Some Artin-Schreier towers are easy

Arnaldo Garcia[1] and Henning Stichtenoth

Abstract: We present a very simple and unified proof about the limits of certain Artin-Schreier towers considered in [8] and [11].

Mathematics Subject Classifications: 11R58, 14H05, 11D59, 14G15.

Keywords: towers of function fields, finite fields, Artin-Schreier extensions, genus, rational places, limits of towers.

1 Introduction

The interest in function fields over finite fields with many rational places has increased lately because of several applications to Coding Theory, Cryptography, Finite Geometry, etc. Especially interesting is the concept of the limit of a tower of function fields. A theorem of Tsfasman-Vladut-Zink shows that towers with big limits provide the existence of linear codes with limit parameters above the so-called Gilbert-Varshamov bound (see [13]).

Among the explicit towers which are known in the literature, Artin-Schreier towers play a prominent role, cf. [7], [8], [11] and [5]. It is the goal of this note to show that some Artin-Schreier towers are surprizingly easy to handle; i.e., one can easily determine the asymptotic behaviour of the genus (see Theorem 1 below), similarly to the case of tame towers (see [9] and [10]). This is obtained via a key lemma (see Lemma 1 below) on the behaviour of different exponents in the composite field of two Artin-Schreier extensions of prime degree p. As an application of our Theorem 1, we provide much simpler proofs for the limits of the towers in [8] and [11], avoiding all the technical computations done in those two papers (see Theorem 2 and also Remark 2 here).

[1]A. Garcia was partially supported by PRONEX # 662408-1996 (CNPq-Brazil).

2 Artin-Schreier towers and the Key Lemma

Throughout this paper, we denote by $\mathbb{F}_q$ the finite field of cardinality q and by p the characteristic of $\mathbb{F}_q$. A *tower* over $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \dots)$ of function fields $F_i/\mathbb{F}_q$ such that:

(i) all extensions F_{i+1}/F_i are finite and separable;

(ii) the field $\mathbb{F}_q$ is algebraically closed in F_i, for all $i \geq 0$;

(iii) the genus $g(F_i)$ goes to infinity for $i \to \infty$.

For a function field F over $\mathbb{F}_q$, we denote by $g(F)$ (resp. $N(F)$) the genus of F (resp. the number of $\mathbb{F}_q$-rational places of F). For a tower $\mathcal{F}$ as above, the following limits do exist (see [9]):

• The *splitting rate* $\nu(\mathcal{F}/F_0)$, defined as

$$\nu(\mathcal{F}) = \lim_{n\to\infty} N(F_n)/[F_n : F_0].$$

• The *genus* $\gamma(\mathcal{F}/F_0)$ of the tower, defined as

$$\gamma(\mathcal{F}/F_0) = \lim_{n\to\infty} g(F_n)/[F_n : F_0].$$

• The *limit* $\lambda(\mathcal{F})$ of the tower, defined as

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} N(F_n)/g(F_n) = \nu(\mathcal{F}/F_0)/\gamma(\mathcal{F}/F_0).$$

The tower $\mathcal{F}$ is called *asymptotically good* if the limit satisfies $\lambda(\mathcal{F}) > 0$; this condition is equivalent to

$$\nu(\mathcal{F}/F_0) > 0 \quad \text{and} \quad \gamma(\mathcal{F}/F_0) < \infty.$$

If all extensions F_{i+1}/F_i of the tower $\mathcal{F}$ are Artin-Schreier extensions, we call $\mathcal{F}$ an *Artin-Schreier tower* (see [1]). The tower $\mathcal{F}$ is *recursive* if it is recursively given by a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$; i.e., if $F_0 = \mathbb{F}_q(x_0)$ is the rational function field and for all $n \geq 0$,

$$F_{n+1} = F_n(x_{n+1}) \text{ with } f(x_n, x_{n+1}) = 0 \text{ and } [F_{n+1} : F_n] = \deg_Y f(X, Y).$$

We mention three important results on the limit of a tower $\mathcal{F}$ over $\mathbb{F}_q$:

