doi:10.3934/amc.2021018

THE CONORM CODE OF AN AG-CODE

María Chara *

Researcher of CONICET at Facultad de Ingeniería Química, (UNL)
Santiago del Estero 2829
(3000) Santa Fe, Argentina

Ricardo A. Podestá

FaMAF – CIEM (CONICET), Universidad Nacional de Córdoba
Av. Medina Allende 2144
(5000) Córdoba, Argentina.

Ricardo Toledano

Facultad de Ingeniería Química, (UNL)
Santiago del Estero 2829
(3000) Santa Fe, Argentina

(Communicated by Daniele Bartoli)

Abstract. Given a suitable extension F'/F of algebraic function fields over a finite field $\mathbb{F}_q$, we introduce the conorm code $\mathrm{Con}_{F'/F}(\mathcal{C})$ defined over F' which is constructed from an algebraic geometry code $\mathcal{C}$ defined over F. We study the parameters of $\mathrm{Con}_{F'/F}(\mathcal{C})$ in terms of the parameters of $\mathcal{C}$, the ramification behavior of the places used to define $\mathcal{C}$ and the genus of F. In the case of unramified extensions of function fields we prove that $\mathrm{Con}_{F'/F}(\mathcal{C})^\perp = \mathrm{Con}_{F'/F}(\mathcal{C}^\perp)$ when the degree of the extension is coprime to the characteristic of $\mathbb{F}_q$. We also study the conorm of cyclic algebraic-geometry codes and we show that some repetition codes, Hermitian codes and all Reed-Solomon codes can be represented as conorm codes.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements. For a given trascendental element x over $\mathbb{F}_q$, the field of fractions of the ring $\mathbb{F}_q[x]$ is denoted as $\mathbb{F}_q(x)$ and it is called a rational function field over $\mathbb{F}_q$. An (algebraic) function field F of one variable over $\mathbb{F}_q$ is a field extension $F/\mathbb{F}_q(x)$ of finite degree where $x \in F$ is a trascendental element over $\mathbb{F}_q$. The finite field $\mathbb{F}_q$ is called the field of constants of F and we will always assume that $\mathbb{F}_q$ is the full constant field of F, that is $\mathbb{F}_q$ is algebraically closed in F. We will frequently use the symbol $F/\mathbb{F}_q$ to express that F is a function field over $\mathbb{F}_q$.

Let $F/\mathbb{F}_q$ be a function field. The *Riemann-Roch space* associated to a divisor G of F is the vector space over $\mathbb{F}_q$ defined as

$$\mathcal{L}(G) = \{x \in F : (x) \geq G\} \cup \{0\},$$

2020 *Mathematics Subject Classification:* Primary: 94B27; Secondary: 94B15, 14H05.
Key words and phrases: AG-codes, cyclic codes, conorm, algebraic function fields.
Partially supported by CONICET, UNL CAI+D 2016, SECyT-UNC, CSIC.
* Corresponding author: María Chara.

where (x) denotes the principal divisor of x. It turns out that $\mathcal{L}(G)$ is a finite dimensional vector space over $\mathbb{F}_q$ for any divisor G of F (see, for instance, Proposition 1.4.9 of [8]).

The *dimension* $\ell(G)$ of a divisor G of F is defined as the dimension of $\mathcal{L}(G)$ as a vector space over $\mathbb{F}_q$. An important result in the theory of algebraic function fields relates the dimension of some divisors and the genus of the considered function field. More precisely (see Theorem 1.5.15 of [8]) given a function field $F/\mathbb{F}_q$ of genus g, a divisor G and a canonical divisor W of F, the Riemann-Roch Theorem asserts that

$$\ell(G) = \deg(G) + 1 - g + \ell(W - G).$$

Given disjoint divisors $D = P_1 + \cdots + P_n$ and G of $F/\mathbb{F}_q$, where $P_1, \ldots, P_n$ are different rational places, the *algebraic geometry code* (AG-code for short) associated to D and G is defined as

$$C_{\mathcal{L}}^F(D,G) = \{(x(P_1), \ldots, x(P_n)) \,:\, x \in \mathcal{L}(G)\} \subseteq (\mathbb{F}_q)^n, \tag{1}$$

where $x(P_i)$ denotes the residue class of x modulo P_i for $i = 1, \ldots, n$. If the context is clear, we will simply write $C_{\mathcal{L}}$ instead of $C_{\mathcal{L}}^F(D,G)$.

It is well known (see Theorem 2.2.2 of [8]) that $C_{\mathcal{L}}(D,G)$ is an $[n,k,d]$-code with $k = \ell(G) - \ell(G - D)$ and

$$d \geq n - \deg G. \tag{2}$$

Also, if $\deg G < n$, then

$$k = \ell(G) \geq \deg G + 1 - g \tag{3}$$

and hence $k + d \geq n + 1 - g$. If, in addition $2g - 2 < \deg G$, we have the equality $k = \deg G + 1 - g$.

The *designed distance* of the code is $d^* = n - \deg G$ and, similarly, one can define its *designed dimension* as

$$k^* = \deg G + 1 - g. \tag{4}$$

Thus $d \geq d^*$ and if $\deg G < n$ then $k \geq k^*$, with equality if $2g - 2 < \deg G$.

From these facts, we see that if $\deg G > 2g - 2$, then the dimension of $C_{\mathcal{L}}(D,G)$ can be computed in an exact way knowing the degree of G and the genus of F. On the other hand, if $\deg G \leq 2g - 2$, then $\ell(D - G)$ does not vanish and no formula is available to compute the dimension of $C_{\mathcal{L}}(D,G)$.

Sometimes it is useful to distinguish 3 levels of AG-codes. Let $\mathcal{C} = C_{\mathcal{L}}(D,G)$ be as in (1). If $\deg G < n$ we will say that $\mathcal{C}$ is a *moderate* AG-code (or *MAG-code*). A moderate AG-code which also satisfies $2g - 2 < \deg G$ will be called a *strong* AG-code (or *SAG-code*). Finally, a *weak* AG-code (or *WAG-code*) will be an AG-code which is not moderate.

The main goals of this paper are to introduce the concept of the conorm code associated to an AG-code, to study some interesting properties of this new code and to show that some well known families of codes such as repetition codes, Hermitian codes and Reed-Solomon codes can be obtained as conorm codes from other more basic codes.

Outline and results. In Section 2, given a suitable extension F'/F of functions fields $F'/\mathbb{F}_{q^t}$ and $F/\mathbb{F}_q$, we define the q^t-ary conorm code $\mathcal{C}' = C_{\mathcal{L}}^{F'}(D', G')$ of the q-ary AG-code $\mathcal{C} = C_{\mathcal{L}}^F(D,G)$ by lifting the code $\mathcal{C}$ using the conorm map of divisors. We denote this code as

$$\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C}).$$

If the context is clear, we will simply write $\mathrm{Con}(\mathcal{C})$ instead of $\mathrm{Con}_{F'/F}(\mathcal{C})$.

In the next section we deal with the parameters and levels of conorm codes. In Proposition 1 and Corollary 1 we give bounds for the parameters of $\mathcal{C}'$ in terms of the parameters of $\mathcal{C}$. Then, we consider conorm codes defined over geometric extensions, that is extensions of function fields F'/F having both the same field of constants $\mathbb{F}_q$ (i.e. $t = 1$) and we study the AG-levels of the construction (see Corollary 2).

In Section 4, we study conorm codes defined over unramified extensions and duality. In general, the dual of the conorm code is not the conorm of the dual code (see Example 5). However, over unramified extensions, this is indeed the case under some conditions. More precisely, in Theorem 4.1 we show that if F'/F is an unramified geometric extension of degree m of function fields over $\mathbb{F}_q$ then

$$\mathrm{Con}(\mathcal{C}^\perp) = \mathrm{Con}(\mathcal{C})^\perp$$

holds provided that $(m, q) = 1$.

In Section 5, we consider the conorm of cyclic AG-codes. We show that, under certain conditions this construction preserves cyclicity. In the particular case that F'/F is a geometric Galois extension of function fields over $\mathbb{F}_q$ and every place in the support of a divisor D of F is totally ramified in F', the conorm code $\mathcal{C}' = \mathrm{Con}(C_\mathcal{L}^F(D,G))$ defined over F' and the AG-code $C_\mathcal{L}^F(D,G)$ are different representations of the same algebraic geometry code over $\mathbb{F}_q$ (see Theorem 5.5). We believe this may have some applications on code-based cryptography.

Finally, in the last section we show that in some general cases, repetition codes, Hermitian codes and Reed-Solomon codes can be represented as conorm codes, i.e. they can be seen as the conorm code of simpler AG-codes defined over function fields of smaller genus.

