MATEMÁTICAS

ELEMENTARY ABELIAN P-EXTENSIONS AND CURVES WITH MANY POINTS

Álvaro Garzón R.*, **Arnoldo Teherán Herrera**§

Abstract

Álvaro Garzón Rojas & Arnoldo Teherán Herrera: Elementary abelian $p-$extensions and curves with many points. Rev. Acad. Colomb. Cienc. **36** (138): 243-252, 2012. ISSN 0370-3908.

In this paper we give a generalization of two results obtained by García and Stichtenoth ([G-S]) and use them to exhibit a method to construct curves over finite fields whose number of rational points is large compared to their genus. Such curves are induced by algebraic functions fields obtained from elementary abelian p-extensions of the rational function field $\mathbb{F}_q(x)$ using the trace operator $Tr_{\mathbb{F}_q/\mathbb{F}_p}$

Key words: Finite Fields, Algebraic Curves, Algebraic Function Fields, Elementary Abelian p-Extensions, Rational Points.

Resumen

En este articulo generalizamos dos resultados obtenidos por García & Stictenoth en ([G-S]) y usamos estas generalizaciones para construir curvas sobre cuerpos finitos cuyo número de puntos racionales es grande en comparación con su género. Tales curvas son obtenidas considerando p extensiones abelianas elementales del cuerpo de funciones racionales $\mathbb{F}_q(x)$ usando el operador traza $Tr_{\mathbb{F}_q/\mathbb{F}_p}$.

Palabras clave: Cuerpos finitos, curvas algebraicas, cuerpos algebraicos de funciones, $p-$extensions abelianas elementales, puntos racionales.

*Departamento de Matemáticas, Universidad del Valle, Apartado Aéreo 25360, Cali, Colombia E-mail: alvarogr@univalle.edu.co
§Universidad Industrial de Santander. Bucaramanga, Colombia. E-mail: ateheran@gmail.com
AMS Classification 2000: 14G05.

1. Elementary Abelian p-Extensions

Throughout this note we denote by K a perfect field of characteristic $p > 0$, by F/K an algebraic function field with constant field K and by

$$\wp : u \longmapsto u^p - u$$

the Artin-Schreier operator.

Definition 1.1. For a subset $A \subseteq F$ we denote by $F\left(\wp^{-1}A\right)$, the splitting field of all polynomials $T^p - T - a$, with $a \in A$. For $u \in F$ such that $u \notin Im(\wp)$, the extension $F' = F(y)$ with $\wp(y) = u$ is called an Artin-Schreier extension of F.

The following theorem provides a complete description of the Artin-Schreier extensions. Its proof depends essentially on the following lemma.

Lemma 1.2. (Hilbert's Theorem 90) *Let F' be a finite extension of F whose Galois group G is cyclic generated by σ. Then $\beta \in F'$ has the form $\beta = \alpha - \sigma(\alpha)$, for some $\alpha \in F'$, if and only if $Tr_{F'/F}(\beta) = 0$.*

Proof: See [L-N] Theorem 2.25. ■

Theorem 1.3. *Let F be a field of characteristic $p > 0$. The polynomial*

$$\varphi(T) = T^p - T - u \in F[T], \tag{1}$$

either splits completely over F or else, $\varphi(T)$ is irreducible over F. Moreover the following assertions are equivalent:

1. *F'/F is a cyclic extension of degree p.*
2. *$F' = F(y)$, whose minimal polynomial over F is $\varphi(T)$, where $\varphi(T)$ is defined as (1), for some $u \in F$.*
3. *F' is the splitting field of an irreducible polynomial of the form (1), for some $u \in F$.*

Proof: Suppose that $\varphi(y) = 0$, then for $t \in \mathbb{F}_p \subset F$ we have $\varphi(y+t) = 0$ and since $\varphi(T)$ is a separable polynomial of degree p, it follows that $y, y+1, y+2, ..., y+(p-1)$ are all its roots.

Now, its is clear that, if $y \in F$, then F is the splitting field of $\varphi(T)$.

It remains to consider the case $y \notin F$. Let $F' = F(y)$. To prove that $\varphi(T)$ is irreducible over F it is enough to prove that $[F' : F] = p$, that is to say, that $\varphi(T)$ is the minimal polynomial of y over F (which, from now on, we will denote by $\min(y, F)$).

Since F' is the splitting field of the polynomial $\varphi(T)$, we have that F'/F is a Galois extension, therefore, it is sufficient to show that $|\text{Gal}\ (F'/F)| = p$.

For this end, observe that since each $\sigma \in \text{Gal}\ (F'/F)$ is completely determined by its action on y and σ permutes all the roots of $\varphi(T)$, then $\sigma(y) = y + t$ for some $t \in \{0, 1, ..., p-1\}$, hence, $|\text{Gal}\ (F'/F)| = p$.

Now we will to prove the equivalences:

$(1 \Longrightarrow 2)$ Suppose that F'/F is a cyclic extension of degree p and let $\sigma \in \text{Gal}\,(F'/F)$ be such that $\text{Gal}\,(F'/F) = \left\{id, \sigma, \sigma^2, ..., \sigma^{p-1}\right\}$. Since $Tr_{F'/F}(-1) = -p = 0$, then by Lemma 1.2, there exist $y \in F'$ such that $y - \sigma(y) = -1$. Moreover, since $y - \sigma(y) \neq 0$ and $\sigma \in \text{Gal}\,(F'/F)$ then $y \in F' - F$.

On the other hand, observe that $(\sigma(y) - y)^p = (1)^p = 1 = \sigma(y) - y$. That is to say, $\sigma(y^p - y) = y^p - y$, then $y^p - y \in F$, therefore, there exist $u \in F$ such that $y^p - y = u$ and consequently y satisfies the polynomial $\varphi(T) = T^p - T - u \in F[T]$.

Now, since

$$p = [F' : F] = [F' : F(y)]\,[F(y) : F] \tag{2}$$

and $y \notin F$ then $[F(y) : F] > 1$. Thus $[F(y) : F] = p$ and (2) ensures that $[F' : F(y)] = 1$, which is the same as, $F' = F(y)$. Therefore $\varphi(T) = \min(y, F)$.

$(2 \Longrightarrow 3)$ If $F' = F(y)$, with $T^p - T - u = \min(y, F)$, we have that F' is the splitting field of $\min(y, F)$.

