On the computational enumeration of superspecial curves: A survey and complements (extended abstract)*

Hiroki Furue and Momonari Kudo

The University of Tokyo, Tokyo, 113-8656, Japan
{furue-hiroki261,m-kudo}@g.ecc.u-tokyo.ac.jp

Keywords: Algebraic curves · Curves of low genera · Superspecial curves.

1 Introduction

Throughout, a curve means a non-singular projective variety of dimension one. Let K be a field of characteristic $p > 0$, and $\overline{K}$ its algebraic closure. We say that a curve C of genus g over K is *superspecial* (resp. s.sp. for short) if its Jacobian variety is isomorphic to a product of supersingular elliptic curves. For a given pair (g, p), there are only finite $\overline{\mathbb{F}_p}$-isomorphism classes of s.sp. curves of genus g over a finite field of characteristic $p > 0$, and the problem of enumerating the isomorphism classes is known to be classically important but difficult in general. For the field of definition, the most important case is $\mathbb{F}_{p^2}$, since any s.sp. curve over K is $\overline{K}$-isomorphic to one over $\mathbb{F}_{p^2}$, see the proof of [3, Theorem 1.1].

For $g \leq 3$, the problem is solved for all $p > 0$, based on the theory of principally polarized abelian varieties (cf. [7, Section 1] for a review of previous studies). On the other hand, the problem for $g \geq 4$ has not been solved in all primes, but in recent years, Kudo-Harashita developed *computational* approaches to enumerate genus-4 or genus-5 s.sp. curves [8], [9], [10], [11]. The idea of their approaches is to reduce the enumeration into solving multivariate systems over finite fields, and they constructed algorithms where each system is solved by the Gröbner basis computation (precisely, the hybrid approach [1]). Executing the algorithms over Magma, they also succeeded in enumerating s.sp. curves in real time for several small p; for $p \leq 11$ (resp. $p \leq 19$) in the genus-4 non-hyperelliptic (resp. hyperelliptic) case [8], [10] (resp. [9]), and for $p \leq 13$ in the genus-5 trigonal case [11]. While Kudo-Harashita's algorithms are applicable to arbitrary p, their complexities have been estimated neither in theory nor in practice; no reason why any computational result for p larger than the above bound has not been obtained is explicitly stated in each of their papers.

The aim of this talk is to investigate the computational difficulty of enumerating s.sp. curves for $g = 4$ and 5. Specifically, we mainly survey Kudo-Harashita's computational approaches, and complement them with complexity analysis. Based on our complexity analysis, we implemented optimized algorithms over Magma, by which we obtain new computational results in $p = 13$ and 17 for $g = 4$. A practical limit of the enumeration will be also discussed.

* The authors thank the anonymous reviewers for their comments and suggestions, which have helped the authors significantly improve this extended abstract. Supported by JSPS Grant-in-Aid for Young Scientists 20K14301.

2 Kudo-Harashita's computational approaches

In this section, we briefly review Kudo-Harashota's computational approaches to enumerate s.sp. curves. For reasons of spaces, this extended abstract focuses on the genus-4 non-hyperelliptic case [8], [10]. Let p, K and $\overline{K}$ be as in Section 1. We choose a non-square element $\epsilon \in K^{\times}$, and fix it until the end of this extended abstract. It is well-known (cf. [6]) that every non-hyperelliptic curve C of genus 4 over K is isomorphic to the complete intersection of quadratic and cubic surfaces in the projective 3-space $\mathbb{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$, say $C = V(Q, P)$, where Q and P are irreducible quadratic and cubic forms in $\overline{K}[x, y, z, w]$ respectively.

The following proposition is useful to test the superspeciality of C:

Proposition 1 ([8, Corollary 3.1.6]). *With notation as above, $C = V(Q, P)$ is superspecial if and only if all the coefficients of $x^{pi-i'}y^{pj-j'}z^{pk-k'}w^{p\ell-\ell'}$ in $(QP)^{p-1}$ are equal to 0, where i, j, k, ℓ, i', j', k' and ℓ' are positive integers with $i + j + k + \ell = i' + j' + k' + \ell' = 5$.*

It is also shown in [8] and [10] that defining equations Q and P can be simplified as follows: First, we may assume that any coefficient of Q and P belongs to the base field K, see [8, Section 2.1]. Next, Q is assumed to be either of the following forms: (**N1**) $Q = 2xw + 2yz$, (**N2**) $Q = 2xw + y^2 - \epsilon z^2$, and (**D**) $Q = 2yw + z^2$, where "N" and "D" stand for non-degenerate and degenerate respectively. The number of unknown coefficients in P can be reduced to be almost 10 (which is close to the whole moduli dimension 9), by considering the action of elements in the (similitude) orthogonal group of Q. For reason of spaces, we here state the case (**N2**) only (see [10, Lemmas 3.4.1 and 3.6.1] for the other cases).