2. The conorm code of an AG-code

Let $F/\mathbb{F}_q$ be a function field and let us denote as usual the set of places of F by $\mathbb{P}(F)$ and the abelian group of divisors of F by $\mathrm{Div}(F)$. Let $F'/\mathbb{F}_{q^t}$ be a function field such that F'/F is a finite extension. We will show how to construct an AG-code $\mathcal{C}' = C_\mathcal{L}^{F'}(D', G')$ over $\mathbb{F}_{q^t}$ starting from an AG-code $\mathcal{C} = C_\mathcal{L}^F(D,G)$ over $\mathbb{F}_q$. This will be accomplished by using the conorm map on divisors

$$\mathrm{Con}_{F'/F} : \mathrm{Div}(F) \to \mathrm{Div}(F'),$$

that we now recall. If P is a place in F, the conorm divisor of P is the divisor

$$\mathrm{Con}_{F'/F}(P) = \sum_{P'|P} e(P'|P)\, P'$$

in F', where $e(P'|P)$ is the *ramification index* of the place P' in F' over P. For $Q \in \mathbb{P}(F)$ and $A = \sum_P n_P P \in \mathrm{Div}(F)$ we define $v_Q(A) = n_Q$. Now, the *conorm divisor* of A in F' is given by

$$A' := \mathrm{Con}_{F'/F}(A) = \sum_P n_P \,\mathrm{Con}_{F'/F}(P). \tag{5}$$

From now on the extension F'/F is a function field extension of degree m. Let $\mathcal{C} = C_\mathcal{L}^F(D,G)$ be an AG-code of length n defined over $\mathbb{F}_q$, where G and $D = P_1 + \cdots + P_n$ are disjoint divisors and $P_1, \ldots, P_n$ are different rational places of F. For any place P in the support of D let us denote by $m_P \in \{1, \ldots, m\}$ the number of different places of F' over P. Suppose that the extension F'/F is such that for every place P in the support of D we have that

$$e(P'|P) = \frac{m}{m_P}, \tag{6}$$

for any place P' of F' lying above P. Then all the places of F' lying above P_i are rational for $i = 1, \ldots, n$. Denote by

$$Q_i^{(1)}, \ldots, Q_i^{(m_{P_i})} \tag{7}$$

the rational places of F' lying above P_i and put

$$D_i = Q_i^{(1)} + \cdots + Q_i^{(m_{P_i})}. \tag{8}$$

Note that by (5) we have

$$\mathrm{Con}_{F'/F}(P_i) = \tfrac{m}{m_{P_i}} \sum_{j=1}^{m_{P_i}} Q_i^{(j)} = \tfrac{m}{m_{P_i}} D_i$$

and since D and G are disjoint divisors of F then $\mathrm{Con}_{F'/F}(D)$ and $\mathrm{Con}_{F'/F}(G)$ are disjoint divisors of F'.

With the above notation we have the following definition of an AG-code "hanging over" another one.

Definition 2.1. Given a code $\mathcal{C} = C_{\mathcal{L}}^F(D, G)$ as in (1) and a finite extension F'/F of function fields such that (6) holds, we define the conorm code associated to $\mathcal{C}$, or just the *conorm of* $\mathcal{C}$, as

$$\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C}) = C_{\mathcal{L}}^{F'}(D', G'), \tag{9}$$

where

$$D' = \tfrac{1}{m} \sum_{i=1}^{n} m_{P_i} \, \mathrm{Con}_{F'/F}(P_i) \qquad \text{and} \qquad G' = \mathrm{Con}_{F'/F}(G).$$

That is, in the notation of (7) and (8),

$$D' = D_1 + \cdots + D_n = \sum_{i=1}^{n} (Q_i^{(1)} + \cdots + Q_i^{(m_{P_i})}).$$

When F'/F is understood, we will write $\mathrm{Con}(\mathcal{C})$ instead of $\mathrm{Con}_{F'/F}(\mathcal{C})$. Similarly for $\mathrm{Con}_{F'/F}(P_i)$ and $\mathrm{Con}_{F'/F}(G)$.

Clearly $\mathcal{C}'$ is an AG-code defined over F'. For $m = 1$ the construction is trivial and $\mathcal{C}' = \mathcal{C}$. By Hurwitz genus formula (see Theorem 3.4.13 of [8]), the genus $g' = g(F')$ of F' is given by

$$g' = \tfrac{m}{t}(g - 1) + \tfrac{1}{2} \deg \mathrm{Diff}(F'/F) + 1, \tag{10}$$

where $g = g(F)$ is the genus of F and

$$\mathrm{Diff}(F'/F) = \sum_{P} \sum_{P'|P} d(P'|P) \, P',$$

is the *different divisor* of F'/F with $d(P'|P)$ the *different exponent* of P' over P. Hence, since $d(P'|P) \geq 0$ for every $P'|P$, we have

$$g' = g(F') \geq g(F) = g. \tag{11}$$

3. Parameters and levels

We study now some parameters and levels of the conorm code $\mathrm{Con}(\mathcal{C})$ of an AG-code $\mathcal{C}$ in different situations. We begin with the following elementary estimates for the parameters of a conorm code.

Proposition 1. *Let $F'/\mathbb{F}_{q^t}$ and $F/\mathbb{F}_q$ be two function fields such that F'/F is a finite extension of degree $m \geq 2$. Let $[n,k,d]$ and $[n',k',d']$ be the parameters of $\mathcal{C} = C_{\mathcal{L}}(D,G)$ and $\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C})$ respectively, where $D = P_1 + \cdots + P_n$. Then*

$$n \leq n' \leq mn, \tag{12}$$

and

$$d' \geq n' - \tfrac{m}{t} \deg G. \tag{13}$$

Moreover if $\mathcal{C}'$ is a MAG-code (i.e. $\deg G' < n'$) then

$$k' \geq \tfrac{m}{t} k^* - \tfrac{1}{2} \deg \mathrm{Diff}(F'/F), \tag{14}$$

where $k^* = \deg G + 1 - g$ is the designed dimension given in (4).

Proof. We see at once that (12) holds because $n' = \# \mathrm{Supp}(D')$ and, by definition of the conorm code, we have

$$n' = \sum_{i=1}^{n} m_{P_i},$$

where $1 \leq m_{P_i} \leq m$ for $i = 1, \ldots, n$.

We prove now the lower bounds (13) and (14). By (2) we have that

$$d' \geq n' - \deg G'.$$

We see that (13) holds because from Corollary 3.1.14 in [8] we have

$$\deg G' = \tfrac{m}{t} \deg G. \tag{15}$$

Finally from (3) we have that if $\deg G' < n'$ then $k' \geq \deg G' + 1 - g'$. From this, and using (10) and (15), we see that (14) also holds. □

With the same hypothesis of Proposition 1 we have the following

Corollary 1. *Let s (resp. r) be the number of places P_i in $D = P_1 + \cdots + P_n$ which split completely (resp. are totally ramified) in F', and assume that $n = r + s$. Then*

(a) the length n' of the conorm code $\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C})$ satisfy

$$n + s \leq n' = ms + r \leq mn - r, \tag{16}$$

and equalities hold if and only if the extension F'/F is quadratic ($m = 2$).

(b) $n' = mn$ if and only if $s = n$ and $r = 0$; and in this case, $d' \geq m(n - \frac{\deg G}{t})$.

(c) $n' = n$ if and only if $s = 0$ and $r = n$; and, in this case, $d' \geq n - \frac{m}{t} \deg G = n - \deg G'$.

Proof. (*a*) It is straightforward to check that both inequalities in (12) hold if and only if $m = 2$. In this case, $n + s = 2s + r = 2n - r$.

(*b*) Since $r = n - s$, we have that $n' = mn$ if and only if $(m-1)s = (m-1)n$, which holds if and only if $s = n$ (and hence $r = 0$), since $m > 1$.

(*c*) Similarly, $n' = n$ if and only if $(m-1)s = 0$, which in turn can only happen if $s = 0$ since $m > 1$. The assertions on the distance are clear now from (13). □

Quadratic extensions. Suppose $F'/\mathbb{F}_{q^t}$ is a quadratic extension of $F/\mathbb{F}_q$. Since $t \mid m$ and $m = 2$, then $t = 1$ or $t = 2$. If $t = 1$ then F'/F is a geometric extension. This case will be studied in the next paragraph. Thus, assume that $t = 2$. In this case we have that F' is a constant field extension of F so that F'/F is an unramified extension ([8, Thm. 3.6.3]). Then

$$n' = 2s = 2n.$$

We know that $d' \geq n' - \deg G'$ and $d \geq n - \deg G$. Thus the bound for d' can be improved since by (13) we have

$$d' \geq 2s - \deg G = n' - \deg G,$$

or in other terms

$$d' \geq (n - \deg G) + s.$$

Regarding the dimension, since the extension is not ramified, then $\deg(\mathrm{Diff}(F'/F))$ $= 0$ and we get

$$k' \geq k^*.$$

So, in general, for conorm codes over non-geometric quadratic extensions the minimum distance and the dimension may increase.

Geometric extensions and levels. We consider now the particular case of geometric extensions, that is finite extensions F'/F of algebraic function fields over the same field of constants $\mathbb{F}_q$. Notice that in this case, the bounds for the parameters in Proposition 1 and Corollary 1 hold with $t = 1$. Recall that the secondary parameters of an $[n, k, d]$-code are the information rate $R = k/n$ and the relative minimum distance $\delta = d/n$.

