計算代数幾何アルゴリズムを用いた超特別曲線の存在性と数え上げの進展状況

工藤 桃成 [1]

[1] 東京大学大学院情報理工学系研究科・助教

早稲田整数論セミナー

2022.10.28

本研究対象 (超特別曲線) の定義と位置づけ

k : 標数 $p > 0$ の代数閉体
C : 種数 g の曲線 $/k$ (曲線 $=$ 1 次元非特異射影多様体)
E : 超特異楕円曲線 $/k$

Definition 1.1

- C : 超特異 (supersingular) $\Leftrightarrow \mathrm{Jac}(C) \sim E^g$ (isogenous).
- C : 超特別 (superspecial) $\Leftrightarrow \mathrm{Jac}(C) \cong E^g$ (isomorphic).

超特異曲線・超特別曲線の重要性

- 曲線のモジュライの階層構造理解
- 種数に関して有理点を多くもつ曲線
- (特に種数 $1, 2$) 同種写像暗号の構成・安全性評価に利用

本講演： 超特別曲線に着目

超特別曲線の性質・特徴付け (1/2)

- C : 種数 g の曲線 $/k$
- $\mathscr{F}$: C 上の絶対フロベニウス射
- $\mathscr{F}$: $H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)$ (誘導された p 線形写像)
- $\mathscr{C}$: $H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$ (Cartier 作用)

Fact 1.2 (Nygaard '82)

C : 超特別 $\iff$ $\mathscr{F}$ が零写像 $\iff$ $\mathscr{C}$ が零写像

Definition 1.3

- $\mathscr{F}$ の表現行列を C の Hasse-Witt 行列,
- $\mathscr{C}$ の表現行列を C の Cartier-Manin 行列という.

超特別曲線の性質・特徴付け (2/2)

Fact 1.4 (Ekedahl '87)

1. $\mathbb{F}_{p^2}$ 上の最大曲線および最小曲線は超特別である.
2. C : 超特別なら, ある最大または最小曲線 C_0 $/\mathbb{F}_{p^2}$ が存在して

$$C_0 \times_{\mathrm{Spec}(\mathbb{F}_{p^2})} \mathrm{Spec}(k) \cong C.$$

Definition 1.5 (Hasse-Weil bound)

X : 種数 g の曲線 $/\mathbb{F}_q$ に対し

$$1 - 2g\sqrt{q} + q \leq \#X(\mathbb{F}_q) \leq 1 + 2g\sqrt{q} + q.$$

上限 (resp. 下限) 値を満たすとき X を $\mathbb{F}_q$ 最大 (resp. 最小) という.

Motivation

Problem (cf. Ekedahl '87)

与えられた (p, g) に対し，種数 g の超特別曲線 $/\overline{\mathbb{F}_p}$ は存在するか？存在する場合，同型類を全て求めよ.

Remark 1.6

与えられた (p, g) に対し，種数 g の超特別曲線 $/\overline{\mathbb{F}_p}$ の同型類は高々有限個 (0 もあり得る).

$\mathrm{Ssp}_g(\mathbb{F}_q)$: 種数 g 超特別曲線 $/\mathbb{F}_q$ の $\mathbb{F}_q$ 同型類の全体

Proposition 1.7 (K. and Harashita '20)

$g \geq 2$ のとき, $a \equiv b \pmod 2 \Longrightarrow \mathrm{Ssp}_g(\mathbb{F}_{p^a}) \simeq \mathrm{Ssp}_g(\mathbb{F}_{p^b})$

先行研究の概要 (1/4)

Theorem 1.8 (Ekedahl '87)

以下を満たす超特別曲線は存在しない.

- $p^2 - p < 2g$
- $p < 2g + 1$, C : 超楕円, $(g, p) \neq (1, 2)$

種数 ≤ 3 : 任意 p に対する $\overline{\mathbb{F}_p}$ 同型類の個数が理論的に決定済み

Deuring, Igusa, Serre, Ibukiyama, Katsura, Oort, ...

先行研究の概要 (2/4)

種数 1 (楕円曲線)

- **[Deuring '41]** :

$$(\text{同型類の個数}) = (\text{四元数環 } B = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \text{ の類数})$$

ここで E は超特異楕円曲線 $/\overline{\mathbb{F}_p}$.

- 右辺は **[Eichler '38]** により計算可能で,

$$(\text{超特異楕円曲線の個数}) = \begin{cases} 1 & (p = 2, 3) \\ \frac{p-1}{12} + \frac{1-(\frac{-1}{p})}{4} + \frac{1-(\frac{-3}{p})}{3} & (p > 3) \end{cases}$$

- cf. **[Igusa '58]** : $y^2 = x(x-1)(x-\lambda)$ を用いて直接的に計算

先行研究の概要 (3/4)

種数 $2, 3$

- **[Ibukiyama-Katsura-Oort '86]** 任意の $g \geq 2$ に対し

$$(*) \quad \begin{array}{l} (\text{次元 } g \text{ 主偏極超特別アーベル多様体の個数}) \\ = (\text{四元数的エルミート空間 } B^g \text{ の pricipal genus の類数 } H_g) \end{array}$$

- **[Oort-Ueno '73]**
  次元 ≤ 3 の任意の主偏極アーベル多様体は
  (possibly reduced な) 曲線のヤコビ多様体に同型

超特別曲線の個数
$\longrightarrow$ 式 $(*)$ から主偏極が decomposable なものの個数を引けばよい

先行研究の概要 (4/4)

種数 $2, 3$ (続き)

g	種数 g 超特別曲線の $\overline{\mathbb{F}_p}$ 同型類の個数	H_g の計算結果
1	H_1	**[Eichler '38]**
2	$H_2 - H_1(H_1+1)/2$	**[Hashimoto-Ibukiyama '80]**
3	$H_3 -$ (H_1, H_2 で表される式)	**[Hashimoto '83]**

Theorem 1.9 (Ibukiyama '93)

任意の $p \geq 3$ に対し, 種数 3 曲線 $/\mathbb{F}_p$ で $\mathbb{F}_{p^{2e}}$ 最大 (resp. $\mathbb{F}_{p^{2e}}$ 最小) なものが存在する. ここで e は奇数 (resp. 偶数).

種数 ≥ 4 の超特別曲線

各種数 $g \geq 4$, 標数 $p > 0$ について存在するか一般には不明

種数 4

- $p = 2, 3$: Ekedahl bound より非存在
- $p = 5$: 一意に存在 [Fuhrmann-Garcia-Torres '97]
- $p \geq 7$: 一般には不明

種数 5

- $p = 2, 3$: Ekedahl bound より非存在
- $p = 5$: 非存在 [Fuhrmann-Torres '96]
- $p \geq 7$: 一般には不明

本講演内容

近年, 講演者らの研究で $g = 4, 5$ で $p \geq 7$ の場合に
超特別曲線の (非) 存在, 数え上げの結果が得られた.

$\longrightarrow$ 代数曲線論 + 計算代数幾何の技法 + 計算機代数システム

本講演 一連の結果と計算代数幾何の技法を併せて紹介

1. Introduction

2. 数え上げ (同型類列挙)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 5 トリゴナル (時間があれば)

3. 大きい標数での存在性 (自己同型群で絞った高速探索)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 3 非超楕円・超楕円 (時間があれば)

4. まとめと今後の課題

1. Introduction

2. 数え上げ (同型類列挙)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 5 トリゴナル (時間があれば)

3. 大きい標数での存在性 (自己同型群で絞った高速探索)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 3 非超楕円・超楕円 (時間があれば)

4. まとめと今後の課題

参考文献

本節の主結果は以下の論文を参照:

- M. Kudo and S. Harashita (2017): Superspecial curves of genus 4 in small characteristic. Finite Fields and Their Applications, **45**, 131–169.
- M. Kudo (2019): On the existence of superspecial and maximal nonhyperelliptic curves of genera four and five. Communications in Algebra, **47**, Issue 12, 5020–5038.
- M. Kudo and S. Harashita (2020): Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4. Tokyo Journal of Mathematics, **43**, Number 1, 259–278.

種数 4 非超楕円曲線の標準モデルと定義体

K : 標数 $p > 2$ の完全体
C : 種数 4 非超楕円曲線 $/K$

Fact 2.1

$\exists Q \in \overline{K}[x, y, z, w]_2$ (既約二次形式),
$\exists P \in \overline{K}[x, y, z, w]_3$ (既約三次形式) が存在して
C は $\mathbb{P}^3$ 内の二次曲面と三次曲面の完全交叉 $V(Q, P)$ に K 上同型.

Lemma 2.2

Q, P の係数は全て K の元にとれる.

以下, $C = V(Q, P) \subset \mathbb{P}^3$ とする.

種数 4 非超楕円曲線の Hasse-Witt 行列 (1/4)

Proposition 2.3

$C = V(Q, P)$ の Hasse-Witt 行列 A の 16 個の成分は

$$(QP)^{p-1} \text{ の } x^{ip-i'} y^{jp-j'} z^{kp-k'} w^{\ell p-\ell'} \text{ の係数}$$

である. ただし
$i, j, k, \ell, i', j', k', \ell' > 0$ かつ $i + j + k + \ell = i' + j' + k' + \ell' = 4$.