(1) The *Drinfeld-Vladut bound* (see [4]): for all towers $\mathcal{F}/\mathbb{F}_q$, one has

$$\lambda(\mathcal{F}) \leq \sqrt{q} - 1.$$

(2) If $q = \ell^2$ is a square, then there exist towers $\mathcal{F}/\mathbb{F}_q$ which attain the Drinfeld-Vladut bound; i.e., there exist towers such that (see [6])

$$\lambda(\mathcal{F}) = \sqrt{q} - 1.$$

(3) If $q = \ell^3$ is a cube, then there exists a tower $\mathcal{F}/\mathbb{F}_q$ with (see [3])

$$\lambda(\mathcal{F}) \geq 2(\ell^2 - 1)/(\ell + 2).$$

In the case $\ell = p$ is a prime, this is the so-called *Zink's bound* [14].

The first *explicit* example in the literature of a tower $\mathcal{F}/\mathbb{F}_q$ with $q = \ell^2$ such that $\lambda(\mathcal{F}) = \sqrt{q} - 1$, is an Artin-Schreier tower (see [7]). This first example is closely related to the Artin-Schreier tower $\mathcal{F}_1/\mathbb{F}_q$ which is recursively given by the polynomial $f_1(X, Y)$ below (see [8]):

$$f_1(X, Y) = (X^{\ell-1} + 1)(Y^\ell + Y) - X^\ell. \qquad (*)$$

The first *explicit* example of a tower over a cubic field $\mathbb{F}_q$ (with $q = \ell^3$) which attains Zink's bound, is the recursive tower $\mathcal{F}_2$ over the field with 8 elements which is given by the polynomial $f_2(X, Y)$ below (see [11]):

$$f_2(X, Y) = X(Y^2 + Y) + X^2 + X + 1. \qquad (**)$$

The proofs in [8] and [11] that these two towers $\mathcal{F}_1$ and $\mathcal{F}_2$ satisfy

$$\lambda(\mathcal{F}_1) = \ell - 1 \quad \text{and} \quad \lambda(\mathcal{F}_2) = 3/2$$

are rather long and very technical. The next lemma is the core of the simplification of those results given in a unified way in this paper.

For a finite separable extension of function fields E/F and a place Q of E above a place P of F, we denote by $d(Q|P)$ the corresponding different exponent.

Lemma 1. (Key Lemma). *Let $F/\mathbb{F}_q$ be a function field and let E_1/F and E_2/F be linearly disjoint Artin-Schreier extensions of F, both of degree p. Denote by $E = E_1 \cdot E_2$ the composite field of E_1 and E_2. Let Q be a place of E and denote by Q_1, Q_2 and P its restrictions to the subfields E_1, E_2 and F. Suppose that we have*

$$d(Q_i|P) \in \{0, 2p-2\}, \text{ for } i = 1, 2.$$

Then $d(Q|Q_i) \in \{0, 2p-2\}$, for $i = 1, 2$.

Proof: We denote by v_P the discrete valuation of F corresponding to the place P (and by v_Q and v_{Q_i}, accordingly). The only non-trivial case is $d(Q_1|P) = d(Q_2|P) = 2p-2$. By the theory of Artin-Schreier extensions (see [12], Sec. III.7) we can find elements $x_1 \in E_1$ and $x_2 \in E_2$ such that $E_1 = F(x_1)$, $E_2 = F(x_2)$ and moreover

$$x_1^p - x_1 = z_1 \quad \text{and} \quad x_2^p - x_2 = z_2,$$

where z_1 and z_2 are functions in F such that $v_P(z_1) = v_P(z_2) = -1$. Hence we also have that $v_{Q_1}(x_1) = -1$. Since the residue field of F at the place P is perfect, there are elements $u, w \in F$ with

$$\frac{z_2}{z_1} = u^p + w, \quad v_P(u) = 0 \quad \text{and} \quad v_P(w) \geq 1.$$

It follows that

$$x_2^p - x_2 = z_1 u^p + z_1 w = (x_1^p - x_1)u^p + z_1 w = ((x_1 u)^p - x_1 u) + x_1(u - u^p) + z_1 w.$$