Corollary 2. *Let F'/F be a geometric extension of function fields over $\mathbb{F}_q$ of degree $m > 1$. Let $\mathcal{C}' = \mathrm{Con}(\mathcal{C})$ as in Corollary 1 with $n = r + s$. The following holds:*

(a) *If $\mathcal{C}'$ is a MAG-code, then $\mathcal{C}$ is a MAG-code. If $r = 0$, then the converse also holds and $d' \geq 2$. If further $d = n - \deg G$, then $d' \geq md$ and $\delta' \geq \delta$.*

(b) *If either $\mathcal{C}'$ is a MAG-code and $2g - 2 < \deg G$, or else $\mathcal{C}$ is a SAG-code and $r = 0$, then $k' \geq mk - \frac{1}{2} \deg \mathrm{Diff}(F'/F)$.*

Proof. (a) Since $\mathcal{C}'$ is a MAG-code,

$$\deg G' < n' = ms + r.$$

Also, $\deg G' = m \deg G$ and $n = s + r$, thus

$$\deg G < s + \tfrac{r}{m} < n.$$

If $r = 0$, then $n' = nm$ and hence $\deg G < n$ implies that $\deg G' < n'$. In this case, $d' \geq m(n - \deg G) > m \geq 2$. If in addition $d = n - \deg G$ then $d' \geq md$ and hence

$$\delta' = \frac{d'}{n'} \geq \frac{md}{mn} = \frac{d}{n} = \delta.$$

(b) Since $\mathcal{C}'$ is a MAG-code we have (14). By (b), $\mathcal{C}$ is also a MAG-code and since $2g - 2 < \deg G$ by assumption, $\mathcal{C}$ is a SAG-code. This implies $k = \deg G + 1 - g$ and hence, by (14), we have

$$k' \geq mk - \tfrac{1}{2} \deg \mathrm{diff}(F'/F).$$

Now, if $\mathcal{C}$ is a SAG-code (in particular a MAG-code), then the hypothesis $r = 0$ implies, by (a), that $\mathcal{C}'$ is a MAG-code, and hence we are in the previous case. □

Examples in quadratic geometric extensions. We now give examples of conorm codes in quadratic geometric extensions of some rational function field.

Example 1. Consider $F=\mathbb{F}_4(x)$ the rational function field over $\mathbb{F}_4=\{0,1,\alpha,\alpha^2\}$, where $\alpha^2+\alpha+1=0$. We define the SAG-code $\mathcal{C}=C_{\mathcal{L}}(D,G)$ with

$$D=P_1+P_\alpha+P_{\alpha^2} \qquad \text{and} \qquad G=2P_\infty$$

where P_1, P_α and P_{α^2} are the rational places which are simple zeroes of $x+1$, $x+\alpha$ and $x+\alpha^2$ respectively, and P_∞ is the rational place that is a simple pole of x in F. We have that $\mathcal{C}$ is a SAG-code over $\mathbb{F}_4$ with parameters $[3,3,1]$, hence MDS (maximum distance separable). In fact, since $\deg G=2$ and $g(F)=0$, we have that $\mathcal{C}$ is a SAG-code. Also, $k=2+1-0=3$ and $d\geq 3-2=1$ but, by Singleton bound, we know that $d\leq 1$.

Let us now consider $F'=F(y)=\mathbb{F}_4(x,y)$ where

$$y^2+y=\frac{x^2}{x+1}.$$

This extension F'/F is the first step of a famous tower of function fields given by Garcia and Stichtenoth in [4]. Since F'/F is an Artin-Schreier extension, we have that P_1 and P_∞ are totally ramified in F' while P_α and P_{α^2} split completely in F'. Moreover, we have

$$[F':F]=2 \qquad \text{and} \qquad g(F')=1.$$

In this case $\mathcal{C}'=\mathrm{Con}_{F'/F}(\mathcal{C})=C_{\mathcal{L}}(D',G')$ is also a SAG-code over $\mathbb{F}_4$ with

$$D'=Q_1+R_\alpha+S_\alpha+R_{\alpha^2}+S_{\alpha^2} \qquad \text{and} \qquad G'=4Q_\infty,$$

where Q_1 (resp. Q_∞) is the only place over P_1 (resp. P_∞) and R_α and S_α (resp. R_{α^2} and S_{α^2}) are the two places over P_α (resp. P_{α^2}). We have now that $n'=5$, $k'=4$ and $d'\geq 1$. Thus, $\mathcal{C}'$ is a $[5,4,d']$-code over $\mathbb{F}_4$ with $1\leq d'\leq 2$. In fact $d'=1$ because if $z=(x-\alpha)(x-\alpha^2)$, the principal divisor $(z)^{F'}$ of z in F' is

$$(z)^{F'}=R_\alpha+S_\alpha+R_{\alpha^2}+S_{\alpha^2}-4Q_\infty.$$

This implies that $z\in\mathcal{L}(G')$ and also that

$$z(Q_1)\neq 0 \quad \text{and} \quad z(R_\alpha)=z(S_\alpha)=z(R_{\alpha^2})=z(S_{\alpha^2})=0.$$

Thus there is a codeword in $\mathcal{C}'$ of weight 1.

Example 2. Let $F=\mathbb{F}_q(x)$ be a rational function field and consider the quadratic extension $F'/\mathbb{F}_q$ of $F/\mathbb{F}_q$ determined by the elliptic function field $F'=\mathbb{F}_q(x,y)$ given by

$$y^2=f(x)$$

where $f(x)\in\mathbb{F}_q[x]$ is square-free of degree 3. We will fix a rational AG-code $\mathcal{C}=C_{\mathcal{L}}^F(D,G)$ and we will consider the elliptic conorm code $\mathcal{C}'=\mathrm{Con}_{F'/F}(\mathcal{C})$.

Let $R_1,\ldots,R_q$ and P_∞ be the rational places of F and let $P_1,\ldots,P_r$ be the places corresponding to the irreducible monic polynomials $p_i(x)$ in the factorization of $f(x)$, hence $1\leq r\leq 3$, and put

$$D_1=R_1+\cdots+R_q \quad \text{and} \quad D_2=P_1+\cdots+P_r.$$

There are various possibilities for $\mathcal{C}$, let us see three of them.

(i) Assume that $\mathbb{F}_q$ has odd characteristic and consider

$$\mathcal{C}_1=C(D_1,\ell P_\infty)$$

for $\ell \in \mathbb{N}$. Then, $P_1, \ldots, P_r$ and P_∞ are the only ramified places of F'. Even more, the places $P_1, \ldots, P_r$ and P_∞ are totally ramified in F'. If $Q_1, \ldots, Q_r$ and Q_∞ denote the corresponding places of F' over them, then $\deg Q_j = \deg P_j$ and $\deg Q_\infty = 1$. Thus, the conorm codes $\mathrm{Con}(\mathcal{C}_1)$ has parameters $[n_1', k_1', d_1']$ where

$$n_1' = \begin{cases} 2q & \text{if } f \text{ is irreducible, } (r=1), \\ 2q-1 & \text{if } f \text{ has only one linear factor, } (r=2), \\ 2q-3 & \text{if } f \text{ has three linear factors, } (r=3). \end{cases}$$

By (13) and (14) in Proposition 1, we have

$$d_1' \geq n_1' - 2\ell$$

and, since $\mathrm{Diff}(F'/F) = Q_1 + \cdots + Q_r + Q_\infty$ we have that $\deg \mathrm{Diff}(F'/F) = 4$ and hence,

$$k_1' \geq 2(k_1^* - 1) = 2 \deg G = 2\ell.$$

Thus, by the above expressions and the Singleton bound, we have that

$$n_1' \leq d_1' + k_1' \leq n_1' + 1.$$

This is in coincidence with the known fact that elliptic codes are almost MDS, that is they are MDS, or the Singleton bound fails by one.

(ii) Another possibility is to take

$$\mathcal{C}_2 = C(D_1 + P_\infty, D_2) \qquad \text{or} \qquad \mathcal{C}_3 = C(D_1, D_2 + \ell P_\infty)$$

for $\ell \geq 1$, with parameters $[q+1, k_2, d_2]$ and $[q, k_3, d_3]$, respectively. Here, to ensure that the supports of the divisors D and G are disjoint we have to assume that f is irreducible over $\mathbb{F}_q$. The associated elliptic conorm codes $\mathcal{C}_2' = \mathrm{Con}_{F'/F}(\mathcal{C}_2)$ and $\mathcal{C}_3' = \mathrm{Con}_{F'/F}(\mathcal{C}_3)$ have parameters $[2q+1, k_2', d_2']$ and $[2q, k_3', d_3']$, respectively. Similarly as in (i), one can obtain bounds for the dimension and minimum distance of these codes.

4. Unramified extensions and duality

We consider now unramified extensions F'/F of function fields over $\mathbb{F}_q$. Under this assumption, it is possible to get some nice results for duality of conorm codes.

We begin by studying the relation between the AG-levels of an AG-code and its conorm code.

Proposition 2. *Let F'/F be an unramified extension of algebraic function fields over $\mathbb{F}_q$ of degree m. Then $\mathcal{C}'$ is a SAG-code (resp. MAG) if and only if $\mathcal{C}$ is a SAG-code (resp. MAG). In this case, $k' = mk$ and $R' = R$. If in addition $d = n - \deg G$, then $d' \geq md$ and $\delta' \geq \delta$.*

Proof. Recall that F'/F is unramified if and only if $\mathrm{Diff}(F'/F) = 0$. Hence,

$$g' - 1 = m(g-1),$$

by (10). Also, $r = 0$ and $n' = mn$. By (b) of Corollary 1, $\mathcal{C}'$ is a MAG-code if and only if $\mathcal{C}$ is a MAG-code. Since

$$2m(g-1) = 2(g'-1) < \deg G' = m \deg G,$$

we see that $\mathcal{C}'$ is a SAG-code if and only if $\mathcal{C}$ is a SAG-code. In this situation, we have both $k' = \deg G' + 1 - g'$ and $k = \deg G + 1 - g$. Putting together all these information we have

$$k' = m \deg G + m(1-g) = m(\deg G + 1 - g) = mk,$$

and then $R' = k'/n' = mk/mn = k/n = R$.

