Algorithms to enumerate superspecial Howe curves of genus 4

◎ Momonari Kudo[1]

Shushi Harashita[2]

Everett Howe[3]

[1]The University of Tokyo

[2]Yokohama National University

[3]Unaffiliated Mathematician

June 26th 2020

Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)

Superspecial/Supersingular curves

Definition of superspecial/supersingular curves

- K : an algebraically closed field of characteristic $p > 0$

Definition C : a non-singular curve of genus g over K

- C is *superspecial (ssp.)* $\Leftrightarrow \mathrm{Jac}(C) \cong E^g$ (**ISOMORPHIC**) over K
- C is *supersingular (ssg.)* $\Leftrightarrow \mathrm{Jac}(C) \sim E^g$ (**ISOGENOUS**) over K
  - $\exists E$: ssg. elliptic curve

Applications to cryptography and coding theory

- Algebraic geometric codes
  - Ssp./ssg. curves tend to have *many rational points* w.r.t. (g, p) over finite fields.
- Isogeny-based cryptography (genus 1 or 2) e.g.
  - [Castryck-Decru-Smith], or Katsura-Takashima's work

[Castryck-Decru-Smith] *Hash functions from superspecial genus-2 curves using Richelot isogenies*, Proceedings of Number-Theoretic Methods in Cryptology 2019 (NutMiC 2019), arXiv: 1903.06451 [cs.CR], 2019.

(Non-)Existence and enumeration of ssp. curves

The finiteness of the number of ssp. curves

Fact; case of principally polarized abelian varieties (PPAV)

Fixed (g, p), the num. of ssp. PPAVs of dim g over $\overline{\mathbb{F}_p}$ is finite $\neq 0$

- In particular, the num. of isomorphism classes of ssp. curves of genus g over $\overline{\mathbb{F}_p}$ is finite (if such a curve exists)

The main problems of this work

Problems

- Given g and p, does there exist a ssp./ssg. curve of genus g in char. p?
- If a ssp. curve exists, count the num. of isom. classes.

[Pries] *Current results on newton polygons of curves*, Chapter 6, Questions in Arithmetic Algebraic Geometry, Advanced Lectures in Mathematics Book Series.

- This work focuses mainly on *ssp. case*.

Related works (1/2)

- Ekedahl's bound

Thm. (Ekedahl, 1987) $\exists\, X/\overline{\mathbb{F}_p}$: ssp. curve of genus $g \Longrightarrow 2g \leq p^2 - p$

[Ekedahl] *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), pp. 151-178.

- Case of $g \leq 3$: There exists a ssp. curve in *every* char. $p > 3$.
  - In fact, the num. of isom. classes is determined by

$(g = 1)$: Deuring 1941

$(g = 2)$: Ibukiyama-Katsura-Oort 1986

$(g = 3)$: Brock 1993

[Deuring] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941), 197-272.
[Ibukiyama-Katsura-Oort] *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no.2, 127-152, MR 827350.
[Brock] *Superspecial curves of genera two and three*, Ph.D. thesis, Princeton University, 1993, MR 2689446

Related works (2/2)

- The next target: $g = 4$

The (non-)existence of a ssp. curve in *general* p is an open problem!

- Some results for *specific small* p are known, e.g.,
  - $(p \leq 3)$: Non-existence by Ekedahl 1987
  - $(p = 5)$: $\exists!$ Isom. class over $\overline{\mathbb{F}_p}$ by Fuhrmann-Garcia-Torres 1997
  - $(p = 7)$: Non-existence by [K. – H. 2017]
  - ➢ Also see [K. – H. 2018] for the hyperelliptic case with $p \leq 23$

[K. – H. 2017], *Superspecial curves of genus 4 in small characteristic*, Finite Fields and Their Applications, **45**, 131-169, 2017.
[K. – H. 2018] *Algorithmic study of superspecial hyperelliptic curves over finite fields*, 2019, arXiv:1907.00894 [math.AG]

- This work aims to obtain results for *much larger* p by:
  - Focusing on *Howe curves* (defined in the next slide) with *algorithmic approaches*

Howe curves (1/2)

Definition of Howe curves

Definition A *Howe curve* is a curve isomorphic to the desingularization of the fiber product $E_1 \times_{\mathbf{P}^1} E_2$ of two genus-1 double covers $E_i \to \mathbf{P}^1$ ramified over S_i, where S_i consists of 4 points and where $|S_1 \cap S_2| = 1$.

Lem. *Every Howe curve is a canonical curve of genus* 4.

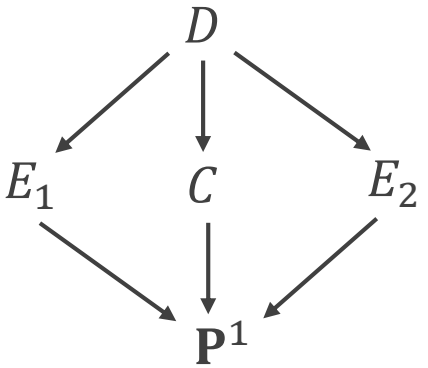


Fig. 1 V_4-diagram

- Namely, a Howe curve is a genus-4 curve D that fits into a V_4-diagram of the form shown in **Fig. 1**, where C is a genus-2 curve.
- The third author [Howe] studied these curves in order to quickly construct genus-4 curves with many rational points.

