

QUANTUM ERROR-CORRECTING CODES FROM ALGEBRAIC GEOMETRY CODES OF CASTLE TYPE

CARLOS MUNUERA, WANDERSON TENÓRIO, AND FERNANDO TORRES

ABSTRACT. We study Algebraic Geometry codes producing quantum error-correcting codes by the CSS construction. We pay particular attention to the family of Castle codes. We show that many of the examples known in the literature in fact belong to this family of codes. We systematize these constructions by showing the common theory that underlies all of them.

1. INTRODUCTION

Quantum error-correcting codes are essential to protect quantum information. In the last years much research has been done to find good quantum codes following several ways. Calderbank and Shor [3], and Steane [22], showed that quantum codes can be derived from classical linear error-correcting codes verifying certain self-orthogonality properties [1], including Euclidean and Hermitian self-orthogonality. This method, known as *CSS construction*, has received a lot of interest and it has allowed to find many powerful quantum *stabilizer* codes.

Among all the classical codes used to produce quantum stabilizer codes, Algebraic Geometry (AG) codes have received considerable attention [4, 7, 13, 14, 15, 16, 20, 21]. Conditions for Euclidean self-orthogonality of AG codes are well known [23] and allow us to translate the combinatorial nature of this problem into geometrical terms concerning the arithmetic of the involved curves. Furthermore, Hermitian self-orthogonality can be easily ensured in a similar manner.

From among all curves used to get AG codes, we can highlight the family of Castle and weak Castle curves [19], that combine the good properties of having a reasonable simple handling and giving codes with excellent parameters. In fact, most of the one-point AG codes studied in the literature belong to the family of Castle codes. Besides these codes have, in a natural way, self-orthogonality properties which are very close to those required for obtaining quantum stabilizer codes. It follows from the foregoing that many of the AG codes used to derive quantum codes are particular cases of weak Castle codes. In this article we systematize these constructions, including them in the overall framework

2000 *Mathematics Subject Classification.* 94B27, 81P70, 11T71.

Key words and phrases. Quantum codes, Self-orthogonal codes, Algebraic geometry codes, Castle codes, Trace codes.

of Castle codes. To this end, we show the common theory that underlies all of them and we include many examples, some of which refer to curves and codes already treated in the literature.

The paper is organized as follows. In Section 2 we overview the constructions of quantum codes from classical codes. Section 3 is devoted to Algebraic Geometry codes, and mainly to Castle codes. These provide sequences of self-orthogonal and formally self-orthogonal codes that can be used to produce quantum codes. We give sufficient conditions for self-duality and study in detail some particular families of curves and codes. In Section 4 we show some parameters of quantum codes we have obtained from the curves presented in Section 3. Rather than obtaining codes with new or excellent parameters, we are interested in showing the common bases on which all of them are based. Finally in Section 5 we consider trace codes of AG codes defined over extensions of \mathbb{F}_q and the quantum codes derived from them. Trace codes are closely related to subfield subcodes, from which have recently been obtained quantum codes with excellent parameters [7, 8].

As a notation, given a finite field \mathbb{F}_q , we write $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$. Given a vector $\mathbf{x} \in \mathbb{F}_q^n$ and an integer t , $\mathbf{x}^t = (x_1^t, \dots, x_n^t)$ (when this makes sense). If $X \subset \mathbb{F}_q^n$, then $X^t = \{\mathbf{x}^t : \mathbf{x} \in X\}$.

2. PRELIMINARIES ON QUANTUM ERROR-CORRECTING CODES

Let q be a prime power. A q -ary *quantum error-correcting code* of length n and dimension $K \geq 1$ is a K -dimensional linear subspace Q of \mathbb{C}^{q^n} , where \mathbb{C} is the field of complex numbers. If Q can detect $d - 1$ errors and correct $\lfloor (d - 1)/2 \rfloor$ errors, then it is usually referred as a quantum $[[n, k, d]]_q$ code, where $k = \log_q(K)$.

q -ary quantum codes can be obtained from classical codes C over \mathbb{F}_q and over \mathbb{F}_{q^2} by the so-called CSS construction, as explained below. Quantum codes constructed in this way are *stabilizer* quantum codes. In this paper we are mainly interested in quantum codes obtained from classical algebraic geometry codes. For all facts concerning quantum codes and how to derive them from classical codes, we refer to [1, 15].

2.1. Quantum codes from linear codes over \mathbb{F}_q . We shall denote by $\langle -, - \rangle$ the usual (Euclidean) inner product in \mathbb{F}_q^n , $\langle \mathbf{a}, \mathbf{b} \rangle = \sum a_i b_i$. Given a linear code C over \mathbb{F}_q , the *dual* of C is the code

$$(1) \quad C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \langle \mathbf{v}, \mathbf{c} \rangle = 0 \text{ for all } \mathbf{c} \in C\}.$$

C is called *self-dual* if $C = C^\perp$, and *self-orthogonal* if $C \subseteq C^\perp$, that is if $\langle \mathbf{a}, \mathbf{b} \rangle = 0$ for all $\mathbf{a}, \mathbf{b} \in C$. The so-called *CSS code construction* allows to obtain quantum codes from classical codes over \mathbb{F}_q as follows [15, Cor. 2.15].

Theorem 2.1. *Let C_1, C_2 be two linear codes over \mathbb{F}_q of length n and dimensions k_1 and k_2 respectively with $C_1 \subseteq C_2$. Then there exists a $[[n, k_2 - k_1, d]]_q$ code with minimum distance $d = \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in (C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$.*

Corollary 2.2. *Let C be a self-orthogonal $[n, k, d]$ code over \mathbb{F}_q . Then there exists a $[[n, n - 2k, d]]_q$ code with minimum distance $d = \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in (C^\perp \setminus C)\} \geq d(C^\perp)$.*

This Corollary has been extensively used to ensure the existence of many quantum codes. In [14] Jin and Xing showed that for q even, the orthogonality condition can be weakened in the sense that we can obtain self-orthogonal codes from other codes "close" to be self-orthogonal. To be more precise, let us denote by $*$ the coordinatewise multiplication in \mathbb{F}_q^n , $\mathbf{a} * \mathbf{b} = (a_1 b_1, \dots, a_n b_n)$. Given an n -tuple \mathbf{x} of nonzero elements in \mathbb{F}_q , the map $\mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, $\mathbf{a} \mapsto \mathbf{x} * \mathbf{a}$, is linear and bijective. Furthermore it is an isometry for the Hamming metric. For a linear code C over \mathbb{F}_q , we shall write $\mathbf{x} * C = \{\mathbf{x} * \mathbf{c} : \mathbf{c} \in C\}$. Two codes C_1 and C_2 over \mathbb{F}_q are called *formally equivalent* (or *twisted* according other authors) if there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C_1 = \mathbf{x} * C_2$. Similarly, C is called *formally self-dual* (respectively, *formally self-orthogonal*) if there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ (the *twist*) such that $\mathbf{x} * C = C^\perp$ (resp. $\mathbf{x} * C \subseteq C^\perp$). Next we shall show a construction of this type.

Let $C_0 = (0) \subset C_1 \subset \dots \subset C_n = \mathbb{F}_q^n$ be an increasing sequence of $n + 1$ linear codes in \mathbb{F}_q^n , where C_i has dimension i and minimum distance $d(C_i)$. This sequence is called *self-dual* if $C_i^\perp = C_{n-i}$ for all i , and *formally self-dual* if there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C_i^\perp = \mathbf{x} * C_{n-i}$ for all i . Given such a sequence, note that for i, j , with $1 \leq i \leq j \leq n$ we have

$$(2) \quad C_i^\perp \setminus C_j^\perp = \mathbf{x} * C_{n-i} \setminus \mathbf{x} * C_{n-j} = \mathbf{x} * (C_{n-i} \setminus C_{n-j})$$

and since coordinatewise multiplication by \mathbf{x} is an isometry, we have

$$(3) \quad \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in \mathbf{x} * (C_{n-i} \setminus C_{n-j})\} = \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in (C_{n-i} \setminus C_{n-j})\}.$$

Now, by applying Theorem 2.1, we obtain a quantum $[[n, j - i, d]]_q$ code with minimum distance

$$(4) \quad d = \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in (C_j \setminus C_i) \cup (C_{n-i} \setminus C_{n-j})\} \geq \min\{d(C_j), d(C_{n-i})\}.$$

2.2. Quantum codes from linear codes over \mathbb{F}_{q^2} . We shall denote by $\langle -, - \rangle_H$ the Hermitian inner product in $\mathbb{F}_{q^2}^n$, $\langle \mathbf{a}, \mathbf{b} \rangle_H = \langle \mathbf{a}, \mathbf{b}^q \rangle$. The *Hermitian dual* of a linear code $C \subseteq \mathbb{F}_{q^2}^n$ is

$$(5) \quad C^{\perp H} = \{\mathbf{v} \in \mathbb{F}_{q^2}^n : \langle \mathbf{v}, \mathbf{c}^q \rangle = 0 \text{ for all } \mathbf{c} \in C\} = (C^q)^\perp.$$

C is *Hermitian self-orthogonal* if $C \subseteq C^{\perp H}$, or equivalently if $C^q \subseteq C^\perp$. Raising to the q -th power we find that $\langle \mathbf{v}, \mathbf{c}^q \rangle = 0$ iff $\langle \mathbf{v}^q, \mathbf{c} \rangle = 0$, hence $(C^q)^\perp = (C^\perp)^q$ and so $d(C^{\perp H}) = d(C^\perp)$. We can derive quantum codes from classical codes over \mathbb{F}_{q^2} as follows [15, Cor. 2.16].