一般の完全交叉や, より一般の射影スキームに対する
コホモロジー群へのフロベニウス作用の計算は次を参照

- K. (2022): Computing representation matrices for the action of Frobenius on cohomology groups.
  Journal of Symbolic Computation, **109**, 441–464.

種数 4 非超楕円曲線の Hasse-Witt 行列 (2/4)

前頁の Prop. の証明

$S = K[x, y, z, w]$
$I := \langle P, Q \rangle_S$
$I_p := \langle P^p, Q^p \rangle_S$

次の可換図式 (横は完全列) を得る :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S(-5p) & \xrightarrow{(Q^p, -P^p)} & S(-3p) \oplus S(-2p) & \xrightarrow{{}^t(P^p, Q^p)} & S & \longrightarrow & S/I_p \longrightarrow 0 \\
 & & \downarrow{\scriptstyle (QP)^{p-1}} & & \downarrow{\scriptstyle \begin{pmatrix} P^{p-1} & 0 \\ 0 & Q^{p-1} \end{pmatrix}} & & \downarrow & & \downarrow \\
0 & \longrightarrow & S(-5) & \xrightarrow[(Q, -P)]{} & S(-3) \oplus S(-2) & \xrightarrow[{}^t(P, Q)]{} & S & \longrightarrow & S/I \longrightarrow 0
\end{array}$$

加群の層をとり, コホモロジー群の長完全列から次を得る (次頁)

種数 4 非超楕円曲線の Hasse-Witt 行列 (3/4)

$$\begin{array}{ccc} H^1(C,\mathcal{O}_C) & \xrightarrow{\cong} & H^3(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(-5)) \\ \downarrow & & \downarrow p\text{ 乗} \\ H^1(C_p,\mathcal{O}_{C_p}) & \xrightarrow{\cong} & H^3(\mathbb{P}^3,\mathcal{O}(-5p)) \\ \downarrow & & \downarrow \times(PQ)^{p-1} \\ H^1(C,\mathcal{O}_C) & \xrightarrow{\cong} & H^3(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(-5)) \end{array}$$

ここで $C_p := V(Q^p, P^p)$ であり, 左縦はフロベニウス作用である.

$$H^3(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(-5)) = \left\langle \frac{1}{x^2yzw}, \frac{1}{xy^2zw}, \frac{1}{xyz^2w}, \frac{1}{xyzw^2} \right\rangle$$

□

種数 4 非超楕円曲線の Hasse-Witt 行列 (4/4)

Proposition 2.4

$C = V(Q, P)$ の Hasse-Witt 行列 A の 16 個の成分は

$$(QP)^{p-1} \text{ の } x^{ip-i'} y^{jp-j'} z^{kp-k'} w^{\ell p-\ell'} \text{ の係数}$$

である. ただし
$i, j, k, \ell, i', j', k', \ell' > 0$ かつ $i + j + k + \ell = i' + j' + k' + \ell' = 4$.

よって, Q, P の未知係数 (10+20 個) をパラメータとみなせば,

超特別な C の数え上げ $\Longleftrightarrow$ 16 個の式からなる系 $A = 0$ の求解

しかしこのままではパラメータ数が多く計算機でも求解困難...

工夫１：同型変換によるパラメータ数削減 (1/4)

以下, 本小節を通して

- K : 標数 $p \neq 2$ の有限体
- $\varepsilon \in K^\times \setminus (K^\times)^2$: 固定

Fact 2.5

有限体上の二次形式は階数と判別式で分類される.

二次形式 Q は次のいずれかと仮定してよい :

(N1): $2xw + 2yz$, (N2): $2xw + y^2 - \varepsilon z^2$, (D): $2yw + z^2$.

あとは三次形式 P の未知係数をいかに減らすか？

工夫１：同型変換によるパラメータ数削減 (2/4)

φ : Q に対応する対称行列

$$\tilde{\mathrm{O}}_Q(K) := \{h \in \mathrm{GL}_4(K) : {}^t h\varphi h = \mu\varphi, \quad \mu \in K^\times\}.$$

Lemma 2.6

種数 4 非超楕円曲線 $V(Q, P_1)$ と $V(Q, P_2)$ が K 上同型
$\iff \exists (M, \lambda) \in \tilde{\mathrm{O}}_Q(K) \times K^\times$ s.t. $M \cdot P_1 \equiv \lambda P_2 \pmod{Q}$.

“mod$Q$” ＋ 定数倍 ＋ $\tilde{\mathrm{O}}_Q(K)$ の作用　で P を変換してよい！

$\tilde{\mathrm{O}}_Q(K)$ の元はどんな形か？ $\longrightarrow$ Bruhat 分解で求まる！

工夫１：同型変換によるパラメータ数削減 (3/4)

(N1) の場合: $Q = 2xw + 2yz$ のとき, $\tilde{\mathrm{O}}_Q(K) = \tilde{\mathrm{B}}\mathrm{WU}$.

$$\mathrm{A} = \left\{ E_4, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}, \ s_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \ s_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\tilde{\mathrm{T}} = \{\mathrm{diag}(a, b, cb^{-1}, ca^{-1}) : a, b, c \in K^\times\}$$

$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & d & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -d \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & e & 0 \\ 0 & 1 & 0 & -e \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid d, e \in K \right\}$$

$$\tilde{\mathrm{B}} = \mathrm{A}\tilde{\mathrm{T}}\mathrm{U}, \qquad \mathrm{W} := \{E_4, s_1, s_2, s_1 s_2\}$$

工夫１：同型変換によるパラメータ数削減 (4/4)

Lemma 2.7 (Reduction for N1-case)

$\tilde{\mathrm{O}}_Q(K)$ の作用により三次形式 P は次の形に変形できる:

$$P' = (y + b_1 z)x^2 + b_2 x z^2 + a_1 y^3 + a_2 y^2 z + a_3 y z^2 + a_4 z^3 + (a_5 y^2 + a_6 yz + a_7 z^2)w + (a_8 y + a_9 z)w^2 + a_{10} w^3.$$

ここで $a_i \in K$, $b_1 \in \{0, 1, \varepsilon\}$, $b_2 \in \{0, 1\}$.

上記変形に対応する同型により $V(Q, P) \cong V(Q, P')$ over K.

(N2), (D) の場合も同様に, P は未知係数の個数 10 以下にできる！
(cf. 種数 4 曲線のモジュライの次元 $= 9$)

工夫 2 ：Hybrid 法＋ Gröbner 基底計算の適用 (1/5)

各 Q ごとに, 対応する P の未知係数をパラメータとみなせば,

超特別な C の数え上げ

$$\Longleftrightarrow \left\{ \begin{array}{l} \text{独立変数：高々10 個} \\ \text{式数：16} \\ \text{最大総次数：} p-1 \end{array} \right\} \text{の系 } A=0 \text{ の解 } /\mathbb{F}_q \text{ の計算}$$

- A : $C = V(Q, P)$ の Hasse-Witt 行列

$\longrightarrow$ **全数探索法** or **Gröbner 基底計算による消去法**？

工夫 2 ：Hybrid 法＋ Gröbner 基底計算の適用 (2/5)

全数探索法

for $a_1 \in K$ **do**
  for $a_2 \in K$ **do**
    $\vdots$
      for $a_{10} \in K$ **do**
        $A = 0$, かつ $V(Q, P)$ が非特異か確認
      end for
    $\vdots$
  end for
end for

$q = 5^2$ でも $(\#K)^{10} = q^{10} = 9765625$ (約 32 ビット) のループ
→ 実時間で停止しない...

工夫 2 ：Hybrid 法＋ Gröbner 基底計算の適用 (3/5)

Gröbner 基底 (Buchberger, 1965) の計算による消去法

- Gröbner 基底：多項式イデアルの “よい” 生成系
- 辞書式項順序に関する Gröbner 基底 (下記は一例)：

$$\begin{cases} g_1(x_1, x_2, \ldots, x_{n-1}, x_n) \\ g_2(x_2, \ldots, x_{n-1}, x_n) \\ \vdots \\ g_{n-1}(x_{n-1}, x_n) \\ g_n(x_n) \end{cases}$$

$\longrightarrow$ 1 変数多項式から順次求根すれば全体の解が求まる！

- 1 変数多項式求根 /$\mathbb{F}_q$：Bearlkamp, Cantor-Zassenhaus, etc.

