LIFTING ISO-DUAL ALGEBRAIC GEOMETRY CODES

MARÍA CHARA, RICARDO PODESTÁ, LUCIANE QUOOS, RICARDO TOLEDANO

November 16, 2023

ABSTRACT. In this work we investigate the problem of producing iso-dual algebraic geometry (AG) codes over a finite field $\mathbb{F}_q$ with q elements. Given a finite separable extension $\mathcal{M}/\mathcal{F}$ of function fields and an iso-dual AG-code $\mathcal{C}$ defined over $\mathcal{F}$, we provide a general method to lift the code $\mathcal{C}$ to another iso-dual AG-code $\tilde{\mathcal{C}}$ defined over $\mathcal{M}$ under some assumptions on the parity of the involved different exponents. We apply this method to lift iso-dual AG-codes over the rational function field to elementary abelian p-extensions, like the maximal function fields defined by the Hermitian, Suzuki, and one covered by the *GGS* function field. We also obtain long binary and ternary iso-dual AG-codes defined over cyclotomic extensions.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with q elements. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ for $n \geq 1$. Associated to a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ we have three parameters: its length n, its dimension k as a vector space over $\mathbb{F}_q$ and its minimum distance d (Hamming distance). In the 1980's, using concepts and tools coming from algebraic geometry, Goppa constructed error-correcting linear codes from function fields defined over a finite field, see [13] and [14]. They are called algebraic geometry (AG) codes and have played an important role in the theory of error-correcting codes. They were used to improve the Gilbert–Varshamov bound about the limit of the parameters of a code [35], and this was a remarkable result at that time. Moreover, every linear code can be realized as an algebraic geometry code [27].

Let us recall first the definition of an algebraic geometry code. We use the language of function fields over finite fields following [32]. For a function field $\mathcal{F}/\mathbb{F}_q$, consider the divisor $D = P_1 + \cdots + P_n$ given by the sum of pairwise distinct rational places of $\mathcal{F}$, and another divisor G such that P_i is not in the support of G for $i = 1, \ldots, n$. The linear *algebraic geometry code* $C_{\mathcal{L}}(D, G)$ defined over $\mathcal{F}$ is given by

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) \, : \, f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n, \tag{1.1}$$

where $\mathcal{L}(G) = \{z \in \mathcal{F} \, : \, (z) \geq -G\} \cup \{0\}$ denotes the Riemann-Roch space associated to the divisor G.

Key words and phrases. Isodual codes, AG-codes, algebraic function field, tower of function fields.

2020 *Mathematics Subject Classification.* Primary 11T71, 14G50, 94B05, 94B27.

The first, second and fourth authors are partially supported by CONICET, FONCyT, SECyT-UNC, and CAI+D-UNL. The third author was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, CAPES MATH AMSUD 88881.647739/2021-01 .

Recall now that the dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is the orthogonal complement of $\mathcal{C}$ in $\mathbb{F}_q^n$ with respect to the standard inner product of $\mathbb{F}_q^n$. A code is said to be *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. Self-dual codes have been investigated in [23], they have applications to quantum codes through a construction in [17] (see also [4], [19] and [24]); and new constructions have been recently proposed in, for example, [29] and [33]. In [5], infinite families of self-dual codes which are asymptotically better than the asymptotic Gilbert–Varshamov bound were constructed.

The condition of being self-dual can be relaxed by considering the following notion of equivalence of linear codes: two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be *equivalent* if there exists a vector $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that $\mathcal{C}_1 = \mathbf{x} \cdot \mathcal{C}_2$. Now a linear code $\mathcal{C}$ is called *iso-dual* if it is equivalent to its dual code $\mathcal{C}^\perp$, that is if there exists a non zero vector $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that

$$\mathcal{C}^\perp = \mathbf{x} \cdot \mathcal{C}.$$

We will speak of $\mathbf{x}$-iso-dual codes when mentioning the vector $\mathbf{x}$ explicitly is needed.

The main goal of this work is to investigate the construction of iso-dual AG codes. They were first studied in full generality in [30], where several concrete examples of iso-dual AG codes over function fields of arbitrary genus over a finite field were given. Much later it was proved in [31] that the class of iso-dual codes attains the Tsfasman-Vladut and Zink bound over a finite field of quadratic cardinality. Iso-dual AG codes also showed up in the study of the so called order bounds for the minimum distance of AG-codes (see, for instance, [11] and the references therein). Overall the construction of iso-dual codes in a function field poses a significant challenge, as it relies on a deep understanding of differentials and function divisors possessing specific properties (see Proposition 2.6). We propose here an alternative method to construct them (see Theorem 4.1): given a finite separable extension $\mathcal{M}/\mathcal{F}$ of function fields and an iso-dual AG-code $\mathcal{C}$ defined over $\mathcal{F}$, we use the conorm map (see Section 2) to lift the AG-code $\mathcal{C}$ to another iso-dual AG-code over $\mathcal{M}$. We obtain in this way a longer iso-dual AG-code whose parameters can be estimated in the standard way (see Corollary 4.3) in many cases. To the best of our knowledge, iso-dual codes have not undergone a thorough investigation.

We employ this method of lifting iso-dual AG-codes across various scenarios. The most favourable of them is when $\mathcal{F}$ is a rational function field, because iso-dual codes over a rational function field can be easily constructed (see item (c) of Proposition 2.6). In particular with our method we can construct iso-dual codes over *maximal function fields*, that is, function fields defined by algebraic curves $\mathcal{X}$ of genus $g(\mathcal{X})$ such that its number $\mathcal{X}(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 + 2g(\mathcal{X})q.$$

Maximal curves are a fruitful ambient for explicit constructions of codes, since its is well know that curves with a small genus with respect its number of rational points, produce codes with better relative parameters. Research in codes in recent years has proven to be a highly productive field of investigation. For instance, construction of locally recoverable codes over maximal curves can be found in [3] or [7], AG-codes over the maximal Beelen-Montanucci curve [20], weights of dual codes over the maximal GK-curve [2], lifting of

AG-codes in [8]. The maximal Hermitian curve was used for applications to quantum codes [9], self orthogonal maximum distance separable codes [21], investigation of the isometry-dual property in flags of codes [6], construction of codes using places of higher degree [22], and many point codes in [18].

The paper is organized as follows. In Section 2 we present the necessary background on the theory of function fields and codes. We recall some definitions and basic facts on AG-codes and iso-dual AG-codes. In Section 3, we construct families of iso-dual and self-dual AG-codes $C_{\mathcal{L}}(D, G)$ over the Hermitian function field $\mathcal{H}/\mathbb{F}_{q^2}$ (see Theorem 3.1). In Section 4, given a finite separable extension $\mathcal{M}/\mathcal{F}$ of algebraic function fields we propose a way to lift an iso-dual code over $\mathcal{F}$ to an iso-dual code over $\mathcal{M}$, given certain constrains in the extension (see Theorem 4.1). In Corollary 4.3 we give the parameters of the lifted code. In Section 5 we consider elementary abelian p-extensions extensions of the rational function field. By lifting iso-dual rational AG-codes we obtain iso-dual AG-codes over the Hermitian, Suzuki and GGS curves. In Section 6 we consider a new curve $\mathcal{X}$ obtained as an extension of the Hermitian function field. We compute its genus and its number of rational points and in Theorem 6.2 we show how to obtain iso-dual AG-codes defined over $\mathcal{X}$ using our method of lifting iso-dual codes. Finally, in Section 7 we consider cyclotomic extensions. By lifting very simple iso-dual codes AG-codes over binary and ternary rational function fields, we get long binary and ternary iso-dual AG-codes over subfields of cyclotomic extensions (see Theorems 7.2 and 7.3).

2. Preliminaries

Here we recall some basic facts of extensions of algebraic function fields, divisors, AG-codes and iso-dual AG-codes.

Algebraic function fields. Let $\mathcal{F}/\mathbb{F}_q$ be an algebraic function field in one variable of genus $g = g(\mathcal{F})$. We denote by $\mathcal{P}_{\mathcal{F}}$ the set of places in $\mathcal{F}$, by $\Omega_{\mathcal{F}}$ the space of Weil differentials in $\mathcal{F}$, by v_P the discrete valuation of $\mathcal{F}/\mathbb{F}_q$ associated to the place $P \in \mathcal{P}_{\mathcal{F}}$, and by $\mathrm{Div}(\mathcal{F})$ the free abelian group generated by the places in $\mathcal{F}$. An element in $\mathrm{Div}(\mathcal{F})$ is called a divisor. For a function $z \in \mathcal{F}$ we let $(z)^{\mathcal{F}}, (z)^{\mathcal{F}}_{\infty}$ and $(z)^{\mathcal{F}}_0$ stand for the principal, pole and zero divisors of the function z in $\mathcal{F}$, respectively. Two divisors $A, B \in \mathrm{Div}(\mathcal{F})$ are equivalent, denoted $A \sim B$, if they differ by a principal divisor, i.e. $B = A + (z)^{\mathcal{F}}$ for some $z \in \mathcal{F}$.

Let us consider now a separable function field extension $\mathcal{F}'/\mathcal{F}$. The conorm of a place P in $\mathcal{F}$ is the divisor in $\mathcal{F}'$ defined by

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

where $e(Q|P)$ denotes the ramification index of Q over P. For a divisor D in $\mathrm{Div}(\mathcal{F})$ the *conorm* map is the natural homomorphism from $\mathrm{Div}(\mathcal{F})$ to $\mathrm{Div}(\mathcal{F}')$ extended by linearity; that is,

$$\mathrm{Con}_{\mathcal{F}'/\mathcal{F}}\Big(\sum_i n_i P_i\Big) = \sum_i n_i\, \mathrm{Con}_{\mathcal{F}'/\mathcal{F}}(P_i). \tag{2.1}$$

Suppose that $\mathcal{F}'$ and $\mathcal{F}$ have fields of constants K' and K, respectively (in the paper, however, we will only consider geometric extensions of functions fields, i.e. with $K' = K$). From Theorem 3.4.6 in [32] we have that for every Weil differential ω of $\mathcal{F}/K$ there exists a unique Weil differential ω' in $\mathcal{F}'/K'$ such that $\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega(\mathrm{Tr}_{F'/F}(\alpha))$ for every α in the adele space $\mathcal{A}_{F'/F} = \{\alpha \in \mathcal{A}_{\mathcal{F}'} : \alpha_{P'} = \alpha_{Q'}$ whenever $P' \cap F = Q' \cap F\}$. This Weil differential is called the *cotrace* of ω in $\mathcal{F}'/\mathcal{F}$ and it is denoted by $\mathrm{Cotr}_{\mathcal{F}'/\mathcal{F}}(\omega)$. If $\omega \neq 0$ and (ω) is the corresponding divisor in $\mathcal{F}$, one has

$$(\mathrm{Cotr}_{\mathcal{F}'/\mathcal{F}}(\omega)) = \mathrm{Con}_{\mathcal{F}'/\mathcal{F}}((\omega)) + \mathrm{Diff}(\mathcal{F}'/\mathcal{F}), \tag{2.2}$$

with $\mathrm{Diff}(\mathcal{F}'/\mathcal{F})$ the different divisor of $\mathcal{F}'/\mathcal{F}$ defined by

$$\mathrm{Diff}(\mathcal{F}'/\mathcal{F}) = \sum_{P \in P_{\mathcal{F}}} \sum_{P'|P} d(P'|P)\, P \tag{2.3}$$

where $d(P'|P) \geq 0$ is the different exponent of $P'|P$ (which is 0 for almost all places). We recall that if $\mathcal{F}'/\mathcal{F}$ is also finite and g' and g denote the genera of $\mathcal{F}'$ and $\mathcal{F}$ respectively, then the Riemann-Hurwitz genus formula asserts that

$$2g' - 2 = [\mathcal{F}' : \mathcal{F}](2g - 2) + \deg(\mathrm{Diff}(\mathcal{F}'/\mathcal{F})) \tag{2.4}$$

(see for instance Theorem 3.4.13 in [32]).

Iso-dual AG-codes. A linear code $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ with $n \geq 1$. Associated to a code we have three important parameters, its length n, its dimension k as a vector subspace over $\mathbb{F}_q$, and its minimum (Hamming) distance d. One says that $\mathcal{C}$ is an $[n, k, d]$-code. From now on we will use AG-codes $C_{\mathcal{L}}(D, G)$ over an algebraic function field $\mathcal{F}/\mathbb{F}_q$ as defined in (1.1).

We now recall the basic bounds for the parameters of an AG-code.

Proposition 2.1. *The AG-code $C_{\mathcal{L}}(D, G)$ as in (1.1) is an $[n, k, d]_q$-code with*

$$k = \ell(G) - \ell(G - D) \qquad \text{and} \qquad d \geq n - \deg(G). \tag{2.5}$$

Moreover, we have that:

(a) If $\deg(G) < n$, then $k = \ell(G) \geq \deg(G) + 1 - g$.

