同種条件を満たさない被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線の分類に関する研究

A Classification of Elliptic and Hyperelliptic Curves Over Finite Fields of Even Characteristic Without the Isogeny Condition Subject to the Cover Attack

情報工学専攻　登丸 尚哉
Naoya TOMARU

要約　GHS攻撃の一般化である被覆攻撃とは，有限体 $k := \mathbb{F}_q$ (q : 素数のベキ乗) の d 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上定義される楕円･超楕円曲線 C_0の離散対数問題を k 上定義される被覆曲線 C の離散対数問題に変換する攻撃手法である．近年，攻撃の対象となる奇標数拡大体上の種数 $1,2,3$ 超楕円曲線暗号に用いられる曲線の完全分類が行われた．また，百瀬ら，村井らにより，偶標数拡大体 k_d上の種数 $g(C_0) = 1,2,3$ 楕円・超楕円曲線 C_0に対して，同種条件 ($g(C) = d \cdot g(C_0)$) 下で曲線の分類及び再検討がされている [1][2]．本論文では，被覆攻撃の対象となる同種条件を満たさない偶標数拡大体上楕円・超楕円曲線の 4 つのクラスに対して分類を行った．

キーワード: 楕円・超楕円曲線暗号，楕円・超楕円曲線，被覆攻撃，GHS 攻撃．

1　はじめに

拡大体上の楕円・超楕円曲線に対する攻撃手法として GHS 攻撃がある．GHS 攻撃は Frey によって Weil descent を拡大体上に定義される楕円・超楕円曲線暗号に導入するアイデアを，Gaudry，Hess，Smart が偶標数有限体の拡大体上の楕円曲線に対して提案した攻撃手法である．その後，この攻撃は奇標数有限体など，より一般的な曲線にも適用され，Frey と Diem によって被覆攻撃として一般化された．この攻撃手法は，有限体 $k := \mathbb{F}_q$ (q : 素数のベキ乗) の d 次拡大体 $k_d := \mathbb{F}_{q^d}$ 上定義される楕円･超楕円曲線 C_0の離散対数問題を k 上定義される被覆曲線 C の離散対数問題に変換して解く攻撃手法である．このとき，C の種数は上がるが定義体が k_dから k へ小さくなるため，離散対数問題の計算量が少なくなる場合がある．後の研究により，被覆攻撃は当初想定されていた数より多くの曲線が対象となり，現存暗号系に強力に作用する事実が明らかになった．しかし，攻撃の対象となる範囲は未だ完全には明らかになっていない．ゆえに，被覆攻撃の対象となる被覆曲線 C を持つ楕円・超楕円曲線 C_0の解析と分類が重要である．

近年，攻撃の対象となる楕円・超楕円曲線の分類が進められている．奇標数の場合，奇標数拡大体上の種数 $1,2,3$ 超楕円曲線の同種条件 ($g(C) = d \cdot g(C_0)$) 下での分類が行われ，飯島らが同種条件を外した一般の場合において系統的に分類する手法を提案した．その手法を用いることで一般の場合を含めた奇標数拡大体上の種数 $1,2,3$ 超楕円曲線の完全分類が行われた．偶標数の場合，奇標数とは異なる扱いが必要となり，完全な分類が困難であるが，百瀬らにより偶標数拡大体 k_d上の種数 $1,2,3$ 楕円・超楕円曲線 C_0に対して，同種条件下での曲線の分類が行われ，村井らによって再検討が行われた [1][2]．また同種条件を外した場合に関しては鐘ヶ江らによって種数 1，4 次拡大体上の一部のクラスに対する分類が行われた [3]．

主結果 本論文では，いまだ分類が行われていない，被覆攻撃の対象となる偶標数有限体の拡大体上の楕円・超楕円曲線 C_0 の以下の Case に対して分類を行った．

(a)： $g(C_0) = 1,\ d = 3,\ n = 3$
(b)： $g(C_0) = 1,\ d = 5,\ n = 4$
(c)： $g(C_0) = 2,\ d = 4,\ n = 3$
(d)： $d = 2^n - 1$

