Superspecial curves of genus 4 in small characteristic

Momonari Kudo
Graduate School of Mathematics, Kyushu University, JAPAN
5th August, @The University of Kaiserslautern, GERMANY
This is a joint work with Shushi Harashita.
Introduction

$p$ : a rational prime
$K$ : a finite field of characteristic $p$
$ar{K}$ : the algebraic closure of $K$
$\mathcal{M}_g$ : the moduli space of curves of genus $g$

Problem.

For given $p$ and $g$, is there a superspecial curve in $\mathcal{M}_g$?
Definition of superspecial curves

\( C \) : a curve over \( k \), algebraically closed of characteristic \( p > 0 \)

**Definition.**

\( C \) is *superspecial* (s.sp.) iff its Jacobian \( J(C) \) is isomorphic to the product of supersingular (s.s.) elliptic curves.
Ekedahl’s problem

**Theorem ([1], Theorem 1.1).**

i) If $\exists C \in \mathcal{M}_g$; s.sp. nonhyperelliptic, then $2g \leq p^2 - p$.

ii) If $\exists C \in \mathcal{M}_g$; s.sp. hyperelliptic and $(p, g) \neq (2,1)$, then $2g \leq p - 1$.

**Problem ([1], p. 173).**

*Does there exist a superspecial curve of genus 4 or 5 for any $p \neq 2,3$?*

Our contribution

Theorem (K. and Harashita, [2]).

A) Any superspecial curves of $g = 4$ over $\mathbb{F}_{25}$ is $\mathbb{F}_{25}$-isomorphic to

$$2yw + z^2 = 0, \quad x^3 + a_1y^3 + a_2w^3 + a_3zw^2 = 0$$

in $\mathbb{P}^3$, where $a_1, a_2 \in \mathbb{F}_{25}^\times$ and $a_3 \in \mathbb{F}_{25}$.

B) There is no superspecial curve of $g = 4$ in $p = 7$.

The result B gives a negative answer to Ekedahl’s problem for $g = 4$ !

Contents:

1. Introduction

2. Nonhyperelliptic curves and maximal curves of genus 4

3. Computing Hasse-Witt matrix

4. Reduction of cubic forms

5. Our enumeration and proof of main theorem
Nonhyperelliptic curves of $g = 4$

$K$ : a finite field of characteristic $p > 0$

$\overline{K}$ : the algebraic closure of $K$

$C$ : a nonhyperelliptic curve of genus 4

Claim.

We may assume:
- $C$ is the complete intersection in $\mathbb{P}^3$ of an irreducible quadratic form $Q$ and an irreducible cubic form $P$.
- Any coefficient of $Q$ and $P$ belongs to $K$. 
Superspecial curves and maximal curves

**Lemma.**

$C$ : s.sp. curve of genus $g$ over an algebraically closed field $k$ with $\text{char}(k) = p$

$g > \frac{p^2 + 1}{2p} \implies \exists X : \text{maximal curve of genus } g \text{ s.t. } X \times_{\text{Spec}(\mathbb{F}_{p^2})} \text{Spec}(k) \cong C$

**Proof.** By Ekedahl’s theorem, $C$ descends to a curve $X$ over $\mathbb{F}_{p^2}$ with

$\# X(\mathbb{F}_{p^2}) = 1 \pm 2gp + p^2$, and thus $\# X(\mathbb{F}_{p^2}) = 1 + 2gp + p^2$. 

**Note.** $C$ is a maximal curve of genus $g$ over $\mathbb{F}_q$ iff $\# X(\mathbb{F}_q) = 1 + 2gq + q$
Contents:

1. Introduction

2. Nonhyperelliptic curves and maximal curves of genus 4

3. Computing Hasse-Witt matrix

4. Reduction of cubic forms

5. Our enumeration and proof of main theorem
Hasse-Witt matrix

**Definition.**

$C$ : algebraic curve of genus $g$ over an algebraically closed perfect field $k$ with $\text{char}(k) = p$

The *Hasse-Witt matrix* of $C$ is defined as a representation matrix of the action of Frobenius to $H^1(C, \mathcal{O}_C)$.

