Università degli Studi di Palermo

Dipartimento di Matematica e Applicazioni

Dottorato di Ricerca in Matematica

- XVIII ciclo -

Automorphisms of Generalized Algebraic Geometry Codes

AUTHOR

Alberto Picone

COORDINATOR

Prof. Vassil Kanev

RESEARCH SUPERVISOR

Prof. Antonino Giorgio Spera

Settore scientifico-disciplinare MAT/03

To my wife.

Table of Contents

Acknowledgements

I would like to thank Professor Antonino Giorgio Spera, my supervisor, for his many suggestions and constant support during this years.
Professors G. Korchmáros and H. Stichtenoth expressed their interest in my work and provided me many useful references and friendly encouragement.
I am grateful to my parents for their **patience** and to my little niece Alessandra for all the times she *studied* with me.

Finally, I thank my wife Carmen: Would I have renounced all my dreams for her?

Palermo Alberto Picone
December 15, 2006

Introduction

In his well-known construction of algebraic geometry codes, Goppa (see [Go]) used rational places of algebraic function fields. This construction was a breakthrough in algebraic coding theory because it gives sequences of linear codes beating the asymptotic Gilbert-Varshamov bound. However, in order to have good algebraic geometry codes, function fields with as many rational places as possible are needed. Unfortunately, function fields over small finite fields have few rational places compared with their genus.

To solve this problem, a new construction of linear codes, said to be *generalized algebraic geometry codes*, based on places of degree not necessarily one, was introduced by Xing, Niederreiter and Lam [X-N-L] and were also used in order to obtain codes with better parameters compared with Brouwer's table (see [Bro] and [D-N-X]). In particular we are interested in generalized algebraic geometry codes constructed by Spera ([Sp1] and [Sp2]) making use of places which are of the same degree.

An important aspect of coding theory is the knowledge of the automorphism group of a code. In fact, it can be also useful in developing a decoding algorithm.
For algebraic geometry codes, Goppa already observed that automorphisms of the underlying function field induce automorphisms of the codes. Stichtenoth in [St2]

gave a detailed exposition of this fact. In the same paper, he proved that all the automorphisms of a rational algebraic geometry code are induced by automorphisms of the underlying rational function field. After, many others authors determined the automorphism groups of special algebraic codes as elliptic, hyperelliptic and Hermitian codes (see [J-K], [Wes], [X1] and [X2]).

In this thesis a special subgroup of the automorphism group of generalized algebraic geometry codes is determined when the underlying function field is rational, elliptic or hyperelliptic.

This work is structured as follows.

In Chapter 1 we recall the necessary basic notions about algebraic function fields and coding theory.

In Chapter 2 we study the automorphism group of a algebraic geometry code constructed over rational (see [St2]), elliptic or hyperelliptic ([Wes]) function field. More precisely, we show under which condition the automorphism group of the code is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(F|\mathbb{F}_q)$ of the underlying function field $F|\mathbb{F}_q$. This subgroup is the stabilizer, in $\mathrm{Aut}(F|\mathbb{F}_q)$, of the divisors associated with the code.

In Chapter 3 we introduce the concept of n-automorphism of a generalized algebraic geometry code and we recall the Spera's result ([Sp2]) which shows that the stabilizer of the divisors in $\mathrm{Aut}(F|\mathbb{F}_q)$ is embedded into the n-automorphism group. Based on this result, starting from Section 3.2.1, it is developed the original work of this thesis. More precisely, we determine conditions on the divisors associated with the code, so that the n-automorphism group is isomorphic to the stabilizer of the divisors in $\mathrm{Aut}(F|\mathbb{F}_q)$ when $F|\mathbb{F}_q$ is a rational, elliptic or hyperelliptic function field.

In Chapter 2 and Chapter 3 we regard an elliptic function field as a special case of a hyperelliptic function field. Moreover, we always suppose the characteristic of $\mathbb{F}_q$ is not equal to 2, even if the obtained results can be similarly proved when $\operatorname{char} \mathbb{F}_q = 2$.

In the last chapter we explicitly construct specific generalized algebraic geometry codes and their $n-$automorphism groups. These constructions show that it is possible to have generalized algebraic geometry codes with a nontrivial $n-$automorphism group. For such constructions we use the software Mathematica v5, with which we check the irreducibility of some polynomials and we do all the computations needed.

Chapter 1

Background

In this chapter we recall some fundamental knowledge about algebraic function fields and linear coding theory. In particular, we focus on those concepts and results that are needed in the next chapters. Sometimes we will state results not in their most general form but in the one in which we need them. The results will be presented without proofs since they are standard results from textbooks. The reader can found them, for instance, in [v.L], [St1] and [T-V].

1.1 Algebraic Function Fields

We introduce some basic notions and results of algebraic function fields theory. For the convenience of the reader, we also recall some basic results even if they are well-known.

An *algebraic function field in one variable* (or simply *function field*) is an extension field $F|K$ such that there exists a transcendental element $x \in F$ over K with $[F : K(x)] < \infty$.

If we denote by $\overline{K}$ the algebraic closure of K in F

$$\overline{K} = \{\, x \in F \mid x \text{ is algebric over } K \,\},$$

then also $F|\overline{K}$ is a function field. When $\overline{K} = K$ we call K the *full constant field of* F.

In the following all the rings considered are commutative with unit and if $\mathcal{O}$ is a such ring, then $\mathcal{O}^*$ will denote its group of units.

A *valuation ring* of a function field $F|K$ is a commutative ring $\mathcal{O}$ such that:

(1) $K \subsetneq \mathcal{O} \subsetneq F$,

(2) $z \in F$ implies $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Proposition 1.1.1. *Let $\mathcal{O}$ be a valuation ring of a function field $F|K$. Then*

(1) *$\mathcal{O}$ is a local ring with unique maximal ideal $P := \mathcal{O} \setminus \mathcal{O}^*$;*

(2) *O is a principal ideals ring;*

(3) *If $P = t\mathcal{O}$, then any $z \in F^*$ has a unique representation of the form $z = t^n u$ for some integer n and $u \in \mathcal{O}^*$. Moreover, n does not depend on t;*

(4) $\overline{K} \cap P = \{\, 0 \,\}$.

A *place* of a function field $F|K$ is the maximal ideal P of a valuation ring $\mathcal{O}$. If $P = t\mathcal{O}$, then t is called a *prime element* (or *local parameter*) for P. Note that $\mathcal{O} = F \setminus \{\, x^{-1} \mid 0 \neq x \in P \,\}$, so $\mathcal{O}$ is univocally determined by its place P and we will denote it by $\mathcal{O}_P$.

Any function field has infinite places and we will denote by $\mathbb{P}_F$ the set of the places of F, that is, we set

$$\mathbb{P}_F := \{\, P \mid P \text{ is a place of } F \,\}.$$

Let $\mathbb{Z}$ be the integer number ring and ∞ be a symbol, not in $\mathbb{Z}$, such that
$\infty + \infty = \infty + n = n + \infty = \infty$ and $\infty > n$ for any $n \in \mathbb{Z}$.
A *discrete valuation* of a function field $F|K$ is a map $v : F \to \mathbb{Z} \cup \{\infty\}$ such that:

(1) $v(x) = \infty$ if and only if $x = 0$;

(2) $v(xy) = v(x) + v(y)$ for any $x, y \in F$;

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ for any $x, y \in F$;

(4) v is surjective;

(5) $v(k) = 0$ for any $k \in K^*$.

The property 3 of the above definition is referred to us as the "Triangle Inequality" and it can be generalized for a finite number of elements of F.
The following proposition will be very useful later.

Proposition 1.1.2 (Strict Triangle Inequality)**.** *Let v be a discrete valuation of $F|K$ and $x_1, x_2, \ldots, x_n \in F$. If there exists $1 \leq i \leq n$ such that $v(x_i) \lneq v(x_j)$ for any $1 \leq j \leq n$, $j \neq i$, then*

$$v(x_1 + x_2 + \cdots + x_n) = \min\{\, v(x_1), v(x_2), \ldots, v(x_n) \,\} = v(x_i).$$

There exists a relationship between places and discrete valuations of a function field. In fact, if P is a place of $F|K$ and t is a local parameter for P, then the map $v_P : F \to \mathbb{Z} \cup \{\infty\}$ defined by

$$v_P(0) := \infty \quad \text{and} \quad v_P(z) := n \ \text{ if } \ 0 \neq z = t^n u \in F \ \text{ with } \ u \in \mathcal{O}^*$$

(see Proposition 1.1.1.(3)) is a discrete valuation of $F|K$. Moreover, we have $\mathcal{O}_P = \{ z \in F \,|\, v_P(z) \geq 0 \}$, $\mathcal{O}_P^* = \{ z \in F \,|\, v_P(z) = 0 \}$ and $P = \{ z \in F \,|\, v_P(z) > 0 \}$. Conversely, if v is a discrete valuation of $F|K$, then $P = \{ z \in F \,|\, v(z) > 0 \}$ is a place of $F|K$ whose valuation ring is $\mathcal{O}_P = \{ z \in F \,|\, v(z) \geq 0 \}$.

Let P be a place of $F|K$. The *residue class field* of P is the field

$$F_P := \mathcal{O}_P / P.$$

An element of F_P will be denoted with $x(P)$ where $x \in \mathcal{O}_P$. Whereas we will set $x(P) = \infty$ if $x \in F \setminus \mathcal{O}_P$. Up to isomorphism, $K \subseteq F_P$, so it makes sense to define *degree* of P as

$$\deg P := [F_P : K].$$

The degree of a place is a positive integer and it results

$$\deg P \leq [F : K(x)] < \infty$$

for any $x \in P$, $x \neq 0$.

A *rational* place is a place of degree one. The set of all rational places will be denoted by $\mathbb{P}_F^{(1)}$.

We say that a place P is a *zero* of an element $z \in F$ if and only if $v_P(z) > 0$. P is a *pole* of z if and only if $v_P(z) < 0$.

Any element $z \in F^*$ has only finitely many zeros and poles (at least one zero and one pole if z is transcendental).

The free abelian group generated by the places of $F|K$ is denoted by $\mathcal{D}_F$ and it is called the *divisor group* of $F|K$. A *divisor* is an element of $\mathcal{D}_F$, so it is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_P P$$

with $n_P \in \mathbb{Z}$ and $n_P \neq 0$ only for a finite number of places. Sometimes we will denote n_P by $v_P(D)$.

The *support* of a divisor D is the set

$$\operatorname{supp} D := \{\, P \in \mathbb{P}_F \,|\, n_P \neq 0 \,\}.$$

In $\mathcal{D}_F$ a partial ordering is defined by

$$A \leq B \text{ if and only if } v_P(A) \leq v_P(B) \text{ for any } P \in \mathbb{P}_F$$

where $A = \sum_{P \in \mathbb{P}_F} v_P(A)P$ and $B = \sum_{P \in \mathbb{P}_F} v_P(B)P$ are two divisors of F.

A divisor D is *positive* (or *effective*) if and only if D is bigger or equal than the null divisor 0 (which is the zero element of $\mathcal{D}_F$). The *degree* of a divisor $D = \sum_{P \in \mathbb{P}_F} n_P P$ is

$$\deg D := \sum_{P \in \mathbb{P}_F} n_P \deg P.$$

Let us denote by Z and N respectively the set of zeros and the set of poles of a fixed element $z \in F^*$. We define the *zero divisor*, *pole divisor* and *principal divisor* of the element z respectively the divisors

$$(z)_0 := \sum_{P \in Z} v_P(z)P,$$

$$(z)_\infty := \sum_{P \in N} (-v_P(z))P \quad \text{and}$$

$$(z) := (z)_0 - (z)_\infty = \sum_{P \in \mathbb{P}_F} v_P(z)P.$$

By definition, the zero and pole divisors of an element are effective divisors. Moreover, $(x) = 0$ if and only if $x \in K$. The set of principal divisors is a subgroup of $\mathcal{D}_F$ and we get $(xy) = (x) + (y)$ for any $x, y \in F$.

Now we give the "Zeros Theorem" which states that the degree of the zero divisor

and the degree of the pole divisor of an element $x \in F$ are bounded by the degree $[F : K(x)]$.

Theorem 1.1.3 (Zeros Theorem)**.** *If $x \in F \setminus K$, then*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

A consequence of the Zeros Theorem is the "Degree Theorem".

Theorem 1.1.4 (Degree Theorem)**.** *If $0 \neq x \in F$, then*

$$\deg(x) = 0.$$

For a divisor $G \in \mathcal{D}_F$ we define the $\mathcal{L}-$*space* (or *Riemann-Roch space*) associated with the divisor G the $K-$vector space

$$\mathcal{L}(G) := \{\, z \in F \,|\, (z) \geq -G \,\} \cup \{0\} = \{\, z \in F \,|\, v_P(z) \geq -v_P(G) \text{ for all } P \in \mathbb{P}_F \}.$$

For any divisor $G \in \mathcal{D}_F$ we define the *dimension* of the divisor G to be the dimension of $\mathcal{L}(G)$ as $K-$vector space, that is, we set

$$\dim G := \dim \mathcal{L}(G).$$

Proposition 1.1.5. *Let $A, B \in \mathcal{D}_F$. Then*

(1) *$\mathcal{L}(A)$ is a $K-$vector space of finite dimension.*

(2) *$\mathcal{L}(0) = K$.*

(3) *If $A \leq B$, then $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ and*

$$dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A.$$

(4) *If* $\deg A < 0$, *then* $\dim A = 0$.

(5) *For a divisor* A *with* $\deg A = 0$ *we have*

$$A \text{ is principal if and only if } \dim A = 1.$$

The set $\{ \deg A - \dim A + 1 \mid A \in \mathcal{D}_F \}$ is superiorly bounded, so it makes sense to define the *genus* of the function field $F|K$ to be the integer

$$g := \max\{ \deg A - \dim A + 1 \mid A \in \mathcal{D}_F \} \geq 0.$$

The next theorem follows by the well-known Riemann-Roch Theorem.

Theorem 1.1.6. *Let* $F|K$ *be a function field of genus* g *and* A *be a divisor. Then*

$$\dim A \geq \deg A + 1 - g.$$

Moreover, if $\deg A \geq 2g - 1$, *then*

$$\dim A = \deg A + 1 - g.$$

The *automorphism group* of a function field $F|K$ is the group

$$\mathrm{Aut}(F|K) := \{ \sigma : F \to F \mid \sigma \text{ is an automorphism with } \sigma(k) = k \text{ for any } k \in K \}.$$

The automorphism group $\mathrm{Aut}(F|K)$ acts on the set $\mathbb{P}_F$ by setting, for a $P \in \mathbb{P}_F$,

$$\sigma(P) := \{ \sigma(x) \mid x \in P \}. \tag{1.1.1}$$

We have

$$\deg \sigma(P) = \deg P$$

since σ induces the isomorphism

$$\begin{array}{rccc} \sigma: & F_P & \to & F_{\sigma(P)} \\ & z(P) & \mapsto & \sigma(z)(\sigma(P)) \end{array} \tag{1.1.2}$$

from the residue class field of P to the one of $\sigma(P)$.

The action of $\mathrm{Aut}(F|K)$ on $\mathbb{P}_F$ can be extended to an action on the set $\mathcal{D}_F$ by setting

$$\sigma(\sum_{P\in\mathbb{P}_F} n_P\, P) := \sum_{P\in\mathbb{P}_F} n_P\, \sigma(P). \tag{1.1.3}$$

Clearly, for a divisor D it results

$$\deg \sigma(D) = \deg D.$$

Lemma 1.1.7. *Let σ be an automorphism of $F|K$.*

(1) *If $x \in \mathcal{O}_P$ with P rational place, then*

$$\sigma(x)(\sigma(P)) = x(P).$$

(2) *If $A \in \mathcal{D}_F$, then*

$$\mathcal{L}(\sigma(A)) = \sigma(\mathcal{L}(A)).$$

(3) *If σ fixes at least $2g+3$ rational places, then σ is the identity map.*

1.1.1 Algebraic extensions

A function field $F'|K'$ is an *algebraic extension* of the function field $F|K$ if $F' \supseteq F$ is an algebraic extension and $K' \supseteq K$.

The algebraic extension $F'|K'$ of $F|K$ is a *finite extension* if $[F' : F] < \infty$.

If $F'|K'$ is an algebraic extension of $F|K$, then $K'|K$ is algebraic and $F \cap K' = K$. Furthermore, $F'|K'$ is a finite extension of $F|K$ if and only if $[K' : K] < \infty$.

Let $F'|K'$ be an algebraic extension of $F|K$. A place $P' \in \mathbb{P}_{F'}$ is said to *lie* over a place $P \in \mathbb{P}_F$ (or to be an *extension* of P) if $P' \supseteq P$. We will write $P'|P$.

Proposition 1.1.8. *Let $F'|K'$ be an algebraic extension of $F|K$. Let $P' \in \mathbb{P}_{F'}$ and $P \in \mathbb{P}_F$. Then the following assertions are equivalent:*

(1) *$P'|P$;*

(2) *$\mathcal{O}_{P'} \supset \mathcal{O}_P$;*

(3) *There exists an integer $e(P'|P) \geq 1$ such that*

$$v_{P'}(z) = e(P'|P) \cdot v_P(z)$$

for any $z \in F$.

If $P'|P$ we also have

$$P = F \cap P' \text{ and } \mathcal{O}_P = F \cap \mathcal{O}_{P'}.$$

The integer $e(P'|P)$ is called the *ramification index* of P' over P.

The extension $P'|P$ is said to be *ramified* if $e(P'|P) > 1$. $P'|P$ is said to be *unramified* if $e(P'|P) = 1$.

Hence, for $P'|P$ we have $F_P \subseteq F_{P'}$ up to the canonical embedding given by

$$\begin{array}{ccc} F_P & \to & F_{P'} \\ x(P) & \mapsto & x(P') \end{array} \tag{1.1.4}$$

and we define *relative degree* $f(P'|P)$ of $P'|P$ to be

$$f(P'|P) := [F_{P'} : F_P].$$

Obviously, $f(P'|P)$ is a positive integer if and only if $[K' : K] < \infty$ and this occurs if and only if $[F' : F] < \infty$.

Proposition 1.1.9. *Let $F'|K'$ be an algebraic extension of $F|K$. The map ρ from $\mathbb{P}_{F'}$ to $\mathbb{P}_F$ defined by*

$$\rho(P') := P' \cap F$$

is a surjective map such that $\rho^{-1}(P)$ is a finite set for any $P \in \mathbb{P}_F$.

For a fixed place P of $F|K$ there is a relation between the numbers $e(P'|P)$ and $f(P'|P)$ when P' runs in $\rho^{-1}(P)$. More precisely, we have the following and useful theorem.

Theorem 1.1.10. *Let $F'|K'$ be a finite extension of $F|K$. If $P \in \mathbb{P}_F$, then*

$$\sum_{P'|P} e(P'|P) \cdot f(P'|P) = [F' : F]. \tag{1.1.5}$$

1.1.2 The Rational Function Field

A function field $F|K$ is said to be a *rational function field* if $F = K(x)$ for some $x \in F$ transcendental over K.

Proposition 1.1.11. *Let $F|K$ be a function field. $F|K$ is rational if and only if it has genus $g = 0$ and there is some divisor $A \in \mathcal{D}_F$ of degree $\deg A = 1$.*

Let $p(x) \in K[x]$ be a monic irreducible polynomial. Then

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \in K(x) \,|\, p(x) \nmid g(x) \text{ and } p(x)|f(x) \right\} \tag{1.1.6}$$

is a place of $K(x)|K$ whose valuation ring is

$$\mathcal{O}_{p(x)} := \Big\{ \frac{f(x)}{g(x)} \in K(x) \,|\, p(x) \nmid g(x) \Big\}. \tag{1.1.7}$$

As usual, if $p(x) = x - \alpha$ we set

$$P_{x-\alpha} := P_\alpha.$$

A rational function field has only one other place which is

$$P_\infty := \Big\{ \frac{f(x)}{g(x)} \in K(x) \,|\, \deg f(x) < \deg g(x) \Big\} \tag{1.1.8}$$

whose valuation ring is

$$\mathcal{O}_\infty := \Big\{ \frac{f(x)}{g(x)} \in K(x) \,|\, \deg f(x) \leq \deg g(x) \Big\}. \tag{1.1.9}$$

P_∞ is said to be the *infinite place* of $F|K$.

Proposition 1.1.12. *Let $K(x)|K$ be a rational function field.*

(1) *K is the full constant field of F.*

(2) *Let $P_{p(x)} \in \mathbb{P}_{K(x)}$ be a place as in* (1.1.6)*, where $p(x) \in K[x]$ is a monic irreducible polynomial. Then*

(i) *$p(x)$ is a local parameter for P;*

(ii) *For any $z \in K(x) \setminus \{0\}$ we have*

$$v_{P_{p(x)}}(z) = n \quad \text{if and only if} \quad z = p(x)^n \cdot (f(x)/g(x))$$

with $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$, $p(x) \nmid f(x)$ and $p(x) \nmid g(x)$;

(iii) $\deg P_{p(x)} = \deg p(x)$.

(3) *Let P_∞ be the infinite place of $K(x)|K$ as in* (1.1.8). *Then*

(i) *$1/x$ is a local parameter for P;*

(ii) $v_{P_\infty}(f(x)/g(x)) = \deg g(x) - \deg f(x)$;

(iii) $\deg P_\infty = 1$.

1.1.3 The Elliptic Function Field

From now on, we always assume that $F|K$ is a function field where K is the full constant field of F.

A function field $F|K$ is said to be an *elliptic function field* if its genus is $g = 1$ and it has some rational place.

Proposition 1.1.13. *Let K be a field with* $\operatorname{char} K \neq 2$.

(1) *If $F|K$ is an elliptic function field, then there exist $x, y \in F$ such that $F = K(x, y)$ and*

$$y^2 = f(x) \in K[x], \tag{1.1.10}$$

where $f(x)$ is a square-free[1] *polynomial of degree* 3.

(2) *Conversely, Suppose that $F = K(x, y)$ with*

$$y^2 = f(x) \in K[x],$$

where $f(x)$ is a square-free polynomial of degree 3. *Consider the decomposition $f(x) = c\prod_{i=1}^{r} p_i(x)$ of $f(x)$ into irreducible monic polynomials $p_i(x) \in K[x]$ with $0 \neq c \in K$. Then the following holds:*

[1] *A square-free polynomial is a polynomial which is not divisible by the square of an irreducible polynomial*

(i) *$F|K$ is an elliptic function field whose full constant field is K.*

(ii) *The extension $F|K(x)$ is cyclic of degree 2. The places $P_{p_1(x)}, \ldots, P_{p_r(x)}$ and P_∞ are ramified in $F|K(x)$; each of them has exactly one extension in F, say $Q_1, \ldots, Q_r$ and Q_∞, and we have $e(Q_j|P_{p_j(x)}) = e(Q_\infty|P_\infty) = 2$, $\deg Q_j = \deg P_{p_j(x)}$ and $\deg Q_\infty = 1$ for any $j = 1, 2, \ldots, r$.*

(iii) *$P_{p_1(x)}, \ldots, P_{p_r(x)}$ and P_∞ are the only places of $K(x)$ which are ramified in $F|K(x)$.*

1.1.4 The Hyperelliptic Function Field

A function field $F|K$ is said to be a *hyperelliptic function field* if the genus of $F|K$ is $g \geq 2$ and if F contains a rational subfield $K(x) \subseteq F$ with $[F : K(x)] = 2$.
It is well-known that a function field of genus 2 is hyperelliptic if and only if there exists a divisor $A \in \mathcal{D}_F$ with $\deg A = 2$ and $\dim A \geq 2$.

Proposition 1.1.14. *Assume that* $\operatorname{char} K \neq 2$.

(1) *Let $F|K$ be a hyperelliptic function field of genus g. Then there exist $x, y \in F$ such that $F = K(x, y)$ and*

$$y^2 - f(x) = 0 \tag{1.1.11}$$

with $f(x) \in K[x]$ a square-free polynomial of degree $d = 2g + 1$ or $2g + 2$.

(2) *Conversely, if $F = K(x, y)$ and $y^2 = f(x) \in K[x]$ with $f(x)$ a square-free polynomial of degree $d > 4$, then $F|K$ is hyperelliptic of genus*

$$g = \begin{cases} (d-1)/2 & \text{if } d \equiv 1 \pmod 2, \\ (d-2)/2 & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

(3) *Let* $F = K(x, y)$ *with* $y^2 = f(x) \in K[x]$ *as in* (1.1.11). *Then the places* $P \in \mathbb{P}_{K(x)}$ *which ramify in* $F|K(x)$ *are as it follows:*

- *all zeros of* $f(x)$ *if* $\deg f(x) \equiv 0 \pmod 2$,
- *all zeros of* $f(x)$ *and the pole of* x *if* $\deg f(x) \equiv 1 \pmod 2$.

1.2 Linear Codes

Error correcting codes were invented to correct errors which can occur when a message is sent through a noisy communication channel to a receiver. The basic idea of coding theory is to encode the message m, to be sent through the channel, into a codeword x. But, before the codification, the message is divided into message words of appropriate length (equal to the dimension of the code). Because of channel's noise, the received word y may be different from x. If we define the *error vector* $e := y - x$, then an error occurred if and only if $e \neq 0$. The decoder must decide, from y, which message was transmitted, even if the decoder can never be certain what e was. However, if e is "small enough" the decoder can decide the right message. In the following we will see more in detail how a code works (see also [MacW-S]).

Let $\mathbb{F}_q$ be the field with q elements. A *linear code* over the alphabet $\mathbb{F}_q$ is an $\mathbb{F}_q-$linear subspace of $\mathbb{F}_q^n$. The elements of the code are called *codewords*. We will call n the *length* of the code and $k = \dim C$ the *dimension* of C over $\mathbb{F}_q$. The *minimum distance* $d(C)$ of C is

$$d(C) := \min\{\, d(a, b) \,|\, a, b \in C \text{ and } a \neq b\}$$

where

$$d(a, b) := |\{\, i \,|\, a_i \neq b_i\}|$$

is the *Hamming distance* between $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1\, b_2, \ldots, b_n)$.

Remark 1.2.1. The minimum distance of a code C is also equal to

$$d(C) = \min\{\, w(c) \,|\, 0 \neq c \in C\}$$

where

$$w(c) := d(c, 0) = |\{\, i \,|\, c_i \neq 0\}|$$

is the *weight* of $c = (c_1, c_2, \ldots, c_n)$.

A *q-ary* $[n, k, d]$ *code* is a code over $\mathbb{F}_q$ of length n, dimension k and minimum distance d.

The decoder's strategy is to decode y as the nearest codeword x (nearest in the sense of Hamming distance), i.e. pick that error vector e which has least weight. This is called *nearest neighbor decoding.*

Let $B_t(c)$ denote the close sphere of radius t centered on c, i.e.

$$B_t(c) = \{\, u \in \mathbb{F}_q^n \mid d(c, u) \leq t \,\}.$$

Note that, if t is the integer part of $(d-1)/2$, then for any $c_1, c_2 \in C$ we have $B_t(c_1) \cap B_t(c_2) = \emptyset$. So if the weight of the error vector e is less or equal than t, then the error can be corrected.

For this reason we will say that the code is a *t-error correcting.*

Practically, the decoder checks if a codeword z is in the sphere $B_t(y)$ and, if so, it decodes y as z. Note that at most one codeword can be in the sphere.

Clearly, if more than t errors occur, the decoder could output the wrong codeword. This is called *decoding error.*

There exists a relation which links the parameters of a code. It is the *Singleton bound.*

Proposition 1.2.1 (Singleton Bound)**.** *If C is an $[n, k, d]$ code, then*

$$k + d \leq n + 1. \tag{1.2.1}$$

A *maximum distance separable* code (for short *MDS* code) is a $[n, k, d]$ code with $k + d = n + 1$.

