Parametrizing generic curves of genus five and its application to finding curves with many rational points

Momonari Kudo* and Shushi Harashita†

February 14, 2021

Abstract

In algebraic geometry, it is important to give good parametrizations of spaces of curves, theoretically and also practically. In particular, the case of non-hyperelliptic curves is the central issue. In this paper, we give a very effective parametrization of curves of genus 5 which are neither hyperelliptic nor trigonal. After that, we construct an algorithm for a complete enumeration of generic curves of genus 5 with many rational points, where "generic" here means non-hyperelliptic and non-trigonal with mild singularities of the associated sextic model which we propose. As an application, we execute an implementation on computer algebra system MAGMA of the algorithm for curves over the prime field of characteristic 3.

1. Introduction

Let K be a field and let $\mathbb{P}^n$ denote the projective n-space over K. Parameterizing the space of curves over K of given genus is an important task in algebraic geometry, number theory and arithmetic geometry. In particular, it is meaningful to construct families of curves, with explicit defining equations, that contain all curves of genus g. For the hyperelliptic case, it is well-known that any hyperelliptic curve over K of genus g is the normalization of $y^2 = f(x)$ for a square-free polynomial $f(x) \in K[x]$ of degree $2g+1$ or $2g+2$. However, it is not so easy that we give a reduction of defining equations for non-hyperelliptic curves. Note that a curve is non-hyperelliptic if and only if it is canonical (cf. [5, Chap. IV, Prop. 5.2]). For genus 3, we find a nice parametrization in Shaska and Thompson [13]. For genus 4, a canonical curve is the complete intersection of a quadric and a cubic in $\mathbb{P}^3$. In [6] and [9], we discussed reductions of the space of pairs of quadratic forms and cubic forms by the projective general linear group $\mathrm{PGL}_4(K)$ of degree 4.

The next target is the case of $g = 5$. In this case, it is known that there are two types of non-hyperelliptic curves; trigonal or not. For the trigonal case, the authors already studied a quintic model in $\mathbb{P}^2$ of a trigonal curve of genus 5 in order to enumerate superspecial ones over small finite fields [8]. Under some assumptions, they presented reductions of quintic forms defining trigonal

*Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo

†Graduate School of Environment and Information Sciences, Yokohama National University.

Keywords: Algebraic curves, Rational points, Curves of genus five, Canonical curves

2010 Mathematical Subject Classification: 14G05, 14G15, 14H10, 14H45, 14H50, 14Q05, 68W30

curves of genus 5, see [8, Section 3] for details. The remaining case is that the curve is canonical and non-trigonal, and it is known that the curve is realized as the complete intersection of three quadratic hypersurfaces in $\mathbb{P}^4$ (cf. [5, Chap. IV, Example 5.5.3 and Exercises 5.5]). As we need so many parameters to give three quadratic forms in 5 variables, it is natural to reduce the parameters by using the natural action by $\mathrm{PGL}_5(K)$. However, it would be hopeless to give an efficient reduction in this way.

In this paper, we give a new effective parameterization of the space of canonical and non-trigonal curves of genus 5. The idea of our parametrization is to consider a projection from the curve in $\mathbb{P}^4$ to $\mathbb{P}^2$ with studying the possible positions of the singular points of the image of the projection. As an application, we propose a method to enumerate such curves over finite fields with many rational points. More precisely, our main contributions are as follows:

(A) In Section 2, we shall prove that any canonical and non-trigonal curve of genus 5 is the normalization of a sextic C' in $\mathbb{P}^2$. The sextic curve may have various kinds of singularities, but in most cases it has five double points. We shall show in Proposition 2.1.3 that the dimension of the space of such curves is 12, which is just(!) the dimension of the moduli space of curves of genus 5. In this paper we treat these sextics with such mild singularities. We say that a curve C of genus 5 is *generic* if it is non-hyperelliptic and non-trigonal, and moreover if its sextic model C' has five double points or has one triple point and two double points. We shall also discuss constraints on the position of singular points in $\mathbb{P}^2$.

(B) Based on the parameterization, in Section 3, we present an algorithm to enumerate *generic* curves C over a finite field K of genus 5 with many rational points. Our algorithm enumerates sextics C' having singular points at a prescribed position in $\mathbb{P}^2$ and computes the number of K'-rational points on C, where K' is a finite extension field of K.

(C) For the case of $K = \mathbb{F}_3$, we shall determine all the possible positions of singular points of C' in Section 4. For each position, we execute the algorithm in (B) with $K' = \mathbb{F}_9$ over MAGMA [1] and [2], where details of computational environment will be described in Section 5. As a computational result, we have the following theorem:

Theorem 1. *The maximal number of $\#C(\mathbb{F}_9)$ of genus-five generic curves C over $\mathbb{F}_3$ is 32. Moreover, there are exactly four $\mathbb{F}_9$-isogeny classes of Jacobian varieties of genus-five generic curves C over $\mathbb{F}_3$ with 32 $\mathbb{F}_9$-rational points, whose Weil polynomials are*

(1) $(t^2 + 2t + 9)(t^2 + 5t + 9)^4$,

(2) $(t + 3)^2(t^4 + 8t^3 + 32t^2 + 72t + 81)^2$,

(3) $(t + 3)^4(t^2 + 2t + 9)(t^2 + 4t + 9)^2$,

(4) $(t + 3)^6(t^2 + 2t + 9)^2$.

In Section 5, examples of generic curves C over $\mathbb{F}_3$ with $\#C(\mathbb{F}_9) = 32$ will be given.

As in the web-site manypoints.org [4], the maximal number of $\#C(\mathbb{F}_9)$ of curves C of genus 5 over $\mathbb{F}_9$ is unknown but is known to belong between 32 and 35 (this upper bound is due to Lauter [11]). On the web-site, three examples of C with 32 $\mathbb{F}_9$-rational points are listed. The above theorem gives at least one new example. More concretely, the Weil polynomial of Fischer's example

$(x^4+1)y^4+2x^3y^3+y^2+2xy+x^4+x^2=0$ is $(t^2+2t+9)(t^2+5t+9)^4$. In fact, this curve appears in our computation, since we obtain a sextic form in $1/x$ and $1/y$ (having distinct 5 singular points) by dividing the example by x^4y^4. The example of Ramos-Ramos [12] (submitted by Ritzenthaler to the site) $y^8=a^2x^2(x^2+a^7)$ with $a^2+a+2=0$ has Weil polynomial $(t+3)^6(t^2+2t+9)^2$. This curve is defined over $\mathbb{F}_9$, but the above theorem found a curve over the prime field $\mathbb{F}_3$ with the same Weil polynomial. Anyway, from this theorem, we see that if one wants to find genus-five curves over $\mathbb{F}_9$ with $\#C(\mathbb{F}_9)>32$, one needs to search those not defined over $\mathbb{F}_3$ or curves whose sextic models have more complex singularities.

