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 28th 2020

Fourteenth Algorithmic Number Theory Symposium
(ANTS-XIV)

Agenda

1. A brief review of the pre-recording talk

2. Main algorithms
   - Isomorphism test for Howe curves
   - Two strategies to produce ssp. Howe curves
     A) (E_1, E_2)-first,
     B) C-first

3. Computational results with complexity comparison

4. Summary and future work

A brief review of pre-recording talk (1/2)

Main problems of this work

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

- Our target: $g = 4$

The (non-)existence of a ssp. curve in *general* p is an open problem, while some results for *specific small* p are known.

- This work aims to obtain results for *much larger* p by focusing on *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 $|S_1 \cap S_2| = 1$.

$$\begin{tikzcd} & D \arrow[dl] \arrow[d] \arrow[dr] & \\ E_1 \arrow[dr] & C \arrow[d] & E_2 \arrow[dl] \\ & \mathbf{P}^1 & \end{tikzcd}$$

- A Howe curve is a genus-4 curve D that fits into a V_4-diagram.

A brief review of pre-recording talk (2/2)

- **Howe curves are useful to find supersingular curves**

> **Thm (K. – H. – Senda, 2019).** *For every $p > 3$, there exists a supersingular Howe curve.*

> **Fact** D is ssp. (resp. ssg.) $\Longleftrightarrow$ Both E_1, E_2 and C are ssp. (resp. ssg.)

$$\begin{tikzcd} & D \arrow[dl] \arrow[d] \arrow[dr] & \\ E_1 \arrow[dr] & C \arrow[d] & E_2 \arrow[dl] \\ & \mathbf{P}^1 & \end{tikzcd}$$

- We also expect the existence of *superspecial* Howe curves!

- **Our contributions**
  - Algorithms to find and enumerate ssp. Howe curves
    1. Two strategies to produce such curves
    2. Efficient isomorphism test for (not necessarily superspecial) Howe curves
  - Computational results by executing the algorithms over Magma
    - The existence of a ssp. Howe curve for every $7 < p < 20000$
    - Enumeration of ssp. Howe curves for every $7 < p \leq 199$

Agenda

1. A brief review of the pre-recording talk

2. Main algorithms
   - Isomorphism test for Howe curves
   - Two strategies to produce ssp. Howe curves
     - A) (E_1, E_2)-first,
     - B) C-first

3. Computational results with complexity comparison

4. Summary and future work

Isomorphism test for Howe curves (1/2)

The three data specifying a Howe curve

- C : a genus-2 curve
- $\{W_1, W_2\}$, where $W_1 \sqcup W_2$ is the set of Weierstrass points of C with $\# W_i = 3$
- $\{P_1, P_2\}$, where P_i's are distinct points on C mapped to one another by hyperelliptic involution

$$\begin{tikzcd} & D \arrow[dl] \arrow[d] \arrow[dr] & \\ E_1 \arrow[dr] & C \arrow[d] & E_2 \arrow[dl] \\ & \mathbf{P}^1 & \end{tikzcd}$$

Given the above data, we call the double cover $\eta \colon D \to C$ the *structure map*.

> **Lem. 3.1 (page 6)** *The data specifying a Howe curve is recoverable up to automorphism of C just from the structure map $\eta \colon D \to C$.*

Note that we can take the set of ramified points of η as $\{P_1, P_2\}$.

Isomorphism test for Howe curves (2/2)

Isomorphism test for Howe curves

<u>Thm. 3.2 (page 6)</u> *If* $\mathrm{char}(K) \neq 2$, *then the two structure maps* $\eta_i : D \to C_i$ *are isomorphic to one another, i.e., there is an isomorphism* γ *and an automorphism* δ *such that the diagram of the r.h.s. commutes.*

$$\begin{tikzcd} D \arrow[r, "\delta"'] \arrow[d, "\eta_1"'] & D \arrow[d, "\eta_2"] \\ C_1 \arrow[r, "\gamma"'] & C_2 \end{tikzcd}$$

- H, H' : Howe curves specified respectively by $(C, \{W_1, W_2\}, \{P_1, P_2\})$ and $(C', \{W_1', W_2'\}, \{P_1', P_2'\})$, where the triples are given as in the previous slides

<u>Cor. 3.3 (page 8)</u> *Assume* $\mathrm{char}(K) \neq 2$. *If* H *and* H' *as above are isomorphic to each other, then there exists an isomorphism* $C \to C'$ *that takes* $\{W_1, W_2\}$ *to* $\{W_1', W_2'\}$ *and* $\{P_1, P_2\}$ *to* $\{P_1', P_2'\}$.

- This allows us to test whether Howe curves are isomorphic or not by determining the (non-)existence of a certain automorphism of $\mathbf{P}^1$ with simple linear algebra!