本稿では抜粋して，5 節で (a)，6 節で (c) の曲線に対して考察を行い，同種条件を満たさない場合の楕円・超楕円曲線の係数条件などを示した．

2　被覆攻撃と $(2,\ldots,2)$ 型被覆

k_d/k 上のフロベニウス自己同型写像を $\sigma_{k_d/k}$ とし，$\sigma_{k_d/k}$ の拡張となる，関数体 $k_d(x)$ の分離閉包における位数 d の自己同型写像 σ を考える．k_d上定義される楕円・超楕円曲線 C_0に対し，$k_d(C_0)/k(x)$ のガロア閉包を $K := k_d(C_0) \cdot k_d({}^{\sigma}C_0) \cdots k_d({}^{\sigma^{d-1}}C_0)$ とすると，ある代数曲線 C が存在して $K \simeq k_d(C)$ となる．$\{C_0, {}^{\sigma}C_0, \cdots, {}^{\sigma^{d-1}}C_0\}$ は $\mathrm{Gal}(k_d/k) = \langle\sigma\rangle$ で不変なので，σ の固定体 $K' := \{\xi \in K \mid \sigma(\xi) = \xi\}$ は $K' \simeq k(C)$ となる．本論文では，次の偶標数の楕円・超楕円曲線 C_0 を用いる．

$$C_0/k_d \ :\ y^2 + g(x)y = f(x)\ (f(x), g(x) \in k_d[x])$$

このとき C_0 は 2 次の被覆を持つ．

$$C_0 \xrightarrow{2} \mathbb{P}^1(x)/k, \quad (x, y) \ \mapsto\ x$$

C_0に共役な楕円・超楕円曲線${}^{\sigma^i}C_0$は，

$$\sigma\ :\ k_d(C) \to k_d(C),\ k_d \ni \alpha \mapsto \alpha^q,\ x \mapsto x,\ y \mapsto {}^{\sigma}y$$
$${}^{\sigma^i}C_0 : {}^{\sigma^i}y^2 + {}^{\sigma^i}g(x)\,{}^{\sigma^i}y = {}^{\sigma^i}f(x) \quad (0 \le i \le d-1)$$

${}^{\sigma^i}C_0$の関数体 $k_d({}^{\sigma^i}C_0) = k_d(x, {}^{\sigma^i}y)$ となる．
さらに，$k_d({}^{\sigma^i}C_0)$ が線形無関連となる最大の n $(\leq d)$ を選ぶと，$k_d(C) \simeq k_d(x, y, {}^{\sigma}y, \cdots, {}^{\sigma^{n-1}}y)$ となる．
被覆 $\pi/k_d : C \to \mathbb{P}^1(x)$ は 次のようになっている．

$$cov(C/\mathbb{P}^1(x)) := \mathrm{Gal}(k_d(C)/k_d(x)) \simeq \mathbb{F}_2^n$$

これを $\overbrace{(2, \ldots, 2)}^{n}$ 型被覆と呼ぶ．

3 同種条件

同種条件とは，[1] の Condition(C) を指す．この条件は，偶標数有限体上の楕円・超楕円曲線 C_0に対する被覆曲線 C について，$g(C) = d \cdot g(C_0)$ と同値である．ここで，C_0と共役な曲線との組合わせて構成される曲線の中で，共役な曲線でない曲線を C_jとすると，同種条件はすべての C_jが $\mathbb{P}^1$となる場合を意味する．同種条件を満たさない一般の場合は $g(C) \geq d \cdot g(C_0) + e$ $(e \in \mathbb{N})$ となる．ここでの e の値は，C_jの中で，$\mathbb{P}^1$にならない曲線の種数の総和になる．

4 楕円・超楕円曲線の標準形と $\mathbb{P}^1$ の条件

本論文では以下の Case の楕円・超楕円曲線 C_0 に対して分類を行う．
(a)： $g(C_0) = 1,\ d = 3,\ n = 3$
(b)： $g(C_0) = 1,\ d = 5,\ n = 4$
(c)： $g(C_0) = 2,\ d = 4,\ n = 3$
それぞれの Case で扱う C_0 の標準形と，考察の際に利用する $\mathbb{P}^1$ になる条件を [2][3] より，楕円曲線の場合と $g(C_0) = 2$ の超楕円曲線の場合 に分けて記載する．また，Case:(a)(b)(c) において，C_j が代数的閉体上で既約であると仮定する．次の Case に関しては $(2, \ldots, 2)$ 型被覆の構造から同種条件を満たさない楕円・超楕円曲線が存在しない点を示す．
(d)： $d = 2^n - 1$
本稿では，Case:(a)(c) の C_0 が Ordinary の場合の分類を抜粋して掲載する．

