## Werk

**Titel:** Elementary Albeian p-Extensions of Algebraic Function Fields.

**Autor:** Garcia, Arnaldo; Sitchtenoth, Henning

**Jahr:** 1991

**PURL:** https://resolver.sub.uni-goettingen.de/purl?365956996_0072|log8

## Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 72, 67 - 79 (1991)

manuscripta
mathematica
© Springer-Verlag 1991

# Elementary Abelian $p$-Extensions of Algebraic Function Fields

ARNALDO GARCIA[1] and HENNING STICHTENOTH

Let $K$ be a field of characteristic $p > 0$ and $F/K$ be an algebraic function field. We obtain several results on Galois extensions $E/F$ with an elementary abelian Galois group of order $p^n$.
(a) $E$ can be generated over $F$ by some element $y$ whose minimal polynomial has the specific form $T^{p^n} - T - z$.
(b) A formula for the genus of $E$ is given.
(c) If $K$ is finite, then the genus of $E$ grows much faster than the number of rational points (as $[E : F] \to \infty$).
(d) We present a new example of a function field $E/K$ whose gap numbers are non-classical.

## 0. Introduction

Let $K$ be a field of characteristic $p > 0$. Algebraic function fields $E = K(x, y)$ with a defining equation of the form

$$(*) \qquad y^q - y = f(x) \in K(x)$$

(where $q = p^n$ is a power of $p$) have been studied from several points of view, since these function fields have very remarkable properties.

[1]This paper was written while the first author was visiting Essen within the exchange program GMD-CNPq. The visit was partially supported by the Alexander von Humboldt-Stiftung.

**I.** Function fields whose automorphism groups are particularly large with respect to their genus are often of the type $(*)$, see [6], [15] and [17].

**II.** Examples of function fields over a finite constant field with many places of degree one are often of the type $(*)$, and some of them reach the Weil bound, see [1], [3] and [21]. Therefore they are of high interest in coding theory, since function fields with many rational places yield Goppa codes with good parameters [2], [18] and [20].

**III.** A function field is called *non-classical* if at any place there exists a Weierstrass gap number bigger than the genus of the field, see [13] and [16]. There are only few examples of non-classical function fields in the literature, and many of them are special cases of $(*)$, see [1], [8], [12] and [16].

A function field $E = K(x, y)$ defined by an equation of the form $(*)$ can be regarded as a Galois extension of the rational function field $F = K(x)$ with an elementary abelian Galois group of exponent $p$ and order $p^n$ (assuming that $K$ contains the finite field $\mathbb{F}_q$ with $q = p^n$ elements). Here a more general class of function fields is studied: we consider Galois extensions $E/F$ of algebraic function fields over $K$ with an elementary abelian Galois group of exponent $p$.

Section 1 contains a review of the Galois theory of elementary abelian $p$-extensions of an arbitary field of characteristic $p$ (Artin-Schreier theory). In section 2 we prove a very useful formula for the genus of elementary abelian $p$-extensions of a function field $F/K$.

In section 3 we consider families of elementary abelian $p$-extensions $E^{(j)}/F$ where $F/K$ is a fixed function field over a finite constant field $K$. The main result here is the following: Let $N(E^{(j)})$ (resp. $g(E^{(j)})$ denote the number of rational places (resp. the genus) of $E^{(j)}$. Then $N(E^{(j)})/g(E^{(j)}) \to 0$ as $[E^{(j)} : F] \to \infty$. This is a disappointing result; although many specific function fields of the type $(*)$ have many rational places, this class of function fields has "asymptotically" few rational places. In particular, we cannot construct "asymptotically good families" of long codes using function fields of the type $(*)$. The situation is similar as with $BCH$ codes. There are many excellent codes in this class of codes, but the class is "asymptotically bad", see [11,p. 269].

In section 4 we show that some new special cases of function fields $E = K(x, y)$ defined by equations of the form $(*)$ are non-classical. These special cases have already been considered from the points of view I. and II., see [3] and [6].

## 1. Galois theory of elementary abelian $p$-extensions

In this section we recall some well-known facts about Galois extensions $E/F$, where $F$ is a field of characteristic $p > 0$, with Galois group $Gal(E/F)$ elementary abelian of exponent $p$ (for brevity we call $E/F$ an *elementary abelian p-extension*). Let $\wp : u \mapsto u^p - u$ denote the *Artin-Schreier operator*. For a subset $A \subseteq F$ define $F(\wp^{-1}A)$ to be the splitting field of all polynomials $T^p - T - a$ ($a \in A$) over $F$.

Let $U \subseteq F$ be a subgroup of the additive group of $F$ with the properties:

$$ord(U) = p^n \text{ and } U \cap \wp(F) = 0. \tag{1}$$

Then $F(\wp^{-1}U)$ is an elementary abelian extension of $F$ of degree $p^n$. If $U' \subseteq F$ is another subgroup of $F$ satisfying (1) then

$$F(\wp^{-1}U) = F(\wp^{-1}U') \Leftrightarrow U + \wp F = U' + \wp F \Leftrightarrow U' \subseteq U + \wp F.$$

There are precisely $t = (p^n - 1)/(p - 1)$ intermediate fields $E_1, \ldots, E_t$ with

$$F \subseteq E_i \subseteq F(\wp^{-1}U) \text{ and } [E_i : F] = p,$$

namely

$$E_i = F(\wp^{-1}(u)) \text{ with } 0 \neq u \in U.$$

Observe that $F(\wp^{-1}(u)) = F(\wp^{-1}(u'))$ (with $u, u' \in U \setminus \{0\}$) if and only if $u' = \nu \cdot u$ for some $\nu \in \mathbb{F}_p^*$.