工夫 2 ：Hybrid 法＋ Gröbner 基底計算の適用 (4/5)

Gröbner 基底の計算機による practical な計算

- 高速アルゴリズム： F4, F5 (signature 系), M4GB など
- 最初から所望の項順序に関して計算するのは悪手
- 当該分野では次数付き逆辞書式順序を使用するのがセオリー
- その後 FGLM 基底変換

(今回の場合)

- 計算代数システム Magma を利用
  - 組み込み関数 `GroebnerBasis` (F4 の高速実装), `Variety`
- 入力： 変数 10 個, 式数 16, 最大総次数 $p-1$ の多項式系

$\longrightarrow$ 停止しない or メモリーアウト (変数：多 & 次数：高)

工夫 2 ：Hybrid 法＋ Gröbner 基底計算の適用 (5/5)

Hybrid 法 (Bettale-Faugére-Perret, 2009)

(今回の場合)

- q^k 回のループ
- 各ループで

$$\left\{ \begin{array}{l} \text{変数：} 10-k \text{ 個} \\ \text{式数：} 16 \\ \text{最大総次数：} p-1 \end{array} \right\} \text{の}$$

  多項式系の Gröbner 基底計算
- k の最適値 ⟵ 実験的に推定

for $a_1 \in K$ **do**
  for $a_2 \in K$ **do**
    ⋮
      for $a_k \in K$ **do**
        Gröbner 基底計算
      end for
    ⋮
  end for
end for

Kudo-Harashita straregy

超特別曲線の数え上げアルゴリズム (概略)

標数 $p > 2$, 有限体 $K = \mathbb{F}_q$ を入力として以下を実行:

(1) 各二次形式 Q について, 対応する三次形式 P に対し
$V(Q, P)$ の Hasse-Witt 行列 A を計算.

- P の未知係数は独立パラメータとみなす.

(2) 代数方程式系 $A = 0$ の K における解を求める (**Hybrid 法**).

- 各解について, 対応する $V(Q, P)$ が非特異なら保存.

(3) 得られた $V(Q, P)$ たちを同型類別する.

工夫 3 ：同型判定

Lemma 2.8 (Recall)

種数 4 非超楕円曲線 $V(Q, P_1)$ と $V(Q, P_2)$ が K 上同型
$\iff \exists (M, \lambda) \in \tilde{\mathrm{O}}_Q(K) \times K^\times$ s.t. $M \cdot P_1 \equiv \lambda P_2 \pmod{Q}$.

$\tilde{\mathrm{O}}_Q(K)$ の Bruhat 分解により M の成分をパラメータで表せば,

$V(Q, P_1)$ と $V(Q, P_2)$ の同型判定
$\iff M \cdot P_1 \equiv \lambda P_2$ から得られる方程式系が解 $/K$ をもつかの判定

$\longrightarrow$ 系に対応するイデアルの簡約 Gröbner 基底が $\{1\}$ か否か.
$\longrightarrow$ 計算機上で判定可能.

計算結果 (1/2)

$g = 4$ に対してアルゴリズムを Magma に実装・実行し次を得た.
(総計算時間：一週間程度)

Theorem 2.9 (K. and Harashita '17 & '20)

$p \leq 11$ において, 種数 4 非超楕円曲線 $/\mathbb{F}_q$ のうち超特別なものの同型類の個数は下表の通り (太字箇所が新しい結果):

p	≤ 3		5		7		11	
q	p	p^2	5	5^2	7	7^2	11	11^2
$\mathbb{F}_q$ 同型類	0		**7**	**21**	**0**		**30**	?
$\overline{\mathbb{F}_q}$ 同型類	0		1		**0**		**9**	?

定義方程式も得たがここでは割愛 (一部を次頁で紹介).

計算結果 (2/2)

Theorem 2.10 (K. and Harashita '17, Theorem A)

種数 4 超特別曲線 /$\mathbb{F}_{5^2}$ は $\mathbb{P}^3$ 内の完全交叉

$$2yw + z^2 = 0, \quad x^3 + a_1y^3 + a_2w^3 + a_3zw^2 = 0$$

に $\mathbb{F}_{5^2}$ 上で同型である. ここで $a_1, a_2 \in \mathbb{F}_{5^2}^{\times}$, $a_3 \in \mathbb{F}_{5^2}$ である.

Theorem 2.11 (K. '19, Theorem 1.2(1))

$\mathbb{P}^3$ 内の完全交叉として定まる $\mathbb{F}_p$ 上の種数 4 曲線

$$C : 2yw + z^2 = 0, \quad x^3 + y^3 + w^3 = 0$$

について, C が $\mathbb{F}_{p^2}$-最大 $\Leftrightarrow p \equiv 5 \pmod 6$.

参考文献

本節の主結果は以下の論文を参照:

- M. Kudo and S. Harashita (2018): Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields.
  In: L. Budaghyan, F. Rodriguez-Henriquez (eds), Arithmetic of Finite Fields, WAIFI 2018, Lecture Notes in Computer Science, **11321**, pp. 58–73, Springer.
- M. Kudo and S. Harashita (2022): Algorithmic study of superspecial hyperelliptic curves over finite fields.
  Commentarii Mathematici Univ. St. Pauli, to appear.

以下しばらく K : 標数 $p \geq 3$ の完全体

超楕円曲線

H : 種数 g の超楕円曲線 $/K$
i.e., $\exists \pi : H \to \mathbb{P}^1$ over K of degree 2

重根をもたない $^{\exists} f \in K[x]$ で $\deg(f) = 2g+1$ or $2g+2$ なるものが存在して，H は $y^2 = f(x)$ に双有理.

もし $\#K > 2g+1$ なら, $\deg(f) = 2g+2$ にとれる.

- H の**分岐点**：$f(x)$ の $2g+2$ 個の根
  ($\deg(f) = 2g+1$ の時は ∞ を入れる)
- **超楕円対合**：$\iota_H : (x, y) \mapsto (x, -y)$
- **簡約自己同型群**：$\overline{\mathrm{Aut}}(H) := \mathrm{Aut}(H)/\langle \iota_H \rangle$

超楕円曲線の定義方程式の簡約形

$\varepsilon \in K^\times \smallsetminus (K^\times)^2$: 固定

Lemma 2.12 (K-model of hyperelliptic curves)

$\#K > 2g+1$ のとき, 種数 g の超楕円曲線 $/K$ は

$$cy^2 = x^{2g+2} + b_1 x^{2g+1} + b_2 x^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1 x + a_0$$

の斉次化の特異点解消に K 上で同型となる. ここで
$a_i \in K$, $c \in \{1, \varepsilon\}$, $b_2 \in \{0, 1, \varepsilon\}$ である. また,
$p \nmid 2g+2$ のとき $b_1 = 0$,
$p \mid 2g+2$ のとき $b_1 \in \{0, 1\}$ である.

未知係数 : $a_0, \ldots, a_{2g-1}$ ($2g$ 個), b_1, b_2, c
(cf. 種数 g 超楕円曲線のモジュライの次元 $= 2g-1$)

超楕円曲線の Cartier-Manin 行列 (1/3)

Fact 2.13 (Yui '78)

超楕円曲線 $H : y^2 = f(x)$ の Cartier-Manin 行列 B は $(c_{pi-j})_{i,j}$ で与えられる. ここで c_k は $f^{(p-1)/2}$ における x^k の係数である.

- $k(C)$: C の関数体, i.e., $k[x, y]/\langle y^2 - f(x)\rangle$ の商体
- $\omega \in H^0(C, \Omega^1_C)$: 正則微分形式
  $\longrightarrow \omega = d\phi + \eta^p x^{p-1} dx$ $(\exists! \phi, \eta \in k(C))$
- **Cartier-Manin 行列** : Cartier 作用

$$\mathscr{C} : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C) \ ; \ \omega \mapsto \eta dx$$

の表現行列 (転置+各成分 p 乗したものが Hasse-Witt 行列).

超楕円曲線の Cartier-Manin 行列 (2/3)

前頁の Fact の証明

$$H^0(C, \Omega^1_C) = \left\langle \omega_j := \frac{x^{j-1}}{y} dx : 1 \leq j \leq g \right\rangle$$

であり, $k(C)$ において $y^{p-1} = f(x)^{(p-1)/2}$ だから

$$\begin{aligned} \omega_j &= y^{-p} f(x)^{(p-1)/2} x^{j-1} dx \\ &= d\left(y^{-p} \sum_{\substack{k \\ j+k \neq 0 \pmod p}} \frac{c_k}{j+k} x^{j+k} \right) + \sum_{i \geq 1} c_{ip-j} \frac{x^{(i-1)p}}{y^p} x^{p-1} dx. \end{aligned}$$

従って $\mathscr{C}(\omega_j) = \sum_{i=1}^{g} c_{ip-j}^{1/p} \omega_i$. □

超楕円曲線の Cartier-Manin 行列 (3/3)

Fact 2.14 (Yui '78)

超楕円曲線 $H : y^2 = f(x)$ の Cartier-Manin 行列 B は $(c_{pi-j})_{i,j}$ で与えられる. ここで c_k は $f^{(p-1)/2}$ における x^k の係数である.