$F :$ the absolute Frobenius of $C$

$F^* : H^1(C, \mathcal{O}_C) \rightarrow H^1(C, \mathcal{O}_C) ;$ the action of Frobenius to the 1st cohomology

**Note.** $F^* : p$-linear
Hasse-Witt matrix and superspeciality

**Known Fact.**

$C$: algebraic curve of genus $g$ over an algebraically closed perfect field $k$ with $\text{char}(k) = p$

Then, $C$: superspecial $\iff F^* = 0$

In the following, we give an explicit method to get the HW matrix for $V(P, Q)$

(for more general cases, see Section 5 of [3]).


MI preprints 2016-1.
Computing Hasse-Witt matrix

Recall.

$C$ : algebraic curve of genus 4

$\Rightarrow C = V(P, Q) \subset \mathbb{P}^3$ for some cubic form $P$ and quadratic form $Q$ in $S := K[x, y, z, w]$ with $\gcd(P, Q) = 1$

Consider general cases; Let $f, g \in S$ with $\deg(f) = c, \deg(g) = d$ and $\gcd(f, g) = 1$. Put $I := \langle f, g \rangle_S, I_n := \langle f^n, g^n \rangle_S$ for $n \in \mathbb{Z}_{\geq 1}$.

Then $S/I$ and $S/I_n$ have the following free resolutions:
Computing Hasse-Witt matrix

\[
\begin{bmatrix}
g^n & -f^n \\
g^n & \\
\end{bmatrix}
\quad \quad
\begin{bmatrix}
f^n \\
g^n \\
\end{bmatrix}
\]

\[
0 \quad \rightarrow \quad S(-(c + d)n) \quad \rightarrow \quad S(-cn) \oplus S(-dn) \quad \rightarrow \quad S \quad \rightarrow \quad S/I_n \quad \rightarrow \quad 0
\]

\[
\varphi_2^{(n)} \quad \varphi_1^{(n)} \quad \varphi_0^{(n)}
\]

\[
0 \quad \rightarrow \quad S(-(c + d)) \quad \rightarrow \quad S(-c) \oplus S(-d) \quad \rightarrow \quad S \quad \rightarrow \quad S/I \quad \rightarrow \quad 0
\]

\[
\begin{bmatrix}
g & -f \\
g & \\
\end{bmatrix}
\quad \quad
\begin{bmatrix}
f \\
g \\
\end{bmatrix}
\]

where \(\varphi_0^{(n)}\) and \(\varphi_0\) are the canonical homomorphisms.
Computing Hasse-Witt matrix

Moreover the following diagram commutes.

\[
\begin{bmatrix}
g^n & -f^n \\
\end{bmatrix}
\]

\[
0 \rightarrow S(-(c+d)n) \xrightarrow{\varphi_2^{(n)}} S(cn) \oplus S(-dn) \xrightarrow{\varphi_1^{(n)}} S \xrightarrow{\varphi_0^{(n)}} S/I_n \rightarrow 0
\]

\[
[(fg)^{n-1}] \downarrow \psi_2 \quad \begin{bmatrix}
f^{n-1} & 0 \\
0 & g^{n-1} \\
\end{bmatrix} \downarrow \psi_1 \quad \downarrow \psi_0 \quad \downarrow \psi
\]

\[
0 \rightarrow S(-(c + d)) \xrightarrow{\varphi_2} S(-c) \oplus S(-d) \xrightarrow{\varphi_1} S \xrightarrow{\varphi_0} S/I \rightarrow 0
\]

\[
\begin{bmatrix}
g & -f \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
f \\
g \\
\end{bmatrix}
\]

where \(\psi_0\) and \(\psi\) are identity map, and \(h + I_n \mapsto h + I\), respectively.
Cohomology

Here take $n = p$ and put

$$\Phi_i := \overline{\varphi_i}, \quad \Phi_i^{(p)} := \overline{\varphi_i^{(p)}}, \quad \Psi := \overline{\psi}, \quad \Psi_i := \overline{\psi_i}.$$  

