

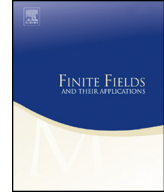


ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa



A graph aided strategy to produce good recursive towers over finite fields



Emmanuel Hallouin ^{a,b}, Marc Perret ^{a,b,*}

^a *Université Toulouse Jean Jaurès, 5, allées Antonio Machado, 31058 Toulouse cedex, France*

^b *Institut de Mathématiques de Toulouse, UMR 5219, France*

ARTICLE INFO

Article history:

Received 11 February 2016

Received in revised form 14 July 2016

Accepted 15 July 2016

Available online 23 August 2016

Communicated by Stephen D. Cohen

MSC:

14G05

14G15

14H20

5C38

33C05

33C90

Keywords:

Algebraic curves

Finite fields

Rational points

ABSTRACT

We propose a systematic method to produce potentially good recursive towers over finite fields. The graph point of view, so as some **magma** and **sage** computations are used in this process. We also establish some theoretical functional criterion ensuring the existence of many rational points on a recursive tower. Both points are illustrated by an example, from the production process, to the theoretical study.

© 2016 Elsevier Inc. All rights reserved.

Contents

0. Introduction	201
1. Preliminary notations and background	203

* Corresponding author.

E-mail addresses: hallouin@univ-tlse2.fr (E. Hallouin), perret@univ-tlse2.fr (M. Perret).

1.1.	Recursive towers	203
1.2.	Graphs and recursive towers	204
2.	Completeness and regularness criteria	206
2.1.	A divisorial criterion for completeness	206
2.2.	A functional criterion for regularness	207
3.	Applications	208
3.1.	Non-existence of totally splitting sets for some recursive towers	208
3.2.	Understanding the splitting set of the optimal tower $y^2 = \frac{x^2+1}{2x}$	209
3.3.	Graph based strategy to produce and to study asymptotically good recursive towers	211
3.3.1.	Producing a potentially good recursive tower using graphs and computer help	211
3.3.2.	Genus sequence computation	214
3.3.3.	Lower bound for the number of points sequence	217
3.3.4.	The last question	223
References	223

0. Introduction

The search of *explicit* examples of sequences of algebraic curves over a given finite field, of genus growing to infinity and having as many rational points as possible with regard to their genera, has become more and more important not only for its own, but also for several uses such as coding theory and cryptography (Garcia and Stichtenoth [8]) or for multiplication algorithms over finite fields (Ballet [1]). For quite a long time, only modular examples were known for square size of the finite field (Tsfasman–Vlăduț–Zink [15] and Ihara [11, “The general case”, p. 723]), and only examples coming from class field theory were known for non-square size. Unfortunately, these examples were not explicit.

In 1995, the important Garcia–Stichtenoth’s paper [7] is released showing the very first explicit example. The explicitness comes from the recursive definition of each floor of the tower; such towers are now called *recursive towers*. Since then, several authors have given many examples of recursive towers (see Garcia and Stichtenoth’s survey [8] or Li’s one [13]). Going through literature, we have been able to put forward two distinct features. First, except from the case of towers coming from modular theory (e.g. Elkies [5] and Bassa, Beelen, Garcia, Stichtenoth [2]), the authors never explain how they have been able to guess their examples. Second, once the explicit tower is given, there is always some difficulty in its study. Either the genus sequence is hard to compute (usually in the wildly ramified case), or the existence of many rational points is hard to prove (usually in the moderately ramified case). For instance, in the particularly interesting Garcia–Stichtenoth’s tower which is recursively defined by the equation $y^2 = \frac{x^2+1}{2x}$ and moderately ramified, the proof of the splitting behavior is quite mysteriously related to some functional equation satisfied by the well known Deuring polynomial.¹

Apart from our previous article [10], the present work joins in the continuation of those of Lenstra’s and Beelen’s [12,3]. A kind of non-existence result is proved by Lenstra [12]

¹ This is the characteristic polynomial of supersingular invariants in characteristic p .

Download English Version:

<https://daneshyari.com/en/article/4582644>

Download Persian Version:

<https://daneshyari.com/article/4582644>

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