Lemma 2.12 の f の未知係数を独立パラメータとみなせば,

超特別な H の数え上げ

$$\Longleftrightarrow \left\{ \begin{array}{l} \text{独立変数：} 2g \text{ 個} \\ \text{式数：} g^2 \\ \text{最大総次数：} \frac{p-1}{2} \end{array} \right\} \text{の方程式系 } B = 0 \text{ の解 } /\mathbb{F}_q \text{ の計算}$$

$\longrightarrow$ 種数 4 非超楕円の場合と同様に, Hybrid 法を適用する！

Kudo-Harashita straregy for hyperelliptic curves

超特別曲線の数え上げアルゴリズム (概略)

種数 g, 標数 $p > 2g+1$, 有限体 $K = \mathbb{F}_q$ を入力として以下を実行:

(1) 超楕円曲線

$$cy^2 = x^{2g+2} + b_1 x^{2g+1} + b_2 x^{2g} + a_{2g-1} x^{2g-1} + \cdots + a_1 x + a_0$$

の Cartier-Manin 行列 B を計算.

- 未知係数は独立パラメータとみなす.

(2) 方程式系 $B = 0$ の K における解を求める.

- 各解について, 対応する $f(x)$ が重根をもたないなら保存.

(3) 得られた $cy^2 = f(x)$ たちを同型類別する.

超楕円曲線の同型判定 (1/2)

- H_i : 種数 g の超楕円曲線 $y^2 = f_i(x)$ $(i = 1, 2)$
- $F_i(x, z) := z^{2g+2} f_i(x/z)$: $f_i(x)$ の z による斉次化
- $\mathrm{Isom}_K(H_1, H_2)$: K 上の同型写像 $H_1 \to H_2$ の全体
- $G_K(f_1, f_2) := \{(h, \lambda) \in \mathrm{GL}_2(K) \times K^\times : h \cdot F_2 = \lambda^2 F_1\}$

このとき

$$\begin{array}{ccc} \mathrm{Isom}_K(H_1, H_2) & \longleftrightarrow & G_K(f_1, f_2)/\equiv \\ \left[(x, y) \mapsto \left(\dfrac{\alpha x + \beta}{\gamma x + \delta}, \dfrac{\lambda y}{(\gamma x + \delta)^{g+1}}\right)\right] & \longleftrightarrow & \left(h = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \lambda\right) \end{array}$$

ここで $(h, \lambda) \in G_K(f_1, f_2)$ と $\mu \in K^\times$ に対し,
$(h, \lambda) \equiv (\mu h, \mu^{g+1}\lambda)$ と定める.

超楕円曲線の同型判定 (2/2)

Lemma 2.15 (K-isomorphims)

H_1 と H_2 が K 上同型
$\iff \exists (h, \lambda) \in \mathrm{GL}_2(K) \times K^\times$ s.t. $h \cdot F_2 = \lambda^2 F_1$.

H_1, H_2 の同型判定

$\iff h \cdot F_2 = \lambda^2 F_1$ から得られる方程式系が解 $/K$ をもつかの判定

$\longrightarrow$ 系に対応するイデアルの簡約 Gröbner 基底が $\{1\}$ か否か.
$\longrightarrow$ 計算機上で判定可能.

計算結果 (1/2)

$g = 4$ に対してアルゴリズムを Magma に実装・実行し次を得た.
(総計算時間 : 一日足らず)

Theorem 2.16 (K. and Harashita '18 & '22)

$p \leq 23$ において, 種数 4 超楕円曲線 $/\mathbb{F}_q$ のうち超特別なものの同型類の個数は下表の通り:

p	≤ 13		17		19		23	
q	p	p^2	17	17^2	19	19^2	23	23^2
$\mathbb{F}_q$ 同型類	**0**		**5**	**25**	**12**	**18**	**14**	?
$\overline{\mathbb{F}_q}$ 同型類	**0**		**2**		**2**		**4**	?

注 : $p \leq 7$ での非存在は Ekedahl bound から従う.
定義方程式も得たがここでは割愛 (一部を次頁で紹介).

計算結果 (2/2)

$p = 17, 19, 23$ における種数 4 超特別超楕円曲線 $/\mathbb{F}_p$ の $\overline{\mathbb{F}_p}$ 同型類:

p	Equation of H representing an isomorphism class	$\overline{\mathrm{Aut}}(H)$	$\mathrm{Aut}(H)$
17	$y^2 = x^{10} + x$	$\mathbb{Z}_9$	$\mathbb{Z}_{18}$
	$y^2 = x^{10} + x^7 + 13x^4 + 12x$	A_4	$\mathrm{SL}_2(\mathbb{F}_3)$
19	$y^2 = x^{10} + 1$	D_{10}	$\mathbb{Z}_5 \rtimes D_4$
	$y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$	V_4	D_4
23	$y^2 = x^{10} + x^7 + 3x^4 + 10x$	$\mathbb{Z}_3$	$\mathbb{Z}_6$
	$y^2 = x^{10} + x^7 + 18x^4 + 6x$	A_4	$\mathrm{SL}_2(\mathbb{F}_3)$
	$y^2 = x^{10} + x^7 + 5x^6 + 3x^5 + 21x^4 + 3x^3 + 9x^2 + 4x + 21$	V_4	D_4
	$y^2 = x^{10} + x^7 + 9x^6 + 11x^5 + 19x^4 + 10x^3 + 16x^2 + 8x + 21$	$\mathbb{Z}_2$	V_4

$\mathbb{Z}_n$: 位数 n の巡回群, D_n : 位数 $2n$ の二面体群

A_n : 位数 $n!/2$ の交代群, V_4 : Klein 四元群 $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$p > 23$ でも $\mathrm{Aut}(H) \supset \mathbb{Z}_6$ or $\mathrm{Aut}(H) \supset V_4$ なる超特別 H がある？

参考文献

本節の主結果は以下の論文を参照:

- M. Kudo and S. Harashita (2022): Superspecial trigonal curves of genus 5.
  Experimental Mathematics, **31**, Issue 3, 908–919.
- M. Kudo (2019): On the existence of superspecial and maximal nonhyperelliptic curves of genera four and five.
  Communications in Algebra, **47**, Issue 12, 5020–5038.

以下しばらく K : 標数 $p \geq 5$ の有限体 or 代数閉体

種数5の曲線

Definition 2.17

曲線 C が d-gonal $\Longleftrightarrow \exists \pi : C \to \mathbb{P}^1$; 次数 d の射

種数 5 曲線のタイプ		実現法	モジュライの次元
超楕円		$y^2 = f(x)$	9
非超楕円	Trigonal	特異平面 5 次曲線	11
	Non-trigonal	$\mathbb{P}^4$ 内の二次曲面 3 つの完全交叉	12

[K. and Harashita '20] : トリゴナルの場合に着目

種数5トリゴナル曲線の定義方程式

K : 標数 $p \geq 5$ の有限体 or 代数閉体
$\varepsilon \in K^\times \setminus (K^\times)^2$: 平方非剰余元を固定
T : 種数 5 トリゴナル曲線 $/K$

Lemma 2.18

次を満たす特異五次曲線 $V(F) \subset \mathbb{P}^2$ が存在する.

- T は $V(F)$ の特異点解消に K 上同型.
- $V(F)$ は $[0:0:1]$ を唯一の特異点 (重複度 2) にもつ.

- $[0:0:1]$: node $\Longrightarrow F = xyz^3 + f$ or $F = (x^2 - \varepsilon y^2)z^3 + f$
- $[0:0:1]$: cusp $\Longrightarrow F = x^2z^3 + f$

f : z の次数 ≤ 2 の五次形式

種数5トリゴナル曲線の定義方程式の簡約形

Lemma 2.19 (Reduction for Cusp-case)

$p \geq 5$ のとき, 種数 5 トリゴナル曲線は

$$x^2z^3 + a_1y^3z^2 + (a_2x^4 + a_3x^3y + a_4x^2y^2 + b_1xy^3 + a_5y^4)z$$
$$+a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + b_2xy^4 + a_{10}y^5 = 0$$

の特異点解消に K 上で同型となる. ここで
$a_i \in K$, $a_1 \neq 0$, $b_1, b_2 \in \{0, 1\}$ である.

未知係数 : $a_1, \ldots, a_{10}$ (10 個), b_1, b_2

Node-case の場合も同様に, F は未知係数の個数 11 以下にできる！
(cf. 種数 5 トリゴナル曲線のモジュライの次元 $= 2g + 1 = 11$)

種数5 トリゴナル曲線の Hasse-Witt 行列

Proposition 2.20

T の Hasse-Witt 行列 A の 25 個の成分は

$$F^{p-1} \text{ の } x^{ip-i'} y^{jp-j'} z^{kp-k'} \text{ の係数}$$

である. ただし
$(i,j,k),(i',j',k') = (3,1,1),(1,3,1),(2,2,1),(2,1,2),(1,2,2).$

よって, F の未知係数をパラメータとみなせば,

超特別な T の数え上げ $\Longleftrightarrow$ 25 個の式からなる系 $A = 0$ の求解

$\longrightarrow$ 種数 4 の場合と同様に, Hybrid 法を適用する！

同型判定

T_i : 種数 5 トリゴナル曲線
$V(F_i)$: T_i の特異平面 5 次曲線モデル

Lemma 2.21

T_1 と T_2 が K 上同型
$\iff \exists \sigma \in \mathrm{Aut}_K(\mathbb{P}^2)$ s.t. $\sigma(V(F_1)) = V(F_2)$
$\iff \exists (M, \lambda) \in \mathrm{GL}_2(K) \times K^\times$ s.t. $M \cdot F_2 = \lambda F_1$

M の成分をパラメータで表せば,

T_1 と T_2 の同型判定
$\iff M \cdot F_2 = \lambda F_1$ から得られる方程式系が解 $/K$ をもつかの判定

$\longrightarrow$ 系に対応するイデアルの簡約 Gröbner 基底が $\{1\}$ か否か.
$\longrightarrow$ 計算機上で判定可能.