Then the following diagram of cohomology groups commutes:

$$
\begin{array}{cccccc}
 H^1(C, \mathcal{O}_C) & \xrightarrow{\approx} & H^2(\mathbb{P}^3, I) & \xrightarrow{\approx} & \text{Ker}(H^3(\Psi)) \\
 (F_1 |_{C^p})^* & \downarrow & F_1^* & \downarrow & F_1^* \\
 H^1(C^p, \mathcal{O}_{C^p}) & \xrightarrow{\approx} & H^2(\mathbb{P}^3, I^p) & \xrightarrow{\approx} & \text{Ker}(H^3(\Psi^{(p)})) \\
 \downarrow & \downarrow & H^2(\Psi) & \downarrow & H^3(\Psi) \\
 H^1(C, \mathcal{O}_C) & \xrightarrow{\approx} & H^2(\mathbb{P}^3, I) & \xrightarrow{\approx} & \text{Ker}(H^3(\Psi)) \\
\end{array}
$$

where $F_1$ and $F$ are the absolute Frobenius maps on $\mathbb{P}^3$ and $C$, respectively.
Moreover if $c \leq 3$ and $d \leq 3$ then

Thus for fixed $c$ and $d$, the Hasse-Witt matrix of $C$ is determined by coefficients in $(fg)^{p-1}$. 

\[
\begin{array}{cccccc}
H^1(C, O_C) & \xrightarrow{\sim} & H^2(\mathbb{P}^3, \mathcal{I}) & \xrightarrow{\sim} & \ker(H^3(\Psi_2)) & \xrightarrow{\sim} & H^3(\mathbb{P}^3, \mathcal{O}(-c - d)) \\
\downarrow (F_1 |_{C^p})^* & & \downarrow F_1^* & & \downarrow F_1^* & & \downarrow \text{power } p \\
H^1(C^p, O_{C^p}) & \xrightarrow{\sim} & H^2(\mathbb{P}^3, \mathcal{I}_p) & \xrightarrow{\sim} & \ker(H^3(\Psi_2^{(p)})) & \xrightarrow{\sim} & H^3(\mathbb{P}^3, \mathcal{O}((-c - d)p)) \\
\downarrow H^1(\Psi) & & \downarrow H^2(\Psi_0) & & \downarrow H^3(\Psi_2) & & \downarrow (fg)^{p-1} \\
H^1(C, O_C) & \xrightarrow{\sim} & H^2(\mathbb{P}^3, \mathcal{I}) & \xrightarrow{\sim} & \ker(H^3(\Psi_2)) & \xrightarrow{\sim} & H^3(\mathbb{P}^3, \mathcal{O}(-c - d)) \\
\end{array}
\]
Hasse-Witt matrix for $V(f, g)$

**Proposition.**

The notations are as above. Write $(fg)^{p-1} = \sum c_{i_1, i_2, i_3, i_4} x^{i_1} y^{i_2} z^{i_3} w^{i_4}$.

If $\deg(f) \leq 3$ and $\deg(g) \leq 3$,

Then the $(i, j)$-entry of HW-matrix of $C$ is given by $c_{-k_i p + k_j, -\ell_i p + \ell_j, -m_i p + m_j, -n_i p + n_j}$,

where $\{(k, \ell, m, n) \in (\mathbb{Z}_{<0})^4 : k + \ell + m + n = -c - d\} = \{(k_i, \ell_i, m_i, n_i)\}_{1 \leq i \leq g}$,

and $g = \dim H^1(C, \mathcal{O}_C)$. 