(b) If $2g - 2 < \deg(G) < n$, then $k = \ell(G) = \deg(G) + 1 - g$.

Proof. See for instance Theorem 2.2.2 and Corollary 2.2.3 in [32]. □

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code and $\mathbf{x} = (x_1, \ldots, x_n) \in (\mathbb{F}_q^\times)^n$. The set

$$\mathbf{x} \cdot \mathcal{C} := \{(x_1 c_1, \ldots, x_n c_n) : (c_1, \ldots, c_n) \in \mathcal{C}\},$$

is clearly another linear code over $\mathbb{F}_q$. We notice that the codes $\mathcal{C}$ and $\mathbf{x} \cdot \mathcal{C}$ have the same length, dimension and minimum distance. We use the same notion of equivalence as in Definition 2.2.13 of [32].

Definition 2.2. Two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_q$ are *equivalent* if $\mathcal{C}_2 = \mathbf{x} \cdot \mathcal{C}_1$ for some $\mathbf{x} \in (\mathbb{F}_q^\times)^n$. In this case we write $\mathcal{C}_1 \sim_{\mathbf{x}} \mathcal{C}_2$, or simply $\mathcal{C}_1 \sim \mathcal{C}_2$ when the distinction of the vector $\mathbf{x}$ is not necessary.

In the next proposition we collect well-known results on the equivalence of AG-codes.

Proposition 2.3. *Let $C_{\mathcal{L}}(D,G)$ be an AG-code with $D = P_1 + \cdots + P_n$.*

(a) *If $C_{\mathcal{L}}(D,G')$ is another AG-code, then $C_{\mathcal{L}}(D,G) \sim C_{\mathcal{L}}(D,G')$ if and only if $G \sim G'$.*
(b) *Moreover, for $z \in \mathcal{F}$ such that $z(P_i) \neq 0$ for $i = 1,\ldots,n$ we have that*

$$C_{\mathcal{L}}(D, G-(z)) = \mathbf{x}\cdot C_{\mathcal{L}}(D,G),$$

where $\mathbf{x} = (z(P_1),\ldots,z(P_n)) \in (\mathbb{F}_q^*)^n$.

Proof. See for instance Proposition 2.2.14 in [32]. □

The dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ over $\mathbb{F}_q$ is the orthogonal complement of $\mathcal{C}$ in $\mathbb{F}_q^n$ with the standard inner product of $\mathbb{F}_q^n$. For AG-codes, we have the following.

Proposition 2.4. *The dual code of $C_{\mathcal{L}}(D,G)$ is still a linear AG-code, in fact*

$$C_{\mathcal{L}}(D,G)^\perp = C_{\mathcal{L}}(D, D-G+(\eta)) \tag{2.6}$$

where η is a Weil differential in $\mathcal{F}$ such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$, for $i = 1,\ldots,n$.

Proof. See for instance Proposition 2.2.10 in [32]. □

Recall that a linear code $\mathcal{C}$ is said to be *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. The notion of equivalence of linear codes allows one to define the following class of linear codes generalizing self-dual codes.

Definition 2.5. Let $\mathbf{x} \in (\mathbb{F}_q^*)^n$. A code $\mathcal{C} \subset \mathbb{F}_q^n$ is called $\mathbf{x}$-*iso-dual* if $\mathcal{C}^\perp = \mathbf{x}\cdot\mathcal{C}$. We will simply speak of *iso-dual* codes when there is no need to specify the vector $\mathbf{x}$.

Clearly the class of iso-dual codes contains the class of the self-dual codes, that is, $\mathbf{x}$-iso-dual codes are just self-dual codes with $\mathbf{x} = (1,1,\ldots,1)$. We observe that our definition of $\mathbf{x}$-iso-dual code is a particular case of iso-dual code where the equivalence of codes is given in terms of the monomial equivalence of codes, that is codes which are isometric to their duals via a permutation of coordinates and multiplying certain coordinates by non-zero constants (see, for instance, [16]).

We now recall necessary and sufficient conditions for an AG-code to be iso-dual.

Proposition 2.6. *Let $C_{\mathcal{L}}(D,G)$ be an AG-code of length n defined as in (1.1) over a function field $\mathcal{F}$ of genus g.*

(a) *$C_{\mathcal{L}}(D,G)$ is iso-dual if there exists a canonical divisor W such that $W \sim 2G - D$. More precisely,*

$$C_{\mathcal{L}}(D,G)^\perp = \mathbf{x}\cdot C_{\mathcal{L}}(D,G)$$

where $\mathbf{x} = (\mathrm{res}_{P_1}(\omega),\ldots,\mathrm{res}_{P_n}(\omega))$ with ω a Weil differential such that $W \sim (w)$.
(b) *Reciprocally, if $C_{\mathcal{L}}(D,G)$ is iso-dual then there exists a canonical divisor W such that $W \sim 2G - D$ with $v_P(W) = -1$ for any $P \in \mathrm{supp}(D)$. In particular, n is even and $\deg(G) = \frac{1}{2}(n + 2g - 2)$.*
(c) *In particular, if $\mathcal{F}$ is a rational function field and $n \geq 2$ is even, then $C_{\mathcal{L}}(D,G)$ is iso-dual if and only if $\deg G = \frac{1}{2}(n-2)$.*

3. Iso-dual AG-codes over the Hermitian function field

In general, it is a challenging problem to construct iso-dual codes in a function field since it strongly depends on the knowledge of differentials and divisors with suitable properties. We illustrate the problem in this section by presenting a family of iso-dual codes over the Hermitian function field that are self-dual in some cases. In the next section we will propose a method to lift a known iso-dual code in an extension of function fields. This method will provide an easier way to obtain iso-dual codes over an algebraic curve.

The Hermitian function field $\mathcal{H}/\mathbb{F}_{q^2}$, as a tamely ramified extension of $\mathbb{F}_{q^2}(x)$, is the function field $\mathcal{H} = \mathbb{F}_{q^2}(x,y)$ given by the affine equation

$$y^{q+1} = x^q + x. \tag{3.1}$$

It is well known (see Lemma 6.4.4 of [32]) that $\mathcal{H}$ has q^3+1 rational places and genus

$$g = \tfrac{1}{2}q(q-1).$$

For $i = 1, \ldots, q$, let Q_i be the totally ramified places; that is, Q_i is a place over P_i in the rational function field $\mathcal{F} = \mathbb{F}_{q^2}(x)$ corresponding to a root α_i of $x^q + x = 0$. For each $\alpha \in \mathbb{F}_{q^2}$ with $\alpha^q + \alpha \neq 0$ we have $q+1$ places in $\mathbb{F}_{q^2}(x,y)$ over the place P_α in $\mathbb{F}_{q^2}(x)$ associated to the zero of the function $x - \alpha$.

In 2021, L. Sok proposed many families of self-dual codes $C_{\mathcal{L}}(D,G)$ over the Hermitian function field in the case the divisor G has support in one point (the only pole of x) in the function field (see [29, Theorem 9]). Here we propose families of iso-dual codes over the Hermitian function field where the support of G consist of all the totally ramified places in $\mathcal{H}/\mathbb{F}_{q^2}(x)$.

Theorem 3.1. *Let $\mathcal{H} = \mathbb{F}_{q^2}(x,y)$ be the Hermitian function field of genus $g = \frac{1}{2}q(q-1)$ defined by $y^{q+1} = x^q + x$. Let β a non-zero integer and consider the disjoint divisors*

$$D = \sum_{\alpha^q+\alpha\neq 0} Q|P_\alpha, \qquad \text{and} \qquad G = \big(\tfrac{1}{2}(q^3+q^2-2q-2) - q\beta\big)Q_\infty + \beta\sum_{i=1}^{q} Q_i,$$

where the Q_i are all the totally ramified places in $\mathcal{H}/\mathbb{F}_{q^2}$ associated to a root α_i of $x^q+x=0$ and $\deg G > 0$. Then, the code $C_{\mathcal{L}}(D,G)$ is $\mathbf{x}$-iso-dual with parameters

$$[n = q^3 - q,\ k = \tfrac{1}{2}(q^3-q),\ d \geq \tfrac{1}{2}q^2(q-1)+1],$$

where $\mathbf{x} = (z(P_1), \ldots, z(P_n))$ with $z = y^{2\beta+2-q^2}$. Moreover, if q^2-1 is a divisor of $2\beta+1$ (hence q is even), then $C_{\mathcal{L}}(D,G)$ is self-dual.

Proof. We will use (a) in Proposition 2.6. Let $\mathcal{H} = \mathbb{F}_{q^2}(x,y)$ be the Hermitian function field defined by the affine equation $y^{q+1} = x^q + x$ and $\mathcal{F} = \mathbb{F}_{q^2}(x)$ the rational function field. Consider the function $t \in \mathbb{F}_p(x)$, where $p = \mathrm{Char}(\mathbb{F}_q)$, given by

$$t = \frac{x^{q^2} - x}{x^q + x}. \tag{3.2}$$

Then, we clearly have that $v_P(t) = 1$ for any $P \in \mathrm{supp}(D)$. Thus, from Proposition 8.1.2 in [32], the Weil differential $\eta := \frac{1}{t}dt$ satisfies $v_P(\eta) = -1$ and $\mathrm{res}_P(\eta) = 1$ for any

$P \in \mathrm{supp}(D)$. Hence, if $W := (\frac{1}{t}dt)^{\mathcal{H}}$ is the canonical divisor of the differential $\frac{1}{t}dt$ in $\mathcal{H}$, we have that

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D, D-G+W).$$

Now, we explicitly compute $W = \left(\frac{1}{t}dt\right)^{\mathcal{H}} = \left(\frac{1}{t}\frac{dt}{dx}dx\right)^{\mathcal{H}}$. From (3.2) we have

$$dt = -\frac{x^{q^2}+x^q}{(x^q+x)^2}dx = -(x^q+x)^{q-2}dx.$$

Hence, from $\mathrm{Diff}(\mathcal{H}/\mathcal{F}) = \sum_{i=1}^{q} qQ_i + qQ_\infty$, we compute the divisor W

$$\begin{aligned}
W &= \Big(-(x^q+x)^{q-2}\,\frac{x^q+x}{x^{q^2}-x}\,dx\Big)^{\mathcal{H}} \\
&= \Big(\frac{(x^q+x)^{q-1}}{x^{q^2}-x}\Big)^{\mathcal{H}} + (dx)^{\mathcal{H}} \\
&= (q-1)(x^q+x)^{\mathcal{H}} - (x^{q^2}-x)^{\mathcal{H}} - 2(x)_{\infty}^{\mathcal{H}} + \mathrm{Diff}(\mathcal{H}/\mathcal{F}) \\
&= (q^2-1)\Big(\sum_{i=1}^{q} Q_i - qQ_\infty\Big) - \Big(D + \sum_{i=1}^{q}(q+1)Q_i - (q^3+q^2)Q_\infty\Big) \\
&\qquad - 2(q+1)Q_\infty + q\sum_{i=1}^{q} Q_i + qQ_\infty \\
&= -D + (q^2-2)\sum_{i=1}^{q} Q_i + (q^2-2)Q_\infty.
\end{aligned}$$

Now, we notice that $2G - D - W$ equals

$$(q^3+q^2-2q-2-2q\beta)Q_\infty + 2\beta\sum_{i=1}^{q} Q_i - D - \big(-D + (q^2-2)\sum_{i=1}^{q} Q_i + (q^2-2)Q_\infty\big)$$

and, hence, we have that

$$2G - D - W = (q^3 - 2q - 2q\beta)Q_\infty + (2\beta - q^2 + 2)\sum_{i=1}^{q} Q_i = (y^{2\beta+2-q^2})^{\mathcal{H}}.$$

Let $z := y^{2\beta+2-q^2}$. Then, we have obtained that $D - G + W = G - (z)^{\mathcal{H}}$ and we can show that the code is iso-dual. In fact, it is $\mathbf{x}$-iso-dual since

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D, D-G+W) = C_{\mathcal{L}}(D, G-(z)^{\mathcal{H}}) = \mathbf{x}\cdot C_{\mathcal{L}}(D,G),$$

where $\mathbf{x} = (z(P_1), \ldots, z(P_n)) \in (\mathbb{F}_{q^2}^*)^n$ is the vector given by the computation of the function z in all the places P in $\mathrm{supp}(D)$.

The length of the code is given by $n = \deg(D) = q^3 - q$. The dimension is $k = \frac{1}{2}n$ since the code is iso-dual. By (2.5), the minimum distance satisfies $d \geq n - \deg(G) = \frac{q^3-q^2+2}{2}$.

