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

Momonari Kudo\textsuperscript{1} and Shushi Harashita\textsuperscript{2}

\textsuperscript{1}The University of Tokyo
\textsuperscript{2}Yokohama National University

June 10\textsuperscript{th} 2021

MEGA2021: Effective Methods in Algebraic Geometry

Our paper is available at arXiv: 2102.07270 [math.AG].
Outline

1. Introduction

Throughout this talk, a “curve” means a non-singular and geometrically irreducible projective variety of dimension one, unless otherwise noted.
Motivation

- **Parametrizing the space of curves of given genus**
  - This is a very basic and classical problem in the theory of algebraic curves.
  - We consider to parameterize the space of curves by an explicit equation.
  - It is desirable that the number of parameters is equal or close to the dimension of the space.
  - In this talk, such a parameterization is said to be effective.

- **Hyperelliptic case is well-known, but non-hyperelliptic case is...**
  - Any hyperelliptic curve of genus $g$ is given by
    \[ y^2 = f(x) \]
    with $\deg f(x) = 2g + 1$ or $2g + 2$, where $g$ is the genus.
  - How about the non-hyperelliptic case for $g \geq 3$?
    - **Note:** Any curve of genus $g = 1, 2$ is hyperelliptic.
Some known parameterizations in genus $g = 3, 4$

- **Genus 3: Canonically embedded into $\mathbb{P}^2$**
  - Bergström proved that a canonical curve of genus 3 over a field admitting a rational point over a field of characteristic $\neq 2, 3$ is given by a quartic with 7 parameters (cf. the moduli dimension is 6).
  - See Proposition 3.7 of the following paper for details.
    

- **Genus 4: Canonically embedded into $\mathbb{P}^3$**
  - Complete intersection $V(Q, P)$ of a quadratic $V(Q)$ and a cubic $V(P)$
  - The authors gave an effective parametrization of the space of $V(Q, P)$’s
    
Our contribution

- For $g = 5$, we present an effective parameterization:
  
  (A) We prove that any non-hyperelliptic and non-trigonal curve $C$ of genus 5 is the desingularization of a sextic $C'$ in $\mathbb{P}^2$ (in most cases $C'$ has five double points). We need 12 parameters to describe $C'$ having fixed five double points, where 12 is just the dimension of their moduli space. Very effective!

  (B) Based on the parametrization, we present an algorithm to enumerate \emph{generic} (defined in a slide below) curves of genus 5 over $\mathbb{F}_q$ with many rational points.

  (C) For $K = \mathbb{F}_3$, we determine all the possible positions of singular points of $C'$. For each position, we executed the algorithm given in (B) over MAGMA. We obtain curves over $K$ with many $\mathbb{F}_9$-rational points.
Outline

1. Introduction

2. Non-hyperelliptic and non-trigonal curves of genus 5

3. Algorithm to enumerate genus-5 generic curves over finite fields with many rational points

4. Position analysis for $\mathbb{F}_3$ and computational results with explicit equations in characteristic 3

5. Concluding remark
Curves of genus 5

• **Hyperelliptic curve:**
  \[ y^2 = f(x) \]
  with \( \deg f(x) = 11, 12 \).

• **Trigonal curve \( C \):**
  By definition, there exists a dominant morphism
  \[ C \to \mathbb{P}^1 \]
  of degree 3.
  **A realization:** the desingularization of a *quintic* in \( \mathbb{P}^2 \)
  with a single singular point of multiplicity two.

  M. Kudo and S. Harashita: *Superspecial trigonal curves of genus 5*,
  Experimental Mathematics, Published online: 16 Apr. 2020.

• **The other case (non-hyperelliptic and non-trigonal)**
  In this case, complete intersection \( V(\varphi_1, \varphi_2, \varphi_3) \)
  of three quadratic forms \( \varphi_1, \varphi_2, \varphi_3 \) in \( \mathbb{P}^4 \).
Non-hyperelliptic and non-trigonal curves

- The complete intersection in $\mathbb{P}^4$:
  \[ C = V(\varphi_1, \varphi_2, \varphi_3), \]
  where $\varphi_i \ (i = 1, 2, 3)$ are quadratic forms.

- Sextic model:
  From the complete intersection above with a divisor $P + Q$ for two distinct points $P$ and $Q$ on $C$, a “projection” using $P + Q$ from $\mathbb{P}^4$ to $\mathbb{P}^2$, we can construct a sextic form $F$ in 3 variables so that
  \[ C' = V(F) \]
  in $\mathbb{P}^2$ is birational to $C$. If $C$ and $P + Q$ is defined over $K$, then $C'$ is also defined over $K$. (The assumption that $P + Q$ is defined over $K$ does not matter for our purpose to find curves with many rational points.)
Singularities of sextic models

- Sextic model:
  \[ C' = V(F) \]

- Sextic model \( C' \) has singularities. Those should be classified.