Setting $x_3 := x_2 - u x_1$, we then see that $E = E_1(x_3)$ and

$$x_3^p - x_3 = \tilde{u} x_1 + \tilde{w} =: z_3,$$

with $v_{Q_1}(\tilde{u}) \geq 0$, $v_{Q_1}(\tilde{w}) \geq 0$ and $v_{Q_1}(x_1) = -1$. Hence $v_{Q_1}(z_3) = -1$ or $v_{Q_1}(z_3) \geq 0$, which implies (see [12], Prop. III.7.8)

$$d(Q|Q_1) = 2p-2 \text{ or } d(Q|Q_1) = 0. \qquad \square$$

In Section 2 we will need two more lemmas:

Lemma 2. *Let E/F be an abelian extension of function fields of degree $[E : F] = p^r$, and let H_1, H_2 be intermediate fields with $F \subseteq H_1 \subseteq H_2 \subseteq E$ and with $[H_2 : H_1] = p$. Let Q be a place of E which is totally ramified in the extension E/F, and denote by P, Q_1 and Q_2 the restrictions of Q to F, H_1 and H_2. Assume that $d(Q|P) = 2(p^r - 1)$. Then it follows that*

$$d(Q_2|Q_1) = 2p - 2.$$

Proof: First we consider the case $F = H_1$, so $F \subseteq H_2 \subseteq E$ with $[H_2 : F] = p$ and $[E : H_2] = p^{r-1}$. By Hilbert's different formula (see [12], Theorem III.8.8) we have that

$$d(Q_2|P) \geq 2(p-1) \text{ and } d(Q|Q_2) \geq 2(p^{r-1} - 1).$$

The transitivity of the different ([12], Corollary III.4.11) gives

$$\begin{aligned} 2(p^r - 1) = d(Q|P) &= p^{r-1} \cdot d(Q_2|P) + d(Q|Q_2) \\ &\geq p^{r-1}(2p-2) + 2(p^{r-1} - 1) = 2(p^r - 1). \end{aligned}$$

Hence $d(Q_2|P) = 2p - 2$ and $d(Q|Q_2) = 2(p^{r-1} - 1)$. Now the result follows easily by induction. □

Lemma 3. *Let $E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_m$ be a chain of function fields $E_i/\mathbb{F}_q$, where each step is Galois of degree $[E_{i+1} : E_i] = p$ $(i = 0, \ldots, m-1)$. Let Q be a place of E_m and denote by Q_i the restriction of Q to E_i. Suppose that*

$$d(Q_{i+1}|Q_i) \in \{0, 2p-2\}, \text{ for } i = 0, \ldots, m-1.$$

Then the different exponent of Q in the extension E_m/E_0 satisfies:

$$d(Q|Q_0) = 2(e-1),$$

where $e = e(Q|Q_0)$ is the ramification degree of $Q|Q_0$.

Proof: Straightforward, using the transitivity of the different (see [12], Corollary III.4.11). □

3 Artin-Schreier towers with Property (A)

The Artin-Schreier towers $\mathcal{F}$ we will consider here are given recursively by a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ with $\deg_X f = \deg_Y f = p^r$. We assume that the "basic function field" $F = \mathbb{F}_q(x,y)$ with $f(x,y) = 0$ has the following property:

Property (A). *Both extensions $F/\mathbb{F}_q(x)$ and $F/\mathbb{F}_q(y)$ are Artin-Schreier extensions of degree p^r. Moreover, each ramified place in $F/\mathbb{F}_q(x)$ or in $F/\mathbb{F}_q(y)$ is totally ramified with different exponent equal to $2(p^r-1)$.*

We consider the pyramid associated to the recursive tower $\mathcal{F}$ (where $k = \mathbb{F}_q$):