4.1 楕円曲線 $(g(C_0) = 1)$ の場合

[3] より，有限体 k_d は完全体なので Ordinary の場合の偶標数有限体 k_d上の楕円曲線は以下の式で表せる．

$$E_1/k_d : y^2 + xy = ax^3 + bx^2 + cx (a, c \in k_d \backslash \{0\}, b \in k_d) \quad (1)$$

(a) では (1) 式の形を扱う．次に，(1) 式を用いて，新たに構成される曲線 C_j が $\mathbb{P}^1$ になる条件を示す．$F(x, y) = y^2 + xy + Ax^3 + Bx^2 + Cx$ とおくと連立方程式

$$\begin{cases} F = 0 \\ \partial F/\partial y = x = 0 \\ \partial F/\partial x = y + Ax^2 + C = 0 \end{cases} \quad (2)$$

より解を持つ場合は $C = 0$ のみである．以上より C_j が $\mathbb{P}^1$ となる条件は $C = 0$ になる場合，または $A = 0$ で右辺が定数でない 2 次曲線となる場合である．

4.2 超楕円曲線 $(g(C_0) = 2)$ の場合

[2] より Ordinary の場合は以下の偶標数有限体 k_4上の超楕円曲線を用いる．

$$\begin{gathered} E_3/k_4 : y^2 + g(x)y = ax^5 + bx^4 + cx^3 + dx^2 + ex + f \\ g(x) = (x + \alpha)(x + \alpha^q) \\ (a \in k_4 \backslash \{0\}, b, c, d, e, f \in k_4, \alpha \in k_2 \backslash k) \end{gathered} \quad (3)$$

(c) では (3) 式を扱う．

次に $\mathbb{P}^1$ となる条件を示す．[2] より今回の Case で新たに構成される曲線 C_j が $\mathbb{P}^1$ になるのは右辺が $g(x)^2 l (l = sx + t, s, t \in k_2)$ となる場合である．実際，$F(x, y) = y^2 + g(x)y + g(x)^2 l$ とおくと連立方程式

$$\begin{cases} F = 0 \\ \partial F/\partial y = g(x) = (x + \alpha)(x + \alpha^q) = 0 \\ \partial F/\partial x = y(\alpha + \alpha^q) + (x + \alpha)^2 (x + \alpha^q)^2 l' = 0 \end{cases} \quad (4)$$

より，$y = 0, g(x) = 0$ で解を持ち，C_j は $\mathbb{P}^1$ となる．

5 (a)： $g(C_0) = 1,\ d = 3,\ n = 3$

4.1 節より本 Case では (1) 式の偶標数有限体 k_3 上の楕円曲線を用いる．これから C_0 に共役な楕円曲線 ${}^{\sigma^i}C_0$ を以下に示す．

$$\begin{cases} C_0 : y^2 + xy = ax^3 + bx^2 + cx (a, c \in k_3 \backslash \{0\}, b \in k_3) \\ {}^{\sigma}C_0 : {}^{\sigma}y^2 + x^{\sigma}y = a^q x^3 + b^q x^2 + c^q x \\ {}^{\sigma^2}C_0 : {}^{\sigma^2}y^2 + x^{\sigma^2}y = a^{q^2} x^3 + b^{q^2} x^2 + c^{q^2} x \end{cases}$$

以降本論文内では，構成される曲線を次の記号で表す．

$$\begin{gathered} C_0 \ : \ y^2 + g(x)y = f(x),\ g(x) = {}^{\sigma}g(x) \\ \emptyset \subsetneq I \subseteq \{0, ..., n-1\} \text{ に対し，} \\ (\textstyle\sum_{i \in I} {}^{\sigma^i}y)^2 + g(x)(\sum_{i \in I} {}^{\sigma^i}y) = f_{\sum_{i \in I} {}^{\sigma^i}C_0}(x) \end{gathered}$$