Theorem 2.3. *Let C be a linear code over \mathbb{F}_{q^2} of parameters $[n, k, d]$ which is self-orthogonal with respect to the Hermitian inner product. Then there exists a $[[n, n - 2k, d]]_q$ quantum code with minimum distance $d = \min\{\text{wt}(\mathbf{c}) : \mathbf{c} \in (C^{\perp H} \setminus C)\} \geq d(C^\perp)$.*

Let $C_0 = (0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_{q^2}^n$ be an increasing sequence of $n + 1$ linear codes in $\mathbb{F}_{q^2}^n$. From Theorem 2.3 we have the following three procedures to obtain quantum codes over \mathbb{F}_q .

(A) When the sequence is self-dual then the theorem can be applied. As $C_n = \mathbb{F}_{q^2}^n$, for given i let $q(i)$ be the smallest index such that $C_i^q \subseteq C_{q(i)}$. When $i + q(i) \leq n$ we have $C_i^q \subseteq C_{q(i)} \subseteq C_{n-i} = C_i^\perp$, and hence we get a $[[n, n - 2i, \geq d(C_{n-i})]]_q$ code. In later sections of this article we will get sequences of one-point AG codes for which it is possible to give an estimate of $q(i)$ and consequently obtain quantum codes by this procedure.

When the sequence $C_0 = (0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_{q^2}^n$ is formally self-dual but not self-dual, then there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C_i^\perp = \mathbf{x} * C_{n-i}$ for all $i = 0, \dots, n$. Following the aforementioned ideas of Jin and Xing, [14], we can still derive quantum codes in some cases, by slightly modifying the codes.

Lemma 2.4. *Let C be a linear code over \mathbb{F} and $\mathbf{x} \in (\mathbb{F}^\times)^n$. Then $\mathbf{x} * C^\perp = (\mathbf{x}^{-1} * C)^\perp$.*

Proof. Since both codes have equal dimension, it suffices to prove one inclusion. Let $\mathbf{v} \in \mathbf{x} * C^\perp$. There exists $\mathbf{a} \in C^\perp$ such that $\mathbf{v} = \mathbf{x} * \mathbf{a}$. Then $\mathbf{v} * \mathbf{x}^{-1} = \mathbf{a} \in C^\perp$, hence $0 = \langle (\mathbf{v} * \mathbf{x}^{-1}), \mathbf{c} \rangle = \langle \mathbf{v}, (\mathbf{x}^{-1} * \mathbf{c}) \rangle$ for all $\mathbf{c} \in C$, so $\mathbf{v} \in (\mathbf{x}^{-1} * C)^\perp$. \square

(B) Suppose the twist \mathbf{x} verifies $\mathbf{x} \in (\mathbb{F}_q^\times)^n$. Since the elements of \mathbb{F}_q are precisely the $(q + 1)$ -th powers in \mathbb{F}_{q^2} , there exists $\mathbf{y} \in \mathbb{F}_{q^2}^n$ such that $\mathbf{y}^{q+1} = \mathbf{x}$, or equivalently $\mathbf{y}^q = \mathbf{y}^{-1} * \mathbf{x}$. Consider the sequence $\mathbf{y} * C_0 = (0) \subset \mathbf{y} * C_1 \subset \cdots \subset \mathbf{y} * C_n = \mathbb{F}_{q^2}^n$. When $i + q(i) \leq n$ we have

$$(6) \quad (\mathbf{y} * C_i)^q = \mathbf{y}^q * C_i^q = \mathbf{y}^{-1} * \mathbf{x} * C_i^q \subseteq \mathbf{y}^{-1} * \mathbf{x} * C_{q(i)} \subseteq \mathbf{y}^{-1} * \mathbf{x} * C_{n-i} = (\mathbf{y} * C_i)^\perp$$

and we can apply Theorem 2.3 to get a $[[n, n - 2i, \geq d(C_{n-i})]]_q$ quantum code.

(C) To give a concrete example in which the condition $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ holds, we can consider the case in which there exists a self-dual sequence $C'_0 = (0) \subset C'_1 \subset \cdots \subset C'_n = \mathbb{F}_q^n$ of codes over \mathbb{F}_q with $C'_i{}^\perp = \mathbf{x} * C'_{n-i}$ and such that C_0, C_1, \dots, C_n are the codes over \mathbb{F}_{q^2} spanned by C'_0, C'_1, \dots, C'_n , respectively. In this situation it is clear that C_i and C'_i have the same parameters, $C_i^\perp = \mathbf{x} * C_{n-i}$ and $(C_i)^q = C_i$. Let $\mathbf{y} \in \mathbb{F}_{q^2}^n$ such that $\mathbf{y}^{q+1} = \mathbf{x}$ and consider now the sequence $\mathbf{y} * C_0 = (0) \subset \mathbf{y} * C_1 \subset \cdots \subset \mathbf{y} * C_n = \mathbb{F}_{q^2}^n$. For $2i \leq n$ we have

$$(7) \quad (\mathbf{y} * C_i)^q = \mathbf{y}^q * C_i = \mathbf{y}^{-1} * \mathbf{x} * C_i \subseteq \mathbf{y}^{-1} * \mathbf{x} * C_{n-i} = \mathbf{y}^{-1} * C_i^\perp = (\mathbf{y} * C_i)^\perp$$

so we can apply Theorem 2.3 to get a $[[n, n - 2i, \geq d(C_{n-i})]]_q$ code.

3. ALGEBRAIC GEOMETRY CODES AND CASTLE CODES

As we have seen, in order to obtain a quantum code from a linear classical code C , we have to check the self-orthogonality (or Hermitian self-orthogonality) of C and we have

to compute the dual distance $d(C^\perp)$ (resp. $d(C^{\perp H})$). Both tasks are difficult in general. For this reason, among all linear codes producing quantum codes, the class of Algebraic Geometry (AG) codes have received considerable attention [7, 8, 13, 14, 15, 21]. For these codes there is a simple criterion of self-orthogonality. In addition, certain families of AG codes allow efficient methods to estimate their minimum distances [9, 12, 17, 24].

Let us briefly remember the construction of AG codes (see [12, 17] for details and proofs). We pay particular attention to AG codes coming from Castle and weak Castle curves, that produce self-dual and formally self-dual sequences of codes in a natural way.

3.1. Algebraic Geometry codes. Let \mathcal{X} be a nonsingular, projective, geometrically irreducible algebraic curve of genus g defined over \mathbb{F}_q . Take two rational divisors D and G on \mathcal{X} with disjoint supports and such that D is the sum of n rational distinct points, $D = P_1 + \dots + P_n$. In what follows we shall assume $n > 2g$. The algebraic geometry code defined by the triple (\mathcal{X}, D, G) is

$$(8) \quad C = C(\mathcal{X}, D, G) = \{(f(P_1), \dots, f(P_n)) : f \in \mathcal{L}(G)\}$$

where $\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X})^\times : G + \text{div}(f) \geq 0\} \cup \{0\}$ is the Riemann-Roch space associated to G . The dimension and minimum distance of this code verify

$$(9) \quad k = \ell(G) - \ell(G - D), \quad d \geq n - \deg(G) + \gamma_{a+1}$$

where $\ell(G)$ is the dimension of $\mathcal{L}(G)$, $a = \ell(G - D)$ is the *abundance* of C and for $r \geq 1$, $\gamma_r = \min\{\deg(A) : A \text{ is a rational divisor on } \mathcal{X} \text{ with } \ell(A) \geq r\}$ is the r -th gonality of \mathcal{X} .