Finally, $C_{\mathcal{L}}(D,G)$ is self-dual if and only if the vector $\mathbf{x}$ equals $(1,\ldots,1)$. Let

$$x_i = z(P_i) = y(P_i)^{2\beta+2-q^2} \in \mathbb{F}_{q^2}.$$

Then, $C_{\mathcal{L}}(D,G)$ is self-dual if and only if

$$x_i^{q^2-1} = x_i^{2\beta+2-q^2} = 1$$

for every $i = 1, \ldots, n$. Choosing β such that q^2-1 divides $2\beta+1$ we obtain that the code $C_{\mathcal{L}}(D,G)$ is self-dual. □

For example, for any choice of $\beta \in \mathbb{Z} \setminus \{0\}$ we get Hermitian iso-dual AG-codes (and self-dual AG-codes if we further take $\beta = \frac{1}{2}((q^2-1)t-1)$ for some $t \in \mathbb{N}$) with parameters $[60, 30, \geq 25]$ over $\mathbb{F}_{4^2}$, $[720, 360, \geq 325]$ over $\mathbb{F}_{9^2}$, $[4080, 2040, \geq 1921]$ over $\mathbb{F}_{16^2}$ and $[15600, 7800, \geq 7501]$ over $\mathbb{F}_{25^2}$.

4. Lifting iso-dual AG-codes on function field extensions

Let $\mathcal{M}/\mathcal{F}$ be a finite and separable extension of function fields defined over $\mathbb{F}_q$. Here we provide a construction that allows to lift an iso-dual dual AG-code defined over $\mathcal{F}$ to an iso-dual AG-code defined over $\mathcal{M}$.

Given an iso-dual AG-code $C_{\mathcal{L}}(D,G)$ over $\mathcal{F}$, we want to lift it to an iso-dual code over $\mathcal{M}$, that is, we want to define a code $\tilde{C}_{\mathcal{L}} = C_{\mathcal{L}}(\tilde{D},\tilde{G})$ over $\mathcal{M}$ such that for some $\tilde{\mathbf{x}} \in \mathbb{F}_q^n$ we have

$$C_{\mathcal{L}}(\tilde{D},\tilde{G})^{\perp} = \tilde{\mathbf{x}} \cdot C_{\mathcal{L}}(\tilde{D},\tilde{G}).$$

In the following result, we give conditions on the function field extension $\mathcal{M}/\mathcal{F}$ for an iso-dual code defined over $\mathcal{F}$ to be lifted to an iso-dual code defined over $\mathcal{M}$.

Theorem 4.1. *Let $\mathcal{M}/\mathcal{F}$ be a finite separable extension of function fields over $\mathbb{F}_q$ of degree $m \geq 2$ with genera $g_{\mathcal{M}}$ and $g_{\mathcal{F}}$, respectively. Let $n \geq 1$ be an even integer and suppose that $\{P_1, \ldots, P_n\}$ and $\{Q_1, \ldots, Q_r\}$ are disjoint set of places of $\mathcal{F}$ such that:*

(a) *$P_1, \ldots, P_n$ are rational places and P_i splits completely in $\mathcal{M}/\mathcal{F}$ for $1 \leq i \leq n$,*
(b) *the extension $\mathcal{M}/\mathcal{F}$ is unramified outside the set $\{Q_1, \ldots, Q_r\}$ for some $r \geq 1$, and*
(c) *for each $1 \leq i \leq r$ and each place R of $\mathcal{M}$ lying over Q_i the different exponent $d(R|Q_i)$ is even.*

Let $(\beta_1, \ldots, \beta_r) \in \mathbb{Z}^r$ be a non zero r-tuple and consider the divisors of $\mathcal{F}$

$$D = \sum_{i=1}^{n} P_i \qquad \text{and} \qquad G = \sum_{i=1}^{r} \beta_i Q_i.$$

If the code $C_{\mathcal{L}}(D,G)$ is iso-dual, then the AG-code $C_{\mathcal{L}}(\tilde{D},\tilde{G})$ defined over $\mathcal{M}$ with

$$\tilde{D} = Con_{\mathcal{M}/\mathcal{F}}(D) \qquad \text{and} \qquad \tilde{G} = \mathrm{Con}_{\mathcal{M}/\mathcal{F}}(G) + \tfrac{1}{2}\mathrm{Diff}(\mathcal{M}/\mathcal{F})$$

is also iso-dual.

Proof. Let us consider the divisor $\tilde{D}$ of $\mathcal{M}$ defined as the conorm of D in $\mathcal{M}/\mathcal{F}$, that is

$$\tilde{D} = \mathrm{Con}_{\mathcal{M}/\mathcal{F}}(D) = \sum_{i=1}^{n} \sum_{j=1}^{m} R_{i,j},$$

where $R_{i,1},\dots,R_{i,m}$ are all the places of $\mathcal{M}$ lying over P_i for each $i=1,\dots,n$.

By (b) of Proposition 2.6, there exist a Weil differential η of $\mathcal{F}$ and an element $f\in\mathcal{F}$ such that

$$(\eta)=2G-D+(f)^F.$$

Let $\tilde{\eta}=\mathrm{Cotr}(\eta)$ be the cotrace of η in M. Then, by (2.2), we have that

$$\begin{aligned}(\tilde{\eta}) &= \mathrm{Con}_{\mathcal{M}/\mathcal{F}}((\eta))+\mathrm{Diff}(\mathcal{M}/\mathcal{F})\\ &= \mathrm{Con}_{\mathcal{M}/\mathcal{F}}(2G-D+(f)^F)+\mathrm{Diff}(\mathcal{M}/\mathcal{F})\\ &= -\tilde{D}+\mathrm{Con}_{\mathcal{M}/\mathcal{F}}(2G+(f)^F)+\mathrm{Diff}(\mathcal{M}/\mathcal{F}).\end{aligned}$$

Consider the divisor $A=2G+(f)^F$, hence $(\eta)=A-D$. There are two possibilities: either $\mathrm{supp}(D)\cap\mathrm{supp}(A)=\varnothing$ or not.

In the first case, we clearly have that $v_{\tilde{R}}(\tilde{\eta})=-1$ for all $\tilde{R}\in\mathrm{supp}(\tilde{D})$. Since $\mathrm{Diff}(\mathcal{M}/\mathcal{F})=\sum_{i=1}^{r}\sum_{S|Q_i}d(S|Q_i)S$ and, by hypothesis, $d(S|Q_i)$ is even for every $i=1,\dots,n$, we have a well defined divisor

$$\tilde{G}=\mathrm{Con}_{\mathcal{M}/\mathcal{F}}(G)+\tfrac{1}{2}\mathrm{Diff}(\mathcal{M}/\mathcal{F}),$$

of $\mathcal{M}$. Since $\tilde{D}$ and $\tilde{G}$ have disjoint supports and $v_{\tilde{R}}(\tilde{\eta})=-1$ for all $\tilde{R}\in\mathrm{supp}(\tilde{D})$, from Proposition 2.6 we have that

$$C_{\mathcal{L}}(\tilde{D},\tilde{G})^{\perp}=\mathbf{a}\cdot C_{\mathcal{L}}(\tilde{D},\tilde{D}-\tilde{G}+(\tilde{\eta})), \tag{4.1}$$

where $\mathbf{a}=(\tilde{\eta}_{R_{1,1}}(1),\dots,\tilde{\eta}_{R_{n,m}}(1))\in\mathbb{F}_q^{nm}$. On the other hand, by the definition of $\tilde{G}$, we also have that

$$\begin{aligned}(\tilde{\eta}) &= \mathrm{Con}(2G-D+(f)^{\mathcal{F}})+\mathrm{Diff}(\mathcal{M}/\mathcal{F})\\ &= 2\,\mathrm{Con}_{\mathcal{M}/\mathcal{F}}(G)-\tilde{D}+\mathrm{Con}_{\mathcal{M}/\mathcal{F}}((f)^{\mathcal{F}})+\mathrm{Diff}(\mathcal{M}/\mathcal{F})\\ &= 2\tilde{G}-\tilde{D}+(f)^{\mathcal{M}},\end{aligned}$$

where $(f)^{\mathcal{M}}=\mathrm{Con}_{\mathcal{M}/\mathcal{F}}((f)^{\mathcal{F}})$ by Proposition 3.1.9 of [32]. Thus $\tilde{D}-\tilde{G}+(\tilde{\eta})=\tilde{G}+(f)^{\mathcal{M}}$ and this means that $\tilde{D}-\tilde{G}+(\tilde{\eta})\sim\tilde{G}$ so that

$$C_{\mathcal{L}}(\tilde{D},\tilde{D}-\tilde{G}+(\tilde{\eta}))=\mathbf{b}\cdot C_{\mathcal{L}}(\tilde{D},\tilde{G}), \tag{4.2}$$

for some vector $\mathbf{b}=(b_1,\dots,b_{nm})\in\mathbb{F}_q^{nm}$. If

$$\mathbf{x}=(\tilde{\eta}_{R_{1,1}}(1)b_1,\dots,\tilde{\eta}_{R_{n,m}}(1)b_{nm})\in\mathbb{F}_q^{nm},$$

from (4.1) and (4.2) we deduce that

$$C_{\mathcal{L}}(\tilde{D},\tilde{G})^{\perp}=\mathbf{x}\cdot C_{\mathcal{L}}(\tilde{D},\tilde{G}),$$

that is $C_{\mathcal{L}}(\tilde{D},\tilde{G})$ is an iso-dual AG-code over $\mathcal{M}$ which is a lifting to $\mathcal{M}$ of the iso-dual AG-code $C_{\mathcal{L}}(D,G)$ over $\mathcal{F}$.

If the second case occurs, that is if $\mathrm{supp}(D)\cap\mathrm{supp}(A)\neq\varnothing$, we know that there exists a divisor $A'\sim A$ such that $\mathrm{supp}(D)\cap\mathrm{supp}(A')=\varnothing$. Thus, there exists an element $h\in\mathcal{F}$ such that $2G+(f)^{\mathcal{F}}=A=A'+(h)^{\mathcal{F}}$ and then

$$(h^{-1}\eta)=(\eta)-(h)=-D+2G+(f)^{\mathcal{F}}-(h)^{\mathcal{F}}=-D+2G+(\tfrac{f}{h})^{\mathcal{F}}=-D+A',$$

with $\operatorname{supp}(D) \cap \operatorname{supp}(A') = \varnothing$. Now, $\omega = h^{-1}\eta$ is a Weil differential of $\mathcal{F}$ and thus, if we define $\tilde{\omega} = \operatorname{Cotr}(\omega)$, we have

$$\begin{aligned}(\tilde{\omega}) &= \operatorname{Con}_{\mathcal{M}/\mathcal{F}}((\omega)) + \operatorname{Diff}(\mathcal{M}/\mathcal{F}) \\ &= \operatorname{Con}_{\mathcal{M}/\mathcal{F}}(-D + A') + \operatorname{Diff}(\mathcal{M}/\mathcal{F}) \\ &= -\tilde{D} + \operatorname{Con}_{\mathcal{M}/\mathcal{F}}(A') + \operatorname{Diff}(\mathcal{M}/\mathcal{F}),\end{aligned}$$

where $\operatorname{supp}(D) \cap \operatorname{supp}(A') = \varnothing$. Therefore, we are in the conditions of the first case just considered and we see that the iso-dual AG-code $C_{\mathcal{L}}(D, G)$ defined over $\mathcal{F}$ can also be lifted to an iso-dual AG-code defined over $\mathcal{M}$. □

Notice that in the above theorem we use extensions of function fields such that the different exponents are even integers. This is not a huge constraint because the condition on the evenness of the different exponents holds in several well-known situations like:

- (i) the ones defined by Artin-Schreier extensions in odd characteristic,
- (ii) tamely ramified extensions of odd degree,
- (iii) the case of the so called weakly ramified extensions (see Definition 7.4.12 of [32]), and also
- (iv) the case where there is a rational place P of $\mathcal{F}$ totally ramified in $\mathcal{M}$ and the extension $\mathcal{M}/\mathcal{F}$ is unramified outside the place P. This is so because in this case if Q is the only place of $\mathcal{M}$ lying over P, then Q is also a rational place and then by Hurwitz genus formula we have that

$$2g_{\mathcal{M}} - 2 = (2g_{\mathcal{F}} - 2)[\mathcal{M} : \mathcal{F}] + d(Q|P), \tag{4.3}$$

showing that $d(Q|P)$ is even.

