Journal of Number Theory 160 (2016) 666–678

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On cubic Kummer type towers of Garcia, Stichtenoth and Thomas ☆

M. Chara [a,*], R. Toledano [a,b]

[a] Instituto de Matemática Aplicada del Litoral (UNL-CONICET), Santa Fe, Argentina
[b] Departamento de Matemática, Facultad de Ingeniería Química (UNL), Santiago del Estero 2829 (3000) Santa Fe, Argentina

A R T I C L E I N F O

Article history:
Received 2 December 2014
Received in revised form 8 June 2015
Accepted 9 July 2015
Available online 2 November 2015
Communicated by Dinesh Thakur

MSC:
11R58
11G20
14H05

Keywords:
Function fields
Towers
Genus
Asymptotic behavior

A B S T R A C T

Text. In this paper we study the structure of a class of cubic tame towers having finite ramification locus. These towers were defined by Garcia, Stichtenoth and Thomas in 1997. We also prove some extensions of a well known result of H. Lenstra Jr. on the infiniteness of the ramification locus of these towers.

Video. For a video summary of this paper, please visit https://youtu.be/NYcajjrrVLI.

☆ This work is partially supported by CONICET and UNL CAI+D 2011 (grant numbers PI 50120110100308 and PJ 500220110100016).

* Corresponding author at: Instituto de Matemática Aplicada del Litoral, Colectora Ruta Nac. N° 168, Paraje El Pozo, 3000 Santa Fe, Argentina.

E-mail addresses: mchara@santafe-conicet.gov.ar (M. Chara), rtoledano@santafe-conicet.gov.ar (R. Toledano).

http://dx.doi.org/10.1016/j.jnt.2015.07.027
0022-314X/

1. Introduction

The importance of asymptotically good recursive towers in coding theory and some other branches of information theory (see e.g. [7,8]) is well-known. Among the class of recursive towers an important one is the class of Kummer type towers, recursively defined by equations of the form $y^m = f(x)$ for some suitable exponent m and rational function $f(x) \in K(x)$. A particular case was studied by Garcia, Stichtenoth and Thomas in [3] where a Kummer tower over a finite field $\mathbb{F}_q$ with $q \equiv 1 \mod m$ is recursively defined by an equation of the form

$$y^m = x^d f(x)\,, \tag{1}$$

where $f(x)$ is a polynomial of degree $m-d$ such that $f(0) \neq 0$, $\gcd(d,m) = 1$ and its leading coefficient is an mth-power in $\mathbb{F}_q$. The authors showed that they always have positive splitting rate and assuming the existence of a finite subset S of an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ such that $0 \in S$ and

$$\{\alpha \in \overline{\mathbb{F}}_q \,:\, \alpha^d f(\alpha) = \beta^m\} \subset S\,, \tag{2}$$

for any $\beta \in S$, the good asymptotic behavior of such towers can be deduced together with a concrete non-trivial lower bound for their limit. Condition (2) imposes serious restrictions on the polynomial f in (1) and little is known on the nature of these restrictions. H. Lenstra Jr. showed in [5] that in the case of an equation of the form (1) over a prime field $\mathbb{F}_p$, there is not such a set $S \subset \overline{\mathbb{F}}_p$ satisfying (2). This situation suggests that it is an interesting problem to understand how the existence of such a set S shapes the structure of equation (1) and what kind of restrictions imposes on the roots and coefficients of f when the associated tower is asymptotically good. The aim of this paper is to provide an answer to these questions in the cubic case of (1), more precisely in the case of good Kummer type towers recursively defined by an equation of the form

$$y^3 = x^d f(x)\,, \tag{3}$$

over a finite field $\mathbb{F}_q$ where $q \equiv 1 \mod 3$, $d = 1, 2$ and $f \in \mathbb{F}_q[x]$ is a polynomial such that $f(0) \neq 0$ whose leading coefficient is a non-zero cubic power in $\mathbb{F}_q$. It was shown in [3] that there are choices of the polynomial f giving good asymptotic behavior and even optimal behavior. For instance if $f(x) = x^2 + x + 1$ then equation (3) defines an optimal tower over $\mathbb{F}_4$ (see [3, Example 2.3]). It is also worth to note that the quadratic case (i.e $m = 2$ in (1)) is already included in the extensive computational search of good quadratic tame towers performed in [6].

The organization of the paper is as follows. In Section 2 we give the basic definitions and we establish the notation to be used throughout the paper. In Section 3 we give an overview of the main ideas, in the general setting of towers of function fields over a perfect field K, used to prove the infiniteness of the genus of a tower and we give a key