From the residue theorem, it follows that the dual of an AG code is again an AG code. More precisely, $C(\mathcal{X}, D, G)^\perp = C(\mathcal{X}, D, D + W - G)$, where $W = \text{div}(\omega)$ is the divisor of a differential form ω with simple poles and residue 1 at every point P_i in the support of D . Thus C is self orthogonal if $G \leq D + W - G$. When C is defined over the field \mathbb{F}_{q^2} , and since $C(\mathcal{X}, D, G)^q \subseteq C(\mathcal{X}, D, qG)$, C is Hermitian self-orthogonal if $qG \leq D + W - G$. More generally, if η is a differential form with simple poles at every point P_i in $\text{supp}(D)$, then $C(\mathcal{X}, D, D + \text{div}(\eta) - G) = \mathbf{x} * C(\mathcal{X}, D, G)^\perp$, where $x_i \neq 0$ is the residue of η at P_i .

3.2. One-point Algebraic Geometry codes. If $Q \in \mathcal{X}(\mathbb{F}_q)$ is a rational point not in the support of D , we can take $G = mQ$. The obtained code is called *one-point*. These are the most known and studied codes among the whole family of AG codes. Let $\mathcal{L}(\infty Q) = \cup_{r \geq 0} \mathcal{L}(rQ)$ be the space of rational functions having poles only at Q and consider the evaluation map $\text{ev} : \mathcal{L}(\infty Q) \rightarrow \mathbb{F}_q^n$, $\text{ev}(f) = (f(P_1), \dots, f(P_n))$. The parameters of $C(\mathcal{X}, D, mQ) = \text{ev}(\mathcal{L}(mQ))$ are closely related to the *Weierstrass semigroup* of Q

$$(10) \quad S = S(Q) = \{-v_Q(f) : f \in \mathcal{L}(\infty Q)\} = \{0 = \rho_1 < \rho_2 < \dots\}$$

where v_Q is the valuation at Q . In what follows, for simplicity we shall write $v(f) = -v_Q(f)$. If for all $i = 0, 1, 2, \dots$ we take a function $f_i \in \mathcal{L}(\infty Q)$ such that $v(f_i) = \rho_i$, then

$\{f_1, f_2, \dots\}$ is a basis of $\mathcal{L}(\infty Q)$. From the set of codes $\{C(\mathcal{X}, D, mQ) : m = 0, \dots, n+2g\}$ we can extract an increasing sequence $C_0 = (0) \subset C_1 \subset \dots \subset C_n = \mathbb{F}_q^n$. This sequence is self-dual if the differential form ω with simple poles and residue 1 at every point P_i in $\text{supp}(D)$ has zeros only at Q . This was first noted by Stichtenoth [23]. The sequence is formally self-dual if the divisors $D + W$ and $(n + 2g - 2)Q$ are equivalent, that is when $(n + 2g - 2)Q - D$ is a canonical divisor, $(n + 2g - 2)Q - D \sim \text{div}(\eta)$, and then the twist is $\mathbf{x} = (\text{res}_D(\eta))$.

3.3. Castle curves and codes. Castle curves and codes were introduced in [19], where it is shown that many of the most interesting known examples of AG codes belong to this family. Let \mathcal{X} be a curve defined over \mathbb{F}_q and Q a rational point. The Lewittes bound [17] implies that $\#\mathcal{X}(\mathbb{F}_q) \leq q\rho_2 + 1$, where ρ_2 is the *multiplicity* of $S(Q)$, that is the first nonzero element of $S(Q)$. The pointed curve (\mathcal{X}, Q) is called *Castle* if

- (C1) $S(Q)$ is symmetric; and
- (C2) $\#\mathcal{X}(\mathbb{F}_q) = q\rho_2 + 1$.

Thus rational curves, Hermitian curves, Suzuki and Ree curves, etc., verify the Castle conditions. This family can be generalized in the following way: a pointed curve (\mathcal{X}, Q) over \mathbb{F}_q is called *weak Castle* if it satisfies the conditions

- (C1) $S(Q)$ is symmetric; and
- (C2') let \mathbb{P}^1 be the projective line over the algebraic closure of \mathbb{F}_q . There exist a morphism $f : \mathcal{X} \rightarrow \mathbb{P}^1$ with $\text{div}_\infty(f) = \ell Q$, and a set $U = \{\alpha_1, \dots, \alpha_h\} \subseteq \mathbb{F}_q$ such that for all $i = 1, \dots, h$, we have $f^{-1}(\alpha_i) \subseteq \mathcal{X}(\mathbb{F}_q)$ and $\#f^{-1}(\alpha_i) = \ell$.

Castle curves are weak Castle: simply take $f \in \mathcal{L}(\infty Q)$ with $v(f) = \rho_2$ and $U = \mathbb{F}_q$ [19]. Conversely, in the above situation of (C2'), observe that $\ell \in S(Q)$. Furthermore, since f is unramified over each α_i , if we write $f^{-1}(\alpha_i) = \{P_1^i, \dots, P_\ell^i\}$, then $\text{div}(f - \alpha_i) = \sum_{j=1}^{\ell} P_j^i - \ell Q$. Let

$$(11) \quad D = D_{U,f} = \sum_{i=1}^h \sum_{j=1}^{\ell} P_j^i.$$

If (\mathcal{X}, Q) is weak Castle and D is the sum of all rational points different from Q , then it is said to be *complete*. The one-point codes $C(\mathcal{X}, D, mQ)$ of length $n = \ell h$ are called *weak Castle codes*, or simply *Castle codes* if (\mathcal{X}, Q) satisfies (C2).

Example 3.1. Let q be odd. A hyperelliptic curve \mathcal{X} over \mathbb{F}_q is given by an equation $y^2 = F(x)$, where F is a squareless polynomial. If $\deg(F) = 2g + 1$ then \mathcal{X} has genus g and one hyperelliptic point at infinity, Q . Then \mathcal{X} is Castle iff $F(\alpha)$ is a nonzero square for all $\alpha \in \mathbb{F}_q$. For example, the curve $y^2 = x^q - x + 1$ has $2q + 1$ points and it is Castle for all q . Otherwise, if \mathcal{X} is not Castle, take $U = \{\alpha \in \mathbb{F}_q : F(\alpha) \text{ is a nonzero square in } \mathbb{F}_q\}$. Whenever $U \neq \emptyset$, (\mathcal{X}, Q) is a weak Castle curve and provides codes of length $n = 2\#U$.

Similarly, if q is even, a hyperelliptic curve \mathcal{X} of genus g over \mathbb{F}_q is given by an equation $y^2 + y = F(x)$, where $F(x)$ is a rational function with $\deg(\operatorname{div}_0(F)), \deg(\operatorname{div}_\infty(F)) \leq 2g + 2$. If F is a polynomial there is one hyperelliptic point at infinity Q and \mathcal{X} is Castle or complete weak Castle. For example, the curves $y^2 + y = x^u$, where $q + 1 \mid u$ and $0 < u \leq q^2 - 1$ are Castle over \mathbb{F}_{q^2} .

Castle and weak Castle curves have several nice properties that can be translated to codes arising from them. Next we describe some ones which are relevant for our study. Proofs can be found in [19].

Proposition 3.2. *Let (\mathcal{X}, Q) be a weak Castle curve of genus g over \mathbb{F}_q and $C(\mathcal{X}, D, mQ)$ a weak Castle code. The following hold.*

- (1) *The divisors D and nQ are equivalent. Then for $m < n$, $C(\mathcal{X}, D, mQ)$ reaches the Goppa bound if and only if $C(\mathcal{X}, D, (n - m)Q)$ does. For $m \geq n$, $C(\mathcal{X}, D, mQ)$ is an abundant code of abundance $l((m - n)Q)$.*
- (2) *$(2g - 2)Q$ is a canonical divisor. In consequence $(n + 2g - 2)Q - D$ is also a canonical divisor and there exists $\mathbf{x} \in (\mathbb{F}_q^\times)^n$ such that $C(\mathcal{X}, D, mQ)^\perp = \mathbf{x} * C(\mathcal{X}, D, m^\perp Q)$, where $m^\perp = n + 2g - 2 - m$.*
- (3) *For $i = 1, \dots, n$, let $m_i = \min\{m : \ell(mQ) - \ell((m - n)Q) \geq i\}$. Then $C_i = C(\mathcal{X}, D, m_i Q)$ has dimension i and the sequence $C_0 = (0) \subset C_1 \subset \dots \subset C_n = \mathbb{F}_q^n$ is a formally self-dual sequence of codes.*

The twist \mathbf{x} of item (2) does not depend on m and can be computed as showed in Section 3.2. It is also interesting to note that the set $M = \{m_1 = 0, m_2, \dots, m_n\}$, is called the *dimension set* of (\mathcal{X}, Q) and can be used to obtain good estimates on the minimum distance of codes $C(\mathcal{X}, D, m_i Q)$ by applying the order bound [9, 17]. When \mathcal{X} is weak Castle this set is easy to compute as $M = S(Q) \setminus (n + S(Q))$.