For the remaining assertion, by (13) we have

$$d' \geq m(n - \tfrac{\deg G}{t}) \geq m(n - \deg G) = md,$$

from which we have $\delta' = d'/n' \geq md/mn = \delta$, as we wanted to show. □

Example 3. Let $F_0 = K(x_0)$ be the rational function field over $K = \mathbb{F}_{4^3}$ and consider the finite tower

$$F_0 \subset F_1 \subset F_2 \subset F_3$$

of functions fields over K, where each field extension is a Kummer extension of degree 3 recursively defined for $i = 1, 2, 3$ by $F_i = F_{i-1}(x_i)$ where

$$x_i^3 = 1 + \frac{x_{i-1}^3}{(x_{i-1} - 1)^3}.$$

Let us denote by P_β the simple zero of $x_0 - \beta$, for $\beta \in \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, and by P_∞ the simple pole of x_0 in F_0. In [10], Wulftange proved that P_0 splits completely in F_3/F_0, P_1 splits completely in F_1/F_0, is totally ramified in F_2/F_1 and then splits completely again in F_3/F_2. Furthermore P_α, P_{α^2} and P_∞ are totally ramified in F_1/F_0 and then they split completely in F_3/F_1. The ramification behavior of the other rational places of F_0 was studied in [10], where the author also proved that the extension F_2/F_1 is ramified but the extension F_3/F_2 is unramified.

Using the above description of the the ramification behavior and the Hurwitz genus formula, we have that $g(F_2) = 4$. We also have that there are exactly nine places $Q_1, \ldots, Q_9$ of F_2 lying above P_0, three places Q_{10}, Q_{11} and Q_{12} of F_2 lying above P_1 and three places R_1, R_2 and R_3 lying above P_∞. All of them are rational places of F_2. We define $\mathcal{C} = C_\mathcal{L}(D, G)$ with

$$D = Q_1 + \cdots + Q_{12} \quad \text{and} \quad G = 3R_1 + 3R_2 + 3R_3.$$

Since

$$2g(F_2) - 2 = 6 < 9 = \deg G < 12 = n,$$

we have that $\mathcal{C}$ is a $[12, 6, d]$ SAG-code with $d \geq 3$. In fact $d = 3$ because the principal divisor $(x_0)^{F_2}$ of x_0 in F_2 is

$$(x_0)^{F_2} = Q_1 + \cdots + Q_9 - G,$$

so that $x_0 \in \mathcal{L}(G)$ and also

$$x_0(Q_1) = \cdots = x_0(Q_9) = 0 \quad \text{and} \quad x_0(Q_{10}) \neq 0, x_0(Q_{11}) \neq 0, x_0(Q_{12}) \neq 0.$$

This implies that there is a codeword of $\mathcal{C}$ of weight 3. Now, since F_3/F_2 is unramified, we see from Proposition 2 that the conorm code $\mathcal{C}'$ of $\mathcal{C}$ is also a SAG-code with $n' = 36$, $k' = 18$ and $d' \geq 9$. In fact $d' = 9$ because the principal divisor $(x_0)^{F_3}$ of x_0 in F_3 is

$$(x_0)^{F_3} = Q'_1 + \cdots + Q'_{27} + Q'_{28} + \cdots + Q'_{36} - G',$$

where $Q'_1, \cdots, Q'_{27}$ are all the places of F_3 lying over P_0, $Q'_{28}, \cdots, Q'_{36}$ are all the places of F_3 lying over P_1 and $G' = \operatorname{Con}_{F_3/F_2} G$. Thus $x_0 \in \mathcal{L}(G')$ and we also have that

$$x_0(Q'_1) = \cdots = x_0(Q'_{36}) = 0 \quad \text{and} \quad x_0(S) \neq 0,$$

for any $S \in \{Q'_{28}, \ldots, Q'_{36}\}$. This implies that there is a codeword of $\mathcal{C}'$ of weight 9. In particular we see that the lower bound for d' given in Proposition 2 can not be improved in general.

Duality. In general, the dual of the conorm code is not the conorm of the dual code. However, this is indeed the case for conorm codes defined over unramified extensions with an additional condition. More precisely

Theorem 4.1. *Let F'/F be an unramified finite extension of algebraic function fields of degree m over $\mathbb{F}_q$ such that* $\gcd(m,q)=1$ *and let $\mathcal{C}=C_{\mathcal{L}}(D,G)$. Then*

$$\mathrm{Con}(\mathcal{C}^{\perp})=\mathrm{Con}(\mathcal{C})^{\perp}. \tag{17}$$

Proof. Let $\mathcal{C}=C_{\mathcal{L}}(D,G)$ and $\mathrm{Con}(\mathcal{C})=C_{\mathcal{L}}(D',G')$ with $D'=\mathrm{Con}(D)$ and $G'=\mathrm{Con}(G)$. On the one hand, from Definition 2.2.6 and Theorem 2.2.8 in [8], we have that $\mathrm{Con}(\mathcal{C})^{\perp}=C_{\Omega}(D',G')$.

On the other hand, we know that $\mathcal{C}^{\perp}=C_{\Omega}(D,G)$ and by Lemma 2.2.9 and Proposition 2.2.10 in [8] there exist a Weil differential η of F such that

$$\mathcal{C}^{\perp}=C_{\Omega}(D,G)=C_{\mathcal{L}}(D,H) \quad \text{with} \quad H=D-G+(\eta)$$

and also $v_{P_i}(\eta)=-1$ and $\eta_{P_i}(1)=1$ for all $i=1,\ldots,n$ where $\{P_1,\ldots,P_n\}=\mathrm{Supp}(D)$. Then

$$\mathrm{Con}(\mathcal{C}^{\perp})=C_{\mathcal{L}}(D',H') \quad \text{with} \quad H'=\mathrm{Con}(H)=D'-G'+\mathrm{Con}((\eta)).$$

Let $\eta'=\mathrm{Cotr}_{F'/F}(\eta)$ be the cotrace of η, that is η' is a Weil differential of F' such that (see [8], Theorem 3.4.6)

$$(\eta')=(\mathrm{Cotr}_{F'/F}(\eta))=\mathrm{Con}_{F'/F}((\eta))+\mathrm{Diff}(F'/F),$$

and since in this case the extension is unramified we have

$$(\eta')=\mathrm{Con}((\eta)).$$

Moreover, if $\mathrm{Supp}(D')=\{Q_1,\ldots,Q_{n'}\}$ then for each j there is an index i such that

$$Q_j\cap F=P_i\in\mathrm{Supp}(D),$$

and since $P_i\notin\mathrm{Supp}(H)$, because $v_{P_i}(\eta)=-1$, then $Q_j\notin\mathrm{Supp}(H')$. Thus, we have

$$\begin{aligned} 0 &= v_{Q_j}(H')=v_{Q_j}(D'-G'+(\eta')) \\ &= v_{Q_j}(D')-v_{Q_j}(G')+v_{Q_j}(\eta')=1-0+v_{Q_j}(\eta'). \end{aligned}$$

Since $m=[F':F]$ is coprime with q, we can consider $\bar{m}\in\mathbb{F}_q^*$ and its inverse $\bar{m}^{-1}$ in the multiplicative group $\mathbb{F}_q^*$ and define $\tilde{\eta}=\bar{m}^{-1}\eta'$. Therefore, $v_{Q_j}(\tilde{\eta})=v_{Q_j}(\eta')=-1$ for each $j=1,\ldots,n'$. Moreover, we also have

$$\tilde{\eta}(1)=\bar{m}^{-1}\eta'(1)=\eta'(\bar{m}^{-1})=\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_q}(\eta'(\bar{m}^{-1}))=\eta(\mathrm{Tr}_{F'/F}(\bar{m}^{-1}))=\eta(1)=1.$$

Then, by using Proposition 2.2.10 in [8] again, we have

$$C_{\Omega}(D',G')=C_{\mathcal{L}}(D',D'-G'+(\tilde{\eta})).$$

Finally, putting all these things together we have that

$$\begin{aligned} \mathrm{Con}(\mathcal{C}^{\perp}) &= C_{\mathcal{L}}(D',H')=C_{\mathcal{L}}(D',D'-G'+(\tilde{\eta})) \\ &= C_{\Omega}(D',G')=(C_{\mathcal{L}}(D',G'))^{\perp}=(\mathrm{Con}(\mathcal{C}))^{\perp} \end{aligned}$$

as we wanted to show. □

Remark 1. Theorem 4.1 probably holds not only for unramified extensions. In general we have that

$$\mathrm{Con}(\mathcal{C})^{\perp} = C(D', D' - G' + (\eta')) \quad \text{and} \quad \mathrm{Con}(\mathcal{C}^{\perp}) = C(D', D' - G' + \mathrm{Con}(\eta)),$$

where η (resp. η') is a Weil differential of F (resp. F'). Thus, by the results of Munuera and Pellikaan in [7], the problem in proving that $\mathrm{Con}(\mathcal{C})^{\perp} = \mathrm{Con}(\mathcal{C}^{\perp})$ reduces to determine whether or not the canonical divisors (η') and $\mathrm{Con}(\eta)$ are equal or rational equivalent.