$(3 \Longrightarrow 1)$ Assume that F' is the splitting field of an irreducible polynomial of the form $\varphi(T) = T^p - T - u$, for some $u \in F$. Again by similar arguments as above we obtain that $|Gal\,(F'/F)| = p$, which means that F'/F is cyclic of degree p. ■

Definition 1.4. An extension E/F is said to be an Elementary Abelian p-Extension of exponent p and degree p^n if E/F is Galois with $Gal(E/F) \equiv (\mathbb{F}_p)^n$

The following Theorem states a relationship between the additive subgroups of F and the elementary abelian p-extensions. To this end, we first need to establish a result.

Theorem 1.5. *Let F be a field of characteristic $p > 0$. There exist a one to one correspondence between the*

additive subgroups U of F containing $\wp F$ which have finite index $(U:\wp F)$, and the elementary abelian p-extensions. This correspondence is given by

$$\Psi : U \longmapsto F\left(\wp^{-1}U\right).$$

In such case

$$\left[F\left(\wp^{-1}U\right):F\right] = (U:\wp F).$$

The inverse map of Ψ is given by

$$\Psi^{-1} : L \longmapsto L \cap \wp L.$$

Proof: See [La] page 263. ■

Remark 1.6. Observe that, regarding abelian p-torsion groups as vector spaces over $\mathbb{F}_p$ we can as well define $\wp^*$ as the map (induced by $\wp^{-1}$) that takes finite-dimensional vector subspaces $\tilde{U}$ (over $\mathbb{F}_p$) of the quotient space $F/\wp F$ to finite dimensional subspaces $\tilde{V}$ of the $\mathbb{F}_p$ vector space $\wp^{-1}F/F$ (where $\wp^{-1}F$ is the inverse image under $\wp$ in some fixed separable closure F^{sep}). That is to say

$$\wp^*(\tilde{U}) := \{x + F \in \wp^{-1}F/F \text{ such that } x^p - x \in U\}.$$

Finally if instead of Ψ we consider the map

$$\tilde{\Psi} : \tilde{U} \longmapsto F(\wp^*\tilde{U}) = F\left(\wp^{-1}U\right),$$

one can see that, one such n-dimensional subspace $U \subset F/\wp F$ corresponds, in the notation of Theorem 1.5 to a subgroup $U \subset F$ with $U \cap \wp F = 0$ that is a "section" of $\tilde{U}$ in the sense that $\tilde{U} = (U + \wp F)/F$. Therefore, if U and U' are subgroups of F such that:

$$|U| = p^n = |U'| \text{ and } U \cap \wp F = \{0\} = U' \cap \wp F \quad (3)$$

then, the following sentences are equivalent.

(1) $F\left(\wp^{-1}U\right) = F\left(\wp^{-1}U'\right)$.
(2) $U + \wp F = U' + \wp F$.
(3) $U' \subseteq U + \wp F$ and $U \subseteq U' + \wp F$.

(Observe that $F\left(\wp^{-1}U\right) = F\left(\wp^{-1}U'\right)$ exactly when $\tilde{U} = \tilde{U'}$ (more accurately, when $(U + \wp F)/\wp F$ and $(U' + \wp F)/\wp F$ are the same subspace of $F/\wp F$.)) Moreover, if $u, u' \in U - \{0\}$, then

$$F\left(\wp^{-1}u\right) = F\left(\wp^{-1}u'\right) \Leftrightarrow u' = \lambda \cdot u, \text{ for some } \lambda \in \mathbb{F}_p^*. \quad (4)$$

■

Theorem 1.7. *Let U be an additive subgroup of F such that*

$$|U| = p^n \quad \textit{and} \quad U \cap \wp F = \{0\}.$$

Then, the extension $E = F\left(\wp^{-1}U\right)$ is an elementary abelian p-extension of F of exponent p.

Proof: First observe that since E is the splitting field of the set of polynomials $\{T^p - T - u : u \in U\}$, then the extension E/F is a Galois extension. On the other hand, since U is an additive subgroup of F and $char(F) = p$, then there exists $u_1, u_2, ..., u_n \in U$ nonzero elements such that

$$U = \bigoplus_{i=1}^{n} \langle u_i \rangle = \bigoplus_{i=1}^{n} \mathbb{F}_p u_i. \quad (5)$$

We can find $y_i \in E$ $(1 \le i \le n)$, such that $y_i^p - y_i = u_i$. Now, by Theorem 1.3 we have that

$$F\left(\wp^{-1}u_i\right) = F(y_i), \quad (6)$$

and since $F(\wp^{-1}u_i) = F(\wp^{-1}\lambda u_i)$ for each $\lambda \in \mathbb{F}_p^*$ (Remark 1.6), we obtain

$$E = F(y_1, y_2, ..., y_n). \quad (7)$$

Now, since y_i is a root of $\varphi_i(T) = T^p - T - u_i$, then the extension E/F is finite. In order to prove that $[E:F] = p^n$, first observe that,

$$F(\wp^{-1}(U + \wp F)) = F(\wp^{-1}U) \quad (8)$$
$$= E. \quad (9)$$

Since $[F(\wp^{-1}(U+\wp F)) : F] = [E:F] < \infty$, by Theorem 1.5 we obtain

$$(U + \wp F : \wp F) < \infty, \quad (10)$$

as well as

$$[E:F] = (U + \wp F : \wp F) = |(U + \wp F)/\wp F|. \quad (11)$$

But

$$(U + \wp F)/\wp F = \{y + \wp F : \ y \in (U + \wp F)\} \quad (12)$$
$$= \{w^p - w + u + \wp F : \ w \in F, \ u \in U\} \quad (13)$$
$$= \{u + \wp F : \ u \in U\}. \quad (14)$$

So, for $a, b \in U$, since $U \cap \wp F = \{0\}$ then

$$a + \wp F = b + \wp F \Longleftrightarrow a - b \in \wp F \Longleftrightarrow a = b, \quad (15)$$

consequently, $[E:F] = p^n$. Next we prove that $\mathrm{Gal}\,(E/F) \equiv (\mathbb{F}_p)^n$: For $i \in \{1, 2, ..., n\}$ we define $\sigma_i : E \longrightarrow E$ as follows,

$$\sigma_i = \begin{cases} \sigma_i(w) = w & \text{if } w \in F \\ \sigma_i(y_j) = y_i + 1 & \text{if } i = j \\ \sigma_i(y_j) = y_j & \text{if } i \neq j. \end{cases} \quad (16)$$