Thus, from a weak Castle curve we obtain in a natural manner a formally self-dual sequence of codes and consequently, by applying the procedures explained in Sections 2.1 and 2.2, a set of quantum stabilizer codes. To be precise, keeping the notation of Proposition 3.2, we have the following results.

Corollary 3.3. *Let (\mathcal{X}, Q) be a weak Castle curve over \mathbb{F}_q and let $C_0 = (0) \subset C_1 \subset \dots \subset C_n = \mathbb{F}_q^n$ be the sequence of codes obtained from it by Proposition 3.2(3). If $2i \leq n$ then we have a quantum code of parameters $[[n, n - 2i, \geq d(C_{n-i})]]_q$, with $d(C_{n-i}) \geq m - m_{n-i} + \gamma_{a+1}$, where $a = \ell((m_{n-i} - n)Q)$ is the abundance of C_{n-i} .*

Proof. Apply construction (C) of Section 2.2 to the formally self-dual sequence $C_0 \subset \dots \subset C_n$. The estimate on the minimum distance follows from the improved Goppa bound stated in equation (9). \square

Corollary 3.4. *Let (\mathcal{X}, Q) be a weak Castle curve over \mathbb{F}_{q^2} such that the sequence $C_0 = (0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_{q^2}^n$ obtained by Proposition 3.2(3) is self-dual. If $qm_i \leq m_{n-i}$ then we have a quantum code over \mathbb{F}_q of parameters $[[n, n - 2i, \geq d(C_{n-i})]]_q$, with $d(C_{n-i}) \geq m - m_{n-i} + \gamma_{a+1}$, where $a = \ell((m_{n-i} - n)Q)$.*

Proof. Similar to the previous corollary, now applying construction (A) and taking into account that $C(\mathcal{X}, D, m_i Q)^q \subseteq C(\mathcal{X}, D, qm_i Q)$. \square

3.4. Duality of Castle codes. In order to obtain quantum codes using the procedure (A) of Section 2.2, formal duality is not enough. In this subsection we give some sufficient conditions on curves verifying Castle assumptions in order to obtain codes satisfying the self-duality property. Given a pointed curve (\mathcal{X}, Q) of genus g , satisfying the condition (C2'), we consider the divisor D of equation (11) and the intrinsic rational function $\phi := \prod_{i=1}^h (f - \alpha_i)$ related to f . As a notation, given an integer m we write $m^\perp = n + 2g - 2 - m$.

Lemma 3.5. *Let (\mathcal{X}, Q) be a pointed curve satisfying (C2'). If $\text{div}(d\phi) = (2g - 2)Q$, then $C(\mathcal{X}, D, mQ)^\perp = C(\mathcal{X}, D, m^\perp Q)$.*

Proof. Consider the differential form $\eta = d\phi/\phi$. From hypothesis we get $\text{div}(\eta) = (n + 2g - 2)Q - D$, and thus η has simple poles and residue 1 at $P \in \text{supp}(D)$. \square

Proposition 3.6. *Let (\mathcal{X}, Q) be a pointed curve satisfying (C2) and let $f \in \mathcal{L}(\infty Q)$ such that $v(f) = \rho_2$. If $\text{div}(df) = (2g - 2)Q$, then $C(\mathcal{X}, D, mQ)^\perp = C(\mathcal{X}, D, m^\perp Q)$.*

Proof. Since in this case $\phi = f^q - f$, we obtain $\text{div}(d\phi) = \text{div}(df)$ and thus the result follows from the previous lemma. \square

Corollary 3.7. *Let (\mathcal{X}, Q) be a pointed curve in the conditions of Lemma 3.5 or Proposition 3.6. Then $C(\mathcal{X}, D, mQ)$ is Euclidean self-orthogonal if $2m \leq n + 2g - 2$. If q is a square, $C(\mathcal{X}, D, mQ)$ is Hermitian self-orthogonal if $(\sqrt{q} + 1)m \leq n + 2g - 2$.*

Corollary 3.8. *Let (\mathcal{X}, Q) be a pointed curve over \mathbb{F}_{q^2} in the conditions of Lemma 3.5 or Proposition 3.6. Let M be the dimension set of (\mathcal{X}, Q) . If $(q + 1)m_i \leq n + 2g - 2$ then we have a quantum code over \mathbb{F}_q of parameters $[[n, n - 2i, \geq d(C_{n-i})]]_q$, with $d(C_{n-i}) \geq m - m_{n-i} + \gamma_{a+1}$, where $a = \ell((m_{n-i} - n)Q)$.*

Remark 3.9. Note that the conditions required by Proposition 3.6 are not verified by all Castle curves. Consider, for example, the hyperelliptic curve \mathcal{X} of equation $y^2 = x^q - x + 1$ over \mathbb{F}_q , q odd of Example 3.1. Here $\rho_2 = 2$ which is the pole order of x at Q , and \mathcal{X} is Castle with $f = x$ in the notation of Proposition 3.6. As the points P over the $x = \alpha$, for α a root of $x^q - x + 1$ in $\overline{\mathbb{F}}_q$, are also ramified, we have $\text{div}(dx) \neq (2g - 2)Q$. On the contrary, for the curves $y^2 + y = x^u$, where $q + 1 | u$, over \mathbb{F}_{q^2} of Example 3.1, a simple computation shows that $\text{div}(dx) = (2g - 2)Q$, hence they provide self-dual sequences of codes.

3.5. *Curves defined by separate equations.* Next we consider the family of curves having a plane model given by a separated variable equation $F(y) = G(x)$, where F and G are univariate polynomials of coprime degrees. The particular case in which one of the polynomials is linearized is interesting since it contains many of the most relevant curves for Coding Theory purposes. For instance, several of the curves studied below were already treated in [23]. Remember that a polynomial F is called *linearized* (or a q -polynomial) if the exponents of all monomials are powers of q .

Proposition 3.10. *Let \mathcal{X} be the curve defined over \mathbb{F}_q by the equation $F(y) = G(x)$, where F and G are polynomials of degrees $a = \deg(F)$, $b = \deg(G)$ with $\gcd(a, b) = 1$. Let Q be the common pole of x and y and ρ_2 the multiplicity of $S(Q)$. Then*

- (1) *The genus of \mathcal{X} is $g = (a - 1)(b - 1)/2$.*
- (2) *The Weierstrass semigroup of Q is $S(Q) = \langle a, b \rangle$. In particular $S(Q)$ is symmetric and $\rho_2 = \min\{a, b\}$.*
- (3) *If F is a linearized separable polynomial, then $\operatorname{div}(dx) = (2g - 2)Q$. If $b > a$ then $\rho_2 = a$ and there exists $f : \mathcal{X} \rightarrow \mathbb{P}^1$ with $\operatorname{div}_\infty(f) = \rho_2 Q$ and $\operatorname{div}(df) = (2g - 2)Q$.*

Proof. (1) It follows from the Riemann-Hurwitz-Zeuthen genus formula. (2) From the equation of \mathcal{X} we have $av(y) = bv(x)$ and since $(a, b) = 1$ we conclude that $v(y) = b, v(x) = a$, hence $S(Q) \supseteq \langle a, b \rangle$. Since the genus of $\langle a, b \rangle$ is g we get equality. As all semigroups generated by two elements are symmetric, the statement follows. (3) Since F is linearized, its derivative is a constant what implies that Q is the only point of \mathcal{X} which ramifies over the morphism x . Using $\operatorname{div}(dx) = -2\operatorname{div}_\infty(x) + R_x$, where R_x is the ramification divisor of the morphism x , we obtain the equality between the divisors. To see the last statement it is enough to take $f = x$. \square

Proposition 3.10 gives a large family of curves verifying the conditions of Proposition 3.6, and hence providing self-dual sequences of Castle and weak Castle codes. Concrete examples of relevant Castle curves used in Coding Theory belonging to this family include those already mentioned above: Hermitian curve, Norm-Trace curve, etc. Recall, however, that not all Castle curves satisfying the conditions of Proposition 3.6 belong to this family. For instance, this happens to the Ree curve [19].

Next we show some examples of curves in the conditions of Lemma 3.5.