A *generator matrix* G of an $[n, k, d]$ code C is a $k \times n$ matrix whose rows form a basis of the code. It results

$$C = \{\, aG \mid a \in \mathbb{F}_q^k \,\}.$$

If $C \subseteq \mathbb{F}_q^n$ is a code, then the orthogonal space

$$C^\perp := \{\, u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0 \text{ for all } c \in \mathcal{C} \,\}$$

(where $\langle a, b\rangle$ is the canonical inner product on $\mathbb{F}_q^n$) is also a linear code and it is called the *dual code* of C. To be more precise, $C^\perp$ is a $q-$ary $[n, n-k, d']$ code. A generator matrix H of $C^\perp$ is said to be a *parity check matrix* for C. It results

$$C = \{\, u \in \mathbb{F}_q^n \mid H \cdot u^t = 0 \,\}$$

(where u^t is the transpose of u).

With a generator matrix and a parity check matrix for a code, it is possible to perform the encoding and decoding that convert a message word to a codeword and back. The encoding of a message m is the vector $x = mG$. The decoding is done checking if there exists an element z of $B_t(y)$ such that $H \cdot z^t = 0$.

The symmetric group S_n acts on the vector space $\mathbb{F}_q^n$ via

$$\pi(c_1, c_2, \ldots, c_n) := (c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)}) \tag{1.2.2}$$

for $\pi \in S_n$ and $(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$. The *(permutation) automorphism group* $\mathrm{Aut}(C)$ of a code $C \subseteq \mathbb{F}_q^n$ is defined by

$$\mathrm{Aut}(C) := \{\pi \in S_n \mid \pi(C) \subseteq C\}. \tag{1.2.3}$$

For a dual code we have $\mathrm{Aut}(C^{\perp}) = \mathrm{Aut}(C)$.

1.2.1 Some performance of long codes

In coding theory, people are interested in codes with large dimension and large minimum distance. However we saw that there are some restrictions regarding them (for instance the Singleton Bound). Sometimes we are, most of all, interested on the performance of long codes. The *rate* and the *relative minimum distance* of a $q-$ary $[n, k, d]$ code C are respectively

$$R = R(C) := k/n \quad \text{and} \quad \delta = \delta(C) := d/n.$$

If we denote by U_q the set of ordered pairs $(\delta, R) \in [0, 1]^2$ for which there exists an infinite sequence $C_1, C_2, \ldots$ of $q-$ary $[n_i, k_i, d_i]$ linear codes with $n_i \to \infty$ for $i \to \infty$ and

$$R = \lim_{i\to\infty} \frac{k_i}{n_i} \quad \text{and} \quad \delta = \lim_{i\to\infty} \frac{d_i}{n_i},$$

the following result holds (see for instance [T-V]).

Proposition 1.2.2. *There exists a continuous function $\alpha_q : [0, 1] \to [0, 1]$ such that*

$$U_q = \{\, (\delta, R) \mid 0 \le \delta \le 1 \text{ and } 0 \le R \le \alpha_q \,\}.$$

Moreover, $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ for $\delta \in [(q-1)/q, 1]$ and $\alpha_q(\delta)$ decreases on the interval $[0, (q-1)/q]$.

The function α_q is unknown explicitly for $\delta \in [0, (q-1)/q]$. However several upper and lower bound are available. For instance, if we define the *q-ary entropy function*

$$H_q(\delta) := \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$$

for $0 < \delta < 1$, an upper and lower bound, respectively, are given (see for instance [MacW-S]) in the following proposition.

Proposition 1.2.3.

(1) *(Bassalygo-Elias Bound). For* $0 \leq \delta \leq (q-1)/q$,

$$\alpha_q(\delta) \leq 1 - H_q\left(\theta - \sqrt{\theta(\theta - \delta)}\right),$$

where $\theta := q(q-1)$.

(2) *(Gilbert-Varshamov Bound). For* $0 \leq \delta \leq (q-1)/q$,

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

Chapter 2

Algebraic Geometry Codes

In this chapter we will describe V.D. Goppa's construction of error-correcting codes using algebraic function fields. We will show, in the rational, elliptic and hyperelliptic cases, under which conditions the automorphism group of an algebraic geometry code is equal to the stabilizer, in the automorphism group of the underlying function field, of the divisors associated with the code.

2.1 Definition

We shall start giving the definition and some basic facts about algebraic geometry codes that we shall adhere to in the rest of this chapter.

Let $F|\mathbb{F}_q$ be an algebraic function field of genus g, where $\mathbb{F}_q$ is the finite field with q elements. Let $P_1, P_2, \ldots, P_n$ be pairwise distinct rational places of $F|\mathbb{F}_q$. If $D = P_1 + P_2 + \ldots + P_n$ and G is a divisor of $F|\mathbb{F}_q$ such that $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$, then the *algebraic geometry* code (or *geometric Goppa* code) $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is defined by

$$C_{\mathcal{L}}(D, G) := \{\, (x(P_1), x(P_2), \ldots, x(P_n)) \,|\, x \in \mathcal{L}(G) \,\} \subseteq \mathbb{F}_q^n. \tag{2.1.1}$$

The parameters of an algebraic geometry code are as in the following theorem.

Theorem 2.1.1. *$C_{\mathcal{L}}(D,G)$ is a $q-$ary $[n,k,d]$ code with*

$$k = \dim G - \dim(G-D) \quad \textit{and} \quad d \geq n - \deg G.$$

Proof. $C_{\mathcal{L}}(D,G)$ is the image of the *evaluation map*

$$\begin{array}{rccc} ev_D: & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & x & \mapsto & (x(P_1), x(P_2), \ldots, x(P_n)) \end{array} \tag{2.1.2}$$

which is a surjective linear map with kernel $Ker(ev_D) = \mathcal{L}(G-D)$. Hence

$$C_{\mathcal{L}}(D,G) \cong \mathcal{L}(G)/\mathcal{L}(G-D)$$

and so

$$k = \dim G - \dim(G-D).$$

Moreover, if d is the minimum distance of $C_{\mathcal{L}}(D,G)$, then there exists an element of $C_{\mathcal{L}}(D,G)$ with weight d, that is, there exists $0 \neq x \in \mathcal{L}(G)$ and exactly $n-d$ places $P_{i_1}, P_{i_2} \ldots, P_{i_{n-d}} \in \operatorname{supp} D$ such that

$$x(P_{i_j}) = 0 \text{ for any } j = 1, 2, \ldots, n-d.$$

Hence,

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d}}))$$

and so, by Proposition 1.1.5.(4), necessarily

$$0 \leq \deg(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d}})) = \deg G - n + d.$$

Finally, $d \geq n - \deg G$. □

Corollary 2.1.2. (1) *If* $\deg G < n$, *then* $C_{\mathcal{L}}(D,G)$ *is a* $q-$*ary* $[n,k,d]$ *code with*

$$k = \dim G \geq \deg G + 1 - g \quad \textit{and} \quad d \geq n - \deg G.$$

(2) *If* $2g-2 < \deg G < n$, *then* $C_{\mathcal{L}}(D,G)$ *is a* $q-$*ary* $[n,k,d]$ *code with*

$$k = \deg G + 1 - g \quad \textit{and} \quad d \geq n - \deg G.$$

(3) *If* $\{ x_1, x_2, \ldots, x_k \}$ *is a base of* $\mathcal{L}(G)$, *then the* $k \times n$ *matrix*

$$G = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \cdots & x_2(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix}$$

is a generator matrix for $C_{\mathcal{L}}(D,G)$.

Proof. (1) If $\deg G < n = \deg D$, then $\deg(G-D) < 0$ and, by Proposition 1.1.5.(4), it follows that $\dim(G-D) = 0$. Thus $k = \dim G - \dim(G-D) = \dim G \geq \deg G + 1 - g$ where last relation follows by Theorem 1.1.6.
(2) If $2g-2 < \deg G < n$, then, by Theorem 1.1.6, we have $\dim G = \deg G + 1 - g$.
(3) G is a generator matrix since $\{ ev_D(x_1), ev_D(x_2), \ldots, ev_D(x_k) \}$ is a base of the code. □

Note that if we define $\pi(D) := P_{\pi(1)} + P_{\pi(2)} + \ldots + P_{\pi(n)}$, where $\pi \in S_n$, then $\pi(D) = D$ as divisors but, in general, $C_{\mathcal{L}}(\pi(D),G) \neq C_{\mathcal{L}}(D,G)$ since a linear code depends on the order of its base as vector space. Anyway, sometimes the equality is verified. In fact, the next lemma holds.

Lemma 2.1.3. *If $\pi \in \mathrm{Aut}(C_{\mathcal{L}}(D,G))$, then*

$$C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(\pi(D),G). \tag{2.1.3}$$

Proof. For any $\pi \in \mathrm{Aut}(C_{\mathcal{L}}(D,G))$ and $z \in \mathcal{L}(G)$,

$$(z(P_{\pi(1)}), z(P_{\pi(2)}), \ldots, z(P_{\pi(n)})) = \pi(z(P_1), z(P_2), \ldots, z(P_n)) \in C_{\mathcal{L}}(D,G)$$

and so $C_{\mathcal{L}}(\pi(D),G) \subseteq C_{\mathcal{L}}(D,G)$. Hence $C_{\mathcal{L}}(\pi(D),G) = C_{\mathcal{L}}(D,G)$ since both codes have the same dimension (see Proposition 2.1.1). □

Lemma 2.1.4. *For all $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$*

$$C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(\sigma(D),\sigma(G)).$$

Proof. Since $D = \sum_{i=1}^{n} P_i$ we have that $\sigma(D) = \sum_{i=1}^{n} \sigma(P_i)$. Hence $C_{\mathcal{L}}(\sigma(D),\sigma(G)) = \{\, (\sigma(z)(\sigma(P_1)), \sigma(z)(\sigma(P_2)), \ldots, \sigma(z)(\sigma(P_n))) \mid \sigma(z) \in \sigma(\mathcal{L}(G)) = \mathcal{L}(\sigma(G))\}$ but, by Lemma 1.1.7.(1), $\sigma(z)(\sigma(P_i)) = z(P_i)$ for all $i = 1, 2, \ldots n$ and so the claim follows. □

2.2 The Automorphism Group of an Algebraic Geometry Code

In the following section, we introduce some notion and proposition given by Stichtenoth (see [St1] and [St2]).

As above, let $D = P_1 + P_2 + \cdots + P_n$ be a divisor of $F|\mathbb{F}_q$ with P_i's pairwise distinct rational places. Let G and G' be divisors of F. The divisor G is said to be $D-$*equivalent* to G', and we will write $G \sim_D G'$, if and only if there exists an element $z \in F$, $z \neq 0$,

such that $G = G' + (z)$ and $z(P_i) = 1$ for every $i = 1, 2, \ldots, n$. Obviously, this is an equivalence relation.

Now let us suppose that G and D have disjoint supports. We define the following subgroup of $\mathrm{Aut}(F|\mathbb{F}_q)$:

$$\mathrm{Aut}_{D,G}(F|\mathbb{F}_q) := \{\sigma \in \mathrm{Aut}(F|\mathbb{F}_q) \mid \sigma(D) = D \text{ and } \sigma(G) \sim_D G\}.$$

Under suitable conditions, this subgroup is the stabilizer of D and G in $\mathrm{Aut}(F|\mathbb{F}_q)$. In fact, in [St2] the next lemma was proved.

Lemma 2.2.1. *If $G = G_0 - G_1$ with $G_0 \geq 0$, $G_1 \geq 0$ and $\deg(G_0 + G_1) \leq n - 1$, then*

$$\mathrm{Aut}_{D,G}(F|\mathbb{F}_q) = \{\sigma \in \mathrm{Aut}(F|\mathbb{F}_q) \mid \sigma(D) = D \text{ and } \sigma(G) = G\}.$$

Proof. Clearly, we have only to prove that if $\sigma(G) \sim_D G$, then $\sigma(G) = G$. So, let us suppose that there exists an element $z \in F$, $z \neq 0$, such that $\sigma(G) = G + (z)$ and $z(P_i) = 1$ for every $i = 1, 2, \ldots, n$. Then $(z) = \sigma(G) - G = \sigma(G_0 - G_1) - (G_0 - G_1) = \sigma(G_0) + G_1 - (G_0 + \sigma(G_1)) \geq -(G_0 + \sigma(G_1))$ and so $z \in \mathcal{L}(G_0 + \sigma(G_1))$. It follows that $z - 1 \in \mathcal{L}(G_0 + \sigma(G_1))$, that is, $(z-1) = (z-1)_0 - (z-1)_\infty \geq -(G_0 + \sigma(G_1))$. So, since $(z-1)_0$, $(z-1)_\infty$ and $(G_0 + \sigma(G_1))$ are effective, $(z-1)_\infty \leq G_0 + \sigma(G_1)$. Hence $\deg(z-1)_\infty \leq \deg(G_0 + \sigma(G_1)) = \deg G_0 + \deg \sigma(G_1) = \deg G_0 + \deg G_1 \leq n - 1$. On the other hand $\deg(z-1)_0 \geq n$. In fact, $z(P_i) = 1$ implies that $z - 1 \in P_i$ for any $i = 1, 2, \ldots, n$. This is in contradiction with Zeros Theorem unless that $z - 1 \in \mathbb{F}_q$. But $z - 1 \in P_i$ too and so, since $\mathbb{F}_q \cap P_i = \{0\}$, $u - 1 = 0$, that is, $\sigma(G) = G + (z) = G + (1) = G$. □

If $\sigma \in \mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$, then for any $i = 1, 2, \ldots, n$ we have $\sigma(P_i) = P_j$ for some $j = 1, 2, \ldots, n$. So it makes sense to define π_σ as the element of S_n such that

$$\pi_\sigma(i) = j \text{ if and only if } \sigma(P_i) = P_j.$$

Theorem 2.2.2. (1) *The map*

$$\begin{array}{rccc} f: & \mathrm{Aut}_{D,G}(F|\mathbb{F}_q) & \to & \mathrm{Aut}(C_{\mathcal{L}}(D,G)) \\ & \sigma & \mapsto & \pi_\sigma \end{array}$$

is a homomorphism.

(2) *If $n > 2g+2$, then f is injective.*

Proof. (1) For $\sigma \in \mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$ we have that $\pi_\sigma \in \mathrm{Aut}(C_{\mathcal{L}}(D,G))$ if and only if, for any $x \in \mathcal{L}(G)$, $\pi_\sigma(x(P_1), x(P_2), \ldots, x(P_n)) = (x(\sigma(P_1)), x(\sigma(P_2)), \ldots, x(\sigma(P_n))) \in C_{\mathcal{L}}(D,G)$. Since $\sigma(G) \sim_D G$ there is an element $z \in F$, $z \neq 0$, such that $\sigma(G) = G + (z)$ and $z(P_i) = 1$ for every $i = 1, 2, \ldots, n$. If $y \in \mathcal{L}(\sigma(G))$, then $(y) \geq -\sigma(G) = -G - (z)$ and so $(zy) = (z) + (y) \geq -G$, that is, $zy \in \mathcal{L}(G)$. Now, it is easy to show that the map $y \mapsto zy$ is an isomorphism from $\mathcal{L}(\sigma(G))$ onto $\mathcal{L}(G)$. Hence, for $x \in \mathcal{L}(G)$ there is an element $w \in \mathcal{L}(\sigma(G))$ such that $zw = x$. But $\mathcal{L}(\sigma(G)) = \sigma(\mathcal{L}(G))$ and so $w = \sigma(y)$ for some $y \in \mathcal{L}(G)$. Then $x(\sigma(P_i)) = (zw)(\sigma(P_i)) = (z\sigma(y))(\sigma(P_i)) = z(\sigma(P_i))\sigma(y)(\sigma(P_i)) = 1 \cdot y(P_i) = y(P_i)$ and we get

$$(x(\sigma(P_1)), x(\sigma(P_2)), \ldots, x(\sigma(P_n))) = (y(P_1), y(P_2), \ldots, y(P_n)) \in C_{\mathcal{L}}(D,G).$$

(2) If $\sigma \in \ker f$, then $\pi_\sigma = id$, that is, $\pi_\sigma(i) = i$ for any $i = 1, 2, \ldots, n$. By definition, we have $\sigma(P_i) = P_i$ for any $i = 1, 2, \ldots, n$ and so σ fixes at least $2g+3$ rational places and so, by Lemma 1.1.7.(3), σ is the identity. Hence f is injective. □

Note that in case $n > 2g + 2$, by the above theorem, $\mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$ can be regarded as a subgroup of $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$. In the following of this section we will see, in some cases, under which conditions $\mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$ is exactly equal to $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$.

2.2.1 The Rational case

Now we assume that $F|\mathbb{F}_q$ is a rational function field. We will prove that the homomorphism from $\mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$ to $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$ given in Theorem 2.2.2 is also surjective. So, up to isomorphism, $\mathrm{Aut}(C_{\mathcal{L}}(D,G)) = \mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$. We need to prove two lemmas.

Lemma 2.2.3. *Let $C_{\mathcal{L}}(D,G)$ and $C_{\mathcal{L}}(D,G')$ be rational algebraic geometry codes of length $n \geq 3$ with $0 \leq \deg G = \deg G' \leq n-2$. Then $C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(D,G')$ if and only if $G \sim_D G'$.*

Proof. If $G \sim_D G'$, then there exists an element $z \in F$, $z \neq 0$, such that $G' = G + (z)$ and $z(P_i) = 1$ for any $i = 1, 2, \ldots, n$. But $G' = G + (z)$ implies that the map $y \mapsto zy$, from $\mathcal{L}(G')$ to $\mathcal{L}(G)$, is an isomorphism (see the proof of Theorem 2.2.2). Hence, if $x \in \mathcal{L}(G)$, $x = zw$ for some $w \in \mathcal{L}(G')$. Therefore $c \in C_{\mathcal{L}}(D,G)$ if and only if $c = (x(P_1), x(P_2), \ldots, x(P_n)) = (zw(P_1), zw(P_2), \ldots, zw(P_n)) = (w(P_1), w(P_2), \ldots, w(P_n))$ and this occur if and only $c \in C_{\mathcal{L}}(D,G')$. For the converse we observe that since $\deg(G - G') = 0$ and F is rational, then, by Proposition 1.1.5.(5) and Theorem 1.1.6, necessarily $G - G' = (u)$ for some $u \in F$ and $0 \neq u(P_i) \in \mathbb{F}_q$ for $i = 1, 2, \ldots, n$ (and this is because P_i does not occur in G and G'). We put $\lambda_i = u(P_i)$ for any $i = 1, 2, \ldots, n$. We have that $(\lambda_1^{-1}u) = (\lambda_1^{-1}) + (u) = (u) = G - G'$ and $\lambda_1^{-1}u(P_i) = \lambda_1^{-1}(P_i)u(P_i) = \lambda_1^{-1}\lambda_i$. So, without loss of generality, we can assume $\lambda_1 = 1$. We want to prove that $\lambda_i = 1$ for all i.

Assume there is an index $j \geq 2$ with $\lambda_j \neq 1$. Since $\deg G \leq n-2$, we can find a divisor D' with

$$0 \leq D' \leq D - (P_1 + P_j) \quad \text{and} \quad \deg D' = \deg G.$$

So $D' - G$ is a not zero divisor with $\deg(D' - G) = 0$. Then $D' - G$ is principal. Let $z \neq 0$ such that $(z) = D' - G$. We observe that $z \in \mathcal{L}(G - D') \subseteq \mathcal{L}(G)$ and $z(P_j) \neq 0$ (since $(z)_0 = D'$). We consider the element $uz \in \mathcal{L}(G')$. We have

$$\begin{aligned}(uz)(P_1) &= \lambda_1 \cdot z(P_1) = z(P_1),\\ (uz)(P_j) &= \lambda_j \cdot z(P_j),\\ (uz)(P_i) &= 0 \quad \text{for all } P_i \in \operatorname{supp} D'.\end{aligned}$$

As $C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D, G')$ there is $y \in \mathcal{L}(G)$ such that $y(P_k) = (uz)(P_k)$ for $k = 1, 2, \ldots, n$. Consequently,

$$(y - z)(P_i) = 0 \qquad \text{for all } \ P_i \in \operatorname{supp} D' \ \text{ and for } i = 1.$$

This shows that $(y - z) \geq P_i$ for all $P_i \in \operatorname{supp} D'$ and $(y - z) \geq P_1$. Since $y, z \in \mathcal{L}(G)$ we have also that $(y - z) \geq -G$ and so $(y - z) \geq -G + P_1 + D'$ (observe that $\operatorname{supp} G$, $\operatorname{supp} P_1$ and $\operatorname{supp} D'$ are pairwise disjoint). Finally, $y - z \in \mathcal{L}(G - P_1 - D')$ but $\deg(G - P_1 - D') < 0$, hence $y - z = 0$. This is a contradiction because $y(P_j) = \lambda_j z(P_j) \neq z(P_j)$. □

Lemma 2.2.4. *Let $F|\mathbb{F}_q$ be a rational function field. Let $D = P_1 + P_2 + \cdots + P_n$ and $D' = P'_1 + P'_2 + \cdots + P'_n$ be two divisors of F with P_i's and P'_j's rational places. Let $C_{\mathcal{L}}(D, G)$ and $C_{\mathcal{L}}(D', G')$ be two rational algebraic geometry codes of length n with $1 \leq \deg G = \deg G' \leq n - 3$. If $C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D', G')$, then there exists an automorphism $\sigma \in \operatorname{Aut}(F|\mathbb{F}_q)$ such that $\sigma(D) = D'$.*

Proof. It is well-known that $\operatorname{Aut}(F|\mathbb{F}_q) = \mathrm{PGL}(2, q)$ acts $3-$transitively on the set of rational places of F, hence there exists $\sigma \in \operatorname{Aut}(F|\mathbb{F}_q)$ such that $\sigma(P_i) = P'_i$ for $i = 1, 2, 3$. By Lemma 2.1.4, $C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(\sigma(D), \sigma(G))$ and so, by assumption,

$$C_{\mathcal{L}}(P'_1 + P'_2 + P'_3 + P'_4 + \cdots + P'_n, G') = C_{\mathcal{L}}(P'_1 + P'_2 + P'_3 + \sigma(P_4) + \cdots + \sigma(P_n), \sigma(G)).$$

We want to prove that $\sigma(P_i) = P'_i$ for $i = 4, \ldots, n$. Suppose this is false. Then there is an index $j \geq 4$ such that $\sigma(P_j) \neq P'_j$. Let k denote the degree of G and G'. Since $k \leq n - 3$ we can choose indices

$$i_1, \ldots, i_{k-1} \in \{\, 4, \ldots, n \,\} \setminus \{\, j \,\}.$$

The divisor

$$G' - \sigma(P_j) - \sum_{\nu=1}^{k-1} P'_{i_\nu}$$

is different to zero and it has degree zero, hence it is principal. Let $w \in F$ such that

$$(w) = -G' + \sigma(P_j) + \sum_{\nu=1}^{k-1} P'_{i_\nu}.$$

Clearly, $w(P'_j) \neq 0$ for $i \in \{\, 1, 2, 3, j \,\}$. Since $w \in \mathcal{L}(G')$ we can find $w' \in \mathcal{L}(\sigma(G))$ such that

$$w'(P'_i) = w(P'_i) \text{ for } i = 1, 2, 3$$

$$w'(\sigma(P_i)) = w(P'_i) \text{ for } i = 4, \ldots, n.$$

Then

$$(w') = -\sigma(G) + R + \sum_{\nu=1}^{k-1} \sigma(P_{i_\nu})$$

for some rational place R with $R \neq P'_1, P'_2, P'_3$. Now we choose $x \in \mathcal{L}(G')$ such that

$$(x) = -G' + P'_j + \sum_{\nu=1}^{k-1} P'_{i_\nu}$$

and $x' \in \mathcal{L}(\sigma(G))$ with

$$x(P'_i) = x'(P'_i) \text{ for } i = 1, 2, 3$$

$$x(P'_i) = x'(\sigma(P_i)) \text{ for } i = 4, \ldots, n.$$

Then

$$(x') = -\sigma(G) + \sigma(P_j) + \sum_{\nu=1}^{k-1} \sigma(P_{i_\nu})$$

and

$$\left(\frac{x}{w}\right) = P'_j - \sigma(P_j), \qquad \left(\frac{x'}{w'}\right) = \sigma(P_j) - R.$$

We conclude

$$0 \neq \frac{x}{w} - \frac{x'}{w'} \in \mathcal{L}(\sigma(P_j) + R).$$

But for $i = 1, 2, 3$ we have

$$\left(\frac{x}{w} - \frac{x'}{w'}\right)(P'_i) = \frac{x(P'_i)}{w(P'_i)} - \frac{x'(P'_i)}{w'(P'_i)} = 0$$

and so $x/w - x'/w'$ has at least three zeroes and at most two poles of degree 1 ($\sigma(P_j)$ and R). This is a contradiction since, by Degree Theorem, $\deg\left(\frac{x}{w} - \frac{x'}{w'}\right) = 0$. □

Finally, we can give the main theorem.

Theorem 2.2.5. *Let $C_{\mathcal{L}}(D, G)$ be a rational algebraic geometry code with $1 \leq \deg G \leq n - 3$. Then*

$$\mathrm{Aut}(C_{\mathcal{L}}(D, G)) = \mathrm{Aut}_{D,G}(F|\mathbb{F}_q).$$

Proof. Since $1 \leq \deg G \leq n - 3$, we have that $n \geq 4 > 2g - 2$. So, by Theorem 2.2.2.(2), $\mathrm{Aut}_{D,G}(F|\mathbb{F}_q) \subseteq \mathrm{Aut}(C_{\mathcal{L}}(D, G))$. Hence we only have to show that every automorphism of $C_{\mathcal{L}}(D, G)$ is induced by an element of $\mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$. Let us consider $\pi \in \mathrm{Aut}(C_{\mathcal{L}}(D, G))$. Then $\pi(C_{\mathcal{L}}(D, G)) = C_{\mathcal{L}}(D, G)$. On the other hand $\pi(C_{\mathcal{L}}(D, G)) = C_{\mathcal{L}}(\pi(D), G)$ and so

$$C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(\pi(D), G).$$

Then, by Lemma 2.2.4, there is $\sigma_\pi \in \mathrm{Aut}(F|\mathbb{F}_q)$ such that $\sigma_\pi(D) = \pi(D) = D$. Now, by Lemma 2.1.4, we have $C_{\mathcal{L}}(\sigma_\pi(D), \sigma_\pi(G)) = C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(\sigma_\pi(D), G)$ and, by Lemma 2.2.3, it results that $\sigma_\pi(G) \sim_D G$. Thus $\sigma_\pi \in \mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$. □

2.2.2 The Hyperelliptic case

Now we want to determine the automorphism group of a large class of hyperelliptic algebraic geometry codes. We will associate to each automorphism π of a hyperelliptic algebraic geometry code $C_{\mathcal{L}}(D, G)$ a linear automorphism λ of the $\mathcal{L}-$space $\mathcal{L}(G)$. We show that, under suitable conditions on the divisor G, there is an automorphism of the underlying function field which preserve $\mathcal{L}(G)$, whose linear restriction to $\mathcal{L}(G)$ is equal to λ and such that it induces π as automorphism of the code.
We shall start proving some properties which are valid for any function field $F|\mathbb{F}_q$.

Lemma 2.2.6. *Let* $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$ *and*

$$G = \sum k_P P > 0$$

be a divisor of F *with* $\deg G \geq 2g$. *If* $\sigma(\mathcal{L}(G)) = \mathcal{L}(G)$, *then* $\sigma(G) = G$.