Our explicit parametrization and the algorithm presented in this paper may derive fruitful applications both for theory and computation, such as classifying canonical and non-trigonal curves of genus 5 with invariants (Hasse-Witt rank and Ekedahl-Oort type and so on). Some open problems will be summarized in Section 6. One of our future works is to enumerate superspecial generic curves of genus 5 over finite fields.

Acknowledgments

This work was supported by JSPS Grant-in-Aid for Scientific Research (C) 17K05196, and JSPS Grant-in-Aid for Young Scientists 20K14301.

2. Non-hyperelliptic and nontrigonal curves of genus 5

In this section, we study curves of genus 5 which are neither hyperelliptic nor trigonal. In order to parametrize these curves, we propose using the realization of these curves by their sextic models in $\mathbb{P}^2$. This method is much more effective than using the realization by the complete intersection of three quadratic hypersurfaces in $\mathbb{P}^4$.

2.1. Sextic models

Let C be a canonical non-trigonal curve of genus 5, which is known to be realized as $V(\varphi_1,\varphi_2,\varphi_3)$ in $\mathbb{P}^4$ for three quadratic forms φ_1, φ_2 and φ_3 in x_0,x_1,x_2,x_3,x_4. A sextic model associated to C is obtained by additional data: two points P and Q on C. We find a short explanation of this construction in [5, Chap. IV, Example 5.5.3], but that appears away from the context of looking at the space of curves. Here we give an explicit construction toward parametrizing the space of these curves. By a linear transformation, we may assume that

$$P=(1:0:0:0:0) \quad \text{and} \quad Q=(0:0:0:0:1).$$

Since φ_i vanishes at P and Q, the quadratic forms φ_i $(i=1,2,3)$ must be of the form

$$\varphi_i = a_i\cdot x_0x_4 + f_i\cdot x_0 + g_i\cdot x_4 + h_i, \tag{2.1.1}$$

where $a_i\in K$ and f_i and g_i are linear forms in x_1,x_2,x_3 and h_i is a quadratic form in x_1,x_2,x_3. Put

$$(v_1,v_2,v_3) := -(h_1,h_2,h_3)\cdot\Delta_A$$

where Δ_A is the adjugate matrix of

$$A := \begin{pmatrix} a_1 & a_2 & a_3 \\ f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \end{pmatrix}.$$

Since $(v_1, v_2, v_3) = \det(A)(x_0x_4, x_0, x_4)$ on C, the sextic

$$C' : \quad \det(A) \cdot v_1 - v_2v_3 = 0$$

in $\mathbb{P}^2 = \operatorname{Proj} K[x_1, x_2, x_3]$ is birational to C. Here we need to see that $\det A \neq 0$ holds generically. Indeed, if $\det A$ were identically zero, then from (2.1.1) we have $(3 - \mathrm{rank}A)$ quadratic forms only in x_1, x_2, x_3. If $\mathrm{rank}A < 2$, then this contradicts with C is irreducible. If $\mathrm{rank}A = 2$, then let ψ be the quadratic form in x_1, x_2, x_3; then there is a dominant morphism $C \to V(\psi) \subset \mathbb{P}^2$, which turns out to be of degree 2. This contradicts with the assumption that C is not hyperelliptic.

This construction of the sextic C' from C with P and Q is canonical in the following sense:

Proposition 2.1.1. (1) *Suppose $\langle \varphi_1, \varphi_2, \varphi_3 \rangle = \langle \phi_1, \phi_2, \phi_3 \rangle$ as a linear space over a field defining φ_i and ψ_i for all $i = 1, 2$ and 3. Then C' obtained from $\varphi_1, \varphi_2, \varphi_3$ is the same as that obtained from ϕ_1, ϕ_2, ϕ_3.*

(2) *The coordinate change*

$$(x_0, x_1, x_2, x_3, x_4) \mapsto (x_4, x_1, x_2, x_3, x_0)$$

does not change the sextic.

(3) *The coordinate change*

$$(x_0, x_1, x_2, x_3, x_4) \mapsto (x_0 + \phi, x_1, x_2, x_3, x_4 + \psi)$$

with any linear ϕ, ϕ in x_1, x_2, x_3 does not change the sextic.

Proof. (1) Let B be the square matrix of size 3 such that $(\varphi_1, \varphi_2, \varphi_3)B = (\phi_1, \phi_2, \phi_3)$. Let v_i' be v_i associated to ϕ_1, ϕ_2, ϕ_3. Then

$$(v_1', v_2', v_3') = -(h_1, h_2, h_3)B \cdot \det(AB)(AB)^{-1} = \det(B)(v_1, v_2, v_3).$$

Hence we have $\det(AB)v_1' - v_2'v_3' = \det(B)(\det(A)v_1 - v_2v_3)$.

(2) The matrix A for the new coordinate is

$$A' := \begin{pmatrix} a_1 & a_2 & a_3 \\ g_1 & g_2 & g_3 \\ f_1 & f_2 & f_3 \end{pmatrix}.$$

Let v_i' be v_i associated to the new coordinate. It is straightforward to see $(v_1', v_2', v_3') = (-v_1, v_3, v_2)$. Thus the sextic does not change.

(3) Let A', h_i' and v_i' be the matrix A, the quadratic form h_i and v_i for the new coordinate. Then we have

$$A' = \begin{pmatrix} 1 & 0 & 0 \\ \psi & 1 & 0 \\ \phi & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 \\ f_1 & f_2 & f_3 \\ g_1 & g_2 & g_3 \end{pmatrix}$$

and $h_i' = h_i + a_i\phi\psi + f_i\phi + g_j\psi$. The equation $\det(A')v_1' - v_2'v_3' = \det(A)v_1 - v_2v_3$ is derived by a straightforward computation, which is tedious but has some beautiful cancellations. $\square$

From Proposition 2.1.1 (1) and (2), we have

Corollary 2.1.2. *Let K be a field. If C and the divisor $P+Q$ on C for distinct two points P and Q is defined over K, then the associated sextic C' is defined over K.*

This corollary suggests us to use the sextic realization to find/enumerate curves over $\mathbb{F}_q$ of genus 5 with many $\mathbb{F}_{q^2}$-rational points, since the assumption that $P+Q$ is defined over $\mathbb{F}_q$ is satisfied if C has many (a few) $\mathbb{F}_{q^2}$-rational points. The case we mainly treat in this paper is the case of $q=3$. Actually, the maximal number $C(\mathbb{F}_9)$ for curves of genus 5 over $\mathbb{F}_9$ is unknown, as mentioned in Section 1. We give an implementation of our algorithm, restricting ourselves the case that C is defined over $\mathbb{F}_3$.

