Journal of Pure and Applied Algebra 215 (2011) 2603–2614

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Rational places in extensions and sequences of function fields of Kummer type

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

[a] IMAL-UNL-CONICET, Güemes 3450, (3000) Santa Fe, Argentina

[b] FIQ-UNL-IMAL, Departamento de Matemática, Stgo. del Estero 2829, (3000) Santa Fe, Argentina

ARTICLE INFO

Article history:
Received 27 October 2010
Received in revised form 7 February 2011
Available online 24 March 2011
Communicated by C.A. Weibel

MSC: 11G20; 14G15; 14H25

ABSTRACT

In this paper we prove results on the number of rational places in extensions of Kummer type over finite fields and give sufficient conditions for non-trivial lower bounds on the number of rational places at each step of sequences of function fields over a finite field, that we call *(a, b)*-sequences. In the case of a prime field, we apply these results to the study of rational places in certain sequences of function fields of Kummer type.

Let q be a prime power and let $F/\mathbb{F}_q$ be a function field. A celebrated result of Weil [13] states that if $N(F)$ and $g(F)$ denote the number of rational places (or places of degree one) and the genus of $F/\mathbb{F}_q$ respectively, then

$$|N(F) - (q+1)| \leq 2g(F)\sqrt{q}.$$

The above inequality is known as the Hasse–Weil bound. There is an improvement due to Serre [5,6] which states that

$$|N(F) - (q+1)| \leq g(F)\lfloor 2\sqrt{q}\rfloor, \tag{1}$$

where $\lfloor x\rfloor$ denotes the largest integer m such that $m \leq x$.

It is well known that function fields with many rational places play an important role in algebraic coding theory (see for example [7] and [8]) and for reasons related to practical implementation of these codes it is imperative that the involved functions fields are given in an explicit way, i.e. in terms of generators and defining equations.

Function fields with many rational places have also received much attention in theoretical considerations related to global function fields after Ihara [4] introduced the function $A(q) = \limsup_{g\to\infty} N_q(g)/g$ where $N_q(g)$ is the maximum number of rational places of a function field over $\mathbb{F}_q$ with genus g. Drinfeld and Vladut [12] showed that $A(q) \leq \sqrt{q} - 1$. It was also shown by Ihara, and independently by Tsfasman, Vladut and Zink that if q is a square then $A(q) = \sqrt{q} - 1$. When q is not a square, the exact value of $A(q)$ is not known. One way of obtaining non-trivial lower bounds for Ihara's function is through the construction of asymptotically good towers of function fields over $\mathbb{F}_q$ (see the survey paper [2]).

As a first step in the construction of such towers, it is necessary to obtain non-trivial lower bounds of the number $N(F_i)$ of rational places of a function field $F_i/\mathbb{F}_q$ belonging to a sequence of functions fields $\{F_i/\mathbb{F}_q\}_{i=1}^{\infty}$ such that $F_i \subsetneq F_{i+1}$. One way of achieving this lower bound is by means of a lower bound for the so-called splitting locus of a sequence of function fields (see Section 2 for definitions). In Proposition 3.13 of [2] the authors showed that there is a lower bound for the splitting locus in terms of the size of a non-empty set $\Sigma \subset \mathbb{F}_q \cup \{\infty\}$ having certain properties. The main goal

* Corresponding author.
E-mail addresses: charamaria@gmail.com (M. Chara), ridatole@gmail.com (R. Toledano).

0022-4049/$ – see front matter
doi:10.1016/j.jpaa.2011.03.003

of this paper is to give sufficient conditions to find such a set Σ for a class of sequences of function fields that we call (a, b)-sequences.

In Section 1 we prove a result on the number of rational places in certain simple extensions of function fields which will be useful for the case of sequences of function fields. As an application, we give two examples of Kummer type extensions over a prime field such that the number of rational places attains $N_p(g)$.

In Section 2 we define the concepts of a recursive sequence and of an (a, b)-sequence of function fields over $\mathbb{F}_q$, where a, b are rational functions in one variable. In one of the main results, Theorem 2.1, we obtain a non-trivial lower bound for the number of rational places at each step of an (a, b)-sequence of function fields over $\mathbb{F}_q$, for a, b satisfying certain conditions.