Conversely, if $E/F$ is an elementary abelian extension of degree $p^n$ then $E = F(\wp^{-1}U)$ for some subgroup $U \subseteq F$ satisfying (1). All this is well-known, cf. [10, p.221].

We give here another description of elementary abelian extensions $E/F$ of degree $p^n$ when $F$ contains the finite field $\mathbb{F}_{p^n}$.

**1.1 Proposition.** Suppose that $E/F$ is an elementary abelian extension of degree $p^n$ and that $\mathbb{F}_{p^n} \subseteq F$. Then there exists an element $y \in E$ with $E = F(y)$ whose minimal polynomial over $F$ has the form

$$\varphi(T) = T^{p^n} - T - z, \text{ with } z \in F.$$

**Proof.** We can find $y_1, \ldots, y_n \in E$ such that $E = F(y_1, \ldots, y_n)$ and $y_i^p - y_i \in F$. The Galois group $Gal(E/F)$ is generated by the automorphisms $\sigma_i$ ($1 \leq i \leq n$) given by:

$$\sigma_i(y_i) = y_i + 1 \ , \ \sigma_i(y_j) = y_j \text{ for } j \neq i.$$

Thus, any $\sigma \in Gal(E/F)$ has a unique representation

$$\sigma = \sigma_1^{\nu_1} \circ \ldots \circ \sigma_n^{\nu_n} \ , \ \nu_i \in \mathbb{F}_p. \tag{2}$$

Choose a basis $\{\mu_1, \ldots, \mu_n\}$ of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ and set

$$y := \sum_{k=1}^{n} \mu_k y_k.$$

If $\sigma \in Gal(E/F)$ is represented by (2) then

$$\sigma(y) = \sum_{k=1}^{n} \mu_k \sigma(y_k) = \sum_{k=1}^{n} \mu_k (y_k + \nu_k) = y + \mu, \text{ with } \mu = \sum_{k=1}^{n} \nu_k \mu_k \in \mathbb{F}_{p^n}.$$

Therefore $\sigma(y) = y$ iff $\sigma = id$. This implies $E = F(y)$. Moreover,

$$y^{p^n} - y = \prod_{\mu \in \mathbb{F}_{p^n}} (y + \mu) = \prod_{\sigma \in Gal(E/F)} \sigma(y) =: z \in F,$$

so $T^{p^n} - T - z$ is the minimal polynomial of $y$ over $F$. □

The converse of Proposition 1.1 also holds. More precisely, we have:

**1.2 Proposition.** Suppose that $\mathbb{F}_{p^n} \subseteq F$ and that the polynomial $\varphi(T) = T^{p^n} - T - z \in F[T]$ is irreducible over $F$. Then the extension $F(y)/F$ with $\varphi(y) = 0$ is an elementary abelian extension of degree $p^n$. The intermediate fields $F \subseteq E_i \subseteq F(y)$ with $[E_i : F] = p$ are the following ones: $E_i = F(y_\mu)$ where for $\mu \in \mathbb{F}_{p^n}^*$,

$$y_\mu := (\mu y)^{p^{n-1}} + (\mu y)^{p^{n-2}} + \ldots + (\mu y)^p + \mu y. \tag{3}$$

The element $y_\mu$ satisfies the equation $y_\mu^p - y_\mu = \mu \cdot z$; therefore $F(y) = F(\wp^{-1}U)$ with

$$U = \{\mu \cdot z \mid \mu \in \mathbb{F}_{p^n}\}.$$

**Proof.** For $\mu \in \mathbb{F}_{p^n}$ we obtain

$$\varphi(y + \mu) = (y + \mu)^{p^n} - (y + \mu) - z = y^{p^n} - y - z = 0.$$

It follows that $\varphi(T)$ has $p^n$ distinct roots in $F(y)$; so $F(y)/F$ is Galois, and any automorphism of $F(y)/F$ has the form $\sigma : y \mapsto y + \mu$ with $\mu \in \mathbb{F}_{p^n}$. The mapping $\sigma \mapsto \mu$ yields an isomorphism from $Gal(F(y)/F)$ to the additive group of $\mathbb{F}_{p^n}$, hence $F(y)/F$ is elementary abelian of degree $p^n$.