Example 3.11. Let \mathcal{X} be the curve given by

$$(12) \quad y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = x^u$$

defined over \mathbb{F}_{q^r} with $u \mid (q^r - 1)/(q - 1)$. We shall see that it is a weak Castle curve with $q^{r-1}(u(q-1)+1)+1$ rational points and genus $g = (u-1)(q^{r-1}-1)/2$. Note that this curve is covered by the Norm-Trace curve over \mathbb{F}_{q^r} ; indeed, it is a quotient curve of the Norm-Trace curve by the cyclic group of automorphisms generated by $(x, y) \mapsto (\zeta x, y)$, where ζ is a primitive u -th root of unity. Also this equation includes many other interesting curves

as the Hermitian curve and its quotients in case of $r = 2$. Now, consider the multiplicative subgroup of $\mathbb{F}_{q^r}^\times$

$$(13) \quad U^\times = \{\beta \in \mathbb{F}_{q^r}^\times ; \beta^u \in \mathbb{F}_q\}$$

of cardinality $u(q-1)$ and set $U = U^\times \cup \{0\}$. Observe that the elements of U are the elements of \mathbb{F}_{q^r} which split totally over the morphism $x : \mathcal{X} \rightarrow \mathbb{P}^1$. Now take

$$(14) \quad \phi = \prod_{\beta \in U} (x - \beta) = x \prod_{\beta \in U^\times} (x - \beta) = x(x^{u(q-1)} - 1) = x^{u(q-1)+1} - x.$$

Since from Proposition 3.10 we have $\text{div}(dx) = (2g-2)Q$, where Q is the unique pole of x , a sufficient condition to have $\text{div}(d\phi) = (2g-2)Q$ is that $u \equiv 1 \pmod{p}$, where p is the characteristic of \mathbb{F}_q . Notice that this always happens in characteristic 2.

3.6. Maximal Curves. Recall that a curve \mathcal{X} of genus g over a field $\mathbb{F}_{q^{2r}}$ is maximal if it attains equality in the Hasse-Weil bound $\#\mathcal{X}(\mathbb{F}_{q^{2r}}) = q^{2r} + 1 + 2gq^r$. Maximal curves often provide AG codes with good parameters. In this subsection we shall give examples of maximal Castle curves verifying the conditions of Proposition 3.10. In particular, the examples we present are Artin-Schreier curves defined over $\mathbb{F}_{q^{2r}}$ by plane models of type $F(y) = G(x)$, where $F(y)$ is linearized and separable of degree ρ a power of $p = \text{char}(\mathbb{F}_q)$, and $G(x)$ of degree $q^r + 1$, bigger than ρ . Thus these curves have genus $2g = (\rho-1)q^r$ and the Weierstrass semigroup $S(Q)$ of Q is generated by ρ and $q^r + 1$. In this situation, maximality implies the Castle condition $\#\mathcal{X}(\mathbb{F}_{q^{2r}}) = q^{2r}\rho + 1$. We just show a couple of examples.

Example 3.12. Let $a \in \mathbb{F}_{q^2}$ such that $a^q + a = 0$ and consider the curve \mathcal{X} defined over \mathbb{F}_{q^2} by

$$(15) \quad y^{q/p} + y^{q/p^2} + \dots + y = ax^{q+1}$$

where $p = \text{char}(\mathbb{F}_q)$. To check the maximality of \mathcal{X} we note that it is covered by the Hermitian curve $\mathcal{H} : w^q + w = z^{q+1}$ via the morphism $x = z$, $y = (-aw)^p + aw$. The cardinality of $\mathcal{X}(\mathbb{F}_{q^2})$ can be computed from this fact by taking into account that its genus g satisfies $2g = (q/p - 1)q$.

Example 3.13. Let \mathcal{X} be the curve over $\mathbb{F}_{q^{2r}}$, r odd, defined by

$$(16) \quad y^q + y = x^{q^r+1}.$$

As in the previous example, \mathcal{X} is maximal as it is covered by the Hermitian curve $\mathcal{H} : w^{q^r} + w = z^{q^r+1}$ over $\mathbb{F}_{q^{2r}}$. A covering is given by $x = z$, $y = w^{q^r-1} - w^{q^r-2} + \dots + w$.

4. SOME EXAMPLES OF QUANTUM CODES

In this Section we shall show a few examples of quantum codes obtained from the curves treated in the above Section. Computations have been done by using the computer system Magma [18]. In order to compare the quality of the obtained parameters we shall use the tables [2, 10] and the quantum Gilbert-Varshamov bound [6]:

Theorem 4.1. *Suppose that $n > k \geq 2$, $d \geq 2$ and $n \equiv k \pmod{2}$. Then there exists a stabilizer quantum code $[[n, k, d]]_q$ provided that*

$$(17) \quad \frac{q^{n-k+2} - 1}{q^2 - 1} > \sum_{i=1}^{d-1} (q^2 - 1)^{i-1} \binom{n}{i}.$$

We shall use the following notation: given a code $[[n, k, d]]_q$, we write $[[n, k, d]]_q^\dagger$ when the parameters n, k, d meet the Gilbert-Varshamov bound with equality. We write $[[n, k, d]]_q^\ddagger$ when the parameters n, k, d strictly improve on the Gilbert-Varshamov bound.

4.1. *Codes from the Suzuki curve.* The curve \mathcal{X} of equation $y^q + y = x^{q_0}(x^q + x)$ over \mathbb{F}_q , where $q_0 = 2^s$ and $q = 2q_0^2$ is called the *Suzuki curve*. It has genus $g = q_0(q - 1)$ and $q^2 + 1$ rational points. Let Q be the common pole of x and y . Then the Weierstrass semigroup $S(Q)$ is generated by $\langle q, q + 1, q + 2q_0, q + 2q_0 + 1 \rangle$ (see [17] and the references therein), so \mathcal{X} is a Castle curve. Codes arising from this curve have been extensively studied and their parameters are rather well known. In particular, the conditions stated in Proposition 3.6 and Corollary 3.7 holds, so that the duals of one point Suzuki codes are again one-point Suzuki codes. We can use them to obtain quantum codes from construction (C) of Section 2.2.

Example 4.2. For $q = 8$, $C(\mathcal{X}, D, mQ)$ has length 64 and is self-orthogonal whenever $m \leq 45$. Then we get quantum codes over \mathbb{F}_8 of parameters $[[64, 62, 2]]_8^\dagger$, $[[64, 54, 3]]_8$, $[[64, 52, 4]]_8^\dagger$, $[[64, 42, 5]]_8$, $[[64, 40, 6]]_8$, $[[64, 38, 7]]_8$, $[[64, 36, 8]]_8$. These are good parameters compared with those listed in [2].

4.2. *Codes from elliptic and hyperelliptic curves.*

Example 4.3. Consider the family of hyperelliptic curves $y^2 + y = x^u$, where $q + 1 \mid u$ and $u \leq q^2 - 1$ over \mathbb{F}_{q^2} , q even, of Example 3.1. In Remark 3.9 we noted that they are Castle and verify $\text{div}(dx) = (2g - 2)Q$. Since they have genus $g = \lfloor u - 1 \rfloor / 2$, $C(\mathcal{X}, D, mQ)$ is self-orthogonal whenever $2m \leq 2q^2 + u - 3$ and Hermitian self-orthogonal whenever $(q + 1)m \leq 2q^2 + u - 3$. We find quantum codes with parameters $[[8, 6, 2]]_2^\ddagger$, $[[32, 30, 2]]_4^\ddagger$, $[[32, 24, 4]]_4^\ddagger$, $[[128, 126, 2]]_8^\ddagger$, $[[128, 116, 4]]_8^\ddagger$, $[[128, 112, 6]]_8^\ddagger$, $[[128, 108, 8]]_8^\ddagger$ among others. The particular case $u = q + 1$ was studied in [13, Sec. III (A)].

Example 4.4. Here we show an example of a complete weak Castle curve which is not Castle. When $q \equiv 3 \pmod{4}$ then -1 is not a square, hence the elliptic curve $\mathcal{X} : y^2 = x^3 + ax$ has $q + 1$ rational points over \mathbb{F}_q . Consequently it has $q^r + 1 + 2\sqrt{q^r}$ rational points over \mathbb{F}_{q^r} for $r \equiv 2 \pmod{3}$. To give a concrete example take $q = 3, r = 2$. A simple computation shows that $\rho_2 = 2$ and \mathcal{X} is not Castle. However \mathcal{X} is a complete weak Castle curve with respect the morphism $f = y$. We obtain codes with the following parameters over \mathbb{F}_9 : $[[15, 13, 2]]_9^\dagger$, $[[15, 7, 4]]_9^\dagger$, $[[15, 5, 5]]_9^\dagger$, $[[15, 3, 6]]_9^\dagger$, $[[15, 1, 7]]_9$. Quantum codes from elliptic curves have been treated in [14].