It is also worth noticing that in the presence of more than one place of $\mathcal{F}$ ramified in $\mathcal{M}$, either a one-point or a multi-point iso-dual code $C_{\mathcal{L}}(D, G)$ over $\mathcal{F}$ can be lifted to an iso-dual code over $\mathcal{M}$, according to the choice of the number of zero coordinates in the r-tuple $(\beta_1, \ldots, \beta_r)$ in the above theorem. However, despite having some flexibility in choosing the r-tuple $(\beta_1, \ldots, \beta_r)$ defining the divisor G, these integers must satisfy the equation

$$\sum_{i=1}^{r} \beta_i \deg(Q_i) = \tfrac{1}{2}(n + 2g_{\mathcal{F}} - 2),$$

according to (b) of Proposition 2.6, because we are requiring that $C_{\mathcal{L}}(D, G)$ is an iso-dual code.

In view of the result obtained in Theorem 4.1, we make the following definition and notation.

Definition 4.2. Given a function field extension $\mathcal{M}/\mathcal{F}$ and an AG-code $C_{\mathcal{L}}(D, G)$ over $\mathcal{F}$ as in Theorem 4.1, the AG-code $C_{\mathcal{L}}(\tilde{D}, \tilde{G})$, where

$$\tilde{D} = \operatorname{Con}_{\mathcal{M}/\mathcal{F}}(D) \qquad \text{and} \qquad \tilde{G} = \operatorname{Con}_{\mathcal{M}/\mathcal{F}}(G) + \tfrac{1}{2}\operatorname{Diff}(\mathcal{M}/\mathcal{F}),$$

will be called the *lifted code* (or *the lift*) of $C_{\mathcal{L}}(D, G)$ to $\mathcal{M}$, and we will denote it by $\mathfrak{L}_{\mathcal{M}/\mathcal{F}}(C_{\mathcal{L}}(D, G))$.

With Definition 4.2, Theorem 4.1 says that if $C_{\mathcal{L}}(D,G)$ is an iso-dual AG-code over $\mathcal{F}$ then the lifted code $\mathfrak{L}_{\mathcal{M}/\mathcal{F}}(C_{\mathcal{L}}(D,G))$ is also an iso-dual AG-code over $\mathcal{M}$.

We now give an estimate of the parameters of the lifted code of an iso-dual code.

Corollary 4.3. *Under the same conditions of Theorem 4.1, if* $mn > 2g_{\mathcal{M}} - 2$ *then* $\mathfrak{L}_{\mathcal{M}/\mathcal{F}}(C_{\mathcal{L}}(D,G))$ *is an* $[\tilde{n},\tilde{k},\tilde{d}]$*-code where*

$$\tilde{n} = mn, \qquad \tilde{k} = \tfrac{1}{2}mn, \qquad \text{and} \qquad \tilde{d} \geq \tfrac{1}{2}(mn - 2g_{\mathcal{M}} + 2).$$

Proof. Clearly, $\tilde{n} = mn$ because the support of $\tilde{D}$ consists of exactly mn (rational) places of $\mathcal{M}$, by definition of $\tilde{D}$. Also, since $C_{\mathcal{L}}(\tilde{D},\tilde{G})$ is an iso-dual code, it holds that $\tilde{k} = \frac{1}{2}mn$ and from Proposition 2.6 we have that

$$\deg(\tilde{G}) = \tfrac{1}{2}(mn + 2g_{\mathcal{M}} - 2).$$

From Proposition 2.1

$$\tilde{d} \geq \tilde{n} - \deg \tilde{G} = mn - \tfrac{1}{2}(mn + 2g_{\mathcal{M}} - 2) = \tfrac{1}{2}(mn - 2g_{\mathcal{M}} + 2),$$

as we wanted to show. □

5. Lifting iso-dual codes from the rational function field

We use now Theorem 4.1 to construct iso-dual AG-codes in function fields by lifting rational iso-dual codes, that is iso-dual codes over the rational function field $\mathbb{F}_q(x)$. This is the most favourable situation for our method because it is rather easy to construct rational iso-dual codes thanks to the characterization given in Proposition 2.6.

In $\mathbb{F}_q(x)$ we choose pairwise distinct rational places $P_1,\ldots,P_n$ for $n \geq 4$ even and we denote by P_∞ the only pole of x in $\mathbb{F}_q(x)$. By considering the divisors

$$D = P_1 + \cdots + P_n \qquad \text{and} \qquad G = \tfrac{1}{2}(n-2)P_\infty,$$

of $\mathbb{F}_q(x)$ we have that the AG-code $C_{\mathcal{L}}(D,G)$ is an iso-dual code over $\mathbb{F}_q(x)$ according to item (c) of Proposition 2.6. Now, we are going to choose suitable places $P_1,\ldots,P_n$ in $\mathbb{F}_q(x)$ in order to be able to lift the iso-dual $C_{\mathcal{L}}(D,G)$ over $\mathbb{F}_q(x)$ to some elementary abelian p-extensions, and also to some Kummer extensions in the next section.

Some of the examples given in this section include the important class of *maximal function fields*, that is, a function field $\mathcal{F}$ over $\mathbb{F}_{q^2}$ of genus $g(\mathcal{F})$ such that its number $\mathcal{F}(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points attains the upper bound on the Hasse-Weil bound, that is

$$\mathcal{F}(\mathbb{F}_{q^2}) = q^2 + 1 + 2g(\mathcal{F})q.$$

Remark 5.1. A distinguished example of maximal function field is the Hermitian function field which was already considered in Section 3 as a tamely ramified extension of $\mathbb{F}_{q^2}(x)$. In that case the constructed iso-dual code was a multi-point AG-code but here, with the Hermitian function field considered as an elementary abelian p-extension of $\mathbb{F}_{q^2}(x)$, the constructed iso-dual code will be a one-point AG-code. An important advantage we have with the elementary abelian p-extensions of $\mathbb{F}_q(x)$, is that it is rather easy to find a generating matrix for the lifted iso-dual codes in many cases.

Elementary abelian p-extensions. Let f be a polynomial over $\mathbb{F}_{q^s}$, $s \geq 1$, of degree $m > 0$ such that $(m, q) = 1$ and let $0 \neq \mu \in \mathbb{F}_{q^s}$. Suppose the polynomial $t^q + \mu t \in \mathbb{F}_{q^s}[t]$ splits completely into linear factors over $K = \mathbb{F}_{q^s}$. A function field of the form $\mathcal{F} = K(x, y)$ where

$$y^q + \mu y = f(x), \tag{5.1}$$

is called an *elementary p-abelian extension extension* of $K(x)$. From Proposition 6.4.1 of [32] we have that the extension $\mathcal{F}/K(x)$ is of degree q and genus

$$g = \tfrac{1}{2}(q-1)(m-1).$$

The only pole P_∞ of x in $K(x)$ is totally ramified in $\mathcal{F}$ and the extension $\mathcal{F}/K(x)$ is unramified outside the place P_∞. Since P_∞ is a rational place we have from (4.3) that the different exponent

$$d(Q_\infty|P_\infty) = (q-1)(m+1), \tag{5.2}$$

is even, where Q_∞ is the only place of $\mathcal{F}$ lying over P_∞.

We now give sufficient conditions to get lifted iso-dual codes over a general elementary abelian p-extension.

Proposition 5.2. *For any $s \in \mathbb{N}$ let us consider the elementary abelian p-extension $\mathcal{F} = \mathbb{F}_{q^s}(x, y)$ as in (5.1). Let $n \geq 4$ be an even integer and suppose that $P_1, \ldots, P_n$ are n different rational places of $\mathbb{F}_{q^s}(x)$ such that each P_i splits completely in $\mathcal{F}/K(x)$. Then there exists a lifted iso-dual AG-code over $\mathcal{F}$ with parameters*

$$[nm,\ \tfrac{1}{2}nm,\ \geq \tfrac{1}{2}(m(n-q+1)+q-3)],$$

and generating matrix

$$M = \left(\alpha_i^a \beta_{i,q}^b : 0 \leq a, 0 \leq b < q, qa + mb < r\right)_{1 \leq i \leq n}, \tag{5.3}$$

with $r = \frac{1}{2}(q(n+m-1)-m-1)$, where α_i is such that P_i is the only zero of $x - \alpha_i$ in $\mathbb{F}_{q^s}(x)$, provided that $\beta_{i,q}, \ldots, \beta_{i,q}$ are the q different roots of $T^q + \mu T = f(\alpha_i)$ for $1 \leq i \leq n$.

Proof. By hypothesis we have that $P_1, \ldots, P_n$ are n different rational places of $\mathbb{F}_{q^s}(x)$ with $n \geq 4$ even and such that each P_i splits completely in $\mathcal{F}/\mathbb{F}_{q^s}(x)$. By taking the divisors

$$D = P_1 + \cdots + P_n \qquad \text{and} \qquad G = \tfrac{1}{2}(n-2)P_\infty,$$

we have that the AG-code $C_{\mathcal{L}}(D, G)$ is an iso-dual code over $\mathbb{F}_{q^s}(x)$ according to (c) of Proposition 2.6. We are now in the conditions of Theorem 4.1 and then we have that $\mathfrak{L}_{\mathcal{F}/\mathbb{F}_{q^s}(x)}(C_{\mathcal{L}}(D, G))$ is an iso-dual code over $\mathcal{F}$. In fact we have that

$$\mathfrak{L}_{\mathcal{F}/\mathbb{F}_{q^s}(x)}(C_{\mathcal{L}}(D, G)) = C_{\mathcal{L}}(\tilde{D}, \tilde{G}) = C_{\mathcal{L}}(\tilde{D}, rQ_\infty),$$

where $\tilde{D} = \sum_{i=1}^{n} \sum_{j=1}^{q} R_{i,j}|P_i$ and $R_{i,1}, \ldots, R_{i,q}$ are the all the places of $\mathcal{F}$ lying over P_i for $i = 1, \ldots, n$ and

$$r = \tfrac{1}{2}(q(n+m-1)-m-1).$$

The latter is because

$$\mathrm{Diff}(\mathcal{F}/K(x)) = d(Q_\infty|P_\infty)Q_\infty = (2q + (q-1)(m-1) - 2)Q_\infty,$$

and so

$$\begin{aligned}\tilde{G} &= \mathrm{Con}_{\mathcal{F}/\mathbb{F}_{q^s}(x)}(\tfrac{1}{2}(n-2)\,P_\infty) + \tfrac{1}{2}\mathrm{Diff}(\mathcal{F}/\mathbb{F}_{q^s}(x)) \\ &= \tfrac{1}{2}q(n-2)\,Q_\infty + \tfrac{1}{2}(2q+(q-1)(m-1)-2)\,Q_\infty \\ &= \tfrac{1}{2}(q(n+m-1)-m-1)\,Q_\infty.\end{aligned}$$

The parameters of the lifted code follow from Corollary 4.3 and the expression of the genus of $\mathcal{F}$.

On the other hand, from Proposition 6.4.1 of [32] we know that the set

$$\{x^a y^b : 0 \leq a, 0 \leq b < q, qa + mb \leq r\}, \tag{5.4}$$

is an $\mathbb{F}_{q^s}$-basis of $\mathcal{L}(rQ_\infty)$. Now for each $1 \leq i \leq n$ the place P_i is the zero of $x - \alpha_i$ in $\mathbb{F}_{q^s}(x)$ and we are assuming that the polynomial $T^q + \mu T = f(\alpha_i)$ has q different roots $\beta_{i,1}, \ldots, \beta_{i,q} \in \mathbb{F}_{q^s}$. Then by Kummer theorem both elements $x - \alpha_i$ and $y - \beta_{i,j}$ belong to $R_{i,j}$ for $j = 1, \ldots, q$ and then the residual class $(x^a y^b)(R_{i,j})$ is

$$(x^a y^b)(R_{i,j}) = \alpha_i^a \beta_{i,q}^b. \tag{5.5}$$

This gives us the explicit generator matrix M of $\mathfrak{L}_{\mathcal{F}/\mathbb{F}_{q^s}(x)}(C_{\mathcal{L}}(D,G))$ as stated in (5.3). □

The following concrete example shows that the estimates given in Corollary 4.3 can not be improved in general.

Example 5.3. Consider the polynomial $t^2+t \in \mathbb{F}_8[t]$ and let $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ where α satisfies $\alpha^3 + \alpha + 1 = 0$. The equation

$$y^2 + y = x^3$$

defines an elementary abelian 2-extension $\mathcal{F}$ of $\mathbb{F}_8(x)$ of genus $g = 1$. It is easy to check using Sage [34] that the polynomial $T^2 + T = f(\gamma)$ splits into 2 different linear factors over $\mathbb{F}_8$ if $\gamma \in \{0, \alpha+1, \alpha^2+1, \alpha^2+\alpha+1\}$. Therefore, we have a rational iso-dual AG-code of the form

$$C_{\mathcal{L}}(P_1 + P_2 + P_3 + P_4, P_\infty)$$

that can be lifted to an iso-dual AG-code over $\mathcal{F}_\mu$ where P_1 is the zero of x in $\mathbb{F}_8(x)$, P_2 is the zero of $x + \alpha + 1$ in $\mathbb{F}_8(x)$, P_3 is the zero of $x + \alpha^2 + \alpha + 1$ in $\mathbb{F}_8(x)$ and P_4 is the zero of $x + \alpha^2 + 1$ in $\mathbb{F}_8(x)$. By Corollary 4.3 the lifted code is an AG-code of length 8, dimension $\tilde{k} = 4$ and minimum distance $\tilde{d} \geq 4$.