Consider the element $y_\mu$ defined by (3). Clearly $[F(y) : F(y_\mu)] \leq p^{n-1}$ and

$$y_\mu^p - y_\mu = \mu^{p^n} y^{p^n} - \mu y = \mu(y^{p^n} - y) = \mu z,$$

so $[F(y_\mu) : F] \leq p$. Since $[F(y) : F] = p^n$, this implies $[F(y_\mu) : F] = p$. For $\alpha, \mu \in \mathbb{F}_{p^n}^*$, we have $F(y_\alpha) = F(y_\mu)$ iff $\alpha z$ and $\mu z$ differ by a factor $\nu \in \mathbb{F}_p^*$. Thus we have constructed $(p^n - 1)/(p - 1)$ distinct intermediate fields $F \subseteq F(y_\mu) \subseteq F(y)$ of degree $p$ over $F$. Now an elementary abelian extension of degree $p^n$ has precisely $(p^n - 1)/(p - 1)$ subextensions of degree $p$, so the above extensions $F(y_\mu)$ are all of them. □

The question arises whether the polynomial $\varphi(T) = T^{p^n} - T - z \in F[T]$ is irreducible. Here is a simple criterion, cf. [9]:

**1.3 Lemma.** Suppose $\mathbb{F}_{p^n} \subseteq F$ and $z \in F$. The following conditions are equivalent:
(a) $T^{p^n} - T - z$ is irreducible over $F$.

(b) For all $\mu \in \mathbb{F}_{p^n}^*$, $T^p - T - \mu z$ is irreducible over $F$.
(c) For all $\mu \in \mathbb{F}_{p^n}^*$, $\mu z \notin \wp F$.

**Proof.** The equivalence (b) $\Leftrightarrow$ (c) is well-known, see [10, p.215]. That (a) implies (b) follows from Proposition 1.2, since $T^p - T - \mu z$ is the minimal ploynomial of $y_\mu$ over $F$.
(b) $\Rightarrow$ (a). We choose a root $y$ of $T^{p^n} - T - z$ (in a suitable extension field of $F$) and we have to show that $[F(y) : F] \geq p^n$. Now $F(y) \supseteq F(y_\mu) \supseteq F$ where, for $\mu \in \mathbb{F}_{p^n}^*$, $y_\mu$ is defined by (3). Since $y_\mu$ is a root of $T^p - T - \mu z$ we conclude $[F(y_\mu) : F] = p$, by assumption (b). The composite field of all $F(y_\mu)$, $\mu \in \mathbb{F}_{p^n}$, has degree $p^n$ over $F$ and it is contained in $F(y)$, thus $[F(y) : F] \geq p^n$. $\square$

**1.4 Remark.** In propositions 1.1 and 1.2, the polynomial $T^{p^n} - T$ can be replaced by any separable, monic, additive polynomial $h(T) \in F[T]$ of degree $p^n$ which has all roots in $F$. One obtains analogous descriptions of elementary abelian $p$-extensions.

## 2. The genus of an elementary abelian $p$-extension of a function field

A theorem of Kani [7, Th. 1] states that certain relations in the group algebra over $\mathbb{Q}$ of $Gal(E/F)$ imply corresponding relations between the genera of the intermediate fields of $E/F$. We use this to get:

**2.1 Theorem.** Let $K$ be a perfect field of characteristic $p > 0$. Let $F/K$ be an algebraic function field of one variable with constant field $K$ and genus $g(F)$. Consider an elementary abelian extension $E/F$ of degree $p^n$ such that $K$ is also the constant field of $E$. Denote by $E_1, \ldots, E_t$ (with $t = (p^n - 1)/(p-1)$) the intermediate fields $F \subseteq E_i \subseteq E$ with $[E_i : F] = p$, and by $g(E)$ (resp. $g(E_i)$) the genus of $E/K$ (resp. $E_i/K$). Then

$$g(E) = \sum_{i=1}^{t} g(E_i) - \frac{p}{p-1}(p^{n-1} - 1) \cdot g(F).$$

**Proof.** Let $\Gamma := Gal(E/F)$. For a subgroup $\Delta \subseteq \Gamma$ consider the fixed field $E_\Delta \subseteq E$ of $\Delta$, whose genus is denoted by $g(E_\Delta)$, and the *norm idempotent* $\varepsilon_\Delta$:

$$\varepsilon_\Delta := \frac{1}{ord\Delta} \cdot \sum_{\sigma \in \Delta} \sigma \in \mathbb{Q}[\Gamma].$$

Suppose there exists a relation

$$\sum_{\Delta \subseteq \Gamma} r_\Delta \cdot \varepsilon_\Delta = 0 \in \mathbb{Q}[\Gamma],$$

with $r_\Delta \in \mathbb{Q}$. Then the genera satisfy the same relation (see [7])

$$\sum_{\Delta \subseteq \Gamma} r_\Delta \cdot g(E_\Delta) = 0.$$

In the situation of Theorem 2.1, let $\Delta_i := Gal(E/E_i)$ be the subgroups of order $p^{n-1}$ (for $i = 1, \ldots, t$) and let $\Delta_0 = \{id\}$ be the trivial subgroup. Any $\sigma \in \Gamma$, $\sigma \neq id$, is contained in precisely $(p^{n-1} - 1)/(p-1)$ subgroups $\Delta_i$, therefore

$$p^{n-1} \sum_{i=1}^{t} \varepsilon_{\Delta_i} = \sum_{i=1}^{t} \sum_{\sigma \in \Delta_i} \sigma = (\frac{p^n - 1}{p-1}) \cdot id + (\frac{p^{n-1} - 1}{p-1}) \cdot \sum_{\sigma \in \Gamma \setminus \{id\}} \sigma =$$

$$= (\frac{p^n - p^{n-1}}{p-1}) \cdot id + (\frac{p^{n-1} - 1}{p-1} \cdot p^n) \cdot \varepsilon_\Gamma.$$