上記記号を使い，共役曲線を組み合わせて構成される曲線 C_j を以下に示す．

$$\begin{cases} f_{C_0 + {}^{\sigma}C_0}(x) = (a + a^q)x^3 + (b + b^q)x^2 + (c + c^q)x \\ f_{C_0 + {}^{\sigma^2}C_0}(x) = (a + a^{q^2})x^3 + (b + b^{q^2})x^2 + (c + c^{q^2})x \\ f_{{}^{\sigma}C_0 + {}^{\sigma^2}C_0}(x) = \\ \qquad (a^q + a^{q^2})x^3 + (b^q + b^{q^2})x^2 + (c^q + c^{q^2})x \\ f_{C_0 + {}^{\sigma}C_0 + {}^{\sigma^2}C_0}(x) = \\ (a + a^q + a^{q^2})x^3 + (b + b^q + b^{q^2})x^2 + (c + c^q + c^{q^2})x \end{cases}$$

以上の C_j と 4.1 節の $\mathbb{P}^1$ になる条件から同種条件を満たさない楕円曲線の係数条件を以下に示す．

表 4.1: Case (a) Ordinary 係数条件

No.	e	係数条件
1	1	$a \in k \backslash \{0\}, c \in k_3 \backslash k, b \in k_3, \mathrm{Tr}(c) \neq 0$
2		$c \in k \backslash \{0\}, a \in k_3 \backslash k, b \in k_3, \mathrm{Tr}(a) \neq 0$
3	3	$a, c, ac \in k_3 \backslash k, b \in k_3, \mathrm{Tr}(a) = 0, \mathrm{Tr}(c) \neq 0$
4		$a, c, ac \in k_3 \backslash k, b \in k_3, \mathrm{Tr}(c) = 0, \mathrm{Tr}(a) \neq 0$
5	4	$a, c, ac \in k_3 \backslash k, b \in k_3, \mathrm{Tr}(a) \neq 0, \mathrm{Tr}(c) \neq 0$

具体例のため，No.1 の係数条件による分類計算を記載する．係数条件から (5) 式の曲線 C_j 次の式で表される．

$$\begin{cases} f_{C_0+{}^{\sigma}C_0}(x) = (b+b^q)x^2 + (c+c^q)x \\ f_{C_0+{}^{\sigma^2}C_0}(x) = (b+b^{q^2})x^2 + (c+c^{q^2})x \\ f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x) = (b^q+b^{q^2})x^2 + (c^q+c^{q^2})x \\ f_{C_0+{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x) = \\ \qquad a^{q^2}x^3 + (b+b^q+b^{q^2})x^2 + (c+c^q+c^{q^2})x \end{cases}$$

よって，C_j の内，$C_0+{}^{\sigma}C_0$, $C_0+{}^{\sigma^2}C_0$, ${}^{\sigma}C_0+{}^{\sigma^2}C_0$ は $\mathbb{P}^1$ となり，$C_0+{}^{\sigma}C_0+{}^{\sigma^2}C_0$ は種数 1 の曲線になるため，同種条件を満たさず $e=1$ となる．

6 (c) : $g(C_0)=2,\ d=4,\ n=3$

4.2 節より本 Case では (3) 式の偶標数有限体 k_4 上の超楕円曲線を用いる．これから C_0 に共役な超楕円曲線 ${}^{\sigma^i}C_0$ を以下に示す．

$$\begin{cases} C_0 : y^2+g(x)y = f(x) \\ \qquad f(x) = ax^5+bx^4+cx^3+dx^2+ex+f \\ g(x) = (x+\alpha)(x+\alpha^q)\ (a\in k_4\backslash\{0\}, b,c,d,e,f\in k_4, \alpha\in k_2\backslash k) \\ \mathrm{Tr}(a)=0, \mathrm{Tr}(b)=0, \mathrm{Tr}(c)=0, \mathrm{Tr}(d)=0, \mathrm{Tr}(e)=0, \mathrm{Tr}(f)=0) \\ {}^{\sigma}C_0 : {}^{\sigma}y^2+g(x){}^{\sigma}y = a^qx^5+b^qx^4+c^qx^3+d^qx^2+e^qx+f^q \\ {}^{\sigma^2}C_0 : {}^{\sigma^2}y^2+g(x){}^{\sigma^2}y = \\ \qquad a^{q^2}x^5+b^{q^2}x^4+c^{q^2}x^3+d^{q^2}x^2+e^{q^2}x+f^{q^2} \\ {}^{\sigma^3}C_0 : {}^{\sigma^3}y^2+g(x){}^{\sigma^3}y = \\ \qquad a^{q^3}x^5+b^{q^3}x^4+c^{q^3}x^3+d^{q^3}x^2+e^{q^3}x+f^{q^3} \end{cases}$$