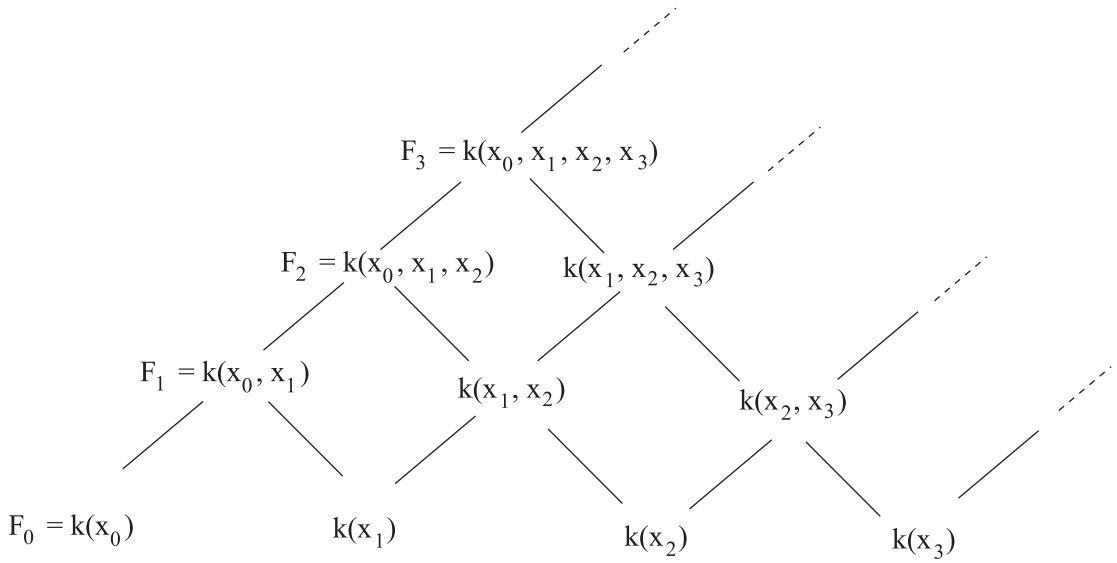

Figure 1

By assumption, all extensions in the base of the pyramid in Figure 1 (i.e., the extensions $k(x_n, x_{n+1})/k(x_n)$ and $k(x_n, x_{n+1})/k(x_{n+1})$) satisfy Property (A). Using Lemma 2 we can refine this pyramid and we then obtain another pyramid (see Figure 2) with cyclic extensions of prime degree p, such that all extensions of the refined pyramid also satisfy Property (A), with $r = 1$, as follows from iterated applications of Lemma 1.

A picture illustrating this refinement process in the case $r = 3$ is given below (Lemma 1 is applied iteratedly starting from the regions marked with $\otimes$ and going upwards to the right and to the left):