Thus we have the following relation in $\mathbb{Q}[\Gamma]$:

$$\varepsilon_{\Delta_0} = \sum_{i=1}^{t} \varepsilon_{\Delta_i} - \frac{p}{p-1}(p^{n-1} - 1) \cdot \varepsilon_\Gamma$$

The theorem now follows from Kani's result. □

The genus $g(E_i)$ can be determined by the following method due to Hasse [4]. We consider a cyclic extension of degree $p$

$$F' = F(\wp^{-1}u) \text{ with } u \in F \setminus \wp F,$$

where $K$ is assumed to be also the constant field of $F'$. For any place $P$ of $F/K$ there exists some $z \in F$ (depending on $P$ and $u$) such that either $v_P(u - \wp(z)) \geq 0$ or $v_P(u - \wp(z)) < 0$ and $v_P(u - \wp(z)) \not\equiv 0 \; mod \; p$ (here $v_P$ denotes the discrete valuation of $F$ associated with $P$). We define

$$m_P(u) := -1 \;\text{ if } v_P(u - \wp(z)) \geq 0$$

and

$$m_P(u) := -v_P(u - \wp(z)) \;\text{ if } v_P(u - \wp(z)) < 0 \text{ and } v_P(u - \wp(z)) \not\equiv 0 \; mod \; p.$$

Observe that this definition is independent of the choice of $z$. The following holds (see [4, p. 42]).
(i) $P$ is unramified in $F'/F$ iff $m_P(u) = -1$.
(ii) If $m_P(u) \neq -1$ then there is precisely one place $P'$ of $F'/K$ lying over $P$. Its ramification index is $e(P'/P) = p$, and the multiplicity of $P'$ in the different of $F'/F$ is equal to $(p-1)(m_P(u) + 1)$.

Therefore the Hurwitz genus formula yields:

**2.2 Proposition.** Let $F' = F(\wp^{-1}u)$ be as above. Then

$$g(F') = p \cdot g(F) + \frac{p-1}{2} \cdot (-2 + \sum_P (m_P(u) + 1) deg P),$$

the sum being extended over all places $P$ of $F/K$.

In [9], Lachaud states a combination of Theorem 2.1 and Proposition 2.2.

## 3. The number of rational places in a sequence of elementary abelian $p$-extensions

Here we use the genus formula obtained in the previous section to analyse the asymptotic behaviour of the number of rational places in a sequence of elementary abelian $p$-extensions. If $E$ is a function field having the finite field $\mathbb{F}_q$ as its constant field, we denote by $N(E)$ the number of places of $E/\mathbb{F}_q$ of degree one.

**3.1 Theorem.** Let $E^{(j)}/F$ $(j = 1, 2, \ldots)$ be a sequence of elementary abelian $p$-extensions of function fields having $\mathbb{F}_q$ as common constant field. Then the quotient $N(E^{(j)})/g(E^{(j)})$ goes to zero as the degree $[E^{(j)} : F]$ goes to infinity.

**Proof.** For a place $P$ of $F$, we denote by $K_P$ its residue class field. Let $\pi_P$ be a uniformizing parameter at $P$. For $u \in F$ there is a uniquely determined element

$$\varphi_P(u) = \sum_{m \geq 0} a_m \pi_P^{-m} \in K_P[\pi_P^{-1}]$$

such that $a_m = 0$ whenever $m > 0$ and $m \equiv 0 \; mod \; p$, and such that for some $z \in F$ $v_P(u - \varphi_P(u) - \wp(z)) \geq 0$. One should think of $\varphi_P(u)$ as the *reduced principal part* of $u$ at $P$ with respect to $\pi_P$. Clearly the map $\varphi_P : F \to K_P[\pi_P^{-1}]$ is $\mathbb{F}_p$-linear. It is well-known that (see [5] or [19])

$$P \text{ ramifies in } F(\wp^{-1}(u)) \Leftrightarrow \varphi_P(u) \notin K_P.$$

We denote by $p^{n_j}$ the degree of the extension $E^{(j)}/F$ and by $U^{(j)}$ an additive subgroup of $F$ of order $p^{n_j}$ associated to $E^{(j)}$, i.e. $[E^{(j)} : F] = p^{n_j}$ and $E^{(j)}$ is the compositum of $F(\wp^{-1}(u)), u \in U^{(j)}$. Suppose that $P$ is a place of $F$ that ramifies in the extension $E^{(j)}/F$. Then $P$ ramifies already in $F(\wp^{-1}(u_0))$ for some $u_0 \in U^{(j)}$, and hence $\varphi_P(u_0)$ has a pole at $P$. We then define the natural number $M_P^{(j)}$ as the biggest pole-order of $\varphi_P(u), u \in U^{(j)}$, i.e.

$$M_P^{(j)} = -min\{v_P(\varphi_P(u)) \mid u \in U^{(j)}\}.$$

Clearly, in each basis of $U^{(j)}$ over $\mathbb{F}_p$ there exists at least one element $u_1$ such that $\varphi_P(u_1)$ has a pole of order $M_P^{(j)}$. Take now a basis $u_1, u_2, \ldots, u_{n_j}$ of $U^{(j)}$ over $\mathbb{F}_p$ with the smallest possible number (say $m$) of elements with that pole-order. So, after renumbering, we get:
1) The elements $\varphi_P(u_1), \ldots, \varphi_P(u_m)$ have pole-order $M_P^{(j)}$.
2) For elements $\nu_1, \ldots, \nu_{n_j}$ of $\mathbb{F}_p$, $\varphi_P(\sum \nu_i u_i)$ has pole-order smaller than $M_P^{(j)}$ if and only if $\nu_1 = \nu_2 = \ldots = \nu_m = 0$.
It follows from 2) that among the subextensions of degree $p$ of $E^{(j)}/F$ at least $p^{n_j - 1}$ of them are of the form $F(\wp^{-1}(u))$ with the pole-order of $\varphi_P(u)$ equal to $M_P^{(j)}$.