4.3. *Codes from Hermitian, Norm-Trace and related curves.* Quantum codes arising from Hermitian curves have been extensively treated, [15, 20]. Here we shall consider the related more general curves \mathcal{X} of Example 3.11 given by an equation of the form

$$(18) \quad y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y = x^u$$

over \mathbb{F}_{q^r} with $u \mid (q^r - 1)/(q - 1)$. We saw that when $u \equiv 1 \pmod{p}$ then \mathcal{X} satisfies the conditions of Lemma 3.5, where p is the characteristic of \mathbb{F}_{q^r} . Note that when $u = (q^r - 1)/(q - 1)$, then \mathcal{X} is the Norm-Trace curve, and if $r = 2$ then \mathcal{X} is the Hermitian curve. In both cases such conditions are also automatically satisfied.

Example 4.5. For $q = 2, r = 4$ and $u = 3$, from Corollary 3.7 the codes $C(\mathcal{X}, D, mQ)$ of length 32 over \mathbb{F}_{16} are Hermitian self-orthogonal whenever $m \leq 8$. The quantum codes over \mathbb{F}_4 obtained from these have parameters $[[32, 30, 2]]_4^\dagger$ and $[[32, 24, 3]]_4^\dagger$.

Example 4.6. For $q = 2, r = 3$ and $u = 7$, we obtain the Norm-Trace curve. The codes $C(\mathcal{X}, D, mQ)$ of length 32 over the field \mathbb{F}_8 are self-orthogonal if $m \leq 24$. We obtain $[[32, 28, 2]]_8^\dagger$, $[[32, 26, 3]]_8^\dagger$, $[[32, 18, 4]]_8$ quantum codes.

Example 4.7. For $r = 2$ we obtain the Hermitian curves and quotients $y^q + y = x^u$ with $u \mid q + 1$, over \mathbb{F}_{q^2} , which are \mathbb{F}_{q^2} -maximal. The case where q is an odd power of 2 and $u = 3$ was considered in [13, Sec. III (B)]. We obtain codes $[[8, 6, 2]]_2^\dagger$, $[[64, 54, 3]]_4^\dagger$, $[[64, 52, 4]]_4^\dagger$, $[[176, 162, 3]]_8$, $[[176, 156, 5]]_8$, $[[176, 154, 6]]_8$, $[[176, 150, 8]]_8^\dagger$, $[[176, 146, 9]]_8^\dagger$.

4.4. *Codes from maximal curves.* To end this section, let us see some quantum codes arising from maximal curves as the ones considered in Section 3.6.

Example 4.8. Let \mathcal{X} be the curve over \mathbb{F}_{q^2} of Example 3.12

$$(19) \quad y^{q/p} + y^{q/p^2} + \cdots + y = ax^{q+1}$$

where $a \in \mathbb{F}_{q^2}$ verifies $a^q + a = 0$ and p is the characteristic of \mathbb{F}_q . For $q = 9$ let us take the curve $y^3 + y = \alpha^5 x^{10}$ over \mathbb{F}_{81} , where α is a primitive element of \mathbb{F}_{81} . It has 244 rational points and genus 9. The codes $C(\mathcal{X}, D, mQ)$ are Hermitian self-orthogonal if $m \leq 25$, by Corollary 3.7. For these values we obtain quantum codes with the following parameters: $[[243, 241, 2]]_9^\dagger$, $[[243, 233, 3]]_9^\dagger$, $[[243, 219, 6]]_9$ and $[[243, 213, 9]]_9^\dagger$. For $q = 8$

take $a = 1$. The curve has 257 rational points and genus 12. From Corollary 3.7, the codes $C(\mathcal{X}, D, mQ)$ are Hermitian self-orthogonal if $m \leq 30$. With these values we can provide quantum codes with the following parameters: $[[256, 254, 2]]_8^\dagger$, $[[256, 248, 3]]_8^\dagger$, $[[256, 238, 4]]_8$ and $[[256, 224, 8]]_8$. These quantum codes have good parameters compared to similar quantum codes in [2].

Example 4.9. This is a particular case of the curve given in Example 3.13. Take $r = 3$ in that example and let \mathcal{X} be the curve over \mathbb{F}_{q^6} given by the equation

$$(20) \quad y^q + y = x^{q^3+1}.$$

When $q = 2$, \mathcal{X} has genus 4 and 129 rational points. From Corollary 3.7, the codes $C(\mathcal{X}, D, mQ)$ are Hermitian self-orthogonal if $m \leq 14$. With these values we obtain the following quantum codes: $[[128, 126, 2]]_8^\dagger$, $[[128, 116, 4]]_8^\dagger$, $[[128, 112, 6]]_8^\dagger$ and $[[128, 108, 8]]_8^\dagger$.

5. TRACES OF CASTLE CODES

Some of the codes we have obtained in the previous sections are defined over large extensions of \mathbb{F}_q . However, in practice we can be interested in codes defined over smaller fields. Such codes can be obtained from the formers by two ways: given a code C over \mathbb{F}_{q^r} , we can consider the subfield subcode of C over \mathbb{F}_q , $C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$, and the trace code $\text{tr}(C)$ (see [24], Chapter VIII, where a detailed treatment of subfield subcodes is done). Both codes over \mathbb{F}_q are closely related by Delsarte’s theorem, $(C|_{\mathbb{F}_q})^\perp = \text{tr}(C^\perp)$. However, as we shall see, at least for AG codes the way of using trace maps is simpler. Remark however that quantum codes from subfield subcodes of affine variety codes have been studied in [7, 8].

As in the previous sections, let (\mathcal{X}, Q) be a pointed curve, now defined over \mathbb{F}_{q^r} . Let $\text{tr} : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q$ be the trace map, defined as $\text{tr}(x) = x + x^q + \dots + x^{q^{r-1}}$. tr is a surjective \mathbb{F}_q -linear map that can be extended to $\mathbb{F}_{q^r}^n$ (coordinatewise) and to $\mathcal{L}(\infty Q)$. Here we list some properties of these extensions.

Lemma 5.1. *The following properties hold.*

- (a) *Both extensions of tr are \mathbb{F}_q -linear and $\text{tr} : \mathbb{F}_{q^r}^n \rightarrow \mathbb{F}_q^n$ is surjective.*
- (b) *If $f \in \mathcal{L}(\infty Q)$ then $v(\text{tr}(f)) = q^{r-1}v(f)$. Thus, if f is nonconstant then $\text{tr}(f) \neq 0$.*
- (c) *For all $f \in \mathcal{L}(\infty Q)$ we have $\text{tr}(\text{ev}(f)) = \text{ev}(\text{tr}(f)) = \text{ev}(\text{tr}(f^q))$.*

Let \mathcal{V} be the set of functions in $\mathcal{L}(\infty Q)$ evaluating to \mathbb{F}_q^n , $\mathcal{V} = \{f \in \mathcal{L}(\infty Q) : \text{ev}(f) \in \mathbb{F}_q^n\}$. \mathcal{V} is a \mathbb{F}_q -linear subspace of $\mathcal{L}(\infty Q)$ containing $\ker(\text{ev})$. As a consequence of Lemma 5.1(c), \mathcal{V} also contains $\text{tr}(\mathcal{L}(\infty Q))$. The next proposition explains why trace codes are simpler to handle than subfield subcodes.

Proposition 5.2. $\mathcal{V} = \text{tr}(\mathcal{L}(\infty Q)) + \ker(\text{ev})$.

Proof. Since $\text{tr} \circ \text{ev}$ is surjective (as both maps are so), if $f \in \mathcal{V}$ there exists $g \in \mathcal{L}(\infty Q)$ such that $\text{ev}(f) = \text{tr}(\text{ev}(g)) = \text{ev}(\text{tr}(g))$, hence $f - \text{tr}(g) \in \ker(\text{ev})$. The converse is clear. \square

Thus $\text{ev}(\mathcal{V}) = \text{ev}(\text{tr}(\mathcal{L}(\infty Q)))$ and henceforth we will only consider trace codes. However note that for Castle codes we can also give a basis of $\ker(\text{ev})$ over \mathbb{F}_{q^r} . For all $m > 0$ we have $\ker(\text{ev}) \cap \mathcal{L}(mQ) = \mathcal{L}(mQ - D)$. Let $\varphi = f_2^{q^r} - f_2$. Since \mathcal{X} is Castle, we have $\text{div}(\varphi) = D - nQ$. Consequently there is an isomorphism $\mathcal{L}((n-m)Q) \rightarrow \mathcal{L}(mQ - D)$ given by $f \mapsto \varphi f$ and the set $\{\varphi f_1, \varphi f_2, \dots\}$ is a basis of $\ker(\text{ev})$.