In general, the curves defined by these sextic forms may have nasty singularities. But in most cases, C' has five singular points with multiplicity 2. The number of monomials of degree 6 in three variables is 28. For each singular point, we have three linear equations which assure that the point is singular . Considering a scalor multiplication to the whole sextic, the number of free parameters is $28-5\times 3-1=12$, see Propositions 2.1.3 and 2.2.2 below for the linear independence of 5×3 linear equations. This is just the dimension of the moduli space of curves of genus 5. This says that the parametrization by the sextic models is very effective.

Proposition 2.1.3. *Let $\{P_1,\dots,P_5\}$ be distinct five points on $\mathbb{P}^2$. Assume that any distinct four points in $\{P_1,\dots,P_5\}$ are not contained in a hyperplane. Then the space of sextics with double points at $P_1,\dots,P_5$ up to scalor multiplications is of dimension* 12.

Proof. We may argue over an algebraically closed field, say K. By a linear transformation by an element of $\mathrm{PGL}_3(K)$, we may assume that $P_1=(1:0:0)$, $P_2=(0:1:0)$ and $P_3=(0:0:1)$. Let $K[x,y,z]$ be the coordinate ring of $\mathbb{P}^2$. Considering the permutation of $\{x,y,z\}$ by the symmetric group of degree 3, we may assume that $P_4=(b:c:1)$ and $P_5=(d:e:1)$, by the assumtion of four points. Then, any sextic with $z=1$ having singularity at P_1, P_2 and P_3 is of the form

$$\begin{aligned}&a_1x^4y^2+a_2x^4y+a_3x^4+a_4x^3y^3+a_5x^3y^2+a_6x^3y+a_7x^3+a_8x^2y^4+a_9x^2y^3+a_{10}x^2y^2\\&+a_{11}x^2y+a_{12}x^2+a_{13}xy^4+a_{14}xy^3+a_{15}xy^2++a_{16}xy+a_{17}y^4+a_{18}y^3+a_{19}y^2.\end{aligned}$$

The condition that this sextic has singularity at P_4 is described in the following way. We substitute $X+b$ for x and $Y+c$ for y and expand the sextic with respect to X and Y. Then, the condition is that the constant term, the coefficiets of X and Y are zero, which makes three linear equations in $a_1,\dots,a_{19}$. For P_5, we have other three linear equations in $a_1,\dots,a_{19}$. The coefficients of these six linear equation makes a 6×19 matrix M. It suffices to show that M is of rank 6. By a direct computation, the determinant of the minor (square matrix of size 6) corresponding to the coefficients of $a_7,a_{11},a_{12},a_{15},a_{18},a_{19}$ is $(be-cd)^5(be+cd)$ and that of $a_6,a_7,a_9,a_{10},a_{11},a_{12}$ is $b^6d^6(c-e)^5$ and that of $a_5,a_{10},a_{14},a_{15},a_{18},a_{19}$ is $c^6e^6(b-d)^5$. If the rank of M were less than 6, then $(be-cd)^5(be+cd)=0$, $b^6d^6(c-e)^5=0$ and $c^6e^6(b-d)^5=0$ has to hold. But this contradicts with the assumtion of four points. Indeed if $b=0$ then we have $c=0$ or $d=0$ by the first equation, and then $P_1=P_4$ holds or P_1,P_3,P_4,P_5 is contained in the hyperplane $y=0$. Thus $b\neq 0$. Similarly c,d and e are not zero. Then we have $b=d$ and $c=e$, which says $P_3=P_4$. This is absurd. Hence M has to be of rank 6. □

2.2. Generic curves of genus 5

As mentioned in the last paragraph of the previous subsection, sextics C' may have various kinds of singularities. It would be natural that we start with the case that the singularity is milder. This paper studies the case that

$$g(C) = \frac{(d-1)(d-2)}{2} - \sum_{P} \frac{m_P(m_P-1)}{2} \tag{2.2.1}$$

holds, where d is the degree of C' in $\mathbb{P}^2$ (i.e., $d = 6$) and m_P is the multiplicity of C' at P. Note that in general the left hand side of (2.2.1) is less than or equal to the right hand side.

Definition 2.2.1. We say that C is *generic* if a sextic model C' associated to $(C, P+Q)$ satisfies (2.2.1). More concretely, there are two cases for generic curves:

(I) C' has five singular points $P_1, \dots, P_5$ with multiplicity two.

(II) C' has one triple point P_1 and two double points P_2 and P_2.

If $(C, P+Q)$ is defined over K, then in case (I) the divisor $P_1 + \cdots + P_5$ is defined over K, and in case (II) the triple point P_1 is defined over K and the divisor $P_2 + P_3$ is defined over K. For example in case (I) the absolute Galois group G_K of K makes permutaions of $\{P_1, \dots, P_5\}$. It is straightforward to see that the patterns of the G_K-orbits in $\{P_1, \dots, P_5\}$ is either of $(1,1,1,1,1)$, $(1,1,1,2)$, $(1,2,2)$, $(1,1,3)$, $(2,3)$, $(1,4)$ and (5), where for example $(1,2,2)$ means that $\{P_1, \dots, P_5\}$ consists of three G_K-orbits each of which has cardinarity 1, 2 and 2 respectively. In Section 4, in the case of $K = \mathbb{F}_3$ we shall give an explict classification of positions of $\{P_1, \dots, P_5\}$ in $\mathbb{P}^2$ up to $\mathrm{PGL}_3(\mathbb{F}_3)$.

Here is another constraint for the position of the singular points.

Proposition 2.2.2. *In case* (I)*, if distinct four elements of* $\{P_1, P_2, P_3, P_4, P_5\}$ *are contained in a hyperplane, then* C' *is geometrically reducible.*

Proof. We may assume that K is algebraically closed. Suppose that $P_1, \dots, P_4$ are contained in a hyperplane. By a linear transformation, we may assume

$$P_1 = (0:0:1), \quad P_2 = (1:0:1), \quad P_3 = (c:0:1), \quad P_4 = (d:0:1)$$

where $0, 1, c$ and d are muturally distinct. Let f be the sextic (in x and p) of C' obtained by substituting 1 for z. Since P_1 is a singular points, the smallest degree of the non-zero terms of f is two. Let a_i be the $x^i y^0$-coefficient of F for $i = 2,3,4,5,6$. Then the constant term and the degree-one term of the Taylor expansion of f at $(x,y) = (b,0)$ are $\sum_{i=2}^{6} b^i a_i$ and $\sum_{i=2}^{6} i b^{i-1} a_i$ for $b \in \{1, c, d\}$. These are zero, as C is singular at P_i for $i = 1, \dots, 5$. Since