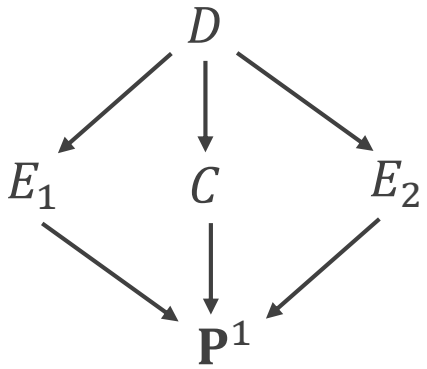
[Howe] *Quickly constructing curves of genus 4 with many points*, pp. 149–173 in: Frobenius Distributions Sato-Tate and Lang-Trotter conjectures (D. Kohel and I. Shparlinski, eds.), Contemporary Mathematics **663**, American Mathematical Society, Providence, RI (2016)

Howe curves (2/2)

- Howe curves are very useful to find ssp. curves and *ssg*. curves!

Thm (K. – H. – Senda). *For every $p > 3$, there exists a supersingular Howe curve.*

[K. – H. – Senda] *The existence of supersingular curves of genus 4 in arbitrary characteristic*, 2019. arXiv:1903.08095 [math.AG]



Fact D is superspecial (resp. supersingular)
$\Leftrightarrow$ Both E_1, E_2 and C are ssp. (resp. ssg.)

- The authors of [K. – H. – Senda] construct a 2-dim. family of Howe curves realized as $E_i : z_i^2 = f_i$ for cubic f_i parametrized by $(\lambda : \mu : \nu) \in \mathbf{P}^2(K)$.

- We expect that the space of Howe curves also includes a *ssp*. points!

Our contribution (1/2)

- Algorithms (in a later slide) to find and enumerate ssp. Howe curves
- Executing the algorithms over Magma, we have the following:
  - Finding an example of ssp. Howe curves;

Theorem *For every prime with* $7 < p < 20000$ *or with* $p \equiv 5 \bmod 6$*, there exists a superspecial Howe curve in characteristic* p*.*

  - Enumeration of isomorphism classes;

Theorem *For every prime with* $7 < p \leq 199$*, the number of isomorphism classes of superspecial Howe curves in characteristic* p *is given in Table 1.*

➢ The upper bounds on p in the theorems can be increased. For instance,
- Enumerating the ssp. Howe curves for $p = 199$ by our algorithm (B) took 124 seconds.
- Finding examples of ssp. Howe curves for every $7 < p < 20000$ took 680 minutes.

on one core of a 2.8 GHz Quad-Core Intel Core i7 with 16GB RAM.

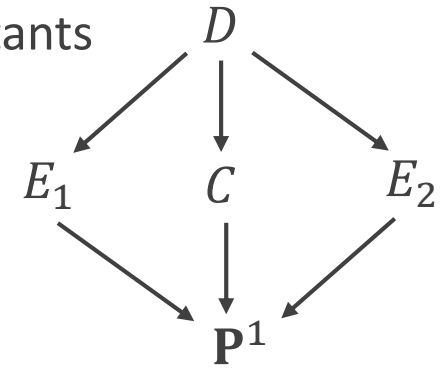
Our contribution (2/2)

Table 1. For each prime p from 11 to 199, we give the number $n(p)$ of superspecial Howe curves over $\overline{\mathbb{F}_p}$, and the ratio of $n(p)$ to the heuristic prediction $p^3/1152$.

p	$n(p)$	Ratio	p	$n(p)$	Ratio	p	$n(p)$	Ratio
11	4	3.462	67	260	0.996	137	2430	1.089
13	3	1.573	71	742	2.388	139	2447	1.050
17	10	2.345	73	316	0.936	149	3082	1.073
19	4	0.672	79	595	1.390	151	3553	1.189
23	33	3.125	83	655	1.320	157	3427	1.020
29	45	2.126	89	863	1.410	163	3518	0.936
31	59	2.281	97	802	1.012	167	6268	1.550
37	41	0.932	101	1207	1.350	173	4780	1.064
41	105	1.755	103	1151	1.213	179	5771	1.159
43	79	1.145	107	1237	1.163	181	5419	1.053
47	235	2.608	109	1193	1.061	191	9610	1.589
53	167	1.292	113	1323	1.056	193	6298	1.009
59	259	1.453	127	2013	1.132	197	6839	1.030
61	243	1.233	131	2606	1.335	199	8351	1.221

Outline of the algorithms (details at live session)

- Two strategies to find superspecial Howe curves
  - A) (E_1, E_2)**-first, using *Cartier-Manin matrices***
    - Use the same realization as in [K. – H. – Senda]
    - Reduced into solving multivariate systems with a few variables
    - Solve them with computer algebra techniques, e.g., resultants
  - B) C**-first, using *Richelot isogenies***
    - Reduced into producing superspecial genus 2-curves
    - Efficiently produce them by applying Richelot isogenies



- Efficient isomorphism test specific to Howe curves
  - Use of ramified points of $E_i \to \mathbf{P}^1$
  - Very efficient compared to the conventional method [K. – H. 2017], which compute Gröbner bases

You are very welcome to our live session!