Proposition 2 ([10, Lemma 3.5.1]). *For $Q = 2xw + y^2 - \epsilon z^2$, every non-hyperelliptic curve C of genus 4 over K is K-isomorphic to $V(Q, P)$, where*

$$\begin{aligned} P =&(a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2) \\ &+ a_5z(3y^2 + \epsilon z^2) + (a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3, \end{aligned} \tag{1}$$

where $a_i \in K$ with $(a_1, a_2) \neq (0, 0)$, and where $b_1, b_2 \in \{0, 1\}$.

Based on Propositions 1 and 2, Kudo-Harashita [8], [10] gave algorithms to enumerate s.sp. C. We here write down a sketch of the algorithms:

Proposition 3. *For the input q, a set of the following procedures computes complete representatives of isomorphism classes of s.sp. C over $\mathbb{F}_q$:*

1. *For each of the three types ((**N1**), (**N2**) and (**D**)) of Q:*
   (a) *Collect cubic forms $P \in \mathbb{F}_q[x, y, z, w]$ as in Proposition 2 such that the 16 coefficients in $(QP)^{p-1}$ given in Proposition 1 are all zero.*
   (b) *For each P collected in (a), test whether $V(Q, P)$ is non-singular or not. If $V(Q, P)$ is non-singular, store $C = V(Q, P)$.*
2. *Compute the isomorphism classes of s.sp. curves C collected in Step 1, and return them.*

Step 1(a) solves the multivariate system "the 16 coefficients in Proposition 1 are zero" with respect to the variables $a_1, \ldots, a_{10}$ for each of possible (b_1, b_2), where "solve over $\mathbb{F}_q$" means to compute exactly all the roots $(a_1, \ldots, a_{10}) \in \mathbb{F}_q^{10}$ of the system. Note that we also add *field equations* $a_i^q - a_i$ for $1 \leq i \leq 10$ to each system to make it zero-dimensional, and thus the number of equations is $16 + 10 = 26$ in total. To solve each system efficiently, one applies the hybrid approach [1], which mixes exhaustive search with the Gröbner basis computation. More specifically, the hybrid approach first fixes the values of k among the whole $n = 10$ variables (e.g., $a_1, \ldots, a_k$), and then solves the remaining system with the $n - k$ variables $a_{k+1}, \ldots, a_n$ by a Gröbner basis algorithm such as F5 [4] together with the FGLM basis conversion [5]. Step 2 is also done with the the Gröbner basis computation, see [10, Section 4] for details. (The complexity of Step 1 would be dominant, and thus we omit details of Step 2 in this extended abstract.)

Implementing the algorithm over Magma, Kudo-Harashita succeeded in enumerating s.sp. curves of genus 4 over $\mathbb{F}_q$ for $q = 5, 5^2, 7, 7^2, 7^2, 11$. In particular, there is no s.sp. curve in characteristic $p = 7$ [8, Theorem B]. However, the complexity has not been determined yet; it might be exponential with respect to p since the maximum total-degree d of equations in each system is $q = p$ or p^2.

3 Our analysis and new computational results

This section complements Kudo-Harashita's approaches with complexity analysis, and reports some new computational results in the enumeration of s.sp. curves with our optimized implementations. In particular, we estimate the complexity of Step 1 of the algorithm in Proposition 3, by which optimal choices of the parameter k of the hybrid approach adopted in Step 1 are also estimated.

For simplicity, we fix Q and (b_1, b_2) in Proposition 3. We denote by $\mathcal{F} \in \mathbb{F}_q[a_1, \ldots, a_{10}]^{26}$ the system of 26 polynomials (including field equations $a_i^q - a_i$) to be solved in Step 1(a). For a zero-dimensional multivariate system $\mathcal{H}$, we denote by slv.deg$(\mathcal{H})$ its *solving degree* [2, Section 3], which means the minimum d such that the row reduction of the Macaulay matrix $M_{\leq d}$ of $\mathcal{H}$ produces a Gröbner basis with respect to a graded reverse lexicographic order. Let $d_k^{(\max)}$ denote $\max_{\mathcal{F}_k}(\mathrm{slv.deg}(\mathcal{F}_k))$, and where $\mathcal{F}_k$ runs through the set of polynomials obtained by substituting values in $\mathbb{F}_q$ to k variables in elements of $\mathcal{F}$.