We show now that, in fact, $\tilde{d} = 4$. Since in this case $q = 2$, $m = 3$ and $n = 4$ we see that $r = 4$ so that $\tilde{G} = 4Q_\infty$ and we also have from (5.4) that the set $\{1, x, x^2, y\}$ is an $\mathbb{F}_8$-basis of $\mathcal{L}(4Q_\infty)$. Using (5.3) we form the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \alpha+1 & \alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2+1 & \alpha^2+1 \\ 0 & 0 & \alpha^2+1 & \alpha^2+1 & \alpha+1 & \alpha+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 \\ 0 & 1 & \alpha^2+\alpha & \alpha^2+\alpha+1 & \alpha^2 & \alpha^2+1 & \alpha & \alpha+1 \end{pmatrix}$$

which is a generator matrix of

$$C_{\mathcal{L}}(\tilde{D}, 4Q_\infty) = \mathfrak{L}_{\mathcal{F}_1/\mathbb{F}_8(x)}(C_{\mathcal{L}}(P_1 + P_2 + P_3 + P_4, P_\infty)).$$

With this matrix we can use now the Coding theory package of SAGE and see that $\tilde{d} = 4$, as claimed. ◊

5.1. **Iso-dual codes over function fields covered by the Hermitian.** In the case of finite fields of quadratic cardinality there are examples of maximal function fields which are elementary abelian p-extensions of $\mathbb{F}_{q^2}(x)$ for any prime p. An instance of this situation is the function field $\mathcal{F}$ defined by the equation

$$y^q + y = x^\ell,$$

where $\ell > 1$ is a divisor of $q+1$, of genus

$$g = \tfrac{1}{2}(q-1)(\ell-1)$$

(the case $\ell = q+1$ is the well known Hermitian function field over $\mathbb{F}_{q^2}$). By Example 6.4.2 of [32] we have $1 + (q-1)\ell$ rational places in $\mathbb{F}_{q^2}(x)$ that splits in $\mathcal{F}/\mathbb{F}_{q^2}(x)$. Let $q \geq 3$ be odd and take $n = (q-1)\ell$. Then $n \geq 4$ is even and

$$qn = q(q-1)\ell > (q-1)(\ell-1) - 2 = 2g - 2.$$

The code $C_{\mathcal{L}}(P_1 + \cdots + P_n, \frac{1}{2}(n-2)P_\infty)$ is a rational iso-dual code, by Proposition 2.6, and the lifted code

$$\mathfrak{L}_{\mathcal{F}/\mathbb{F}_q(x)}(C_{\mathcal{L}}(P_1 + \cdots + P_n, \tfrac{1}{2}(n-2)P_\infty))$$

is an iso-dual AG-code over $\mathcal{F}$ of length, dimension and minimum distance given by

$$\tilde{n} = q(q-1)\ell, \qquad \tilde{k} = \tfrac{1}{2}q(q-1)\ell, \qquad \text{and} \qquad \tilde{d} \geq \tfrac{1}{2}((q-1)^2\ell + q + 1),$$

respectively.

5.2. **Iso-dual codes on the Suzuki curve.** Let $q = 2^{2m+1}$ and $q_0 = 2^m, m \geq 1$. The Suzuki function field $\mathcal{S}_q = \mathbb{F}_{q^4}(x,y)$ is defined by the affine equation

$$\mathcal{S}_q : \quad y^q + y = x^{q_0}(x^q + x). \tag{5.6}$$

This curve has genus

$$g(\mathcal{S}_q) = q_0(q-1)$$

and it is $\mathbb{F}_{q^4}$-maximal; with only one place at infinity, P_∞, the only pole of x and y.

We now show that we can lift iso-dual AG-codes over this function field.

Proposition 5.4. *For $q = 2^{2m+1}$ and $q_0 = 2^m$, with $m \geq 1$, there exist lifted iso-dual AG-codes on the curve $\mathcal{S}_q$ over $\mathbb{F}_{q^4}$ with parameters satisfying*

$$\big[q(q^3-q),\ \tfrac{1}{2}q(q^3-q),\ \geq \tfrac{1}{2}(q^4 - q^2 - 2q_0(q-1) + 2)\big]. \tag{5.7}$$

Proof. Let $f(x) = x^{q_0}(x^q + x)$. We notice that if α in $\mathbb{F}_{q^4}$ is such that $\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(\alpha) = 0$ and $a^q + a \neq 0$ then $\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(f(\alpha)) = 0$ and we conclude, from the 90's Hilbert Theorem, that there exists q solutions $y \in \mathbb{F}_{q^4}$ to $y^q + y = f(\alpha)$. That is, the rational place P_{x-a} in $\mathbb{F}_{q^4}(x)$ splits in the extension $\mathcal{S}_q/\mathbb{F}_{q^4}(x)$.

Let $n = q^3 - q$ and let $P_1, \ldots, P_n$ be the $\mathbb{F}_{q^4}$-rational places splitting in the extension $\mathcal{S}_q/\mathbb{F}_{q^4}(x)$. The code $C_{\mathcal{L}}(D,G)$ with

$$D = P_1 + \cdots + P_n \qquad \text{and} \qquad G = \tfrac{1}{2}(n-2)P_\infty$$

is a rational iso-dual code by Proposition 2.6, since n is even. Thus, we are in the conditions of Theorem 4.1 and then $\mathfrak{L}_{\mathcal{S}_q/\mathbb{F}_{q^4}(x)}(C_{\mathcal{L}}(D,G))$ is an iso-dual code over $\mathcal{S}_q$ with parameters as stated in (5.7), by Corollary 4.3. □

5.3. **Iso-dual codes on an maximal curve covered by the GGS-curve.** From a result by J. P. Serre it is known that any $\mathbb{F}_{q^2}$-rational curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal. For some decades, ideas exploring this result were used to obtain examples of maximal curves, most of them were covered by the famous $\mathbb{F}_{q^2}$-maximal Hermitian curve. In 2009, Giulietti and Korchmáros provided in [12] the first example of a $\mathbb{F}_{q^6}$-maximal curve, nowadays referred to as the GK-curve, which is not covered by the Hermitian curve over $\mathbb{F}_{q^3}$, for any $q \geq 2$. In the same year, Garcia, Güneri and Stichtenoth presented a generalization of the GK-curve [10], now known as the GGS-curve, that is, a maximal curve over $\mathbb{F}_{q^{2r}}$ for $r \geq 3$ odd and isomorphic to the GK-curve for $r = 3$.

For $r \geq 3$ odd consider the $\mathbb{F}_{q^{2r}}$ maximal curve covered by the GGS-curve (see [1] and [10]) defined by the affine equation

$$\mathcal{X}: \quad y^{q^2} - y = x^{\frac{q^r+1}{q+1}}. \tag{5.8}$$

and has genus

$$g(\mathcal{X}) = \tfrac{1}{2}(q-1)(q^n - q).$$

This curve defines an elementary abelian p-extension, so it ramifies only at the place Q_∞ over P_∞ in $\mathbb{F}_{q^{2r}}(x)$ with even different exponent

$$d(Q_\infty|P_\infty) = (q^2-1)\tfrac{q^r+q+2}{q+1} = (q-1)(q^r+q+2)$$

by (5.2). So we can apply Theorem 4.1 and lift an iso-dual code over $\mathbb{F}_{q^{2r}}(x)$.

Proposition 5.5. *For q and $r \geq 3$ both odd there exist a lifted iso-dual AG-code on the function field of the curve $\mathcal{X}$ over $\mathbb{F}_{q^{2r}}$ with parameters satisfying*

$$\big[q^2(q^r+1)(q^{r-1}-1),\ \tfrac{1}{2}q^2(q^r+1)(q^{r-1}-1),\ \geq \tfrac{1}{2}(q^{2r+1} - q^{r+2} + q^r - q - 2)\big]. \tag{5.9}$$

Proof. Let $n = (q^r+1)(q^{r-1}-1)$ and let $P_1, \ldots, P_n$ be the $\mathbb{F}_{q^{2r}}$-rational places splitting in the extension $\mathbb{F}_{q^{2r}}(\mathcal{X})/\mathbb{F}_{q^{2r}}(x)$, see [1, Lemma 2]. The code $C_{\mathcal{L}}(D,G)$ with

$$D = P_1 + \cdots + P_n \qquad \text{and} \qquad G = \tfrac{1}{2}(n-2)P_\infty$$

is a rational iso-dual code by Proposition 2.6 since n is even. Thus, we are in the conditions of Theorem 4.1 and then $\mathfrak{L}_{\mathcal{X}/\mathbb{F}_{q^{2r}}(x)}(C_{\mathcal{L}}(D,G))$ is an iso-dual code over $\mathcal{X}$ with parameters as stated in (5.7), by Corollary 4.3. □

6. Lifting iso-dual codes over the Hermitian function field

In order to lift an iso-dual code in an extension of function fields, some technical requirements are given in Theorem 4.1. We start this section proposing an algebraic curve over $\mathbb{F}_{q^2}$ satisfying the requirements. After that, we are going to lift a certain iso-dual code.

Consider the algebraic variety $\mathcal{X}$ over $\mathbb{F}_{q^2}$ defined by the equations

$$\mathcal{X}: \quad \begin{cases} z^{q+1} = y^q + y, \\ y^{q+1} = x^q + x. \end{cases} \tag{6.1}$$

We now prove that $\mathcal{X}$ is an absolutely irreducible curve over $\mathbb{F}_{q^2}$ and compute the genus and the number of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$.

Proposition 6.1. *$\mathcal{X}$ is an absolutely irreducible curve over $\mathbb{F}_{q^2}$, has genus $g(\mathcal{X}) = q^3 - q$ and its number of rational points over $\mathbb{F}_{q^2}$ is $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^4 + 1$.*

Proof. For simplicity, we put $\mathcal{M} = \mathbb{F}_{q^2}(x, y, z)$ and $\mathcal{F} = \mathbb{F}_{q^2}(x, y)$. The first equation $y^{q+1} = x^q + x$ defines the maximal Hermitian function field $\mathcal{F}$ of genus $\frac{1}{2}q(q-1)$. We denote by P_α the place in $\mathbb{F}_{q^2}(x)$ associated to the zero of $x - \alpha$ and by P_∞ the pole of x. In the extension $\mathcal{F}/\mathbb{F}_q(x)$ we have the following well-known structure for the rational places: each P_α for $\alpha^q + \alpha = 0$ is totally ramified and we denote by $Q_{\alpha,0}$ be the only place over it. For $\alpha \in \mathbb{F}_{q^2}$ that is not a root of $x^q + x = 0$ the place P_α splits and we denote by Q_{α,β_i} the $q+1$ places over it, where $\beta_i^{q+1} = \alpha^q + \alpha$.

We notice that $\mathcal{X}$ is an absolutely irreducible curve since Q_∞ is totally ramified in $\mathcal{M}/\mathbb{F}_q(x)$. Now we prove that $\mathcal{M}/\mathcal{F}$ defines a Kummer extension. We start by computing the divisor of $y^q + y$ in $\mathcal{F}$. Clearly Q_∞ and $Q_{\alpha,0}$ are totally ramified in $\mathcal{M}/\mathcal{F}$. Consider the sets

$$S_0 = \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha = 0\},$$

$$S_1 = \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha \neq 0 \text{ and } x^2 + \alpha^q + \alpha \in \mathbb{F}_q[x] \text{ is irreducible}\},$$

$$S_2 = \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha \neq 0 \text{ and } x^2 + \alpha^q + \alpha \in \mathbb{F}_q[x] \text{ is reducible}\}.$$

Let $Q_{\alpha,\beta}$ be a zero of $y^q + y$ in $\mathcal{F}$, with $\alpha \neq 0$. If $\beta = 0$ we have that $\alpha \in S_0$. From now on we consider $\beta \neq 0$. Then, it is a simple zero and we have that $\beta^q = -\beta$ and $\beta^{q+1} = \alpha^q + \alpha$ and hence $\beta^2 - \alpha^q - \alpha = 0$ and $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We conclude that $\alpha \in S_1$, i.e. $\alpha \in \mathbb{F}_{q^2}$ such that $x^2 + \alpha^q + \alpha$ is an irreducible polynomial over $\mathbb{F}_q$ with two distinct roots β_α and β_α^q in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We denote by Q_{α,β_α} and $Q_{\alpha,\beta_\alpha^q}$ these places in $\mathcal{F}$. Moreover, since Q_∞ is the only pole of y of order q we have that

$$(y^q + y)^{\mathcal{F}} = \sum_{\alpha \in S_0} Q_{\alpha,0} + \sum_{\alpha \in S_1} (Q_{\alpha,\beta_\alpha} + Q_{\alpha,\beta_\alpha^q}) - q^2 Q_\infty. \tag{6.2}$$

Hence, we conclude that the extension $\mathcal{M}/\mathcal{F}$ defines a Kummer extension. By Kummer theory, the places Q_{α,β_α} and $Q_{\alpha,\beta_\alpha^q}$ are totally ramified in the extension $\mathcal{M}/\mathcal{F}$. Since $|S_1| = \frac{1}{2}(q^2 - q)$, we have a total of $q^2 + 1$ totally ramified places in the extension $\mathcal{M}/\mathcal{F}$. In Figure 1 we summarize the ramification in the curve $\mathcal{X}$.