5. The conorm of cyclic AG-codes

Here we assume, as we did in Section 3, that all the extensions of function fields considered are geometric. By using Galois extensions we study the conorm codes of cyclic AG-codes. We will show that under certain conditions on the ramification behavior of the rational places of D, we can represent a cyclic AG-code $\mathcal{C} = C_{\mathcal{L}}^{F}(D, G)$ defined over F as a cyclic AG-code defined over F' by using the conorm.

First we will need some auxiliary results. Let F'/F be a function field extension and let $G' \in \mathrm{Div}(F')$. The set of all places of F lying below the places in $\mathrm{Supp}(G')$ will be denoted as $\mathrm{Supp}(G') \cap F$. In other words

$$\mathrm{Supp}(G') \cap F = \{Q' \cap F : Q' \in \mathrm{Supp}(G')\}.$$

Lemma 5.1. *Let F'/F be a extension of algebraic function fields over $\mathbb{F}_q$. Assume that $G \in \mathrm{Div}(F)$ and $G' \in \mathrm{Div}(F')$ are such that $\mathrm{Supp}(G') \cap F = \mathrm{Supp}(G)$. If $v_{Q'}(G') \geq e(Q'|Q)\, v_Q(G)$ for every $Q' \in \mathrm{Supp}(G')$ and $Q = Q' \cap F$, then*

$$\mathcal{L}(G) \subseteq \mathcal{L}(G').$$

Proof. Let $Q' \in \mathrm{Supp}(G')$, put $Q = Q' \cap F$ and take $x \in \mathcal{L}(G)$. By hypothesis $Q \in \mathrm{Supp}(G)$ and therefore $v_Q(x) \geq -v_Q(G)$. Then we have,

$$\begin{aligned} v_{Q'}(x) &= e(Q'|Q)\, v_Q(x) \geq -e(Q'|Q)\, v_Q(G) \\ &\geq -e(Q'|Q)\big(\tfrac{1}{e(Q'|Q)} v_{Q'}(G')\big) = -v_{Q'}(G'), \end{aligned}$$

and thus $x \in \mathcal{L}(G')$. □

Remark 2. The result in the previous lemma holds in a more general situation, namely when $\mathrm{Supp}(G') \cap F \subseteq \mathrm{Supp}(G)$, provided that $G = G_0 - G^{+}$ where $\mathrm{Supp}(G_0) = \mathrm{Supp}(G') \cap F$ and $G^{+} \in \mathrm{Div}(F)^{+}$ is a positive divisor of F. In the particular case that $G^{+} = 0$ we are in the situation of Lemma 5.1.

Lemma 5.2. *Let F'/F be a finite extension of algebraic function fields over $\mathbb{F}_q$ of degree $m = [F' : F]$. If $G \in \mathrm{Div}(F)$ and $G' = \mathrm{Con}_{F'/F}(G)$ then $\mathcal{L}(G) \subseteq \mathcal{L}(G')$. Furthermore,*

(a) $\mathcal{L}(G) \subseteq \mathrm{Tr}(\mathcal{L}(G'))$ if $(m, q) = 1$, and

(b) $\mathrm{Tr}(\mathcal{L}(G')) \subseteq \mathcal{L}(G)$ if F'/F is Galois,

where $\mathrm{Tr}(\mathcal{L}(G')) = \{\mathrm{Tr}(x) : x \in \mathcal{L}(G')\}$ and Tr is the trace map from F' to F.

Proof. The fact that $\mathcal{L}(G) \subseteq \mathcal{L}(G')$ follows from the previous Lemma.

(*a*) Now, let $x \in \mathcal{L}(G) \subseteq F$. Note that in this case $\mathrm{Tr}(x) = mx$. Let $x' = m^{-1}x$ where m^{-1} is the inverse of m modulo $p = \mathit{char}(\mathbb{F}_q)$. Then, if $Q' \in \mathbb{P}(F')$, we have that $\mathrm{Tr}(x') = m^{-1}\,\mathrm{Tr}(x) = x$ and

$$v_{Q'}(x') = v_{Q'}(m^{-1}x) = v_{Q'}(x) = e(Q'|Q)\, v_Q(x) \geq -e(Q'|Q)\, v_Q(G) = -v_{Q'}(G').$$

Thus, $x' \in \mathcal{L}(G')$ and therefore $x \in \mathrm{Tr}(\mathcal{L}(G'))$.

(b) Now let us assume that F'/F is Galois. In this case we have that $e(Q'|Q) = e_Q$ is the same for every $Q'|Q$ and if $\mathcal{G} = Gal(F'/F)$ then $\mathrm{Tr}(x) = \sum_{\sigma \in \mathcal{G}} \sigma(x)$. Let $x \in \mathrm{Tr}(\mathcal{L}(G'))$, i.e. $x = \mathrm{Tr}(x')$ with $x' \in \mathcal{L}(G')$. Then $v_{Q'}(x') \geq -v_{Q'}(G')$ for every $Q' \in \mathbb{P}(F')$. Let $Q \in \mathrm{Supp}(G)$ and $Q'|Q$. Note that

$$\begin{aligned} v_{Q'}(x) &= v_{Q'}(\mathrm{Tr}(x')) = v_{Q'}\Big(\sum_{\sigma \in \mathcal{G}} \sigma(x')\Big) \geq \min_{\sigma \in \mathcal{G}}\{v_{Q'}(\sigma(x')\} \\ &= v_{Q'}(\sigma_0(x')) = v_{\sigma_0^{-1}(Q')}(x') = v_{Q''}(x') \geq -v_{Q''}(G'), \end{aligned}$$

for some σ_0 and some $Q''|Q$. Then, by the above calculation, we have

$$v_Q(x) = \tfrac{1}{e_Q} v_{Q''}(x) = \tfrac{1}{e_Q} v_{Q'}(x) \geq \tfrac{-1}{e_Q} v_{Q''}(G') = -v_Q(G),$$

and thus $x \in \mathcal{L}(G)$. □

Remark 3. Item (b) also holds if we replace the trace map with the norm map from F' to F, since $N(x') = \prod_{\sigma \in \mathcal{G}} \sigma(x')$ and we have

$$v_{Q'}(N(x')) = v_{Q'}\Big(\prod_{\sigma \in \mathcal{G}} \sigma(x')\Big) = \sum_{\sigma \in \mathcal{G}} v_{Q'}(\sigma(x')) \geq \min_{\sigma \in \mathcal{G}}\{v_{Q'}(\sigma(x'))\}.$$

The next result is a direct consequence of Lemmas 5.1 and 5.2.

Corollary 3. *If F'/F is a finite Galois extension of degree m and $G' = \mathrm{Con}_{F'/F}(G)$, then $\mathrm{Tr}(\mathcal{L}(G')) \subseteq \mathcal{L}(G) \subseteq \mathcal{L}(G')$. If, in addition, $(m, q) = 1$, then we have*

$$\mathrm{Tr}(\mathcal{L}(G')) = \mathcal{L}(G). \tag{18}$$

Totally ramified places and cyclicity of AG-codes. We recall that a linear code $C \subseteq \mathbb{F}_q^n$ is cyclic if it is closed under the cyclic shift of its coordinates. Namely, for every $(c_1, \ldots, c_n) \in C$ we have that the word $(c_n, c_1, \ldots, c_{n-1})$ is also in C.

We will show that the conorm construction preserves cyclicity in a special case. First we give this simple result.

Lemma 5.3. *Let F'/F a finite extension of function fields over $\mathbb{F}_q$. Let $\mathcal{C} = C_{\mathcal{L}}^F(D, G)$ be an AG-code such that* $\mathrm{Supp}(D)$ *has only totally ramified places. Then $\mathcal{C}$ is a subcode of its conorm code $\mathcal{C}' = \mathrm{Con}(\mathcal{C})$ and $\mathcal{C}$ is cyclic if $\mathcal{C}'$ is cyclic.*

Proof. Let $D = P_1 + \cdots + P_n$ with every P_i totally ramified in F'. Let Q_i be the only place of F' over P_i, for $i = 1, \ldots, n$, and thus $D' = \sum_{i=1}^n Q_i$. Now, consider $c = (c_1, \ldots, c_n) \in \mathcal{C}$. Then, there is some $x \in \mathcal{L}(G)$ such that $c_i = x(P_i)$ for every $i = 1, \ldots, n$. Since $G' = \mathrm{Con}(G)$, we have that $\mathcal{L}(G) \subset \mathcal{L}(G')$, by Lemma 5.1. Hence, $x(Q_i) = x(P_i) = c_i$ and therefore $c \in \mathcal{C}'$. The remaining assertion is clear. □

We recall the condition for an AG-code $\mathcal{C} = C_{\mathcal{L}}(D = P_1 + \cdots + P_n, G)$ to be cyclic. Any codeword of $\mathcal{C}$ is of the form $c = (x(P_1), x(P_2), \ldots, x(P_n))$ with $x \in \mathcal{L}(G)$. The code $\mathcal{C}$ is cyclic if and only if $s(c) = (x(P_n), x(P_1), \ldots, x(P_{n-1}))$ is also in $\mathcal{C}$. But this happens if and only if there exists $z \in \mathcal{L}(G)$ such that

$$(x(P_n), x(P_1), \ldots, x(P_{n-1})) = (z(P_1), z(P_2), \ldots, z(P_n)). \tag{19}$$

That is, $\mathcal{C}$ is cyclic if and only if for each $x \in \mathcal{L}(G)$ there is a $z = z(x) \in \mathcal{L}(G)$ such that (19) holds.