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ c^2 & c^3 & c^4 & c^5 & c^6 \\ 2c & 3c^2 & 4c^3 & 5c^4 & 6c^5 \\ d^2 & d^3 & d^4 & d^5 & d^6 \\ 2d & 3d^2 & 4d^3 & 5d^4 & 6d^5 \end{pmatrix} = c^4 d^4 (c-1)^2 (d-1)^2 (c-d)^2,$$

we have that a_i are zero for all $i = 2, \dots, 6$. This says that f is divided by y, in particular C' is geometrically reducible. □

We have a similar result also in case (II):

Proposition 2.2.3. *In case* (II)*, if P_1, P_2 and P_3 are contained in a hyperplane, then C' is geometrically reducible.*

Proof. We may assume that K is algebraically closed. Suppose that P_1, P_1 and P_3 are contained in a hyperplane. By a linear transformation, we may assume

$$P_1 = (0:0:1), \quad P_2 = (1:0:1), \quad P_3 = (c:0:1)$$

where 0, 1 and c are muturally distinct. Let f be the sextic (in x and p) of C' obtained by substituting 1 for z. Since P_1 is a triple point, the smallest degree of the non-zero terms of f is three. Let a_i be the $x^i y^0$-coefficient of F for $i = 3,4,5,6$. Then the constant term and the degree-one term of the Taylor expansion of f at $(x,y) = (b,0)$ are $\sum_{i=3}^{6} b^i a_i$ and $\sum_{i=3}^{6} i b^{i-1} a_i$ for $b \in \{1, c\}$. These are zero, as C is singular at P_i for $i = 1, \ldots, 5$. Since

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 4 & 5 & 6 \\ c^2 & c^3 & c^4 & c^5 \\ 2c & 3c^2 & 4c^3 & 5c^4 \end{pmatrix} = c^6(c-1)^4,$$

we have that a_i is zero for all $i = 3, \ldots, 6$. This says that f is divided by y, in particular C' is geometrically reducible. □

Finally we give a remark about the number of rational points on a generic curve C over finite field $\mathbb{F}_q$. As the singularity of C is very mild, we have the following formula

$$\#C(\mathbb{F}_q) = \#C'(\mathbb{F}_q) + \sum_{P \in C'(\mathbb{F}_q)} \left(\#V(h_P)(\mathbb{F}_q) - 1\right), \tag{2.2.2}$$

where h_P is the homogeneous part of the least degree (i.e., m_P) of the Taylor expansion at P of an affine model containing P of the sextic defining C' and $V(h_P)$ is the closed subscheme of $\mathbb{P}^1$ defined by the ideal (h_P). If h_P is quadratic, then $\#V(h_P)(\mathbb{F}_q) - 1$ is equal to 1 if the discriminant $\Delta(h_P)$ of h_P is nonzero square and to -1 if $\Delta(h_P)$ is nonzero non-square and to 0 if $\Delta(h_P) = 0$. From a computational point of view, it may have a little advantage to use the fact that if $q = p^2$ and $\Delta(h_P)$ belongs to $\mathbb{F}_p$, then $\Delta(h_P) \neq 0$ is equivalent to that $\Delta(h_P)$ is nonzero square in $\mathbb{F}_{p^2}$.

3. Concrete Algorithm

Let K be a finite field with characteristic p, and K' a finite extension field of K. As it was shown in Subsection 2.1, any canonical non-trigonal curve of genus 5 over K is realized as the normalization of a sextic in $\mathbb{P}^2$. In particular, such a curve C is said to be generic if it satisfies either of the conditions (I) or (II) stated in Definition 2.2.1 of Subsection 2.2.

In this section, we first present a concrete algorithm (Algorithm 3.1.1 below) to enumerate all generic curves C of genus 5 over K satisfying (I) and $\#C(K') \geq N$, where N is a given positive integer. Similarly to (I), we can construct an algorithm for (II), but we omit to write down it in this paper. After presenting the algorithm for (I), we also give some remarks for implementation.

3.1. Algorithm for the case (I)

Let $\{P_1, P_2, P_3, P_4, P_5\}$ be a set of distinct five points in $\mathbb{P}^2(L)$, where L is a finite extension field of K. Assume that $\mathrm{Gal}(L/K)$ stabilizes the set $\{P_1, P_2, P_3, P_4, P_5\}$. Given $\{P_1, P_2, P_3, P_4, P_5\}$ and an integer $N \geq 1$, Algorithm 3.1.1 below enumerates all sextic forms F in $K[x, y, z]$ such that $C' : F = 0$ is a singular (irreducible) curve of geometric genus 5 in $\mathbb{P}^2$ with $\mathrm{Sing}(C') = \{P_1, P_2, P_3, P_4, P_5\}$ and $\#C(K') \geq N$, where C is the normalization of C'.

Algorithm 3.1.1. *Input.* $\{P_1, P_2, P_3, P_4, P_5\}$ and $N \geq 1$.
Output. A set $\mathcal{F}$ of sextic forms in $K[x, y, z]$.

(1) Set $\mathcal{F} := \emptyset$.

(2) Construct $F = \sum_{i=1}^{28} a_i x^{\alpha_1^{(i)}} y^{\alpha_2^{(i)}} z^{\alpha_3^{(i)}} \in K[a_1, \ldots, a_{28}][x, y, z]$ with

$$\{(\alpha_1^{(1)}, \alpha_2^{(1)}, \alpha_3^{(1)}), \ldots, (\alpha_1^{(28)}, \alpha_2^{(28)}, \alpha_3^{(28)})\} = \{(\alpha_1, \alpha_2, \alpha_3) \in (\mathbb{Z}_{\geq 0})^{\oplus 3} : \alpha_1 + \alpha_2 + \alpha_3 = 6\},$$

where $a_1, \ldots, a_{28}$ are indeterminates.

(3) For each $\ell \in \{1, \ldots, 5\}$:

  (a) Write $P_\ell = (p_1 : p_2 : p_3)$ for $p_1, p_2, p_3 \in L$.
  (b) Let k be the minimal element in $\{1, 2, 3\}$ such that $p_k \neq 0$, and put $z_k = p_k$, $z_i = X$ and $z_j = Y$ for $i, j \in \{1, 2, 3\} \smallsetminus \{k\}$ with $i < j$.
  (c) Compute $F_\ell := F(z_1, z_2, z_3) \in L[a_1, \ldots, a_{28}][X, Y]$. Let f_ℓ and $f_{\ell+1}$ be the coefficients of X and Y in F_ℓ respectively, and $f_{\ell+2}$ the constant term of F_ℓ as a polynomial in X, Y.

(4) Compute a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\} \subset K^{\oplus 28}$ of the null-space of the linear system over L defined by $f_t(a_1, \ldots, a_{28}) = 0$ for $1 \leq t \leq 15$, where d is the dimension of the null-space. By Proposition 2.1.3 we have $d = 12$.