8/5/2016
Criterion for superspeciality of $V(P, Q)$

**Corollary.**

If $P, Q$ are cubic and quadratic forms, then $F^* = 0$ if and only if

all the 16 coefficients of

$$
(x^2yzw)^{p-1}, \ x^{2p-1}y^{p-2}z^{p-1}w^{p-1}, \ x^{2p-1}y^{p-1}z^{p-2}w^{p-1}, \ x^{2p-1}y^{p-1}z^{p-1}w^{p-2},
$$

$$
x^{p-2}y^{2p-1}z^{p-1}w^{p-1}, \ (xy^2zw)^{p-1}, \ x^{p-1}y^{2p-1}z^{p-2}w^{p-1}, \ x^{p-1}y^{2p-1}z^{p-1}w^{p-2},
$$

$$
x^{p-2}y^{p-1}z^{2p-1}w^{p-1}, \ x^{p-1}y^{p-2}z^{2p-1}w^{p-1}, \ (xyz^2w)^{p-1}, \ x^{p-1}y^{p-1}z^{2p-1}w^{p-2},
$$

$$
x^{p-2}y^{p-1}z^{p-1}w^{2p-1}, \ x^{p-1}y^{p-2}z^{p-1}w^{2p-1}, \ x^{p-1}y^{p-1}z^{p-2}w^{2p-1}, \ (xyzw^2)^{p-1}
$$

in $(PQ)^{p-1}$ are zero.
Our strategy for enumeration

For “possible” $P$ and $Q$,

1. Regard unknown coefficients of $P$ and $Q$ as indeterminates $a_1, \ldots, a_t$.
2. Compute $(PQ)^{p-1}$ (over $K[a_1, \ldots, a_t][x, y, z, w]$).
3. Construct a system of algebraic equations of the indeterminate from Corollary, and solve it by a known algorithm.
4. For each solution, test $C$ is non-singular or not (over $K[x, y, z, w]$).

We conduct the above procedures over a computer algebra system MAGMA [4].

What is the problem for enumeration?

1. The number of indeterminates is large..., $20 + 10 = 30$.

2. Even if one reduces the number, depending on multivariate systems, the computation might be costly...

3. If $p$ is large, the computation of $(PQ)^{p-1}$ might be expensive...
Reducing indeterminates and heuristic

1. Considering the reduction by elements of the orthogonal group associated to $Q$, reduce the number of indeterminates as much as possible!

2. By experiments, determine how many and which coefficients are optimal to be regarded as indeterminates to solve multivariate systems. (In our computation, apply the so-called hybrid method.)
Contents:

1. Introduction

2. Nonhyperelliptic curves and maximal curves of genus 4

3. Computing Hasse-Witt matrix

4. Reduction of cubic forms

5. Our enumeration and proof of main theorem
Reduction of cubic forms

\[ C : \text{a nonhyperelliptic curve of genus } 4 \text{ over a finite field } K \]

**Recall**: \( C \) is defined by an irr. quadratic form \( Q \) and an irr. cubic form \( P \) in \( K[x, y, z, w] \)

**Note**: - The rank of \( Q \) is \( \geq 3 \) (otherwise \( Q \) is reducible)

- In general, the quadratic forms are classified by their ranks and disc.

  since \( K \) is a finite field with \( p \neq 2 \)

From this, we may assume \( Q = 2xw + 2yz, \quad 2xw + y^2 - \varepsilon z^2 \text{ with } \varepsilon \notin (K^X)^2, \)

  or \( Q = 2yw + z^2 \) (degenerate case)
Orthogonal group

$C$ : a nonhyperelliptic curve of genus 4 defined by $P$ and $Q$ in $K[x, y, z, w]$

$\varphi$ : symmetric matrix corresponding to $Q$

$O_{\varphi}(K) := \{ g \in GL_4(K) : g^T \varphi g = \varphi \}$,

$\tilde{O}_{\varphi}(K) := \{ g \in GL_4(K) : g^T \varphi g = \mu \varphi \text{ for some } \mu \in K^\times \}$.

Transforming $P$ into $g \cdot P$ for $g \in \tilde{O}_{\varphi}(K)$, reduce unknown coefficient of possible $P$.