Observe that σ_i is the identity on

$$F_i := F(y_1, ..., y_{i-1}, y_{i+1}, .., y_n),$$

therefore by Theorem 1.3, the polynomial $\varphi_i(T) = T^p - T - u_i$ is irreducible over F_i (otherwise $y_i \in F_i$ and $[E : F] \leq p^{n-1}$ which is a contradiction) hence the σ_i are actually well defined. Now it is clear that each $\sigma_i \in \text{Gal}\,(E/F)$ and $\langle \sigma_i \rangle \equiv \mathbb{F}_p$, also

(1) $\sigma_i = \sigma_j$ if and only if $i = j$.
(2) If $\sigma_i = \sigma_j^m$ then, $i = j$ and $m \equiv 1 (\text{mod } p)$.

In fact, if $\sigma_i = \sigma_j^m$ then,

$$y_i + 1 = \sigma_i(y_i) = \sigma_j^m(y_i) = \begin{cases} y_i + m & \text{if } i = j \\ y_i & \text{if } i \neq j, \end{cases} \quad (17)$$

it follows that $i = j$ and $m \equiv 1 \pmod p$. Therefore

$$\text{Gal}\,(E/F) = \prod_{i=1}^{n} \langle \sigma_i \rangle \equiv (\mathbb{F}_p)^{n.}$$

■

The converse of the Theorem 1.7 also holds. To prove it, we need the following lemma.

Lemma 1.8. *Suppose that L/M is a finite Galois extension with Galois Group of the form*

$$G = \text{Gal}\,(E/F) = G_1 \times G_2 \times ... \times G_n. \quad (18)$$

If

$$H_i = G_1 \times ...G_{i-1} \times \{\iota\} \times G_{i+1} \times ... \times G_n \quad (19)$$

where $\{\iota\}$ is the i-th coordinate and

$$L_i = M\,(H_i) = \{\alpha \in L : \sigma\,(\alpha) = \alpha, \forall \sigma \in H_i\}$$

then

(1) *L_i/M is a Galois extension with Galois group* $\text{Gal}\,(L_i/M) \cong G_i$.
(2) $L = L_1L_2...L_n = \prod_{i=1}^{n} L_j$.
(3) *For each* $i \in \{1, 2, ..., n\}$: $L_i \cap (L_{i+1}...L_n) = F$.

Proof: See [Ro] Corollary 5.5.4. ■

Theorem 1.9. *If E/F is an elementary abelian p-extension of F of degree p^n, then*

$$E = F\left(\wp^{-1}U\right), \quad (20)$$

for some additive subgroup U of F which satisfies (3).

Proof: Since E/F is an elementary abelian extension of degree p^n, then

$$G = \text{Gal}\,(F'/F) \equiv (\mathbb{F}_p)^n, \quad (21)$$

thus, $G = G_1 \times ... \times G_n$, where each G_i has order p. Let us define for $j \in \{1, 2, ..., n\}$ H_j and E_j, be as in the Lemma 1.8. Then by 1.8 (a)

$$[E_j : F] = |\text{Gal}\ (E_j/F)| = |G_j| = p, \quad (22)$$

consequently, by Theorem 1.3, there exist $u_j \in F \backslash \text{Im}(\wp)$ such that $E_j = F\,(y_j)$ for some $y_j \in E_j$ with ${y_j}^p - y_j = u_j \in F$, which amounts to, $\langle u_j \rangle \cap \wp F = \{0\}$. Observe that $F\,(y_1, y_2, ...y_n) \subseteq E$ and since $E_j = F\,(y_j) \subseteq F\,(y_1, y_2, ...y_n)$, from Lemma 1.8 (b), $E = \prod_{j=1}^{n} E_j \subseteq F\,(y_1, y_2, ...y_n)$, and therefore

$$E = F\,(y_1, y_2, ...y_n) = F\left(\wp^{-1}(\{u_1, ..., u_n\})\right). \quad (23)$$

We now claim that $u_1, ..., u_n$ are linearly independent over $\mathbb{F}_p$. In fact suppose there is a non-trivial linear combination $\sum_{i=1}^{n} \alpha_i u_i = 0$ with $\alpha_1, ..., \alpha_n \in \mathbb{F}_p$, then

$$0 = \sum_{i=1}^{n} \alpha_i u_i = \sum_{i=1}^{n} \alpha_i\,(y_i^p - y_i) = \left(\sum_{i=1}^{n} \alpha_i y_i\right)^p - \sum_{i=1}^{n} \alpha_i y_i,$$

hence $x := \sum_{i=1}^{n} \alpha_i y_i \in \mathbb{F}_p \subset E_i$. Now if we assume that $\alpha_1 \neq 0$, then $y_1 = 1/\alpha_1(x - \sum_{i=2}^{n} \alpha_i y_i)$ and since, for $j = 2, ..., n$, we have that $y_j \in E_j \subseteq E_2E_3...E_n$, then $y_1 \in E_2E_3...E_n$. On the other hand by Lemma 1.8, $y_1 \in E_1 \cap (E_2E_3...E_n) = F$, consequently $E_1 = F\,(y_1) = F$, which is a contradiction since $[E_1 : F] = p > 1$. Therefore, $\alpha_1 = 0$. Similar arguments will lead us to prove that $\alpha_2 = ... = \alpha_n = 0$. Let U be the subgroup generated by $u_1, u_2, ..., u_n$. Then by (23), $E = F\left(\wp^{-1}U\right)$ therefore only remains to prove that $U \cap \wp F = \{0\}$. In fact, if $x \in U \cap \wp F$, then $x = y^p - y = \sum_{i=1}^{n} \lambda_i u_i$, with $y \in F$ and each $\lambda_i \in \mathbb{F}_p$. Therefore it is enough to prove that $\lambda_1 = 0$. For this end, observe that