From (6.2) we obtain that the degree of the different $\mathrm{Diff}(\mathcal{M}/\mathcal{F})$ is $q^3 + q$, since there are $q^2 + 1$ totally ramified places in the extension $\mathcal{M}/\mathcal{F}$. Now, since $[\mathcal{M} : \mathcal{F}] = q + 1$, the Hurwitz genus formula yields

$$2g(\mathcal{M}) - 2 = 2g(\mathcal{F}) - 2 + \deg(\mathrm{Diff}(\mathcal{M}/\mathcal{F})) = (q+1)(q^2 - q - 2) + q^3 + q.$$

That is $2g(\mathcal{M}) - 2 = 2(q^3 - q - 1)$, from which we get $g(\mathcal{X}) = g(\mathcal{M}) = q^3 - q$.

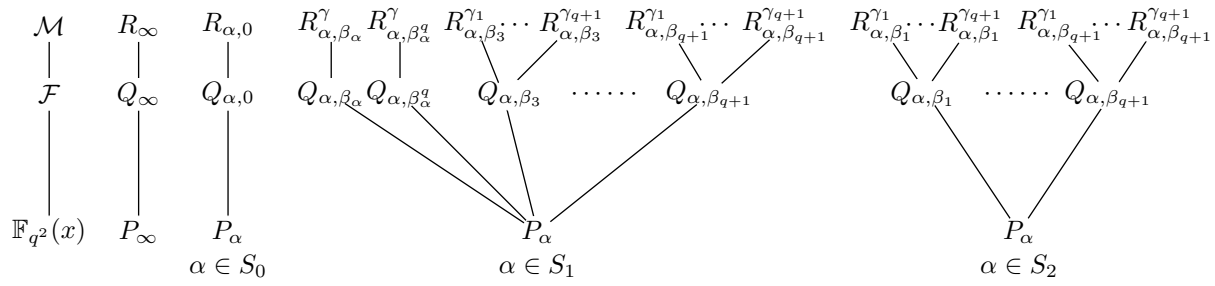

FIGURE 1. Decomposition of places of $\mathbb{F}_{q^2}(x)$ in $\mathcal{M}$.

Now we compute the number of $\mathbb{F}_{q^2}$-rational points on the curve $\mathcal{X}$. The place at infinity R_∞ is rational. Clearly, there are q places of the form $R_{\alpha,0}$ with $\alpha \in S_0$. Let $R^{\gamma}_{\alpha,\beta}$ be a rational place in $\mathcal{M}$ over $Q_{\alpha,\beta}$ in $\mathcal{F}$ for $\beta \neq 0$, then

$$\gamma^{q+1} = \beta^q + \beta \qquad \text{and} \qquad \beta^{q+1} = \alpha^q + \alpha \neq 0.$$

We consider two cases.

Case 1: If $\beta^q + \beta = 0$, then $\beta^{q+1} = \alpha^q + \alpha$ implies $-\beta^2 = \alpha^q + \alpha, \beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So $x^2 + \alpha^q + \alpha$ is irreducible over $\mathbb{F}_q$ and we obtain (as before) that the two places Q_{α,β_α} and $Q_{\alpha,\beta^q_\alpha}$ are both totally ramified in $\mathcal{M}/\mathcal{F}$, all the other Q_{α,β_i} split in $\mathcal{M}/\mathcal{F}$.

Case 2: If $\beta^q + \beta \neq 0$ then the equation $z^{q+1} - \beta^q - \beta$ factors into $q+1$ factors of degree one over $\mathbb{F}_{q^2}$. Hence the place $Q_{\alpha,\beta}$ splits in the extension $\mathcal{M}/\mathcal{F}$.

Considering the two cases we have a total of

$$2\tfrac{(q^2-q)}{2} + (q+1)\big((q-1)\tfrac{q^2-q}{2} + (q+1)(\tfrac{q^2-q}{2})\big) = (q^2-q) + (q+1)(q^2-q)q$$

rational places over $\mathbb{F}_{q^2}$ (recall that $\frac{q^2-q}{2}$ is the number of α in $\mathbb{F}_{q^2}$ such that $\alpha^q + \alpha \neq 0$ and $\alpha^q + \alpha$ is a square in $\mathbb{F}_q$, or not a square in $\mathbb{F}_q$).

Summarizing, the curve $\mathcal{X}$ has in total

$$1 + q + (q^2-q) + (q^2-q)(q+1)q = q^4 + 1$$

rational points over $\mathbb{F}_{q^2}$. □

We now present an iso-dual code defined in $\mathcal{M} = \mathbb{F}_{q^2}(\mathcal{X})$ for certain values of q. We will also consider an intermediate function field $\mathcal{F}$ as in the proof of Proposition 6.1.

Theorem 6.2. *For any $q = 2^s$ with $s > 1$ there is a lifted iso-dual code over $\mathcal{M} = \mathbb{F}_{q^2}(\mathcal{X})$, where $\mathcal{X}$ is as in (6.1), with parameters*

$$n = \tfrac{1}{2}(q^2-q)(q+1)^2, \quad k = \tfrac{1}{4}(q^2-q)(q+1)^2, \quad \text{and} \quad d \geq \tfrac{1}{4}(q^4 - q^3 - q^2 + 3q + 4).$$

Proof. Taking the divisors

$$D = \sum_{\alpha \in S_2} P_\alpha \qquad \text{and} \qquad G = \tfrac{1}{4}(q^2 - q - 4)P_\infty$$

in the rational function field $\mathbb{F}_q(x)$ we have, by (c) in Proposition 2.6, that the code $C_{\mathcal{L}}(D, G)$ is a rational iso-dual code with parameters

$$n = \tfrac{1}{2}(q^2 - q) \text{ even}, \qquad k = \tfrac{1}{4}(q^2 - q) \qquad \text{and} \qquad d \geq \tfrac{1}{2}(q^2 - q + 1).$$

This code can be lifted to $\mathcal{F}$ using Theorem 4.1 to an iso-dual code $\mathfrak{L}_{\mathcal{F}/\mathbb{F}_{q^2}(x)}(C_{\mathcal{L}}(D^{\mathcal{F}}, G^{\mathcal{F}}))$ of length and dimension given by

$$n^{\mathcal{F}} = \tfrac{1}{2}(q^2 - q)(q + 1) \qquad \text{and} \qquad k^{\mathcal{F}} = \tfrac{1}{4}(q^2 - q)(q + 1).$$

Since this code is iso-dual we have $\deg(G^{\mathcal{F}}) = \frac{1}{4}(q^3 + 2q^2 - 3q - 4)$ and

$$d^{\mathcal{F}} \geq n^{\mathcal{F}} - \deg(G^{\mathcal{F}}) = \tfrac{1}{4}(q^3 - 2q^2 + q + 4).$$

Now, we are again in the conditions of Theorem 4.1 and then the lifted code $\mathfrak{L}_{\mathcal{M}/\mathcal{F}}(C_{\mathcal{L}}(D^{\mathcal{M}}, G^{\mathcal{M}}))$ is an iso-dual code over $\mathcal{M}$, where

$$n^{\mathcal{M}} = \tfrac{1}{2}(q^2 - q)(q + 1)^2 \qquad \text{and} \qquad k^{\mathcal{M}} = \tfrac{1}{4}(q^2 - q)(q + 1)^2.$$

We also have $\deg(G^{\mathcal{M}}) = \frac{1}{4}(q^4 + 5q^3 - q^3 - 5q - 4)$ and, therefore,

$$d^{\mathcal{M}} \geq n^{\mathcal{M}} - \deg(G^{\mathcal{M}}) = \tfrac{1}{4}(q^4 - q^3 - q^2 + 3q + 4),$$

as we wanted to show. □

7. Binary and ternary cyclotomic iso-dual codes

Some subfields of a cyclotomic function field has been used by Quebbemann in [28] to give examples of long AG-codes (called cyclotomic Goppa codes). Here, we will construct long binary and ternary iso-dual AG-codes by using an alternative approach introduced in [25] to produce optimal function fields over $\mathbb{F}_2$. In view of the terminology used by Quebbemann in [28], we will call these codes binary and ternary cyclotomic iso-dual codes.

We follow the presentation of Hayes [15] of cyclotomic function fields (see also Section 3.2 of [26] where a summary of the main results of Hayes using divisors in additive notation is presented). Let $R = \mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$ and let $\bar{\mathcal{F}}$ be an algebraic closure of the rational function field $\mathcal{F} = \mathbb{F}_q(x)$. Let φ the $\mathbb{F}_q$-vector space endomorphism of $\bar{\mathcal{F}}$ defined as

$$\varphi(u) = u^q + xu,$$

for all $u \in \bar{\mathcal{F}}$. Then φ induces a ring homomorphism from R to $\mathrm{End}_{\mathbb{F}_q}(\bar{\mathcal{F}})$ by $f \mapsto f(\varphi)$; that is, if $f(x) = \sum_i a_i x^i$ then $f(\varphi) = \sum_i a_i \varphi^i$. This, in turn, allows to define an R-module structure on $\bar{\mathcal{F}}$ by defining an action of R on $\bar{\mathcal{F}}$ as

$$u^f = f(\varphi)(u),$$

for $f \in R$ and $u \in \bar{\mathcal{F}}$.

Let $f \in R$. By considering the submodule of f-torsion points of this action

$$\Lambda_f = \{u \in \bar{\mathcal{F}} : u^f = 0\},$$

we have the field $\mathcal{F}(\Lambda_f)$ generated over $\mathcal{F}$ by the elements of Λ_f. This field is a finite abelian extension of $\mathcal{F}$ and its Galois group is isomorphic to the group of units of the quotient ring $R/(f)$, where (f) denotes the principal ideal of R generated by f, that is

$$\mathrm{Gal}(\mathcal{F}(\Lambda_f)/\mathcal{F}) \simeq (R/(f))^* .$$

Assume that $h \in R$ is monic and irreducible over $\mathbb{F}_q$. As before, we denote by P_h the place of $\mathcal{F}$ associated to h. The unique automorphism $\sigma_{\bar{h}} \in \mathrm{Gal}(\mathcal{F}(\Lambda_f)/\mathcal{F})$ determined by its residual class $\bar{h} \in (R/(f))^*$ acts as $\sigma_{\bar{h}}(u) = u^h$ for all $u \in \Lambda_f$. In particular, if h does not divide f, the Artin symbol

$$\left[\frac{\mathcal{F}(\Lambda_f)/\mathcal{F}}{P_h}\right]$$

of the place P_h is the automorphism $\sigma_{\bar{h}}$. Therefore, if H is the subgroup of $(R/(f))^*$ generated by $\bar{h}$, where $h \in R$ is irreducible and does not divide f, then P_h splits completely in the fixed subfield

$$\mathcal{K} = \mathcal{F}(\Lambda_f)^H \tag{7.1}$$

of $\mathcal{F}(\Lambda_f)$ (see, for instance, Proposition 1.4.12 of [26]). Thus, with a suitable choice of such a polynomial h we can find many rational places in a subfield of $\mathcal{F}(\Lambda_f)$ whose genus and degree can be explicitly computed. Some optimal function fields over $\mathbb{F}_2$ were found in [25] in this way.