(5) For each $(v_1, \ldots, v_d) \in K^{\oplus d} \smallsetminus \{(0, \ldots, 0)\}$ with $v_1 \in \{0, 1\}$:

  (a) Compute $\mathbf{c} := \sum_{j=1}^{d} v_j \mathbf{b}_j \in K^{\oplus 28} \smallsetminus \{(0, \ldots, 0)\}$. For each $1 \leq i \leq 28$, we denote by c_i the i-th entry of $\mathbf{c}$.
  (b) If $\sum_{i=1}^{28} c_i x^{\alpha_1^{(i)}} y^{\alpha_2^{(i)}} z^{\alpha_3^{(i)}} \in K[x, y, z]$ is irreducible, and if $\sum_{i=1}^{28} c_i x^{\alpha_1^{(i)}} y^{\alpha_2^{(i)}} z^{\alpha_3^{(i)}} = 0$ in $\mathbb{P}^2$ has geometric genus 5:
    (i) Set $F_{\mathbf{c}} := \sum_{i=1}^{28} c_i x^{\alpha_1^{(i)}} y^{\alpha_2^{(i)}} z^{\alpha_3^{(i)}}$, and let C' be the plane curve in $\mathbb{P}^2$ defined by $F_{\mathbf{c}} = 0$.
    (ii) Compute $\#C(K')$ by the formula (2.2.2) given in Subsection 2.2, where C is the normalization of C'.
    (iii) If $\#C(K') \geq N$, replace $\mathcal{F}$ by $\mathcal{F} \cup \{F_{\mathbf{c}}\}$.

(6) Output $\mathcal{F}$.

Remark 3.1.2. (1) We can take a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$ in Step (4) so that $\mathbf{b}_i \in K^{\oplus 28}$ for all $1 \leq i \leq d$, by the following general fact: Let E/K be a separable extension of fields, and L the Galois closure of E over K. If a linear system over E is $\mathrm{Gal}(L/K)$-stable, then each entry of the Echelon form of the coefficient matrix of the system belongs to K.

(2) In Step (5)(b)(ii), we need to compute the discriminant Δ_ℓ of the degree-2 part of the Taylor expansion of $F_{\mathbf{c}}$ at each P_ℓ. For this, we can use F_ℓ computed in Step (3) as follows: Let $D_\ell \in K[a_1, \ldots, a_{28}]$ denote the discriminant of the degree-2 part of F_ℓ as a polynomial in X and Y. Then clearly we have $\Delta_\ell = D_\ell(\mathbf{c})$.

3.2. Correctness of our algorithm and remarks for implementation

The correctness of Algorithm 3.1.1 follows mainly from the definition of the multiplicity of a projective plane curve at a singular point: Indeed, each polynomial F_ℓ computed in Step (3) is equal to the Taylor expansion of F at P_ℓ. Since any vector $\mathbf{c}$ defining $F_{\mathbf{c}}$ in Step (5)(b)(i) is a root of the system $f_\ell = f_{\ell+1} = f_{\ell+2} = 0$ for all $1 \leq \ell \leq 5$, we have that P_ℓ is a singular point of $C' : F_{\mathbf{c}} = 0$ with multiplicity 2 for each $1 \leq \ell \leq 5$. Conversely, we suppose that $\mathbf{c}$ is a vector in $K^{\oplus 28} \smallsetminus \{(0, \ldots, 0)\}$ such that $F_{\mathbf{c}} = 0$ is an irreducible plane curve of geometric genus 5 with multiplicity 2 at the points $P_1, \ldots, P_5$. By the definition of the multiplicity of a singularity, the vector $\mathbf{c}$ is a root of the system $f_\ell = f_{\ell+1} = f_{\ell+2} = 0$ for all $1 \leq \ell \leq 5$. As it was described in Remark 3.1.2 (1), each entry of the Echelon form of the coefficient matrix of the system belongs to K, and thus $\mathbf{c}$ is a root of a linear system over K whose null-space over L is the same as that of $f_\ell = f_{\ell+1} = f_{\ell+2} = 0$ for all $1 \leq \ell \leq 5$. Hence $\mathbf{c}$ is written as $\mathbf{c} = \sum_{j=1}^{d} v_j \mathbf{b}_j$ for some $(v_1, \ldots, v_d) \in K^{\oplus d} \smallsetminus \{(0, \ldots, 0)\}$. Note that it suffices to compute the part with $v_1 \in \{0, 1\}$, because any scalor multiplication does not change the isomorphism class of the sextic.

We implemented Algorithm 3.1.1 and its variant for the case (II) over MAGMA V2.25-8 [1], [2] in its 64-bit version. Details of our computational environment will be described in Section 5. For Step (5)(b), our implementation utilizes MAGMA's built-in functions `IsIrreducible`, `GeometricGenus` and `Variety`. In particular, we use `Variety` to compute $\#C'(K') = \#V(F_{\mathbf{c}})$.

4. Position analysis for $\mathbb{F}_3$

In this section, we classify positions of five (resp. three) points in $\mathbb{P}^2$ which can be singular points of a generic curve C' over $\mathbb{F}_3$ in the case (I) (resp. in the case (II)), up to the action by $\mathrm{PGL}_3(\mathbb{F}_3)$. In each case, this is the problem to enumerate the orbits of an action of a finite group on a finite set. As this is done by a computer calculation (with MAGMA), we state only the results.

4.1. Case (I): C' has five double points

The Frobenius map over $\mathbb{F}_3$ makes a permutaion of $\{P_1, \ldots, P_5\}$. The patterns of the Frobenis orbits in $\{P_1, \ldots, P_5\}$ is either of $(1,1,1,1,1)$, $(1,1,1,2)$, $(1,2,2)$, $(1,1,3)$, $(2,3)$, $(1,4)$ and (5), where for example $(1,2,2)$ means that $\{P_1, \ldots, P_5\}$ consists of three Frobenius orbits each of which has cardinarity 1, 2 and 2 respectively.

Case (1,1,1,1,1): This is the case where every singular point is $\mathbb{F}_3$-rational. By a linear transformation of an element of $\mathrm{PGL}_3(\mathbb{F}_p)$, we may assume

$$P_1 = (1 : 0 : 0), \quad P_2 = (0 : 1 : 0), \quad P_3 = (0 : 0 : 1).$$

A computation shows that every position of $\{P_1, \ldots, P_5\}$ such that any four points among them are not contained in a hyperplane is equivalent by a linear transformaion of a diagonal matrix and a permutation of $\{x, y, z\}$ to either of the following two cases:

(1) $P_4 = (1 : 1 : 0)$ and $P_5 = (0 : 1 : 1)$,

(2) $P_4 = (1:1:0)$ and $P_5 = (1:2:1)$.

