Finite Fields and Their Applications 45 (2017) 131–169

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Superspecial curves of genus 4 in small characteristic

Momonari Kudo [a,*], Shushi Harashita [b]

[a] *Graduate School of Mathematics, Kyushu University, Japan*
[b] *Graduate School of Environment and Information Sciences, Yokohama National University, Japan*

ARTICLE INFO

Article history:
Received 30 August 2016
Accepted 1 December 2016
Available online 4 January 2017
Communicated by Gary L. Mullen

MSC:
11G20
68W30
14G05
14Q05
13P10
14G15

Keywords:
Superspecial curves
Maximal curves
Hasse–Witt matrices
Complete intersections

ABSTRACT

This paper contains a complete study of superspecial curves of genus 4 in characteristic $p \leq 7$. We prove that there does not exist a superspecial curve of genus 4 in characteristic 7. This is a negative answer to the genus 4 case of the problem proposed by Ekedahl [9] in 1987. This implies the non-existence of maximal curve of genus 4 over $\mathbb{F}_{49}$, which updates the table at `manypoints.org`. We give an algorithm to enumerate superspecial nonhyperelliptic curves in arbitrary $p \geq 5$, and for $p \leq 7$ we execute it with our implementation on a computer algebra system Magma. Our result in $p = 5$ re-proves the uniqueness of maximal curves of genus 4 over $\mathbb{F}_{25}$, see [11] for the original theoretical proof.

In Appendix, we present a general method determining Hasse–Witt matrices of curves which are complete intersections.

1. Introduction

Let p be a rational prime. Let K be a perfect field of characteristic p. Let $\overline{K}$ denote the algebraic closure of K. By a curve, we mean a non-singular projective variety of

* Corresponding author.
E-mail addresses: m-kudo@math.kyushu-u.ac.jp (M. Kudo), harasita@ynu.ac.jp (S. Harashita).

http://dx.doi.org/10.1016/j.ffa.2016.12.001
1071-5797/

dimension 1. A curve over K is called *superspecial* if its Jacobian is isomorphic to a product of supersingular elliptic curves over $\overline{K}$. It is known that C is superspecial if and only if the Frobenius on $H^1(C, \mathcal{O}_C)$ is zero.

This paper concerns the enumeration of superspecial curves of genus $g = 4$. Our interest in the case of $g = 4$ comes from the fact that for $g \geq 4$ the dimension of the moduli space of curves of genus g is strictly less than that of the moduli space of principally polarized abelian varieties of dimension g. This fact means that the theory on abelian varieties is not so effective for our purpose for $g \geq 4$. In [9], Theorem 1.1, Ekedahl proved that if there exists a superspecial curve C of genus g in characteristic p, then $2g \leq p^2 - p$, and $2g \leq p - 1$ if C is hyperelliptic and $(g, p) \neq (1, 2)$. In particular there is no superspecial curve of genus 4 in characteristic ≤ 3 and there is no superspecial hyperelliptic curve of genus 4 in characteristic ≤ 7. Hence in this paper we restrict ourselves to the nonhyperelliptic case in $p \geq 5$.

Our main results in this paper are the following.

Theorem A. *Any superspecial curve of genus* 4 *over* $\mathbb{F}_{25}$ *is* $\mathbb{F}_{25}$*-isomorphic to*

$$2yw + z^2 = 0, \qquad x^3 + a_1 y^3 + a_2 w^3 + a_3 z w^2 = 0$$

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

By Theorem A, we can give another proof of the uniqueness of maximal curves over $\mathbb{F}_{25}$ (Corollary 5.1.1 and Example 6.2.4), see [11] for the original theoretical proof.

Theorem B. *There is no superspecial curve of genus* 4 *in characteristic* 7*.*

Theorem B gives a negative answer to the genus 4 case of the problem proposed by Ekedahl in 1987, see p. 173 of [9]. Also this implies the non-existence of maximal curve of genus 4 over $\mathbb{F}_{49}$, which updated the table at `manypoints.org`. The site updates the upper and lower bounds of $N_q(g)$ the maximal number of rational points on curves of genus g over $\mathbb{F}_q$, after the paper [12] of van der Geer and van der Vlugt was published. See Section 5.1 for the details of our contribution to the value of $N_{49}(4)$. The authors learn much about this from E. W. Howe.

Here, we briefly describe our strategy to prove Theorems A and B. First we give a criterion for the superspeciality of curves defined by two equations, which is reminiscent of Yui's result [18] on hyperelliptic curves. We regard a quadric as a (possibly degenerate) quadratic form Q. Considering transformations by elements of the orthogonal group associated to Q, we reduce parameters of cubic forms as much as possible. After that, we enumerate cubic forms P such that $V(P, Q)$ are superspecial. Our concrete algorithm of the enumeration is as follows. We regard coefficients of P as variables, and construct a multivariate system by our criterion for the superspeciality. We solve the system with the hybrid method [2]. In this paper, we are only interested in the solutions whose entries