Efficient search for superspecial hyperelliptic curves of genus 4 in large characteristic (extended abstract)*

Tasuku Nakagawa[1], Momonari Kudo[1], and Tsuyoshi Takagi[1]

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

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

1 Introduction

Throughout, all the complexities are measured by the number of arithmetic operations in $\mathbb{F}_{p^2}$ for a prime p, unless otherwise noted. Soft-O notation omits logarithmic factors. 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. A curve C of genus g over K is said to be *superspecial* (*s.sp.* for short) if its Jacobian variety is isomorphic to a product of supersingular elliptic curves. S.sp. curves are of course important objects in theory, but also in practical applications such as cryptography using algebraic curves, see e.g., [1], where s.sp. genus-2 curves are used. Given a pair (g, p), only finite s.sp. curves of genus g over $\overline{\mathbb{F}_p}$ exist, and the problem of finding or enumerating them is known to be classically important. 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 [4, Theorem 1.1].

For $g \leq 3$, the problem is solved for all $p > 0$, based on the theory of principally polarized abelian varieties. Specifically, for $g = 1$ (resp. 2 and 3), Deuring [2] (resp. Ibukiyama-Katsura-Oort [8, Theorem 2.10]) showed that the number of $\overline{\mathbb{F}_p}$-isomorphism classes of s.sp. curves is determined by computing the class numbers of a quaternion algebra (resp. quaternion hermitian lattices). These class numbers were computed in [3] (resp. [7], [6]) for $g = 1$ (resp. 2, 3).

On the other hand, the problem for $g \geq 4$ has not been solved in all primes, but in recent years, Kudo-Harashita developed several algorithms to count genus-4 or 5 s.sp. curves [9], [10], [11]. In particular, an algorithm for enumerating s.sp. *hyperelliptic* curves of genus 4 was proposed in [10] at WAIFI2018, but is practical only for small p (in fact $p \leq 19$), due to the cost of solving multivariate systems (cf. Section 2). Cf. In non-hyperelliptic case, Kudo-Harashita-Howe [12] presented an algorithm at ANTS-XIV, specific to finding s.sp. curves of genus 4 with complexity $\tilde{O}(p^4)$ (arithmetic operations in $\mathbb{F}_{p^4}$).

This paper proposes a more efficient algorithm than [10] to produce s.sp. hyperelliptic curves of genus 4, restricting ourselves to a certain parametric family of curves. The complexity is proved to be $\tilde{O}(p^3)$. By executing the algorithm over Magma, we also prove the existence of such a curve for every p with $17 \leq p < 1000$ and $p \equiv 2 \bmod 3$.

* Supported by JSPS Grant-in-Aid for Young Scientists 20K14301, and JST CREST Grant Number JPMJCR2113.

2 Preliminaries

This section reviews general facts on hyperelliptic curves, and Kudo-Harashita's enumeration [10] of s.sp. hyperelliptic curves of genus 4.

A hyperelliptic curve H of genus g over a field K of characteristic $p > 2$ is realized as the desingularization of the projective closure of the affine plane curve $y^2 = f(x)$, where $f(x) \in K[x]$ is a separable polynomial of degree $2g + 1$ or $2g + 2$. As for the form of $f(x)$, we have the following lemma:

Lemma 1 ([10, Lemma 2]). *Assume that p and $2g + 2$ are coprime, and let $\epsilon \in K^\times \smallsetminus (K^\times)^2$. Any hyperelliptic curve H of genus g over K is isomorphic to the desingularization of the projective closure of*

$$cy^2 = x^{2g+2} + bx^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1x + a_0, \tag{2.1}$$

where $a_i \in K$ for $0 \le i \le 2g - 1$, and where $b = 0, 1, \epsilon$ and $c = 1, \epsilon$.