- We study a \textit{generic case}, i.e., when the genus formula
  \[ g(C) = \frac{(d - 1)(d - 2)}{2} - \sum_{P} \frac{m_P(m_P - 1)}{2} \]
  with \( d = 6 \) and the multiplicity \( m_P \) at \( P \) holds. This case is given by I and II below.

- Several types of singularities on \( C' = V(F) \)
  I. Five double points \( P_1, P_2, P_3, P_4, P_5 \)
  II. One triple point \( P_1 \) and two double points \( P_2, P_3 \)
  III. Other cases (bad singularities: future work.)
Moduli theoretic viewpoint (Case I: generic case)

\#\{monomials of degree 6 in 3 variables\} = 28. For each singular point $P \in \{P_1, P_2, P_3, P_4, P_5\}$, we have three linear equations assuring that the $P$ is a double point, i.e., for example: if $P \notin V(z)$, then $F(P) = F_x(P) = F_y(P) = 0$.

The linear independence of $5 \times 3$ linear equations is checked. Considering a scalar multiplication to the whole sextic, the number of free parameters is

$$28 - 5 \times 3 - 1 = 12.$$  

This 12 is just the dim. of the moduli of curves of genus 5!, where dim. of choices of two points on $C$ making $C \to C'$ and the dim. of the space of 5 points on $\mathbb{P}^2$ up to $\text{Aut}(\mathbb{P}^2)$ are both 2 and are considered to be canceled. The parametrization by the sextic models is very effective!
Remark on arrangement of singularities

• We consider the following two cases:
  I. Five double points $P_1, P_2, P_3, P_4, P_5$
  II. One triple point $P_1$ and two double points $P_2, P_3$

Proposition

(1) 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.
(2) In case II, if $P_1, P_2, P_3$ are contained in a hyperplane,
    then $C'$ is geometrically reducible.
1. Introduction

2. Non-hyperelliptic and non-trigonal curves of genus 5

3. Algorithm to enumerate genus-5 generic curves over finite fields with many rational points

4. Position analysis for $\mathbb{F}_3$ and computational results with explicit equations in characteristic 3

5. Concluding remark
A sextic form $F$ giving a model of genus-5 generic curve

- $F$ has 28 unknown coefficients (write $a_1, \ldots, a_{28}$)
- $(a_1, \ldots, a_{28})$ is a solution of a system of 15 linear equations derived from the definition of the multiplicity of a singular point.
  - e.g. If $V(F)$ is singular at $P = (a: b: 1)$ with multiplicity 2, then the linear and constant parts of $F(X + a, X + b, 1)$ are zero. $\Rightarrow$ Obtain 3 equations.
- $F$ is irreducible and $V(F)$ has geometric genus 5.

An algorithm to enumerate curves with many rational points

- Regarding $a_1, \ldots, a_{28}$ as indeterminates, we can construct an algorithm (see Section 3 of our paper for details) to enumerate genus-5 generic curves $C$ with $#C(F_q) \geq N$, where $N$ is given.
- Counting $#C(F_q)$, we use a formula given in the next slide.
Enumeration of curves with many rational points (2/2)

 Formula for the number of rational points

- For $K = \mathbb{F}_q$, we have
  \[
  \#C(\mathbb{F}_q) = \#C'(\mathbb{F}_q) + \sum_{P \in \text{Sing}(C')} \left( \#V(h_P)(\mathbb{F}_q) - 1 \right),
  \]
  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 $C'$.
  - $V(h_P)$ is the closed subscheme of $\mathbb{P}^1$ defined by the ideal $\langle h_P \rangle$.

- If $h_P$ is quadratic, then
  \[
  \#V(h_P) - 1 = \begin{cases} 
  1 & \text{if } \frac{\Delta(h_P)}{q-1} = 1 \\
  -1 & \text{if } \frac{\Delta(h_P)}{q-1} = -1 \\
  0 & \text{if } \frac{\Delta(h_P)}{q-1} = 0 
  \end{cases}
  \]
  where $\Delta(h_P)$ is the discriminant of $h_P$. 

Outline

1. Introduction

2. Non-hyperelliptic and non-trigonal curves of genus 5

3. Algorithm to enumerate genus-5 generic curves over finite fields with many rational points

4. Position analysis for $\mathbb{F}_3$ and computational results with explicit equations in characteristic 3

5. Concluding remark
Position analysis of singular points for $C'$ over $\mathbb{F}_3$

- We classify all arrangements of singular points on $\mathbb{P}^2$ up to automorphisms over $\mathbb{F}_3$ of $\mathbb{P}^2$ in each case of
  1. Five double points $P_1, P_2, P_3, P_4, P_5$
  2. One triple point $P_1$ and two double points $P_2, P_3$
- Since $C'$ is defined over $\mathbb{F}_3$,
  1. The set $\{P_1, P_2, P_3, P_4, P_5\}$ is defined over $\mathbb{F}_3$.
  2. The point $P_1$ is defined over $\mathbb{F}_3$ and the set $\{P_2, P_3\}$ is defined over $\mathbb{F}_3$.