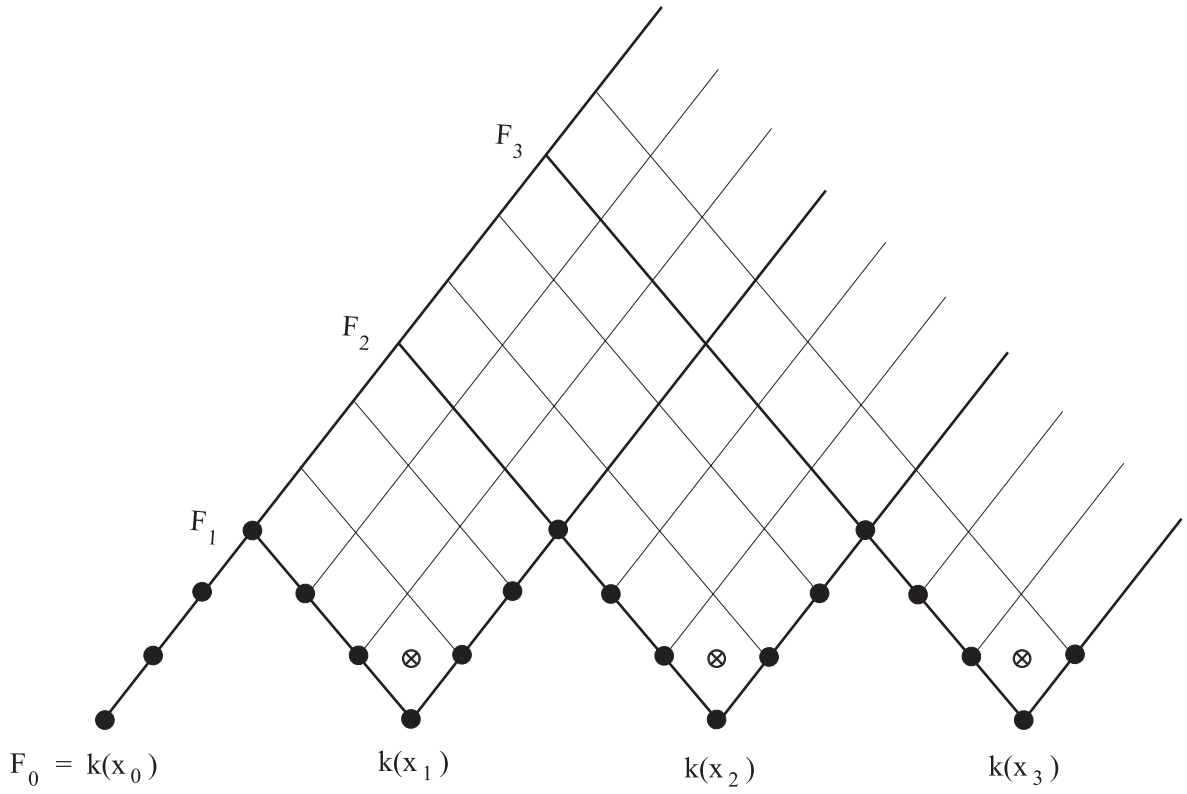

Figure 2

This gives a refinement $\mathcal{F}'$ of the original tower $\mathcal{F}$. Every field F_n belonging to the tower $\mathcal{F}$ is also a member of the refined tower $\mathcal{F}'$, and we obtain from Lemma 3 that for any place Q of F_n, the different exponent for Q over F_0 is given by

$$d(Q|P) = 2(e(Q|P) - 1).$$

As before, we denoted above by P the place of F_0 below Q and by $e(Q|P)$ the ramification degree of $Q|P$.

The *ramification locus* $V(\mathcal{F}/F_0)$ of a tower $\mathcal{F} = (F_i)_{i\geq 0}$ is defined as

$V(\mathcal{F}/F_0) := \{P \mid P$ is a place of F_0 which is ramified in F_n/F_0, for some $n \geq 1\}$.

We say that the tower $\mathcal{F}$ is of *finite ramification type* if the ramification locus is finite, and then we set

$$\deg V(\mathcal{F}/F_0) := \sum_{P \in V(\mathcal{F}/F_0)} \deg P.$$

Now we can state our main result:

Theorem 1. *Let $\mathcal{F}$ be a recursive Artin-Schreier tower of finite ramification type satisfying Property (A). Then the genus $\gamma(\mathcal{F}/F_0)$ is finite, and we have*

$$\gamma(\mathcal{F}/F_0) \leq \deg V(\mathcal{F}/F_0) - 1.$$

Proof: The degree of the different of the extension F_n/F_0 is given by

$$\deg \mathrm{Diff}(F_n/F_0) = \sum_P \sum_{Q|P} d(Q|P) \cdot \deg Q,$$

where P runs over the ramification locus $V(\mathcal{F}/F_0)$ and Q runs over all places of the field F_n above P. We then obtain

$$\begin{aligned} \deg \mathrm{Diff}(F_n/F_0) &= \sum_P \sum_{Q|P} 2(e(Q|P) - 1) \cdot \deg Q \\ &\leq 2 \cdot \sum_P \sum_{Q|P} e(Q|P) \cdot \deg Q \\ &= 2 \cdot \sum_P [F_n : F_0] \cdot \deg P = 2[F_n : F_0] \cdot \deg V(\mathcal{F}/F_0). \end{aligned}$$

Observe that the field F_0 is rational, so the Hurwitz genus formula for the function field extension F_n/F_0 yields

$$\begin{aligned} 2g(F_n) - 2 &= -2[F_n : F_0] + \deg \mathrm{Diff}(F_n/F_0) \\ &\leq 2[F_n : F_0](\deg V(\mathcal{F}/F_0) - 1). \end{aligned}$$

Dividing by $2 \cdot [F_n : F_0]$ and letting $n \to \infty$, we obtain the desired result. □

4 Application to the towers $\mathcal{F}_1$ and $\mathcal{F}_2$

Here we show that Theorem 1 easily implies the main results of [8] and [11].