$$y^p - y = \sum_{i=1}^{n} \lambda_i u_i = \sum_{i=1}^{n} \lambda_i\,(y_i^p - y_i) = \left(\sum_{i=1}^{n} \lambda_i y_i\right)^p - \sum_{i=1}^{n} \lambda_i y_i, \quad (24)$$

therefore $z = \sum_{i=1}^{n} \lambda_i y_i - y \in \mathbb{F}_p$, so if $\lambda_1 \neq 0$, we have that

$$y_1 = \frac{1}{\lambda_1}\left(z + y - \sum_{i=2}^{n} \lambda_i y_i\right) \in E_1 \cap (E_2 E_3 ... E_n) = F, \quad (25)$$

which is a contradiction. ■

Theorem 1.10. *Let U be an additive subgroup of F such that*

$$|U| = p^n \quad \text{and} \quad U \cap \wp F = \{0\}.$$

If $E = F(\wp^{-1}U)$, then there exist $t = (p^n - 1)/(p - 1)$ intermediate fields $F \subseteq E_i \subseteq E$ such that $[E_i : F] = p$, where $E_i = F\left(\wp^{-1}u\right)$ with $u \in U - \{0\}$.

Proof: If $u \in U - \{0\}$, then $F\left(\wp^{-1}u\right) = F(y)$ with $y^p - y = u$ and by Theorem 1.3, $\left[F\left(\wp^{-1}u\right) : F\right]$ is either 1 or p. But if $\left[F\left(\wp^{-1}u\right) : F\right] = 1$, then $F = F(y)$ therefore $u = y^p - y \in U \cap \wp F = \{0\}$ which is a contradiction with the choice of u, hence $\left[F\left(\wp^{-1}u\right) : F\right] = p$. On the other hand, if E_i is a subfield such that $F \subseteq E_i \subseteq F\left(\wp^{-1}U\right)$ and $[E_i : F] = p$, then by Theorem 1.3, E_i is the splitting field of one irreducible polynomial of the form $\varphi(T) = T^p - T - u$ for some $u \in F$. Now, since $E_i = F\left(\wp^{-1}u\right) \subseteq F\left(\wp^{-1}U\right)$, then by Remark 1.6 we have that $\langle u \rangle + \wp F \subseteq U + \wp F$, hence $u = u' + w^p - w$, for some $u' \in U$ and $w \in F$, from which $E_i = F\left(\wp^{-1}u\right) = F\left(\wp^{-1}u'\right)$ for some $u' \in U$. In sum each subfield E_i such that $F \subseteq E_i \subseteq E$ and $[E_i : F] = p$ has the form $E_i = F\left(\wp^{-1}u\right)$ for some $u \in U - \{0\}$. Finally by Remark 1.6 we obtain the number of these subfields. ■

Theorem 1.11. *Let K be a field of characteristic $p > 0$ and F/K an algebraic function field of transcendence degree one over K, 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 $E_1, ..., E_t$ (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*

$$g(E) = \sum_{j=1}^{t} g(E_j) - \frac{p}{p-1}(p^{n-1} - 1)g(F). \quad (26)$$

Proof: Let $G = Gal\,(E/F)$. For a subgroup $H \subseteq G$ consider the fixed field $E_H \subseteq E$ whose genus $g(E_H)$ is denoted by g_H and the trace idempotent ϵ_H:

$$\epsilon_H = \frac{1}{|H|}\sum_{\sigma \in H} \sigma \in \mathbb{Q}(G).$$

The idea of the proof is to construct a relationship of the kind

$$\sum_{H \subseteq G} r_H \cdot \epsilon_H = 0 \in \mathbb{Q}(G),$$

with $r_H \in \mathbb{Q}$,because in this case the genera would satisfy the same relation (see [Ka])

$$\sum_{H \subseteq G} r_H \cdot g(E_H) = 0.$$

First, observe that G has exactly t subgroups with order p^{n-1}. In fact, by one side, for $j \in \{1, ..., t\}$ the Galois group H_j of the extension E_j/F, is one of such subgroups. On the other hand, if $H \subseteq G$ is a subgroup such that $|H| = p^{n-1}$, then since E/E_H is a Galois extension with $H = Gal(E/E_H)$, we have $[E : E_H] = |H| = p^{n-1}$, from which we get $[E_H : F] = p$ and $E_H = E_j$ for some $j \in \{1, ..., t\}$ consequently,

$$H = \text{Gal}\,(E/E_H) = \text{Gal}\,(E/E_j) = H_j. \quad (27)$$

Now we shall show that any $\sigma \in G - \{id\}$ is contained in precisely t subgroups H_j. In fact, each H_j has the form

$$H_j = \bigoplus_{m=1}^{n-1} \langle \lambda_{jm} \rangle = \bigoplus_{m=1}^{n-1} \mathbb{F}_p \lambda_{jm}, \quad (28)$$

where each λ_{jm} has order p and the set $\{\lambda_{j1}, ..., \lambda_{jn-1}\}$ is a basis of H_j over $\mathbb{F}_p$. Now, if $\sigma \in G - \{id\}$, then $\sigma \notin H_j$ if and only if $\sigma \notin \mathbb{F}_p \lambda_{jm}$ for $m = 1, ..., n-1$. That is to say, there exist p^{n-1} subgroups H_j such that $\sigma \notin H_j$. In other words σ is contained in precisely $t - p^{n-1} = (p^{n-1} - 1)/(p - 1)$ subgroups H_j of G, therefore

$$p^{n-1}\sum_{j=1}^{t} \epsilon_{H_j} = \sum_{j=1}^{t}\sum_{\sigma \in H_j} \sigma \quad (29)$$

$$= \sum_{j=1}^{t} id + \sum_{j=1}^{t}\sum_{\sigma \in H_j \setminus \{id\}} \sigma \quad (30)$$

$$= \frac{p^n - 1}{p - 1} \cdot id + \frac{p^{n-1} - 1}{p - 1}\sum_{\sigma \in G - \{id\}} \sigma. \quad (31)$$