計算結果 (1/2)

数え上げアルゴリズムを Magma に実装・実行し次を得た.
(総計算時間：四日余り)

Theorem 2.22 (K. and Harashita '22)

$p \leq 13$ において, 種数 5 トリゴナル曲線 $/\mathbb{F}_q$ のうち超特別なものの同型類の個数は下表の通り (太字箇所が新しい結果):

p	≤ 5		7		11		13	
q	p	p^2	7	7^2	11	11^2	13	13^2
$\mathbb{F}_q$ 同型類	0		**0**		**4**	?	**0**	?
$\overline{\mathbb{F}_q}$ 同型類	0		**0**		**1**	?	**0**	?

定義方程式も得たがここでは割愛 (一部を次頁で紹介).

計算結果 (2/2)

$p = 11$ における種数 5 超特別トリゴナル曲線 $/\mathbb{F}_p$ の $\mathbb{F}_p$ 同型類:

種数 5 トリゴナル曲線 T の定義式 F	$\mathrm{Aut}_{\mathbb{F}_p}(T)$	$\mathrm{Aut}(T)$	$\overline{\mathrm{Aut}}(T)$
$xyz^3 + x^5 + y^5$	D_5	$\mathbb{Z}_3 \times D_5$	D_5
$xyz^3 + 2x^5 + y^5$	$\mathbb{Z}_5$		
$xyz^3 + 3x^5 + y^5$	$\mathbb{Z}_5$		
$(x^2 - 2y^2)z^3 + x^5 + 9x^3y^2 + 9xy^4$	$\mathbb{Z}_2$		

$\overline{\mathrm{Aut}}(T)$: $\mathrm{Aut}(T)$ の $\exists$ 位数 3 の群による剰余群

Theorem 2.23 (K. '19, Theorem 1.2(2))

$\mathbb{F}_p$ 上の種数 5 トリゴナル曲線 $T : xyz^3 + x^5 + y^5 = 0$ について,
T が $\mathbb{F}_{p^2}$-最大 $\iff p \equiv -1$ or $11 \pmod{15}$.

補足：自己同型群の計算

T：種数 5 トリゴナル曲線
$V(F)$：T の特異平面 5 次曲線モデル

Lemma 2.24

$\mathrm{Aut}_K(T) \cong \{M \in \mathrm{PGL}_3(K) : M \cdot F = \lambda F \text{ for some } \lambda \in K^\times\}$.

M の成分をパラメータで表せば,

$\mathrm{Aut}_K(T)$ の元の計算
$\Longleftrightarrow$ $M \cdot F = \lambda F$ から得られる方程式系の求解 $/K$

$\longrightarrow$ 系に対応するイデアルの Gröbner 基底を求めればよい.
$\longrightarrow$ 計算機上で計算可能.

1. Introduction

2. 数え上げ (同型類列挙)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 5 トリゴナル (時間があれば)

3. 大きい標数での存在性 (自己同型群で絞った高速探索)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 3 非超楕円・超楕円 (時間があれば)

4. まとめと今後の課題

本節のモチベーション

ここまでの内容

種数 $4, 5$ 超特別曲線の計算機による全数え上げ

$$\to \left\{ \begin{array}{l} \text{モジュライ次元} + \epsilon \text{ 個の変数} \\ \text{式数 } g^2 \\ \text{最大総次数 } O(p) \end{array} \right\} \text{の代数方程式系 } /\mathbb{F}_{p^2} \text{ の求解}$$

$\longrightarrow$ p の指数時間計算量 ($p \leq 23$ くらいが関の山)

より大きい任意 p での存在を調べたい！

$\longrightarrow$ 自己同型群による絞り込み (**ここからの内容**)

参考文献

本節の主結果は以下の論文を参照:

- M. Kudo, S. Harashita and E. W. Howe (2020):
  Algorithms to enumerate superspecial Howe curves of genus four.
  Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), Open Book Series **4**, 301–316.

以下しばらく k : 標数 $p \geq 5$ の代数閉体

Howe 曲線

Definition 3.1 (Howe '15 & K., Harashita and Senda '20)

分岐点を唯一共有する種数 1 曲線 E_1, E_2 に対し, $E_1 \times_{\mathbb{P}^1} E_2$ の特異点解消に同型な種数 4 曲線 H を Howe 曲線という.

[Howe '15] : H は有理点を多く持ちやすい ($\mathbb{F}_q$ 最大となりうる)

Proposition 3.2 (K., Harashita and Howe '20)

Howe 曲線 H は非超楕円的であり, $\mathrm{Aut}(H) \supset V_4 := \mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition 3.3 (Katsura-Takashima '21)

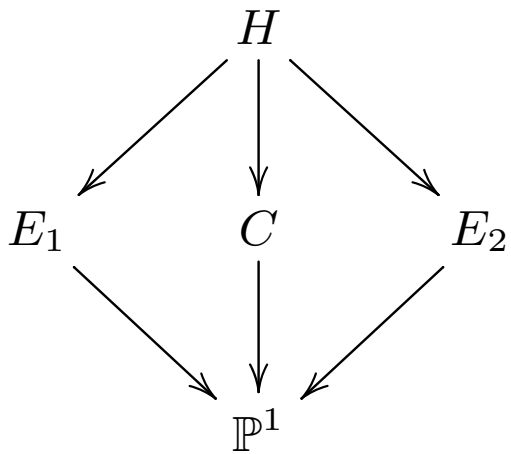
一般に, 二つの超楕円曲線 C_1, C_2 のファイバー積 $C_1 \times_{\mathbb{P}^1} C_2$ の特異点解消に同型な曲線を一般化 Howe 曲線という.

Howe 曲線の超特異性・超特別性

$E_i : y^2 = (x-a)f_i(x)$: 分岐点を唯一共有する種数 1 曲線
$(a \in k \cup \{\infty\},\ f_i$ は 3 次分離で $\gcd(f_1, f_2) = 1$ かつ $f_i(a) \neq 0)$

$C : y^2 = f_1(x)f_2(x)$ (種数 2 曲線)

- $\mathrm{Jac}(H) \sim E_1 \times E_2 \times \mathrm{Jac}(C)$
- $\mathrm{Jac}(H)[p] \cong E_1[p] \times E_2[p] \times \mathrm{Jac}(C)[p]$



H : 超特別 (resp. 超特異)
$\iff E_1, E_2, C$: 超特別 (resp. 超特異)

Proposition 3.4 (K., Harashita and Senda '20)

任意の $p > 3$ に対し種数 4 超特異 Howe 曲線が存在する.

$\longrightarrow$ 超特別なものもあるかも？

Howe 曲線の同型, 提案アルゴリズム

H, H' : Howe 曲線
C, C' : 対応する種数 2 曲線

Theorem 3.5 (K., Harashita and Howe '20)

$H \cong H' \Longrightarrow C \cong C'$.

提案アルゴリズム (超特別 Howe 曲線の数え上げ) の概略

Step 1. まず種数 2 超特別曲線の同型類 C を列挙
Step 2. 各 C に対し次を実行
(2-1) C の分岐点集合を二等分割
(2-2) 考えられる (E_1, E_2) を全て構成
(2-3) (E_1, E_2) に対応する H たちを同型類別

Step 1. 種数 2 超特別曲線の全数え上げ

Definition 3.6

主偏極アーベル曲面の同種写像 $\phi : A \to A'$ が Richelot 同種写像
$\iff \mathrm{Ker}(\phi)$ が 2-Weil ペアリングに関して $A[2]$ の極大等方部分群

Theorem 3.7 (Jordan-Zaytman '20 and Florit-Smith '21)

次元 2 超特別ヤコビ多様体 $/\mathbb{F}_{p^2}$ を頂点, Richelot 同種写像を辺とするグラフは連結である.

よって, 種数 2 超特別曲線を全て求めるには

1. 種数 2 超特別曲線 H を (幾つか) 生成
2. $\mathrm{Jac}(H)$ に Richelot 同種なヤコビ多様体を全て計算

を繰り返せばよい.