It now follows from Theorem 2.1 and Proposition 2.2:

$$g(E^{(j)}) \geq p^{n_j}(g(F) - 1) + \frac{(p-1)p^{n_j - 1}}{2} \sum_{P \in R^{(j)}} (M_P^{(j)} + 1) \cdot degP,$$

where $R^{(j)}$ is the finite set of places of $F$ which ramify in $E^{(j)}$. On the other hand we have

$$N(E^{(j)}) \leq p^{n_j} \cdot N(F).$$

To finish the proof of the theorem we just have to show that $\sum_{P \in R^{(j)}} (M_P^{(j)} + 1) \cdot degP$ goes to infinity as the degree of the extension goes to infinity. For that purpose consider the diagonal $\mathbb{F}_p$-homomorphism $\varphi^{(j)}$:

$$\varphi^{(j)} : U^{(j)} \to \prod_{P \in R^{(j)}} K_P[\pi_P^{-1}] \ , \ u \mapsto (\varphi_P(u) | P \in R^{(j)}).$$

The cardinality of the image satisfies:

$$|\varphi^{(j)}(U^{(j)})| \leq q^{\sum_{P \in R^{(j)}} (M_P^{(j)}+1) \cdot degP}.$$

The kernel of $\varphi^{(j)}$ (see [5] or [19]) corresponds to the unramified subextensions of degree $p$ of $E^{(j)}/F$ in which all places $P \in R^{(j)}$ decompose totally. Hence

$$|Ker(\varphi^{(j)})| \leq p^{\sigma(F)}, \text{ where } \sigma(F) \text{ is the Hasse-Witt invariant.}$$

We then have that:

$$p^{n_j} \leq p^{\sigma(F)} \cdot q^{\sum_{P \in R^{(j)}} (M_P^{(j)}+1) \cdot degP}.$$

This finishes the proof of the theorem. □

## 4. A new class of non-classical function fields

Let $K$ be an algebraically closed field of characteristic $p > 0$ and let $F = K(x)$ be the rational function field over $K$. We consider the field $E = F(y)$:

$$E = K(x, y) \text{ with } y^q - y = x^{q_0}(x^q - x); q \text{ and } q_0 \text{ are powers of } p \text{ and } q_0^2 \neq q > q_0. \quad (4)$$

**4.1 Proposition.** The equation in (4) is irreducible and the genus of $E$ is given by :

$$g(E) = \frac{q-1}{2} \cdot max\{q_0, q/q_0\}.$$

**Proof.** To prove the irreducibility, one considers the equation $z^p - z = x^{q+q_0} - x^{q_0+1}$. Introducing the new variable $z_1 := z - x^{(q+q_0)/p} - x^{(q+q_0)/p^2} - \ldots - x^{(q+q_0)/q_0}$, we get the equation $z_1^p - z_1 = x^{(q/q_0)+1} - x^{q_0+1}$, which is clearly irreducible (since $q_0^2 \neq q$) and which has genus equal to $\frac{p-1}{2} \cdot max\{q_0, q/q_0\}$. Applying the same arguments to the other possible subextensions of degree $p$ of $E/F$ (which are given by $z^p - z = \mu x^{q_0}(x^q - x)$, with $\mu \in \mathbb{F}_q^*$), we conclude from Lemma 1.3 the irreducibility of $y^q - y = x^{q_0}(x^q - x)$. Since there are $(q-1)/(p-1)$ subextensions of degree $p$ of $E/F$, we get from theorem 2.1:

$$g(E) = \sum g(E_i) = \frac{q-1}{p-1} \cdot \frac{p-1}{2} \cdot max\{q_0, q/q_0\} = \frac{q-1}{2} \cdot max\{q_0, q/q_0\}. \quad \square$$

The above genus was already computed in [14] using the same method (higher ramification groups) as in [3].

**4.2 Proposition.** The field $E$ given by (4) is isomorphic to the field $E' = K(v, w)$ with $w^q - w = v^{q/q_0}(v^q - v)$.