Proof. Suppose $\sigma(G) \neq G$, then there exists $P \in \operatorname{supp} G$ such that $v_P(G) \neq v_P(\sigma(G))$. Suppose $v_P(G) > v_P(\sigma(G))$. Since $\deg G \geq 2g$, then $\deg(G - P) \geq 2g - 1$. Then, by Theorem 1.1.6, $\dim(G - P) = \deg(G - P) + 1 - g = \deg G - \deg P + 1 - g < \deg G + 1 - g \leq \dim G$. Therefore there exists $f \in \mathcal{L}(G) \setminus \mathcal{L}(G - P)$ and so $v_P(f) = -v_P(G)$. But $f \in \mathcal{L}(G) = \sigma(\mathcal{L}(G)) = \mathcal{L}(\sigma(G))$ from which $v_P(f) \geq -v_P(\sigma(G))$. Hence $-v_P(G) \geq -v_P(\sigma(G))$, that is, $v_P(G) \leq v_P(\sigma(G))$ which contradicts the fact that $v_P(G) > v_P(\sigma(G))$. Obviously, the same happens if $v_P(G) < v_P(\sigma(G))$. Hence $\sigma(G) = G$. □

Lemma 2.2.7. *Let* $u, v \in \mathcal{L}(G)$ *for some divisor* $G = G_0 - G_1$ *with* $G_0, G_1 \geq 0$. *Let* $\deg G_0 < n$ *and* $P_1, P_2, \ldots, P_n$ *be* n *distinct rational places which are not in the support of* G_0. *If* $u(P_i) = v(P_i)$ *for each* $i = 1, 2, \ldots, n$, *then* $u = v$.

Proof. Suppose $u \neq v$. Since $u - v \in \mathcal{L}(G)$, then $(u - v) = (u - v)_0 - (u - v)_\infty \geq -G_0 + G_1$ that means $(u - v)_\infty \leq G_0$. Hence $\deg(u - v)_\infty \leq \deg G_0 < n$. On the other hand, if $u(P_i) = v(P_i)$ it follows that $(u - v)(P_i) = 0$. So $u - v \in P_i$ for all $i = 1, 2, \ldots, n$. Hence $u - v$ has at least n zeros and so $\deg(u - v)_\infty \geq n$ which contradicts the above considerations. □

Let $D = \sum_{i=1}^{n} P_i$ and $D' = \sum_{i=1}^{n} P'_i$ be two divisors with $\deg P_i = \deg P'_i = 1$ for any $i = 1, 2, \ldots, n$. Let G be a divisor of degree $\deg G < n$ such that $\operatorname{supp} G \cap \operatorname{supp} D = \operatorname{supp} G \cap \operatorname{supp} D' = \emptyset$. Let us consider the linear isomorphisms ev_D and $ev_{D'}$ as in (2.1.2). If $C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D', G)$ we can define a linear isomorphism $\lambda : \mathcal{L}(G) \to \mathcal{L}(G)$ by

$$\lambda := ev_{D'}^{-1} \circ ev_D. \tag{2.2.1}$$

Note that for all $z \in \mathcal{L}(G)$ we have that $\lambda(z) \in \mathcal{L}(G)$ is the only element in $\mathcal{L}(G)$ such that

$$\lambda(z)(P'_i) = z(P_i) \quad \text{for all } i = 1, 2, \ldots n.$$

In fact, $\lambda(z) = ev_{D'}^{-1} \circ ev_D(z)$ if and only if $ev_{D'}(\lambda(z)) = ev_D(z)$ if and only if $(\lambda(z)(P'_1), \lambda(z)(P'_2), \ldots, \lambda(z)(P'_n)) = (z(P_1), z(P_2), \ldots, z(P_n))$.
The next lemma shows that our map λ, under certain conditions on the degree of G, has similar properties with the ones of a field automorphism.

Lemma 2.2.8. *Let G be a divisor of $F|\mathbb{F}_q$.*

(1) *If $\deg G < n$ and $1 \in \mathcal{L}(G)$, then $\lambda(1) = 1$.*

(2) *If $G > 0$ with $\deg G < \frac{n}{2}$ and*

(i) *if $f, g, fg \in \mathcal{L}(G)$, then $\lambda(fg) = \lambda(f)\lambda(g)$.*

(ii) *if* $f, f^k \in \mathcal{L}(G)$ *for some* $k \geq 2$, *then* $\lambda(f^k) = \lambda(f)^k$ *and* $\deg(\lambda(f)_\infty) \leq \frac{\deg G}{k}$.

Proof. (1) Since $1(P) = 1$ for all rational places, we have $1(P'_i) = 1 = 1(P_i) = \lambda(1)(P'_i)$ for all $i = 1, 2, \ldots, n$, that is, $(1(P'_1), \ldots, 1(P'_n)) = (\lambda(1)(P'_1), \ldots, \lambda(1)(P'_n))$ which is equivalent to $ev_{D'}(1) = ev_{D'}(\lambda(1))$. It follows that $\lambda(1) = 1$ since $ev_{D'}$ is injective.

(2) If $f, g, fg \in \mathcal{L}(G)$, then $\lambda(fg), \lambda(f), \lambda(g) \in \mathcal{L}(G)$ and so, a fortiori, they will be in $\mathcal{L}(2G)$. Moreover, $\lambda(f)\lambda(g) \in \mathcal{L}(2G)$ because $(\lambda(f)) \geq -G$ and $(\lambda(g)) \geq -G$. In fact, $(\lambda(f)\lambda(g)) = (\lambda(f)) + (\lambda(g)) \geq -2G$. We remark that $(\lambda(f)\lambda(g))(P'_i) = (\lambda(f)(P'_i))(\lambda(g)(P'_i)) = (f(P_i))(g(P_i)) = (fg)(P_i) = \lambda(fg)(P'_i)$. Since $G > 0$ and $2 \deg G < n$, by Lemma 2.2.7, we have that $\lambda(fg) = \lambda(f)\lambda(g)$.

If $f, f^k \in \mathcal{L}(G)$, then $v_P(f) \geq -v_P(G)$ and $v_P(f^k) \geq -v_P(G)$ for each $P \in \mathbb{P}_F$.

For $i = 2, 3, \ldots, k-1$ and $P \in \mathbb{P}_F$ we consider two cases.

If $v_P(f) \geq 0$, then $v_P(f^i) = iv_P(f) \geq v_P(f) \geq -v_P(G)$;

If $v_P(f) \leq 0$, then $v_P(f^i) = iv_P(f) \geq kv_P(f) = v_P(f^k) \geq -v_P(G)$.

Therefore, in any case, $v_P(f^i) \geq -v_P(G)$, that is, $f^i \in \mathcal{L}(G)$. By the previous case, we have that $\lambda(f^2) = \lambda(f)^2$ and so on we get that $\lambda(f^k) = \lambda(f)^k$. □

The following proposition links λ with an automorphism of the function field. With it, we will show how λ can be used to associate to an automorphism of the code, an automorphism of the function field.

Proposition 2.2.9. *Let* $F = \mathbb{F}_q(x, y)$ *be a function field and* $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$. *Let us suppose that* $C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D', G)$ *where*

$$D = \sum_{i=1}^{n} P_i, \quad D' = \sum_{i=1}^{n} P'_i$$

and the support of G is disjoint from the supports of D and D'. Let λ be the map described in (2.2.1) *and suppose $x, y \in \mathcal{L}(G)$. If $\sigma(G) = G$ and $\sigma|_{\mathcal{L}(G)} = \lambda$, then $\sigma(P_i) = P'_i$ for any $i = 1, 2, \ldots, n$.*

Proof. By hypothesis, $x \in \mathcal{L}(G)$, therefore there exists $f \in \mathcal{L}(G)$ such that $x = \lambda(f)$ and so $x(P'_i) = \lambda(f)(P'_i) = f(P_i) = \sigma(f)(\sigma(P_i)) = \lambda(f)(\sigma(P_i)) = x(\sigma(P_i))$. Similarly, $y(P'_i) = y(\sigma(P_i))$. But for a rational place P the values $x(P)$ and $y(P)$ uniquely determine P and so, since $x(P'_i) = x(\sigma(P_i))$ and $y(P'_i) = y(\sigma(P_i))$, then $\sigma(P_i) = P'_i$ for $1 \leq i \leq n$. □

From now on we suppose that $F|\mathbb{F}_q$ is a hyperelliptic function field of genus g. We regard an elliptic function field as a special case of a hyperelliptic function field. By Proposition 1.1.13 and Proposition 1.1.14, we have:

Proposition 2.2.10. *Assume that* $\operatorname{char} \mathbb{F}_q \neq 2$.

(1) *Let $F|\mathbb{F}_q$ be a hyperelliptic function field of genus g. Then there exist $x, y \in F$ such that $F = \mathbb{F}_q(x, y)$ and*

$$y^2 - f(x) = 0 \tag{2.2.2}$$

where $f(x) \in \mathbb{F}_q[x]$ is a square-free polynomial of degree $d = 2g + 1$ or $2g + 2$.

(2) *Conversely, if $F = \mathbb{F}_q(x, y)$, where $y^2 = f(x) \in \mathbb{F}_q[x]$ and $f(x)$ is a square-free polynomial of degree $d \geq 3$, then $F|\mathbb{F}_q$ is hyperelliptic of genus*

$$g = \begin{cases} (d-1)/2, & \text{if } d \equiv 1 \pmod 2 \\ (d-2)/2, & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

(3) *Let $F = \mathbb{F}_q(x, y)$ where $y^2 = f(x) \in \mathbb{F}_q[x]$ and $f(x)$ is as in* (2.2.2). *Then the places $P \in \mathbb{P}_{\mathbb{F}_q(x)}$ which ramify in $F|\mathbb{F}_q(x)$ are the following:*

- *all zeros of* $f(x)$ *if* $\deg f(x) \equiv 0 \pmod 2$

- *all zeros of* $f(x)$ *and the pole of* x *if* $\deg f(x) \equiv 1 \pmod 2$.

Proposition 2.2.11. *Let* $d := \deg f(x)$ *where* $f(x)$ *is given by* (2.2.2). *If we denote the place (or the places) which lies over the pole* P_∞ *of* x *with* Q_∞ *(or* $Q_{\infty,1}$, $Q_{\infty,2}$ *in the split case), then:*

$$(x)_\infty = \begin{cases} 2Q_\infty, & \text{if the pole of } x \text{ ramifies in } F|\mathbb{F}_q(x) \\ Q_{\infty,1} + Q_{\infty,2}, & \text{if the pole of } x \text{ splits in } F|\mathbb{F}_q(x) \\ Q_\infty, & \text{if the pole of } x \text{ stays inert in } F|\mathbb{F}_q(x) \end{cases}$$

and

$$(y)_\infty = \begin{cases} dQ_\infty, & \text{if the pole of } x \text{ ramifies in } F|\mathbb{F}_q(x) \\ \frac{d}{2}Q_{\infty,1} + Q_{\infty,2}, & \text{if the pole of } x \text{ splits in } F|\mathbb{F}_q(x) \\ \frac{d}{2}Q_\infty, & \text{if the pole of } x \text{ stays inert in } F|\mathbb{F}_q(x). \end{cases}$$

Proof. Let us suppose the pole of x ramified in $F|\mathbb{F}_q(x)$. Then $e(Q_\infty|P_\infty) = 2$. Since P_∞ is the unique pole of x and of $f(x)$ in $\mathbb{F}_q(x)$, it is easy to show that Q_∞ is the unique pole of x and of $f(x)$ in F. Let us denote with N_x and with $N_{f(x)}$ respectively the set of poles of x and of $f(x)$ in F. By definition we have:

$$(x)_\infty = \sum_{P' \in N_x} (-v_{P'}(x))P' = -e(Q_\infty|P_\infty)v_{P_\infty}(x)Q_\infty = 2Q_\infty.$$

and

$$(y^2)_\infty = (f(x))_\infty = \sum_{P' \in N_{f(x)}} (-v_{P'}(f(x)))P' = -e(Q_\infty|P_\infty)v_{P_\infty}(f(x))Q_\infty = 2dQ_\infty$$

and the claim follows easily.

The other cases are similar. □

We denote by D_∞ the divisor of $F|\mathbb{F}_q$ defined via:

$$D_\infty = \begin{cases} Q_\infty, & \text{if the pole of } x \text{ ramifies} \\ Q_{\infty,1} + Q_{\infty,2}, & \text{if the pole of } x \text{ splits} \\ Q_\infty, & \text{if the pole of } x \text{ stays inert.} \end{cases}$$

Note that the degree of the divisor D_∞ is 1 in the first case and 2 in the other ones. We will also denote by

$$H(\mathbb{F}_q) := \mathbb{P}_F^{(1)} \cup \operatorname{supp}(D_\infty),$$

$$H_r(\mathbb{F}_q) := \{\, P \in H(\mathbb{F}_q) \setminus \operatorname{supp}(D_\infty) \mid P \text{ is ramified in } F|\mathbb{F}_q(x) \,\},$$

$$H_s(\mathbb{F}_q) := \{\, P \in H(\mathbb{F}_q) \setminus \operatorname{supp}(D_\infty) \mid P \text{ splits in } F|\mathbb{F}_q(x) \,\}.$$

For each $P \in \mathbb{P}_F^{(1)}$ we define $x_P := x(P)$ and $y_P := y(P)$. We identify P with its coordinates x_P and y_P and we set

$$P = (x_P, y_P).$$

For each $P \in \mathbb{P}_F^{(1)}$ we denote by $\overline{P}$ the conjugate $\xi(P)$ of P with respect at the non trivial automorphism ξ of $F|\mathbb{F}_q(x)$ defined by $\xi(x) = x$ and $\xi(y) = -y$. So

$$\overline{P} = (x_P, -y_P).$$

Lemma 2.2.12. (1) *If $P \in H_r(\mathbb{F}_q)$, then*

$$(x - x_P) = \begin{cases} 2P - 2D_\infty, & \text{if } d \equiv 1 \pmod 2 \\ 2P - D_\infty, & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

(2) *If $P \in H_s(\mathbb{F}_q)$, then*

$$(x - x_P) = \begin{cases} P + \overline{P} - 2D_\infty, & \text{if } d \equiv 1 \pmod 2 \\ P + \overline{P} - D_\infty, & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

Proof. (1) By definition, x_P is the unique element in $\mathbb{F}_q$ such that $x - x_P \in P$. Hence, P is a zero of $x - x_P$. Now if $x - x_P \in P$, then $x - x_P = \xi(x) - \xi(x_P) = \xi(x - x_P) \in \overline{P}$. Hence, also $\overline{P}$ is a zero of $x - x_P$.

By Zeros Theorem, we have that $\deg(x - x_P)_0 = [F : \mathbb{F}_q(x - x_P)] = [F : \mathbb{F}_q(x)] = 2$, then P and $\overline{P}$ are the only zeroes of $x - x_P$ and $(x - x_P)_0 = P + \overline{P} = 2P$, where the last equality is because P is ramified and so $P = \overline{P}$.

It is well-known that the unique pole of $x - x_P$ in $\mathbb{F}_q(x)|\mathbb{F}_q$ is P_∞. Therefore the poles of $x - x_P$ in $F|\mathbb{F}_q$ are the places which lie over P_∞ and so $(x - x_P) = 2P - 2D_\infty$ or $(x - x_P) = 2P - D_\infty$ according to d.

(2) The proof is similar to the previous case. □

Lemma 2.2.13. *Let $P = (x_P, y_P) \in H_s(\mathbb{F}_q) \setminus \mathrm{supp}(D_\infty)$. Then for each $1 \leq i \leq \left[\frac{d+1}{2}\right] = g + 1$ there exists a polynomial $h_i(x) \in \mathbb{F}_q[x]$ such that $\deg h_i(x) \leq i - 1$, $v_P(y - h_i(x)) \geq i$ and $v_{\overline{P}}(y - h_i(x)) = 0$. Moreover, if we set*

$$g_{i\overline{P}} := \frac{y - h_i(x)}{(x - x_P)^i},$$

then

$$v_{\overline{P}}(g_{i\overline{P}}) = -i$$

and

$$v_\infty(g_{i\overline{P}}) \geq \begin{cases} -(2g + 1 - 2i), & \text{if } d \equiv 1 \pmod 2 \\ -(g + 1 - i), & \text{if } d \equiv 0 \pmod 2 \end{cases}$$

(here, if $h \in F$, $v_\infty(h) := \sum_{Q \in \mathrm{supp}\,(D_\infty)} v_Q(h)$).

Proof. If we set

$$k := \begin{cases} 2g + 2, & \text{if } d \equiv 1 \pmod 2 \\ g + 1, & \text{if } d \equiv 0 \pmod 2 \end{cases}$$

then the divisor kD_∞ has, in both cases, degree $2g+2$ and the divisor $A_i := -iP + kD_\infty$, for $1 \leq i \leq g+1$, has degree $\deg A_i = \deg(-iP + kD_\infty) = -i + 2g + 2$. So, by Theorem 1.1.6, we have

$$\dim A_i \geq \deg A_i + 1 - g = (-i + 2g + 2) + 1 - g = g + 3 - i.$$

By Lemma 2.2.12.(2), it follows that

$$((x - x_P)^j) = j(x - x_P) = \begin{cases} jP + j\overline{P} - 2jD_\infty, & \text{if } d \equiv 1 \pmod 2 \\ jP + j\overline{P} - jD_\infty, & \text{if } d \equiv 0 \pmod 2. \end{cases} \tag{2.2.3}$$

Moreover,

$$A_i = \begin{cases} -iP + (2g+2)D_\infty, & \text{if } d \equiv 1 \pmod 2 \\ -iP + (g+1)D_\infty, & \text{if } d \equiv 0 \pmod 2, \end{cases}$$

so $(x - x_P)^j \in \mathcal{L}(A_i)$ if and only if

$$\begin{cases} jP + j\overline{P} - 2jD_\infty \geq iP - (2g+2)D_\infty, & \text{if } d \equiv 1 \pmod 2 \\ jP + j\overline{P} - jD_\infty \geq iP - (g+1)D_\infty, & \text{if } d \equiv 0 \pmod 2, \end{cases}$$

that is, in both cases, $i \leq j \leq g+1$.

Then, if S_i denotes the $\mathbb{F}_q-$vector space generated by $\{\, (x - x_P)^j \mid i \leq j \leq g+1 \,\}$ we have that

$$S_i \subset \mathcal{L}(A_i) \subset \mathcal{L}(kD_\infty) = \langle\, 1, (x - x_P), (x - x_P)^2, \ldots, (x - x_P)^{g+1}, y - y_P \,\rangle$$

where the last inclusion follows from the fact that $A_i < kD_\infty$.

Since $\dim S_i \leq (g+1) - i + 1 = g + 2 - i$ and $\dim A_i \geq g + 3 - i$, there exists $f' \in \mathcal{L}(A_i) \setminus S_i$. Because $\mathcal{L}(A_i)$ is a subspace of $\mathcal{L}(kD_\infty)$ we know that f' is an $\mathbb{F}_q-$linear combinations of $y - y_P$ and $(x - x_P)^r$ $(0 \leq r \leq g+1)$:

$$f' = a(y - y_P) + \sum_{r=0}^{g+1} a_r (x - x_P)^r.$$

Since $\sum_{r=i}^{g+1} a_r(x-x_p)^r \in S_i$, we have that

$$f_{iP} := f' - \sum_{r=i}^{g+1} a_r(x-x_P)^r = a(y-y_P) + \sum_{r=0}^{i-1} a_r(x-x_P)^r$$

is also an element of $\mathcal{L}(A_i) \setminus S_i$.

Using the "Strict Triangle Inequality", it is possible to show that $a \neq 0$ and so if we set $y - h_i(x) := a^{-1} f_{iP} \in \mathcal{L}(A_i)$ we have

$$\deg h_i(x) \leq i-1$$

and

$$v_P(y-h_i(x)) \geq -v_P(A_i) = i.$$

Moreover, since $(y-h_i(x))(\overline{P}) = -y_P - y_P + \sum_{r=i}^{g+1} a^{-1}a_r(x_P-x_P)^r = -2y_P \neq 0$, then

$$v_{\overline{P}}(y-h_i(x)) = 0.$$

Furthermore, we have

$$v_{\overline{P}}(g_{i\overline{P}}) = v_{\overline{P}}\left(\frac{y-h_i(x)}{(x-x_P)^i}\right) = v_{\overline{P}}(y-h_i(x)) - v_{\overline{P}}((x-x_P)^i) = -iv_{\overline{P}}(x-x_P) = -i.$$

Finally,

$$v_\infty(y-h_i(x)) \geq \begin{cases} -(2g+1), & \text{if } d \equiv 1 \pmod 2 \\ -(g+1), & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

Hence, by the (2.2.3),

$$v_\infty(g_{i\overline{P}}) \geq \begin{cases} -(2g+1-2i), & \text{if } d \equiv 1 \pmod 2 \\ -(g+1-i), & \text{if } d \equiv 0 \pmod 2. \end{cases}$$

□

Proposition 2.2.14. *Let $J \subseteq H(\mathbb{F}_q) \setminus \operatorname{supp}((x)_\infty)$ and G be a divisor of the form*

$$G = n_\infty D_\infty + \sum_{Q \in J} n_Q Q \tag{2.2.4}$$

where $n_Q \geq 1$ for each $Q \in J$ and $n_\infty \geq \begin{cases} 2g+2 & \text{if } d \equiv 1 \pmod 2 \\ g+1 & \text{if } d \equiv 0 \pmod 2. \end{cases}$
If $m := g+1$, then a base B of $\mathcal{L}(G)$ is the following:

$$B = \left\{ x^\alpha y^\beta \mid \alpha \geq 0, \beta \in \{0,1\} \text{ and } x^\alpha y^\beta \in \mathcal{L}(n_\infty D_\infty) \right\} \cup$$
$$\cup \left\{ \left(\tfrac{1}{x-x_Q}\right)^\alpha \left(\tfrac{y}{x-x_Q}\right)^\beta \mid 2\alpha+\beta \leq n_Q, \alpha \geq 0, \beta \in \{0,1\} \text{ and } Q \in J \cap H_r(\mathbb{F}_q) \right\} \cup$$
$$\cup \left\{ (g_{mQ})^\alpha (g_{\beta Q}) \mid m\alpha+\beta \leq n_Q, \alpha \geq 0, 0 \leq \beta < m \text{ and } Q \in J \cap H_s(\mathbb{F}_q) \right\}.$$

Proof. Case $d \equiv 1 \pmod 2$.

First we shall check that all functions of B are actually in $\mathcal{L}(G)$. Obviously the functions of the form $x^i y^j$ are in $\mathcal{L}(G)$ and the number of them is

$$\dim(\mathcal{L}(n_\infty D_\infty)) = n_\infty + 1 - g$$

(the equality follows by Theorem 1.1.6 since $\deg n_\infty D_\infty = n_\infty \geq 2g+2$).
Now looking at $Q \in J \cap H_r(\mathbb{F}_q)$ we note that $\left(\frac{y}{x-x_Q}\right) = (y) - (x-x_Q) =$ $\left(\left(\sum_{P \in H_r} P\right) - dD_\infty\right) - (2Q - 2D_\infty) = \left(\sum_{P \in H_r,\ P \neq Q} P\right) + (2-d)D_\infty - Q =$ $\left(\sum_{P \in H_r,\ P \neq Q} P\right) - (2g-1)D_\infty - Q$ (where H_r is the set of all ramified place of $F|\mathbb{F}_q$) and that $\left(\frac{1}{x-x_Q}\right) = -(x-x_Q) = 2D_\infty - 2Q$.
Thus, for $1 \leq i \leq n_Q$ we can write $i = 2\alpha + \beta$ with $\alpha \geq 0$, $\beta \in \{0,1\}$ and we have $v_Q\left(\left(\frac{1}{x-x_Q}\right)^\alpha \left(\frac{y}{x-x_Q}\right)^\beta\right) = \alpha \cdot v_Q\left(\frac{1}{x-x_Q}\right) + \beta \cdot v_Q\left(\frac{y}{x-x_Q}\right) = -2\alpha - \beta = -i \geq -n_Q = -v_Q(G)$ and $v_\infty\left(\left(\frac{1}{x-x_Q}\right)^\alpha \left(\frac{y}{x-x_Q}\right)^\beta\right) = \alpha \cdot v_\infty\left(\frac{1}{x-x_Q}\right) + \beta \cdot v_\infty\left(\frac{y}{x-x_Q}\right) = 2\alpha - \beta(2g-1) \geq -(2g+2) \geq -n_\infty = -v_\infty(G)$ and so all the n_Q considered functions are in $\mathcal{L}(G)$.

Finally, we look at $Q \in J \cap H_s(\mathbb{F}_q)$. For $1 \leq i \leq n_Q$ we can write $i = m\alpha+\beta$ with $\alpha \geq 0$ and $0 \leq \beta < m$. Thus, by Lemma 2.2.13, we have $v_Q((g_{mQ})^\alpha(g_{\beta Q})) = -(m\alpha + \beta) = -i \geq -n_Q = -v_Q(G)$ and $v_\infty((g_{mQ})^\alpha(g_{\beta Q})) \geq -\alpha(2g + 1 - 2m) - (2g + 1 - 2\beta) = \alpha - (2g + 1 - 2\beta) \geq -(2g + 1 - 2\beta) \geq -(2g + 2) \geq -n_\infty = -v_\infty(G)$ if $\beta \neq 0$; whereas $v_Q((g_{mQ})^\alpha(g_{\beta Q})) = -m\alpha = -i \geq -n_Q = -v_Q(G)$ and $v_\infty((g_{mQ})^\alpha(g_{\beta Q})) \geq -\alpha(2g + 1 - 2m) = \alpha \geq 0 \geq -(2g + 2) \geq -n_\infty = -v_\infty(G)$ if $\beta = 0$ (we recall that $m = g + 1$ and so $2g + 1 - 2m = -1$). We realize that all these n_Q functions are in $\mathcal{L}(G)$.

Since

$$\deg G = n_\infty + \sum_{Q \in J} n_Q \geq 2g + 2$$

it follows, by Theorem 1.1.6, that

$$\dim G = \deg G + 1 - g = n_\infty + \sum_{Q \in J} n_Q + 1 - g.$$

Hence $|B| = \dim G$. From the "Strict Triangle Inequality" follows also that these elements are linearly independent and the claim is proved.

Case $d \equiv 0 \pmod 2$.

The proof is omitted since it is similar to the previous case. □

Remark 2.2.1. If G is as in (2.2.4), then $x, y \in \mathcal{L}(G)$.

Now we are ready to give the main theorem in the hyperelliptic case.

Theorem 2.2.15. *Let*

$$G = n_\infty D_\infty + \sum_{Q \in J} n_Q Q$$

be a divisor as in (2.2.4). *Let* $I \subseteq H(\mathbb{F}_q) \setminus \operatorname{supp} G$ *and let* $D = \sum_{P \in I} P$ *be a divisor of degree* n. *If* $n > \max\{2 \deg G, 2g + 2\}$, *then*

$$\operatorname{Aut}(C_{\mathcal{L}}(D, G)) \cong \operatorname{Aut}_{D,G}(F|\mathbb{F}_q).$$

Proof. By Theorem 2.2.2.(2), $\mathrm{Aut}_{D,G}(F|\mathbb{F}_q)$ is isomorphic to a subgroup of $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$. We prove that such subgroup is actually isomorphic to the whole group $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$. Consider $\pi \in \mathrm{Aut}(C_{\mathcal{L}}(D,G))$. By Lemma (2.1.3), we know that $C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(\pi(D),G)$ and so we can consider the corresponding map $\lambda = \lambda_\pi$ (see (2.2.1)). Furthermore, by Lemma 2.2.8, it is possible to prove that

$$\lambda(x^\alpha y^\beta) = \lambda(x)^\alpha \lambda(y)^\beta, \quad \text{for } x^\alpha y^\beta \in \mathcal{L}(G).$$

Since $1 = \lambda(1) = \lambda\left(\frac{1}{x-x_Q}\right)\lambda(x-x_Q) = \lambda\left(\frac{1}{x-x_Q}\right)(\lambda(x)-x_Q)$, we have $\lambda\left(\frac{1}{x-x_Q}\right) = \frac{1}{\lambda(x)-x_Q}$ and $\lambda\left(\frac{y}{x-x_Q}\right) = \lambda(y)\lambda\left(\frac{1}{x-x_Q}\right) = \frac{\lambda(y)}{\lambda(x)-x_Q}$. Hence,

$$\lambda\left(\left(\frac{1}{x-x_Q}\right)^\alpha \left(\frac{y}{x-x_Q}\right)^\beta\right) = \left(\frac{1}{\lambda(x)-x_Q}\right)^\alpha \left(\frac{\lambda(y)}{\lambda(x)-x_Q}\right)^\beta$$

for $2\alpha+\beta \le n_Q$, $\alpha \ge 0$, $\beta \in \{0,1\}$ and $Q \in J \cap H_r(\mathbb{F}_q)$.

