Finite Fields and Their Applications 42 (2016) 200–224

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.

Contents

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

http://dx.doi.org/10.1016/j.ffa.2016.07.008
1071-5797/

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–Vlăduţ–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.