**Proof.** Consider the map $\varphi : E \to E'$ defined by $\varphi(x) = v^{q/q_0}$ and $\varphi(y) = v^{(q/q_0)+1} - w$. One easily checks that $\varphi$ is well-defined and that $\varphi(E) = (E')^{q/q_0}$. □

From now on we assume that $q_0^2 > q > q_0$. We denote by $P_\infty$ the common pole of $x$ and $y$. It is the only place that ramifies in the extension $E/F$ and it is fully ramified. Consider the functions:

$$\Theta = y^{q/q_0} - x^{(q/q_0)+1} \quad \text{and} \quad \eta_1 = \Theta^{q_0^2/q} + x^{(q_0^2/q)-1} \cdot y.$$

The functions $x, y, \Theta$ and $\eta_1$ give rise to the following non-gaps at $P_\infty$:

$$q, q + q_0, q + (q/q_0) \text{ and } q_0^2 - q + q_0 + 1.$$

To determine the non-gaps at $P_\infty$ arising from $\Theta$ and $\eta_1$, we have used the equations:

$$\Theta^{q_0} = y - x^{q_0+1} \quad \text{and} \quad \eta_1^{q/q_0} = y + x^{q_0-(q/q_0)} \cdot \Theta$$

Therefore the semigroup $G = \mathbb{N} \cdot q + \mathbb{N} \cdot (q + q_0) + \mathbb{N} \cdot (q + (q/q_0)) + \mathbb{N} \cdot (q_0^2 - q + q_0 + 1)$ is contained in the semigroup of non-gaps at $P_\infty$.

**4.3 Proposition.** The semigroup $G$,

$$G = \mathbb{N} \cdot q + \mathbb{N} \cdot (q + q_0) + \mathbb{N} \cdot (q + (q/q_0)) + \mathbb{N} \cdot (q_0^2 - q + q_0 + 1),$$

is the semigroup of non-gaps at $P_\infty$.

**Proof.** The equality of both semigroups follows from the following relation:

$$\#(\mathbb{N} \setminus G) = g(E) = q_0(q-1)/2.$$

The relation above can be proved by showing that the semigroup $G$ is symmetric and that its conductor is equal to $2g(E)$. Another proof of the relation follows from the remark below. Both proofs are quite computational and we omit the details here. □

**4.4 Remark.** Given an integer $1 \leq m < q$, we set

$$G(m) := \{n \in \mathbb{N} \setminus G \mid n \equiv m (mod q)\}.$$

Here we show how to determine the set $G(m)$. First of all we divide $m$ by $q/q_0$ :

$$m = m_1 q/q_0 + j_0, \; 0 \leq m_1 < q_0 \text{ and } 0 \leq j_0 < q/q_0.$$

We consider two cases:

<u>Case 1.</u> $(m_1 - j_0 \cdot q_0^2/q) \geq 0$. Dividing by $q_0^2/q$ we get:

$$(m_1 - j_0 \cdot q_0^2/q) = j_1 q_0^2/q + j_2, \; 0 \leq j_1 < q/q_0 \text{ and } 0 \leq j_2 < q_0^2/q.$$

The set $G(m)$ is then given by:

$$G(m) = \{m + \lambda q \mid 0 \leq \lambda < j_0((q_0^2/q) - 1) + j_1 + j_2\}.$$

<u>Case 2.</u> $(m_1 - j_0 \cdot q_0^2/q) < 0$. In this case we divide:

$$(q_0 + m_1 - j_0 q_0^2/q) = j_1 \cdot q_0^2/q + j_2, \ 0 \leq j_1 < q/q_0 \text{ and } 0 \leq j_2 < q_0^2/q.$$

The set $G(m)$ is now given by:

$$G(m) = \{m + \lambda q \mid 0 \leq \lambda \leq j_0((q_0^2/q) - 1) + j_1 + j_2\}.$$

This remark gives an algorithm to obtain the Weierstrass gap numbers of $E$ at $P_\infty$.

From now on we assume that $p = 2$ and that $q_0^2 = 2q$. Such a field $E$ has already been considered by Henn [6] and by Hansen and Stichtenoth [3]. Henn proved that $E$ has a big automorphism group (the Suzuki group of order $q^2(q^2+1)(q-1)$). Hansen and Stichtenoth showed that $E$ has maximal number of rational points over $\mathbb{F}_q$ (namely $1 + q^2$) among the fields with genus equal to $g(E)$. This ensures good parameters for their Goppa codes.

We are going to show that the function field $E/K$ is *non-classical*, i.e. at every place $P$ of $E$ one can find a holomorphic differential of $E$ vanishing at $P$ with multiplicity bigger or equal to the genus $g(E)$. By the Riemann-Roch theorem, this definition is equivalent to the one given in the introduction. For $(a, b) \in K^2$ satisfying the equation in (4), we denote by $P_{a,b}$ the common zero of $(x - a)$ and $(y - b)$. Consider the functions:

$Y(a,b) = (y-b) - a^{q_0}(x-a)$.
$\Theta(a,b) = (y-b)^{q/q_0} - (x-a)^{(q/q_0)+1} - a(x-a)^{q/q_0}$.
$\eta(a,b) = \Theta(a,b)^{q_0^2/q} + (x-a)^{(q_0^2/q)-1} \cdot Y(a,b) + (a^q - a)^{(q_0^2/q)-1} \cdot Y(a,b)$.

In our case ($p = 2$ and $q_0^2 = 2q$) we have that:
$\eta(a,b) = \Theta(a,b)^2 + (x + a^q) \cdot Y(a,b)$.

