DOI: 10.2478/auom-2023-0040
An. Şt. Univ. Ovidius Constanţa **Vol. 31(3),2023, 221–227**

On a relation between GAG codes and AG codes

Engin Şenel and Figen Öke

Abstract

In this paper, we first give a relationship between generalized algebraic geometry codes (GAG codes) and algebraic geometry codes (AG codes). More precisely, we show that a GAG code is contained (up to isomorphism) in a suitable AG code. Next we recall the concept of an N_1N_2-automorphism group, a subgroup of the automorphism group of a GAG code. With the use of the relation we obtained between these two classes of codes, we show that the N_1N_2-automorphism group is a subgroup of the automorphism group of an AG code.

1 Introduction

AG codes were first constructed by V. D. Goppa using the function field theory [1]. GAG codes, inspired by the structure of AG codes, were constructed by C.P. Xing, H. Niederreiter and K.Y. Lam to use places of degrees greater than one [5]. A direct relationship between these two code families was given by A. Picone [2]. A. Picone showed that a GAG code generated by places of the same degree can be embedded into a suitable AG code and established a connection between an automorphism group of a GAG code of this type and an automorphism group of an AG code. In this paper, we extend the Picone's results to GAG codes generated by places of different degrees. Our main tool

Key Words: Algebraic geometry codes, generalized algebraic geometry codes, geometric Goppa codes, code automorphisms, algebraic function fields.
2010 Mathematics Subject Classification: Primary 94B27; Secondary 14H05, 14G50.
Received: 10.09.2022
Accepted: 20.12.2022

is the algebraic extensions of function fields. We mainly use the method given in Section 3 of [2]. The paper is organized as follows.

In Section 2, we state the necessary definitions and give some preliminary results. In Section 3, we construct a connection between the corresponding function fields of a GAG code and an AG code. Next we present the first main result of this paper. In Section 4, we consider a constrained structure that still allows GAG codes to be generated by places of different degrees. We recall the concept of an N_1N_2-automorphism group defined by E. Şenel and F. Öke [4]. Using the arguments given in Section 3, we show that the N_1N_2-automorphism group is a subgroup of the automorphism group of a suitable AG code.

2 Preliminaries

We start by giving the basic definitions of algebraic function field theory. For the notations not explained in this paper, we refer the reader to [3].

Definition 2.1. *For a transcendental element $x \in F$ over K, let F be a finite extension of $K(x)$. The field extension $K \subseteq F$ is called an algebraic function field F/K of one variable over K.*

We sometimes simply call F/K a function field. Throughout this paper, algebraic function fields of one variable are considered. Any algebraic function field of one variable is usually expressed as a simple algebraic field extension of the field $K(x)$. Hence for an irreducible polynomial $f(T) \in K(x)[T]$ such that $f(y) = 0$, we write $F = K(x, y)$ when it is needed.

The field $\tilde{K} := \{z \in F \mid z \text{ is algebraic over } K\}$ is called the *field of constants* of F/K. If $\tilde{K} = K$, we say that K is the *full constant field*.

In the rest of the paper, F/K denotes a function field with full constant field K. This assumption is not a restriction of generality (see [3, p. 15]).

In the applications of function fields to coding theory, the function fields over finite fields are used. We introduce AG codes. Let $\mathbb{F}_q$ be a finite field with q elements and let $F/\mathbb{F}_q$ be a function field. Consider the divisor $D := P_1 + P_2 + \cdots + P_N$ where $P_1, P_2, \ldots, P_N$ are pairwise distinct rational places and a divisor G with $\operatorname{supp} G \cap \{P_1, P_2, \ldots, P_N\} = \emptyset$. The linear code

$$C_{\mathcal{L}}(D, G) := \{(z(P_1), z(P_2), \ldots, z(P_N)) \mid z \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^N$$

is called an *algebraic geometry* code.