But from $\epsilon_{H_0} = id$ and

$$\epsilon_G = \frac{1}{|G|}\sum_{\sigma \in G} \sigma = \frac{1}{p^n}\left(id + \sum_{\sigma \in G - \{id\}} \sigma\right), \quad (32)$$

it follows that, $\sum_{\sigma\in G-\{id\}} \sigma = p^n\cdot\epsilon_G - id$. Thus

$$p^{n-1}\sum_{j=1}^{t}\epsilon_{H_j} = \frac{p^n-1}{p-1}id + \frac{p^{n-1}-1}{p-1}\left(p^n\epsilon_G - id\right) \quad (33)$$

$$= p^{n-1}id + \frac{p^{n-1}-1}{p-1}p^n\epsilon_G, \quad (34)$$

and

$$\sum_{j=1}^{t}\epsilon_{H_j} = id + \frac{p}{p-1}\left(p^{n-1}-1\right)\cdot\epsilon_G, \quad (35)$$

which amounts to, we have the following relation in $\mathbb{Q}(G)$:

$$\epsilon_{H_0} - \left(\sum_{j=1}^{t}\epsilon_{H_j} - \frac{p}{p-1}\left(p^{n-1}-1\right)\cdot\epsilon_G\right) = 0. \quad (36)$$

The theorem now follows from Kani's result. ■

Observe that the intermediate extension E_j/F mentioned in Theorem 1.10 is an Artin-Schreier extension, whose genus, $g(E_j/K)$ can be computed by [[ST], III.7.8]. This takes us to determine explicitly such intermediate fields, which we will call Artin-Schreier intermediate subfields, for which we give the following results generalizing Propositions 1.1 and 1.2 in ([G-S]).

Before that, we should give a definition. We call a polynomial of the specific form

$$a(T) = a_nT^{p^n} + a_{n-1}T^{p^{n-1}} + ... + a_1T^p + a_0T \in K[T]$$

(where $p = \mathrm{char}\,(K)$) an *additive* polynomial over K. Observe that $a(T)$ is separable if and only if $a_0 \neq 0$.

Theorem 1.12. *Let $h(T) \in F[T]$ be a separable, monic, additive polynomial of degree p^n, with its roots in F. If E/F is an elementary abelian p-extension of degree p^n, then there exists an element $y \in E$ such that $E = F(y)$ whose minimal polynomial over F has the form*

$$\varphi(T) = h(T) - z \in F[T], \qquad with \qquad z \in F. \quad (37)$$

Proof: Let us consider the set $W = \{\alpha :\ h(\alpha) = 0\} \subseteq F$, it is clear that W is a vectorial space over $\mathbb{F}_p$, moreover W is an additive finite subgroup of F. Now, since each cyclic subgroup of W has order 1 or p, then there exist nonzero elements $\mu_1, \mu_2, ..., \mu_n \in W$ such that

$$W = \bigoplus_{i=1}^{n}\langle\mu_i\rangle, \quad (38)$$

and, the set $\beta = \{\mu_1, \mu_2, ..., \mu_n\}$ is a basis of W over $\mathbb{F}_p$. Now, from Lemma 1.8 we can choose $y_1, y_2, ...y_n \in E$ such that $E = F(y_1, y_2, ...y_n)$, with ${y_i}^p - y_i = \mu_i \in F$. If we define σ_i for $i \in \{1, 2, ..., n\}$ as in (16), it is clear that each σ_i is an element of order p of $\mathrm{Gal}\,(E/F)$ and therefore

$$\mathrm{Gal}\,(E/F) = \prod_{i=1}^{n}\langle\sigma_i\rangle. \quad (39)$$

On the other hand, since $\sigma \in \mathrm{Gal}\,(E/F)$, then σ has a unique representation

$$\sigma = \sigma_1^{\nu_1}\circ\sigma_2^{\nu_2}\circ ...\circ\sigma_n^{\nu_n}. \quad (40)$$

with $\nu_i \in \mathbb{F}_p$, then the action of σ over the element $y = \sum_{k=1}^{n}\mu_k y_k$, is given by

$$\sigma(y) = \sum_{k=1}^{n}\mu_k(y_k + \nu_k) =: y + \mu, \quad (41)$$

where $\mu = \sum_{k=1}^{n}\mu_k\nu_k \in W$. It follows from (40) that $\sigma(y) = y$ if and only if $\nu_k = 0$ for $k = 1, 2, ..., n$, that is, $\sigma(y) = y$ if and only if $\sigma = id$, and therefore $E = F(y)$. On the other hand, if $z = h(y)$ and $\sigma \in \mathrm{Gal}\,(E/F)$ then, since $\sigma\,(y) = y + \mu$, for some $\mu \in W$, we have

$$\begin{aligned}\sigma(z) &= \sigma\,(h\,(y))\\ &= h\,(\sigma\,(y))\\ &= h\,(y) + h\,(\mu)\\ &= z.\end{aligned}$$

That is to say $\sigma(z) = z$ and therefore $z \in F$, consequently y is a root of the monic polynomial $\varphi(T)$ whose degree is $p^n = [E : F] = [F(y) : F]$. This implies $\varphi(T) = \min(y, F)$. ■

Reciprocally we have:

Theorem 1.13. *Let $h(T) \in F[T]$ be a separable, monic, additive polynomial of degree p^n, with its roots in F and $z \in F$ such that the polynomial $\varphi(T) = h(T) - z \in F[T]$ is irreducible over F, then the extension $F(y)/F$ where $\varphi(y) = 0$ is an elementary abelian p-extension of degree p^n. The intermediate subfields $F \subseteq E_i \subseteq F(y)$ with $[E_i : F] = p$, have the form $E_i = F(y_\mu)$, where $\mu \in W - 0$, with $W = \{\alpha : h(\alpha) = 0\}$ and each y_μ satisfies the equation $(y_\mu)^p - y_\mu = \mu\cdot z$, therefore $F(y) = F(\wp^{-1}U)$, with $U = \{\mu\cdot z :\ \mu \in W\}$.*

Proof: It is clear that $\varphi(T)$ is the minimal polynomial for y over F. Now, for each $\mu \in W$, $\varphi(y + \mu) = 0$, then all roots of the polynomial $\varphi(T)$ have the form $y + \mu$, with $\mu \in W \subseteq F$, and therefore $F(y)$ is the splitting field of the polynomial $\varphi(T)$. On the other hand since $\sigma \in Gal(F(y)/F)$ permutes the roots of $\varphi(T)$ then

$\sigma(y) = y + \mu$, for some $\mu \in W$, therefore, the application $\sigma \longmapsto \mu$, of $Gal(F(y)/F)$ into group $\langle W, + \rangle$ is an isomorphism, that is to say, $F(y)/F$ is an elementary abelian p-extension of degree p^n.