Moreover, since $(x-x_Q)^i, y-p_i(x) \in \mathcal{L}(G)$ if $Q \in \mathrm{supp}\,(G) \cap H_s(\mathbb{F}_q)$, $1 \le i \le \min\{n_Q, g+1\}$ and $\deg p_i(x) \le i-1$, it makes sense considering $\lambda((x-x_Q)^i) = (\lambda(x)-x_Q)^i$ and $\lambda(y-p_i(x)) = \lambda(y)-p_i(\lambda(x))$. Therefore, $\lambda(g_{iQ}) = \frac{\lambda(y-p_i(x))}{\lambda((x-x_Q)^i)} = \frac{\lambda(y)-p_i(\lambda(x))}{(\lambda(y)-x_Q)^i}$ and so

$$\lambda((g_{mQ})^\alpha(g_{\beta Q})) = \left(\frac{\lambda(y)-p_m(\lambda(x))}{(\lambda(x)-x_Q)^i}\right)^\alpha \frac{\lambda(y)-p_\beta(\lambda(x))}{(\lambda(x)-x_Q)^i}$$

for $m\alpha+\beta \le n_Q$, $\alpha \ge 0$, $0 \le \beta < m$ and $Q \in J \cap H_s(\mathbb{F}_q)$.

Since every element $h(x,y) \in \mathcal{L}(G)$ can be written as linear combination of some of the above elements, we proved that $\lambda(h(x,y)) = h(\lambda(x),\lambda(y))$. Now we will prove that $\lambda(x)$ and $\lambda(y)$ are such that

$$\lambda(y)^2 - f(\lambda(x)) = 0.$$

We start noticing that x and $x^{[\frac{d+1}{2}]}$ belong to $\mathcal{L}(G)$ and so, by Lemma 2.2.8, $\deg(\lambda(x))_\infty \le \frac{\deg G}{g+1} \le \frac{2\deg G}{d}$, that is, $\deg((\lambda(x)^d)_\infty) \le 2\deg G < n$. Since $\deg f(x) = d$, we

have $\deg(f(\lambda(x)))_\infty \leq 2\deg G$; also, since $\lambda(y) \in \mathcal{L}(G)$ we have $\deg(\lambda(y)^2)_\infty = 2\deg(\lambda(y))_\infty \leq 2\deg G$. So we have that $\lambda(y)^2, f(\lambda(x)) \in \mathcal{L}(2G)$. We also remark that $\lambda(y)^2(P) = f(\lambda(x))(P)$ for each $P \in \operatorname{supp} D$. In fact, $\lambda(y)^2(P_{\pi(i)}) = (\lambda(y)(P_{\pi(i)}))^2 = (y(P_i))^2 = y^2(P_i) = f(x)(P_i) = f(x(P_i)) = f(\lambda(x)(P_{\pi(i)})) = f(\lambda(x))(P_{\pi(i)})$. Then, since $\deg 2G < n$, by Lemma 2.2.7, we have $\lambda(y)^2 = f(\lambda(x))$. Hence, there exists an $\mathbb{F}_q-$endomorphism

$$\begin{array}{rccc} \widetilde{\lambda}: & F & \longrightarrow & F \\ & h(x,y) & \mapsto & h(\lambda(x),\lambda(y)) \end{array}$$

of the function field $F|\mathbb{F}_q$ such that the restriction of $\widetilde{\lambda}$ to $\mathcal{L}(G)$ is equal to λ. Since x and y are in the image of λ, we have $\widetilde{\lambda}$ is an automorphism of $\operatorname{Aut}(F|\mathbb{F}_q)$. We only have to prove that $\widetilde{\lambda} \in \operatorname{Aut}_{D,G}(F|\mathbb{F}_q)$. By Lemma 2.2.6, $\widetilde{\lambda}(G) = G$ and so Lemma 2.2.9 can be applied to prove that $\widetilde{\lambda}(P_i) = P_{\pi(i)}$, that is, $\widetilde{\lambda}(D) = D$. □

Chapter 3

Generalized Algebraic Geometry Codes

In this chapter we will describe the generalized algebraic geometry codes which are constructed making use of places of the same degree $n > 1$. We will determine the $n-$automorphism group of a such class of generalized algebraic geometry codes associated with rational, elliptic and hyperelliptic function fields. Such group is, up to isomorphism, a subgroup of the automorphism group of the underlying function field (see [P-S]).

3.1 $\phi-$places

Let $F|\mathbb{F}_q$ be an algebraic function field of genus g and P a place of F of degree n. The residue class field F_P of P is, up to isomorphism, an extension of degree n of the field $\mathbb{F}_q$. So there exist exactly n $\mathbb{F}_q-$isomorphisms from F_P to $\mathbb{F}_{q^n}$. A $\phi - place$ (see [Sp1]) is a pair (P, ϕ_P) where P is a place of degree n of $F|\mathbb{F}_q$ and $\phi_P : F_P \longrightarrow \mathbb{F}_{q^n}$ is an $\mathbb{F}_q-$isomorphism.

If (P, ϕ_P) is a $\phi-$place of F and $z \in F$ is regular on P we set $z(P, \phi_P) := \phi_P(z(P))$.

A $\phi - divisor$ is an element of the free abelian group generated by $\phi-$places, that is, it is a formal sum

$$\Phi = \sum_{P \in \mathbb{P}_F} n_P \, (P, \phi_P)$$

with $n_P \in \mathbb{Z}$ and $n_P \neq 0$ only for a finite number of places.

If $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$, we also denote by σ the $\mathbb{F}_q-$isomorphism from F_P to $F_{\sigma(P)}$ which is induced by σ (see (1.1.2), pag. 11). So, if (P, ϕ_P) is a $\phi-$place, then $\phi\sigma^{-1}$ is an $\mathbb{F}_q-$isomorphism from $F_{\sigma(P)}$ to $\mathbb{F}_{q^n}$. Hence, it is natural to define an action of $\mathrm{Aut}(F|\mathbb{F}_q)$ on the set of the $\phi-$places (see [Sp1]) by

$$\sigma(P, \phi_P) := (\sigma(P), \phi_P \sigma^{-1}). \tag{3.1.1}$$

This action can be extended on the group of the $\phi-$divisors in obvious way:

$$\sigma\big(\sum_{P \in \mathbb{P}_F} n_P (P, \phi_P) \big) := \sum_{P \in \mathbb{P}_F} n_P (\sigma(P), \phi_P \sigma^{-1}).$$

Let us consider the finite fields $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$. It is well-known that $\mathbb{F}_{q^n}$ can be represented as $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ where $\alpha \in \overline{\mathbb{F}_q}$. So $\{\ 1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\ \}$ is an $\mathbb{F}_q-$base for $\mathbb{F}_{q^n}$ and we can identify every element $\sum_{i=0}^{n-1} a_i \alpha^i$ of $\mathbb{F}_{q^n}$ with $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$. Let $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ be a $\phi-$divisor of $F|\mathbb{F}_q$ with the P_i's pairwise distinct places all of the same degree $n > 1$. Let G be a divisor such that $\mathrm{supp}\, G \cap \mathrm{supp}\, D = \emptyset$ where $D = \sum_{i=1}^{N} P_i$. For any $z \in \mathcal{L}(G)$ and for any $i = 1, 2, \ldots, N$ we have that $z(P_i, \phi_i) \in \mathbb{F}_{q^n}$ and so, by the above identification, $z(P_i, \phi_i) \in \mathbb{F}_q^n$. Let us consider the linear map $ev_\Phi : \mathcal{L}(G) \to \mathbb{F}_q^{nN}$ defined via

$$ev_\Phi(z) := (z(P_1, \phi_1), z(P_2, \phi_2), \ldots, z(P_N, \phi_N)), \tag{3.1.2}$$

for all $z \in \mathcal{L}(G)$.

We will call the linear code $C(\Phi; G; n) := ev_\Phi(\mathcal{L}(G))$ a *generalized algebraic geometry*

code (for short GAG-*code*). Note that GAG-codes defined as above are a particular class of the more general GAG-codes considered in [X-N-L] and in [Hey].

Proposition 3.1.1. *$C(\Phi; G; n)$ is a $q-$ary $[nN, k, d]$ code with*

$$k = \dim G - \dim(G - D) \quad \textit{and} \quad d \geq N - \left\lfloor \frac{\deg G}{n} \right\rfloor.$$

Here $\lfloor x \rfloor$ denotes the greatest integer smaller than or equal to x.

Proof. $\mathrm{Ker}\,(ev_\Phi) = \{\, x \in \mathcal{L}(G) \,|\, x(P_i, \phi_i) = 0 \text{ for any } i = 1, 2, \ldots, N \,\} = \{\, x \in \mathcal{L}(G) \,|\, \phi_i(x(P_i)) = 0 \text{ for any } i = 1, 2, \ldots, N \,\} = \{\, x \in \mathcal{L}(G) \,|\, v_{P_i}(x) \geq 1 \text{ for any } i = 1, 2, \ldots, N \,\} = \{\, x \in \mathcal{L}(G) \,|\, v_{P_i}(x) \geq v_{P_i}(D) \text{ for any } P_i \in \mathrm{supp}\, D \,\} = \mathcal{L}(G - D)$. Hence

$$C(\Phi; G; n) = \mathcal{L}(G)/\mathcal{L}(G - D)$$

and we get

$$k = \dim G - \dim(G - D).$$

Moreover, if d is the minimum distance of $C(\Phi; G; n)$, then there exists an element $0 \neq x \in \mathcal{L}(G)$ such that the weight of $ev_\Phi(x)$ is d. Let us denote by $d' = d'(x)$ the number of indexes $i \in \{\, 1, 2, \ldots, N \,\}$ such that $x(P_i, \phi_i) \neq 0$. Hence, there are exactly $N - d'$ indexes $i_1, i_2, \ldots, i_{N-d'}$ such that $x(P_{i_j}, \phi_{i_j}) = 0$. But ϕ_{i_j} is a bijection, so $x(P_{i_j}) = 0$ for every $j = 1, 2, \ldots, N - d'$. It follows that

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{N-d'}}))$$

and so, by Proposition 1.1.5.(4), necessarily

$$0 \leq \deg(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{N-d'}})) = \deg G - (N - d')n.$$

Finally, $d \geq d' \geq N - \left\lfloor \frac{\deg G}{n} \right\rfloor$. □

Corollary 3.1.2. (1) *If* $\deg G < nN$, *then* $C(\Phi; G; n)$ *is a* $q-$*ary* $[nN, k, d]$ *code with*

$$k = \dim G \geq \deg G + 1 - g \quad \textit{and} \quad d \geq N - \Big\lfloor \frac{\deg G}{n} \Big\rfloor.$$

Moreover, if $\{ x_1, x_2, \ldots, x_k \}$ *is a base for* $\mathcal{L}(G)$, *then the matrix*

$$M = \begin{pmatrix} x_1(P_1, \phi_1) & x_1(P_2, \phi_2) & \cdots & x_1(P_N, \phi_N) \\ x_2(P_1, \phi_1) & x_2(P_2, \phi_2) & \cdots & x_2(P_N, \phi_N) \\ \vdots & \vdots & & \vdots \\ x_k(P_1, \phi_1) & x_k(P_2, \phi_2) & \cdots & x_k(P_N, \phi_N) \end{pmatrix}$$

is a generator matrix for $C(\Phi; G; n)$.

(2) *If* $2g - 2 \leq \deg G < nN$, *then* $C(\Phi; G; n)$ *is a* $q-$*ary* $[nN, k, d]$ *code with*

$$k = \deg G + 1 - g \quad \textit{and} \quad d \geq N - \Big\lfloor \frac{\deg G}{n} \Big\rfloor.$$

Proof. (1) If $\deg G < nN = \deg D$, then $\deg(G-D) < 0$ and, by Proposition 1.1.5.(4), it follows that $\dim(G-D) = 0$. Thus $k = \dim G - \dim(G-D) = \dim G \geq \deg G + 1 - g$ where last relation follows by Theorem 1.1.6.

A generator matrix for an $[nN, k, d]$ code is a $k \times nN$ matrix whose rows are a basis of the code. But $\dim(G - D) = 0$, then ev_Φ is an isomorphism and so $\{ ev_\Phi(x_1), ev_\Phi(x_2), \ldots, ev_\Phi(x_k) \}$ is a base for $C(\Phi; G; n)$. From this follows easily that M is a generator matrix for $C(\Phi; G; n)$.

(2) If $2g - 2 < \deg G < nN$, then, by Theorem 1.1.6, $\dim G = \deg G + 1 - g$ and so we get the thesis. □

3.2 The $n-$Automorphism Group of a GAG-Code

Let n and m be positive integers, and suppose that n divides m. We can write every element of $c \in \mathbb{F}_q^m$ as $c = (a_1, a_2, \ldots, a_{m/n})$ where $a_i = c_{i1}c_{i2}\cdots c_{in}$ with $c_{ij} \in \mathbb{F}_q$ for $1 \leq i \leq m/n$ and $1 \leq j \leq n$.

$S_{m/n}$ acts on $\mathbb{F}_q^m$ via

$$\pi(c) = (a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(m/n)})$$

if $\pi \in S_{m/n}$ and $c = (a_1, a_2, \ldots, a_{m/n}) \in \mathbb{F}_q^m$.

Obviously, π is also an element of S_m. Moreover, if $n = 1$ we get the usual action of S_m on $\mathbb{F}_q^m$.

Let $F|\mathbb{F}_q$ be a function field of genus g. Let $C(\Phi; G; n) \subseteq \mathbb{F}_q^{nN}$ be a GAG-code associated with Φ and G. If $\pi \in S_{\frac{nN}{n}}$, π is said to be an *n-automorphism* of the code $C(\Phi; G; n)$ if

$$\pi(c) = (a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(N)}) \in C(\Phi; G; n)$$

for any $c = (a_1, a_2, \ldots, a_N) \in C(\Phi; G; n)$. The *$n$-automorphism group* $\mathcal{H}(\Phi; G; n)$ of the GAG-code will be the following subgroup of $\mathrm{Aut}(C(\Phi; G; n))$:

$$\mathcal{H}(\Phi; G; n) := \{\pi \in S_N \mid \pi(c) \in C(\Phi; G; n) \text{ for any } c \in C(\Phi; G; n)\}.$$

Now we give a lemma which we will use later.

Lemma 3.2.1. *If $\pi \in \mathcal{H}(\Phi; G; n)$, then*

$$C(\Phi; G; n) = C(\pi\Phi; G; n) \tag{3.2.1}$$

where $\pi\Phi := \sum_{i=1}^{N}(P_{\pi(i)}, \phi_{\pi(i)})$ if $\Phi := \sum_{i=1}^{N}(P_i, \phi_i)$.

Proof. For any $\pi \in \mathcal{H}(\Phi; G; n)$ and for any $z \in \mathcal{L}(G)$

$$(z(P_{\pi(1)}, \phi_{\pi(1)}), \ldots, z(P_{\pi(N)}, \phi_{\pi(N)})) = \pi(z(P_1, \phi_1), \ldots, z(P_N, \phi_N)) \in C(\Phi; G; n)$$

and so $C(\pi\Phi; G; n) \subseteq C(\Phi; G; n)$. Hence, $C(\pi\Phi; G; n) = C(\Phi; G; n)$ since both codes have the same dimension (see Proposition 3.1.1). □

Let $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$ and G and G' be divisors of $F|\mathbb{F}_q$. The divisor G is said to be $\Phi-$equivalent to G', and we will write $G \sim_\Phi G'$, if and only if there exists an element $z \in F$, $z \neq 0$, such that $G = G' + (z)$ and $z(P_i, \phi_i) = 1$ for every $i = 1, 2, \ldots, N$. Obviously, $\sim_\Phi$ is an equivalence relation and so we are able to define the following subgroup of $\mathrm{Aut}(F|\mathbb{F}_q)$

$$\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G) := \{\, \sigma \in \mathrm{Aut}(F|\mathbb{F}_q) \mid \sigma(\Phi) = \Phi \text{ and } \sigma(G) \sim_\Phi G\}.$$

Lemma 3.2.2. *If $G = G_0 - G_1$, where G_0 and G_1 are effective divisors, and if $\deg(G_0 + G_1) \leq nN - 1$, then*

$$\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G) = \{\, \sigma \in \mathrm{Aut}(F|\mathbb{F}_q) \mid \sigma(\Phi) = \Phi \text{ and } \sigma(G) = G\,\}.$$

Proof. We have to prove that if G and $\sigma(G)$ are $\sim_\Phi$ $-$equivalent, then $\sigma(G) = G$. Let $\sigma(G) = G + (u)$ with $u(P_i, \phi_i) = 1$ for every $i = 1, 2, \ldots, N$. Then $(u) = \sigma(G) - G = \sigma(G_0 - G_1) - (G_0 - G_1) = (\sigma(G_0) + G_1) - (\sigma(G_1) + G_0) \geq -(\sigma(G_1) + G_0)$. It follows that $u \in \mathcal{L}(\sigma(G_1) + G_0)$ and, since $\sigma(G_1) + G_0 \geq 0$ implies $1 \in \mathbb{F}_q \subseteq \mathcal{L}(\sigma(G_1) + G_0)$, we have $u - 1 \in \mathcal{L}(\sigma(G_1) + G_0)$. So the pole divisor $(u-1)_\infty$ of $u - 1$ is smaller or equal than $\sigma(G_1) + G_0$ and we obtain

$$\deg(u-1)_\infty \leq nN - 1. \tag{3.2.2}$$

Now suppose $u \notin \mathbb{F}_q$. Since $u(P_i, \phi_i) = 1$ for every $i = 1, 2, \ldots, N$ we get P_i is a zero of $u - 1$ for each $i = 1, 2, \ldots, N$, so $\deg(u-1)_0 \geq nN$, which is in contradiction with (3.2.2). Therefore $u \in \mathbb{F}_q$ and we have $(u) = 0$ which implies $\sigma(G) = G$. □

Remark 3.2.1. By the previous lemma we have that if $G > 0$ and $\deg G < nN$, then $\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ is the stabilizer of Φ and G in $\mathrm{Aut}(F|\mathbb{F}_q)$, that is,

$$\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G) = \mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,G}$$

and, by (3.1.1)

$$\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G) = \{\, \sigma \in \mathrm{Aut}(F|\mathbb{F}_q) \mid \sigma(G) = G,\ \sigma(D) = D \text{ and } \phi_{\sigma(P_i)} = \phi_{P_i}\sigma^{-1} \text{ for all } i = 1, 2, \ldots, N \,\}.$$

By Lemma 1.1.7, we known that if $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$ fixes at least $2g + 3$ rational places, then σ is the identity map. After we have proved some lemmas, we will analyze the case where σ fixes places of degree greater than one (see [Sp2]).

Lemma 3.2.3. *If P is a place of $F|\mathbb{F}_q$ and if $s \geq 0$ is a integer such that $s-1 \geq \frac{2g-1}{\deg P}$, then there exists $x \in F$, $x \neq 0$, such that $(x)_\infty = sP$.*

Proof. $s-1 \geq \frac{2g-1}{\deg P}$ implies $\deg(s-1)P \geq 2g-1$ and $\deg sP \geq 2g-1$. So, by Theorem 1.1.6, $\dim(s-1)P = (s-1)\deg P + 1 - g < s \cdot \deg P + 1 - g = \dim sP$ and we obtain that there exists $x \in \mathcal{L}(sP) \setminus \mathcal{L}((s-1)P)$. Hence necessarily $(x)_\infty = sP$. □

Lemma 3.2.4. *If $x, y \in F \setminus \mathbb{F}_q$ and $(\deg(x)_\infty, \deg(y)_\infty) = 1$, then $F = \mathbb{F}_q(x, y)$.*

Proof. By Zeros Theorem, we have $\deg(x)_\infty = [F : \mathbb{F}_q(x)]$ and $\deg(y)_\infty = [F : \mathbb{F}_q(y)]$. But $\mathbb{F}_q(x, y) \supseteq \mathbb{F}_q(x), \mathbb{F}_q(y)$ and so $[F : \mathbb{F}_q(x, y)]$ divides $[F : \mathbb{F}_q(x)]$ and $[F : \mathbb{F}_q(y)]$. Therefore, by hypotheses, $[F : \mathbb{F}_q(x, y)] = 1$ and we get $F = \mathbb{F}_q(x, y)$. □

Lemma 3.2.5. *There exist $x, y \in F \setminus \mathbb{F}_q$ such that $F = \mathbb{F}_q(x, y)$, $(x)_\infty = (2g+1)P$ and $(y)_\infty = 2P'$ where P and P' are places of degree $4g+3$ and $4g+4$ respectively.*

Proof. It is known (see for instance [St1]) that if $n \geq 4g+3$, then there exists at least a place of degree n. So there exist two places P and P' of degree $4g+3$ and $4g+4$ respectively. Moreover, by Lemma 3.2.3, there exist $x, y \in F^*$ such that $(x)_\infty = (2g+1)P$ and $(y)_\infty = 2P'$. Thus, by Lemma 3.2.4, it is enough to show that $((2g+1)(4g+3), 8(g+1)) = 1$. In fact, if r is a odd number which divides $g+1$ and $2g+1$, then r divides g and so $r = 1$. On the other hand if r divides $g+1$ and $4g+3 = (2g+1) + 2(g+1)$, then r divides $2g+1$ and so, as in the previous case, $r = 1$ as well. □

Lemma 3.2.6. *If $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$ fixes the ϕ-place (P, ϕ_P), then P is zero of $\sigma(x) - x$ for every $x \in F$ which is regular in P.*

Proof. By the (3.1.1), we have that σ fixes (P, ϕ_P) if and only if $\sigma(P) = P$ and $\phi_{\sigma(P)} = \phi_P \sigma^{-1}$. Hence, $\phi_P = \phi_P \sigma^{-1}$ and we get $\sigma : F_P \longrightarrow F_{\sigma(P)}$ is the identity automorphism. It follows that for every $x \in F$ which is regular on P, $\sigma(x(P)) = x(P)$ and so we obtain $\sigma(x) - x \in P$. □

Theorem 3.2.7. *Let $F|\mathbb{F}_q$ be a function field of genus g. Let (P_i, ϕ_i), for $i = 1, 2, \ldots, N$, be N ϕ-places whose places P_i are pairwise distinct and all of the same degree $n > 1$. If $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$ is an automorphism which fixes (P_i, ϕ_i) for every $i = 1, 2, \ldots, N$, then σ is the identity map if at least one of the following hypotheses is satisfied:*

(1) $N - 1 > \frac{16(g+1)^2}{n}$;

(2) *$F|\mathbb{F}_q$ has some rational place and $N \geq \frac{4g+3}{n}$;*

(3) *σ fixes some rational place and $N \geq \frac{2g+2}{n}$.*

Proof. (1) Let x, y and P, P' as in Lemma 3.2.5. Since at most only one of P and P' is in $\operatorname{supp} D$, then x, y are regular on at least $N-1$ of the elements of $\operatorname{supp} D$ where D is the divisor associated to $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$. So, by Lemma 3.2.6, $x - \sigma(x)$ and $y - \sigma(y)$ have at least $N-1$ zeroes of degree n. If $x - \sigma(x) \neq 0 \neq y - \sigma(y)$ (or either of them), we have that

$$\deg(x - \sigma(x))_0 \geq (N-1)n \quad \text{and} \quad \deg(y - \sigma(y))_0 \geq (N-1)n \tag{3.2.3}$$

if one of P and P' belongs to $\operatorname{supp} D$ or

$$\deg(x - \sigma(x))_0 \geq Nn \quad \text{and} \quad \deg(y - \sigma(y))_0 \geq Nn \tag{3.2.4}$$

if $P, P' \notin \operatorname{supp} D$. So in any case (3.2.3) hold.

Now, $v_P(x - \sigma(x)) \geq \min\{ v_P(x), v_{\sigma^{-1}(P)}(x) \} \geq -(2g+1)$ because of $v_{\sigma^{-1}(P)}(x) = -(2g+1)$ if $\sigma(P) = P$ and $v_{\sigma^{-1}(P)}(x) \geq 0$ if $\sigma(P) \neq P$. For $Q = \sigma(P)$ and $Q \neq P$, $v_Q(x - \sigma(x)) \geq -(2g+1)$ since $v_{\sigma^{-1}(Q)}(x) \geq -(2g+1)$ and $v_Q(x) \geq 0$. Whereas for $Q \neq P$ and $Q \neq \sigma(P)$ we obtain $v_Q(x - \sigma(x)) \geq 0$. Hence, $(x - \sigma(x))_\infty \leq (2g+1)P + (2g+1)\sigma(P)$. It follows $\deg(x - \sigma(x))_\infty \leq 2(2g+1)(4g+3) < 16(g+1)^2 < (N-1)n$ which is a contradiction to the (3.2.3). In a similar way, we are able to prove that $\deg(y - \sigma(y))_\infty \leq 2^2(4g+4) = 16(g+1) \leq 16(g+1)^2 < (N-1)n$ which is again a contradiction to the (3.2.3). Therefore σ fixes x and y and so we get that σ fixes each element of $F = \mathbb{F}_q(x, y)$, that is, σ is the identity map.

(2) Let Q be a rational place of $F|\mathbb{F}_q$. By Lemma 3.2.3, there exist $x, y \in F^*$ such that $(x)_\infty = 2gQ$ and $(y)_\infty = (2g+1)Q$. Moreover, since $(2g, 2g+1)$, by Lemma 3.2.4, we have $F = \mathbb{F}_q(x, y)$.

From $n > 1$ we have $Q \notin \operatorname{supp} D$ and so x, y are regular on P_i for every $i = 1, 2, \ldots, N$. It follows that $P_1, P_2, \ldots, P_N$ are zeroes of $x - \sigma(x)$ and $y - \sigma(y)$. Thus $\deg(x - \sigma(x))_\infty \geq nN \geq 4g + 3$ and $\deg(y - \sigma(y))_\infty \geq 4g + 3$. On the other hand $v_Q(x - \sigma(x)) \geq \min\{v_Q(x), v_{\sigma^{-1}(Q)}(x)\} = -2g$ because of $v_{\sigma^{-1}(Q)}(x) \geq 0$ if $\sigma(Q) \neq Q$ and $v_{\sigma^{-1}(Q)}(x) = -2g$ if $\sigma(Q) = Q$. If $P' \neq Q$ and $P' = \sigma(Q)$, then $v_{P'}(x - \sigma(x)) \geq \min\{v_{\sigma(Q)}(x), v_Q(x)\} \geq -2g$ being $v_{\sigma(Q)}(x) \geq 0$ and $v_Q(x) = -2g$. Now if we suppose $P' \neq Q$ and $P' \neq \sigma(Q)$, then $v_{P'}(x - \sigma(x)) \geq \min\{v_{P'}(x), v_{\sigma^{-1}(P')}(x)\} \geq 0$ since $\sigma^{-1}(P') \neq Q$. Therefore $(x - \sigma(x))_\infty \leq 2gQ + 2g\sigma(Q)$. This implies $\deg(x - \sigma(x))_\infty \leq 4g$. Therefore $\sigma(x) = x$. In the same way we obtain $\deg(y - \sigma(y))_\infty \leq 4g + 2$. So we get again a contradiction. Therefore we have again $\sigma(y) = y$ and so σ is the identity map.