Example 4. Let F'/F be an algebraic function field extension over $\mathbb{F}_q$ of finite degree m. Let $\mathcal{C} = C_{\mathcal{L}}^{F}(P, G)$ where $P \notin \mathrm{Supp}(G)$ is a rational place which splits completely in F'. The code $\mathcal{C}$, being of length 1, is just $\{0\}$ or the whole $\mathbb{F}_q$ depending on the degree of G, and hence trivially cyclic. If $\mathcal{C}$ is not trivial, its conorm code is $\mathcal{C}' = C_{\mathcal{L}}^{F'}(D', G')$, where $D' = \sum_{P'|P} P'$ and $G' = \mathrm{Con}(G)$. If F'/F is a cyclic extension, the elements in the Galois group $\mathcal{G} = \mathrm{Gal}(F'/F)$ cyclically permute the places over P and hence it is (equivalent to) a cyclic code.

We will need the following well-known equality for the residue classes of a rational place on F and any place in F' lying over it.

Lemma 5.4. *Let $F'/\mathbb{F}_{q^t}$ be a finite extension of algebraic function fields of $F/\mathbb{F}_q$. If P is a rational place of F, then $x(P) = x(Q)$ for any x in the valuation ring $\mathcal{O}_P$ of the place P and every place Q of F' lying over P.*

Proof. Since P is a rational place of $F/\mathbb{F}_q$, the residue class field $F_P = \mathcal{O}_P/P$ of P is just $\mathbb{F}_q$, and thus $x(P) \in \mathbb{F}_q$, for every $x \in \mathcal{O}_P$. This means that there is some $\alpha \in \mathbb{F}_q$ such that $v_P(x - \alpha) > 0$. That is, we have $x - \alpha \in P$ and hence $0 = (x - \alpha)(P) = x(P) - \alpha(P)$ from which we get $x(P) = \alpha$. Now, let Q be a place of F' lying over P. Then, we have $v_Q(x - \alpha) = e(Q|P)\, v_P(x - \alpha) > 0$. Therefore, proceeding as before we get $x(Q) = \alpha = x(P)$ as desired. □

Despite the trivial case of the previous example, we will show now that in finite Galois extensions of function fields, the conorm lift of (certain) cyclic AG-code is also cyclic.

Theorem 5.5. *Let F'/F be a Galois extension of algebraic function fields over $\mathbb{F}_q$ of degree m, with $(m, q) = 1$ or $q \mid m$. Let $\mathcal{C} = C_{\mathcal{L}}^{F}(D, G)$ be an AG-code such that every place in $\mathrm{Supp}(D)$ is totally ramified in F'. Then, $\mathcal{C}$ is cyclic if and only if $\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C})$ is cyclic.*

Proof. By Lemma 5.3 we know that $\mathcal{C} \subseteq \mathcal{C}'$ and hence $\mathcal{C}$ is cyclic if $\mathcal{C}'$ is cyclic.

Now, assume that $\mathcal{C} = C_{\mathcal{L}}^{F}(D, G)$ is cyclic. We want to show that $\mathcal{C}' = C_{\mathcal{L}}^{F'}(D', G')$ is cyclic too. Suppose that $D = P_1 + \cdots + P_n$ where the P_i's are different rational places totally ramified in F'. For every $i = 1, \ldots, n$, let P_i' be the only place in F' above P_i. Thus, we have $D' = P_1' + \cdots + P_n'$.

Hence, given a codeword $c' = (x'(P_1'), \ldots, x'(P_n')) \in \mathcal{C}'$, where $x' \in \mathcal{L}(G')$, we want to show that we can find an element $z' = z'(x') \in \mathcal{L}(G')$ satisfying (19), i.e.

$$(z'(P_1'), z'(P_2'), \ldots, z'(P_n')) = (x'(P_n'), x'(P_1'), \ldots, x'(P_{n-1}')). \tag{20}$$

Let us first assume that $(m, q) = 1$. Let $\mathcal{G} = \mathrm{Gal}(F'/F)$ and consider the element

$$x := \mathrm{Tr}(x') = \sum_{\sigma \in \mathcal{G}} \sigma(x') \ \in F. \tag{21}$$

Since $\mathrm{Tr}(\mathcal{L}(G')) = \mathcal{L}(G)$, by Corollary 3, we have that $x \in \mathcal{L}(G)$, actually. Since $\mathcal{C}$ is cyclic, by (19) there is an element $z \in \mathcal{L}(G)$ such that

$$(z(P_1), z(P_2), \ldots, z(P_n)) = (x(P_n), x(P_1), \ldots, x(P_{n-1})). \tag{22}$$

Now, put $z' = m^{-1} z \in \mathcal{L}(G')$ where m^{-1} is the inverse modulo $p = \mathrm{char}(\mathbb{F}_q)$. Hence for every i mod n we have

$$z'(P_i') = m^{-1} z(P_i') = m^{-1} z(P_i) = m^{-1} x(P_{i-1}) = m^{-1} x(P_i')$$

where we have used (22) and Lemma 5.4. Thus, by (21) we get

$$\begin{aligned} z'(P_i') &= m^{-1}\Big(\sum_{\sigma\in\mathcal{G}} \sigma(x')\Big)(P_{i-1}') = m^{-1}\sum_{\sigma\in\mathcal{G}} x'(\sigma^{-1}(P_{i-1}')) \\ &= m^{-1}\sum_{\sigma\in\mathcal{G}} x'(P_{i-1}') = m^{-1}m\, x'(P_{i-1}') = x'(P_{i-1}')\,. \end{aligned}$$

In this way, we see that $z'\in\mathcal{L}(G')$ satisfies (20) and therefore $\mathcal{C}'$ is a cyclic code as desired.

In the case $q \mid m$ we use a similar argument but now considering

$$x := N(x') = \prod_{\sigma\in\mathcal{G}} \sigma(x') \ \in F,$$

where $\mathcal{G} = \mathrm{Gal}(F'/F)$. Now, we have that $N(\mathcal{L}(G')) \subseteq \mathcal{L}(G)$ by Remark 3 so that $x\in\mathcal{L}(G)$. We define $z'=z$. For every i mod n, we have

$$\begin{aligned} z'(P_i') = z(P_i') = x(P_{i-1}') &= \Big(\prod_{\sigma\in\mathcal{G}} \sigma(x')\Big)(P_{i-1}') = \prod_{\sigma\in\mathcal{G}} x'(\sigma^{-1}(P_{i-1}')) \\ &= \prod_{\sigma\in\mathcal{G}} x'(P_{i-1}') = (x'(P_{i-1}'))^m = x'(P_{i-1}')\,. \end{aligned}$$

In this way we see that $z'\in\mathcal{L}(G')$ satisfies (20) and therefore $\mathcal{C}'$ is a cyclic code, as desired. □

We have seen in Lemma 5.3 that under certain conditions, the original code $\mathcal{C}$ is a subcode of its conorm lift $\mathcal{C}'$. If, in addition, the code $\mathcal{C}$ is cyclic, then both codes coincide. That is, as algebraic codes over $\mathbb{F}_q$, $\mathcal{C}$ and $\mathcal{C}'$ are the same code.

Corollary 4. *Under the same hypothesis of Theorem 5.5, if $\mathcal{C}$ is cyclic then $\mathcal{C}=\mathcal{C}'$.*

Proof. We know by Lemma 5.3 that $\mathcal{C}\subseteq\mathcal{C}'$. Let $c'\in\mathcal{C}'$. Then $c'=(x'(P_1'),\ldots,x'(P_n'))$ with $x'\in\mathcal{L}(G')$. By Theorem 5.5, $\mathcal{C}'$ is cyclic and hence the cyclic shift $s(c')\in\mathcal{C}'$. Thus, there is $z'\in\mathcal{L}(G')$ satisfying the cyclic condition

$$z'(P_1') = x(P_n'), \quad z'(P_2') = x(P_1'), \quad \ldots, \quad z'(P_n') = x(P_{n-1}').$$

In the proof of Theorem 5.5 we showed how to construct this element z' performing the shift, and that z' is actually in $\mathcal{L}(G)$, by construction. Therefore, $s(c')\in\mathcal{C}$ and, in this way, $c'=s^n(c')\in\mathcal{C}$. This implies that $\mathcal{C}'\subseteq\mathcal{C}$ and thus $\mathcal{C}=\mathcal{C}'$. □

In other words, given a cyclic AG-code $\mathcal{C}=C_{\mathcal{L}}(D,G)$ over a finite Galois extension F'/F of degree m, such that either m is coprime to q or q divides m, and where the support of D is totally ramified, the conorm lift gives a geometric representation $\mathcal{C}'=\mathrm{Con}(\mathcal{C})$ of $\mathcal{C}$ in a function field of greater genus.