係数条件より ${}^{\sigma^3}C_0$ は C_0, ${}^{\sigma}C_0$, ${}^{\sigma^2}C_0$ で表せるため，$n=3$ となる．よって以降の考察では C_0, ${}^{\sigma}C_0$, ${}^{\sigma^2}C_0$ のみの共役曲線を扱う．これら共役曲線を組み合わせて構成される曲線 C_j を以下に示す．

$$\begin{cases} f_{C_0+{}^{\sigma}C_0}(x) = (a+a^q)x^5+(b+b^q)x^4+(c+c^q)x^3 \\ \qquad +(d+d^q)x^2+(e+e^q)x+(f+f^q) \\ f_{C_0+{}^{\sigma^2}C_0}(x) = (a+a^{q^2})x^5+(b+b^{q^2})x^4+(c+c^{q^2})x^3 \\ \qquad +(d+d^{q^2})x^2+(e+e^{q^2})x+(f+f^{q^2}) \\ f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x) = (a^q+a^{q^2})x^5+(b^q+b^{q^2})x^4+(c^q+c^{q^2})x^3 \\ \qquad +(d^q+d^{q^2})x^2+(e^q+e^{q^2})x+(f^q+f^{q^2}) \end{cases}$$

以上の C_j と 4.2 節の $\mathbb{P}^1$ になる条件から同種条件を満たさない超楕円曲線の係数条件について考察する．以降 $l=sx+t(s,t\in k_2)$ を用いる．

6.1 $f_{C_0+{}^{\sigma^2}C_0}(x) = g(x)^2l$

$f_{C_0+{}^{\sigma^2}C_0}(x) = g(x)^2l$ になる場合を考える．

$$\begin{aligned} f_{C_0+{}^{\sigma^2}C_0}(x) &= (a+a^{q^2})x^5+(b+b^{q^2})x^4+(c+c^{q^2})x^3 \\ &\quad +(d+d^{q^2})x^2+(e+e^{q^2})x+(f+f^{q^2}) \\ g(x)^2l &= sx^5+tx^4+s(\alpha+\alpha^q)^2x^3 \\ &\quad +t(\alpha+\alpha^q)^2x^2+s(\alpha\alpha^q)^2x+t(\alpha\alpha^q)^2 \end{aligned}$$

より係数比較を行う．

$$a+a^{q^2}=s,\quad b+b^{q^2}=t,\quad c+c^{q^2}=s(\alpha+\alpha^q)^2,$$
$$d+d^{q^2}=t(\alpha+\alpha^q)^2,\ e+e^{q^2}=s(\alpha\alpha^q)^2,\ f+f^{q^2}=t(\alpha\alpha^q)^2$$

以上の結果より，s,t に関する条件を定める．
$\mathrm{Tr}(a)=0$ より，

$$(a+a^{q^2})^q = a^q+a^{q^3} = a^q+a+a^q+a^{q^2} = a+a^{q^2}$$

より $a+a^{q^2}\in k$. よって $s\in k$. 同様に $t\in k$ である．次に $\alpha+\alpha^q,\ \alpha\alpha^q\in k$ を示す．$\alpha\in k_2$ より，

$$\begin{aligned} (\alpha+\alpha^q)^q &= \alpha^q+\alpha^{q^2} = \alpha^q+\alpha \\ (\alpha\alpha^q)^q &= \alpha^q\alpha^{q^2} = \alpha^q\alpha \end{aligned}$$

