)^2 x \tag{248}$$

When either n_1 or n_2 is 1, C is hyperelliptic.

For an example, $(n_1, n_2) = (2, 1), d = 3, \lambda_2 = \rho_2 = 1$,

$$C_0: \quad y^2 + xy = x^3 + bx^2 + cx \tag{249}$$

$$Tr(c) = 0, \quad c \in k_3 \setminus k \tag{250}$$

9 Lists of classifications

List 1: Classification for char$k \neq 2$

$g(C_0)$	d, n	C_0	hyper/non	$\#C_0$
1	$d=2, n=2$	$y^2=(x-\alpha)g(x)$	Hyper	$O(q^2)$
	$d=5, n=4$	$y^2=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$	Non-hyper	$O(q^2)$
	$d=3, n=2$	$y^2=(x-\alpha)(x-\alpha^q)(x-\beta^q)(x-\beta^{q^2})$ either $\alpha,\beta \in k_3 \setminus k$ or $\alpha \in k_6 \setminus (k_2 \cup k_3),\quad \beta=\alpha^{q^3}$ C_0:Hyper $\iff \exists A \in GL_2(k), \beta = A\cdot\alpha, Tr(A)=0$	 Hyper	$O(q^3)$ $O(q^2)$
	$d=7, n=3$	$y^2=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^r}),\quad r=4,5$	Nonhyper	$O(q^4)$?
2	$d=2, n=2$	$y^2=(x-\alpha)g(x)$	Hyper	$O(q^4)$
	$d=3, n=3$	$y^2=(x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)(x-\gamma)(x-\gamma^q)$ either $\alpha \in k_9 \setminus k_3, \beta=\alpha^{q^3}, \gamma=\alpha^{q^6}$ or $\alpha \in k_6 \setminus (k_2 \cup k_3), \beta=\alpha^{q^3}, \gamma = k_3 \setminus k$ or $\alpha,\beta,\gamma \in k_3 \setminus k$	Nonhyper	$O(q^6)$?
3	$d=2, n=2$	$y^2=(x-\alpha)g(x)$	Hyper	$O(q^6)$
	$d=3, n=2$	$y^2=(x-\alpha)(x-\alpha^q)(x-\beta)(x-\beta^q)(x-\gamma)(x-\gamma^q)$ $\times(x-\delta)(x-\delta^q)$ Either $\alpha \in k_{12} \setminus (k_6 \cup k_4), \beta=\alpha^{q^3}, \gamma=\alpha^{q^6}, \delta=\alpha^{q^9}$ or $\alpha \in k_9 \setminus k_3, \beta=\alpha^{q^3}, \gamma=\alpha^{q^6}, \delta \in k_3 \setminus k$ or $\alpha \in k_6 \setminus (k_2 \cup k_3), \beta=\alpha^{q^3}, \gamma \in k_6 \setminus (k_2 \cup k_3), \delta=\alpha^{q^3}$ or $\alpha \in k_6 \setminus (k_2 \cup k_3), \beta=\alpha^{q^3}, \gamma,\delta \in k_3 \setminus k$ or $\alpha,\beta,\gamma,\delta \in k_3 \setminus k$	Nonhyper	$O(q^9)$?
	$d=7, n=3$	$y^2=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^r})$ $\times(x-\beta)(x-\beta^q)(x-\beta^{q^2})(x-\beta^{q^r}),\quad r=4,5$ either $\alpha \in k_{14} \setminus (k_2 \cup k_7), \beta=\alpha^{q^7}$ or $\alpha,\beta \in k_7 \setminus k$	Nonhyper	$O(q^{11})$?
	$d=15, n=4$	$y^2=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $\times(x-\alpha^{q^7})(x-\alpha^{q^{10}})(x-\alpha^{q^{11}})(x-\alpha^{q^{13}})$ or $y^2=(x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})(x-\alpha^{q^3})$ $\times(x-\alpha^{q^5})(x-\alpha^{q^7})(x-\alpha^{q^8})(x-\alpha^{q^{11}})$ $\alpha \in k_{15} \setminus k$	Nonhyper	$O(q^{12})$?