Case I: The patterns of the Frobenius orbits in $\{P_1, P_2, P_3, P_4, P_5\}$ is either of $(1,1,1,1,1), (1,1,1,2), (1,2,2), (1,1,3), (2,3), (1,4)$ and $(5)$: for example $(1,2,2)$ means that $\{P_1, P_2, P_3, P_4, P_5\}$ consists of three Frobenius orbits each of which has cardinality 1, 2 and 2 respectively.
Computational results of position analysis for Case I

- **Case (1,1,1,1,1):** two positions up to $\text{Aut}_{F_3}(\mathbb{P}^2)$
  - $P_1 = (1:0:0), P_2 = (0:1:0), P_3 = (0:0:1)$
    1. $P_4 = (1:1:0), P_5 = (0:1:1),$
    2. $P_4 = (1:1:0), P_5 = (1:2:1)$
- **Case (1,1,1,2):** three positions up to $\text{Aut}_{F_3}(\mathbb{P}^2)$
  - $P_1 = (1:0:0), P_2 = (0:1:0), P_3 = (0:0:1)$
    1. $P_4 = (1:ζ^5:ζ^7), P_5 = P_4^\sigma$, where $ζ$ is a primitive element in $F_9$
    2. $P_4 = (1:ζ^7:1), P_5 = P_4^\sigma$
    3. $P_4 = (1:ζ^2:ζ^2), P_5 = P_4^\sigma$ with Frobenius $\sigma$.
- **Case (1,2,2):** five positions (omit)
- **Case (1,1,3):** four positions (omit)
- **Case (2,3):** three positions (omit)
- **Case (1,4):** five positions (omit)
- **Case (5):** two positions (omit)
Computational results of position analysis for Case II

- **Case (1,1):** unique position up to $\text{Aut}_{\mathbb{F}_3}(\mathbb{P}^2)$
  
  \[ P_1 = (0:0:1), P_2 = (1:0:0), P_3 = (0:1:0) \]

- **Case (2):** unique position up $\text{Aut}_{\mathbb{F}_3}(\mathbb{P}^2)$
  
  \[ P_1 = (0:0:1), P_2 = (1:\zeta:0), P_3 = (1:\zeta^3:0) \]

➢ For each position in Cases I and II, we executed our algorithm over MAGMA to enumerate genus-5 generic curves over $\mathbb{F}_3$ with many $\mathbb{F}_9$-rational points. Computational results are described in the next slides.
Computational results (1/2)

Executing our algorithm over MAGMA, we have the following:

**Theorem** The maximal number of $\#C(F_9)$ of genus-5 generic curves $C$ over $F_3$ is 32. Moreover, there are precisely four $F_9$-isogeny classes of Jacobian varieties of genus-5 generic curves $C$ over $F_3$ with 32 $F_9$-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. \((t + 3)^6(t^2 + 2t + 9)^2\)

**Note:** The maximal number of $\#C(F_9)$ of curves of genus 5 over $F_9$ is unknown, but is known to belong between 32 and 35 (cf. [manypoints.org](http://manypoints.org)).

While a curve with the Weil polynomial (1) (resp. (4)) was found by Fischer (resp. Ramos-Ramos), our curves with (2) and (3) are new examples with $\#C(F_9) = 32$. 
Some examples ($\zeta$: a primitive element of $\mathbb{F}_9$)

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

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

$$+ 2y^3z^3 + x^2z^4 + 2xyz^4 + 2y^2z^4 + z^6$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial

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

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

$$F = x^4y^2 + 2x^3y^3 + 2xy^5 + 2y^6 + x^2y^3z + 2y^5z + 2x^4z^2 + x^3yz^2 + xy^3z^2$$

$$+ 2x^3z^3 + x^2yz^3 + xyz^4 + y^2z^4 + 2xz^5 + 2yz^5 + z^6$$

has 32 $\mathbb{F}_9$-rational points with Weil polynomial

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

1. Introduction

2. Non-hyperelliptic and non-trigonal curves of genus 5

3. Algorithm to enumerate genus-5 generic curves over finite fields with many rational points

4. Position analysis for $\mathbb{F}_3$ and computational results with explicit equations in characteristic 3

5. Concluding remark
Summary and open problems

- In this work, we presented the following:
  - Parametrization of the space of genus-5 generic curves
    - A plane sextic model with mild singularities
    - The number of parameters is just(!) the moduli dimension (= 12)
  - Algorithm to enumerate genus-5 generic curves with many rational points
  - Enumeration of such curves over $\mathbb{F}_3$
    - We found new examples which are not listed in manypoints.org

- Future works
  - Parameterization of the space of curves with more complex singularities.
  - Present methods to compute invariants of genus-5 generic curves.
    - How do we test whether two such curves are isomorphic or not?
  - Improve the efficiency of the proposed algorithm.