より $\alpha+\alpha^q,\ \alpha\alpha^q\in k$. よって $g(x)^2l\in k[x]$ である．次に，$f_{C_0+{}^{\sigma^2}C_0}(x) = g(x)^2l$ のとき，$f_{C_0+{}^{\sigma}C_0}(x) = g(x)^2l'$ となる場合を考える．係数比較の結果から，

$$a+a^{q^2}=s \longrightarrow a+a^q = s+a^q+a^{q^2}$$

となり，$a+a^q$は $g(x)^2l$ と $f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x)$ の x の 5 次項の和として考えられる．よって

$$\begin{aligned} f_{C_0+{}^{\sigma}C_0}(x) &= (s+a^q+a^{q^2})x^5+(t+b^q+b^{q^2})x^4+ \\ &\{s(\alpha+\alpha^q)^2+c^q+c^{q^2}\}x^3+\{t(\alpha+\alpha^q)^2+d^q+d^{q^2}\}x^2 \\ &\quad +\{s(\alpha\alpha^q)^2+e^q+e^{q^2}\}x+\{t(\alpha\alpha^q)^2+f^q+f^{q^2}\} \\ &\quad = g(x)^2l+\{{}^{\sigma}f(x)+{}^{\sigma^2}f(x)\} \end{aligned}$$

になり，$f_{C_0+{}^{\sigma}C_0}(x)$ は $g(x)^2l+\{{}^{\sigma}f(x)+{}^{\sigma^2}f(x)\}$ で表現できる．今，$f_{C_0+{}^{\sigma}C_0}(x)=g(x)^2l'$ となる場合を考えているため，上式より，

$$\begin{aligned} &g(x)^2l+\{{}^{\sigma}f(x)+{}^{\sigma^2}f(x)\} = g(x)^2l' \\ &\qquad \longrightarrow {}^{\sigma}f(x)+{}^{\sigma^2}f(x) = g(x)^2(l+l') \end{aligned}$$

となる．この式より，$f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x)$ は $g(x)^2l$ の形になり $\mathbb{P}^1$ となる．このとき，すべての C_j が $\mathbb{P}^1$ となるため，同種条件を満たす場合となる．本論文では同種条件を満たさない場合に関して考えるため，今後，$f_{C_0+{}^{\sigma^2}C_0}(x)=g(x)^2l$ のとき，$f_{C_0+{}^{\sigma}C_0}(x)\neq g(x)^2l'$, または $f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x)\neq g(x)^2l'$ となると仮定する．以上の条件より，同種条件を満たさない超楕円曲線の係数条件を決定する．

- $l=sx\quad (s\in k)$

$g(x)^2l(l=sx)$ と $f_{C_0+{}^{\sigma^2}C_0}(x)$ との係数比較を行うと，

$$a+a^{q^2}=s,\ b+b^{q^2}=0,\qquad c+c^{q^2}=s(\alpha+\alpha^q)^2,$$
$$d+d^{q^2}=0,\ e+e^{q^2}=s(\alpha\alpha^q)^2,\ f+f^{q^2}=0$$

となる．この結果から $b,d,f\in k_2,\ a,c,e\in k_4\backslash k_2$ が分かる．$b,d,f\in k_2$ より，$C_0+{}^{\sigma}C_0, {}^{\sigma}C_0+{}^{\sigma^2}C_0$ に関しても，x^4, x^2, 定数項 の係数が 0 になる場合が考えられる．いずれかの係数が 0 になると考えたとき，種数が 2 となる場合しか存在しない．よって $l=sx$ の場合は

次の係数条件が考えられる.

表 6.1: Case:(c) Ordinary No.6 係数条件

No.	e	係数条件
6	4	$\alpha \in k_2\backslash k,\ b,d,f \in k_2,\ a,c,e \in k_4\backslash k_2$

この他の条件に関しては分類表にて記載する.

6.2 $f_{C_0+{}^{\sigma}C_0}(x) = g(x)^2 l$

$f_{C_0+{}^{\sigma}C_0}(x) = g(x)^2 l$ になる場合を考える.
$f_{C_0+{}^{\sigma}C_0}(x) = g(x)^2 l$ より,

$$f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x) = g(x)^{2\sigma} l$$
$$f_{C_0+{}^{\sigma^2}C_0}(x) = g(x)^2(l + {}^{\sigma}l)$$

よってすべての C_j が $\mathbb{P}^1$ のため, 同種条件を満たさない場合は存在しない. これは $f_{{}^{\sigma}C_0+{}^{\sigma^2}C_0}(x) = g(x)^2 l$ の場合も同様である.