Next we introduce GAG codes. We now present some notations given in [2] that are not relevant for our exposition, but make the structure of GAG codes and the results easier to understand. For a place P of degree n of the function field $F/\mathbb{F}_q$, we know that the residue class field F_P is $\mathbb{F}_q$-isomorphic to $\mathbb{F}_{q^n}$. For such an isomorphism $\phi_P : F_P \longrightarrow \mathbb{F}_{q^n}$, the pair (P, ϕ_P) is called a *ϕ-place*. A *ϕ-divisor* is defined as an element of the free abelian group generated by ϕ-places. We define $z(P, \phi_P) := \phi_P(z(P))$, where z is an element of the valuation ring $\mathcal{O}_P$ corresponding to the place P. Note that since $\mathbb{F}_q^n$ and $\mathbb{F}_{q^n}$ are isomorphic, $z(P, \phi_P)$ can be considered as an element of $\mathbb{F}_q^n$.

Consider the ϕ-divisor $\varPhi := (P_1, \phi_1) + (P_2, \phi_2) + \cdots + (P_N, \phi_N)$ where $(P_1, \phi_1), (P_2, \phi_2), \ldots, (P_N, \phi_N)$ are pairwise distinct ϕ-places of degree $n_i \geq 1$ respectively and a divisor G with $\operatorname{supp} G \cap \{P_1, P_2, \ldots, P_N\} = \emptyset$. The linear code

$$C(\varPhi; G) := \{(z(P_1, \phi_1), \ldots, z(P_N, \phi_N)) \mid z \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^{\sum_{i=1}^{N} n_i} \simeq \prod_{i=1}^{N} \mathbb{F}_q^{n_i}$$

is called an *generalized algebraic geometry* code. For a suitable divisor G, we also say that the GAG code $C(\varPhi; G)$ is generated by the places $P_1, P_2, \ldots, P_N$. Notice that the definition of GAG codes given above is not in the most general state given in [5].

Now we recall some definitions and facts about algebraic extensions of function fields that will be needed in the next chapters. The field K is assumed to be perfect.

Definition 2.2. *Let $F \subseteq F'$ be an algebraic field extension and let $K \subseteq K'$. The algebraic function field F'/K' is called an algebraic extension of F/K. If $F' = FK'$, the composite field of F and K' then F'/K' is called a constant field extension.*

Let F'/K' be an algebraic extension of the function field F/K. Consider the residue class fields $F_P = \mathcal{O}_P/P$ and $F'_{P'} = \mathcal{O}_{P'}/P'$ where $P \in \mathcal{P}_F$ and $P' \in \mathcal{P}_{F'}$. If P lies over P', then by [3, Proposition 3.1.4], we have the following canonical embedding of F_P into $F'_{P'}$

$$\varphi : F_P \longrightarrow F'_{P'}\,,\ x(P) \longmapsto x(P') \tag{2.1}$$

where $x \in \mathcal{O}_P$. So, we consider F_P as a subfield of $F'_{P'}$.

The next theorem gives the relation between a divisor $A \in \operatorname{Div}(F)$ and its conorm $\operatorname{Con}_{F'/F}(A) \in \operatorname{Div}(F')$ and is important for our purposes.

Theorem 2.3. *([3, Theorem 3.6.3]) Consider the constant field extension F'/K' of the function field F/K.*

(1) For every divisor $A \in \operatorname{Div}(F)$, we have $\deg \operatorname{Con}_{F'/F}(A) = \deg A$

(2) For every divisor $A \in \operatorname{Div}(F)$,

$$\ell(\operatorname{Con}_{F'/F}(A)) = \ell(A).$$

More explicitly, every basis of $\mathcal{L}(A)$ *is also a basis of* $\mathcal{L}(\operatorname{Con}_{F'/F}(A))$. *Also, one should note that* $\mathcal{L}(A) \subseteq F$ *is a* K*-vector space whereas* $\mathcal{L}(\operatorname{Con}_{F'/F}(A)) \subseteq F'$ *is a* K'*-vector space.*

3 GAG codes and AG codes

We provide some needed tools to prove the first main result of this paper. We start by introducing a useful vector space. Let $\mathbb{F}_q(x,y)/\mathbb{F}_q$ be a function field. Let $\varPhi = \sum_{i=1}^{N} (P_i, \phi_i)$ be a ϕ-divisor of $\mathbb{F}_q(x,y)/\mathbb{F}_q$ with P_i pairwise distinct places of degree $n_i \geq 1$ such that $x, y \in \mathcal{O}_{P_i}$ and let G be a divisor with $\operatorname{supp} G \cap \{P_1, P_2, \ldots, P_N\} = \emptyset$. Consider the GAG code $C(\varPhi; G)$.