In Section 3 we show that some known non-trivial lower bounds for $N(F_i)$ for certain sequences due to Garcia et al. [3] and van der Geer and van der Vlugt [11] can be deduced from Theorem 2.1. An auxiliary result that gives sufficient conditions on (a, b) is needed in order to prove that the element generating the extension F_{i+1} over F_i, at each step i, satisfies one of the assumptions of Theorem 2.1.

Finally, in Section 4, we focus on the interesting case of prime fields applying the results of Sections 2 and 3 to construct sequences of Kummer type over F_p for every prime p with non-trivial lower bounds for $N(F_i)$ (see Theorem 4.2). Since finding an example of an explicit asymptotically good tower over a prime field is still an open problem it would be very interesting to study the behavior of the genus of these sequences.

1. Rational places in Kummer extensions

Throughout this paper we use the following notation: for any set A we denote by $|A|$ the cardinality of A. If $g(T) \in \mathbb{F}_q(T)$ we denote by Z_g the set of zeros of $g(T)$ in an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.

For any monic and irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ we denote by $P_{f(x)}$ the rational place of the rational function field $\mathbb{F}_q(x)$ corresponding to $f(x)$. We denote by ν_∞ the discrete valuation induced by the infinite place P_∞ of $\mathbb{F}_q(x)$.

Let $F/\mathbb{F}_q$ be a function field. We will always assume that $\mathbb{F}_q$ is the full constant field of F. We denote by $\mathbb{P}(F)$ the set of places of F. For $P \in \mathbb{P}(F)$ we denote by $\mathcal{O}_P$ the valuation ring of P, by ν_P the discrete valuation induced by P in F and by $u(P)$ the residue class mod P of $u \in F$. The set of places of degree n of F is denoted by $\mathbb{P}_n(F)$. The places of F of degree one are called rational places of F. We denote by $N(F)$ the number of rational places of F, i.e. $N(F) = |\mathbb{P}_1(F)|$. When F'/F is an algebraic field extension, $P \in \mathbb{P}(F)$, $Q \in \mathbb{P}(F')$ and Q lies above P we denote by $e(Q|P)$ and $f(Q|P)$ the ramification index and the inertia degree of Q over P respectively. For complete definitions and properties of function fields see [7].

The following general result is a direct consequence of Kummer's theorem and the Eisenstein's irreducibility criterion (Theorem 3.3.7 and Proposition 3.1.15 in [7] respectively) for function fields.

Proposition 1.1. *Let $F/\mathbb{F}_q$ be a function field. Suppose that there are polynomials $a_1(T)$ and $a_2(T) \in \mathbb{F}_q[T]$ and an element $u \in F$ such that the polynomial*

$$\sigma(T) := a_1(T) - a_2(T)u \in F[T],$$

is monic and irreducible in $F[T]$. Let us consider the extension

$$F' := F(y) \quad \text{where } \sigma(y) = 0.$$

For $P \in \mathbb{P}(F)$ and $u \in \mathcal{O}_P$ we define

$$\overline{\sigma}_P(T) := a_1(T) - a_2(T)u(P),$$

which is a polynomial with coefficients in the residue field $\mathcal{O}_P/P = \mathbb{F}_{q^r}$ where $r = \deg(P)$. Let

$$S_1 := \{P \in \mathbb{P}(F) \,:\, \nu_P(u) \geq 0\},$$

$$S_2 := \{P \in \mathbb{P}(F) \,:\, \overline{\sigma}_P(T) \text{ is separable}\},$$

and

$$S_3 := \{P \in \mathbb{P}(F) \,:\, \overline{\sigma}_P(T) \text{ is not separable}\}.$$

Let $S = S_1 \cap S_2 \cap \mathbb{P}_1(F)$ and suppose that $S \neq \emptyset$. For $P \in S$ let L_P be the number of linear factors in the factorization of $\overline{\sigma}_P(T)$ in $\mathbb{F}_q[T]$. Then

(i) *All the ramified places of F in F' are in $(S_1 \cap S_3) \cup \{\text{poles of } u \text{ in } F\}$.*
(ii) $N(F') \geq \sum_{P \in S} L_P$.