Now, if $f(T) = \sum_{k=0}^{n-1} \mu^{p^k} T^{p^k} - y_\mu$, then $f(T) \in F(y_\mu)[T]$ and $f(y) = 0$, it follows that $[F(y) : F(y_\mu)] \leq p^{n-1}$. On the other hand, since $(y_\mu)^p - y_\mu = \mu \cdot z$ then $[F(y_\mu) : F] \leq p$ and therefore

$$\begin{aligned} p^n &= [F(y) : F] \\ &= [F(y) : F(y_\mu)][F(y_\mu) : F] \\ &\leq p^{n-1} \cdot p \\ &= p^n, \end{aligned}$$

consequently $[F(y_\mu) : F] = p$. It is to say, $F(y_\mu) = F(\wp^{-1}\mu \cdot z)$. Now, by Remark 1.6, there exist $(p^n - 1)/(p - 1)$ such subextensions $F(y_\mu)/F$ and therefore $F(y) = F(\wp^{-1}U)$ where $U = \{\mu \cdot z : \mu \in \mathbb{F}_{p^n}\}$. Finally by Theorem 1.10 there exist exactly $(p^n - 1)/(p - 1)$ intermediate fields $F \subseteq E_i \subseteq F(y)$ with $[E_i : F] = p$, therefore such $F(y_\mu)$ must be one of the E_i. ■

2. An application to the construction of curves over finite fields

It is well known that algebraic function fields over finite fields have many applications in coding theory, and the latter is closely related to cryptography, see for example [N-Ch]. In this section we exhibit a method to construct algebraic function fields over finite fields (algebraic curves) with many rational places (rational points).

Let p be a prime number, $K = \mathbb{F}_q$ the finite field with $q = p^n$ elements and $F := \mathbb{F}_q(x)$ the rational function field over the finite field $\mathbb{F}_q$. By E/K we mean a function field of transcendence degree one over K, with constant field K. We denote by $N_g(q)$ the maximum number of rational places of the function field E/K of genus $g(E/K) = g$. The Hasse-Weil bound implies

$$N_g(q) \leq q + 1 + 2 \cdot g\sqrt{q}. \tag{42}$$

After Weil proved his bound around 1940 the question how many rational places may lie on a function field over a finite field $\mathbb{F}_q$ remained untouched for many years. In 1980 Goppa came up with the beautiful idea to associate an error-correcting code to a linear system on a curve over a finite field, see [Go]. In order to construct good codes one needs function fields with many places and thus Goppa's work led to a revival of interest in rational points on function fields (algebraic curves) over finite fields. Applications in cryptography and recent constructions of quasi-random point sets also require curves with many points and added a further impetus to work in the field.

In 1981 Ihara showed in [I] that

$$N_g(q) \leq q + 1 + [(\sqrt{(8q+1) + 4(q^2 - q)g} - g)/2]. \tag{43}$$

For $g > (q - \sqrt{q})/2$ this bound is better that Weil's bound and gives the asymptotic bound

$$A(q) := \limsup_{g \to \infty} \frac{N_g(q)}{g} \leq \sqrt{2q + \frac{1}{4}} - \frac{1}{2} \tag{44}$$

Refining Ihara's idea to derive (44) Drinfeld and Vladut proved that

$$A(q) \leq \sqrt{q} - 1. \tag{45}$$

Since the asymptotic bound (45) of Drinfeld-Vladut is approximately $1/\sqrt{2}$ times the asymptotic Ihara bound (44) we think that it is reasonable to put this qualification as requirement to filter out curves which should be considered 'poor'.

To begin our construction, let us denote by $a(T)$ the additive polynomial

$$a(T) = T^{p^{n-1}} + T^{p^{n-2}} + ... + T^p + T \in \mathbb{F}_q[T]. \tag{46}$$

We will consider extensions of the rational function field $\mathbb{F}_q(x)$ of the kind $E/\mathbb{F}_q$ where $E = \mathbb{F}_q(x, y)$ is defined by the equation:

$$\begin{aligned} a(y) &= y^{p^{n-1}} + y^{p^{n-2}} + ... + y^p + y \\ &= \mu(x) := \mathcal{R}_\ell(a(f(x))) \end{aligned} \tag{47}$$

where $f(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$ and $\mathcal{R}_\ell(a(f(x)))$ denotes the remainder of the Euclidean division of the polynomial $f(x)$ by $\ell(x) = x^q - x$. That is to say extensions of the kind,

$$\begin{array}{c} E := \mathbb{F}_q(x, y)/(a(y) - \mu(x)) \\ \uparrow \\ F := \mathbb{F}_q(x) \end{array}$$

The reason to consider this type of extensions is that the number of rational places of E/K is related with the image of the function $a : \mathbb{F}_q \longrightarrow \mathbb{F}_p$. More precisely we have.

Theorem 2.1. *The polynomial $\mu(x) = \mathcal{R}_\ell(a(f(x)))$ defined as (47) has the following property:*

$$\text{for all } \alpha \in \mathbb{F}_q, \quad \mu(\alpha) \in \mathbb{F}_p$$

Proof: It is enough to prove that

$$x^q - x \,|\, \mu(x)^p - \mu(x)\,.$$

Since

$$a(f(x)) = (x^q - x)h(x) + \mu(x)\,,$$

for some polynomial $h(x) \in \mathbb{F}_p[x]$, then

$$\mu(x)^p - \mu(x) = a(f(x))^p - (x^q - x)^p \cdot h(x)^p - a(f(x)) + (x^q - x) \cdot (x)\,.$$

Now, since $f(x) \in \mathbb{F}_p[x]$ and $a(T)$ is additive, the result follows. ■

Remark 2.2. Observe that in accordance with Theorem 2.1, we have that, for $\alpha \in \mathbb{F}_q$, the equation

$$a(T) = T^{p^{n-1}} + T^{p^{n-2}} + ... + T^p + T = \mu(\alpha), \quad (48)$$

has p^{n-1} solutions in $\mathbb{F}_q$, therefore the induced curve by the function field E/K has at least $p^n \cdot p^{n-1}$ places of degree one. This leads us to expect to get good curves. ■

The following result provides us a relationship among the genus of the function field E/K and the genus of the Artin-Schreier intermediate subfields E_1, E_2,..., E_t. $(t = (p^{n-1} - 1)/(p - 1))$.