Since $\deg P_i = n_i$, we have $z(P_i, \phi_i) \in \mathbb{F}_{q^{n_i}}$ for every $i \in \{1, 2, \ldots, N\}$. Then we have the following $\mathbb{F}_q$-vector space,

$$\overline{C}(\varPhi; G) := \{(z(P_1, \phi_1), \ldots, z(P_N, \phi_N)) \mid z \in \mathcal{L}(G)\} \subseteq \prod_{i=1}^{N} \mathbb{F}_{q^{n_i}}.$$

Hence we can define the following $\mathbb{F}_q$-isomorphism,

$$\begin{aligned} \varphi : \overline{C}(\varPhi; G) &\longrightarrow C(\varPhi; G) \\ (z(P_1, \phi_1), \ldots, z(P_N, \phi_N)) &\longmapsto (\lambda_1(z(P_1, \phi_1)), \ldots, \lambda_N(z(P_N, \phi_N))) \end{aligned}$$

where λ_i is a $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^{n_i}}$ onto $\mathbb{F}_q^{n_i}$.

Next with the use of the $\mathbb{F}_q$-vector space $\overline{C}(\varPhi; G)$, we show that the GAG code $C(\varPhi; G)$ can be embedded into an AG code.

From [2, Proposition 3.5], we know that for every $i \in \{1, 2, \ldots, N\}$, there is a rational place R_i of the constant field extension $\mathbb{F}_{q^{n_i}}(x,y)/\mathbb{F}_{q^{n_i}}$ which lies over (P_i, ϕ_i) such that $z(R_i) = z(P_i, \phi_i)$ for each $z \in \mathcal{O}_{P_i}$. Now consider the constant field extension $\mathbb{F}_{q^{\operatorname{lcm}(n_1, \ldots, n_N)}}(x,y)/\mathbb{F}_{q^{\operatorname{lcm}(n_1, \ldots, n_N)}}$ of $\mathbb{F}_{q^{n_i}}(x,y)/\mathbb{F}_{q^{n_i}}$. We have a place S_i of $\mathbb{F}_{q^{\operatorname{lcm}(n_1, \ldots, n_N)}}(x,y)/\mathbb{F}_{q^{\operatorname{lcm}(n_1, \ldots, n_N)}}$ which lies over R_i by [3, Proposition 3.1.7]. Since R_i is rational, S_i is rational by (1) of Theorem 2.3.

Also, by [2, Proposition 3.5] and the canonical embedding given in (2.1), for every $i \in \{1, 2, \ldots, N\}$ we have

$$z(S_i) = z(R_i) = z(P_i, \phi_i) \tag{3.1}$$

where $z \in \mathcal{O}_{P_i}$.

Now we can state and prove the first main result of this paper, which is a generalization of [2, Proposition 3.6].

Theorem 3.1. *With S_i as above for each $i \in \{1, 2, \ldots, N\}$, let $D' = S_1 + \cdots + S_N$. Consider the AG code $C_{\mathcal{L}}(D', G')$ where $G' \in \mathrm{Div}(\mathbb{F}_{q^{\mathrm{lcm}(n_1,\ldots,n_N)}}(x, y))$ is the conorm of the divisor $G \in \mathrm{Div}(\mathbb{F}_q(x, y))$. Then we have*

$$\overline{C}(\Phi; G) \subseteq C_{\mathcal{L}}(D', G').$$

Hence, the AG code $C_{\mathcal{L}}(D', G')$ contains a subspace which is $\mathbb{F}_q$-isomorphic to the GAG code $C(\Phi; G)$.