To do this, first consider the Bruhat decomposition of the orthogonal group.
Bruhat decomposition of $O_\varphi(K)$

In this talk, I describe only the degenerate case.

$$\varphi = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad U := \{ U(a) := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & -2^{-1}a^2 \\ 0 & 0 & 1 & -a \\ 0 & 0 & 0 & 1 \end{bmatrix} : a \in K \}, \quad s := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$A := \{1_4, \text{diag}(1,1,-1,-1)\},$$

$$T := \{ T(a) := \text{diag}(1,a,1,a^{-1}) : a \in K^\times \}, \quad V := \{ \begin{bmatrix} a & b & c & d \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} : a \in K^\times, \text{ and } b, c, d \in K \},$$

$$\tilde{T} := \{ \text{diag}(1,b,b,b) : b \in K^\times \},$$

$$B := ATU \text{ and } \tilde{B} := A\tilde{T}U.$$

**Lemma.** $O_\varphi(K) = (B \sqcup BsU)V$ and $\tilde{O}_\varphi(K) = (\tilde{B} \sqcup \tilde{B}sU)V$
Reduction of cubic forms $P$

Assume $p \neq 2,3$ and $\# K > 5$. First $P$ has 20 unknown coefficients:

$$P = a_0 x^3 + (a_1 y + a_2 z + a_3 w)x^2 + (a_4 y^2 + a_5 z^2 + a_6 w^2 + a_7 yz + a_8 yw + a_9 zw)x$$
$$+a_{10} y^3 + a_{11} z^3 + a_{12} w^3 + (a_{13} z + a_{14} w)y^2 + (a_{15} z^2 + a_{16} w^2 + a_{17} zw)y + a_{18} wz^2 + a_{19} w^2 z$$

1. $(x \mapsto x + ay + bz + cw) \in V$ transforms $P$ into a cubic without $x^2 y, x^2 z, x^2 w$.
2. By $yw \equiv -2^{-1}z^2 \mod Q$, assume $P$ does not have any term containing $yw$.

$$P = a_0 x^3 + (a_1 y^2 + a_2 z^2 + a_3 w^2 + a_4 yz + a_5 zw)x + a_6 y^3 + a_7 z^3 + a_8 w^3$$
$$+a_9 zy^2 + a_{10} z^2 y + a_{11} wz^2 + a_{12} w^2 z$$
Reduction of cubic forms $P$

**Claim.** $\exists g \in O_\varphi(K)$ s.t. $g$ stabilizes $x$ and $g \cdot P$ has non-zero $y^3$-term.

**Proof.** Assume the coefficients of $y^3$ and $w^3$ in $P$ equals 0, say

$P = a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_7z^3 + a_9zy^2 + a_{10}z^2y + a_{11}wz^2 + a_{12}w^2z$

Then $P(x = 0) = \alpha y^2z + \beta yz^2 + \gamma z^3 + \lambda z^2w + \mu zw^2$ for some $\alpha, ..., \mu \in K$, and

by the element $g := (z \mapsto z - cy, \ w \mapsto w + cz - 2^{-1}c^2y) \in sUs$,

the $y^3$-coefficient of $g \cdot P$ is

$$-\alpha c + \beta c^2 - \gamma c^3 - (2^{-1}\lambda)c^4 - (4^{-1}\mu)c^5$$

: degree 5 w.r.t. $c$

Since $\# K \geq 5$, the above value is not zero for some $c \in K^\times$. ■
Reduction of cubic forms $P$

3. From the claim, we may assume (the $y^3$-coefficient of $P$) $\neq 0$.

Further, $U(a)$ transforms $P$ into one without $y^2z$-term.

$$P = a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6y^3 + a_7z^3 + a_8w^3$$
$$+ a_9z^2y + a_{10}wz^2 + a_{11}w^2z, \text{ with } a_6 \neq 0$$

4. $(y \mapsto cy, \quad w \mapsto c^{-1}w) \in T$ and a constant multiplication to the whole $P$,
the $z^2w$ and $zw^2$-terms become 0 or 1.