Suppose now that $f \in R$ is monic of degree d and irreducible over $\mathbb{F}_q$. We have that

$$\mathcal{F}(\Lambda_{f^n})/\mathcal{F}$$

is a finite abelian field extension of degree

$$q^{dn} - q^{d(n-1)} = q^{d(n-1)}(q^d - 1),$$

where the places P_f and P_∞ (the only pole of x in $\mathcal{F}$) are the only places of $\mathcal{F}$ that can be ramified in $\mathcal{F}(\Lambda_{f^n})$. In fact, P_f is always totally ramified in $\mathcal{F}(\Lambda_{f^n})$ and the place P_∞ is totally ramified in $\mathcal{F}(\Lambda_f)$ and then it splits completely in $\mathcal{F}(\Lambda_{f^n})/\mathcal{F}(\Lambda_f)$. In terms of ramification indices, we have that if we denote by Q_∞ the only place of $\mathcal{F}(\Lambda_f)$ lying over P_∞ then Q_∞ is a rational place, $e(Q_\infty|P_\infty) = q-1$ and there are exactly

$$r = q^{d(n-1)}(q^{d-1} + q^{d-2} + \cdots + q + 1)$$

places of $\mathcal{F}(\Lambda_{f^n})$ lying over Q_∞ and they are all rational places. For the place P_f, the only place of $\mathcal{F}(\Lambda_{f^n})$ is denoted by R_f and its restriction to $\mathcal{F}(\Lambda_f)$ is denoted by Q_f. This situation is illustrated in Figure 2 below.

From now on, we consider the particular case $f = x$ in (7.1) and then $\mathcal{F}(\Lambda_{x^n})/\mathcal{F}$ is a cyclotomic extension of $\mathcal{F}$ of degree $q^{n-1}(q-1)$. We know that

$$2g(\mathcal{F}(\Lambda_{x^n})) - 2 = q^{n-1}(n(q-1) - q - 1) \tag{7.2}$$

(see Corollary 4.2 of [15]) and thus the function field $\mathcal{F}(\Lambda_x)$ is, in fact, a rational function field over $\mathbb{F}_q$ (see Proposition 1.6.3 of [32]).

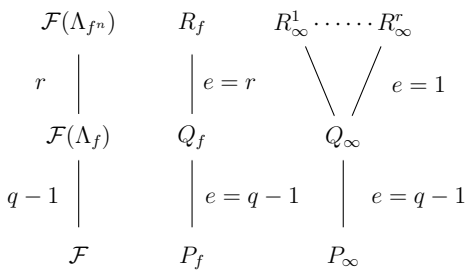

FIGURE 2. Decompositions of P_f and P_∞.

We will define a cyclic subgroup H of $(R/(x^n))^*$ of order q^m generated by a suitable residual class $\overline{x-\alpha}$ for some $\alpha \in \mathbb{F}_q$. With this choice of H we have that the subfield

$$\mathcal{K}_n = \mathcal{F}(\Lambda_{x^n})^H$$

defines a cyclic extension $\mathcal{F}(\Lambda_{x^n})/\mathcal{K}_n$ of degree q^m and we will try to lift a rational iso-dual AG-code to an iso-dual AG-code over $\mathcal{K}_n$.

For an estimate of the minimum distance of these liftings we need to compute the genus of $\mathcal{K}_n$ according to Corollary 4.3. The case $q = 2$ of item (b) of the following proposition was proved in Theorem 2 of [25].

Proposition 7.1. *Let $n, q \in \mathbb{N}$ with q a prime power and put $m = \lceil \log_q(n) \rceil$. Let H be the subgroup of $(R/(x^n))^*$ generated by the residual class $\overline{x+1}$. Let $\mathcal{K}_n = \mathcal{F}(\Lambda_{x^n})^H$ be the fixed subfield of $\mathcal{F}(\Lambda_{x^n})$ by H and let $S_x = R_x \cap \mathcal{K}_n$ be the restriction to $\mathcal{K}_n$ of the only place R_x of $\mathcal{F}(\Lambda_{x^n})$ lying over P_x. Then, we have the following.*

(a) *H is a cyclic group of order q^m. In particular, the extension $\mathcal{F}(\Lambda_{x^n})/\mathcal{K}_n$ is cyclic of degree q^m, the extension $\mathcal{K}_n/\mathcal{F}$ is of degree $q^{n-m-1}(q-1)$ and the place S_x is a rational place of $\mathcal{K}_n$ which is totally ramified in $\mathcal{F}(\Lambda_{x^n})$ (see Figure 3 below).*

(b) *If $\mathcal{F}(\Lambda_x) \subset \mathcal{K}_n$, then the extension $\mathcal{K}_n/\mathcal{F}(\Lambda_x)$ is unramified outside the place Q_x and the genus of $\mathcal{K}_n$ is*

$$g(\mathcal{K}_n) = \tfrac{1}{2}q^{-m}\Big(q^{n-1}(n(q-1)-q-1) - \sum_{i=1}^{q^m-1} q^{e_i}\Big) + 1, \tag{7.3}$$

where e_i denotes the least integer such that $p = \mathrm{Char}(\mathbb{F}_q)$ does not divide the binomial number $\binom{i}{j}$ for $1 \le j \le i < n$.

Proof. (a) We clearly have that m is the unique integer such that $q^{m-1} < n \le q^m$. Since

$$(x+1)^{q^m} = x^{q^m} + 1 \equiv 1 \pmod{x^n},$$

we see not only that $\overline{x+1} \in (R/(x^n))^*$ but also that H is a cyclic group of order q^m because of the choice of the integer m. Thus, $\mathcal{F}(\Lambda_{x^n})/\mathcal{K}_n$ is a cyclic extension of degree q^m.

Since R_x is a rational place so is S_x and since R_x is the only place of $\mathcal{F}(\Lambda_{x^n})$ lying over S_x we must have that $e(R_x|S_x) = q^m$, that is S_x is totally ramified in $\mathcal{F}(\Lambda_{x^n})$. We sketch this situation in the following picture:

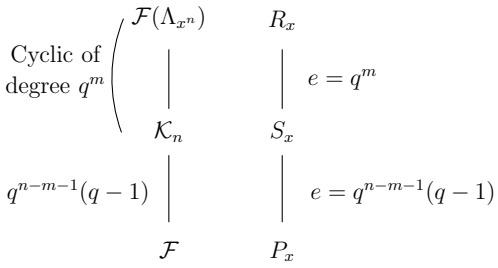

FIGURE 3. Ramification of S_x.

(b) Assume that $\mathcal{F}(\Lambda_x) \subset \mathcal{K}_n$. From the ramification situation described in Figure 2, we immediately see that the extension $\mathcal{K}_n/\mathcal{F}(\Lambda_x)$ is unramified outside the place Q_x. In particular, since S_x is the only place of $\mathcal{K}_n$ lying over Q_x, the extension $\mathcal{F}(\Lambda_{x^n})/\mathcal{K}_n$ is unramified outside the place S_x and from (4.3) we have that

$$2g(\mathcal{F}(\Lambda_{x^n})) - 2 = (2g(\mathcal{K}_n) - 2)q^m + d(R_x|S_x).$$

Now notice that from (7.2) we just need to compute the different exponent $d(R_x|S_x)$ to find the genus of $\mathcal{K}_n$. In order to do so, we recall that any root λ of the polynomial $h(u) = u^{x^n}/u^{x^{n-1}}$is a prime element of R_x, that is $\nu_{R_x}(\lambda) = 1$ (Proposition 2.4 of [15]). Clearly the minimal polynomial $g(u)$ of λ over $\mathcal{K}_n$ is

$$g(u) = \prod_{\sigma \in H} (u - \sigma(\lambda)),$$

so that from Proposition 3.5.12 of [32] we have that

$$d(R_x|S_x) = \nu_{R_x}(g'(\lambda)).$$

Since $H = \{(\overline{x+1})^i : 0 \leq i < q^m\}$ we can write

$$g'(\lambda) = \prod_{i=1}^{q^m-1} (\lambda - \lambda^{(x+1)^i}).$$

On the other hand (because $\lambda^{x^j} = 0$ for $j \geq n$) we have that

$$\lambda^{(x+1)^i} = \sum_{j=0}^{i} \binom{i}{j} \lambda^{x^j} = \lambda + \sum_{j=1}^{i<n} \binom{i}{j} \lambda^{x^j},$$

so that

$$g'(\lambda) = -\prod_{i=1}^{q^m-1} \sum_{j=1}^{i<n} \binom{i}{j} \lambda^{x^j},$$

By induction on j, it is easy to see (since $\nu_{R_x}(\lambda) = 1$) that $\nu_{R_x}(\lambda^{x^j}) = q^j$ for $1 \leq j \leq n-2$ and $\nu_{R_x}(\lambda^{x^{n-1}}) \geq q^{n-1}$. Then

$$\nu_{R_x}\Big(\sum_{j=1}^{i<n} \tbinom{i}{j}\lambda^{x^j}\Big) = q^{e_i},$$

where e_i is the least integer such that $p = \mathrm{Char}(\mathbb{F}_q)$ does not divide $\binom{i}{j}$ for $1 \leq j \leq i$, and thus

$$d(R_x|S_x) = \nu_{R_x}(g'(\lambda)) = \sum_{i=1}^{q^m-1} q^{e_i}.$$

Therefore

$$2g(\mathcal{K}_n) - 2 = q^{-m}\Big(q^{n-1}(n(q-1) - q - 1) - \sum_{i=1}^{q^m-1} q^{e_i}\Big), \tag{7.4}$$

from which (7.3) readily follows. □

We define now iso-dual AG-codes over $\mathcal{K}_n$ in the cases $q = 2$ and $q = 3$ by lifting to $\mathcal{K}_n$ some rational iso-dual codes.

7.1. **Binary cyclotomic iso-dual codes.** Let $q = 2$ and $\mathcal{F} = \mathbb{F}_2(x)$. Since we have exactly three rational places in $\mathcal{F}$ (namely P_x, P_{x+1} and P_∞), if we want to define an iso-dual code over $\mathcal{F}$ of the form $C_{\mathcal{L}}(D, G)$ which can be lifted to an iso-dual code over another field, we are forced to consider D as a divisor of $\mathcal{F}$ whose support consists of exactly two rational places (the length must be even) and G must be a divisor of $\mathcal{F}$ of degree zero. In the present situation the place P_∞ splits completely in any cyclotomic extension of $\mathcal{F}$ and so we define

$$D = P_{x+1} + P_\infty. \tag{7.5}$$

Since we must have $\deg G = 0$ (according to item (c) of Proposition 2.6) we define

$$G = P_{x^2+x+1} - 2P_x, \tag{7.6}$$

and thus $C_{\mathcal{L}}(D, G)$ is an iso-dual AG-code over $\mathcal{F}$.

This code is the repetition code $Rep_2(2) = \{(0,0),(1,1)\}$ with parameters $[2,1,2]$, which is actually self-dual. By lifting this code to a properly chosen subfield $\mathcal{K}$ of a cyclotomic function field we will get a not trivial iso-dual AG-code over $\mathcal{K}$. We now show that for every integer $n \geq 2$ there is a binary iso-dual AG-code defined over $\mathcal{K}_n$.

Theorem 7.2. *For any integer $n \geq 2$ the lifted code $\mathfrak{L}_{\mathcal{K}_n/\mathcal{F}}(C_{\mathcal{L}}(D, G))$, where D and G are as in (7.5) and (7.6), is a binary iso-dual AG-code over $\mathcal{K}_n$ of length 2^{n-m} and dimension 2^{n-m-1}, where $m = \lceil \log_2(n) \rceil$.*

Proof. First notice that when $q = 2$ the rational place P_∞ splits completely in $\mathcal{F}(\Lambda_{x^n})$ and thus it splits completely in any subfield of $\mathcal{F}(\Lambda_{x^n})$. In particular P_∞ splits completely in $\mathcal{K}_n$. The only ramified place in $\mathcal{F}(\Lambda_{x^n})/\mathcal{F}$ is the place P_x which is, in fact, totally ramified in $\mathcal{F}(\Lambda_{x^n})/\mathcal{F}$. Therefore

$$\mathrm{Diff}(\mathcal{K}_n/\mathcal{F}) = d(S_x|P_x)S_x,$$

and since S_x is rational (see item (a) of Proposition 7.1) we have, from (4.3), that the different exponent $d(S_x|P_x)$ is even.

On the other hand, since $x+1$ is irreducible over $\mathbb{F}_2$ and does not divide x, we have that P_{x+1} splits completely in $\mathcal{K}_n$. Hence, we can apply Theorem 4.1 in this situation with D and G as in (7.5) and (7.6) respectively, and we have that the lifted code $\mathfrak{L}_{\mathcal{K}_n/\mathcal{F}}(C_{\mathcal{L}}(D,G))$ is an iso-dual AG-code over $\mathcal{K}_n$. In fact, since $[\mathcal{K}_n:\mathcal{F}]=2^{n-m-1}$ (see Figure 3 above), $\mathfrak{L}_{\mathcal{K}_n/\mathcal{F}}(C_{\mathcal{L}}(D,G))$ is a binary iso-dual AG-code over $\mathcal{K}_n$ of length 2^{n-m} and dimension 2^{n-m-1}. □

7.2. **Ternary cyclotomic iso-dual codes.** Assume now that $q=3$ so that $\mathcal{F}=\mathbb{F}_3(x)$. In this case we have four rational places P_x, P_{x-1}, P_{x-2} and P_∞ in $\mathcal{F}$. We take again $f=x$ and, unlike the previous case in which $q=2$, we have now that P_∞ is ramified in $\mathcal{F}(\Lambda_{x^n})$. In fact, P_∞ ramifies in $\mathcal{F}(\Lambda_x)$ and then it splits completely into 3^{n-1} rational places of $\mathcal{F}(\Lambda_{x^n})$ (see Figure 2 with $f=x$). Since in this case $e(R|P_\infty)=2$ for any place R of $\mathcal{F}(\Lambda_{x^n})$ lying over P_∞ and $q=3$, each different exponent $d(R|P_\infty)=1$ and we can not use Theorem 4.1 directly to lift an iso-dual rational AG-code over $\mathcal{F}$ into a subextension of $\mathcal{F}(\Lambda_{x^n})$.