Proof. If $z \in \mathcal{L}(G)$, then $z \in \mathcal{O}_{P_i}$ for each $i \in \{1, 2, \ldots, N\}$. Hence by (3.1), we have

$$\overline{C}(\Phi; G) = \{(z(S_1), z(S_2), \ldots, z(S_N)) \mid z \in \mathcal{L}(G)\}.$$

Since $\mathcal{L}(G) \subseteq \mathcal{L}(G')$ from (2) of Theorem 2.3, the result follows. □

4 The automorphisms

In this section, with the notation as in Theorem 3.1 we show that the automorphism groups of $C(\Phi; G)$ and $C_{\mathcal{L}}(D', G')$ have the same subgroup. For this purpose, we restrict the structure of GAG codes in the following sense: let $\{P_1, P_2, \ldots, P_{N_1}\}$ be a set of pairwise distinct places of degree $n_1 \geq 1$ and let $\{P_{N_1+1}, P_{N_1+2}, \ldots, P_{N_1+N_2}\}$ be a set of pairwise distinct places of degree $n_2 \geq 1$. Consider the ϕ-divisor $\Phi = \sum_{i=1}^{N_1+N_2} (P_i, \phi_i)$ and a divisor G with $\mathrm{supp}\, G \cap \{P_1, P_2, \ldots, P_{N_1+N_2}\} = \emptyset$. For the rest of this section, we consider the GAG code $C(\Phi; G)$.

Next we recall the definition of an automorphism group of a code and introduce the concept of an N_1N_2-automorphism group of a GAG code given in [4]. The automorphism group of a code C of length n is

$$\mathrm{Aut}(C) = \{\pi \in \mathcal{S}_n \mid \pi(C) = C\}$$

where $\mathcal{S}_n$ is the symmetric group on n elements. It should be noted that $\mathrm{Aut}(C(\Phi; G)) \subseteq \mathcal{S}_{n_1N_1+n_2N_2}$, since the length of the code $C(\Phi; G)$ is $n_1N_1 + n_2N_2$. We know that for each $i \in \{1, 2, \ldots, N_1\}$ (respectively $i \in \{N_1+1, N_1+2, \ldots, N_1+N_2\}$), we have $z(P_i, \phi_i) \in \mathbb{F}_q^{n_1}$ (respectively $z(P_i, \phi_i) \in \mathbb{F}_q^{n_2}$). So we can assume that a codeword of the code $C(\Phi; G)$ consists of $N_1 + N_2$ blocks. By interchanging the first N_1 blocks and the other N_2 blocks among themselves, respectively, an element of the symmetric group $\mathcal{S}_{n_1N_1+n_2N_2}$ is obtained. The subgroup of $\mathrm{Aut}(C(\varPhi;G))$ that provides this property will be called an N_1N_2-automorphism group and denoted by $\mathcal{H}_{N_1N_2}(\varPhi;G)$. An element $\pi \in \mathcal{H}_{N_1N_2}(\varPhi;G)$ acts on a codeword of $C(\varPhi;G)$ in the following way:

$$\begin{aligned}&\pi\left(z(P_1,\phi_1),\dots,z(P_{N_1+N_2},\phi_{N_1+N_2})\right)\\ &=\left(z(P_{\pi(1)},\phi_{\pi(1)}),\dots,z(P_{\pi(N_1+N_2)},\phi_{\pi(N_1+N_2)})\right)\end{aligned}$$

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

We give the main theorem of this section, which is a generalization of [2, Proposition 3.7] to a broader class of the automorphism groups of GAG codes.

Theorem 4.1. *N_1N_2-automorphism group $\mathcal{H}_{N_1N_2}(\varPhi;G)$ is a subgroup of the automorphism group of $C_{\mathcal{L}}(D',G')$.*

Proof. First we recall the automorphism group of $C_{\mathcal{L}}(D',G')$

$$\begin{aligned}\mathrm{Aut}(C_{\mathcal{L}}(D',G')) =&\{\pi \in \mathcal{S}_{N_1+N_2} \mid (z(S_{\pi(1)}),\dots,z(S_{\pi(N_1+N_2)})) \in C_{\mathcal{L}}(D',G')\\ &\text{for each } z \in \mathcal{L}(G')\}.\end{aligned}$$

Let $\pi \in \mathcal{H}_{N_1N_2}(\varPhi;G)$. Since $\mathbb{F}_q^{n_i}$ and $\mathbb{F}_{q^{n_i}}$ are isomorphic for $i \in \{1,2,\dots,N_1+N_2\}$, the action of an element of $\mathcal{H}_{N_1N_2}(\varPhi;G)$ on $\overline{C}(\varPhi;G)$ is same as on $C(\varPhi;G)$. So for an element $\frac{u(x,y)}{v(x,y)} \in \mathcal{L}(G)$, we have

$$\left(\frac{u(x,y)}{v(x,y)}(P_{\pi(1)},\phi_{\pi(1)}),\dots,\frac{u(x,y)}{v(x,y)}(P_{\pi(N_1+N_2)},\phi_{\pi(N_1+N_2)})\right) \in \overline{C}(\varPhi;G).$$