List 2 : Classification for $\mathbf{char}(k) = 2$

$g(C_0)$	d, n	Ordinary	C_0	Hyper	$\#C_0$
1	$d=2$ $n=2$	ordinary	$y^2+xy=x^3+ax^2+bx$	Hyper	$O(q^2)$
		non-ordin	$y^2+y=ax^3+bx^2+cx+d$ $a^q=a\neq 0, b^q+b\neq 0$ or $c^q+c\neq 0$	Hyper	
	$d=4$ $n=3$	ordinary	$y^2+xy=x^3+cx$ $c\in k_4\setminus k_2, Tr(c)=0$	Hyper	$O(q^3)$
		non-ordin	$y^2+y=ax^3+bx^2+cx+d$ $a^q=a\neq 0, Tr(b)=Tr(c)=Tr(d)=0$ b or $c\in k_4\setminus k_2$	Hyper	
	$d=2^n-1$ $n\geq 2$		(1) ${}^\sigma g(x)=g(x), n\geq 2$ $y^2+g(x)y=f(x), \quad L(f)=0$		$O(q^{2n-1})$
		ordinary	The same as above e.g. $n=2$ $y^2+xy=x^3+ax^2+bx$ $a\in k, Tr(b)=0$	Hyper	$O(q^n)$? $O(q^2)$
		ordinary	(2) ${}^\sigma g(x)\neq g(x), d=3, n=2$ $g(x)=(x+\alpha^q)(x+\alpha^{q^2}), \alpha\in k_3\setminus k$ $Tr((x+\alpha)^2 f)=0$		$O(q^3)$?
2	$d=2$ $n=2$		$y^2+g(x)y=f(x)$ $\deg f(x)=5, \deg_k g(x)\leq 2$ ${}^\sigma f=f+g^2 l, l\in k[x], \deg l=1,2$	Hyper	$O(q^4)$
	$d=4$ $n=3$		$y^2+g(x)y=f(x)$ $\deg f(x)=5, \deg_k g(x)\leq 2$ ${}^\sigma f=f+g^2 l, l\in k_2[x]$, $\deg l=1,2, \deg(l+{}^\sigma l=1,2)$	Hyper	$O(q^5)$
	$d=2^n-1$ $n\geq 2$		${}^\sigma g(x)=g(x)$ $y^2+g(x)y=f(x), \; L(f)=0$	Nonhyper	$O(q^{3n})$
3	$d=2, n=2$		$y^2+g(x)y=f(x)$ (*1)	Hyper	$O(q^6)$
	$d=4, n=3$		$y^2+g(x)y=f(x)$ $(*2)$	Hyper	$O(q^7)$?
	$d=2^n-1$		(1) ${}^\sigma g(x)=g(x)$ $y^2+g(x)y=f(x), \; L(f)=0$	Nonhyper	$O(q^{4n+1})$
	$d=3$		(2) ${}^\sigma g(x)\neq g(x)$ Either $g=g_1(x)(x+\alpha^q)(x+\alpha^{q^2}), \alpha\in k_3\setminus k$ $g_1\in k[x], \deg g_1\leq 2, L((x+\alpha)^2 f)=0$ Or $g=(x+\alpha^q)^2(x+\alpha^{q^2})^2$, $\alpha\in k_3\setminus k, L((x+\alpha)^4 f)=0$	Nonhyper	
	$d=7$	ordinary	$g=(x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^r})$, $r=4,5, \quad \alpha\in k_7\setminus k$, $L((x+\alpha^{q^3})^2(x+\alpha^{q^5})^2(x+\alpha^{q^7})^2 f)\equiv 0$ (*3)	Nonhyper	
	$d=15$	ordinary	$g=(x+\alpha^q)(x+\alpha^{q^2})(x+\alpha^{q^3})(x+\alpha^{q^4})$, $\alpha\in k_5\setminus k, L((x+\alpha^{q^4})^2 f)\equiv 0$ $(*3)$	Nonhyper	

(*1) With the same conditions as $g_0 = 2, d = n = 2$.
(*2) With the same conditions as $g_0 = 2, d = 4, n = 3$
(*3) Here "$\equiv$" means $\equiv 0 \bmod L(\ell^2 + \hat{g}\ell)$.
Note: Ordinary nonhyper curves also exist for $g_0 = 1, d = (2^{n_1} - 1)(2^{n_2 - 1})$,
$2 \le n_1, n_2, (2^{n_1} - 1, 2^{n_2} - 1) = 1$

References

[1] L.Adleman, J.DeMarrais, and M.Huang, “A subexpotential 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 elliptive 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. Cohn, G. Frey, “Handbook of elliptic and hyperelliptic curve cryptography”, Chapman & Hall, 2006

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

[6] C. Diem, “Index calculus in class groups of plane curves of small degree”, Proceedings of ANTS VII, 2006.

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

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

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

[10] S.D.Galbraith “Weil descent of Jacobians,” Discrete Applied Mathmatics, vol.128 no.1, pp.165-180, 2003.

[11] 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.

[12] P.Gaudry, N.Theriault, E.Thome “ A double large prime variation for small genus hyperelliptic index calculus” Preprint, Feb.2005.

[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] 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.

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

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

[17] 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.

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

[19] F. Momose, J. Chao ”Scholten Forms and Elliptic/Hyperelliptic Curves with Weak Weil Restrictions” Cryptology ePrint Archive: Report 2005/277 http://eprint.iacr.org/2005/277

[20] K.Nagao “Improvement of Theriault algorithm of index calculus of Jacobian of hyperelliptic curves of small genus”, preprint 2004.

[21] Jasper Scholten ”Weil restriction of an elliptic curve over a quadratic extension”, available at (http://homes.esat.kuleuven.be/ jscholte/

[22] J.P. Serre ”Local fields”

[23] 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

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

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