Theorem 2.3. *With the previous notations, the genus of E/K is given by*

$$g(E/K) = \frac{p-1}{2} \sum_{i=1}^{t} (m_{P_\infty}(\lambda_i \cdot \mu(x)) - 1), \quad (49)$$

where m_{P_∞} is defined as follows:

$$m_{P_\infty}(u) = \begin{cases} -1 & \text{if there is } z \in F:\ v_{P_\infty}(u - \wp(z)) \geq 0, \\ m & \text{if there is } \ z \in F:\ v_{P_\infty}(u - \wp(z)) = \\ & -m < 0 \text{ and } m \not\equiv 0 \bmod p. \end{cases} \quad (50)$$

and $\lambda_i \in (W - \{0\})/\mathbb{F}_p^*$, with $W = \{\alpha : a(\alpha) = 0\} \subseteq \mathbb{F}_q$.

Remark 2.4. Lemma **III.7.7** in [ST], guarantees that we can exclude the case $v_{P_\infty}(u - \wp(z)) = -m < 0$ for an integer $m \equiv 0\,(mod\, p)$ in the above definition for $m_{P_\infty}(u)$

Indeed, first observe that from ([ST], I.4.18) together with Theorem 1.11 we have that:

$$g(E/K) = \sum_{i=1}^{t} g(E_j/K). \quad (51)$$

On the other hand, by Theorem 1.13, each Artin-Schreier subfield E_λ/F has the form

$$E_\lambda = \mathbb{F}_q(x, y_\lambda) \quad (52)$$

where $y_\lambda^p - y_\lambda = \lambda \cdot \mu(x)$ and $\lambda \in W - \{0\}$. Now, since $\mu(x) \in \mathbb{F}_q[x]$, then each place of F different from P_∞ is unramified in E_λ, in this way, from ([ST], III.7.8), the genus of E_λ/K is given by

$$g(E_\lambda/F) = \frac{p-1}{2}(m_{P_\infty}(\lambda \cdot \mu(x)) - 1), \quad (53)$$

Now, since there exist exactly t different subfields of Artin-Schreier, then there are $\lambda_1, ..., \lambda_t$ in W such that, each one of those Artin-Schreier subfields have the form $E_{\lambda_i} = \mathbb{F}_q(x, y_{\lambda_i})$. Finally, from (53) and (51) we have the result.

Next, we exhibit a technique that allow us to count the rational places of E/K. For this, we will denote by $\mathcal{C}(E/F)$, the induced curve by the function field E/K.

Lemma 2.5. *Let us consider the polynomial*

$$\varphi_t(T) = \mu(T) - t, \quad (54)$$

where $t \in \mathbb{F}_p$ and $\mu(T)$ are defined as in (47). Then, for $x \in \mathbb{F}_q$, there exist $y \in \mathbb{F}_q$ such that $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ belongs to $\mathcal{C}(E/F)$ if and only if $\varphi_t(x) = 0$, for some $t \in \mathbb{F}_p$.

Proof: Let us suppose that exists $y \in \mathbb{F}_q$ such that (x, y) belongs to $\mathcal{C}(E/F)$, it is to say, $a(y) = \mu(x)$. Since $a(y) \in \mathbb{F}_p$, then by taking $t = a(y)$ we obtain the desired result. Reciprocally, if $\mu(x) = t$ for some $t \in \mathbb{F}_p$, and since the function a is surjective ([L-N], 2.23), then $a(y) = t$ for some $y \in \mathbb{F}_q$, it is to say, $\mu(x) = a(y)$. ■

Lemma 2.6. *With the above notations, $\mu(\alpha) = a(f(\alpha))$ for all $\alpha \in \mathbb{F}_q$.*

Proof: By the division algorithm, there exists $h(x), \mathcal{R}_\ell(a(f(x))) \in \mathbb{F}_q[x]$ such that

$$a(f(x)) = h(x)\ell(x) + \mathcal{R}_\ell(a(f(x))),$$

with degree $(\mathcal{R}_\ell(a(f(x))))$ < degree $(\ell(x))$. Then,

$$\mu(x) = \mathcal{R}_\ell(a(f(x))) \quad (55)$$
$$= a(f(x)) - h(x)\ell(x) \quad (56)$$

and since $\ell(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$, we have $\mu(\alpha) = a(f(\alpha))$ ■

As consequence of all the above mentioned we have,

Theorem 2.7. *The number of rational places of the elementary abelian p-extension defined by (47) is given by*

$$N(E/\mathbb{F}_q) = p^{n-1}\sum_{t\in\mathbb{F}_p}\deg(\gcd(\varphi_t(x),\ell(x))) + \gamma, \quad (57)$$

where, γ denotes the number of rational places of E coming from the ramification, which is one or zero.

Proof: For fixed $x \in \mathbb{F}_q$, we have that (x, y) is a rational point of the curve $\mathcal{C}(E/\mathbb{F}_q(x))$ if and only if $y = f(x) + \alpha$, where $\alpha \in W$. In fact, if (x, y) is a rational point of $\mathcal{C}(E/\mathbb{F}_q(x))$ then

$$a(y - f(x)) = a(y) - a(f(x)) = \mu(x) - \mu(x) = 0, \quad (58)$$

therefore $y - f(x) \in W$. Reciprocally, if $y = f(x) + \alpha$, where $\alpha \in W$, then

$$a(y) = a(f(x)) + a(\alpha) = \mu(x) \quad (59)$$

and therefore (x, y) is a rational point of $\mathcal{C}(E/\mathbb{F}_q)$. Now, for each $x \in \mathbb{F}_q$ such that $\varphi_t(x) = 0$, we have $p^{n-1} = \deg(a(T))$ places of degree one of E. Additionally, since for all place P of F different of P_∞, P is unramified in E, then $\gamma = 1$ or 0. Therefore,

$$\begin{aligned} &N(E/\mathbb{F}_q) = \\ &= \deg(a(T))\,|\{\alpha\in\mathbb{F}_q:\ (\exists\, t\in\mathbb{F}_p)(\varphi_t(\alpha)=0)\}| \ +\gamma \quad (60)\\ &= p^{n-1}\sum_{t\in\mathbb{F}_p}|C_t| + \gamma, \quad (61)\end{aligned}$$

where $C_t = \{\alpha \in \mathbb{F}_q :\ \varphi_t(\alpha) = 0\}$ y $t \in \mathbb{F}_p$. On the other hand, if $d_t(x) = \gcd(\varphi_t(x), \ell(x))$, then $d_t(\alpha) = 0$ if and only if $\alpha \in \mathbb{F}_q$ and $\varphi_t(\alpha) = 0$ and since $d_t(x)$ is separable, then $|C_t| = deg(d_t(x))$. ■