Example 4.1.1. In characteristic 3, the defining equation of any sextic having singluar points $P_1 = (0:0:1)$, $P_2 = (0:1:0)$, $P_3 = (1:0:0)$ $P_4 = (1:1:0)$, $P_5 = (0:1:1)$ is

$$\begin{aligned}&a_1x^4y^2 + a_2x^4yz + a_3x^4z^2 + a_4x^3y^3 + a_5x^3y^2z + a_6x^3yz^2 + a_7x^3z^3\\&+a_8x^2y^4 + a_9x^2y^3z + a_{10}x^2y^2z^2 + a_{11}x^2yz^3 + a_{12}x^2z^4 + a_{13}xy^4z\\&+a_{14}xy^3z^2 + a_{15}xy^2z^3 + a_{16}xyz^4 + a_{17}y^4z^2 + a_{18}y^3z^3 + a_{19}y^2z^4\end{aligned}$$

with

$$\begin{cases} a_1 + a_4 + a_8 = 0, \\ 2a_1 + a_8 = 0, \\ a_2 + a_5 + a_9 + a_{13} = 0, \end{cases} \qquad \begin{cases} a_{17} + a_{18} + a_{19} = 0, \\ a_{13} + a_{14} + a_{15} + a_{16} = 0, \\ a_{17} + 2a_{19} = 0. \end{cases}$$

The quadratic form assosiated to the singular point P_i (of multiplicity 2) is as follows:

$$\begin{aligned}Q_1 &:= a_{12}x^2 + a_{16}xy + a_{19}y^2,\\Q_2 &:= a_8x^2 + a_{13}xz + a_{17}z^2,\\Q_3 &:= a_1y^2 + a_2yz + a_3z^2,\\Q_4 &:= a_1(y-x)^2 + (a_2 + 2a_5 + a_{13})(y-x)z + (a_3 + a_6 + a_{10} + a_{14} + a_{17})z^2,\\Q_5 &:= (a_8 + a_9 + a_{10} + a_{11} + a_{12})x^2 + (a_{13} + 2a_{14} + a_{16})x(y-z) + a_{17}(y-z)^2\end{aligned}$$

respectively.

Case (1,1,1,2) with linear independent P_1, P_2, P_3: We consider the case where $\{P_1, \dots, P_5\}$ contains three $\mathbb{F}_p$-rational points, say P_1, P_2, P_3, where P_1, P_2, P_3 are linearly indepenent, and the other points are defined over $\mathbb{F}_{p^2}$ (not over $\mathbb{F}_p$) and are conjugate to each other, i.e., $(P_4, P_5) = (P_4, \sigma(P_4))$, where σ is the Frobenius map (taking p-th power of each entry). By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_p)$, we may assume

$$P_1 = (1:0:0), \quad P_2 = (0:1:0), \quad P_3 = (0:0:1).$$

Let ζ be a primitive element of $\mathbb{F}_{p^2}$. A computation shows that every position of $\{P_1, \dots, P_5\}$ such that any four points among them are not contained in a hyperplane is equivalent by a linear transformaion of a diagonal matrix and a permutation of $\{x, y, z\}$ to either of the three cases:

(1) $P_4 = (1 : \zeta^5 : \zeta^7)$,

(2) $P_4 = (1 : \zeta^7 : 1)$,

(3) $P_4 = (1 : \zeta^2 : \zeta^2)$.

with $P_5 = \sigma(P_4)$.

Case (1,1,1,2) with linear dependent P_1, P_2, P_3: We consider the case where $\{P_1, P_2, P_3, P_4, P_5\}$ contains three $\mathbb{F}_p$-rational points, say P_1, P_2, P_3, where P_1, P_2, P_3 are linearly depenent, and the other points are defined over $\mathbb{F}_{p^2}$ and are conjugate to each other.

By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_p)$, we may assume

$$P_1 = (1:0:0), \quad P_2 = (0:1:0), \quad P_3 = (1:1:0).$$

Let ζ be a primitive element of $\mathbb{F}_{p^2}$. We have three equivalent classes:

(1) $P_4 = (1 : \zeta^5 : \zeta^7)$,

(2) $P_4 = (1 : 1 : \zeta^7)$,

(3) $P_4 = (1 : \zeta^2 ; \zeta^2)$

with $P_5 = \sigma(P_4)$.

Case (1,2,2): We consider the case where $\{P_1, P_2, P_3, P_4, P_5\}$ contains one $\mathbb{F}_p$-rational point P_1 and two pairs (P_2, P_3) and (P_4, P_5) of $\mathbb{F}_{p^2}$-rational points, where $P_3 = \sigma(P_2)$ and $P_5 = \sigma(P_4)$. By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_p)$, we may assume

$$P_1 = (1 : 0 : 0).$$

Let ζ be a primitive element of $\mathbb{F}_{p^2}$. We have five equivalent classes:

(1) $(P_2, P_4) = ((1 : 1 : \zeta^2), (0 : 1 : \zeta^6))$,

(2) $(P_2, P_4) = ((1 : 2 : \zeta^5), (1 : \zeta^2 : \zeta^7))$,

(3) $(P_2, P_4) = ((1 : \zeta : 1), (1 : \zeta^7 : \zeta^7))$,

(4) $(P_2, P_4) = ((1 : \zeta^2 : \zeta^6), (1 : 0 : \zeta^5))$,

(5) $(P_2, P_4) = ((1 : 0 : \zeta^2), (1 : 1 : \zeta^5))$.

Case (1,1,3): We consider the case where $\{P_1, P_2, P_3, P_4, P_5\}$ contains two $\mathbb{F}_p$-rational points P_1, P_2 and conjugate three points (P_3, P_4, P_5) of $\mathbb{F}_{p^3}$-rational points, where

$$(P_3, P_4, P_5) = (P_3, \sigma(P_3), \sigma^2(P_3)).$$

By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_p)$, we may assume

$$P_1 = (1 : 0 : 0), \quad P_2 = (0 : 1 : 0).$$

Let ζ be a primitive element of $\mathbb{F}_{p^3}$. We have four cases

(1) $P_3 = (1 : 2 : \zeta^5)$,

(2) $P_3 = (1 : \zeta^6 : \zeta^{25})$,

(3) $P_3 = (1 : \zeta^{17} : \zeta^2)$,

(4) $P_3 = (1 : 2 : \zeta^{10})$.

Case (2,3): We consider the case where $\{P_1, P_2, P_3, P_4, P_5\}$ contains conjugate two points (P_1, P_2) of $\mathbb{F}_{p^2}$-rational points with $(P_1, P_2) = (P_1, \sigma(P_2))$ and conjugate three points (P_3, P_4, P_5) of $\mathbb{F}_{p^3}$-rational points, where $(P_3, P_4, P_5) = (P_3, \sigma(P_3), \sigma^2(P_3))$. By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_p)$, we may assume

$$P_1 = (1 : \xi : 0)$$

where ξ is a primitive element of $\mathbb{F}_{p^2}$. Let ζ be a primitive element of $\mathbb{F}_{p^3}$. We have three cases:

(1) $P_3 = (1 : 2 : \zeta^5)$,

(2) $P_3 = (1 : \zeta^{22} : 2)$,

(3) $P_3 = (1 : \zeta^{17} : \zeta^2)$.