The following results allows us to obtain self-orthogonal trace codes over \mathbb{F}_q when the pointed curve (\mathcal{X}, Q) of genus g over \mathbb{F}_{q^r} has the self-dual property. Let $f_1 = 1$ and for $i = 2, 3, \dots$ let $f_i \in \mathcal{L}(\infty Q)$ such that $v(f_i) = \rho_i$. In view of Lemma 5.1(c), if $\rho_i = q\rho_t$ then we take $f_i = f_t^q$. Then $L = \{f_1, f_2, \dots\}$ is a basis of $\mathcal{L}(\infty Q)$ over \mathbb{F}_{q^r} verifying $L^q \subset L$, and the sets $L_m = \{f_i \in L : \rho_i \leq m\}$ are bases of $\mathcal{L}(mQ)$ for all $m \geq 0$. Let α be a primitive element of \mathbb{F}_{q^r} over \mathbb{F}_q . Then $\{1, \alpha, \dots, \alpha^{r-1}\}$ is a basis of \mathbb{F}_{q^r} over \mathbb{F}_q and every element $a \in \mathbb{F}_{q^r}$ can be written as $a = \lambda_1 + \lambda_2\alpha + \dots + \lambda_r\alpha^{r-1}$ with $\lambda_1, \dots, \lambda_r \in \mathbb{F}_q$.

Proposition 5.3. *The set $\mathcal{B} = \{1\} \cup \{\text{tr}(\alpha^j f_i) : j = 0, \dots, r-1, f_i \in L \text{ for } i > 1\}$ is a basis of $\text{tr}(\mathcal{L}(\infty Q))$ over \mathbb{F}_q . The set $\mathcal{B}_m = \{1\} \cup \{\text{tr}(\alpha^j f_i) : j = 0, \dots, r-1, f_i \in L_m \text{ for } i > 1\}$ is a basis of $\text{tr}(\mathcal{L}(mQ))$ over \mathbb{F}_q .*

Proof. It suffices to show the first statement. That \mathcal{B} is a generator set follows from the \mathbb{F}_q -linearity of tr and the fact that L is a basis of $\mathcal{L}(\infty Q)$ over \mathbb{F}_{q^r} . To see that \mathcal{B} is an independent set, and since $v(\text{tr}(f_i)) \neq v(\text{tr}(f_t))$ if $i \neq t$, it suffices to show that $\text{tr}(f_i), \text{tr}(\alpha f_i), \dots, \text{tr}(\alpha^{r-1} f_i)$ are independent for all $i > 1$. If $0 = \sum_j \lambda_j \text{tr}(\alpha^{j-1} f_i) = \text{tr}(\sum_j \lambda_j \alpha^{j-1} f_i)$ then $\text{tr}(a f_i) = 0$, where $a = \sum_j \lambda_j \alpha^{j-1}$. By Lemma 5.1(b), we have $a f_i = 0$ hence $a = 0$ and $\lambda_j = 0$ for all j . \square

For $j = 0, \dots, r-1$, let $\beta_j \in \mathbb{F}_{q^r}$ such that $\beta_j^q = \alpha^j$. Then, if $f_i = f_t^q$ we have $\text{ev}(\text{tr}(\alpha^j f_i)) = \text{ev}(\text{tr}((\beta_j f_t)^q)) = \text{ev}(\text{tr}(\beta_j f_t))$ by Lemma 5.1(c). Consider the sets $L' = \{1\} \cup (L \setminus L^q)$ and $L'_m = L' \cap L_m$. Define accordingly the sets \mathcal{B}' and \mathcal{B}'_m by substituting L by L' and L_m by L'_m .

Corollary 5.4. *The set $\text{ev}(\mathcal{B}')$ generates $\text{ev}(\text{tr}(\mathcal{L}(\infty Q)))$ over \mathbb{F}_q . The set $\text{ev}(\mathcal{B}'_m)$ generates $\text{tr}(C(\mathcal{X}, D, mQ))$ over \mathbb{F}_q .*

In order to ensure the self-orthogonality of trace codes, we shall use the following fact.

Lemma 5.5. *Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^r}^n$. We have $\langle \text{tr}(\mathbf{x}), \text{tr}(\mathbf{y}) \rangle = \text{tr}(\langle \mathbf{x}, \text{tr}(\mathbf{y}) \rangle)$.*

Proof. For $\mathbf{x}, \mathbf{z} \in \mathbb{F}_{q^r}^n$ and $0 \leq i \leq r$ we have $\langle \mathbf{x}^{q^i}, \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{z}^{q^{r-i}} \rangle^{q^i}$. Take $\mathbf{z} = \text{tr}(\mathbf{y})$. Note that $\mathbf{z} \in \mathbb{F}_q^n$ and hence $\mathbf{z}^{q^{r-i}} = \mathbf{z}$. Thus

$$(21) \quad \langle \text{tr}(\mathbf{x}), \text{tr}(\mathbf{y}) \rangle = \sum_{i=0}^{r-1} \langle \mathbf{x}^{q^i}, \text{tr}(\mathbf{y}) \rangle = \sum_{i=0}^{r-1} \langle \mathbf{x}, \text{tr}(\mathbf{y}) \rangle^{q^i} = \text{tr}(\langle \mathbf{x}, \text{tr}(\mathbf{y}) \rangle).$$

□

Remember that given an integer m , with $0 \leq m \leq n+2g-2$, we write $m^\perp = n+2g-2-m$. The self-orthogonality and the parameters of trace codes can be checked by using the following result.

Proposition 5.6. *Let (\mathcal{X}, Q) be a pointed curve of genus g over \mathbb{F}_{q^r} verifying the self-dual property.*

- (1) *If $mq^{\lfloor r/2 \rfloor} \leq m^\perp$ then $\text{tr}(C(\mathcal{X}, D, mQ))$ is self-orthogonal over \mathbb{F}_q .*
- (2) *If $mq^{r-1} < n$ then $\text{ev}(\text{tr}(f)) \neq 0$ for all $f \in \mathcal{L}(mQ)$.*
- (3) *$d(\text{tr}(C(\mathcal{X}, D, mQ))^\perp) = d(C(\mathcal{X}, D, m^\perp Q)|_{\mathbb{F}_q}) \geq d(C(\mathcal{X}, D, m^\perp Q))$.*

Proof. (1) Assume r is even. If $mq^{r/2} \leq m^\perp$ then for all $i = 0, \dots, r/2$, we have

$$(22) \quad C(\mathcal{X}, D, mQ)^{q^i} \subseteq C(\mathcal{X}, D, mq^i Q) \subseteq C(\mathcal{X}, D, mQ)^\perp.$$

Let $f, g \in \mathcal{L}(mQ)$. According to Lemma 5.5 we have

$$(23) \quad \langle \text{tr}(\text{ev}(f)), \text{tr}(\text{ev}(g)) \rangle = \text{tr} \left(\sum_{j=0}^{r-1} \langle \text{ev}(f), \text{ev}(g)^{q^j} \rangle \right)$$

$$(24) \quad = \text{tr} \left(\sum_{j=0}^{r/2-1} \langle \text{ev}(f), \text{ev}(g)^{q^j} \rangle \right) + \text{tr} \left(\sum_{j=r/2}^{r-1} \langle \text{ev}(f), \text{ev}(g)^{q^j} \rangle \right).$$

By eq. (21) all summands in the first sum of eq. (23) are zero and so its trace is zero. For the second sum note that as seen in the proof of Lemma 5.5 we can write $\langle \text{ev}(f), \text{ev}(g)^{q^j} \rangle = \langle \text{ev}(f)^{q^{r-j}}, \text{ev}(g) \rangle^{q^j}$, with $r-j \leq r/2$. Then $\langle \text{ev}(f)^{q^{r-j}}, \text{ev}(g) \rangle = 0$ and the second trace is also 0. The case r odd is similar. (2) Let $f \in \mathcal{L}(mQ)$. It holds that $v(\text{tr}(f)) \leq mq^{r-1} < n$, hence $\text{ev}(\text{tr}(f)) \neq \mathbf{0}$. (3) Follows from Delsarte's theorem. □

Example 5.7. Consider the Suzuki curve with 65 rational points and genus 14 over \mathbb{F}_8 . According to Proposition 5.6(1), the traces $\text{tr}(C(\mathcal{X}, D, mQ))$ over \mathbb{F}_2 are self-orthogonal for $0 \leq m \leq 30$. Furthermore since $\dim(\text{tr}(C(\mathcal{X}, D, 30Q))) = 32$, this code is self-dual. Thus the bound stated in item (1) is sharp in this case. From these traces, we derive quantum codes with parameters $[[64, 62, 2]]_2^\dagger$, $[[64, 50, 4]]_2^\dagger$, where the notation $[[n, k, d]]_q^\dagger$ is as in Section 4.