3. Examples

In this section we give examples of elementary Abelian p-extensions of the kind given by (47). We will to consider the particular case when n is odd and $f(x) = x^{p^{k+1}}$ with $k = (n-1)/2$ and we will determine the genus and the number of rational places of these extensions using the formulas (49) and (57).

Example 3.1. If $p = 2$, and $n = 3$, then $k = 1$, $q = 8$. Also,

$$\begin{aligned} f(x) &= x^3, \quad (62)\\ a(T) &= T^4 + T^2 + T, \quad (63)\\ \mu(x) &= \mathcal{R}_\ell(a(f(x))) = x^6 + x^5 + x^3, \quad (64)\end{aligned}$$

in this case, there are exactly $t = 3$ different subfields E which are Artin-Schreier extensions over F. For all $\lambda \in (W - \{0\})/\mathbb{F}_2^*$ we have $v_{\mathcal{P}_\infty}(\lambda\cdot\mu(x) + \wp(z(x))) = -5 < 0$ and since $-5 \ncong 0(\mathrm{mod}2)$ then, from ([ST], III.7.8), we obtain $m_{\mathcal{P}_\infty}(\lambda\cdot\mu(x)) = 5$. Observe that this value is independ of the root λ, therefore there exist exactly 3 different Artin-Schreier extensions generated by such roots, and in accordance with (49) we have

$$g(E/\mathbb{F}_8) = \frac{2-1}{2}(3)(5-1) = 6. \quad (65)$$

Now, for the number of rational places we have that

$$\begin{aligned} \gcd(\varphi_0(x),\ell(x)) &= x^4 + x^3 + x, \quad (66)\\ \gcd(\varphi_1(x),\ell(x)) &= x^4 + x^3 + x^2 + x. \quad (67)\end{aligned}$$

Since, the place P_∞ of F is the only place that ramifies in the extensionE/F then by (57) we have

$$N(E/\mathbb{F}_8) = 4(4+4) + 1 = 33. \quad (68)$$

This is the best value known. See [VV].

Example 3.2. Taking $p = n = 3$, then $q = 27$ and $k = 1$. Also,

$$\begin{aligned} f(x) &= x^4, \quad (69)\\ a(T) &= T^9 + T^3 + T. \quad (70)\\ \mu(x) &= \mathcal{R}_\ell(a(f(x))) = x^{12} + x^{10} + x^4. \quad (71)\end{aligned}$$

Then $t = 4$ and for all $\lambda \in (W - \{0\})/\mathbb{F}_3^*$ we have, $v_{\mathcal{P}_\infty}(\lambda\cdot\mu(x) + \wp(z(x))) = -10 < 0$ and $m_{\mathcal{P}_\infty}(\lambda\cdot\mu(x)) = 10$. Therefore,

$$g(E/K) = \frac{3-1}{2}(4)(10-1) = 36. \quad (72)$$

Now,

$$\begin{aligned} \gcd(\varphi_0(x),\ell(x)) &= x^9 + x^7 + x, \quad (73)\\ \gcd(\varphi_1(x),\ell(x)) &= x^6 + x^4 + x^2, \quad (74)\\ \gcd(\varphi_2(x),\ell(x)) &= x^{12} + x^{10} + x^4 + 1, \quad (75)\end{aligned}$$

and since P_∞ is totally ramified and rational in $E/\mathbb{F}_{27}$ then we have

$$N(E/\mathbb{F}_{27}) = 9(9+6+12) + 1 = 244. \quad (76)$$

We do not known any function field over $\mathbb{F}_{27}$ of genus 36 having more than 244 rational places (see [VV]).

The following table contains the values obtained for the genus and the number of rational points by taking different values for p and n, also we compare this values obtained with the Ihara's bound.

p	n	g	$Ihara$	N
2	5	60	$[383, 542]$	513
2	7	504	$[5965, 8437]$	8193
3	5	1080	$[17549, 24817]$	19684

(77)

Acknowledgements. The authors deeply appreciate the helpful comments and suggestions made by the referees.

References

[G-S] Garcia and Stichtenoth. Elementary abelian p-extensions of algebraic functions fields. Manuscripta mathematica, Springer-Verlag. pag 67-79, 1991.

[L-N] Lidl Rudolf and Niederreiter Harald. Introduction to finite fields and their applications. Cambridge university press, 1994.

[Go] V.D.Goppa, Codes on algebraic curves. Sov Math.Dokl 24 (1981), 170-172.

[La] Lang Serge, Algebra, Adisson Wesley Publishing Company, 1970.

[Ka] Kani Ernest, *Relations between the genera and between the Hasse-Witt invariants of Galois covering of curves*, Canad. Math. Bull, Vol 28, pag 321-327, 1985.

[N-Ch] Harald Niederreiter, Huaxiong Wang and Chaoping Xing, Function Fields over Finite Fields and their applications to Cryptography. Topics in Geometry, Coding Theory and Cryptography, Springer-Verlag. 2007

[I] Ihara Y. Some remarks on number of rational points of algebraic curves over finite fields. J Fac Sci Tokyo 28 (1981), p. 721-724.

[Ro] Roman Steve. Field Theory. Springer-Verlag, 1991.

[ST] Stichtenoth Hennig. Algebraic funtions fields and codes. Springer-Verlag, 1993.

[VV] Van Der Geer Gerard and Van Der Vlugt Marcel. Tables of curves with many points. [Online], http://www.science.uva.nl/ geer.

Recibido el 4 de noviembre de 2009

Aceptado para su publicación el 21 de junio de 2010

Versión revisada recibida el 5 de marzo de 2012