(3) Similar to the case (2). □

The next corollary is an obvious consequence of the previous theorem.

Corollary 3.2.8. *Let $F|\mathbb{F}_q$ be a function field of genus g which admits some rational place. If $\sigma \in \operatorname{Aut}(F|\mathbb{F}_q)$ fixes a ϕ-place (P, ϕ_P) with $\deg P = n \geq 4g + 3$, then σ is the identity map.*

Finally, we give the theorem which connects automorphisms of a GAG-code $C(\Phi; G; n)$ with automorphisms of the underlying function field $F|\mathbb{F}_q$.

Theorem 3.2.9. *Let $F|\mathbb{F}_q$ be a function field, $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$ where the (P_i, ϕ_i)'s are N ϕ-places whose places are pairwise distinct and of the same degree $n > 1$. Let G be a divisor of $F|\mathbb{F}_q$ such that $\operatorname{supp} G \cap \{ P_1, P_2, \ldots, P_N \} = \emptyset$ and let $C(\Phi; G; n)$ be the* GAG*-code associated with Φ and G. Then*

(1) *Any automorphism* $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ *induces an* $n-$*automorphism of* $C(\Phi; G; n)$ *by*

$$\sigma(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) = (x(\sigma(P_1, \phi_1)), \ldots, x(\sigma(P_N, \phi_N)))$$

for every $x \in \mathcal{L}(G)$.

(2) $\mathrm{Aut}(C(\Phi; G; n))$ *admits a subgroup which is isomorphic to* $\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ *if* (1) *or* (2) *of* Theorem 3.2.7 *is satisfied.*

(3) *If* $G = rQ$, *where* Q *is a rational place and* $r \leq nN-1$, *and if* $2g+2 \leq nN$, *then* $C(\Phi; G; n)$ *admits an automorphism group which is isomorphic to* $\mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,Q}$.

Proof. (1) We have to prove that $(x(\sigma(P_1, \phi_1)), \ldots, x(\sigma(P_N, \phi_N))) \in C(\Phi; G; n)$ for any $x \in \mathcal{L}(G)$. Observe that if $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$, then $\sigma(G) \sim_\Phi G$, that is, there exists $u \in F$ such that $\sigma(G) = G+(u)$ and $u(P_i, \phi_i) = 1$ for every $i = 1, 2, \ldots, N$. But $\sigma(G) = G + (u)$ implies that the map $y \longmapsto uy$, from $\mathcal{L}(\sigma(G))$ to $\mathcal{L}(G)$, is an isomorphism. Hence if $x \in \mathcal{L}(G)$, $x = uw$ for some $w \in \mathcal{L}(\sigma(G))$. But $\mathcal{L}(\sigma(G)) = \sigma(\mathcal{L}(G))$ and so we have $w = \sigma(y)$ for some $y \in \mathcal{L}(G)$.

Therefore, if $c = (x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) \in C(\Phi; G; n)$, we get

$\sigma(c) = (x(\sigma(P_1), \phi_{P_1}\sigma^{-1}), \ldots, x(\sigma(P_N), \phi_{P_N}\sigma^{-1})) =$

$(u(\sigma(P_1), \phi_{P_1}\sigma^{-1})\sigma(y)(\sigma(P_1), \phi_{P_1}\sigma^{-1}), \ldots, u(\sigma(P_N), \phi_{P_N}\sigma^{-1})\sigma(y)(\sigma(P_N), \phi_{P_N}\sigma^{-1})) =$

$(\sigma(y)(\sigma(P_1), \phi_{P_1}\sigma^{-1}), \ldots, \sigma(y)(\sigma(P_N), \phi_{P_N}\sigma^{-1})) = (y(P_1, \phi_1), \ldots, y(P_N, \phi_N))$ where the last equality follows from $\sigma(y)(\sigma(P_i), \phi_{P_i}\sigma^{-1}) = \phi_{P_i}\sigma^{-1}(\sigma(y)(\sigma(P_i)))$ for any $i = 1, 2, \ldots, N$. Therefore, $\sigma(c) = (y(P_1, \phi_1), \ldots, y(P_N, \phi_N)) \in C(\Phi; G; n)$ since $y \in \mathcal{L}(G)$.

(2) Let $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ such that

$$\sigma(x(P_1, \phi_1), x(P_2, \phi_2), \ldots, x(P_N, \phi_N)) = (x(P_1, \phi_1), x(P_2, \phi_2), \ldots, x(P_N, \phi_N))$$

for any $x \in \mathcal{L}(G)$. Then

$$(x(\sigma(P_1, \phi_1)), \ldots, x(\sigma(P_N, \phi_N))) = (x(P_1, \phi_1), \ldots, x(P_N, \phi_N)),$$

that is, $x(\sigma(P_i, \phi_i)) = x(P_i, \phi_i)$ for any $i = 1, 2, \ldots, N$ and for any $x \in \mathcal{L}(G)$. Hence, $\sigma(P_i, \phi_i) = (P_i, \phi_i)$ for any $i = 1, 2, \ldots, N$ and so, by Theorem 3.2.7, σ is the identity map. Hence different elements of $\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ induce different automorphism of $C(\Phi; G; n)$ and so the thesis follows.
(3) By Lemma 3.2.2, $\mathrm{Aut}(F|\mathbb{F}_q, \Phi, G) = \mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,G} = \mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,Q}$ being $G = rQ \geq 0$ and $\deg G = r < nN$ by hypothesis. Suppose now σ induces the identity automorphism of $C(\Phi; G; n)$ and so it fixes each P_i for $i = 1, 2, \ldots, N$. Since σ fixes also Q (being $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,Q}$) and $N \geq \frac{2g+2}{n}$, by Theorem 3.2.7.(3), the thesis follows. □

From now on, we will always suppose N big enough, that is, we will suppose that one of the conditions (1) or (2) of Theorem 3.2.7 is satisfied. Let $H \simeq \mathrm{Aut}(F|\mathbb{F}_q, \Phi, G)$ be the automorphism group of $C(\Phi; G; n)$ given in (2) or (3) of Theorem 3.2.9. Clearly,

$$H = \{\, \pi_\sigma \mid \sigma \in \mathrm{Aut}(F|\mathbb{F}_q, \Phi, G) \,\}$$

where

$$\pi_\sigma(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) = (x(\sigma(P_1, \phi_1)), \ldots, x(\sigma(P_N, \phi_N))$$

for any $x \in \mathcal{L}(G)$. Note that if $x \in \mathcal{L}(G)$, since σ fixes G, we have $\sigma^{-1}(x) \in \mathcal{L}(G)$. Moreover, $x(\sigma(P_i, \phi_i)) = x(\sigma(P_i), \phi_i\sigma^{-1}) = \phi_i\sigma^{-1}(x(\sigma(P_i))) = \phi_i(\sigma^{-1}(x)(P_i)) = \sigma^{-1}(x)(P_i, \phi_i)$ for any $i = 1, 2, \ldots, N$. Hence

$$\pi_\sigma(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) = (\sigma^{-1}(x)(P_1, \phi_1), \ldots, \sigma^{-1}(x)(P_N, \phi_N)).$$

Let us define the automorphism group E of $C(\Phi; G; n)$ given by

$$E = \{\, (\pi_1, \pi_2, \ldots, \pi_N) \in (S_n)^N \mid \text{ for any } x \in \mathcal{L}(G) \text{ and}$$
$$\text{for any } i = 1, 2, \ldots, N, \pi_i(x(P_i, \phi_i)) = y(P_i, \phi_i) \text{ for some } y \in \mathcal{L}(G) \,\}.$$

We have the following proposition.

Proposition 3.2.10. *Let $F|\mathbb{F}_q$ be a function field, $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$ where the (P_i, ϕ_i)'s are N ϕ-places whose places are pairwise distinct and of the same degree $n > 1$. Let G be a divisor of $F|\mathbb{F}_q$ such that* $\operatorname{supp} G \cap \{\, P_1, P_2, \ldots, P_N \,\} = \emptyset$. *If* (2) *or* (3) *of* Theorem 3.2.9 *is satisfied, then the* GAG*-code $C(\Phi; G; n)$ admits an automorphism group which is isomorphic to the semidirect product HE of the group E by the group H.*

Proof. Let $\pi = (\pi_1, \pi_2, \ldots, \pi_N) \in E$, $\pi_\sigma \in H$ and suppose $\pi_\sigma = \pi \in E \cap H$. Consider the holomorphy ring

$$O_S := \bigcap_{i=1}^{N} O_{P_i}$$

associated with $S := \{\, P_1, P_2, \ldots, P_N \,\}$ (see [St1]). For any $x \in O_S$ we have

$$\pi_\sigma(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) = (\sigma^{-1}(x)(P_1, \phi_1), \ldots, \sigma^{-1}(x)(P_N, \phi_N))$$

and, from the other hand,

$$\pi(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) = (\pi_1(x(P_1, \phi_1)), \ldots, \pi_N(x(P_N, \phi_N))).$$

Hence, we have $\pi_i(x(P_i, \phi_i)) = \sigma^{-1}(x)(P_i, \phi_i)$ for any $i = 1, 2, \ldots, N$.

If x is also in P_i, then $x(P_i, \phi_i) = 0$, and, since π_i is $\mathbb{F}_q-$linear on $\mathbb{F}_q^n$, we have $\sigma^{-1}(x)(P_i, \phi_i) = \pi_i(x(P_i, \phi_i)) = 0$, that is, $\sigma^{-1}(x) \in P_i$ and therefore $x \in \sigma(P_i)$. Hence, $P_i \cap O_S \subseteq \sigma(P_i)$.

Moreover, $P_i \cap O_S \subseteq O_S = O_{\sigma(S)} = \bigcap_{i=1}^{N} O_{\sigma(P_i)} = \bigcap_{i=1}^{N} \sigma(O_{P_i}) = \sigma(\bigcap_{i=1}^{N} O_{P_i}) = \sigma(O_S)$

(note that $O_S = O_{\sigma(S)}$ since σ fixes the set S). Hence, $P_i \cap O_S \subseteq \sigma(P_i) \cap \sigma(O_S) = \sigma(P_i \cap O_S)$ and, since the ideal $P_i \cap O_S$ is maximal in O_S, we have

$$P_i \cap O_S = \sigma(P_i \cap O_S). \tag{3.2.5}$$

There is a bijection from S to the set of maximal ideals of O_S, given by $P \mapsto P \cap O_S$ (see [St1]). Thus $P_i \neq \sigma(P_i)$ implies $P_i \cap O_S \neq \sigma(P_i) \cap O_S$. But $\sigma(P_i) \cap O_S = \sigma(P_i) \cap \sigma(O_S) = \sigma(P_i \cap O_S)$ and so $P_i \cap O_S \neq \sigma(P_i \cap O_S)$ which is a contradiction with the (3.2.5).

Hence, for any $i = 1, 2, \ldots, N$, we have $\sigma(P_i) = P_i$ and so $\sigma(P_i, \phi_i) = (P_i, \phi_i)$ since $\sigma(\Phi) = \Phi$. Now, by Theorem 3.2.7, we have σ is the identity map and so $\pi_\sigma = id$. Therefore $H \cap E = \{1\}$.

Now we have to prove that H normalizes E, that is, that for any $\pi_\sigma \in H$ and for any $\pi \in E$, we have $\pi_\sigma^{-1}\pi\pi_\sigma \in E$. We note that if $\pi = (\pi_1, \pi_2, \ldots, \pi_N) \in E$ and if we set $\overline{\pi}_i = (1, \ldots, 1, \pi_i, 1, \ldots, 1)$, for $i = 1, 2, \ldots, N$, then $\pi = \overline{\pi}_1\overline{\pi}_2 \cdots \overline{\pi}_N$ is a product of disjoint permutations of S_{nN} and (see for instance [Pas]) $\pi_\sigma^{-1}\pi\pi_\sigma$ has the same disjoint permutation structure as π. In fact $\pi_\sigma^{-1}\pi\pi_\sigma = \overline{\pi}_{\pi_\sigma^{-1}(1)}\overline{\pi}_{\pi_\sigma^{-1}(2)} \cdot \ldots \cdot \overline{\pi}_{\pi_\sigma^{-1}(N)} = (\pi_{\pi_\sigma^{-1}(1)}, \pi_{\pi_\sigma^{-1}(2)}, \ldots, \pi_{\pi_\sigma^{-1}(N)}) \in (S_n)^N$.

Now, for any $x \in \mathcal{L}(G)$ we have

$$\begin{aligned} \pi\pi_\sigma(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) &= \pi(\sigma^{-1}(x)(P_1, \phi_1), \ldots, \sigma^{-1}(x)(P_N, \phi_N)) \\ &= (y(P_1, \phi_1), \ldots, y(P_N, \phi_N)) \end{aligned}$$

for some $y \in \mathcal{L}(G)$ since $\pi \in E$. Therefore

$$\begin{aligned} \pi_\sigma^{-1}\pi\pi_\sigma(x(P_1, \phi_1), \ldots, x(P_N, \phi_N)) &= \pi_\sigma^{-1}(y(P_1, \phi_1), \ldots, y(P_N, \phi_N)) \\ &= (\sigma^{-1}(y)(P_1, \phi_1), \ldots, \sigma^{-1}(y)(P_N, \phi_N)) \end{aligned}$$

where $\sigma^{-1}(y) \in \mathcal{L}(G)$. So $\pi_\sigma^{-1}\pi\pi_\sigma \in E$ and we have that H normalizes E. □

Now we give an example of GAG-code, over a rational function field, in which the

automorphism groups E and H are complectly determined.

Example 1. Let $\mathbb{F}_7(x)|\mathbb{F}_7$ be a rational function field. Let $\mathbb{F}_{7^5} = \mathbb{F}_7(\alpha)$ where α is a root of the irreducible polynomial $4 + x + 5x^2 + 4x^4 + x^5$. We can write any element $\sum_{i=0}^{4} a_i\alpha^i \in \mathbb{F}_{7^5}$ as $(a_0, a_1, a_2, a_3, a_4) \in \mathbb{F}_7^5$.

Let us consider the divisor $G = 2P_\infty$ and the $\phi-$divisor $\Phi = \sum_{i=1}^{6}(P_i, \phi_i)$ where $P_1 = P_{4+x+5x^2+4x^4+x^5}$, $P_2 = P_{2+2x+5x^2+x^4+x^5}$, $P_3 = P_{6+4x+2x^2+5x^4+x^5}$, $P_4 = P_{1+4x+5x^2+2x^4+x^5}$, $P_5 = P_{5+2x+2x^2+6x^4+x^5}$ and $P_6 = P_{3+x+2x^2+3x^4+x^5}$ are $N = 6$ places of degree $n = 5$ and, for $1 \leq i \leq 6$,

$$\phi_i : \quad F_{P_i} \quad \longrightarrow \quad \mathbb{F}_{7^5}$$

is defined by $\phi_i(\frac{u(x)}{v(x)}(P_i)) := \frac{u(i\alpha)}{v(i\alpha)}$ for any $\frac{u(x)}{v(x)}(P_i) \in F_{P_i}$.

Clearly,

$$\mathcal{L}(G) = \{\, a + bx + cx^2 \,|\, a, b, c \in \mathbb{F}_7 \,\}.$$

The GAG-code $C(\Phi; G; n)$ is a $7-$ary $[30, 3, d]$ code with $6 \leq d \leq 28$ (see Corollary 3.1.2).

We have $\mathrm{Aut}(F|\mathbb{F}_7, \Phi, G) = \langle\, \sigma \,\rangle$ where $\sigma(x) = 3x$ (see Proposition 4.1.4). Since $\sigma(P_1, \phi_1) = (P_3, \phi_3)$, $\sigma(P_2, \phi_2) = (P_6, \phi_6)$, $\sigma(P_3, \phi_3) = (P_2, \phi_2)$, $\sigma(P_4, \phi_4) = (P_5, \phi_5)$, $\sigma(P_5, \phi_5) = (P_1, \phi_1)$ and $\sigma(P_6, \phi_6) = (P_4, \phi_4)$, we have that $\pi_\sigma = (132645)$. So the automorphism group H is

$$H = \{\, id, (13265), (124)(365), (16)(25)(34), (142)(356), (154623) \,\} \simeq \mathbb{Z}_6.$$

The automorphism group E contains the following group of order 64

$$N = \{(\pi_1, \pi_2, \ldots, \pi_6) \in (S_5)^6 \,|\, \pi_i = id \text{ or } \pi_i = (45) \text{ for any } i = 1, 2, \ldots, 6\,\}.$$

In fact, if $(\pi_1, \pi_2, \ldots, \pi_6) \in N$, then for any $a + bx + cx^2 \in \mathcal{L}(G)$ we have $\pi_i((a + bx + cx^2)(P_i, \phi_i)) = \pi_i(a, ib, i^2c, 0, 0) = (a, ib, i^2c, 0, 0) = (a + bx + cx^2)(P_i, \phi_i)$ and so for

any $a+bx+cx^2 \in \mathcal{L}(G)$ we can find $y = a+bx+cx^2 \in \mathcal{L}(G)$ such that

$$\pi_i((a+bx+cx^2)(P_i,\phi_i)) = y(P_i,\phi_i)$$

for any $i = 1,2,\ldots,6$. Thus $(\pi_1,\pi_2,\ldots,\pi_6) \in E$. With an exhaustive research, it is also possible to prove that no other element of $(S_5)^6$ is in E and so

$$E = \{(\pi_1,\pi_2,\ldots,\pi_6) \in (S_5)^6 \,|\, \pi_i = id \text{ or } \pi_i = (45) \text{ for any } i = 1,2,\ldots,6\,\}.$$

3.2.1 The Rational case

We want to prove that, in some cases, the $n-$automorphism group of a GAG-code $C(\Phi;G;n)$ is equal to the stabilizer of Φ and G in $\mathrm{Aut}(F|\mathbb{F}_q)$. In order to do this, we will use the same idea used in Section 2.2.2 and so we will extend on $\phi-$places, some results proved for places.

The next results hold for any function field $F|\mathbb{F}_q$ of genus g.

Lemma 3.2.11. *Let $u,v \in \mathcal{L}(G)$ for some divisor $G = G_0 - G_1$ with $G_0, G_1 \geq 0$. Let $\deg G_0 < nN$. Let (P_i,ϕ_i), for $i = 1,2,\ldots,N$, be N $\phi-$places with P_i pairwise distinct places of the same degree n, which are not in the support of G_0. If $u(P_i,\phi_i) = v(P_i,\phi_i)$ for any i, then $u = v$.*

Proof. Suppose $u \neq v$. Since $u - v \in \mathcal{L}(G)$, then $(u-v) = (u-v)_0 - (u-v)_\infty \geq -G_0 + G_1$, which means $(u-v)_\infty \leq G_0$. Hence, $\deg(u-v)_\infty \leq \deg G_0 < nN$. On the other hand, if $u(P_i,\phi_i) = v(P_i,\phi_i)$ it follows that $\phi_i(u-v+P_i) = (u-v)(P_i,\phi_i) = 0$. But ϕ_i is a field isomorphism and so $u - v \in P_i$ for every $i = 1,2,\ldots,N$. Hence $u-v$ has at least N zeroes and so $\deg(u-v)_\infty \geq nN$ which contradicts the above consideration. □

Now we define an $\mathbb{F}_q-$liner map which will be useful to associate to each $n-$automorphism of a GAG-code an element of $\mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,G}$.
Let $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$ and $\Psi = \sum_{i=1}^{N}(P'_i, \psi_i)$ be two $\phi-$divisors with $\deg P_i = \deg P'_i = n > 1$ for any $i = 1, 2, \ldots, N$. Let G be a divisor of degree $\deg G < nN$ such that $\mathrm{supp}\, G \cap \{P_1, P_2, \ldots, P_N\} = \mathrm{supp}\, G \cap \{P'_1, P'_2, \ldots, P'_N\} = \emptyset$. Consider the linear isomorphisms ev_Φ and ev_Ψ as in (3.1.2). If $C(\Phi; G; n) = C(\Psi; G; n)$ we can define a linear isomorphism $\lambda : \mathcal{L}(G) \to \mathcal{L}(G)$ by

$$\lambda := ev_\Psi^{-1} \circ ev_\Phi. \tag{3.2.6}$$

Note that, for all $z \in \mathcal{L}(G)$, we have that $\lambda(z) \in \mathcal{L}(G)$ is the only element in $\mathcal{L}(G)$ such that

$$\lambda(z)(P'_i, \psi_i) = z(P_i, \phi_i) \quad \text{for all } i = 1, 2, \ldots N.$$

In fact, $\lambda(z) = ev_\Psi^{-1} \circ ev_\Phi(z)$ if and only if $ev_\Psi(\lambda(z)) = ev_\Phi(z)$ if and only if $(\lambda(z)(P'_1, \psi_1), \ldots, \lambda(z)(P'_N, \psi_N)) = (z(P_1, \phi_1), \ldots, z(P_N, \phi_N))$.

Also in the case of GAG-codes, the map λ has similar properties with the ones of a field automorphism.

Lemma 3.2.12. *Let G be a divisor of $F|\mathbb{F}_q$.*

(1) *If $\deg G < n$ and $1 \in \mathcal{L}(G)$, then $\lambda(1) = 1$.*

(2) *If $G > 0$ with $\deg G < \frac{n}{2}$ and*

   (i) *if $f, g, fg \in \mathcal{L}(G)$, then $\lambda(fg) = \lambda(f)\lambda(g)$.*

   (ii) *if $f, f^k \in \mathcal{L}(G)$ for some $k \geq 2$, then $\lambda(f^k) = \lambda(f)^k$ and $\deg(\lambda(f)_\infty) \leq \frac{\deg G}{k}$.*

Proof. (1) Since $\phi_P : F_P \to \mathbb{F}_{q^n}$ is a field isomorphism, $\phi_P(1+P) = 1$ for all $P \in \mathbb{P}_F$. So $1(P'_i, \psi_i) = 1 = 1(P_i, \phi_i) = \lambda(1)(P'_i, \psi_i)$ for any $i = 1, 2, ..., N$ and so $ev_\Psi(1) = ev_\Psi(\lambda(1))$ from which follows that $\lambda(1) = 1$, since ev_Ψ is injective.

(2) If $f, g, fg \in \mathcal{L}(G)$, then $\lambda(fg), \lambda(f), \lambda(g) \in \mathcal{L}(G)$ and so, a fortiori, they will be in $\mathcal{L}(2G)$. Moreover, $(\lambda(f)\lambda(g)) = (\lambda(f)) + (\lambda(g)) \geq -2G$ and so $\lambda(f)\lambda(g) \in \mathcal{L}(2G)$. But $(\lambda(f)\lambda(g))(P'_i, \psi_i) = \lambda(f)(P'_i, \psi_i)\lambda(g)(P'_i, \psi_i) = f(P_i, \phi_i)g(P_i, \phi_i) = fg(P_i, \phi_i) = \lambda(fg)(P'_i, \psi_i)$. So, since $G > 0$ and $2(\deg G) < nN$, we have that $\lambda(fg) = \lambda(f)\lambda(g)$ by Lemma 3.2.11.

If $f, f^k \in \mathcal{L}(G)$, then $v_P(f) \geq -v_P(G)$ and $v_P(f^k) \geq -v_P(G)$ for each $P \in \mathbb{P}_F$. Then, for $i = 2, 3, \ldots, k-1$, $v_P(f^i) \geq -v_P(G)$, that is, $f^i \in \mathcal{L}(G)$. We have just seen that $\lambda(f^2) = \lambda(f)^2$ and so on, we get $\lambda(f^k) = \lambda(f)^k$. Moreover, since $\lambda(f)^k \in \mathcal{L}(G)$, $(\lambda(f)^k) \geq -G$ from which follows that $G \geq (\lambda(f)^k)_\infty$ and so $\deg G \geq k \deg((\lambda(f))_\infty)$, that is, $\deg(\lambda(f)_\infty) \leq \frac{\deg G}{k}$. □

The next lemma is a generalization of the fact that for a rational place the values $x(P)$ and $y(P)$ uniquely determine P.

Lemma 3.2.13. *Let $F = \mathbb{F}_q(x, y)$ be a function field and let (P_1, ϕ_1) and (P_2, ϕ_2) be two $\phi-$places such that x and y are regular on P_1 and P_2. If $x(P_1, \phi_1) = x(P_2, \phi_2)$ and $y(P_1, \phi_1) = y(P_2, \phi_2)$, then $(P_1, \phi_1) = (P_2, \phi_2)$.*

Proof. For each $z = \frac{f(x,y)}{g(x,y)} \in F$, if z is regular to P_2, then $\phi_2(z(P_2)) = \phi_2(\frac{f(x(P_2),y(P_2))}{g(x(P_2),y(P_2))})$ $= \frac{f(x(P_2,\phi_2),y(P_2,\phi_2))}{g(x(P_2,\phi_2),y(P_2,\phi_2))} = \frac{f(x(P_1,\phi_1),y(P_1,\phi_1))}{g(x(P_1,\phi_1),y(P_1,\phi_1))} = \phi_1(\frac{f(x(P_1),y(P_1))}{g(x(P_1),y(P_1))}) = \phi_1(z(P_1))$, that is, $\phi_2(z(P_2)) = \phi_1(z(P_1))$. Therefore, $z \in P_2$ if and only if $\phi_2(z(P_2)) = 0$ if and only if $\phi_1(z(P_1)) = 0$ and this if and only if $z \in P_1$. Hence $P_1 = P_2$.

We have only to prove that $\phi_1 = \phi_2$. For any $z(P_2) \in F_{P_2}$, we have $\phi_2(z(P_2)) = \phi_1(z(P_2))$ and so ϕ_1 and ϕ_2 act in the same way on F_{P_2}. Necessarily, $\phi_1 = \phi_2$. □

The following proposition links λ to an automorphism of the function field. With it, we will show how λ can be used to associate to an automorphism of the code, an automorphism of the stabilizer.

Proposition 3.2.14. *Let $F = \mathbb{F}_q(x, y)$ be a function field and $\sigma \in \mathrm{Aut}(F|\mathbb{F}_q)$. Suppose $C(\Phi; G; n) = C(\Psi; G; n)$ where*

$$\Phi = \sum_{i=1}^{N}(P_i, \phi_i) \quad \textit{and} \quad \Psi = \sum_{i=1}^{N}(P'_i, \psi_i).$$

Suppose the support of G is disjoint from the supports of $D := \sum_{i=1}^{N} P_i$ and $D' := \sum_{i=1}^{N} P'_i$. Moreover, let λ be the map described in (3.2.6) and $x, y \in \mathcal{L}(G)$. If $\sigma(G) = G$ and $\sigma|_{\mathcal{L}(G)} = \lambda$, then $\sigma(P_i, \phi_i) = (P'_i, \psi_i)$ for each $i = 1, 2, \ldots, N$.

Proof. By hypothesis, $x \in \mathcal{L}(G)$ therefore there exists $f \in \mathcal{L}(G)$ such that $x = \lambda(f)$ and so $x(P'_i, \psi_i) = \lambda(f)(P'_i, \psi_i) = f(P_i, \phi_i) = \phi_i(f(P_i)) = \phi_i\sigma^{-1}(\sigma(f)(\sigma(P_i))) = \sigma(f)(\sigma(P_i), \phi_i\sigma^{-1}) = \lambda(f)(\sigma(P_i), \phi_i\sigma^{-1}) = x(\sigma(P_i), \phi_i\sigma^{-1})$. Similarly, $y(P'_i, \psi_i) = y(\sigma(P_i), \phi_i\sigma^{-1})$. By the above lemma, it follows that $(P'_i, \psi_i) = (\sigma(P_i), \phi_i\sigma^{-1})$, that is, $(P'_i, \psi_i) = \sigma(P_i, \phi_i)$ for each $i = 1, 2, \ldots, N$. □

From now on we suppose that $F|\mathbb{F}_q$ is a rational function field.

