

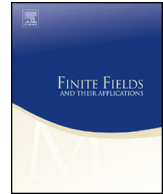


ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa



Differential operators and hyperelliptic curves over finite fields



Iván Blanco-Chacón^{a,*,1}, Alberto F. Boix^{b,2},
Stiofáin Fordham^{a,3}, Emrah Sercan Yilmaz^{a,3}

^a School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland

^b Department of Mathematics, Ben-Gurion University of the Negev, Marcus Family Campus, Deichmann Building for Mathematics 58, P.O.B. 653 Beer-Sheva 84105, Israel

ARTICLE INFO

Article history:

Received 8 December 2017

Accepted 23 February 2018

Available online xxxx

Communicated by Gary L. Mullen

MSC:

13A35

13N10

14B05

Keywords:

Algorithm

Differential operator

Frobenius map

Prime characteristic

ABSTRACT

Boix, De Stefani and Vanzo have characterised ordinary/supersingular elliptic curves over \mathbb{F}_p in terms of the level of the defining cubic homogeneous polynomial. We extend their study to arbitrary genus, in particular we prove that every ordinary hyperelliptic curve \mathcal{C} of genus $g \geq 2$ has level 2. We provide a good number of examples and raise a conjecture.

© 2018 Elsevier Inc. All rights reserved.

* Corresponding author.

E-mail addresses: ivan.blanco-chacon@ucd.ie (I. Blanco-Chacón), fernanal@post.bgu.ac.il (A.F. Boix), stiofain.fordham@ucdconnect.ie (S. Fordham), emrahsercanyilmaz@gmail.com (E.S. Yilmaz).

¹ Partially supported by Science Foundation Ireland Grant 13/IA/1914 and by MINECO grant MTM2016-79400-P.

² Partially supported by Israel Science Foundation (grant No. 844/14) and Spanish Ministerio de Economía y Competitividad MTM2016-7881-P.

³ Partially supported by Science Foundation Ireland Grant 13/IA/1914.

1. Introduction

Let k be any perfect field and $R = k[x_1, \dots, x_d]$ its polynomial ring in d variables. In this case it is known [1, IV, Théorème 16.11.2] that the ring \mathcal{D}_R of k -linear differential operators on R is the R -algebra (which we take here as a definition)

$$\mathcal{D}_R := R \langle D_{x_i, t} \mid i = 1, \dots, d \text{ and } t \geq 1 \rangle \subseteq \text{End}_k(R),$$

generated by the operators $D_{x_i, t}$, defined as

$$D_{x_i, t}(x_j^s) = \begin{cases} \binom{s}{t} x_i^{s-t}, & \text{if } i = j \text{ and } s \geq t, \\ 0, & \text{otherwise.} \end{cases}$$

For a non-zero $f \in R$, the natural action of \mathcal{D}_R on R extends to R_f in such a way that $R_f = \mathcal{D}_R \frac{1}{f^m}$, for some $m \geq 1$. Whilst there are examples of $m > 1$ in characteristic 0 (e.g. [2, Example 23.13]), it is $m = 1$ in positive characteristic ([3, Theorem 3.7 and Corollary 3.8]). This is shown by proving the existence of a differential operator $\delta \in \mathcal{D}_R$ such that $\delta(1/f) = 1/f^p$, i.e., δ acts as Frobenius on $1/f$. We will suppose that $k = \mathbb{F}_p$ and fix an algebraic closure \bar{k} of k from now on.

For an integer $e \geq 0$, let $R^{p^e} \subseteq R$ be the subring of all the p^e powers of all the elements of R and set $\mathcal{D}_R^{(e)} := \text{End}_{R^{p^e}}(R)$, the ring of R^{p^e} -linear ring-endomorphism of R . Since R is a finitely generated R^p -module, by [4, 1.4.8 and 1.4.9], it is

$$\mathcal{D}_R = \bigcup_{e \geq 0} \mathcal{D}_R^{(e)}.$$

Therefore, for $\delta \in \mathcal{D}_R$, there exists $e \geq 0$ such that $\delta \in \mathcal{D}_R^{(e)}$ but $\delta \notin \mathcal{D}_R^{(e')}$ for any $e' < e$. Such number e is called the level of f .

The level of a polynomial has been studied in [3] and [5]. In [5], an algorithm is given to compute the level and a good number of examples are exhibited. Moreover, if f is a cubic smooth homogeneous polynomial defining an elliptic curve $\mathcal{C} = V(f) = \{(x : y : z) \in \mathbb{P}_k^2 : f(x, y, z) = 0\}$, the level of f can be used to characterise the supersingularity of \mathcal{C} in the following way:

Theorem 1.1. ([5, Theorem 1.1]) *Let $f \in R$ be a cubic homogeneous polynomial such that $\mathcal{C} = V(f)$ is an elliptic curve over k . Denote by e the level of f . Then*

- (i) \mathcal{C} is ordinary if and only if $e = 1$.
- (ii) \mathcal{C} is supersingular if and only if $e = 2$.

The goal of the present work is to extend the results of [5] to hyperelliptic curves of genus $g \geq 2$ defined over k . Such a curve \mathcal{C} is birationally equivalent to the vanishing

Download English Version:

<https://daneshyari.com/en/article/8895672>

Download Persian Version:

<https://daneshyari.com/article/8895672>

[Daneshyari.com](https://daneshyari.com)