Theorem 2. *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be the towers defined by (*) and (**) as in Section 2. Their limits satisfy*

$$\lambda(\mathcal{F}_1) \geq \ell - 1 \quad \textit{and} \quad \lambda(\mathcal{F}_2) \geq 3/2.$$

Proof: It is shown in [8] that

$$\nu(\mathcal{F}_1/F_0) \geq \ell^2 - \ell \quad \text{and} \quad \deg V(\mathcal{F}_1/F_0) = \ell + 1.$$

In [11] one shows that

$$\nu(\mathcal{F}_2/F_0) = 6 \quad \text{and} \quad \deg V(\mathcal{F}_2/F_0) = 5.$$

In fact, these statements are the "trivial" parts of the papers [8] and [11]. It is also easy that the basic function fields corresponding to the towers $\mathcal{F}_1$ and $\mathcal{F}_2$ satisfy Property (A). From Theorem 1 we then get

$$\lambda(\mathcal{F}_1) \geq \ell - 1 \quad \text{and} \quad \lambda(\mathcal{F}_2) \geq 3/2.$$

□

Remark 1. The equality $\lambda(\mathcal{F}_1) = \ell - 1$ now follows from the Drinfeld-Vladut bound. Since $\lambda(\mathcal{F}_1) = \nu(\mathcal{F}_1)/\gamma(\mathcal{F}_1)$, it also follows that $\nu(\mathcal{F}_1) = \ell^2 - \ell$ and $\gamma(\mathcal{F}_1) = \ell$.

Remark 2. In the literature there are other explicit examples (see [7] and [2]) of wildly ramified towers over $\mathbb{F}_q$ (with $q = \ell^2$ a square), which attain the Drinfeld-Vladut bound. The tower in [2] which is the same as the one given by Eq.(25) in [5], can be seen as a *subtower* of the tower $\mathcal{F}_1$ above. The tower in [7] can be obtained in a simple way from the tower $\mathcal{F}_1$ as a *composite tower* with a cyclic Kummer extension of the field $F_0 = \mathbb{F}_q(x_0)$ (see [8], Remark 3.11). In this way, the optimality of the towers in [7] and [2] can also be proved without long and technical calculations.

References

[1] P. Beelen, A. Garcia and H. Stichtenoth, *On towers of function fields of Artin-Schreier type*. Bull. Braz. Math. Soc. **35** (2004), 151–164.

[2] J. Bezerra and A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*. J. Number Theory **106** (2004), 142–154.

[3] J. Bezerra, A. Garcia and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, preprint.

[4] V.G. Drinfeld and S.G. Vladut, *The number of points of an algebraic curve*. Func. Anal. **17** (1983), 53–54.

[5] N. Elkies, *Explicit towers of Drinfeld modular curves*. Progress in Math. **202** (2001), 189–198.

[6] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*. J. Fac. Sci. Univ. Tokyo **28** (1981), 721–724.

[7] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*. Inventiones Math. **121** (1995), 211–222.

[8] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*. J. Number Theory **61** (1996), 248–273.

[9] A. Garcia and H. Stichtenoth, *On tame towers over finite fields.* J. Reine Angew. Math. **557** (2003), 53–80.

[10] A. Garcia, H. Stichtenoth and M. Thomas, *On towers and composita of towers of function fields over finite fields.* Finite Fields Appl. **3** (1997), 257–274.

[11] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of function fields over the field with eight elements.* Bull. London Math. Soc. **34** (2002), 291–300.

[12] H. Stichtenoth, "Algebraic Function Fields and Codes". Springer Universitext, Berlin-Heidelberg, 1993.

[13] M.A. Tsfasman, S.G. Vladut and T. Zink, *Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound*. Math. Nachrichten **109** (1982), 21–28.

[14] T. Zink, *Degeneration of Shimura surfaces and a problem in Coding Theory*. Lecture Notes in Computer Science **199** (1985), 503–511.

Arnaldo Garcia
IMPA - Estr. Dona Castorina 110
22460-320 - Rio de Janeiro-RJ - Brazil
e-mail: garcia@impa.br

Henning Stichtenoth
Fachbereich Mathematik
Universität Duisburg-Essen, Campus Essen
45117 Essen, Germany
e-mail: stichtenoth@uni-essen.de
and
Sabanci University
MDBF
Orhanli, Tuzla 34.956
Istanbul, Turkey
e-mail: henning@sabanciuniv.edu