We have the following table:

| function | pole-order at $P_\infty$ | for a $\notin \mathbb{F}_q$; zero-order at $(a,b)$ | for a $\in \mathbb{F}_q$; zero-order at $(a,b)$ |
|---|---|---|---|
| $(x-a)$ | $q$ | 1 | 1 |
| $Y(a,b)$ | $q + q_0$ | $q_0$ | $q_0 + 1$ |
| $\Theta(a,b)$ | $q + (q/q_0)$ | $q/q_0$ | $(q/q_0) + 1$ |
| $\eta(a,b)$ | $q + q_0 + 1$ | $q$ | $q + q_0 + 1$ |

This table follows from the following expansions at $P_{a,b}$, where $\alpha := (a^q - a)$:

$$Y(a,b) = -\alpha(x-a)^{q_0} + (x-a)^{q_0+1} + \alpha^{q_0}(x-a)^q - (x-a)^{q+q_0} + \ldots$$

$$\Theta(a,b) = \alpha(x-a)^{(q/q_0)} - (x-a)^{(q/q_0)+1} - \alpha^{q/q_0}(x-a)^q + (x-a)^{q+(q/q_0)} + \dots$$

From these expansions we get:

$$\eta(a,b) = \alpha^{(q_0^2/q)-1} \cdot (x-a)^{q_0+1} - \alpha(x-a)^{q_0+(q_0^2/q)-1} + \alpha^{q_0+(q_0^2/q)-1} \cdot (x-a)^q +$$

$$+\alpha^{q_0}(x-a)^{q+(q_0^2/q)-1} - \alpha^{(q_0^2/q)-1} \cdot (x-a)^{q+q_0} - (x-a)^{q+q_0+(q_0^2/q)-1} + \dots .$$

The first two terms in the expansion of $\eta(a,b)$ cancel out since we assume that $q_0^2 = 2q$. Now a word about the pole-order at $P_\infty$ of $\eta(a,b)$. This pole-order is the same as that of $\eta_1(a,b) := \Theta(a,b)^{q_0^2/q} + (x-a)^{(q_0^2/q)-1} \cdot Y(a,b)$, which can be computed to be $(q_0^2 - q + q_0 + 1)$ by using the following equation:

$$\eta_1(a,b)^{q/q_0} = Y(a,b) + (x-a)^{q_0-(q/q_0)} \cdot \Theta(a,b).$$

In our situation ($p = 2$ and $q_0^2 = 2q$) we have:

$$2g(E) - 2 = (q_0 - 2)(q + q_0 + 1).$$

We consider the following set:

$$S = \{(\lambda, j_2, j_1, j_0) \in \mathbb{N}^4 \mid \lambda, j_1 \in [0, q/q_0); j_2 \in \{0,1\} \text{ and } j_0 \geq 0 \text{ satisfying}$$

$$\lambda q + j_2(q + (q/q_0)) + j_1(q + q_0) + j_0(q + q_0 + 1) \leq (q_0 - 2)(q + q_0 + 1)\}.$$

After some computations one can show that the cardinality of the set above is given by:

$$\#S = g(E) - (q - q_0)/2.$$

We have determined this cardinality by showing that there are $(q_0 q)/4$ elements in $S$ with $j_2 = 0$ and $(q_0 q - 2q)/4$ elements in $S$ with $j_2 = 1$.
The following set of differentials $\mathcal{D}_{a,b}$ is part of a Hermite basis at $P_{a,b}$ of holomorphic differentials, i.e. the differentials have pairwise distinct zero-orders at $P_{a,b}$:

$$\mathcal{D}_{a,b} = \{dx \cdot (x-a)^\lambda \cdot \Theta(a,b)^{j_2} \cdot Y(a,b)^{j_1} \cdot \eta(a,b)^{j_0} \mid (\lambda, j_2, j_1, j_0) \in S\}.$$

For $a \notin \mathbb{F}_q$, we get the corresponding set $\mathcal{O}$ of pairwise distinct orders at $P_{a,b}$:

$$\mathcal{O} = \{\lambda + j_2 \cdot q/q_0 + j_1 \cdot q_0 + j_0 \cdot q \mid (\lambda, j_2, j_1, j_0) \in S\}.$$

Although we have not determined the full order-sequence of the field $E$ (there are yet $(q - q_0)/2$ orders to be determined), we can already conclude the non-classicality of $E$ since we have:

$$(q_0 - 2)q \in \mathcal{O} \text{ and } (q_0 - 2)q \geq g(E) = q_0(q-1)/2.$$

So we have proved:

**4.5 Theorem.** Let $K$ be an algebraically closed field of characteristic $p = 2$. Let $q_0 > 2$ be a power of the characteristic and let $q = q_0^2/2$. The function field $E = K(x,y)$ with $y^q - y = x^{q_0}(x^q - x)$ is non-classical, that is, at every place $P$ one can find a holomorphic differential vanishing at $P$ with order bigger or equal to the genus $g(E) = q_0(q-1)/2$.