7 むすび

本論文では, 被覆攻撃の対象となる同種条件を満たさない偶標数有限体上の楕円・超楕円曲線の 4 つのクラスに対して分類を行い, 楕円・超楕円曲線の係数条件を明らかにした. 今後の課題として, 別の種数や拡大次数に対する曲線の分類などが挙げられる.

謝辞

本研究を進めるにあたり, 適切な御指導, 御助言, 御検討を頂いた中央大学理工学部 趙晋輝 教授, 共同で研究を行った東海大学理系教育センター准教授 志村真帆呂 先生に深く感謝いたします. また, 日頃の研究において, 有益な議論と御助言を頂きました中央大学理工学部情報工学科 趙研究室の皆様に感謝いたします.

関連発表

• 登丸尚哉, 飯島努, 志村真帆呂, 趙晋輝 “被覆攻撃の対象となる有限体の拡大体上の楕円・超楕円曲線から被覆曲線の構成に関する研究”, Proc. of IEICE Society Conference 2022, IEICE Japan, 2022.
• 登丸尚哉, 志村真帆呂, 趙晋輝 “同種条件を満たさない被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線の分類”, Proc. of SCIS2024, IEICE Japan, 2024.

参考文献

[1] F. Momose and J. Chao, “Classification of Weil restrictions obtained by $(2,\ldots,2)$ coverings of $\mathbb{P}^1$”, preprint, 2006. Available from https://eprint.iacr.org/2006/347 (accessed 2024-2-12).
[2] 村井公輔, 志村真帆呂, 飯島努, 趙晋輝“被覆攻撃の対象となる偶標数有限体上の楕円・超楕円曲線に対する同種条件下の完全分類”, Proc. of SCIS2022, IEICE Japan, 2022.
[3] 鐘ケ江柊子, 志村真帆呂, 趙晋輝 “同種条件を満たさない被覆攻撃の対象となる偶標数 4 次拡大体上の楕円・超楕円曲線の分類”, Proc. of IEICE Society Conference 2022, IEICE Japan, 2022.

No.	$g(C_0), d, n$	e	$g(C)$	C_0	係数条件
1	$g(C_0)=1$ $d=3$ $n=3$	1	4	$y^2+xy=ax^3+bx^2+cx$	$a \in k\backslash\{0\}, c \in k_3\backslash k, b \in k_3,\ \mathrm{Tr}(c) \neq 0$
2					$c \in k\backslash\{0\}, a \in k_3\backslash k, b \in k_3,\ \mathrm{Tr}(a) \neq 0$
3		3	6		$a, c, ac \in k_3\backslash k, b \in k_3, \mathrm{Tr}(a)=0, \mathrm{Tr}(c) \neq 0$
4					$a, c, ac \in k_3\backslash k, b \in k_3, \mathrm{Tr}(c)=0, \mathrm{Tr}(a) \neq 0$
5		4	7		$a, c, ac \in k_3\backslash k, b \in k_3, \mathrm{Tr}(a) \neq 0, \mathrm{Tr}(c) \neq 0$
6	$g(C_0)=2$ $d=4$ $n=3$	4	12	$y^2+g(x)y=f(x)$ $f(x)=ax^5+bx^4+cx^3+dx^2+ex+f \quad (*)$ $g(x)=(x+\alpha)(x+\alpha^q)$ $f(x)+{}^{\sigma^2}f(x)=g(x)^2 l$ (†)	$\alpha \in k_2\backslash k,\ b,d,f \in k_2, a,c,e \in k_4\backslash k_2,$ $l = sx, (s \in k\backslash\{0\})$
7					$\alpha \in k_2\backslash k, a,b,c,d,e,f \in k_4\backslash k_2,$ $l = sx+t, (s,t \in k\backslash\{0\})$
8		6	14	C_0は (†) と同じ ${}^{\sigma^i}C_0 + {}^{\sigma^j}C_0 : \mathbb{P}^1$ではない $i \neq j\ (i,j \in \{0,1,2\})$	$\alpha \in k_2\backslash k, a \in k_4\backslash k_2, b,c,d,e,f \in k_4$

$g(C)$ は被覆曲線 C の種数の下限を表している

$(*) \quad \mathrm{Tr}(a)=0, \mathrm{Tr}(b)=0, \mathrm{Tr}(c)=0, \mathrm{Tr}(d)=0, \mathrm{Tr}(e)=0, \mathrm{Tr}(f)=0$