Let us consider the case $r = 2$ and let $C = C(\mathcal{X}, D, mQ)$ be a code over \mathbb{F}_{q^2} . Note that the condition on m stated in Corollary 3.7 to ensure the Hermitian self-orthogonality of C , is

exactly the same as the condition of Proposition 5.6(1), to ensure the self-orthogonality of $\text{tr}(C)$. Thus, in some sense, the construction of quantum codes from traces of self-orthogonal codes, extends to $r > 2$ the construction of quantum codes from Hermitian self-orthogonal codes over \mathbb{F}_{q^2} . Note also that besides considering traces $\text{tr}(C(\mathcal{X}, D, mQ))$, we can use 'incomplete' traces, that is subcodes generated by some (but not all) elements of $\text{ev}(\mathcal{B}'_m)$. In many cases these subcodes can provide quantum codes with better parameters than trace codes themselves.

Example 5.8. Consider the elliptic Hermitian curve $\mathcal{X} : y^2 + y = x^3$ with 9 rational points over \mathbb{F}_4 and let α be a primitive element of \mathbb{F}_4 over \mathbb{F}_2 . The trace code $\text{tr}(C(\mathcal{X}, D, 3Q)) = \langle \mathbf{1}, \text{ev}(\text{tr}(x)), \text{ev}(\text{tr}(\alpha x)), \text{ev}(\text{tr}(y)), \text{ev}(\text{tr}(\alpha y)) \rangle$ has dimension 5 and dual distance 4. Thus it cannot be self-orthogonal. Remove the generator $\text{ev}(\text{tr}(y))$. Then we get a self-dual code of dimension 4 whose dual distance is also 4, that gives a quantum $[[8, 0, 4]]_2$ code whose parameters cannot be improved [10]. Furthermore this code cannot be obtained from \mathcal{X} by using Hermitian self-orthogonality and construction (A). In the same way, consider the Hermitian curve over $\mathbb{F}_{q^{2r}}$ with $q^{3r} + 1$ points. The dual distance of the code $C(\mathcal{X}, D, (q^r + 1)Q)$ can be computed by using the order bound. Consider the trace $\text{tr}(C(\mathcal{X}, D, (q^r + 1)Q))$ of this code over \mathbb{F}_q of dimension $2r + 1$ and remove at most $r - 1$ generators from $\text{ev}(\text{tr}(y)), \dots, \text{ev}(\text{tr}(\alpha^{r-1}y))$ in order to obtain a self-orthogonal code with the same dual distance as $\text{tr}(C(\mathcal{X}, D, (q^r + 1)Q))$. Direct computations show that we get quantum codes $[[64, 50, 4]]_2^\dagger$, $[[512, 492, 4]]_2^\dagger$, $[[27, 19, 3]]_3^\dagger$, $[[729, 715, 3]]_3^\dagger$, $[[64, 56, 3]]_4^\dagger$, $[[125, 117, 3]]_5^\dagger$, $[[343, 335, 3]]_7^\dagger$, $[[512, 504, 3]]_8^\dagger$, $[[729, 721, 3]]_9^\dagger$, reaching good parameters in all cases. The same procedure can be carried out by using codes from other curves. For example, from the Norm-Trace curve over \mathbb{F}_{q^r} we obtain quantum codes $[[32, 20, 4]]_2^\dagger$, $[[128, 112, 4]]_2^\dagger$, etc.

ACKNOWLEDGEMENTS

The first author was supported by Spanish Ministerio de Economía y Competitividad under grant MTM2015-65764-C3-1-P MINECO/FEDER. The second and third authors were supported by CNPq-Brazil under grants 201584/2015-8 and 308326/2014-8 respectively. This paper was written partially during a visit of the second and third authors to the University of Valladolid. Both wish to thank the institution for the hospitality and support. The authors are grateful to the anonymous referees for their invaluable comments and suggestions which substantially helped improving the quality of this paper.

REFERENCES

- [1] Ashikhim, A., Knill, E.: Non-binary quantum stabilizer codes. *IEEE Transactions on Information Theory* **47**, 3065-3072 (2001).
- [2] Edel, Y.: Some good quantum twisted codes. Online available at <http://www.mathi.uni-heidelberg.de/~yves/Matrizen/QT BCH/QT BCHindex.html>

- [3] Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. *Physical Review A* **54**, 1098-1105 (1996).
- [4] Chen, H.: Some good quantum error-correcting codes from algebraic geometry codes. *IEEE Transactions on Information Theory* **47**, 2059-2061 (2001).
- [5] Cossidente, A., Korchmáros, G., Torres, F.: On curves covered by the Hermitian curve. *J. Algebra* **216**(1), 56-76 (1999).
- [6] Feng, K., Ma, Z.: A Finite Gilbert-Varshamov Bound for Pure Stabilizer Quantum Codes. *IEEE Transactions on Information Theory* **50**, 3323-3325 (2004).
- [7] Galindo, C., Hernando, F.: Quantum codes from affine variety codes and their subfield-subcodes. *Designs, Codes and Cryptography* **76**(1), 89-100 (2015).
- [8] Galindo, C., Hernando, F., Ruano, D.: Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. *Quantum Information Processing* **14**(9), 3211-3231 (2015).
- [9] Geil, O., Munuera, C., Ruano, D., Torres, F.: On the order bounds for one point codes. *Advances in Mathematics of Communications* **5**(3), 489-504 (2011).
- [10] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at <http://www.codetables.de>.
- [11] Hirschfeld, J., Korchmáros, G., Torres, F.: Algebraic curves over a finite field. Princeton Series in Applied Mathematics. Princeton University Press, Princeton (2008).
- [12] Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic Geometry codes. In: Handbook of Coding Theory, vol. 1, 871-961. Pless, V., Huffman, W.C. (Eds.). Elsevier, Amsterdam, (1998).
- [13] Jin, L.: Quantum stabilizer codes from maximal curves. *IEEE Transactions on Information Theory* **60**(1), 313-316 (2014).
- [14] Jin, L., Xing, C.P.: Euclidean and Hermitian self-orthogonal Algebraic Geometry codes and their application to Quantum codes. *IEEE Transactions on Information Theory* **58**(8), 5484-5489 (2012).
- [15] Kim, J., Mathews, G.L.: Quantum error-correcting codes from algebraic curves. In: Advances in Algebraic Geometry codes, 419-444. Martinez, E., Munuera, C., Ruano, D. (Eds.). World Scientific, Hackensack (2008).
- [16] Kim, J., Walker, J.: Nonbinary quantum error-correcting codes from algebraic curves. *Discrete Mathematics* **308**, 3115-3124 (2008).
- [17] Olaya, W., Munuera, C.: An introduction to Algebraic Geometry codes. In: Algebra for Secure and Reliable Communication Modeling, 87-117. Lahyane, M., Martinez, E. (Eds.). Contemporary Mathematics 642, American Mathematical Society, Providence (2015).
- [18] Magma Computational Algebra System. Online available at <http://magma.maths.usyd.edu.au/magma/>.
- [19] Munuera, C., Sepulveda, A., Torres, F.: Castle curves and codes. *Advances in Mathematics of Communications* **3**, 399-408 (2009).
- [20] Sarpevalli, P.K., Klappenecker, A.: Nonbinary quantum codes from Hermitian curves. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 136-143. Lecture Notes in Computer Science 3857, Springer, Berlin (2006).
- [21] Shaska, T.: Quantum codes from algebraic curves with automorphisms. *Condensed Matter Physics* **11**(2) (2008), 383-396 (2008).
- [22] Steane, A.M.: Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London-Series A* **452**, 2551-2557 (1996).
- [23] Stichtenoth, H.: Self-dual Goppa codes. *Journal of Pure and Applied Algebra* **55**(1-2), 199-211 (1988).
- [24] Stichtenoth, H.: Algebraic Function Fields and Codes. Springer-Verlag, Berlin (1993).

DEPARTMENT OF APPLIED MATHEMATICS, UNIVERSITY OF VALLADOLID, AVDA SALAMANCA SN,
47014 VALLADOLID, CASTILLA, SPAIN

E-mail address: `cmunuera@arq.uva.es`

UNIVERSITY OF CAMPINAS (UNICAMP), INSTITUTE OF MATHEMATICS, STATISTICS AND COMPUTER
SCIENCE (IMECC), R. SÉRGIO BUARQUE DE HOLANDA, 651, CIDADE UNIVERSITÁRIA “ZEFERINO
VAZ”, 13083-059, CAMPINAS, SP, BRAZIL

E-mail address: `dersonwt@yahoo.com.br`

UNIVERSITY OF CAMPINAS (UNICAMP), INSTITUTE OF MATHEMATICS, STATISTICS AND COMPUTER
SCIENCE (IMECC), R. SÉRGIO BUARQUE DE HOLANDA, 651, CIDADE UNIVERSITÁRIA “ZEFERINO
VAZ”, 13083-059, CAMPINAS, SP, BRAZIL

E-mail address: `ftorres@ime.unicamp.br`