However, since $\mathcal{F}(\Lambda_x)$ is a rational function field, if we show that

$$\mathcal{F}(\Lambda_x)\subset\mathcal{K}_n,$$

then we will be able to use Theorem 4.1 to lift a rational iso-dual code over $\mathcal{F}(\Lambda_x)$ to $\mathcal{K}_n$ by showing that an even number of rational places of $\mathcal{F}(\Lambda_x)$ split completely in $\mathcal{K}_n$ (notice that if $\mathcal{F}(\Lambda_x)\subset\mathcal{K}_n$ then, from Theorem 7.3, we see that we are in the situation of formula (4.3), so that the different exponent $d(S_x|Q_x)$ is even.)

We show now that $\mathcal{F}(\Lambda_x)$ is also a subextension of $\mathcal{K}_n$. For any $u\in\bar{\mathcal{F}}$ the action is $u^x=u^3+xu$, and hence we see that

$$\Lambda_x=\{u\in\bar{\mathcal{F}}:u^3+xu=0\}=\{0\}\cup\{u\in\bar{\mathcal{F}}:u^2+x=0\},$$

so that $\mathbb{F}_3(x)=\mathbb{F}_3(y^2)\subsetneq\mathbb{F}_3(y)\subset\mathcal{F}(\Lambda_x)$ where $y^2+x=0$. Since $\Lambda_x\subset\mathbb{F}_3(y)$ we conclude that $\mathcal{F}(\Lambda_x)=\mathbb{F}_3(y)$ and since

$$y^{x+1}=(x+1)(\varphi+\mu_x)(y)=(\varphi+\mu_x)(y)+y=y^3+xy+y=y,$$

we also have that $\mathcal{F}(\Lambda_x)$ is fixed by H so that $\mathcal{F}(\Lambda_x)\subset\mathcal{K}_n$.

Now, since the rational place $P_{x-2}=P_{x+1}$ of $\mathcal{F}$ splits completely into $2\cdot 3^{n-m-1}$ rational places of $\mathcal{K}_n$, then P_{x-2} splits completely into two rational places of $\mathcal{F}(\Lambda_x)$ because $\mathcal{F}(\Lambda_x)/\mathcal{F}$ is a quadratic extension when $q=3$. In this way, we have three rational places of $\mathcal{F}(\Lambda_x)$ splitting completely in $\mathcal{K}_n$, namely the two rational places of $\mathcal{F}(\Lambda_x)$ lying over P_{x-2}, say Q^1_{x-2} and Q^2_{x-2}, and Q_∞.

We define the divisors D and G of $\mathcal{F}(\Lambda_x)$ as

$$D=Q^1_{x-2}+Q^2_{x-2}, \tag{7.7}$$

and $G=(y)$. From the equation $y^2+x=0$ we see that

$$G=Q_x-Q_\infty \tag{7.8}$$

so that $\operatorname{supp}(D) \cap \operatorname{supp}(G) = \varnothing$. Since $\deg G = 0$ and $\mathcal{F}(\Lambda_x)$ is a rational function field, we have from (c) of Proposition 2.6 that $C_{\mathcal{L}}(D, G)$ is an iso-dual AG-code over $\mathcal{F}(\Lambda_x)$. Since

$$\operatorname{Diff}(\mathcal{K}_n/\mathcal{F}(\Lambda_x)) = d(S_x|Q_x)S_x,$$

and $d(S_x|Q_x)$ is even, we see that the extension $\mathcal{K}_n/\mathcal{F}(\Lambda_x)$ satisfies the conditions of Theorem 4.1. In this way we have that the lifted code $\mathfrak{L}_{\mathcal{K}_n/\mathcal{F}}(C_{\mathcal{L}}(D, G))$ is a ternary iso-dual AG-code over $\mathcal{K}$ of length $4 \cdot 3^{n-m-1}$. Hence, we have proved the following.

Theorem 7.3. *For any $n \in \mathbb{N}$, the lifted code $\mathfrak{L}_{\mathcal{K}_n/\mathcal{F}}(C_{\mathcal{L}}(D, G))$, where D and G are as in (7.7) and (7.8), is a ternary iso-dual AG-code over $\mathcal{K}_n$ of length $4 \cdot 3^{n-m-1}$ and dimension $2 \cdot 3^{n-m-1}$, where $m = \lceil \log_3(n) \rceil$.*

Remark 7.4. The genus of $\mathcal{K}_n$ for $q = 2$ as well as for $q = 3$ grows too quickly with respect to the length of the lifted iso-dual codes, and then the standard estimate for the minimum distance of the lifted iso-dual codes given in Corollary 4.3 is meaningless except for very small values of n. For example in the binary case, already for $n = 7$ (hence $m = 3$) we have that the length of the lifted iso-dual code given in Theorem 7.2 is smaller than $2g(\mathcal{K}_7) - 2$. In fact, for $n = 7$ the length of the lifted binary iso-dual code is 16, and since the integers $e_1 = e_7 = 2$, $e_2 = e_6 = 4$, $e_3 = e_5 = 2$ and $e_4 = 16$, from (7.4) we see that

$$2g(\mathcal{K}_7) - 2 = \tfrac{1}{2^m}\Big(2^{n-1}(n-3) - \sum_{i=1}^{2^m-1} 2^{e_i}\Big) = \tfrac{1}{8}(5 \cdot 2^6 - 32) = 28 > 16,$$

as stated. A similar situation holds for the case of the lifted ternary iso-dual codes given in Theorem 7.3. Therefore, since these codes are rather long, it seems an interesting problem to determine if there are alternative ways of getting meaningful estimates for the minimum distance of these cyclotomic iso-dual AG-codes.

In view of Remark 7.4 the authors propose the investigation of the minimum distance of the binary and ternary cyclotomic iso-dual codes.

References

[1] M. Abdón, J. Bezerra, and L. Quoos. Further examples of maximal curves. *J. Pure Appl. Algebra*, 213(6):1192–1196, 2009.

[2] E. Ballico and M. Bonini. On the weights of dual codes arising from the GK curve. *Appl. Algebra Engrg. Comm. Comput.*, 34(1):67–79, 2023.

[3] D. Bartoli, M. Montanucci, and L. Quoos. Locally recoverable codes from automorphism group of function fields of genus $g \geq 1$. *IEEE Trans. Inform. Theory*, 66(11):6799–6808, 2020.

[4] D. Bartoli, M. Montanucci, and G. Zini. On certain self-orthogonal AG codes with applications to quantum error-correcting codes. *Des. Codes Cryptogr.*, 89(6):1221–1239, 2021.

[5] A. Bassa and H. Stichtenoth. Self-dual codes better than the Gilbert-Varshamov bound. *Des. Codes Cryptogr.*, 87(1):173–182, 2019.

[6] M. Bras-Amorós, A. S. Castellanos, and L. Quoos. The isometry-dual property in flags of two-point algebraic geometry codes. *IEEE Trans. Inform. Theory*, 68(2):828–838, 2022.

[7] M. Chara, S. Kottler, B. Malmskog, B. Thompson, and M. West. Minimum distance and parameter ranges of locally recoverable codes with availability from fiber products of curves. *Des. Codes Cryptogr.*, 91(5):2077–2105, 2023.

[8] M. Chara, R. A. Podestá, and R. Toledano. The conorm code of an AG-code. *Adv. Math. Commun.*, 17(3):714–732, 2023.
[9] W. Fang, J. Wen, and F.-W. Fu. Quantum MDS codes with new length and large minimum distance. *Discrete Math.*, 347(1):Paper No. 113662, 2024.
[10] A. Garcia, C. Güneri, and H. Stichtenoth. A generalization of the Giulietti-Korchmáros maximal curve. *Adv. Geom.*, 10(3):427–434, 2010.
[11] O. Geil, C. Munuera, D. Ruano, and F. Torres. On the order bounds for one-point AG codes. *Adv. Math. Commun.*, 5(3):489–504, 2011.
[12] M. Giulietti and G. Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.*, 343(1):229–245, 2009.
[13] V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981.
[14] V. D. Goppa. Algebraic-geometric codes. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(4):762–781, 896, 1982.
[15] D. R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.
[16] H. J. Kim and Y. Lee. Construction of isodual codes over $GF(q)$. *Finite Fields Appl.*, 45:372–385, 2017.
[17] J.-L. Kim and G. L. Matthews. Quantum error-correcting codes from algebraic curves. In *Advances in algebraic geometry codes*, volume 5 of *Ser. Coding Theory Cryptol.*, pages 419–444. World Sci. Publ., Hackensack, NJ, 2008.
[18] G. Korchmáros, G. P. Nagy, and M. Timpanella. Codes and gap sequences of Hermitian curves. *IEEE Trans. Inform. Theory*, 66(6):3547–3554, 2020.
[19] G. G. La Guardia and F. R. F. Pereira. Good and asymptotically good quantum codes derived from algebraic geometry. *Quantum Inf. Process.*, 16(6):Paper No. 165, 12, 2017.
[20] L. Landi and L. Vicino. Two-point AG codes from the Beelen-Montanucci maximal curve. *Finite Fields Appl.*, 80:Paper No. 102009, 17, 2022.
[21] Y. Li, Y. Su, S. Zhu, S. Li, and M. Shi. Several classes of Galois self-orthogonal MDS codes and related applications. *Finite Fields Appl.*, 91:Paper No. 102267, 28, 2023.
[22] G. L. Matthews and T. W. Michel. One-point codes using places of higher degree. *IEEE Trans. Inform. Theory*, 51(4):1590–1593, 2005.
[23] C. Munuera, A. Sepúlveda, and F. Torres. Castle curves and codes. *Adv. Math. Commun.*, 3(4):399–408, 2009.
[24] C. Munuera, W. Tenório, and F. Torres. Quantum error-correcting codes from algebraic geometry codes of Castle type. *Quantum Inf. Process.*, 15(10):4071–4088, 2016.
[25] H. Niederreiter and C. Xing. Explicit global function fields over the binary field with many rational places. *Acta Arith.*, 75(4):383–396, 1996.
[26] H. Niederreiter and C. Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2001.
[27] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee. Which linear codes are algebraic-geometric? *IEEE Trans. Inform. Theory*, 37(3):583–602, 1991.
[28] H.-G. Quebbemann. Cyclotomic goppa codes. volume 34, pages 1317–1320. 1988. Coding techniques and coding theory.
[29] L. Sok. New families of self-dual codes. *Des. Codes Cryptogr.*, 89(5):823–841, 2021.
[30] H. Stichtenoth. Self-dual Goppa codes. *J. Pure Appl. Algebra*, 55(1-2):199–211, 1988.
[31] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vlăduţ-Zink bound. *IEEE Trans. Inform. Theory*, 52(5):2218–2224, 2006.
[32] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
[33] J. Sui, Q. Yue, and F. Sun. New constructions of self-dual codes via twisted generalized Reed-Solomon codes. *Cryptogr. Commun.*, 15(5):959–978, 2023.
[34] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.0)*, 2017. `https://www.sagemath.org`.

[35] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

María Chara, Researcher of CONICET at Facultad de Ingeniería Química, Universidad Nacional del Litoral, Santiago del Estero 2829, (3000) Santa Fe, Argentina.
E-mail: mchara@santafe-conicet.gov.ar

Ricardo Podestá, FaMAF – CIEM (CONICET), Universidad Nacional de Córdoba, Av. Medina Allende 2144, Ciudad Universitaria, (5000) Córdoba, Argentina.
E-mail: podesta@famaf.unc.edu.ar

Luciane Quoos, Universidade Federal do Rio de Janeiro, Centro de Tecnologia, Cidade Universitária, Av. Athos da Silveira Ramos 149, Ilha do Fundão, CEP 21.941-909, Brazil. *E-mail: luciane@im.ufrj.br*

Ricardo Toledano, Facultad de Ingeniería Química, Universidad Nacional del Litoral, Santiago del Estero 2829, (3000) Santa Fe, Argentina. *E-mail: ridatole@gmail.com*