Lemma 3.2.15. *Let $\mathbb{F}_q(x)|\mathbb{F}_q$ be a rational function field and r a non negative integer. For $i = 1, 2, \ldots, m$, let P_{α_i} be m rational places and r_i positive integers. Then*

$$B = \{\, x^j \,|\, 0 \le j \le r \,\} \cup \{\, \frac{1}{(x-\alpha_i)^j} \,|\, 1 \le j \le r_i \textit{ and } 1 \le i \le m \,\}$$

is a base for $\mathcal{L}(rP_\infty + \sum_{i=1}^{m} r_i P_{\alpha_i})$.

Proof. $x^i \in \mathcal{L}(rP_\infty + \sum_{i=1}^{m} r_i P_{\alpha_i})$ if and only if $(x^i) \ge -rP_\infty - \sum_{i=1}^{m} r_i P_{\alpha_i}$. But $(x^i) = i(x) = i(x)_0 - i(x)_\infty = iP_0 - iP_\infty$. Therefore $(x^i) \ge -rP_\infty - \sum_{i=1}^{m} r_i P_{\alpha_i}$ if and

only if $0 \leq i \leq r$.

For each $i = 1, 2, \ldots, m$, $\frac{1}{(x-\alpha_i)^j} \in \mathcal{L}(rP_\infty + \sum_{i=1}^m r_i P_{\alpha_i})$ if and only if $\left(\frac{1}{(x-\alpha_i)^j}\right) \geq -rP_\infty - \sum_{i=1}^m r_i P_{\alpha_i}$. But $\left(\frac{1}{(x-\alpha_i)^j}\right) = -j(x-\alpha_i) = -j(x-\alpha_i)_0 + j(x-\alpha_i)_\infty = -jP_{\alpha_i} + jP_\infty$. Therefore, $\left(\frac{1}{(x-\alpha_i)^j}\right) \geq -rP_\infty - \sum_{i=1}^m r_i P_{\alpha_i}$ if and only if $1 \leq j \leq r_i$. Hence, $B \subseteq \mathcal{L}(rP_\infty + \sum_{i=1}^m r_i P_{\alpha_i})$.

With the "Strict Triangle Inequality" it is also possible to prove that the elements of B are $\mathbb{F}_q-$linearly independent and, since $\dim(\mathcal{L}(rP_\infty + \sum_{i=1}^m r_i P_{\alpha_i})) = \deg(rP_\infty + \sum_{i=1}^m r_i P_{\alpha_i}) + 1 = r + \sum_i^m r_i + 1 = |B|$, then the thesis follows. □

Theorem 3.2.16. *Let $\mathbb{F}_q(x)|\mathbb{F}_q$ be a rational function field. Let $\Phi = \sum_{i=1}^N (P_i, \phi_i)$ be a $\phi-$divisor with P_i pairwise distinct places all of the same degree n. Let*

$$G = rP_\infty + \sum_{i=1}^m r_i P_{\alpha_i}$$

with $r > 0$, $r_i \geq 0$ and P_{α_i} rational places. Let $C(\Phi; G; n)$ be the GAG*-code associated with Φ and G. If $\deg G < \frac{nN}{2}$ and $nN \geq 3$, then*

$$\mathcal{H}(\Phi; G; n) \cong \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G}.$$

Proof. By Theorem 3.2.9, $\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G}$ is isomorphic to a subgroup of $\mathcal{H}(\Phi; G; n)$. We prove that such subgroup is actually isomorphic to the whole group $\mathcal{H}(\Phi; G; n)$. Consider $\pi \in \mathcal{H}(\Phi; G; n)$. By Lemma (3.2.1), we know that $C(\Phi; G; n) = C(\pi\Phi; G; n)$ and so we can consider the corresponding map $\lambda = \lambda_\pi$ (see (3.2.6)). By the above lemma, $B = \{\, x^j \,|\, 0 \leq j \leq r \,\} \cup \{\, \frac{1}{(x-\alpha_i)^j} \,|\, 1 \leq j \leq r_i \text{ and } 1 \leq i \leq m \,\}$ is a base for $\mathcal{L}(G)$ and, by Lemma 3.2.12, we have that

$$\lambda(x^j) = (\lambda(x))^j \text{ for each } j = 0, 1, \ldots, r.$$

Moreover, since $1 = \lambda(1) = \lambda\left(\frac{1}{x-\alpha_i}(x-\alpha_i)\right) = \lambda(\frac{1}{x-\alpha_i})\lambda(x-\alpha_i)$ and so $\lambda(\frac{1}{x-\alpha_i}) = \frac{1}{\lambda(x-\alpha_i)} = \frac{1}{\lambda(x)-\alpha_i}$, it follows also that

$$\lambda\left(\left(\frac{1}{x-\alpha_i}\right)^j\right) = \left(\frac{1}{\lambda(x)-\alpha_i}\right)^j$$

for every $1 \leq j \leq r_i$.

Since every element $h(x) \in \mathcal{L}(G)$ can be written as linear combination of the elements of B, we have shown that $\lambda(h(x)) = h(\lambda(x))$.

Hence there exists an $\mathbb{F}_q-$endomorphism

$$\begin{array}{rccc} \widetilde{\lambda}: & \mathbb{F}_q(x) & \longrightarrow & \mathbb{F}_q(x) \\ & h(x) & \mapsto & h(\lambda(x)) \end{array}$$

of the function field $\mathbb{F}_q(x)|\mathbb{F}_q$ such that the restriction of $\widetilde{\lambda}$ to $\mathcal{L}(G)$ coincides with λ and so, since x is in the image of λ, $\widetilde{\lambda}$ is an automorphism of $\mathbb{F}_q(x)|\mathbb{F}_q$. By Lemma 2.2.6, $\widetilde{\lambda}(G) = G$ and so it is possible to apply also Proposition 3.2.14 from which follows that $\widetilde{\lambda}(P_i, \phi_i) = (P_{\pi(i)}, \phi_{\pi(i)})$, that is, $\widetilde{\lambda}(\Phi) = \Phi$. Finally, we have associated to each $\pi \in \mathcal{H}(\Phi; G; n)$ an element $\widetilde{\lambda} \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G}$ and so the claim follows. □

Note that, by Point (3) of Theorem 3.2.9, if $G = rP_\infty$ the hypothesis $nN \geq 3$ is not necessary.

3.2.2 The Hyperelliptic case

Let $F|\mathbb{F}_q$ be a hyperelliptic function field of genus g. We regard an elliptic function field as a special case of a hyperelliptic function field (see [St1]). For simplicity, we suppose $\mathrm{char}\,\mathbb{F}_q \neq 2$ even if, with opportune modifications, similar results can also be proved for $\mathrm{char}\,\mathbb{F}_q = 2$ case. We will use the same notation used in Section 2.2.2.

Theorem 3.2.17. *Let $J \subseteq H(\mathbb{F}_q) \setminus \operatorname{supp}((x)_\infty)$ and let*

$$G = n_\infty D_\infty + \sum_{Q \in J} n_Q Q$$

be a divisor, where $n_\infty \geq \begin{cases} 2g+2 & \text{if } d \equiv 1 \pmod 2 \\ g+1 & \text{if } d \equiv 0 \pmod 2 \end{cases}$ and $n_Q \geq 1$ for each $Q \in J$. Let $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ be a $\phi-$divisor with P_i distinct places all of the same degree $n > 1$. If $\deg G < \frac{nN}{2}$ and one of the following conditions is satisfied:

(1) *$nN > 16(g+1)^2 + n$;*

(2) *$F|\mathbb{F}_q$ has some rational place and $nN \geq 4g+3$;*

then

$$\mathcal{H}(\Phi; G; n)) \cong \operatorname{Aut}(F|\mathbb{F}_q)_{\Phi,G}.$$

Proof. We proceed as in the proof of Theorem 3.2.16. So, consider $\pi \in \mathcal{H}(\Phi; G; n)$ and the corresponding map $\lambda = \lambda_\pi$. A base of $\mathcal{L}(G)$ is as in Proposition 2.2.14. By Lemma 3.2.12, it is possible to prove that

$$\lambda(x^\alpha y^\beta) = \lambda(x)^\alpha \lambda(y)^\beta, \quad \text{for } x^\alpha y^\beta \in \mathcal{L}(G).$$

Moreover, since $1 = \lambda(1) = \lambda\left(\frac{1}{x-x_Q}\right)\lambda(x - x_Q) = \lambda\left(\frac{1}{x-x_Q}\right)(\lambda(x) - x_Q)$ we have $\lambda\left(\frac{1}{x-x_Q}\right) = \frac{1}{\lambda(x)-x_Q}$ and $\lambda\left(\frac{y}{x-x_Q}\right) = \lambda(y)\lambda\left(\frac{1}{x-x_Q}\right) = \frac{\lambda(y)}{\lambda(x)-x_Q}$. Hence

$$\lambda\left(\left(\frac{1}{x-x_Q}\right)^\alpha \left(\frac{y}{x-x_Q}\right)^\beta\right) = \left(\frac{1}{\lambda(x)-x_Q}\right)^\alpha \left(\frac{\lambda(y)}{\lambda(x)-x_Q}\right)^\beta$$

for $2\alpha + \beta \leq n_Q$, $\alpha \geq 0$, $\beta \in \{0, 1\}$ and $Q \in J \cap H_r(\mathbb{F}_q)$.

Finally, since $(x-x_Q)^i, y-p_i(x) \in \mathcal{L}(G)$ if $Q \in \operatorname{supp}(G) \cap H_s(\mathbb{F}_q)$, $1 \leq i \leq \min\{n_Q, g+1\}$ and $\deg p_i(x) \leq i-1$, it makes sense considering $\lambda((x-x_Q)^i) = (\lambda(x) - x_Q)^i$ and

$\lambda(y - p_i(x)) = \lambda(y) - p_i(\lambda(x))$. Therefore, $\lambda(g_{iQ}) = \frac{\lambda(y-p_i(x))}{\lambda((x-x_Q)^i)} = \frac{\lambda(y)-p_i(\lambda(x))}{(\lambda(y)-x_Q)^i}$ and so

$$\lambda((g_{mQ})^\alpha(g_{\beta Q})) = \left(\frac{\lambda(y) - p_m(\lambda(x))}{(\lambda(x) - x_Q)^i}\right)^\alpha \frac{\lambda(y) - p_\beta(\lambda(x))}{(\lambda(x) - x_Q)^i}$$

for $m\alpha + \beta \leq n_Q$, $\alpha \geq 0$, $0 \leq \beta < m$ and $Q \in J \cap H_s(\mathbb{F}_q)$.

Since every element $h(x, y) \in \mathcal{L}(G)$ can be written as linear combination of the above elements, we proved that $\lambda(h(x, y)) = h(\lambda(x), \lambda(y))$. We will prove now that $\lambda(x)$ and $\lambda(y)$ satisfy the relation

$$\lambda(y)^2 - f(\lambda(x)) = 0.$$

Note that x and $x^{[\frac{d+1}{2}]}$ belong to $\mathcal{L}(G)$ and so, by Lemma 3.2.12, we have $\deg(\lambda(x))_\infty \leq \frac{t}{g+1} \leq \frac{2t}{d}$, that is, $\deg((\lambda(x)^d)_\infty) \leq 2t < nN$ from which follows, since $\deg f(x) = d$, that $\deg(f(\lambda(x)))_\infty \leq 2t$. Moreover, since $\lambda(y) \in \mathcal{L}(G)$ we have $\deg(\lambda(y)^2)_\infty = 2\deg(\lambda(y))_\infty \leq 2t$. So we have that $\lambda(y)^2, f(\lambda(x)) \in \mathcal{L}(2G)$. We also remark that $\lambda(y)^2(P, \phi) = f(\lambda(x))(P, \phi)$ for each $(P, \phi) \in \operatorname{supp}\Phi$. In fact,

$\lambda(y)^2(P_{\pi(i)}, \phi_{\pi(i)}) = \phi_{\pi(i)}(\lambda(y)^2(P_{\pi(i)})) = \phi_{\pi(i)}((\lambda(y)(P_{\pi(i)}))^2) = (\phi_{\pi(i)}(\lambda(y)(P_{\pi(i)})))^2$

$= (\lambda(y)(P_{\pi(i)}, \phi_{\pi(i)}))^2 = (y(P_i, \phi_i))^2 = y^2(P_i, \phi_i) = f(x)(P_i, \phi_i) = \phi_i(f(x)(P_i))$

$= \phi_i(f(x(P_i))) = f(\phi_i(x(P_i))) = f(x(P_i, \phi_i)) = f(\lambda(x)(P_{\pi(i)}, \phi_{\pi(i)}))$

$= f(\phi_{\pi(i)}(\lambda(x)(P_{\pi(i)}))) = \phi_{\pi(i)}(f(\lambda(x)(P_{\pi(i)}))) = \phi_{\pi(i)}(f(\lambda(x))(P_{\pi(i)}))$

$= f(\lambda(x))(P_{\pi(i)}, \phi_{\pi(i)})$.

Then, since $\deg 2G < nN$, by Lemma 3.2.11, we have $\lambda(y)^2 = f(\lambda(x))$. Hence, proceeding as in the proof of Theorem 3.2.16 the claim follows. □

Chapter 4

Applications

In this chapter we explicitly construct the $n-$automorphism group for specific one point GAG-codes, in the rational and hyperelliptic cases (the elliptic case is considered as a special case of the hyperelliptic case). Moreover, we calculate some examples of q-ary linear codes for various values of q. These examples show that it is possible to construct GAG-codes with a nontrivial $n-$automorphism group.

4.1 The Rational case

Let $\mathbb{F}_q(x)|\mathbb{F}_q$ be a rational function field. Let $P = P_{p(x)}$ be a place of degree $n \geqslant 1$ (where $p(x)$ is a monic irreducible polynomial of degree n). Let $\alpha \in \overline{\mathbb{F}_q}$ be a fixed root of $p(x)$ (here $\overline{\mathbb{F}_q}$ denotes the algebraic closure of the finite field $\mathbb{F}_q$). It is well-known (see for instance [L-N]) that $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ are exactly the n roots of $p(x)$. Therefore, one root of the polynomial $p(x)$ identifies $p(x)$ uniquely and so, $P_{p(x)}$ can be written as $P_{[\alpha]}$. With abuse of notation we will also indicate P_∞ with $P_{[\infty]}$ and we will call the $\phi-$place $(P_{[\infty]}, id)$ the infinity $\phi-$place of $\mathbb{F}_q(x)|\mathbb{F}_q$.

Let $F_P = F_{P_{p(x)}}$ be the residue class field of the place P. There are exactly n

F_q-isomorphisms from F_P to the field $\mathbb{F}_{q^n}$. In fact, let $\phi_\alpha : F_P \to \mathbb{F}_{q^n}$ be defined as it follows: for all $z(P) = \frac{u(x)}{v(x)}(P) \in F_P$

$$\phi_\alpha(z(P)) := \frac{u(\alpha)}{v(\alpha)}.$$

Clearly, ϕ_α is a field $\mathbb{F}_q-$isomorphism and the n $\mathbb{F}_q-$isomorphisms from F_P to $\mathbb{F}_{q^n}$ are the following

$$\phi_\alpha^{(i)} := \rho^i \phi_\alpha \quad \text{for } i = 0, 1, \ldots, n-1$$

where ρ is the Frobenius automorphism of $\mathbb{F}_{q^n}$ defined by

$$\begin{array}{rccc} \rho: & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & a & \mapsto & a^q. \end{array}$$

Therefore, if (P, ϕ) is a $\phi-$place different to the infinity place, then $(P, \phi) = (P_{[\alpha]}, \phi_\alpha)$ for some $\alpha \in \mathbb{F}_{q^n}$ and $i \in \{\, 0, 1, \ldots, n-1 \,\}$ where $n = \deg P$.
Since $\phi_\alpha^{(i)}(z(P)) = \frac{u(\alpha^{q^i})}{v(\alpha^{q^i})}$, we have $\phi_\alpha^{(i)} = \phi_{\alpha^{q^i}}$ and so $(P_{[\alpha]}, \phi_\alpha^{(i)}) = (P_{[\alpha^{q^i}]}, \phi_{\alpha^{q^i}})$. This means that, if we choose a root of the polynomial properly, then we can always suppose a $\phi-$place to be of the type $(P_{[\alpha]}, \phi_\alpha)$.

Proposition 4.1.1. *If $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ are distinct elements of $\mathbb{F}_{q^n}$, then*

(1) $q(x) = (x-\alpha)(x-\alpha^q)(x-\alpha^{q^2})\cdots(x-\alpha^{q^{n-1}}) \in \mathbb{F}_q[x]$;

(2) $q(x)$ *is irreducible in* $\mathbb{F}_q[x]$;

(3) $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha^{q^i})$ *for each* $0 \le i \le n-1$.

Proof. For $n = 1$ the proposition is trivial. If $n > 1$ we can write $q(x) = x^n - (\alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{n-1}})x^{n-1} + (\sum_{0 \le i_1 < i_2 \le n-1} \alpha^{q^{i_1}} \alpha^{q^{i_2}})x^{n-2} + \ldots + (-1)^n(\alpha\alpha^q\alpha^{q^2}\cdots\alpha^{q^{n-1}}) =$

$x^n + \sum_{k=1}^{n}(-1)^k(\sum_{0\le i_1<i_2<\ldots<i_k\le n-1}\alpha^{q^{i_1}}\alpha^{q^{i_2}}\cdots\alpha^{q^{i_k}})x^{n-k}$. So, $q(x)\in\mathbb{F}_q[x]$ if

$$a_k = \sum_{0\le i_1<i_2<\ldots<i_k\le n-1}\alpha^{q^{i_1}}\alpha^{q^{i_2}}\cdots\alpha^{q^{i_k}} \in \mathbb{F}_q \tag{4.1.1}$$

for any $k = 1, 2, \ldots, n$.

We recall that $\mathbb{F}_{q^n}|\mathbb{F}_q$ is a Galois extension and $Gal(\mathbb{F}_{q^n}|\mathbb{F}_q) = \{1, \rho, \rho^2, \ldots, \rho^{n-1}\}$ where ρ is the Frobenius automorphism. So, it is enough to prove that a_k is fixed by every element of $Gal(\mathbb{F}_{q^n}|\mathbb{F}_q)$. In fact, for any $i = 0, 1, \ldots, n-1$

$$\begin{aligned}\rho^i(a_k) &= \rho^i(\textstyle\sum_{0\le i_1<i_2<\ldots<i_k\le n-1}\alpha^{q^{i_1}}\alpha^{q^{i_2}}\cdots\alpha^{q^{i_k}})\\ &= \rho^i(\textstyle\sum_{0\le i_1<i_2<\ldots<i_k\le n-1}\rho^{i_1}(\alpha)\rho^{i_2}(\alpha)\cdots\rho^{i_k}(\alpha))\\ &= \textstyle\sum_{0\le i_1<i_2<\ldots<i_k\le n-1}\rho^i\rho^{i_1}(\alpha)\rho^i\rho^{i_2}(\alpha)\cdots\rho^i\rho^{i_k}(\alpha)\end{aligned}$$

and so, up to permutation of the factors and of the addends,

$$\rho^i(a_k) = \textstyle\sum_{0\le i_1<i_2<\ldots<i_k\le n-1}\rho^{i_1}(\alpha)\rho^{i_2}(\alpha)\cdots\rho^{i_k}(\alpha) = a_k.$$

We have also that $q(x)$ is irreducible. In fact, if we suppose that $q(x) = s(x)t(x)$ with $s(x), t(x)\in\mathbb{F}_q[x]$ and $\deg s(x), \deg t(x)\ge 1$, then there exists at least an index $i = 0, 1, \ldots, n-1$ such that $(x-\alpha^{q^i})$ divides $s(x)$. It follows that α^{q^i} is a root of $s(x)$ and so also $\alpha^{q^i}, (\alpha^{q^i})^q, (\alpha^{q^i})^{q^2}, \ldots, (\alpha^{q^i})^{q^{n-1}}$ are roots of $s(x)$. Hence $\alpha^{q^i}, (\alpha^q)^{q^i}, (\alpha^{q^2})^{q^i}, \ldots, (\alpha^{q^{n-1}})^{q^i}$ are roots of $s(x)$. By hypothesis, $\alpha, \alpha^q, \alpha^{q^2}, , \ldots, \alpha^{q^{n-1}}$ are pairwise distinct, and, since $\alpha\in\mathbb{F}_{q^n}$, also their q^i- powers are pairwise distinct. Hence, $s(x)$ has n distinct roots, contradicting the fact that $\deg q(x) = n$ and $\deg t(x)\ge 1$.

To prove the last claim we note that $[\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha^{q^i})] = 1$, since $\mathbb{F}_q\subseteq\mathbb{F}_q(\alpha^{q^i})\subseteq\mathbb{F}_{q^n}$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_q(\alpha^{q^i}) : \mathbb{F}_q] = n$ (we recall that α^{q^i} is a root of an irreducible polynomial of degree n with coefficients in $\mathbb{F}_q$). This implies that $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha^{q^i})$. □

We recall that the projective group $\mathrm{PGL}(2, q)$ acts on $\mathrm{PG}(1, q) = \mathbb{F}_q\cup\{\infty\}$ as follows.

Let $\sigma_{[A]} \in \mathrm{PGL}(2,q)$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$ and $[A] = A\mathcal{Z}$ where $\mathcal{Z}$ is the center of $\mathrm{GL}(2,q)$, and let $\alpha \in \mathrm{PG}(1,q) = \mathbb{F}_q \cup \{\infty\}$, then

$$\sigma_{[A]}(\alpha) = \begin{cases} \frac{a\alpha+b}{c\alpha+d} & \text{if } \alpha \in \mathbb{F}_q \text{ and } c\alpha+d \neq 0 \\ \infty & \text{if } \alpha \in \mathbb{F}_q \text{ and } c\alpha+d = 0 \\ \frac{a}{c} & \text{if } \alpha = \infty \text{ and } c \neq 0 \\ \infty & \text{if } \alpha = \infty \text{ and } c = 0 \end{cases} \tag{4.1.2}$$

The projective group $\mathrm{PGL}(2,q)$ acts also on $\mathbb{F}_q(x)|\mathbb{F}_q$ as follows.
Let $\sigma_{[A]} \in \mathrm{PGL}(2,q)$ and $\frac{f(x)}{g(x)} \in \mathbb{F}_q(x)$

$$\sigma_{[A]}\left(\frac{f(x)}{g(x)}\right) = \frac{f(\sigma_{[A]}^{-1}(x))}{g(\sigma_{[A]}^{-1}(x))}$$

where $\sigma_{[A]}^{-1}(x) = \sigma_{[A^{-1}]}(x) = \frac{dx-b}{-cx+a}$ if A is as above.
It is also well-known (see for instance [Rom] and [St1]) that every projectivity acts as an $\mathbb{F}_q-$automorphism of $\mathbb{F}_q(x)$ and that

$$\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q) \cong \mathrm{PGL}(2,q).$$

When $\sigma_{[A]}$ will denote an automorphism of $\mathbb{F}_q(x)|\mathbb{F}_q$ it will be simply denoted by σ_A.

Since $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$, then $\mathrm{PGL}(2,q)$ is, up to isomorphism, a subgroup of $\mathrm{PGL}(2,q^n)$ (and so $\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q) \cong \mathrm{PGL}(2,q)\widetilde{\subseteq}\mathrm{PGL}(2,q^n) \cong \mathrm{Aut}(\mathbb{F}_{q^n}(x)|\mathbb{F}_{q^n})$). So $\mathrm{PGL}(2,q)$ acts on $\mathbb{F}_{q^n} \cup \{\infty\}$ too. In fact, if $\sigma_{[A]} \in \mathrm{PGL}(2,q)$ and $\alpha \in \mathbb{F}_{q^n}$, we have that

$$\sigma_{[A]}(\alpha) = \frac{a\alpha+b}{c\alpha+d} \quad \text{if } \alpha \notin \mathbb{F}_q,$$

while $\sigma_{[A]}(\alpha)$ is defined as in (4.1.2) if $\alpha \in \mathbb{F}_q \cup \{\infty\}$. We remark that if $\alpha \notin \mathbb{F}_q \cup \{\infty\}$, then $c\alpha + d \neq 0$ and so $\sigma_{[A]}(\alpha) \in \mathbb{F}_{q^n}$.

We also remark that, since $\sigma_{[A]}(\alpha^{q^i}) = \frac{a\alpha^{q^i}+b}{c\alpha^{q^i}+d} = \left(\frac{a\alpha+b}{c\alpha+d}\right)^{q^i} = (\sigma_{[A]}(\alpha))^{q^i}$, we have

$$\sigma_{[A]}(\alpha^{q^i}) = (\sigma_{[A]}(\alpha))^{q^i}.$$

Now we are ready to consider the action of $\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$ on the places of $\mathbb{F}_q(x)|\mathbb{F}_q$. Let $\mathcal{P}^{(n)}$ be the set of the places of degree $n \geqslant 1$ of $\mathbb{F}_q(x)|\mathbb{F}_q$. If $n > 1$, then $\mathcal{P}^{(n)} = \{ P_{p(x)} \mid p(x) \in \mathbb{F}_q[x]$ is monic, irreducible and of degree $n\} = \{ P_{[\alpha]} \mid \alpha$ is a root of an irreducible polynomial of degree $n \}$, while $\mathcal{P}^{(1)} = \{P_{x-\alpha} \mid \alpha \in \mathbb{F}_q\} \cup \{P_\infty\} = \{P_{[\alpha]} \mid \alpha \in \mathbb{F}_q \cup \{\infty\}\}$.

Proposition 4.1.2. *If $P_{[\alpha]} \in \mathcal{P}^{(n)}$ and if $\sigma_A \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$, then*

$$\sigma_A(P_{[\alpha]}) = P_{[\sigma_{[A]}(\alpha)]}.$$

Proof. Suppose $\sigma_A \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$ and $P_{[\alpha]} \in \mathcal{P}^{(n)}$ where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $n > 1$ or $n = 1$ with $c\alpha+d \neq 0$. In this case $P_{[\alpha]} = P_{p(x)}$ where $p(x) \in \mathbb{F}_q[x]$ is an irreducible, monic polynomial of degree $n \geq 1$. We know that $p(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$ and so we have to prove that $\sigma_A(P_{p(x)}) = P_{(x-\sigma_{[A]}(\alpha))(x-\sigma_{[A]}(\alpha)^q)\cdots(x-\sigma_{[A]}(\alpha)^{q^{n-1}})}$.
Note that α, α^q, $\ldots$, $\alpha^{q^{n-1}}$ are pairwise distinct and so also the elements $\sigma_{[A]}(\alpha)$, $\sigma_{[A]}(\alpha)^q, \ldots, \sigma_{[A]}(\alpha)^{q^{n-1}}$ are pairwise distinct. Then, by Proposition 4.1.1, $q(x) = (x-\sigma_{[A]}(\alpha))(x-\sigma_{[A]}(\alpha)^q)\cdots(x-\sigma_{[A]}(\alpha)^{q^{n-1}})$ is an irreducible polynomial with coefficients in $\mathbb{F}_q$.
We are able to prove the claim now. If $P = P_{(x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})}$ and $t = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$, then $\sigma_A(t)$ is a local parameter of $\sigma_A(P)$. But

$$\begin{aligned}\sigma_A(t) &= \sigma_A((x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}}))\\ &= (\sigma_{[A]}^{-1}(x)-\alpha)(\sigma_{[A]}^{-1}(x)-\alpha^q)\cdots(\sigma_{[A]}^{-1}(x)-\alpha^{q^{n-1}})\\ &= \left(\tfrac{dx-b}{-cx+a}-\alpha\right)\left(\tfrac{dx-b}{-cx+a}-\alpha^q\right)\cdots\left(\tfrac{dx-b}{-cx+a}-\alpha^{q^{n-1}}\right)\\ &= \left[\tfrac{d+\alpha c}{-cx+a}\left(x-\tfrac{\alpha a+b}{d+\alpha c}\right)\right]\left[\tfrac{d+\alpha^q c}{-cx+a}\left(x-\tfrac{\alpha^q a+b}{d+\alpha^q c}\right)\right]\cdots\left[\tfrac{d+\alpha^{q^{n-1}}c}{-cx+a}\left(x-\tfrac{\alpha a+b}{d+\alpha^{q^{n-1}}c}\right)\right].\end{aligned}$$

For the last equality we remark that, since $\alpha^{q^i} \notin \mathbb{F}_q$, then $d+\alpha^{q^i}c \neq 0$ for any $i = 0, 1, \ldots, n-1$. Therefore $\sigma_{[A]}(t) = \frac{\prod_{i=0}^{n-1}(d+\alpha^{q^i}c)}{(-cx+a)^n}(x-\sigma_{[A]}(\alpha))(x-\sigma_{[A]}(\alpha)^q)\cdots(x-\sigma_{[A]}(\alpha)^{q^{n-1}})$. If we prove that $\frac{\prod_{i=0}^{n-1}(d+\alpha^{q^i}c)}{(-cx+a)^n}$ is an unit of $O_{[\sigma_{[A]}(\alpha)]}$, it will follow that $\sigma_A(t)$ is also a local parameter of $P_{[\sigma_{[A]}(\alpha)]}$ and hence $\sigma_A(P_{[\alpha]}) = P_{[\sigma_{[A]}(\alpha)]}$.