**4.6 Remark.** For $a \in \mathbb{F}_q$ we have that the set of orders $\mathcal{O}_q$ at $P_{a,b}$ arising from the set of differentials $\mathcal{D}_{a,b}$ is given by:

$$\mathcal{O}_q = \{\lambda + j_2 \cdot ((q/q_0) + 1) + j_1 \cdot (q_0 + 1) + j_0 \cdot (q + q_0 + 1) \mid (\lambda, j_2, j_1, j_0) \in S\}.$$

It is straightforward to see that $\mathcal{D}_{a,b} \cup \mathcal{D}'_{a,b} \cup \mathcal{D}''_{a,b}$ is a Hermite basis at a rational place $P_{a,b}$ over $\mathbb{F}_q$, where the sets of holomorphic differentials $\mathcal{D}'_{a,b}$ and $\mathcal{D}''_{a,b}$ are as follows:
$\mathcal{D}'_{a,b} := \{dx \cdot (x-a)^{q/q_0} \cdot Y(a,b)^{j_1} \cdot \eta(a,b)^{j_0} \mid j_0 + j_1 \leq (q_0/2) - 2\}$ and
$\mathcal{D}''_{a,b} := \{dx \cdot (x-a)^{\lambda} \cdot Y(a,b)^{q/q_0} \cdot \eta(a,b)^{j_0} \mid \lambda + j_0 \leq (q_0/2) - 2\}$.
The order-sequence at a rational place over $\mathbb{F}_q$ is the same as the one at $P_\infty$. This follows since there is an autormorphism of $E$ permuting them (see [6, p. 109]). One can also prove that directly using Remark 4.4.

**4.7 Remark.** Based on strong computational evidence we are convinced that the following holds:
The Weierstrass points of $E$ are exactly the rational places of $E$ over the finite field $\mathbb{F}_q$. Moreover, the set of generic orders of $E$ yet to be determined is the union of the sets $\mathcal{O}(j_0)$ for $q_0/2 \leq j_0 \leq q_0 - 2$ where, setting $N(j_0) = q_0 - 1 - j_0$,

$$\mathcal{O}(j_0) = \{\lambda + j_2 q_0/2 + j_1 q_0 + j_0 q \mid j_2 < 2; j_1 < N(j_0) \text{ and } \lambda + j_2 + j_1 = N(j_0)\}.$$

Clearly we have $\#\mathcal{O}(j_0) = 2N(j_0)$, and hence the union of the above sets $\mathcal{O}(j_0)$ has $(q - q_0)/2$ elements, as desired.

We thank Prof. P. Viana for doing some of the computations mentioned in Remark 4.7.

## References

[1] Garcia, A. and Viana, P. Weierstrass points on certain non-classical curves. Arch. Math. 46, 315-322 (1986)
[2] Goppa, V.D. Algebraic-geometric codes. Math. U.S.S.R. Izvestiya 21, 75-91 (1983)
[3] Hansen, J.P. and Stichtenoth, H. Group codes on certain algebraic curves with many rational points. AAECC 1, 67-77 (1990)
[4] Hasse, H. Theorie der relativ zyklischen algebraischen Funktionenkörper. J. Reine Angew. Math. 172, 37-54 (1934)
[5] Hasse, H. and Witt, E. Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad $p$ über einem algebraischen Funktionenkörper der Charakteristik $p$. Monatsh. Math. Phys. 43, 477-492 (1936)
[6] Henn, H.W. Funktionenkörper mit großer Automorphismengruppe. J. Reine Angew. Math. 302, 96-115 (1978)
[7] Kani, E. Relations between the genera and between the Hasse-Witt invariants of Galois coverings of curves. Canad. Math. Bull. 28 (3), 321-327 (1985)
[8] Komiya, K. Algebraic curves with non-classical types of gap sequences for genus three and four. Hiroshima Math. J. 8, 371-400 (1978)
[9] Lachaud, G. Artin-Schreier Curves, Exponential Sums and the Carlitz-Uchiyama Bound for Geometric Codes. To appear in J. of Number Theory

[10] Lang, S. Algebra. Addison-Wesley, 2nd edition (1970)
[11] Mac Williams, F.J. and Sloane, N.J.A. The Theory of Error-correcting Codes. North Holland (1977)
[12] Matzat, H. Über die Weierstrasspunkte von Fermatkörpern. Thesis, Univ. Karlsruhe (1972)
[13] Neeman, A. Weierstrass points in characteristic $p$. Invent. Math. 75, 359-376 (1984)
[14] Pedersen, J.P. and Sørensen, A.B. Codes from certain algebraic function fields with many rational places. Preprint, Kopenhagen (1990)
[15] Roquette, P. Abschätzung der Automorphismenzahl von Funktionenkörpern bei Primzahlcharakteristik. Math. Z. 117, 157-163 (1970)
[16] Schmidt, F.K. Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte. Math. Z. 45, 75-96 (1939)
[17] Stichtenoth, H. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. Arch. Math. 24, 527-544 and 615-631 (1973)
[18] Stichtenoth, H. Self-dual Goppa Codes. J. Pure Appl. Algebra 55, 199-211 (1988)
[19] Stöhr, K.O. and Viana, P. A study of Hasse-Witt matrices by local methods. Math. Z. 200, 397-407 (1989)
[20] van Lint, J.H. and van der Geer, G. Introduction to Coding Theory and Algebraic Geometry. Birkhäuser (1988)
[21] Wolfmann, J. The number of points on certain algebraic curves over finite fields. Comm. in Algebra 17, 2055-2060 (1989)

Arnaldo Garcia
Instituto de Matematica
Pura e Aplicada,
Estrada Dona Castorina 110
22.460 Rio de Janeiro,
Brazil

Henning Stichtenoth
Fachbereich 6 - Mathematik
Universität GHS Essen
D-4300 Essen 1,
Fed. Rep. Germany

(Received November 8, 1991)