Case (1,4): We consider the case where $\{P_1, P_2, P_3, P_4, P_5\}$ contains one $\mathbb{F}_3$-rational point P_1 and the other 4 points are over $\mathbb{F}_{3^4}$ and are conjugate to each other, say

$$(P_2, P_3, P_4, P_5) = (P_2, \sigma(P_2), \sigma^2(P_2), \sigma^3(P_2)).$$

By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_3)$, we may assume $P_1 = (1 : 0 : 0)$. Let ζ be a primitive element of $\mathbb{F}_{3^4}$. We have five equivalent classes:

(1) $P_2 = (1 : \zeta^{75} : \zeta^{49})$,

(2) $P_2 = (1 : \zeta^8 : \zeta^{70})$,

(3) $P_2 = (1 : \zeta^{59} : \zeta^{53})$,

(4) $P_2 = (1 : \zeta^{72} : \zeta^{29})$,

(5) $P_2 = (1 : \zeta^5 : \zeta^{75})$.

Case (5): This is the case where singular points on C' are defined over $\mathbb{F}_{3^5}$ (but not over $\mathbb{F}_3$). Then $\{P_1, \ldots, P_5\}$ consists of a single Frobenius orbit, namely

$$\{P_1, P_2, P_3, P_4, P_5\} = \{P_1, \sigma(P_1), \sigma^2(P_1), \sigma^3(P_1), \sigma^4(P_1)\}.$$

In this case, the five points are determined only by P_1. A computation says that there are two cases:

(1) $P_1 = (1 : \zeta^{127} : \zeta^{143})$,

(2) $P_1 = (1 : \zeta^{218} : \zeta^{72})$

for a primitive element ζ of $\mathbb{F}_{3^5}$.

4.2. Case (II): C' has one triple point with two double points

We consider sextics C' with singular points consisting of one triple point and two double points. The single triple point should be defined over $\mathbb{F}_3$. Let P_1 be the triple point. By a tranformation by an element of $\mathrm{PGL}_3(\mathbb{F}_3)$, we may assume

$$P_1 = (0 : 0 : 1).$$

The patterns of the Frobenius orbits of the two remaining double points $\{P_2, P_3\}$ are $(1, 1)$ and (2).

Case (1,1): This is the case where C' has one triple point with two $\mathbb{F}_3$-rational double points. Up to actions by elements of $\mathrm{PGL}_3(\mathbb{F}_3)$ stabilizing P_1, we have a unique case:

$$P_2 = (1:0:0), \qquad P_3 = (0:1:0).$$

Up to actions by elements of $\mathrm{PGL}_3(\mathbb{F}_3)$ stabilizing P_1 and $\{P_2, P_3\}$, we may assume that F is of the form

$$F = b_1 x^3 z^3 + b_2 x^2 y z^3 + b_3 x^3 y^3 + \text{other terms}$$

with $b_1, b_2, b_3 \in \{0, 1\}$ and $(b_1, b_2) \neq (0, 0)$.

Case (2): This is the case where C' has one triple point with two $\mathbb{F}_9$-rational double points. Up to actions by elements of $\mathrm{PGL}_3(\mathbb{F}_3)$ stabilizing P_1, we have a unique case:

$$P_2 = (1:\zeta:0), \qquad P_3 = (1:\zeta^3:0),$$

where ζ is the primitive element of $\mathbb{F}_9$ satisfing $\zeta^2 - \zeta - 1 = 0$. Up to actions by elements of $\mathrm{PGL}_3(\mathbb{F}_3)$ stabilizing P_1 and $\{P_2, P_3\}$, we may assume that F is of the form

$$F = b_1 x^3 z^3 + b_2 x^2 y z^3 + b_3 x^3 y^3 + \text{other terms}$$

with $b_1 = 1$ and $b_2, b_3 \in \{0, 1\}$.

5. Computational results with explicit equations in characteristic 3

For $K = \mathbb{F}_p$ and $K' = \mathbb{F}_{p^2}$ with $p = 3$, we executed Algorithm 3.1.1 for (I) and its variant for (II) over MAGMA V2.25-8 [1] and [2] in each case given in Section 4, in order to prove Theorem 1. We choose $N = 32$ as the input, since 32 is the maximal number among the known numbers of $\mathbb{F}_9$-rational points of genus-five curves over $\mathbb{F}_9$. Our implementations over MAGMA were run on a PC with ubuntu 18.04.5 LTS OS at 3.50GHz quadcore CPU (Intel(R) Xeon(R) E-2224G) and 64GB RAM. It took about 58 hours in total to execute the algorithms for obtaining Theorem 1. For curves C with $\#C(\mathbb{F}_{p^2}) \geq 32$ listed up, we also computed their Weil polynomials with MAGMA. We have also obtained explicit equations of generic curves of genus 5 over $\mathbb{F}_3$ with 32 $\mathbb{F}_9$-rational points. Here, we show some examples:

(1) Case $(1,1,1,1,1)$ with $P_5 = (1:2:1)$. The sextic

$$F = x^4y^2 + x^3y^3 + x^2y^4 + x^4yz + x^3y^2z + 2x^2y^3z + 2xy^4z + 2x^2yz^3 + xy^2z^3 + x^2z^4 + 2xyz^4 + y^2z^4$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial $(t+3)^6(t^2+2t+9)^2$.

(2) Case $(1,1,1,2)$ with linearly independent P_1, P_2, P_3 where $P_4 = (1:\zeta^2:\zeta^2)$. The sextic

$$F = x^2y^4 + x^4yz + 2y^4z^2 + x^2z^4 + 2y^2z^4$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial $(t^2+2t+9)(t^2+5t+9)^4$.

(3) Case $(1,1,1,2)$ with linearly dependent P_1, P_2, P_3 where $P_4 = (1:\zeta^5:\zeta^7)$. The sextic

$$\begin{aligned} F \;=\;& x^4y^2 + x^3y^3 + x^2y^4 + 2x^3y^2z + xy^4z + x^2y^2z^2 + 2xy^3z^2 + 2x^3z^3 \\ & + 2y^3z^3 + x^2z^4 + 2xyz^4 + 2y^2z^4 + z^6 \end{aligned}$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial $(t+3)^4(t^2+2t+9)(t^2+4t+9)^2$.