5. $(x \mapsto dx) \in V$ for $\exists d \in K^\times$, the leading coefficient of $R := a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$
is 1 or $R = 0$. 
Reduction of cubic forms $P$

Consequently,

**Lemma.** If $\# K > 5$ then $P$ is transformed into

$$P = a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6y^3 + a_7z^3 + a_8w^3$$

$$+ a_9z^2y + b_1wz^2 + b_2w^2z$$

for $a_i \in K$ with $a_0, a_6 \in K^\times$ and $b_1, b_2 \in \{0,1\}$, and the leading coefficient of $R := a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$ is 1 or $R = 0$. 
Some remarks for non-degenerate cases

Similarly, under some assumptions ($C$ has “sufficiently” many $K$-rational points), the number of unknown coefficients of $P$ can be reduced for non-degenerate cases.

20 to at most 10, cf. the dimension of the moduli space $\mathcal{M}_4$ is 9!
Contents:

1. Introduction

2. Nonhyperelliptic curves and maximal curves of genus 4

3. Computing Hasse-Witt matrix

4. Reduction of cubic forms

5. Our enumeration and proof of main theorem
Our enumeration

$C$ : a nonhyperelliptic curve of genus 4 defined by $P$ and $Q$ in $K[x, y, z, w]$

By the action of $O_\varphi(K)$, the number of unknown coefficients of $P$ was reduced.

**Recall.** Our strategy is for each possible $b_i$’s,
- Compute $(PQ)^{p-1}$. (Keep $a_i$’s indeterminates)
- Construct a system of algebraic equations of the indeterminates from Corollary, and solve it. (at most 10 variables)
- For each solution, test $C$ is non-singular or not.
Problems remaining

Still problems are here:

In the step of solving a multivariate system, depending on the case, our computation does not terminate... (or out of memory...)

cf. the number of $a_i$’s is at most 10, at least 9,

\[ K = \mathbb{F}_{25} \text{ or } \mathbb{F}_{49}. \]
Our solution

For enumeration, we apply the “hybrid method” to solve multivariate systems.

- Choose some $a_{i_1}, \ldots, a_{i_s}$, say $\{a_1, \ldots, a_n\} = \{a_{i_1}, \ldots, a_{i_s}\} \cup \{a_{j_1}, \ldots, a_{j_t}\}$.
- For each (possible) $(a_{j_1}, \ldots, a_{j_t}) \in K^t$, solve the multivariate system in $K[a_{i_1}, \ldots, a_{i_s}]$.

Then, heuristically and experimentally

decide how many and which coefficients are optimal to be regarded as indeterminates.

As a result, all the computation terminated in real time!
Computational result (Degenerate case)

**Proposition.** Consider $Q = 2yw + z^2$ and

$$P = a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6y^3 + a_7z^3 + a_8w^3 + a_9z^2y + b_1wz^2 + b_2w^2z$$

where $a_0, a_6 \in \mathbb{F}_{49}^\times$, $b_1, b_2 \in \{0,1\}$.

Then there does not exist $(b_1, b_2, a_0, ..., a_9)$ s.t. $C = V(P, Q)$ is superspecial.
Computational proof of Proposition

Proof. For \( b_1, b_2 \in \{0,1\} \), conduct the following procedures on a computer algebra system.

(1) Regard the 7 unknown coefficients \( a_2, a_3, a_4, a_5, a_7, a_8, a_9 \) as variables with

\[
a_8 < a_7 < a_9 < a_3 < a_5 < a_2 < a_4 \quad \text{(grev. Lex)}
\]

\( \cdots \) Order A

(2) For each \( a_0, a_6 \in \mathbb{F}_{49}^\times \) and \( a_1 \in \mathbb{F}_{49} \), solve a multivariate system derived from our criterion for superspeciality, and for each solution, decide \( V(P, Q) \) is non-sing. or not.