The following lemma gives a criterion to test whether two hyperelliptic curves over K are K-isomorphic to each other, or not:

Lemma 2 ([10, Lemma 1]). *Let $H_1 : c_1y^2 = f_1(x)$ and $H_2 : c_2y^2 = f_2(x)$ be hyperelliptic curves over K, where $c_iy^2 = f_i(x)$ is of the form (2.1). For any K-isomorphism $\sigma\colon H_1 \to H_2$, there exist $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K)$ and $\lambda \in K^\times$ such that $\sigma(x, y) = \left(\frac{\alpha x+\beta}{\gamma x+\delta}, \frac{\lambda y}{(\gamma x+\delta)^{g+1}}\right)$ for all (x, y) on $c_1y^2 = f_1(x)$.*

As for the superspeciality, it is known that a curve C is s.sp. if and only if the Cartier operator on the space $H^0(C, \Omega_C^1)$ of regular differential forms on C acts as zero. A matrix representing the operator with respect to a suitable basis is called the *Cartier-Manin matrix*, and in the case where C is hyperelliptic, there is a well-known explicit formula to compute it:

Lemma 3 (cf. [14, Section 2]). *With notation as above, the Cartier-Manin matrix of H is the $g \times g$ matrix whose (i, j)-entry is the coefficient of x^{pi-j} in $f^{(p-1)/2}$ for $1 \le i, j \le g$. Hence, H is s.sp. if and only if the coefficients of x^{pi-j} in $f^{(p-1)/2}$ are equal to 0 for all pairs of integers $1 \le i, j \le g$.*

Based on Lemmas 1 – 3, an algorithm for enumerating s.sp. hyperelliptic curves over $K = \mathbb{F}_q$ with $q = p$ or p^2 was proposed by Kudo-Harashita [10], and it consists of the following two steps: In the first step, regarding unknown coefficients in (2.1) as variables, construct a multivariate system "the Cartier-Manin matrix is zero" (with $2g$ variables), and solve it over $\mathbb{F}_q$ with the Gröbner basis computation. The second step classifies the collected curves corresponding to the solutions to the system into isomorphism classes, by Lemma 2. Kudo-Harashita executed the algorithm over Magma for $g = 4$ with $q = 11, 11^2, 13, 13^2, 17, 17^2, 19$. However, the complexity has not been determined, due to the use of the Gröbner basis computation. In fact, it might be exponential with respect to p, since the multivariate system to be solved in the first step has the maximal total-degree $(p-1)/2$. Moreover, the second step might also be costly, due to the growth of the number of solutions found in the first step.

3 Main results

We shall construct an algorithm specific to producing s.sp. hyperelliptic curves of genus 4, which is practical for p extremely larger than some number mentioned in [10]. For this, we focus on a family of hyperelliptic curves of genus 4 given by

$$H_{a,b} : y^2 = f_{a,b}(x) := x^{10} + x^7 + ax^4 + bx, \tag{3.1}$$

where $a, b \in \mathbb{F}_{p^2}$. This kind of a curve appears as a s.sp. curve over $\mathbb{F}_{17^2}$ enumerated in [10], and it tends to be s.sp. from our preliminary computation; by exhaustive search for (a, b), we confirmed that there exists (resp. does not exist) (a, b) such that $H_{a,b}$ is s.sp. for any $17 \leq p < 100$ with $p \equiv 2 \bmod 3$ (resp. $p \equiv 1 \bmod 3$). The main results are summarized in Theorems 1 and 2 below.

Theorem 1. *Main Algorithm below can enumerate s.sp. hyperelliptic curves of the form* (3.1) *in time* $\tilde{O}(p^3)$.

Main Algorithm (sketch). For a prime p as the input, conduct the following:

1. Regarding a, b as variables, compute the Cartier-Manin matrix $M_{a,b}$ of $H_{a,b}$.
2. Collect all (a, b) such that $H_{a,b}$ is a s.sp. hyperelliptic curve, as follows:
   2-1. Compute the solutions $(a_0, b_0) \in \mathbb{F}_{p^2}$ to $M_{a,b} = 0$.
   2-2. For each solution (a_0, b_0), check if the equation (3.1) for $(a, b) = (a_0, b_0)$ defines a hyperelliptic curve, by computing $\gcd(f_{a,b}, f'_{a,b})$.
3. Classify the $H_{a,b}$'s collected in Step 2 into isomorphism classes, based on Lemma 2. Return the isomorphism classes.

The correctness follows from Lemmas 2 and 3. The complexity of Step 2 is estimated as that of computing resultants, say $\tilde{O}(p^3)$ [13]. The complexities of Steps 1 and 3 are estimated by Lemmas 4 and 5 below: Lemma 4 is proved by reducing the computation of 16 specific coefficients in $f^{(p-1)/2}$ into that of linear recurrences on coefficients of the powers of f described in [5]. Lemma 5 is proved by investigating a multivariate system in $\alpha, \beta, \gamma, \delta, \lambda$ constructed by σ in Lemma 2, and it is also applicable to arbitrary hyperelliptic curves.