Since $(-cx+a)^n$ does not divide $(x-\sigma_{[A]}(\alpha))(x-\sigma_{[A]}(\alpha)^q)\cdots(x-\sigma_{[A]}(\alpha)^{q^{n-1}})$, then $\frac{1}{(-cx+a)^n}$ is an unit element of $O_{[\sigma_{[A]}(\alpha)]}$. In a similar way as we showed in the proof of Proposition 4.1.1, it is possible to prove also that $\prod_{i=0}^{n-1}(d+\alpha^{q^i}c) \in \mathbb{F}_q \subseteq O_{[\sigma_{[A]}(\alpha)]}$. Note that $\prod_{i=0}^{n-1}(d+\alpha^{q^i}c) \neq 0$ since every factor is different from zero. Therefore the claim follows. The proofs of the cases $c\alpha + d = 0$ or $\alpha = \infty$ are omitted since they are similar. □

Finally, we can describe the action of $\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$ on the set of $\phi-$places of $\mathbb{F}_q(x)|\mathbb{F}_q$. As above, let $p(x) \in \mathbb{F}_q[x]$ be a monic, irreducible polynomial of degree $n > 1$ and let α be one of its roots. Consider the place $P_{p(x)} = P_{[\alpha]}$.

Proposition 4.1.3. *If $(P_{[\alpha]}, \phi_\alpha)$ is a $\phi-$place of degree n of $\mathbb{F}_q(x)|\mathbb{F}q$ and $\sigma_A \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$, then*

$$\sigma_A(P_{[\alpha]}, \phi_\alpha) = (P_{[\sigma_{[A]}(\alpha)]}, \phi_{\sigma_{[A]}(\alpha)}) \tag{4.1.3}$$

Proof. By definition, $\sigma_A(P_{[\alpha]}, \phi_\alpha) = (\sigma_A(P_{[\alpha]}), \phi_\alpha\sigma_A^{-1})$ so, by Proposition 4.1.2, it is enough to prove that $\phi_\alpha\sigma_A^{-1} = \phi_{\sigma_{[A]}(\alpha)}$. In fact, for all $\frac{f(x)}{g(x)}(\sigma_A(P_{[\alpha]}))$ we have
$\phi_\alpha\sigma_A^{-1}(\frac{f(x)}{g(x)}(\sigma_A(P_{[\alpha]}))) = \phi_\alpha(\frac{f(\sigma_{[A]}(x))}{g(\sigma_{[A]}(x))}(P_{[\alpha]})) = \frac{f(\sigma_{[A]}(\alpha))}{g(\sigma_{[A]}(\alpha))} = \phi_{\sigma_{[A]}(\alpha)}(\frac{f(x)}{g(x)}(\sigma_A(P_{[\alpha]}))).$ □

Now we provide a description of $\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G}$ when $G = rP_\infty$ in order to have a different version of Theorem 3.2.16.

Proposition 4.1.4. *Let $\Phi = \sum_{i=1}^{N}(P_{[\alpha_i]}, \phi_{\alpha_i})$ be a $\phi-$divisor with $P_{[\alpha_i]}$ distinct places of degree $n > 1$ of the function field $\mathbb{F}_q(x)|\mathbb{F}_q$. If $G = rP_\infty$, then the automorphisms of $\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$ fixing Φ and G are, up to isomorphism, the affinities of the affine line over $\mathbb{F}_q$ which permute the roots α_i.*

Proof. We recall that if $G = rP_\infty$

$$\mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G} = \{\, \sigma_A \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q) \mid \sigma_A(P_\infty) = P_\infty \text{ and for any } i \ \ \sigma_A(P_{[\alpha_i]}, \phi_{\alpha_i}) = (P_{[\alpha_j]}, \phi_{\alpha_j}) \text{ for some } j \,\}.$$

Let $\sigma_A \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)_{\Phi,G}$ be fixed. By Proposition 4.1.2, in order to have $\sigma_{[A]}(P_\infty) = P_\infty$, it must be

$$A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

So $\sigma_{[A]}$ fixes ∞ and we can think of $\sigma_{[A]}$ as an affinity of the affine line. By (4.1.3), $(P_{[\alpha_j]}, \phi_{\alpha_j}) = \sigma_A(P_{[\alpha_i]}, \phi_{\alpha_i}) = (P_{[\sigma_{[A]}(\alpha_i)]}, \phi_{\sigma_{[A]}(\alpha_i)})$ and so $P_{[\alpha_j]} = P_{[\sigma_{[A]}(\alpha_i)]}$ and $\phi_{\alpha_j} = \phi_{\sigma_{[A]}(\alpha_i)}$. But $P_{[\alpha_j]} = P_{[\sigma_{[A]}(\alpha_i)]}$ if and only if $\sigma_{[A]}(\alpha_i) = \alpha_j^{q^s}$ for some $0 \le s \le n-1$. So $\phi_{\alpha_j} = \phi_{\sigma_{[A]}(\alpha_i)} = \phi_{\alpha_j^{q^s}}$ and this occurs if and only if $s = 0$. Hence $\sigma_{[A]}(\alpha_i) = \alpha_j$, that is, $\sigma_{[A]}$ permutes the α_i.

Conversely, let $\sigma_A \in \mathrm{Aut}(\mathbb{F}_q(x)|\mathbb{F}_q)$ such that $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\sigma_{[A]}(\alpha_i) = \alpha_j$. Then $\sigma_A(P_\infty) = P_\infty$ and $\sigma_A(P_{[\alpha_i]}, \phi_{\alpha_i}) = (P_{[\sigma_{[A]}(\alpha_i)]}, \phi_{\sigma_{[A]}(\alpha_i)}) = (P_{[\alpha_j]}, \phi_{\alpha_j})$, that is, σ_A is an automorphism of $\mathbb{F}_q(x)|\mathbb{F}_q$ which fixes Φ and G. □

Corollary 4.1.5. *Let $\mathbb{F}_q(x)|\mathbb{F}_q$ be a rational function field and let $C(\Phi; G; n)$ be the* GAG*-code associated with $\Phi = \sum_{i=1}^{N}(P_{[\alpha_i]}, \phi_{\alpha_i})$ and $G = rP_\infty$. Moreover, let*

$\mathcal{H}(n;\Phi;G)$ be the $n-$automorphism group of $C(\Phi;G;n)$. If $r < \frac{nN}{2}$, then $\mathcal{H}(n;\Phi;G)$ is isomorphic to the group of the affinities of the affine line over $\mathbb{F}_q$ which permute the roots α_i.

Proof. By Theorem 3.2.16, the $n-$automorphism group of $C(\Phi;G;n)$ is the stabilizer of Φ and G and, by Proposition 4.1.4, it is isomorphic to the affinities of the affine line over $\mathbb{F}_q$ that permute all the roots α_i. □

Finally, we give some examples of $n-$automorphism groups for GAG-codes over rational function fields $\mathbb{F}_q(x)|\mathbb{F}_q$.

We recall that the number of monic irreducible polynomials of degree n with coefficients in the field $\mathbb{F}_q$ is (see for instance [Jun])

$$D_{n,q} = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}$$

where

$$\mu(d) := \begin{cases} 1 & \text{if } d = 1 \\ (-1)^s & \text{if } d \text{ is the product of } s \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Such a number $D_{n,q}$, in case $n > 1$, is the number of places of degree n of the function field $\mathbb{F}_q(x)|\mathbb{F}_q$, whereas the number of places of degree $n = 1$ is exactly $D_{1,q} + 1$.

In all the following examples, the necessary calculations have been made using the software *Mathematica v5*.

Example 2. Let $\mathbb{F}_q = \mathbb{F}_2$. The number of monic irreducible polynomials of degree 5

with coefficients in $\mathbb{F}_2$ is $D_{5,2} = 6$ and they are

$$\begin{aligned} p_1(x) &= x^5 + x^3 + 1 & p_2(x) &= x^5 + x^3 + x^2 + x + 1 \\ p_3(x) &= x^5 + x^2 + 1 & p_4(x) &= x^5 + x^4 + x^3 + x^2 + x + 1 \\ p_5(x) &= x^5 + x^4 + x^3 + x + 1 & p_6(x) &= x^5 + x^4 + x^2 + x + 1. \end{aligned}$$

Let $\mathbb{F}_{32} = \mathbb{F}_2(\alpha)$ where α is an element in $\overline{\mathbb{F}_2}$ such that $\alpha^5 + \alpha^3 + 1 = 0$. Let $\Phi = \sum_{i=1}^{6}(P_{p_i(x)}, \phi_{\alpha_i})$ where $\alpha_1 = \alpha$, $\alpha_2 = \alpha^3$, $\alpha_3 = \alpha + \alpha^2$, $\alpha_4 = \alpha + 1$, $\alpha_5 = \alpha^3 + 1$, $\alpha_6 = \alpha^2 + \alpha + 1$ are all in $\mathbb{F}_{32}$. If $G = 14P_\infty$, then $C(\Phi, 14P_\infty, 5)$ is a $2-$ary $[30, 15, d]$ code with $4 \leq d \leq 17$ (see Corollary 3.1.2). Moreover, the $n-$automorphism group $\mathcal{H}(\Phi; 14P_\infty; 5)$ of $C(\Phi; 14P_\infty; 5)$ is isomorphic to AGL$(1, 2)$ since any element of AGL$(1, 2)$ fixes the set $\{\, \alpha_i \mid i = 1, 2, \ldots, 6 \,\}$ (see Corollary 4.1.5).

Example 3. Let $\mathbb{F}_q = \mathbb{F}_3$. The number of monic irreducible polynomials of degree 3 with coefficients in $\mathbb{F}_3$ is $D_{3,3} = 8$ and they are

$$\begin{aligned} p_1(x) &= x^3 + 2x + 1 & p_2(x) &= x^3 + 2x + 2 \\ p_3(x) &= x^3 + x^2 + x + 2 & p_4(x) &= x^3 + x^2 + 2x + 1 \\ p_5(x) &= x^3 + x^2 + 2 & p_6(x) &= x^3 + 2x^2 + x + 1 \\ p_7(x) &= x^3 + 2x^2 + 1 & p_8(x) &= x^3 + 2x^2 + 2x + 2. \end{aligned}$$

We use $p_1(x)$ to construct $\mathbb{F}_{27}$. So $\mathbb{F}_{27} = \mathbb{F}_3(\alpha)$ where α is an element in $\overline{\mathbb{F}_3}$ such that $\alpha^3 + 2\alpha + 1 = 0$. Whereas we use $p_3(x), p_4(x), \ldots, p_8(x)$ to define the $\phi-$divisor $\Phi = \sum_{i=3}^{8}(P_{p_i(x)}, \phi_{\alpha_i})$ where $\alpha_3 = \alpha^2$, $\alpha_4 = \alpha^2+1$, $\alpha_5 = \alpha^2+2$, $\alpha_6 = 2\alpha^2$, $\alpha_7 = 2\alpha^2+1$, $\alpha_8 = 2\alpha^2 + 2$ are all in $\mathbb{F}_{27}$. If $G = 8P_\infty$, then $C(\Phi, 8P_\infty, 3)$ is a $3-$ary $[18, 9, d]$ code with $4 \leq d \leq 10$ (see Corollary 3.1.2). Moreover, $\mathcal{H}(\Phi; 8P_\infty; 3)$ is isomorphic to the subgroup of AGL$(1, 3)$ which is generated by $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and so

$$\mathcal{H}(\Phi; 8P_\infty; 3) \simeq S_3.$$

Example 4. Let $\mathbb{F}_q = \mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ where α is an element such that $\alpha^4 + \alpha + 1 = 0$. Let $\mathbb{F}_{256} = \mathbb{F}_{16}(\beta)$ where β is an element such that $\beta^2 + \alpha\beta + \alpha = 0$. Let us consider the next 15 $\phi-$places

$$\begin{aligned}
(P_1, \phi_1) &= (P_{x^2+\alpha^2 x+\alpha^2}, \phi_{\alpha\beta+\alpha}) \\
(P_2, \phi_2) &= (P_{x^2+\alpha^3 x+\alpha+1}, \phi_{\alpha^2\beta+\alpha^2}) \\
(P_3, \phi_3) &= (P_{x^2+(\alpha+1)x+\alpha^3+\alpha^2}, \phi_{\alpha^3\beta+\alpha^3}) \\
(P_4, \phi_4) &= (P_{x^2+(\alpha^2+\alpha)x+\alpha^2+1}, \phi_{(\alpha+1)\beta+\alpha+1}) \\
(P_5, \phi_5) &= (P_{x^2+(\alpha^3+\alpha^2)x+\alpha^2+\alpha+1}, \phi_{(\alpha^2+\alpha)\beta+\alpha^2+\alpha}) \\
(P_6, \phi_6) &= (P_{x^2+(\alpha^3+\alpha+1)x+\alpha^3+\alpha^2+\alpha+1}, \phi_{(\alpha^3+\alpha^2)\beta+\alpha^3+\alpha^2}) \\
(P_7, \phi_7) &= (P_{x^2+(\alpha^2+1)x+\alpha^3+1}, \phi_{(\alpha^3+\alpha+1)\beta+\alpha^3+\alpha+1}) \\
(P_8, \phi_8) &= (P_{x^2+(\alpha^3+\alpha)x+\alpha}, \phi_{(\alpha^2+1)\beta+\alpha^2+1}) \\
(P_9, \phi_9) &= (P_{x^2+(\alpha^2+\alpha+1)x+\alpha^3}, \phi_{(\alpha^3+\alpha)\beta+\alpha^3+\alpha}) \\
(P_{10}, \phi_{10}) &= (P_{x^2+(\alpha^3+\alpha^2+\alpha)x+\alpha^2+\alpha}, \phi_{(\alpha^2+\alpha+1)\beta+\alpha^2+\alpha+1}) \\
(P_{11}, \phi_{11}) &= (P_{x^2+(\alpha^3+\alpha^2+\alpha+1)x+\alpha^3+\alpha+1}, \phi_{(\alpha^3+\alpha^2+\alpha)\beta+\alpha^3+\alpha^2+\alpha}) \\
(P_{12}, \phi_{12}) &= (P_{x^2+(\alpha^3+\alpha^2+1)x+\alpha^3+\alpha}, \phi_{(\alpha^3+\alpha^2+\alpha+1)\beta+\alpha^3+\alpha^2+\alpha+1}) \\
(P_{13}, \phi_{13}) &= (P_{x^2+(\alpha^3+1)x+\alpha^3+\alpha^2+\alpha}, \phi_{(\alpha^3+\alpha^2+1)\beta+\alpha^3+\alpha^2+1}) \\
(P_{14}, \phi_{14}) &= (P_{x^2+x+\alpha^3+\alpha^2+1}, \phi_{(\alpha^3+1)\beta+\alpha^3+1}) \\
(P_{15}, \phi_{15}) &= (P_{x^2+\alpha x+1}, \phi_{\beta+1}).
\end{aligned}$$

Let $\Phi = \sum_{i=1}^{15}(P_i, \phi_i)$. If $G = 14P_\infty$, then $C(\Phi, 14P_\infty, 2)$ is a $16-$ary $[30, 15, d]$ code with $8 \leq d \leq 16$ (see Corollary 3.1.2). Moreover, $\mathcal{H}(\Phi; 14P_\infty; 2)$ is, up to isomorphism, generated by $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ and so

$$\mathcal{H}(\Phi; 14P_\infty; 2) \simeq \mathbb{Z}_{15}.$$

4.2 The Hyperelliptic case

Let $\mathcal{C}$ be a plane curve defined over $\mathbb{F}_q$. We remember that a point $P(\alpha, \beta)$ of $\mathcal{C}$ is said to be a *point of degree* i if α, β are in $\mathbb{F}_{q^i}$ but not in $\mathbb{F}_{q^j}$ for $j < i$, that is, if $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_{q^i}$.

A *plane model* of a function field $F|\mathbb{F}_q$ is an irreducible curve $\mathcal{C} : f(X, Y) = 0$ defined over $\mathbb{F}_q$ such that $F = \mathbb{F}_q(x, y)$ and $f(x, y) = 0$.

Consider an algebraic extension $F'|K'$ of $F|K$. A $\phi-$place (P', ϕ') of F' is said to *lie over* a $\phi-$place (P, ϕ) of F if $P \subseteq P'$ and $\phi'|_{F_P} = \phi$.

Proposition 4.2.1. *Let $F|\mathbb{F}_q$ be a function field and*

$$\mathcal{C} : f(X, Y) = 0, \tag{4.2.1}$$

a plane model of it.

If (P', ϕ') is a $\phi-$place of F which lies over the $\phi-$place $(P_{[\alpha]}, \phi_\alpha)$ of $\mathbb{F}_q(x)$ (where $\alpha \neq \infty$), then $(x(P', \phi'), y(P', \phi'))$ is a point of $\mathcal{C}$ whose degree is equal to $\deg P'$. *Furthermore we have $x(P', \phi') = \alpha$.*

Proof. We start to prove that $(x(P', \phi'), y(P', \phi'))$ is a point of $\mathcal{C}$. In fact $f(x(P', \phi'), y(P', \phi')) = f(\phi'(x(P')), \phi'(y(P'))) = \phi'(f(x(P'), y(P'))) = \phi'(f(x, y)(P'))$ $= \phi'(0(P')) = 0$. In order to prove that $\deg(x(P', \phi'), y(P', \phi')) = \deg P'$ it is enough to show that $\mathbb{F}_q(x(P', \phi'), y(P', \phi')) = \mathbb{F}_{q^{\deg P'}}$. Clearly $\mathbb{F}_q(x(P', \phi'), y(P', \phi')) \subseteq \mathbb{F}_{q^{\deg P'}}$ since ϕ' is a map from $F_{P'}$ into $\mathbb{F}_{q^{\deg P'}}$ and so $x(P', \phi'), y(P', \phi') \in \mathbb{F}_{q^{\deg P'}}$. Vice versa for any $\gamma \in \mathbb{F}_{q^{\deg P'}}$, being ϕ' an isomorphism, there exists $\frac{u(x,y)}{v(x,y)}(P') \in F_{P'}$ such that $\gamma = \phi'(\frac{u(x,y)}{v(x,y)}(P')) = \frac{u((x(P',\phi'),y(P',\phi'))}{v((x(P',\phi'),y(P',\phi'))} \in \mathbb{F}_q((x(P', \phi'), y(P', \phi'))$. Finally, $x(P', \phi') = \phi'(x(P')) = \phi_\alpha(x(P)) = \alpha$ where the second equality is true since (P', ϕ') lies over $(P_{[\alpha]}, \phi_\alpha)$. □

The converse of Proposition 4.2.1 is certainly true when $F|\mathbb{F}_q$ is a hyperelliptic function field.

Proposition 4.2.2. *Let $F = \mathbb{F}_q(x, y)$, with $\operatorname{char}\mathbb{F}_q \neq 2$, be a hyperelliptic function field and*

$$\mathcal{C} : Y^2 = f(X) \in \mathbb{F}_q[X], \tag{4.2.2}$$

a standard plane model of it.

If (α, β) is a point of $\mathcal{C}$, then there exists only one $\phi-$place (P', ϕ') of F which lies over the $\phi-$place $(P_{[\alpha]}, \phi_\alpha)$ of $\mathbb{F}_q(x)$ such that $\deg P' = \deg(\alpha, \beta)$, $x(P', \phi') = \alpha$ and $y(P', \phi') = \beta$.

Proof. Let (α, β) be a point of $\mathcal{C}$.

If $\beta = 0$, then $f(\alpha) = 0$ and so $P_{[\alpha]}$ is ramified. Then there exists exactly one place P' of F which lies over $P_{[\alpha]}$ and $\deg P' = \deg P_{[\alpha]}$. Moreover, up to isomorphism, $F_{P'} = F_{P_{[\alpha]}}$ and so the only $\phi-$place which lies over $(P_{[\alpha]}, \phi_\alpha)$ is (P', ϕ_α).

We have $x(P', \phi_\alpha) = \phi_\alpha(x(P')) = \alpha$ and $(y(P', \phi_\alpha))^2 = (\phi_\alpha(y(P')))^2 = \phi_\alpha(y^2(P')) = \phi_\alpha(f(x)(P')) = f(\alpha) = 0$ and so $y(P', \phi_\alpha) = 0$. Moreover, since $\beta = 0$, then $\deg(\alpha, \beta) = \deg P_{[\alpha]} = \deg P'$.

If $\beta \neq 0$, then $f(\alpha) \neq 0$ and so $P_{[\alpha]}$ is not ramified. Then $P_{[\alpha]}$ splits completely or stays inert.

If $P_{[\alpha]}$ splits completely, then there exist exactly two distinct places P' and P'' of F which lie over $P_{[\alpha]}$ and $\deg P' = \deg P'' = \deg P_{[\alpha]}$. Moreover, up to isomorphism, $F_{P'} = F_{P''} = F_{P_{[\alpha]}}$ and so the only $\phi-$places which lie over $(P_{[\alpha]}, \phi_\alpha)$ are (P', ϕ_α) and (P'', ϕ_α). We have $x(P', \phi_\alpha) = \alpha = x(P'', \phi_\alpha)$. Moreover, $(y(P', \phi_\alpha))^2 = (\phi_\alpha(y(P')))^2 = \phi_\alpha(y^2(P')) = \phi_\alpha(f(x)(P')) = f(\alpha) = \beta^2$ and, in the same way, $(y(P'', \phi_\alpha))^2 = \beta^2$. Then $y(P', \phi_\alpha) = \beta$ and $y(P'', \phi_\alpha) = -\beta$ (or vice versa) since

in case $y(P', \phi_\alpha) = y(P'', \phi_\alpha)$, by Lemma 3.2.13, it would result $(P', \phi_\alpha) = (P'', \phi_\alpha)$ which is a contradiction with the fact that $P' \neq P''$. Hence (P', ϕ_α) is a $\phi-$place which lies over $(P_{[\alpha]}, \phi_\alpha)$ such that $x(P', \phi_\alpha) = \alpha$ and $y(P', \phi_\alpha) = \beta$. Finally, $\deg P' = \deg P_{[\alpha]} = \deg(\alpha, \beta)$ since $\alpha, \beta \in \mathbb{F}_{q^{\deg P_{[\alpha]}}}$ being both images of ϕ_α which is a map with values onto $\mathbb{F}_{q^{deg\, P_{[\alpha]}}}$.

If $P_{[\alpha]}$ stays inert, then there exists exactly one place P' of F which lies over $P_{[\alpha]}$ and $2n := \deg P' = 2 \deg P_{[\alpha]}$. Moreover, $[F_{P'} : F_{P_{[\alpha]}}] = 2$ and $F_{P'} = F_{P_{[\alpha]}}(y(P'))$, in fact $y(P') \in F_{P'} \setminus F_{P_{[\alpha]}}$ is a root of the irreducible polynomial $T^2 - (f(x)(P_{[\alpha]})) \in F_{P_{[\alpha]}}[T]$. The polynomial $T^2 - (f(x)(P_{[\alpha]})) \in F_{P_{[\alpha]}}[T]$ is irreducible, in fact in the oppositive case, $T^2 - (f(x)(P_{[\alpha]})) = (T - \frac{u(x)}{v(x)}(P_{[\alpha]}))(T + \frac{u(x)}{v(x)}(P_{[\alpha]}))$ with $\frac{u(x)}{v(x)} \in O_{P_{[\alpha]}}$ such that $(\frac{u(x)}{v(x)})^2(P_{[\alpha]}) = f(x)(P_{[\alpha]})$ and so, by Kummer's Theorem (see for instance [St1]), it would exist two distinct places P_1 and P_2 which lie over $P_{[\alpha]}$. This is a contradiction with the fact that $P_{[\alpha]}$ stays inert. The only two ways to extend ϕ_α to an isomorphism from $F_{P'}$ to $\mathbb{F}_{q^{2n}}$ are those to associate to $y(P')$ one of the two roots of the irreducible polynomial $T^2 - f(\alpha)$. Therefore if $\beta, -\beta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ are such roots, then the unique $\phi-$places which extend $(P_{[\alpha]}, \phi_\alpha)$ are $(P', \phi_{\alpha,\beta})$ and $(P', \phi_{\alpha,-\beta})$ where $\phi_{\alpha,\beta}(\frac{u(x,y)}{v(x,y)}(P')) := \frac{u(\alpha,\beta)}{v(\alpha,\beta)}$ and $\phi_{\alpha,-\beta}(\frac{u(x,y)}{v(x,y)}(P')) := \frac{u(\alpha,-\beta)}{v(\alpha,-\beta)}$ for any $\frac{u(x,y)}{v(x,y)}(P') \in F_{P'}$.

So there exists the $\phi-$place $(P', \phi_{\alpha,\beta})$ which lies over $(P_{[\alpha]}, \phi_\alpha)$ such that $x(P', \phi_{\alpha,\beta}) = \alpha$, $y(P', \phi_{\alpha,\beta}) = \beta$ and $\deg(\alpha, \beta) = 2 \deg P_{[\alpha]} = \deg P'$.

The uniqueness is trivial. □

Corollary 4.2.3. *Any $\phi-$place which does not lie over $(P_{[\infty]}, id)$ of a hyperelliptic function field $\mathbb{F}_q(x, y)|\mathbb{F}_q$ is of the type $(P_{[\alpha,\beta]}, \phi_{\alpha,\beta})$ with*

$$P_{[\alpha,\beta]} = \{\frac{u(x,y)}{v(x,y)} \in F \,|\, u(\alpha, \beta) = 0 \text{ and } v(\alpha, \beta) \neq 0\}$$

and

$$\phi_{\alpha,\beta}(\frac{u(x,y)}{v(x,y)}) := \frac{u(\alpha,\beta)}{v(\alpha,\beta)} \quad \textit{for any} \quad \frac{u(x,y)}{v(x,y)} \in \mathcal{O}_{[\alpha,\beta]}$$

where $\mathcal{O}_{[\alpha,\beta]}$ *is the valuation ring of* $P_{[\alpha,\beta]}$.