Agenda

1. A brief review of the pre-recording talk

2. Main algorithms
   - Isomorphism test for Howe curves
   - Two strategies to produce ssp. Howe curves
     - A) (E_1, E_2)-first,
     - B) C-first

3. Computational results with complexity comparison

4. Summary and future work

A) (E_1, E_2)-first, using Cartier-Manin matrices (1/2)

2-dim. parameterization of Howe curves by [K. – H. – Senda]

- Given elliptic curves $y^2 = x^3 + A_i x + B_i$ $(A_i, B_i \in K)$ with $i = 1,2$, we say that a point $(\lambda : \mu : \nu) \in \mathbf{P}^2(K)$ is *of Howe type* if

  (1) $\mu \neq 0$ and $\nu \neq 0$, **(2)** f_1 and f_2 are coprime,

  where

  - $f_1 = x^3 + A_1\mu^2 x + B_1 \mu^3$
  - $f_2 = (x-\lambda)^3 + A_2 \nu^2 (x-\lambda) + B_2 \nu^3$

$$\begin{tikzcd} & H \arrow[dl] \arrow[d] \arrow[dr] & \\ E_1 \arrow[dr] & C \arrow[d] & E_2 \arrow[dl] \\ & \mathbf{P}^1 & \end{tikzcd}$$

- The space of these points $(\lambda : \mu : \nu) \in \mathbf{P}^2(K)$ parameterizes Howe curves D by $E_1 : z^2 y = f_1^{\mathrm{h}}$, $E_2 : w^2 y = f_2^{\mathrm{h}}$ and $C : y^2 = f_1 f_2$, where f_i^{h} is the homogenization of f_i w.r.t. y.

The field of definition of superspecial Howe curves

> **<u>Prop. 4.1 (page 9)</u>**. *Any superspecial Howe curve is K-isomorphic to H obtained as above for A_1, B_1, A_2, B_2, λ, μ and ν belonging to $\mathbb{F}_{p^2}$.*

A) (E_1, E_2)-first, using Cartier-Manin matrices (2/2)

A criterion for superspeciality from Cartier-Manin matrices for C

- C : the hyperelliptic curve $y^2 = f := f_1 f_2$
- γ_i : the coefficient of x^i in $f^{(p-1)/2}$

Lem. 2.2 (page 5). *The Howe curve H is superspecial if and only if* $\gamma_{p-2} = \gamma_{p-1} = \gamma_{2p-2} = \gamma_{2p-1} = 0.$

The problem to find ssp. Howe curves is reduced into solving a zero-dim. system of (multivariate) algebraic equations!

Outline of algorithm (Alg. 4.2 on pp. 9-10 for details)

1. Compute $(A, B) \in \left(\mathbb{F}_{p^2}\right)^2$ such that $y^2 = x^3 + Ax + B$ is supersingular.
2. For each set of pairs (A_1, B_1) and (A_2, B_2):
   a. Compute $\gamma_{p-2}, \gamma_{p-1}, \gamma_{2p-2}, \gamma_{2p-1}$, where λ, μ are variables and $\nu = 1$
   b. Solve the (multivariate) system in Lem. 2.2 over $\mathbb{F}_{p^2}$.

Agenda

1. A brief review of the pre-recording talk

2. Main algorithms
   - Isomorphism test for Howe curves
   - Two strategies to produce ssp. Howe curves
     - A) (E_1, E_2)-first,
     - B) C-first

3. Computational results with complexity comparison

4. Summary and future work

B) C-first, using Richelot isogenies (1/4)

The strategy

1. Enumerate superspecial genus 2-curves C.
   - Apply Algorithm 5.7 of [Howe] with the IKO formula:

$$\sum_{C:\text{ssp.genus }2} \frac{1}{\#\mathrm{RedAut}(C)} = \frac{(p-1)(p-2)(p-3)}{2880}$$

$$\begin{tikzcd}
 & H \arrow[dl] \arrow[d] \arrow[dr] & \\
E_1 \arrow[dr] & C \arrow[d] & E_2 \arrow[dl] \\
 & \mathbf{P}^1 &
\end{tikzcd}$$

   where $\mathrm{RedAut}(C)$ is the reduced group of automorphisms of C.

   Note: An isomorphism test for genus 2-curves is done by computing Igusa-invariants

2. For each C, check whether it fits into V_4-diagram.
3. Execute our isomorphism test of Howe curves for each pair of computed (f_1, f_2) and (f_1', f_2') defining $C: y^2 = f_1 f_2$ and $C': y^2 = f_1' f_2'$.

[Ibukiyama-Katsura-Oort] *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no.2, 127-152, MR 827350.

[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)

B) C-first, using Richelot isogenies (2/4)

- Enumeration of ssp. genus 2-curves (variant of Alg. 5.7 of [Howe])

1. Set $\mathcal{L} \leftarrow \emptyset$, and compute all $\mathbb{F}_{p^2}$-maximal elliptic curves over $\mathbb{F}_{p^2}$.
2. For every pair (E, E') of $\mathbb{F}_{p^2}$-maximal elliptic curves E and E' over $\mathbb{F}_{p^2}$, add at most six genus-2 curves C to $\mathcal{L}$ such that $J(C)$ is $(2,2)$-isogenous to $E \times E'$, computed by Prop. 4 of [H. – Leprévost – Poonen].
3. Repeat the following until *IKO formula* holds:
   - For each $C \in \mathcal{L}$: compute non-singular curves C' which are *Richelot isogenous* to C. If C' is not isomorphic to any element of $\mathcal{L}$, then $\mathcal{L} \leftarrow \mathcal{L} \cup \{C'\}$.
   - This is done by using a method in Section 4 of [Bruin - Doerksen] (or see Section 3 of [Castryck et al.]) for computing Richelot isogenies.