Thus there is some element $\frac{u'(x,y)}{v'(x,y)} \in \mathcal{L}(G)$ such that $\frac{u(x,y)}{v(x,y)}(P_{\pi(i)},\phi_{\pi(i)}) = \frac{u'(x,y)}{v'(x,y)}(P_i,\phi_i)$ for each $i \in \{1,2,\dots,N_1+N_2\}$. Hence, from (3.1) it follows that $\frac{u(x,y)}{v(x,y)}(S_{\pi(i)}) = \frac{u'(x,y)}{v'(x,y)}(S_i)$ for each $i \in \{1,2,\dots,N_1+N_2\}$.

Let $B = \left\{\frac{u_1(x,y)}{v_1(x,y)},\frac{u_2(x,y)}{v_2(x,y)},\dots,\frac{u_r(x,y)}{v_r(x,y)}\right\}$ be a basis of $\mathcal{L}(G)$. Then for any $j \in \{1,2,\dots,r\}$, there exists an element $\frac{u_j'(x,y)}{v_j'(x,y)} \in \mathcal{L}\,(G)$ such that $\frac{u_j(x,y)}{v_j(x,y)}(S_{\pi(i)}) = \frac{u_j'(x,y)}{v_j'(x,y)}(S_i)$ for each $i \in \{1,2,\dots,N_1+N_2\}$.

Since B is also a base of $\mathcal{L}(G')$ by (2) of Theorem 2.3, for an $z \in \mathcal{L}(G')$, we can write $z = \sum_{j=1}^{r} a_j \frac{u_j(x,y)}{v_j(x,y)}$ where $a_j \in \mathbb{F}_{q^{\mathrm{lcm}\,(n_1,n_2)}}$. Hence for each

$i \in \{1, 2, \ldots, N_1 + N_2\}$, we have

$$\begin{aligned} z(S_{\pi(i)}) &= \left(\sum_{j=1}^{r} a_j \frac{u_j(x,y)}{v_j(x,y)}\right)(S_{\pi(i)}) = \sum_{j=1}^{r} a_j \left(\frac{u_j(x,y)}{v_j(x,y)}(S_{\pi(i)})\right) \\ &= \sum_{j=1}^{r} a_j \left(\frac{u'_j(x,y)}{v'_j(x,y)}(S_i)\right) = \left(\sum_{j=1}^{r} a_j \frac{u'_j(x,y)}{v'_j(x,y)}\right)(S_i). \end{aligned}$$

Since $\sum_{j=1}^{r} a_j \frac{u'_j(x,y)}{v'_j(x,y)} \in \mathcal{L}(G')$, it follows that $\pi \in \mathrm{Aut}(C_{\mathcal{L}}(D', G'))$. So we have $\mathcal{H}_{N_1 N_2}(\varPhi; G) \subseteq \mathrm{Aut}(C_{\mathcal{L}}(D', G'))$. □

References

[1] V. D. Goppa, *Codes on algebraic curves*, Sov. Math. Dokl., 24(1) (1981), 170172.

[2] A. Picone, *New lower bounds for the minimum distance of generalized algebraic geometry codes*, J. Pure Appl. Algebr., 217(6) (2013), 1164-1172.

[3] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, (2009).

[4] E. Şenel, F. Öke, *On the automorphisms of generalized algebraic geometry codes*, Des. Codes Cryptogr., 90(6) (2022), 1369-1379.

[5] C. P. Xing, H. Niederreiter, K. Y. Lam, *A generalization of algebraic-geometry codes*, IEEE Trans. Inf. Theory, 45(7) (1999), 24982501.

Engin ŞENEL,
Department of Mathematics,
Trakya University,
22030 Edirne, Türkiye.
Email: enginsenel@trakya.edu.tr

Figen ÖKE,
Department of Mathematics,
Trakya University,
22030 Edirne, Türkiye.
Email: figenoke@trakya.edu.tr