Proof. By Proposition 4.2.1, if (α,β) is a point of a standard plane model $\mathcal{C}$ of F, then there exists only one $\phi-$place (P',ϕ') of F which lies over the $\phi-$place $(P_{[\alpha]},\phi_\alpha)$ of $\mathbb{F}_q(x)$ such that $x(P',\phi') = \alpha$ and $y(P',\phi') = \beta$. So $\phi' : F_{P'} \to \mathbb{F}_{q^{\deg P'}}$ is defined via $\phi'(\frac{u(x,y)}{v(x,y)}) = \frac{u(\alpha,\beta)}{v(\alpha,\beta)}$ for any $\frac{u(x,y)}{v(x,y)} \in F_{P'}$. Clearly, the valuation ring $\mathcal{O}'$ of P' is contained in the ring $\mathcal{O}_{[\alpha,\beta]} = \{\frac{u(x,y)}{v(x,y)} \in F \,|\, v(\alpha,\beta) \neq 0\}$ and, for the maximality of a valuation ring (see for instance [St1]), the claim follows. □

Note that from the proof of Proposition 4.2.2 we have:

(1) if $\beta = 0$, then the place extension $P_{[\alpha,\beta]}|P_{[\alpha]}$ is ramify;

(2) if $0 \neq \beta \in \mathbb{F}_q(\alpha)$, then $P_{[\alpha]}$ splits completely and $e(P_{[\alpha,\beta]}|P_{[\alpha]}) = f(P_{[\alpha,\beta]}|P_{[\alpha]}) = 1$;

(3) If $\beta \notin \mathbb{F}_q(\alpha)$, then $P_{[\alpha]}$ stays inert with $e(P_{[\alpha,\beta]}|P_{[\alpha]}) = 1$ and $f(P_{[\alpha,\beta]}|P_{[\alpha]}) = 2$.

Let $\mathbb{F}_q(x,y)|\mathbb{F}_q$ be a hyperelliptic function field ($\operatorname{char}\mathbb{F}_q \neq 2$) with $g > 1$, and

$$\mathcal{C} : Y^2 = f(X) \in \mathbb{F}_q[X], \tag{4.2.3}$$

a standard plane model of it.

We suppose that the monic polynomial $f(X)$ has degree $d = 2g+1$ (note that this happens if $f(X)$ has at least one root in $\mathbb{F}_q$). Let $\gamma_0, \gamma_1, \ldots, \gamma_{2g}$ be the distinct roots of $f(X)$ and $\operatorname{Aut}(\mathcal{C})$ be the group of all automorphisms of $\mathcal{C}$.

Let us consider the subgroup W of $\mathrm{PGL}(2,\overline{\mathbb{F}_q})$ whose projectivity which map the set $T=\{\gamma_0,\gamma_1,\ldots,\gamma_{2g},\infty\}$ onto itself.

The $\overline{\mathbb{F}_q}-$automorphism group $\mathrm{Aut}(\mathcal{C})$ of $\mathcal{C}$ (see [H-K-T]) consists of all birational transformations σ defined as follows:

$$\begin{cases} \sigma(x)=\sigma_{[A]}(x), & \text{with } \sigma_{[A]}\in W \text{ and } A=\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \\ \sigma(y)=\epsilon y, & \text{with } \epsilon^2=a^d; \end{cases}$$

or

$$\begin{cases} \sigma(x)=\sigma_{[A]}(x), & \text{with } \sigma_{[A]}\in W \text{ and } A=\begin{pmatrix} a & b \\ 1 & -\gamma_0 \end{pmatrix} \\ \sigma(y)=\epsilon\frac{y}{(x-\gamma_0)^{g+1}}, & \text{with } \epsilon^2=(b+a\gamma_0)\prod_{i=1}^{2g}(\gamma_0-\gamma_i). \end{cases}$$

Any $\sigma\in\mathrm{Aut}(\mathcal{C})$ induces an $\overline{\mathbb{F}_q}$-automorphism $\overline{\sigma}$ of $\overline{\mathbb{F}_q}(x,y)|\overline{\mathbb{F}_q}$ defined via

$$\overline{\sigma}\Big(\frac{f(x,y)}{g(x,y)}\Big):=\frac{f(\sigma^{-1}(x),\sigma^{-1}(y))}{g(\sigma^{-1}(x),\sigma^{-1}(y))}$$

for each $\frac{f(x,y)}{g(x,y)}\in\overline{\mathbb{F}_q}(x,y)$.

Obviously, the elements of $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C})$ induce automorphisms of $\mathbb{F}_q(x,y)|\mathbb{F}_q$ and we have

$$\mathrm{Aut}(\mathbb{F}_q(x,y)|\mathbb{F}_q)\cong\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}).$$

Proposition 4.2.4. *Let $F|\mathbb{F}_q$ be a hyperelliptic function field. If $(P_{[\alpha,\beta]},\phi_{\alpha,\beta})$ is a $\phi-$place of degree n of $F|\mathbb{F}q$ and $\overline{\sigma}\in\mathrm{Aut}(F|\mathbb{F}_q)$, then*

$$\overline{\sigma}(P_{[\alpha,\beta]},\phi_{\alpha,\beta})=(P_{[\sigma(\alpha),\sigma(\beta)]},\phi_{\sigma(\alpha),\sigma(\beta)}). \tag{4.2.4}$$

Proof. By definition $\overline{\sigma}(P_{[\alpha,\beta]},\phi_{\alpha,\beta})=(\overline{\sigma}(P_{[\alpha,\beta]}),\phi_{\alpha,\beta}\overline{\sigma}^{-1})$ so it is sufficiently to prove that $\overline{\sigma}(P_{[\alpha,\beta]})=P_{[\sigma(\alpha),\sigma(\beta)]}$ and $\phi_{\alpha,\beta}\overline{\sigma}^{-1}=\phi_{\sigma(\alpha),\sigma(\beta)}$. In fact, for any $\frac{u(x,y)}{v(x,y)}\in P_{[\alpha,\beta]}$ result $\overline{\sigma}(\frac{u(x,y)}{v(x,y)})=\frac{u(\sigma^{-1}(x),\sigma^{-1}(y))}{v(\sigma^{-1}(x),\sigma^{-1}(y))}\in P_{[\sigma(\alpha),\sigma(\beta)]}$ since $u(\sigma^{-1}(\sigma(\alpha)),\sigma^{-1}(\sigma(\beta)))=u(\alpha,\beta)=$

0 and $v(\sigma^{-1}(\sigma(\alpha)),\sigma^{-1}(\sigma(\beta))) = v(\alpha,\beta) \neq 0$. Conversely, for any $\frac{u(x,y)}{v(x,y)} \in P_{[\sigma(\alpha),\sigma(\beta)]}$ it results $\frac{u(x,y)}{v(x,y)} = \overline{\sigma}(\frac{u(\sigma(x),\sigma(y))}{v(\sigma(x),\sigma(y))}) \in \overline{\sigma}(P_{[\alpha,\beta]})$ since $u(\sigma(\alpha),\sigma(\beta)) = 0$, $v(\sigma(\alpha),\sigma(\beta)) \neq 0$. Now for any $\frac{u(x,y)}{v(x.y)}(\overline{\sigma}(P_{[\alpha,\beta]}))$ we have $\phi_{\alpha,\beta}\overline{\sigma}^{-1}(\frac{u(x,y)}{v(x,y)}(\overline{\sigma}(P_{[\alpha,\beta]}))) = \phi_{\alpha,\beta}(\frac{u(\sigma(x),\sigma(y))}{v(\sigma(x),\sigma(y))}(P_{[\alpha,\beta]}))$ $= \frac{u(\sigma(\alpha),\sigma(\beta))}{v(\sigma(\alpha),\sigma(\beta))} = \phi_{\sigma(\alpha),\sigma(\beta)}(\frac{u(x,y)}{v(x,y)}(\overline{\sigma}(P_{[\alpha,\beta]})))$. □

Note that if (α,β) is a point of $\mathcal{C}$ of degree n, then $(\sigma(\alpha),\sigma(\beta))$ is a point of $\mathcal{C}$ of degree n for any $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C})$. In fact, $\deg(\sigma(\alpha),\sigma(\beta)) = \deg \overline{\sigma}(P_{[\alpha,\beta]}) = \deg P_{[\alpha,\beta]} = \deg(\alpha,\beta)$. Then $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C})$ also acts on the set of the $\mathbb{F}_{q^n}-$rational points of $\mathcal{C}$.

Proposition 4.2.5. *Let $F|\mathbb{F}_q$ be the hyperelliptic function field which plane model is*

$$\mathcal{C} : Y^2 = \prod_{\gamma\in\mathbb{F}_q}(X-\gamma).$$

Let $\Phi = \sum_{i=1}^{N}(P_{[\alpha_i,\beta_i]},\phi_{\alpha_i,\beta_i})$ be a $\phi-$divisor of F with $P_{[\alpha_i,\beta_i]}$ distinct places of degree $n>1$. If $G = rD_\infty$, then the stabilizer of Φ and G in $\mathrm{Aut}(F|\mathbb{F}_q)$ is the group of all transformations $\overline{\sigma} \in \mathrm{Aut}(F|\mathbb{F}_q)$ with $\sigma(x) = ax+b$ and $\sigma(y) = \epsilon y$ with $\epsilon^2 = a$ such that σ fixes the set $\{\,(\alpha_i,\beta_i) \mid i = 1,2,\ldots,N\,\}$.

Proof. Note that, since $f(X) = \prod_{\gamma\in\mathbb{F}_q}(X-\gamma)$, then $W = \mathrm{PGL}(2,\mathbb{F}_q)$. We recall that

$$\mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,G} = \{\overline{\sigma} \in \mathrm{Aut}(F|\mathbb{F}_q) \,|\, \overline{\sigma}(D_\infty) = D_\infty$$
$$\text{and for all } i,\ \overline{\sigma}(P_{[\alpha_i,\beta_i]},\phi_{\alpha_i,\beta_i}) = (P_{[\alpha_j,\beta_j]},\phi_{\alpha_j,\beta_j}) \text{ for some } j\}.$$

Let $\overline{\sigma} \in \mathrm{Aut}(F|\mathbb{F}_q)_{\Phi,G}$ be fixed. In order to have $\overline{\sigma}(D_\infty) = D_\infty$, it must be $\sigma(x) = ax+b$ and consequently $\sigma(y) = \epsilon y$ with $\epsilon^2 = a^d = a^q = a$ (note that $\deg f(X) = q$). By (4.2.4), we also have that $(P_{[\alpha_j,\beta_j]},\phi_{\alpha_j,\beta_j}) = \overline{\sigma}(P_{[\alpha_i,\beta_i]},\phi_{\alpha_i,\beta_i}) = (P_{[\sigma(\alpha_i),\sigma(\beta_i)]},\phi_{\sigma(\alpha_i),\sigma(\beta_i)})$ and so $(\alpha_j,\beta_j) = \sigma(\alpha_i,\beta_i)$.

Conversely, let $\overline{\sigma} \in \mathrm{Aut}(F|\mathbb{F}_q)$ such that $\sigma(x) = ax+b$, $\sigma(y) = \epsilon y$ with $\epsilon^2 = a$ and $\sigma(\alpha_i,\beta_i) = (\alpha_j,\beta_j)$. Then $\overline{\sigma}(D_\infty) = D_\infty$ and $\overline{\sigma}(P_{[\alpha_i,\beta_i]},\phi_{\alpha_i,\beta_i}) = (P_{[\sigma(\alpha_i),\sigma(\beta_i)]},\phi_{\sigma(\alpha_i),\sigma(\beta_i)})$ $= (P_{[\alpha_j,\beta_j]},\phi_{\alpha_j,\beta_j})$, that is, $\overline{\sigma}$ is an automorphism of $F|\mathbb{F}_q$ which fixes Φ and G. □

Corollary 4.2.6. *Let $F|\mathbb{F}_q$ be the hyperelliptic function field which plane model is*

$$\mathcal{C} : Y^2 = \prod_{\gamma \in \mathbb{F}_q} (X - \gamma)$$

and let $C(\Phi; G; n)$ be the GAG−code associated with $\Phi = \sum_{i=1}^{N} (P_{[\alpha_i,\beta_i]}, \phi_{\alpha_i,\beta_i})$ and $G = rD_\infty$. If $2g + 2 < r < \frac{nN}{2}$ and $nN \geq 4g + 3$, then $\mathcal{H}(n; \Phi; G)$ is the group of all transformations $\overline{\sigma} \in \mathrm{Aut}(F|\mathbb{F}_q)$ with $\sigma(x) = ax + b$ and $\sigma(y) = \epsilon y$ with $\epsilon^2 = a$ such that σ fixes the set $\{ (\alpha_i, \beta_i) \mid i = 1, 2, \ldots, N \}$.

Proof. It follows easily by Theorem 3.2.17 and by Proposition 4.2.5. □

Example 5. Let $\mathbb{F}_q = \mathbb{F}_5$ and $\mathbb{F}_{3125} = \mathbb{F}_5(\alpha)$ where α is an element such that $\alpha^5 + 4\alpha^4 + 3\alpha^3 + \alpha^2 + 2\alpha + 3 = 0$. Let

$\Phi = (P_{[\alpha^4+\alpha, 2\alpha^4+\alpha+2]}, \phi_{\alpha^4+\alpha, 2\alpha^4+\alpha+2}) + (P_{[\alpha^4+\alpha, 3\alpha^4+4\alpha+3]}, \phi_{\alpha^4+\alpha, 3\alpha^4+4\alpha+3})$

$+ (P_{[4\alpha^4+4\alpha+1, \alpha^4+3\alpha+1]}, \phi_{4\alpha^4+4\alpha+1, \alpha^4+3\alpha+1}) + (P_{[4\alpha^4+4\alpha+1, 4\alpha^4+2\alpha+4]}, \phi_{4\alpha^4+4\alpha+1, 4\alpha^4+2\alpha+4})$

be a Φ−divisor of the hyperelliptic function field $\mathbb{F}_q(x, y)|\mathbb{F}_q$ where $y^2 = x(x - \overline{1})(x - \overline{2})(x - \overline{3})(x - \overline{4})$. If $G = 9D_\infty$, then $C(\Phi, 9D_\infty, 5)$ is a 5−ary $[20, 8, d]$ code with $3 \leq d \leq 13$ (see Corollary 3.1.2). Moreover, $\mathcal{H}(\Phi; 9D_\infty; 5)$ is generated by the automorphism $\overline{\sigma}$ defined via $\overline{\sigma}(\frac{u(x,y)}{v(x,y)}) = \frac{u(4x+1,2y)}{v(4x+1,2y)}$ and so

$$\mathcal{H}(\Phi; 9D_\infty; 5) \simeq \mathbb{Z}_4.$$

Example 6. Let $\mathbb{F}_7(x, y)|\mathbb{F}_7$ be a hyperelliptic function field with $y^2 = x(x - \overline{1})(x - \overline{2})(x - \overline{3})(x - \overline{4})(x - \overline{5})(x - \overline{6})$. Let $\mathbb{F}_{q^n} = \mathbb{F}_{2401} = \mathbb{F}_7(\alpha)$ where α is an element such that $\alpha^4 + 5\alpha^3 + 2\alpha^2 + 3 = 0$. Let Φ be the sum of the next 42 ϕ−places of $\mathbb{F}_7(x, y)$

$(P_{[\alpha,\alpha]}, \phi_{\alpha,\alpha})$	$(P_{[\alpha,6\alpha]}, \phi_{\alpha,6\alpha})$	$(P_{[\alpha+1,\alpha]}, \phi_{\alpha+1,\alpha})$
$(P_{[\alpha+1,6\alpha]}, \phi_{\alpha+1,6\alpha})$	$(P_{[\alpha+2,\alpha]}, \phi_{\alpha+2,\alpha})$	$(P_{[\alpha+2,6\alpha]}, \phi_{\alpha+2,6\alpha})$

$(P_{[\alpha+3,\alpha]}, \phi_{\alpha+3,\alpha})$ $(P_{[\alpha+3,6\alpha]}, \phi_{\alpha+3,6\alpha})$ $(P_{[\alpha+4,\alpha]}, \phi_{\alpha+4,\alpha})$
$(P_{[\alpha+4,6\alpha]}, \phi_{\alpha+4,6\alpha})$ $(P_{[\alpha+5,\alpha]}, \phi_{\alpha+5,\alpha})$ $(P_{[\alpha+5,6\alpha]}, \phi_{\alpha+5,6\alpha})$
$(P_{[\alpha+6,\alpha]}, \phi_{\alpha+6,\alpha})$ $(P_{[\alpha+6,6\alpha]}, \phi_{\alpha+6,6\alpha})$ $(P_{[2\alpha,3\alpha]}, \phi_{2\alpha,3\alpha})$
$(P_{[2\alpha,4\alpha]}, \phi_{2\alpha,4\alpha})$ $(P_{[2\alpha+1,3\alpha]}, \phi_{2\alpha+1,3\alpha})$ $(P_{[2\alpha+1,4\alpha]}, \phi_{2\alpha+1,4\alpha})$
$(P_{[2\alpha+2,3\alpha]}, \phi_{2\alpha+2,3\alpha})$ $(P_{[2\alpha+2,4\alpha]}, \phi_{2\alpha+2,4\alpha})$ $(P_{[2\alpha+3,3\alpha]}, \phi_{2\alpha+3,3\alpha})$
$(P_{[2\alpha+3,4\alpha]}, \phi_{2\alpha+3,4\alpha})$ $(P_{[2\alpha+4,3\alpha]}, \phi_{2\alpha+4,3\alpha})$ $(P_{[2\alpha+4,4\alpha]}, \phi_{2\alpha+4,4\alpha})$
$(P_{[2\alpha+5,3\alpha]}, \phi_{2\alpha+5,3\alpha})$ $(P_{[2\alpha+5,4\alpha]}, \phi_{2\alpha+5,4\alpha})$ $(P_{[2\alpha+6,3\alpha]}, \phi_{2\alpha+6,3\alpha})$
$(P_{[2\alpha+6,4\alpha]}, \phi_{2\alpha+6,4\alpha})$ $(P_{[4\alpha,2\alpha]}, \phi_{4\alpha,2\alpha})$ $(P_{[4\alpha,5\alpha]}, \phi_{4\alpha,5\alpha})$
$(P_{[4\alpha+1,2\alpha]}, \phi_{4\alpha+1,2\alpha})$ $(P_{[4\alpha+1,5\alpha]}, \phi_{4\alpha+1,5\alpha})$ $(P_{[4\alpha+2,2\alpha]}, \phi_{4\alpha+2,2\alpha})$
$(P_{[4\alpha+2,5\alpha]}, \phi_{4\alpha+2,5\alpha})$ $(P_{[4\alpha+3,2\alpha]}, \phi_{4\alpha+3,2\alpha})$ $(P_{[4\alpha+3,5\alpha]}, \phi_{4\alpha+3,5\alpha})$
$(P_{[4\alpha+4,2\alpha]}, \phi_{4\alpha+4,2\alpha})$ $(P_{[4\alpha+4,5\alpha]}, \phi_{4\alpha+4,5\alpha})$ $(P_{[4\alpha+5,2\alpha]}, \phi_{4\alpha+5,2\alpha})$
$(P_{[4\alpha+5,5\alpha]}, \phi_{4\alpha+5,5\alpha})$ $(P_{[4\alpha+6,2\alpha]}, \phi_{4\alpha+6,2\alpha})$ $(P_{[4\alpha+6,5\alpha]}, \phi_{4\alpha+6,5\alpha})$.

If $G = 83D_\infty$, then $C(\Phi, 83D_\infty, 4)$ is a $7-$ary $[168, 81, d]$ code with $22 \leq d \leq 88$ (see Corollary 3.1.2). Moreover, $\mathcal{H}(\Phi; 83D_\infty; 4)$ is a group of order 42 whose presentation is

$$\mathcal{H}(\Phi; 14P_\infty; 2) = \langle\, \overline{\sigma}, \overline{\tau} \,|\, \overline{\sigma}^6, \overline{\sigma}^3\overline{\tau}^7, \overline{\sigma}\,\overline{\tau}\,\overline{\sigma}^5\overline{\tau}^5 \,\rangle$$

where $\overline{\sigma}(x, y) = (2x, 3y)$ and $\overline{\tau}(x, y) = (x + 1, 6y)$.

List of Notation

Symbol	*Meaning*
$F\|K$	algebraic function field, 4
F	field, 4
K	field, 4
$[F : K]$	degree of a field extension $F\|K$, 4
$\overline{K}$	algebraic closure of K, 5
$\mathcal{O}^*$	group of units of $\mathcal{O}$, 5
$\mathcal{O}$	valuation ring of $F\|K$, 5
P	place of $F\|K$, 5
F^*	$F \setminus \{ 0 \}$, 5
$\mathbb{P}_F$	set of places of $F\|K$, 5
$\mathbb{Z}$	rational integers, 6
v	discrete valuation of $F\|K$, 6
min	minimum of a set, 6
v_P	discrete valuation corresponding to a place P, 6

$\mathcal{O}_P$	valuation ring of P, 7
F_P	residue class field of P, 7
$x(P)$	residue class of $x \in \mathcal{O}_P$ in F_P, 7
$\deg P$	degree of P, 7
$\mathbb{P}_F^{(1)}$	set of rational places, 7
$\mathcal{D}_F$	divisor group of $F\|K$, 7
$\operatorname{supp} D$	support of the divisor D, 8
$A \leq B$	ordering of divisors, 8
$v_P(A)$	coefficient of P in the formal sum of the divisor A, 8
$\deg D$	degree of the divisor D, 8
$(z)_0$	zero divisor of z, 8
$(z)_\infty$	pole divisor of z, 8
(z)	principal divisor of z, 8
$\mathcal{L}(G)$	$\mathcal{L}-$space associated with the divisor G, 9
$\dim G$	dimension of the $\mathcal{L}-$space associated with G, 9
g	genus of a function field, 10
max	maximum of a set, 10
$\operatorname{Aut}(F\|K)$	automorphism group of a function field, 10
$\sigma(P)$	image of P through the automorphism σ, 10
$P'\|P$	P' lies over P, 12
$e(P'\|P)$	ramification index of $P'\|P$, 12
$f(P'\|P)$	relative degree of $P'\|P$, 13

$K(x)$	quotient field of $K[x]$, 13
$K[x]$	polynomial ring in the variable x over K, 13
$P_{p(x)}$	place of $K(x)\|K$ corresponding to $p(x)$, 14
$\mathcal{O}_{p(x)}$	valuation ring of $K(x)\|K$ corresponding to $p(x)$, 14
P_α	place of $K(x)\|K$ corresponding to $x-\alpha$, 14
P_∞	infinite place of $K(x)\|K$, 14
$\mathcal{O}_\infty$	valuation ring of $K(x)\|K$ corresponding to P_∞, 14
$v_{p(x)}$	discrete valuation corresponding to $p(x)$, 14
v_∞	discrete valuation corresponding to P_∞, 15
$\operatorname{char} K$	characteristic of K, 15
$\mathbb{F}_q$	finite field with q elements, 17
$\mathbb{F}_q^n$	$n-$dimensional vector space over $\mathbb{F}_q$, 17
$d(C)$	minimum distance of a code C, 17
$d(a,b)$	Hamming distance between a and b, 18
$w(c)$	weight of c, 18
[n,k,d]	parameters of a code, 18
$B_t(c)$	close sphere of radius t centered on c, 18
MDS	maximum distance separable code, 19
$C^\perp$	dual code, 19
S_n	symmetric group over n elements, 19
$\operatorname{Aut}(C)$	automorphism group of a code C, 19
$R(C)$	rate of a linear code, 20

$\delta(C)$	relative minimum distance, 20
$H_q(\delta)$	q-ary entropy function, 20
$C_{\mathcal{L}}(D, G)$	algebraic geometry code associated with D and G, 22
ev_D	evaluation map, 23
$G \sim_D G'$	$D-$equivalence of divisors, 25
$\mathrm{Aut}_{D,G}(F\|\mathbb{F}_q)$	stabilizer of D and G in $\mathrm{Aut}(F\|\mathbb{F}_q)$, 26
$\overline{P}$	conjugate of P, 37
(P, ϕ_P)	ϕ-place, 45
$\sigma(P, \phi_P)$	image of (P, ϕ_P) thought the automorphism σ, 46
$C(\Phi; G; n)$	GAG-code associated with Φ and G, 46
GAG-code	generalized algebraic geometry code, 47
$\mathcal{H}(\Phi; G; n)$	n-automorphism group of a GAG-code, 49
$G \sim_\Phi G'$	$\Phi-$equivalence of divisors, 50
$\mathrm{Aut}(F\|\mathbb{F}_q, \Phi, G)$	stabilizer of ϕ and G in $\mathrm{Aut}(F\|\mathbb{F}_q)$, 50
$\overline{\mathbb{F}_q}$	algebraic closure of the finite field $\mathbb{F}_q$, 68
ρ	Frobenius automorphism, 69
$\mathrm{Gal}(\mathbb{F}_{q^n}\|\mathbb{F}_q)$	Galois group of $\mathbb{F}_{q^n}\|\mathbb{F}_q$, 70
$\mathrm{Aut}(\mathcal{C})$	automorphism group of a curve $\mathcal{C}$, 81

Index

Bibliography

[Bro] A.E. Brouwer, *Bounds on minimum distance of linar codes*, [Online], available at http://www.win.tue.nl/∼aeb/voorlincod.html.

[D-N-X] C. Ding, H. Niederreiter and C.P. Xing, *Some New Codes from Algebraic Curves*, IEEE Trans. Inform. Theory, Vol. 46, No. 7, 2638-2642 (2000).

[Go] V.D. Goppa, *Codes on Algebraic Curves*, Soviet Math. Dokl. 24, No. 1, 170-172 (1981).

[H-K-T] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press, to appear.

[Hey] A.E. Heydtmann, *Generalized Geometric Goppa Codes*, Comm. Algebra 30, No. 6 2763-2789 (2002).

[J-K] D. Joyner and A. Ksir, *Automorphism group of some AG Codes*, available at http://arxiv.org/abs/AG/0412459, v2, (2005).

[Jun] D. Jungnickel, *Finite Fields-Structure and Arithmetics*, BI-Wiss.-Verlag, Maunheim, Leipzig, Wien, Zürich 1993.

[L-N] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Massachusetts, 1983.

[v.L] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, 1991.

[MacW-S] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Corrrecting Codes*, North-Holland, Amsterdam, 1997.

[Pas] D.S. Passman, *Permutation groups*, Benjamin, 1969.

[P-S] A. Picone and A.G. Spera, *Automorphisms of hyperelliptic GAG-codes*, Electron. Notes Discrete Math., Vol. 26, 123-130 (2006).

[Rom] S. Roman, *Field Theory*, Springer-Verlag, New York-Berlin-Heidelberg 1995.

[Sp1] A.G. Spera, *Asymptotically Good Codes from Generalized Algebraic-Geometric Codes*, Des. Codes Cryptogr., Vol. 37, No. 2, 305-312 (2005).

[Sp2] A.G. Spera, *On Automorphisms of generalized Algebraic-Geometry Codes*, To appear on J. Pure Appl. Algebra (2007).

[St1] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin-Heidelberg 1993.

[St2] H. Stichtenoth, *On Automorphisms of Geometric Goppa Codes*, J. Algebra 130, 113-121 (1990).

[Wes] S. Wesemeyer, *On the Automorphism Group of Various Goppa Codes*, IEEE Trans. Inform. Theory, Vol. 44, No. 2, 630-643 (1998).

[T-V] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer Acad. Publ., Dordrecht-Boston-London 1991.

[X1] C.P. Xing, *On Automorphism Groups of the Hermitian Codes*, IEEE Trans. Inform. Theory, Vol. 41, No. 6, 1629-1635 (1995).

[X2] C.P. Xing, *Automorphism Group of Elliptic Codes*, Comm. Algebra 23, No. 11 4061-4072 (1995).

[X-N-L] C.P. Xing, H. Niederreiter and K.Y. Lam, *A Generalization of Algebraic-Geometric Codes*, IEEE Trans. Inform. Theory, Vol. 45, No. 7, 2438-2501 (1999).