From the output*, our claim holds. ■

* The source codes and log files are published, see my web page:

http://www2.math.kyushu-u.ac.jp/~m-kudo/kudo-harashita-comp.html
Comparison with other choices

Table: Timing data of the computation for degenerate case with \( q = 49, b_1 = b_2 = 0 \) and \( a_0 = 1 \)

<table>
<thead>
<tr>
<th>Order</th>
<th>Total Iterations</th>
<th>Number of indeterminates</th>
<th>Ave. Time for ((fg)^{p-1})</th>
<th>Ave. Time for solving SA</th>
<th>Ave. Time for testing non-singularity</th>
<th>Total time</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2352</td>
<td>7</td>
<td>0.061681s</td>
<td>0.0096143s</td>
<td>0.0050817s</td>
<td>181s</td>
</tr>
<tr>
<td>B</td>
<td>2352</td>
<td>7</td>
<td>0.059429s</td>
<td>0.16105s</td>
<td>0.0046765s</td>
<td>531s</td>
</tr>
<tr>
<td>C</td>
<td>2352/49</td>
<td>8</td>
<td>0.064813s</td>
<td>14.177s</td>
<td>0.25106s</td>
<td>695s</td>
</tr>
<tr>
<td>D</td>
<td>2352 \times 49</td>
<td>6</td>
<td>0.056109s</td>
<td>0.00087351s</td>
<td>0.00011386s</td>
<td>7402s</td>
</tr>
</tbody>
</table>

B: \( a_9 < a_7 < a_5 < a_4 < a_3 < a_2 < a_1 \) (grev. lex), \( (a_6, a_8) \) runs through \( \mathbb{F}_{49}^x \times \mathbb{F}_{49} \)

C: \( a_8 < a_7 < a_9 < a_3 < a_5 < a_2 < a_4 < a_1 \) (grev. lex), \( a_6 \) runs through \( \mathbb{F}_{49}^x \)

D: \( a_8 < a_7 < a_9 < a_3 < a_5 < a_2 \) (grev. lex), \( (a_6, a_1, a_4) \) runs through \( \mathbb{F}_{49}^x \times (\mathbb{F}_{49})^2 \)

**EV:** MAGMA V2.20-10, Windows 8.1 Pro 64 bit, 2.60 GHz CPU (intel Core i5), 8 GB memory
Proof of main theorem

Theorem (K. and Harashita, [2]).

A) Any superspecial curves of $g = 4$ over $\mathbb{F}_{25}$ is $\mathbb{F}_{25}$-isomorphic to

$$2yw + z^2 = 0, \quad x^3 + a_1y^3 + a_2w^3 + a_3zw^2 = 0$$

in $\mathbb{P}^3$, where $a_1, a_2 \in \mathbb{F}_{25}^\times$ and $a_3 \in \mathbb{F}_{25}$.

B) There is no superspecial curve of $g = 4$ in $p = 7$.

Proof. (Only the degenerate case for $q = 49$)

Recall that $\not\exists C :$ s.sp. hyperelliptic curve of genus 4 in characteristic $p = 7$.

Let $C$ be a nonhyperelliptic curve of genus 4 over $\mathbb{F}_{49}$.
Proof of main theorem

Recall that \( \not\exists C : \text{s.sp. hyperelliptic curve of genus 4 in characteristic } p = 7 \).

Let \( C \) be a nonhyperelliptic curve of genus 4 over \( \mathbb{F}_{49} \).

As mentioned in the 2\textsuperscript{nd} section, \( C \) is defined by a quadratic form \( Q \) and a cubic form \( P \) in \( \mathbb{F}_{49}[x, y, z, w] \).

Moreover, if \( Q \) is degenerate, \( Q = 2yw + z^2 \) and \( P \) is of the from

\[
P = a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6y^3 + a_7z^3 + a_8w^3
\]

\[
+ a_9z^2y + b_1wz^2 + b_2w^2z
\]

where \( a_0, a_6 \in \mathbb{F}_{49}^\times, b_1, b_2 \in \{0,1\} \).

By the previous proposition, the result holds. \( \blacksquare \)
Some remarks

1. For the other cases (non-degenerate cases and $q = 25$ cases),
   the claims hold in similar ways to the degenerate case for $q = 49$.

2. As a corollary, all s.sp. curves of $g = 4$ in $p = 5$ are isomorphic to each other over $\bar{K}$.

3. Also, the automorphism groups $\text{Aut}_{\bar{K}}(C)$ are determined.

Next Target: $g = 5$ or large $p$

Thank you for your attention!