6. Classic codes as conorm codes

In this final section we show that repetition codes, Hermitian codes and Reed-Solomon codes can be considered, in many general cases, as conorm codes of rational AG-codes.

Repetition codes. Any repetition code

$$\mathcal{R}_q(n) = \{(c, \ldots, c) : c \in \mathbb{F}_q\}$$

of length $n \leq q+1$ can be represented as a rational AG-code in $F = \mathbb{F}_q(x)$ as $\mathcal{C} = C_{\mathcal{L}}(D, (y))$, with $D = P_1 + \cdots + P_n$, where $P_1, \ldots, P_n$ are rational places of F and (y) is any principal divisor disjoint with D. In fact, if $c \in \mathcal{C}$, then

$$c = (x(P_1), \ldots, x(P_n)) = (x, \ldots, x),$$

since $x \in \mathcal{L}((y)) = \mathbb{F}_q$ ($\deg G = 0$ implies $\dim \mathcal{L}(G) = 1$) and hence,

$$\mathcal{R}_q(n) = \mathcal{C} = C_{\mathcal{L}}(D, (y)). \tag{23}$$

Furthermore, we have the following.

Lemma 6.1. *In the case of geometric extensions, the conorm code of a repetition code is a repetition code.*

Proof. Consider the repetition code $\mathcal{R}_q(n)$ as in (23) defined over a rational function field $F = \mathbb{F}_q(x)$. Suppose that F'/F is a geometric extension over $\mathbb{F}_q$ of degree m and genus $g' > 0$. Since $\mathrm{Con}_{F'/F}((y)^F) = (y)^{F'}$, we have

$$\mathcal{C}' = \mathrm{Con}_{F'/F}\left(C_{\mathcal{L}}^F(D, (y)^F)\right) = C_{\mathcal{L}}^{F'}\left(D', (y)^{F'}\right),$$

with $D' = D_1 + \cdots + D_n$. But $\mathcal{C}'$ is a repetition code by the previous comments and thus we get

$$\mathcal{C}' = \mathcal{R}_q(n'),$$

with n' as in (12), as we wanted to show. □

By using Kummer extensions we can give a partial converse of the previous result. In fact, we will show that any repetition code is the conorm lift to a Kummer extension of the field $\mathbb{F}_q$ viewed as a rational AG-code.

Proposition 3. *If $n \mid q-1$, the repetition code $\mathcal{R}_q(n)$ is a conorm code.*

Proof. Consider the rational function field $F = \mathbb{F}_q(x)$ and let $F' = F(y)$ be the Kummer extension of F given by

$$y^n = (x-\alpha)(x-\alpha^{-1})$$

where $n \mid q-1$, $\alpha \in \mathbb{F}_q^*$ and $\alpha \neq \alpha^{-1}$.

By Proposition 6.3.1 in [8] we have that F'/F is cyclic of degree n and $\mathbb{F}_q$ is the full constant field of F' whose genus is $g = [\frac{n-1}{2}]$. Also, the places P_α and $P_{\alpha^{-1}}$, the zeroes of $x-\alpha$ and $x-\alpha^{-1}$ respectively, are totally ramified in F'/F.

Let $\varphi(T) = T^n - (x-\alpha)(x-\alpha^{-1}) \in \mathbb{F}_q[T]$ and let $\bar{\varphi}(T)$ be its reduction mod P_0, the zero of x in F. Since $x(P_0) = 0$ and $n \mid q-1$ then

$$\bar{\varphi}(T) = T^n - 1 = \prod_{i=1}^{n} (T - a_i) \in \mathbb{F}_q[T]\,.$$

Therefore, by Kummer Theorem, P_0 splits completely in F.

Let $D = P_1 + \cdots + P_n$, where $P_1, \ldots, P_n$ are the (rational) places of F' lying over P_0 and $G = (z)^{F'}$ with $z \in F$. By the previous example we have

$$\mathcal{C}' := C_{\mathcal{L}}(D, (z)^{F'}) = \mathcal{R}_q(n)$$

and clearly $\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C})$ where $\mathcal{C} = C_{\mathcal{L}}(P_0, (z)^F) = \mathbb{F}_q$. □

Hermitian codes. We now show that certain Hermitian codes are conorm codes over Hermitian function fields of rational AG-codes.

Consider the Hermitian function field $H = \mathbb{F}_{q^2}(x,y)$ as the degree q extension of the rational function field $F = \mathbb{F}_{q^2}(x)$, given by the equation

$$y^q + y = x^{q+1}.$$

The field F has q^2+1 rational places $P_1, \ldots, P_{q^2}$ and P_∞, the pole of x. For each $\alpha \in \mathbb{F}_{q^2}$ there are q elements $\beta \in \mathbb{F}_{q^2}$ satisfying

$$\beta^q + \beta = \alpha^{q+1},$$

and for all such pairs (α, β) there is a unique place $P_{\alpha,\beta}$ in H such that $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$. Thus, H has q^3+1 rational places, q places over each rational place $P_{\alpha,\beta}$ of F and Q_∞, the common pole of x and y in H, lying over P_∞.

Hermitian codes are the 1-point AG-codes defined as

$$\mathcal{H}_a = C_{\mathcal{L}}^H(D', aQ_\infty), \tag{24}$$

where

$$D' = \sum_{P \in \mathbb{P}(H) \smallsetminus \{Q_\infty\}} P = \sum_{\beta^q + \beta = \alpha^{q+1}} P_{\alpha,\beta}. \tag{25}$$

Remark 4. In order to construct codes from the Hermitian function field in which the divisor G is not a one-point divisor, one can consider the function field H not as an Artin-Schreier extension of $\mathbb{F}_q^2(x)$, but rather as a Kummer extension of $F = \mathbb{F}_q^2(y)$ defining the divisor G by means of the zeroes of $y^q + y$ and D by the places which are unramified over F (see Example 4.8 in [1]).

Proposition 4. *If $q \mid a$ then $\mathcal{H}_a$ is a conorm code.*

Proof. Using the above notation, let us consider the code

$$\mathcal{C}_t = C_{\mathcal{L}}^F(D, tP_\infty),$$

where $D = P_1 + \cdots + P_{q^2}$. Note that if $q \mid a$ then

$$\mathcal{H}_a = \mathrm{Con}_{H/F}(\mathcal{C}_{a/q})$$

where $H = \mathbb{F}_{q^2}(x,y)$ is the Hermitian field given by $y^q + y = x^{q+1}$, because we have $\mathrm{Con}(D) = D'$ as in (25) and $\mathrm{Con}(sP_\infty) = sqQ_\infty$ for any s. □

As an application of these results, we show next that the identity (17) fails to hold in general, that is the dual of a the conorm code of $\mathcal{C}$ is not necessarily the conorm of the dual code of $\mathcal{C}$.

Example 5. Consider the Hermitian function field $H = \mathbb{F}_{q^2}(x,y)$, i.e. the extension of the rational function field $F = \mathbb{F}_{q^2}(x)$ defined by $y^q + y = x^{q+1}$. Consider the rational AG-code $\mathcal{C}_q = C_{\mathcal{L}}^F(D, qP_\infty)$, where D is the sum of all the rational places of F different from P_∞, with parameters $[q^2, q+1]$ and let $\mathcal{H}_a = C_{\mathcal{L}}^H(D', aQ_\infty)$ be the Hermitian code, where D' is the sum of all the places over the support of D, with parameters $[q^3, k']$.

We have seen that $\mathcal{H}_a$ is the conorm code of C_q if q divides a. Thus we can take, for instance, $a = 3q^2$. By (b) of Proposition 8.3.3 of [8], the code $\mathcal{H}_{3q^2}$ has dimension

$$k' = \dim(\mathcal{H}_{3q^2}) = 3q^2 + 1 - \tfrac{1}{2}q(q-1) = \tfrac{5q^2+q}{2} + 1.$$

Now, on the one hand, since $\mathcal{H}_a^\perp = \mathcal{H}_{q^3+q^2-q-2-a}$ for any a, in our case we have

$$\mathrm{Con}(\mathcal{C}_q)^\perp = \mathcal{H}_{3q^2}^\perp = \mathcal{H}_{q^3-2q^2-q-2}$$

with parameters $[q^3, k^\perp]$. It is clear that

$$k^\perp = q^3 - k' = q^3 - \tfrac{5q^2+q+2}{2} > 0,$$

for any $q \geq 3$.

On the other hand, $\mathcal{C}_q^\perp = C_\mathcal{L}^F(D, G^\perp)$ with $G^\perp = D - qP_\infty + (\eta)$ is a $[q^2, q^2-q-1]$-code, where η is a Weil differential. The conorm code is $\mathrm{Con}(\mathcal{C}_q^\perp)$ with parameters $[q^3, \tilde{k}]$. By (14) of Proposition 1 we have

$$\begin{aligned} \tilde{k} &\geq q(\deg G^\perp + 1 - g) - \tfrac{1}{2}\deg \mathrm{Diff}(H/F) \\ &= q(q^2-q-2) - \tfrac{1}{2}(q^2-q) = q^3 - \tfrac{3q^2-3q}{2} = q^3 - \tfrac{3}{2}q(q+1) > 0, \end{aligned}$$

for any $q \geq 3$.