Proposition 4. *With notation as above, the complexity of Step 1 of the algorithm in Proposition 3 is (roughly) upper-bounded by* $O(\min_k T_{k,q})$ *with*

$$T_{k,q} := q^k \left(26 \binom{10+q}{q} + \binom{10 - k + d_k^{(\max)}}{d_k^{(\max)}}^{\omega} \right),$$

where ω *is the exponent for matrix multiplication with* $2 < \omega < 2.38$.

We can also prove $d_k^{(\max)} \leq (10-k)(q-1)+1$. With this bound, we can obtain several numerical examples of $\min_k T_{k,q}$ with k, see Table 1.

Table 1. Comparison of the number k of fixed variables in Step 1 of the algorithm in Proposition 3 for several small q. For each q, we denote by k_{KH} the number chosen in [8] and [10], and by k_{opt} the value of k minimizing $T_{k,q}$, assuming $d_k^{(\max)} = (10-k)(q-1)+1$.

q	5	7	11	13	17	19	23
k_{KH}	2 or 3	3	5	-	-	-	-
k_{opt}	8	8	8	8	8	8	8
$\min_k T_{k_{\mathrm{opt}},q}$ (bits)	35.1	41.6	50.9	54.5	60.4	63.0	67.4

Based on our complexity analysis, we re-implemented Kudo-Harashita's enumeration algorithm in Proposition 3 with optimal choices of the parameter k in the hybrid approach. Executing the optimized implementation on Magma V2.26-10 on a PC with 2.10GHz Intel(R) Xeon(R) Gold 6130 CPU, we obtain the following new computational results:

Theorem 1. *For $q = 13$ and 17, the number of cubic forms P in each case such that $V(Q,P)$ is superspecial is summarized in a table at [12], where the time for executing our implementation is also shown.*

We are now executing the isomorphism classification on obtained s.sp. curves. In our talk at the conference, we will also report results by the isomorphism classification, and will determine its complexity. A shape bound on $d_k^{\max}$ and discussion for the case $g = 5$ will also be presented.

References

1. Bettale, L., Faugere, J.-C. and Perret, L., Hybrid approach for solving multivariate systems over finite fields, *J. Math. Cryptol.*, **3** (2009) 177–197.
2. Caminata, A. and Gorla, E., Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra, In: Bajard, J. C., Topuzoğlu, A. (eds) Arithmetic of Finite Fields. WAIFI 2020. LNCS, **12542**. Springer, Cham, 2022.
3. Ekedahl, T.: On supersingular curves and abelian varieties, *Math. Scand.*, **60** (1987), 151–178.
4. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), In: Proc. of ISSAC 2002, 75-–83.
5. Faugère, J.-C., Gianni P. M., Lazard, D. and Mora, T.: Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering, J. Symb. Comput., **16**, 329–344, 1993.
6. Hartshorne, R., Algebraic Geometry, GTM **52**, Springer-Verlag (1977).
7. Kudo, M.: *Counting isomorphism classes of superspecial curves*, Accepted for publication in RIMS Kôkyûroku Bessatsu, arxiv: 2106.12409.
8. Kudo, M. and Harashita, S., Superspecial curves of genus 4 in small characteristic, *Finite Fields and Their Applications*, **45**, 131–169 (2017).
9. Kudo, M. and Harashita, S., Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields, In: L. Budaghyan, F. Rodriguez-Henriquez (eds), Arithmetic of Finite Fields, WAIFI 2018, LNCS, **11321**, 58–73, Springer, Cham, 2018.
10. Kudo, M. and Harashita, S., Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4, *Tokyo Journal of Mathematics*, Vol. **43**, Number 1, 259–278, 2020.
11. Kudo, M. and Harashita, S., Superspecial trigonal curves of genus 5, *Experimental Mathematics*, published online: 16 Apr. 2020.
12. https://sites.google.com/view/m-kudo-official-website/english/code/ssp4