(4) Case $(1,2,2)$ with $P_2 = (1 : 2 : \zeta^5)$ and $P_4 = (1 : \zeta^2 : \zeta^7)$. The sextic

$$\begin{aligned} F &= x^4y^2 + 2x^3y^3 + 2xy^5 + 2y^6 + x^2y^3z + 2y^5z + 2x^4z^2 + x^3yz^2 + xy^3z^2 \\ &\quad +2x^3z^3 + x^2yz^3 + xyz^4 + y^2z^4 + 2xz^5 + 2yz^5 + z^6 \end{aligned}$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial $(t+3)^2(t^4 + 8t^3 + 32t^2 + 72t + 81)^2$.

(5) Case $(1,1,3)$ with $P_3 = (1 : 2 : \zeta^5)$. The sextic

$$\begin{aligned} F &= x^4y^2 + x^2y^4 + x^4yz + 2xy^4z + 2x^4z^2 + 2x^3yz^2 + x^2y^2z^2 + 2xy^3z^2 + 2y^4z^2 + 2x^3z^3 \\ &\quad +2x^2yz^3 + xy^2z^3 + y^3z^3 + 2x^2z^4 + xyz^4 + 2y^2z^4 + xz^5 + 2yz^5 + 2z^6 \end{aligned}$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial $(t^2 + 2t + 9)(t^2 + 5t + 9)^4$.

(6) Case $(2,3)$ with $P_1 = (1 : \xi : 0)$ and $P_3 = (1 : 2 : \zeta^5)$. The sextic

$$\begin{aligned} F &= x^5y + x^4y^2 + 2x^2y^4 + 2y^6 + x^5z + x^4yz + 2x^3y^2z + 2x^3yz^2 + x^2y^2z^2 + x^3z^3 \\ &\quad +2x^2yz^3 + xy^2z^3 + 2x^2z^4 + xyz^4 + 2y^2z^4 + xz^5 + z^6 \end{aligned}$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial $(t^2 + 2t + 9)(t^2 + 5t + 9)^4$.

6. Concluding remarks with some open problems

We provided a new effective parameterization of the space of canonical and non-trigonal curves of genus 5. We realized such a curve as the normalization of a sextic in $\mathbb{P}^2$. It was also proved that if the associated sextic model has five double pounts, the dimension of the space of such curves is 12, which is just(!) the dimension of the moduli space of curves of genus 5. As an application, we also presented an algorithm to enumerate generic curves of genus 5 over finite fields with many rational points. By executing the algorithm over MAGMA, we showed that the maximal number of $\mathbb{F}_9$-rational points of generic curves of genus 5 over $\mathbb{F}_3$ is 32.

Our explicit parametrization and the algorithm presented in this paper may derive fruitful applications both for theory and computation, such as classifying possible invariants (Hasse-Witt rank and so on) of canonical and non-trigonal curves of genus 5. Finally, we list some considerable open problems:

(a) Extend the parameterization to the case where curves have more complex singularities. Concretely, present a parameterization of non-hyperelliptic and non-trigonal curves C of genus 5 such that the equality (2.2.1) in Subsection 2.2 does not hold. A more general problem is to give an explicit model in $\mathbb{P}^2$ of non-hyperelliptic curves of the other genus ≥ 4. Cf. a parameterization of generic curves of genus 3 is presented in [13], where an equation with 6 parameters (the moduli dimension is also 6) is given.

(b) Present methods to compute invariants of generic curves of genus 5 such as Cartier-Manin and Hasse-Witt matrices. If we can compute Cartier-Manin and Hasse-Witt matrices, we can determine whether given curves are superspecial or not, as in [6], [7], [8] and [9]. For computing Cartier-Manin matrices, we may apply a method in [14] for a plane curve.

(c) Construct an algorithm to test whether given two generic curves of genus 5 are isomorphic or not. Computing the automorphism group of such a curve is also an interesting problem. Cf. for the case of genus-4 non-hyperelliptic curves, the authors (resp. the authors and Senda) already presented an algorithm for the isomorphism test (resp. for computing automorphism groups), see [9] (resp. [10]).

(d) Improve the efficiency of Algorithm 3.1.1 and its variant for the case (II), and then enumerate generic curves of genus 5 with many rational points for $p > 3$. For this, it important to reduce the number of curves C which we need to search.

References

[1] Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**, 235–265 (1997)

[2] Cannon, J., et al.: *Magma A Computer Algebra System*, School of Mathematics and Statistics, University of Sydney, 2016. `http://magma.maths.usyd.edu.au/magma/`

[3] van der Geer, G. and van der Vlugt, M.: *Tables of curves with many points*, Math. Comp. **69** (2000), no. 230, 797–810.

[4] van der Geer, et al.: *Tables of Curves with Many Points*, 2009, `http://www.manypoints.org`, Retrieved at 13th February, 2021.

[5] Hartshorne, R.: *Algebraic Geometry*, GTM **52**, Springer-Verlag (1977)

[6] Kudo, M. and Harashita, S.: *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields and Their Applications **45**, 131–169 (2017)

[7] 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, Lecture Notes in Computer Science, Vol. **11321**, pp. 58–73, Springer, Cham, 2018, (DOI) 10.1007/978-3-030-05153-2_3.

[8] Kudo, M. and Harashita, S.: *Superspecial trigonal curves of genus* 5. Experimental Mathematics, Published online: 16 Apr 2020. (DOI) 10.1080/10586458.2020.1723745 (preprint ver: arXiv:1804.11277 [math.AG]).

[9] Kudo, M. and Harashita, S.: *Computational approach to enumerate non-hyperelliptic superspecial curves of genus* 4, Tokyo Journal of Mathematics, Vol. **43**, Number 1, pp. 259–278, 2020, doi:10.3836/tjm/1502179310.

[10] Kudo, M., Harashita, S. and Senda, S.: *Automorphism groups of superspecial curves of genus* 4 *over* $\mathbb{F}_{11}$, Journal of Pure and Applied Algebra, Vol. **224**, Issue 9, 2020, (DOI) 10.1016/j.jpaa.2020.106339.

[11] Lauter, K. E.: *Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields*, Journal of Algebraic Geometry **10** (2001), no. 1, 19–36.

[12] Andrade Ramos, C. and Garzón Ramos, A.: *Polynomials with a restricted range and curves with many points.* Rev. Acad. Colomb. Cienc. **34** (131): 229–239, 2010.

[13] Shaska, T. and Thompson, J. T.: *On the generic curve of genus 3*, Communications in Contemporary Mathematics **369**, 233–243, 2005, DOI: 10.1090/conm/369/06814

[14] Stöhr, K.-O. and Voloch, J. F.: *A formula for the Cartier operator on plane algebraic curves*, J. Reine Angew. Math. **377** (1987), 49–64.

E-mail address of the first author: `kudo@mist.i.u-tokyo.ac.jp`
E-mail address of the second author: `harasita@ynu.ac.jp`