Lemma 4. *The Cartier-Manin matrix* $M_{a,b}$ *in Step 1 is computed in time* $O(p^3)$.

Lemma 5. *Fix the genus* g. *Then testing if two hyperellliptic curves of genus* g *over* $\mathbb{F}_{p^2}$ *are* $\overline{\mathbb{F}_p}$*-isomorphic or not is done in constant time with respect to* p.

We implemented the algorithm on Magma V2.26-10 on a PC with macOS Monterey 12.0.1, at 2.6 GHz CPU 6 Core (Intel Core i7) and 16GB memory (cf. [15] for the source codes). Executing the implemented algorithm, we obtain:

Theorem 2. *For every prime* $17 \leq p < 1000$*, the number of* $\overline{\mathbb{F}_p}$*-isomorphism classes of s.sp.* $H_{a,b}$*'s are summarized in a table at [15]. In particular, for each* $17 \leq p < 1000$ *with* $p \equiv 2 \bmod 3$ *(resp.* $p \equiv 1 \bmod 3$*), there exists (resp. does not exist)* $(a, b) \in \mathbb{F}_{p^2}$ *such that* $H_{a,b}$ *is a s.sp. hyperelliptic curve.*

We can easily increase the upper bound on p in Theorem 2. For example, on the PC described above, computing all the s.sp. $H_{a,b}$'s took 230,719 seconds (about 64 hours), and finding a single example of a s.sp. $H_{a,b}$ took only 98 seconds, for every p between 17 and 1000 .

4 Concluding remarks

We realized an algorithm with complexity $\tilde{O}(p^3)$ specific to producing s.sp. hyperelliptic curves of genus 4, restricting to a family of $H_{a,b}$ as in (3.1). Our algorithm cannot enumerate all s.sp. hyperelliptic curves of genus 4 different from the algorithm in [10] at WAIFI2018, but it is expected from Theorem 2 to surely find such a curve for arbitrary $p \geq 17$ with $p \equiv 2 \bmod 3$. By executing the algorithm over Magma, we succeeded in enumerating s.sp. hyperelliptic curves $H_{a,b}$ for every p between 17 to 1000, which is drastically larger than $p = 17, 19$ as in the enumeration of [10]. A future work is to construct an algorithm for finding s.sp. hyperelliptic curves of genus 4 in the case where $p \equiv 1 \bmod 3$, with complexity lower than the algorithm of [10].

References

1. Castryck, W., Decru, T., Smith, B.: Hash functions from superspecial genus 2 curves using Richelot isogenies, *J. of Math. Cryptol.*, **14**(1), 268–292, 2020.
2. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg*, **14** (1941), no. 1, 197–272.
3. Eichler, M.: Über die Idealklassenzahl total definiter Quaternionenalgebren, *Math. Z.*, **43** (1938), 102–109.
4. Ekedahl, T.: On supersingular curves and abelian varieties, *Math. Scand.*, **60** (1987), 151–178.
5. Harvey, D. and Sutherland, A. V.: Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, *LMS J. Comput. Math.*, **17** (2014), no. suppl. A, 257–273.
6. Hashimoto, K.: Class numbers of positive definite ternary quaternion Hermitian forms, *Proc. Japan Acad. Ser. A Math. Sci.*, **59** (1983), no. 10, 490–493.
7. Hashimoto, K. and Ibukiyama, T.: On class numbers of positive definite binary quaternion Hermitian forms II, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 3, 695–699 (1982).
8. Ibukiyama, T., Katsura, T. and Oort, F.: Supersingular curves of genus two and class numbers, *Compositio Mathematica*, **57** (1986), 127–152.
9. Kudo, M. and Harashita, S.: Superspecial curves of genus 4 in small characteristic, *Finite Fields and Their Applications*, **45**, 131–169 (2017).
10. 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**, pp. 58–73, Springer, Cham, 2018.
11. 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.
12. Kudo, M., Harashita, S. and Howe, E. W.: Algorithms to enumerate superspecial Howe curves of genus four, *Proceedings of Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)*, Open Book Series, Vol. **4** (2020), No. 1, 301–316.
13. van der Hoeven, J. and Lecerf, G.: Fast computation of generic bivariate resultants, *Journal of Complexity*, Vol. **62**, 2021.
14. Yui, N., On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, *Journal of algebra*, **52**, 378–410 (1978).
15. `https://sites.google.com/view/m-kudo-official-website/english/code/hyp`