種数 2 超特別曲線 H の生成

$$E_i : y^2 = f_i = c_i(x - \alpha_1^{(i)})(x - \alpha_2^{(i)})(x - \alpha_3^{(i)}) \in \mathbb{F}_{p^2}[x] \text{ [楕円曲線]}$$

$$\begin{aligned} a_1^{(i)} &:= \frac{(\alpha_3^{(i)} - \alpha_2^{(i)})^2}{\alpha_3^{(i+1)} - \alpha_2^{(i+1)}} + \frac{(\alpha_2^{(i)} - \alpha_1^{(i)})^2}{\alpha_2^{(i+1)} - \alpha_1^{(i+1)}} + \frac{(\alpha_1^{(i)} - \alpha_3^{(i)})^2}{\alpha_1^{(i+1)} - \alpha_3^{(i+1)}} \\ a_2^{(i)} &:= \alpha_1^{(i)}(\alpha_3^{(i+1)} - \alpha_2^{(i+1)}) + \alpha_2^{(i)}(\alpha_1^{(i+1)} - \alpha_3^{(i+1)}) + \alpha_3^{(i)}(\alpha_2^{(i+1)} - \alpha_1^{(i+1)}) \end{aligned}$$

Theorem 3.8 (Howe-Leprévost-Poonen '00)

上の状況で, $a_j^{(i)} \neq 0$ であり, $A_i = \Delta_{f_{i+1}} a_1^{(i)} / a_2^{(i)}$ とおくと,

$$h := -\prod_{j=1}^{3} \left(A_1(\alpha_{j+1}^{(1)} - \alpha_j^{(1)})(\alpha_j^{(1)} - \alpha_{j+2}^{(1)})x^2 + A_2(\alpha_{j+1}^{(2)} - \alpha_j^{(2)})(\alpha_j^{(2)} - \alpha_{j+2}^{(2)}) \right)$$

は $\mathbb{F}_{p^2}[x]$ の 6 次分離多項式であり, $H : y^2 = h(x)$ とすると,
$E_1 \times E_2$ は $\mathrm{Jac}(H)$ に Richelot 同種である.

$\mathrm{Jac}(H)$ に Richelot 同種なヤコビ多様体

- $H : y^2 = f(x)$: 種数 2 曲線 (必ず超楕円的になる)
- $f(x) = d\, G_1(x)G_2(x)G_3(x) \quad (d \in k^\times,\ G_j$ は 2 次)
- $g_{j,k}$: G_j の x^k の係数
- $\tilde{G}_j := \frac{dG_{j+1}}{dx} \cdot G_{j+2} - G_{j+1} \cdot \frac{dG_{j+2}}{dx}$ (ただし $G_{j+3} := G_j$).

Theorem 3.9 (Smith '05)

上の状況で, もし $\det(g_{j,k}) \neq 0$ なら, 種数 2 曲線

$$\tilde{H} : y^2 = \tilde{f}(x) := d\, \tilde{G}_1(x)\tilde{G}_2(x)\tilde{G}_3(x)$$

について, Richelot 同種写像 $\mathrm{Jac}(H) \to \mathrm{Jac}(\tilde{H})$ が存在する.
逆に $\mathrm{Jac}(H) \to \mathrm{Jac}(H')$ なる Richelot 同種写像があれば, H' は上のように構成される種数 2 曲線に同型である.

計算結果

Theorem 3.10 (K., Harashita and Howe '20)

提案アルゴリズムは $\tilde{O}(p^4)$ の計算量で種数 4 超特別 Howe 曲線の $\overline{\mathbb{F}_p}$ 同型類を全て計算する.

アルゴリズムを Magma で実装し次を得た (計算時間：680 分)：

Theorem 3.11 (K., Harashita and Howe '20)

$p \neq 7$ なる各素数 $5 \leq p \leq 20000$ に対し, 種数 4 超特別 Howe 曲線が存在する.

$p \leq 200$ で同型類の全列挙も行った
(詳細は [K., Harashita and Howe '20]).

1. Introduction
2. 数え上げ (同型類列挙)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 5 トリゴナル (時間があれば)
3. 大きい標数での存在性 (自己同型群で絞った高速探索)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 3 非超楕円・超楕円 (時間があれば)
4. まとめと今後の課題

参考文献

本節の主結果は以下の論文を参照:

- R. Ohashi, M. Kudo and S. Harashita (2022):
  Fast enumeration of superspecial hyperelliptic curves of genus 4 with automorphism group V_4.
  Proceedings of International Workshop on the Arithmetic of Finite Fields (WAIFI 2022), 16 pages, to appear.
- M. Kudo, T. Nakagawa and T. Takagi (2022):
  Efficient search for superspecial hyperelliptic curves of genus four with automorphism group containing $\mathbb{Z}_6$.
  arXiv: 2210.14822 [math.AG].

以下しばらく k : 標数 $p \geq 7$ の代数閉体

種数 4 超楕円曲線の自己同型群による分類 (1/2)

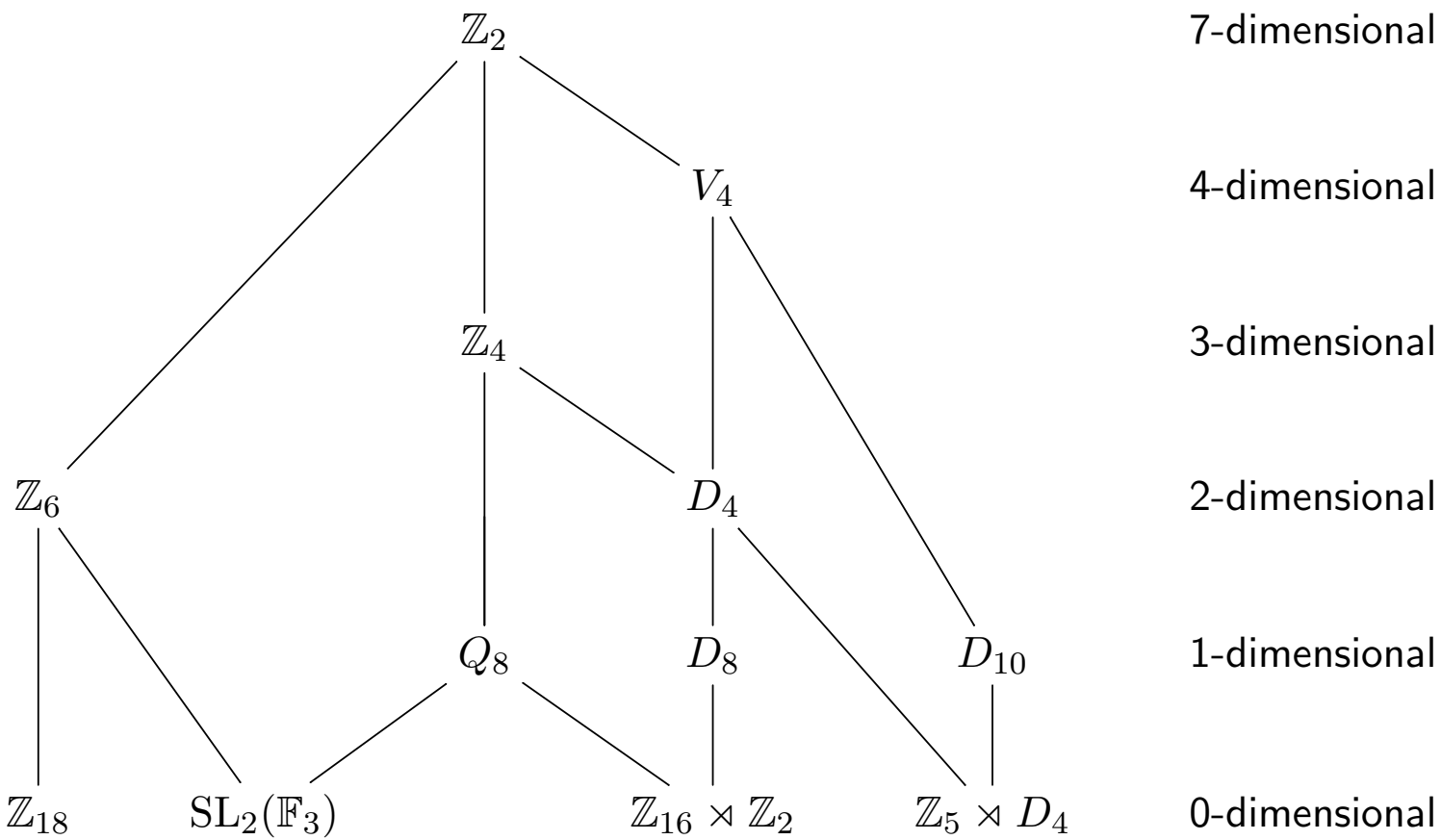
Theorem 3.12 (K., Nakagawa and Takagi '22)

$p \geq 7$ のとき, 種数 4 超楕円曲線 H $/k$ の自己同型群は以下の通り:

Type	$\overline{\mathrm{Aut}}(H)$	$\mathrm{Aut}(H)$	H の定義方程式
1	$\{0\}$	$\mathbb{Z}_2$	$y^2 =$ (次数 9 or 10 の無平方多項式/k)
2-1	$\mathbb{Z}_2$	V_4	$y^2 = x^{10} + ax^8 + bx^6 + cx^4 + dx^2 + 1$
2-2	$\mathbb{Z}_2$	$\mathbb{Z}_4$	$y^2 = x^9 + ax^7 + bx^5 + cx^3 + x$
3	$\mathbb{Z}_3$	$\mathbb{Z}_6$	$y^2 = x^{10} + ax^7 + bx^4 + x$
4-1	V_4	D_4	$y^2 = x^{10} + ax^8 + bx^6 + bx^4 + ax^2 + 1$, or $y^2 = x^9 + ax^7 + bx^5 + ax^3 + x$
4-2	V_4	Q_8	$y^2 = x(x^4 - 1)(x^4 + ax^2 + 1)$
5	D_4	D_8	$y^2 = x^9 + ax^5 + x$
6	D_5	D_{10}	$y^2 = x^{10} + ax^5 + 1$
7	A_4	$\mathrm{SL}_2(\mathbb{F}_3)$	$y^2 = x(x^4 - 1)(x^4 + 2\sqrt{-3}x^2 + 1)$
8	D_8	$\mathbb{Z}_{16} \rtimes \mathbb{Z}_2$	$y^2 = x^9 + x$
9	$\mathbb{Z}_9$	$\mathbb{Z}_{18}$	$y^2 = x^{10} + x$
10	D_{10}	$\mathbb{Z}_5 \rtimes D_4$	$y^2 = x^{10} + 1$

種数 4 超楕円曲線の自己同型群による分類 (2/2)

Figure: 種数 4 超楕円曲線の $\mathrm{Aut}(H)$ と対応するモジュライの次元の上界



種数 4 超楕円における超特別曲線の効率的探索

[Ohashi, K. and Harashita '22]
$\mathrm{Aut}(H) \supset V_4$ を満たす種数 4 超特別超楕円的 H の高速数え上げ

Lemma 3.13 (Ohashi, K. and Harashita '22 or Moriya and K. '22)

種数 g の超楕円曲線 $C\ /k$ に対し, 次は同値 :

- $\mathrm{Aut}(C) \supset V_4$.
- 分岐点を丁度 $g+1$ 個共有する種数 $g_1 := \lfloor g/2 \rfloor$, $g_2 := \lceil g/2 \rceil$ の超楕円曲線 C_1, C_2 が存在し C は $C_1 \times_{\mathbb{P}^1} C_2$ に双有理.

さらにこのとき, $\mathrm{Jac}(C)[p] \cong \mathrm{Jac}(C_1)[p] \times \mathrm{Jac}(C_2)[p]$.

Our case : $g = 4$ より $g_1 = g_2 = 2$, 共有分岐点は 5 個

超特別 H の列挙 $\longrightarrow$ 種数 2 超特別曲線 (のペア) の列挙に帰着

C_1, C_2, H の方程式

H：種数 4 超楕円曲線で $\mathrm{Aut}(H) \supset V_4$ を満たす

Lemma 3.14 (Ohashi, K. and Harashita '22)

上の状況で，H は

$$C_i : y^2 = x(x-1)(x-a_4)(x-a_5)(x-b_i) \quad \text{(Rosenhaim form)}$$

で定義される $C_1 \times_{\mathbb{P}^1} C_2$ に双有理であり

$$H : y^2 = (x^2-1)(x^2-c_2)(x^2-c_3)(x^2-c_4)(x^2-c_5)$$

となる．ここで $c_i := (a_i - b_1)/(a_i - b_2)$.

$\longrightarrow$ 種数 2 超特別曲線の各同型類から Rosenhaim form を生成し，
$0, 1, \infty$ 以外に分岐点 2 つを共有するペアを求めればよい

提案アルゴリズム (概要)

Theorem 3.15 (Ohashi, K. and Harashita '22)

下記アルゴリズムは種数 4 超特別超楕円曲線 H で $\mathrm{Aut}(H) \supset V_4$ を満たすものの同型類を全て出力し, その計算量は $\tilde{O}(p^4)$ である.

1. **種数 2 超特別曲線 $/\overline{\mathbb{F}_p}$ の同型類全てのリスト $\mathsf{SSp}_2(p)$ を生成**
2. **種数 2 超特別曲線のペアのリスト $\mathcal{L}$ を計算**
   - 各 $C \in \mathsf{SSp}_2(p)$ を Rosenhaim form

$$C_{a,b,c} : y^2 = x(x-1)(x-a)(x-b)(x-c)$$

     に同型変換する（分岐点を $0, 1, \infty$ に移す Möbius 変換）
   - ペア $\{C_{a,b,c}, C_{a',b',c'}\}$ で $\#\{a,b,c\} \cap \{a',b',c'\} = 2$ なるものを全て求める
3. **$\mathcal{L}$ の元を種数 4 超楕円曲線として同型類別し，結果を出力**

計算結果

同型類列挙：
$\mathrm{Aut}(H) = V_4$ に絞り実行 (右図)
計算時間は $\tilde{O}(p^3)$ に従う

探索：
$\mathrm{Aut}(H) \supsetneq V_4$ を許し，超特別な H を 1 つ見つけた時点で停止

Theorem 3.16

各素数 $19 \leq p \leq 7000$ に対し，種数 4 の超特別超楕円的一般化 Howe 曲線で $\mathbb{F}_{p^2}$ 上 defined なものが存在する．

p	N_p	Time (sec.)	p	N_p	Time (sec.)
17	0	0.1	103	85	1927.2
19	1	4.0	107	101	2535.4
23	0	7.0	109	99	2604.2
29	0	6.1	113	87	2595.8
31	5	35.2	127	186	5114.2
37	4	38.4	131	159	4805.0
41	7	63.5	137	135	6882.4
43	8	75.2	139	154	7907.9
47	14	145.8	149	189	11821.1
53	13	148.9	151	294	15865.3
59	17	183.8	157	203	20647.5
61	15	576.2	173	306	32910.1
67	16	178.0	167	386	47790.8
71	61	576.2	173	306	32910.1
73	38	397.0	179	321	47790.8
79	63	662.3	181	263	61735.1
83	62	675.3	191	501	104923.2
89	60	751.7	193	289	64025.0
97	70	1029.5	197	344	82069.3
101	93	1411.7	199	556	96996.3

EV: Magma V2.25-3, Windows 10 Pro OS, 1.80GHz CPU, Intel Core i7, 16GB

補足：$\mathrm{Aut}(H) \supset \mathbb{Z}_6$ の場合の計算結果

種数 4 超楕円曲線の自己同型群 $\supsetneq \mathbb{Z}_2$

1. $\mathrm{Aut}(H) \supset V_4 \longleftarrow$ [Ohashi-K.-Harashita '22]
2. $\mathrm{Aut}(H) \supset \mathbb{Z}_4$
3. $\mathrm{Aut}(H) \supset \mathbb{Z}_6 \longleftarrow$ [K.-Nakagawa-Takagi '22]

Theorem 3.17 (K. Nakagawa and Takagi '22)

各素数 $17 \leq p \leq 1000$ で $p \equiv 5 \pmod 6$ を満たすものに対し, 種数 4 超特別超楕円曲線で $\mathrm{Aut}(H) \supset \mathbb{Z}_6$ を満たすものが存在する.

(計算の概略) Magma 上で以下を実行: 各 p に対し,

$$H_{a,b} : y^2 = x^{10} + x^7 + ax^4 + bx \quad (a, b \text{ はパラメータ})$$

の Cartier-Manin 行列を計算し, 2 変数方程式系を解く.

1. Introduction
2. 数え上げ (同型類列挙)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 5 トリゴナル (時間があれば)
3. 大きい標数での存在性 (自己同型群で絞った高速探索)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 3 非超楕円・超楕円 (時間があれば)
4. まとめと今後の課題

参考文献

本節の主結果は以下の論文を参照:

- T. Moriya and M. Kudo (2022):
  Some explicit arithmetics on curves of genus three and their applications.
  arXiv: 2209.02926 [math.AG].

以下しばらく k : 標数 $p \geq 3$ の代数閉体

種数 3 の一般化 Howe 曲線

種数 3 の一般化 Howe 曲線 H は次のいずれか：

超楕円的のとき：$E \times_{\mathbb{P}^1} C$ with

- $\mathrm{Jac}(H)[p] \cong E[p] \times \mathrm{Jac}(C)[p]$
- E と C は分岐点を丁度 4 つ共有する種数 1, 2 の曲線

非超楕円的のとき $E_1 \times_{\mathbb{P}^1} E_2$ with

- $\mathrm{Jac}(H)[p] \cong E_1[p] \times E_2[p] \times E_3[p]$
- E_i と E_j は分岐点を丁度 2 つ共有する種数 1 曲線

超特別 H の列挙 $\longrightarrow$ 種数 1 または 2 の超特別曲線の列挙に帰着

問題は, 得られた H たちをどのように同型類別するか？
$\longrightarrow$ H の明示的な方程式がほしい！

超楕円的種数 3 一般化 Howe 曲線

E, C : 分岐点を丁度 4 つ共有する種数 1 曲線
H : ファイバー積 $E \times_{\mathbb{P}^1} C$ の特異点解消

適当な Möbius 変換 ($\mathbb{P}^1$ の自己同型) をほどこすことで

- $E : y^2 = (x-1)(x-a)(x-b)(x-c)$
- $C : y^2 = x(x-1)(x-a)(x-b)(x-c)$

と仮定してよい.