[Howe - Leprévost – Poonen] *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315-364. MR 1748483

[Bruin – Doerksen] *The arithmetic of genus two curves with (4, 4)-split jacobians*. Canadian Journal of Mathematics, 63(5):992–1024, 2011.

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

B) C-first, using Richelot isogenies (3/4)

Correctness of the enumeration of ssp. genus 2-curves

Conj. 5.1 (page 12). *If we seed the list of curves as above, and then take the closure of the list under Richelot isogenies, we will obtain all superspecial genus 2-curves.*

- See also **Conjecture 1 of [Castryck et al.]**, which conjectures the graph of (2,2)-isogenies of ssp. p.p. abelian surfaces is connected.
  - Recently it seems to be shown in **Corollary 18 in [Jordan-Zaytman]** (unpublished).
- Fortunately, we *do not need to prove* this conjecture in general, because for any specific p we can verify it computationally by *IKO formula*.

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

[Jordan - Zaytman] *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*, arXiv:2005.09031.

B) C-first, using Richelot isogenies (4/4)

Testing whether a genus 2-curve fits into V_4-diagram (pp. 12-13)

- Assume $C \in \mathcal{L}$ is given by $y^2 = \prod_{i=1}^{6}(x - a_i)$
- For each of 10 ways to split $\{a_i\}$ to 2 sets of 3 points (e.g., $\{a_1, a_2, a_3\}, \{a_4, a_5, a_6\}$): Conduct 1, 2 to compute $b \in \mathbb{F}_{p^2}$ such that the following are both supersingular:

$$(5.1) \qquad y^2 = (x-b)(x-a_1)(x-a_2)(x-a_3)$$
$$(5.2) \qquad y^2 = (x-b)(x-a_4)(x-a_5)(x-a_6)$$

1. For each ssg. j-invariant j_0 ($p/12$ choices): solve $j(b) = j_0$.
   - $j(b)$: the j-invariant of an elliptic curve isom. to (5.1)
   - $j(b)$ is degree 6 as a poly. of b
2. For each root b, check the λ-invariant of (5.2) is supersingular.
   - A randomly chosen λ-inv. is ssg. with probability $(6 \times p/12)/p^2 = 1/2p$

Approximation of the num. of ssp. Howe curves

IKO formula $\boxed{\frac{p}{2880}} \times 10 \times \left(6 \times \frac{p}{12}\right) \times \frac{1}{2p} = \frac{p^3}{1152}$

Agenda

1. A brief review of the pre-recording talk

2. Main algorithms
   - Isomorphism test for Howe curves
   - Two strategies to produce ssp. Howe curves
     - A) (E_1, E_2)-first,
     - B) C-first

3. Computational results with complexity comparison

4. Summary and future work

Computational results with complexity remark

Our results (recall)

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

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.

  over Magma on one core of a 2.8 GHz Quad-Core Intel Core i7 with 16GB RAM.
- The results with $p \equiv 5 \bmod 6$ are obtained not by computer (a proof on page 14)

Estimated complexities (upper bounds) of the two algorithms

- The method A): $\tilde{O}(p^6)$ $>$ The method B): $\tilde{O}(p^4)$

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

Table 2. Benchmark timing data for the strategies (A) and (B). All times shown are in seconds.

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53
(A)	0.02	0.01	0.17	0.76	3.92	6.14	27.59	114.70	193.82	617.23	1118.63	1423.26	2686.17	5678.32
(B)	0.08	0.01	0.04	0.05	0.09	0.12	0.21	0.31	0.34	0.54	0.71	0.80	1.03	1.46

Agenda

1. A brief review of the pre-recording talk

2. Main algorithms
   - Isomorphism test for Howe curves
   - Two strategies to produce ssp. Howe curves
     A) (E_1, E_2)-first,
     B) C-first

3. Computational results with complexity comparison

4. Summary and future work

Summary and future work

- **Results introduced in this talk**
  - Algorithms to find and enumerate ssp. Howe curves
    - Two strategies to produce such curves
    - Efficient isomorphism test for (not necessarily superspecial) Howe curves
  - Computational results by executing the algorithms over Magma
    - The existence of a ssp. Howe curve for every $7 < p < 20000$
    - Enumeration of ssp. Howe curves for every $7 < p \leq 199$

- **Future work (Open problems)**
  - Improve the proposed algorithms
  - Prove the following conjecture from our computational results:
    - *For every $p > 7$, there exists a ssp. Howe curve, and thus a ssp. curve of genus 4 always exists except for $p = 7$.*
  - Case of genus > 4 ?