It is straightforward to check that $k^\perp < \tilde{k}$ if and only if $q^2+1 > q$ and this last inequality holds for every q. Since the dimensions of the codes $\mathrm{Con}(\mathcal{C}_q)^\perp$ and $\mathrm{Con}(\mathcal{C}_q^\perp)$ are different, we have that

$$\mathrm{Con}(\mathcal{C}_q)^\perp \neq \mathrm{Con}(\mathcal{C}_q^\perp),$$

as we wanted to show. For instance, if $q = 3$ the parameters of the codes $\mathrm{Con}(\mathcal{C}_3)^\perp$ and $\mathrm{Con}(\mathcal{C}_3^\perp)$ over $H = \mathbb{F}_9(x,y)$, $y^3 + y = x^4$, are $[27, 2]$ and $[27, \geq 9]$, respectively. Also, the parameters of the codes $\mathrm{Con}(\mathcal{C}_4)^\perp$ and $\mathrm{Con}(\mathcal{C}_4^\perp)$ over $H = \mathbb{F}_{16}(x,y)$ with $y^4 + y = x^5$ are $[64, 21]$ and $[64, \geq 34]$, respectively.

Reed-Solomon codes. As a final application, we show that classical Reed-Solomon codes can be obtained as conorm codes of rational cyclic AG-codes.

Proposition 5. *Any Reed-Solomon code is a conorm code.*

Proof. Let $n = q-1$ and k be such that $1 \leq k \leq n$ and let us consider the Reed-Solomon code

$$\mathcal{C}_k = \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) : f \in \mathcal{L}_k)\}$$

over $\mathbb{F}_q$, where $\beta \in \mathbb{F}_q$ is a primitive element of the subgroup $\mathbb{F}_q^*$ and

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[x] : \deg f \leq k-1\}.$$

The code $\mathcal{C}_k$ can be represented as a rational AG-code as follows. Let $F = \mathbb{F}_q(x)$ be a rational function field and denote by P_i the zero of $x - \beta^i$ in F for $i = 1, \ldots, n$, and by P_∞ the pole of x in F. Let $u \in F$ be such that $u(P_i) = 1$ for $i = 1, \ldots, n$ (such an element exists by the Approximation theorem). Now, letting

$$D = P_1 + \cdots + P_n \qquad \text{and} \qquad G = (k-1)P_\infty + (u),$$

where (u) denotes the principal divisor of u in F, we have (see Proposition 2.3.5 of [8]) that $\mathcal{C}_k = \mathcal{C}_\mathcal{L}(D, G)$.

Let us consider now the field extension $F'/F = \mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ where x and y satisfy

$$y^n = (x-\beta)(x-\beta^2)\cdots(x-\beta^n).$$

By Proposition 6.3.1 in [8] we have that F'/F is a cyclic extension of degree n and the places $P_1, \ldots, P_n$ are totally ramified in F'/F. In this way, we are in the hypothesis of Theorem 5.5 and Corollary 4 and thus

$$\mathcal{C}' = \mathrm{Con}(\mathcal{C}_k) = \mathcal{C}_\mathcal{L}(\mathrm{Con}(D), \mathrm{Con}(G))$$

satisfies $\mathcal{C}' = \mathcal{C}_k$, as we wanted to show. □

Final Remarks

Generalized conorm codes. The definition of conorm code given in Section 2 can be generalized as follows. Let F'/F be a finite extension of function fields over $\mathbb{F}_q$ and let $\mathcal{C} = C_{\mathcal{L}}^{F}(D,G)$ be an AG-code as in (1). Suppose that every place P' of F' over any place $P \in \mathrm{Supp}(D)$ is rational. We define the *generalized conorm code* associated to $\mathcal{C}$, or just the *conorm of* $\mathcal{C}$, as

$$\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C}) = C_{\mathcal{L}}^{F'}(D',G'), \tag{26}$$

where

$$D' = \sum_{i=1}^{n} \sum_{Q|P_i} Q \qquad \text{and} \qquad G' = \mathrm{Con}_{F'/F}(G).$$

Note: For any given AG-code $\mathcal{C} = C_{\mathcal{L}}^{F}(D,G)$ over a function field $F/\mathbb{F}_q$, we can always find a field extension F' of F such that the condition on the rationality of the places above the places in the support of D holds: we just take a suitable constant field extension $F' = F\mathbb{F}_{q^t}$ of F.

This construction of generalized conorm codes behaves well on finite towers of function fields. That is, given $F \subset F' \subset F''$ and $\mathcal{C} = C_{\mathcal{L}}^{F}(D,G)$ we have

$$\mathrm{Con}_{F''/F}(\mathcal{C}) = \mathrm{Con}_{F''/F'}(\mathrm{Con}_{F'/F}(\mathcal{C})), \tag{27}$$

or, in other words, if $\mathcal{C}' = \mathrm{Con}_{F'/F}(\mathcal{C})$, then

$$\mathcal{C}'' = \mathrm{Con}_{F''/F'}(\mathcal{C}') = \mathrm{Con}_{F''/F}(\mathcal{C}).$$

This is a direct consequence of the fact that

$$\mathrm{Con}_{F''/F}(G) = \mathrm{Con}_{F''/F'}(\mathrm{Con}_{F'/F}(G)),$$

for any divisor G in F and the fact that if every place R in F'' over a place P in the support of D is rational, then every place Q in F' over a place P in the support of D is also rational. Furthermore

$$\bigcup_{P \,\in\, \mathrm{Supp}\, D} \{R \mid P : R \in \mathbb{P}(F'')\} = \bigcup_{Q \,\in\, \mathrm{Supp}\, D'} \{R \mid Q : R \in \mathbb{P}(F'')\}.$$

Notice that with the definition of conorm codes given in Section 2, the equality (27) was obtained in the particular cases of complete splitting or total ramification of the places in $\mathrm{Supp}(D)$. Moreover when every place in $\mathrm{Supp}(D)$ splits completely in F', we have that D' is actually the conorm of D.

Code-based cryptography. Different families of codes have proved to be insecure for code-based cryptography and there have been many attempts to replace traditional Goppa codes. In [5], Janwa and Moreno proposed to use a collection of AG-codes on curves for the McEliece cryptosystem, but this was broken for codes on curves of genus $g \leq 2$ by Faure and Minder ([3]).

Couvreur, Márquez-Corbella, Martínez-Moro, Pellikaan and Ruano ([2] and [6]) have managed to break certain higher-genus cryptosystems based on evaluation codes, but none of these attacks are against subfield subcodes. The security status of the McEliece public key cryptosystem using algebraic geometry codes is, to the best of our knowledge, still not completely settled and remains as an open problem.

The construction of taking conorm codes can be iterated, so in principle it can be applied to a code defined over the base field of a tower of function fields. By the results in Theorem 5.5 and Corollary 4 we can begin with a cyclic AG-code defined over the rational function field ($g = 0$). Under appropriate conditions, we get the same code (as a conorm code) defined on a bigger field with greater genus. The procedure can be repeated in such a manner to get the same algebraic cyclic code defined on a function field of genus arbitrarily large. Can this procedure be useful in some way in code-based cryptography? This is a question we hope to answer in a forthcoming work.

References

[1] D. Bartoli, L. Quoos and G. Zini, Algebraic geometric codes on many points from Kummer extensions, *Finite Fields and Their Applications*, **52** (2018), 319–335.

[2] A. Couvreur, I. Márquez-Corbella and R. Pellikaan, A polynomial time attack against algebraic geometry code based public key cryptosystem, *IEEE International Symposium on Information Theory*, (2014), 1446–1450.

[3] C. Faure and H. Minder, Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes, *11th Int. Workshop Algebraic and Combinat. Coding Theory, Pamporovo Bulgaria*, **8** (2008), 99–107.

[4] A. Garcia and H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *Journal of Number Theory*, **61:2** (1996), 248–273.

[5] H. Janwa and O. Moreno, McEliece public crypto system using algebraic-geometric codes, *Designs, Codes and Cryptography*, **8** (1996), 293–307.

[6] I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan and D. Ruano, Computational aspects of retrieving a representation of an algebraic geometry code, *Journal of Symbolic Computation*, **64**, (2014) 67–87.

[7] C. Munuera and R. Pellikaan, Equality of geometric Goppa codes and equivalence of divisors, *Journal of Pure and Applied Algebra*, **90** (1993) 229–252.

[8] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2^{nd} edition, Graduate Texts in Mathematics, 254, Springer-Verlag, Berlin, 2009.

[9] C. Voss and T. Hoholdt, An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps, *IEEE Transactions on Information Theory*, **43:1** (1997), 128–135.

[10] J. Wülftange, On the construction of some towers over finite fields, in *Finite Fields and Applications. Fq 2003*, Lecture Notes in Computer Science, 2948, Springer, Berlin, Heidelberg, 2004.

Received November 2020; revised March 2021.

E-mail address: mchara@santafe-conicet.gov.ar
E-mail address: podesta@famaf.unc.edu.ar
E-mail address: ridatole@gmail.com