Lemma 3.18

H は $y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)(x^2-c^2)$ に同型.

非超楕円的種数 3 一般化 Howe 曲線

E_1, E_2 : 分岐点を丁度 2 つ共有する種数 1 曲線
H : ファイバー積 $E_1 \times_{\mathbb{P}^1} E_2$ の特異点解消

E_1, E_2 の共有分岐点を $\infty, 0,$ その他 1 つを 1 に移す Möbius 変換 ($\mathbb{P}^1$ の自己同型) をほどこすことで

$$E_1 : y^2 = x(x-1)(x-\nu), \quad E_2 : y^2 = x(x-\mu)(x-\mu\lambda).$$

と仮定してよい.

Proposition 3.19 (Oort '91)

$\nu = \mu^2\lambda \iff H$ は超楕円的

(B) の種数 3 一般化 Howe 曲線の定義方程式

- $E_1 \colon y^2 = x(x-1)(x-\nu), \quad E_2 \colon y^2 = x(x-\mu)(x-\mu\lambda)$
- H：ファイバー積 $E_1 \times_{\mathbb{P}^1} E_2$ の特異点解消

Theorem 3.20 (Moriya and K. '22)

1. $\nu = \mu^2\lambda$ (H：超楕円的) のとき

$$H : y^2 = \prod_{i,j\in\{0,1\}} \left(x^2 - \frac{((-1)^i + \sqrt{\mu})^2((-1)^{i+j} + \sqrt{\mu\lambda})^2}{(1-\mu\lambda)(1-\mu)} \right).$$

2. $\nu \neq \mu^2\lambda$ (H：非超楕円的) のとき

$$\begin{aligned} H : \mu^2\lambda(x^2+\nu+1)^2 + \nu(y^2+\mu(1+\lambda))^2 + (\mu^2\lambda-\nu)^2 \\ -(\mu^2\lambda+\nu)(x^2+\nu+1)(y^2+\mu(1+\lambda)) = 0. \end{aligned}$$

注：種数 3 非超楕円曲線は非特異四次曲線 $\subset \mathbb{P}^2 = \mathrm{Proj}(\overline{K}[x,y,z])$

アルゴリズム

Theorem 3.21

種数 3 超楕円 Howe 曲線 $E \times_{\mathbb{P}^1} C$ のうち超特別なものを全て数え上げるアルゴリズムが存在し, その計算量は $\tilde{O}(p^3)$ である.

Theorem 3.22

種数 3 非超楕円 Howe 曲線 $E_1 \times_{\mathbb{P}^1} E_2$ のうち超特別なものを全て数え上げるアルゴリズムが存在し, その計算量は $\tilde{O}(p^4)$ である.

得られる Howe 曲線の同型類別
$\longrightarrow$ 超楕円曲線 or 平面 4 次曲線としての同型判定

計算結果

Theorem 3.23

$2, 3, 5, 13$ を除く全ての $p \leq 200$ で種数 3 超楕円曲線で超特別かつ $\mathrm{Aut}(H) \supset V_4$ を満たすものが存在する. このうち $p \equiv 3 \pmod 4$ では $\mathbb{F}_p$ 上定義され $\mathbb{F}_{p^2}$ 最大となるものがある.

Cf. [Oort '91] : $\forall p \equiv 3 \pmod 4$ で上のような H は存在
$\longrightarrow \forall p \equiv 1 \pmod 4$ でも存在するかも？

Theorem 3.24

$11 \leq \forall p \leq 20000$ に対し, 種数 3 非超楕円曲線で超特別かつ $\mathrm{Aut}(H) \supset V_4$ を満たすものが存在する. このうち $p \equiv 3 \pmod 4$ では $\mathbb{F}_p$ 上定義され $\mathbb{F}_{p^2}$ 最大となるものがある.

補足：素体上 defined な超特別曲線の存在

Theorem 3.25 (Ibukiyama '93)

任意の $p \geq 3$ に対し, 種数 3 曲線 H /$\mathbb{F}_p$ で $\mathbb{F}_{p^{2e}}$ 最大 (resp. $\mathbb{F}_{p^{2e}}$ 最小) なものが存在する. ここで e は奇数 (resp. 偶数).

※ 各 p での $\mathbb{F}_{p^2}$ 最大な H が超楕円的か否かは一般には不明
$\longrightarrow$ 我々の計算結果から $p \equiv 3 \pmod 4$ では両方存在し,
$\mathrm{Aut}(H) \supset V_4$ を満たすようにとれると期待

Question

$p \equiv 1 \pmod 4$ では H は超楕円的 or 非超楕円的？

1. Introduction

2. 数え上げ (同型類列挙)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 5 トリゴナル (時間があれば)

3. 大きい標数での存在性 (自己同型群で絞った高速探索)
   - 種数 4 非超楕円
   - 種数 4 超楕円
   - 種数 3 非超楕円・超楕円 (時間があれば)

4. まとめと今後の課題

まとめと今後の課題 (1/2)

扱った問題：

Problem (cf. Ekedahl '87)

与えられた (p, g) に対し，種数 g の超特別曲線 $/\overline{\mathbb{F}_p}$ は存在するか？存在する場合，同型類を全て求めよ．

先行研究：

種数 ≤ 3：任意 p に対する $\overline{\mathbb{F}_p}$ 同型類の個数が理論的に決定済み

Deuring, Igusa, Serre, Ibukiyama, Katsura, Oort, ...

まとめと今後の課題 (2/2)

本研究成果：

$g = 4, 5$ における超特別曲線の (非) 存在, 計算機による数え上げ

$\longrightarrow$ 代数曲線論 + 計算代数幾何の技法 + 計算機代数システム

今後の課題：

- $g = 4$ での存在・非存在の理論的証明
- $g = 5$ での高速探索 (一般化 Howe 曲線)
- $g = 3$ での精密化
  - 定義体・(非) 超楕円性, 自己同型群ごとの数え上げ

補足 (1/3)

講演中に指摘や質問があったことについて補足します.
(1) $\mathbb{F}_q$ 最大性・最小性と超特別性の関係について
$\longrightarrow$ 一般的に言えるのは以下です. $C : \mathbb{F}_q$ $(p > 2)$ 上の曲線のとき

Theorem 1 (Rück-Stichtenoth '94)

1. C が $\mathbb{F}_q$ 最大なら, 任意の偶数 *(resp.* 奇数*)* 次拡大体 $\mathbb{F}_{q^e}$ 上で最小 *(resp.* 最大*)*.
2. C が $\mathbb{F}_q$ 最小なら, 任意の有限次拡大体 $\mathbb{F}_{q^e}$ 上でも最小.

Theorem 2 (Ekedahl '87 or Kazemifard-Naghipour-Tafazolian '13)

以下は同値:

- C は $\mathbb{F}_{p^2}$ 上最大または最小な曲線 $/\mathbb{F}_{p^2}$ に閉体上で同型.
- C は超特別曲線.

補足 (2/3)

$\mathbb{F}_{p^{2e}}$ 上 ($e \geq 2$) 上最大または最小であっても, 一般には超特別とは言えないようです (私の知る限り). 特定の曲線や, ある条件下では成り立つような先行結果があるかもしれません.
一方, 超特異性については次が成り立ちます:

Theorem 3 (Stichenoth-Xing '95 and Tafazolian '08)

有限体 K 上の曲線 C に対し以下は同値:

- C は K のある有限次拡大体上で最小曲線.
- C は超特異曲線.

(2) p. 19–21 の体 K : Bruhat 分解や種数 4 曲線の同型に関する主張は標数 $p > 2$ であれば任意の体で OK です. p. 18 で有限体としたのは Q を 3 つに絞るためで, Q をそのいずれかに固定してしまった後の上記議論は K は有限体でなくても成り立つ話です.

補足 (3/3)

(3) 超特別曲線の探索では自己同型群が小さいものに絞る方がよい？

$\longrightarrow$ 小さい／大きいがどれくらいの位数を指すかによりますが, 私の経験・感覚的にはそう思います. 自己同型群が小さいとモジュライも大きくなるので超特別曲線がある可能性が高いのはもちろんそうで, しかし計算量的にはきつくなります. 自己同型群が自明なものまで絞ってしまうと結局全数え上げに近くなるので, 今回扱った V_4 のように自己同型群が “少し” 大きいところを探るのは有効だと思います.

自己同型群が巨大な例として Hermitian 曲線 $y^p + y = x^{p+1}$ があり, これは $\mathbb{F}_{p^2}$ 最大曲線 (よって超特別) ですが, $g = p(p-1)/2$ を満たす必要があります. 他にもあるかもしれませんが, 大概 p に制約がつく気がします.