QUANTUM CODES FROM A NEW CONSTRUCTION OF SELF-ORTHOGONAL ALGEBRAIC GEOMETRY CODES

F. HERNANDO, G. MCGUIRE, F. MONSERRAT, AND J. J. MOYANO-FERNÁNDEZ

ABSTRACT. We present new quantum codes with good parameters which are constructed from self-orthogonal algebraic geometry codes. Our method permits a wide class of curves to be used in the formation of these codes. These results demonstrate that there is a lot more scope for constructing self-orthogonal AG codes than was previously known.

1. INTRODUCTION

Polynomial time algorithms on quantum computers for integer prime factorization and discrete logarithms were given by Shor [38]. This justifies the great importance of quantum computation and, specifically, the relevance of quantum error-correcting codes because they protect quantum information from decoherence and quantum noise. Over the last twenty-five years, error-correction has proved to be one of the main obstacles to scaling up quantum computing and quantum information processing. One of the first examples of a quantum error-correcting code is Shor's 9-qubit code [39] which has been generalized in a series of many papers, including [3, 4, 8, 10, 9, 22, 23, 5, 7, 13, 24, 33]. Nowadays the theory of quantum error-correcting codes is a very active area of research (see [30, 31, 15, 16, 17, 25, 18] for some recent publications).

A classical linear error-correcting code is called *self-orthogonal* if it is contained in its dual code. The CSS (Calderbank-Shor-Steane) construction [9, 40] showed that classical self-orthogonal codes with certain properties are useful in the construction of quantum error-correcting codes. As a result, people looking for good quantum error-correcting codes started trying to find classical self-orthogonal codes with the required properties.

In the 1970s and early 1980s, using concepts and tools coming from algebraic geometry, Goppa constructed error correcting linear codes from smooth and geometrically irreducible projective curves defined over a finite field (see [20, 21, 41, 27]). They are called Goppa or algebraic geometry (AG) codes and have played an important role in the theory

2010 *Mathematics Subject Classification.* 94B27, 11T71, 81P70, 14G50.

Key words and phrases. Algebraic geometry codes, quantum error-correction, algebraic curves, finite fields.

The second author was partially supported by Science Foundation Ireland Grant 13/IA/1914. The remainder authors were partially supported by the Spanish Government and the EU funding program FEDER, grants MTM2015-65764-C3-2-P and PGC2018-096446-B-C22. The first and fourth authors are also partially supported by Universitat Jaume I, grant UJI-B2018-10.

of error-correcting codes. They were used to improve the Gilbert-Varshamov bound [42] which was a surprising result at that time. In fact, every linear code can be realized as an algebraic geometry code [37]. In the area of quantum information processing, what is important is that AG codes provide a natural context and method for finding classical self-orthogonal codes. Thus, researchers have focussed on finding suitable self-orthogonal AG codes because they give rise to good quantum error-correcting codes.

Many of the properties of AG codes that give rise to good quantum error-correcting codes were captured in the definition of Castle curves by Munuera, Sepúlveda, and Torres [35]. In [36], Munuera, Tenório and Torres use the specific properties of algebraic geometry codes coming from Castle and weak Castle curves to provide new sequences of self-orthogonal codes. Essentially, they use Lemma 2 and Proposition 2 of [36] to provide those sequences.

The main purpose of this paper is to show that there is a much larger family of curves from which to obtain self-orthogonal AG codes and good quantum codes. This family includes Castle curves. As a demonstration we provide some examples and some families of curves giving sequences of one-point self-orthogonal AG codes which are not covered in [36].

This paper is laid out as follows. In Section 2 we briefly summarize the construction of AG codes and establish some notation that will be used in the paper. In Section 3 we state and prove the main theoretical results (Theorem 3.1 and corollaries) that generalize the construction of Castle curves and will allow us to present the afore-mentioned sequences of self-orthogonal codes. The next sections are devoted to applying these results and obtaining explicit families of curves giving rise to those sequences. In Section 7, we use them to obtain quantum codes with good parameters, and we compare our results to previous papers.

In the numerical examples we use the computational algebra system MAGMA [6].

2. AG CODES AND THEIR DUALS

Throughout this and next section, we fix an arbitrary finite field $\mathbf{F}$. Let χ be a nonsingular, projective and geometrically irreducible curve χ of genus g over $\mathbf{F}$ (we will say simply 'curve' for abbreviation). We write $\overline{\mathbf{F}}$ for an algebraic closure of $\mathbf{F}$ and $\chi(\mathbf{F}')$ denotes the set of $\mathbf{F}'$-valued points of χ for any field extension $\mathbf{F}'/\mathbf{F}$.

A *divisor* of χ is a formal sum $D = \sum_{i=1}^{r} n_i P_i$, where r is a positive integer, $P_i \in \chi(\overline{\mathbf{F}})$ and $n_i \in \mathbb{Z} \setminus \{0\}$ for all $i = 1, \ldots, r$, and moreover $P_i \neq P_j$ if $i \neq j$. We will say that the divisor D is $\mathbf{F}$-*rational* if $D^\sigma = D$, where $D^\sigma := \sum_{i=1}^{r} n_i \sigma(P_i)$, and $\sigma : \overline{\mathbf{F}} \to \overline{\mathbf{F}}$ is the Frobenius $\mathbf{F}$-automorphism. Equivalently, D can be regarded as a linear combination of places of $\mathbf{F}(\chi)/\mathbf{F}$ with integer coefficients [41, Def. 1.1.8], where $\mathbf{F}(\chi)$ denotes the function field of χ. The *support* of D, denoted by $\mathrm{Supp}(D)$, is the set of points $\{P_1, \ldots, P_r\}$, and the *degree*

of D is defined as $\deg(D) := \sum_{i=1}^{r} n_i \deg(P_i)$, where $\deg(P_i)$ denotes the cardinality of the orbit of P_i under the action of σ (or, equivalently, the degree of the extension $k(P_i)/\mathbf{F}$, where $k(P_i)$ is the residue field of P_i). Notice that a point P is $\mathbf{F}$-*rational* (i.e. $P \in \chi(\mathbf{F})$) if and only if $\deg(P) = 1$.

For every rational function f on χ, not identically 0, the *divisor of* f is

$$(f) := \sum_{P \in \chi(\overline{\mathbf{F}})} \nu_P(f) P$$

where, for each point $P \in \chi(\overline{\mathbf{F}})$, ν_P denotes the discrete valuation at P defined as follows: for any z belonging to the local ring $\mathscr{O}_{\chi,P}$ of χ at P, $\nu_P(z)$ is defined as the non-negative integer m such that $z = ut^m$, u being a unit and t a generator of the maximal ideal of $\mathscr{O}_{\chi,P}$. A point $P \in \chi(\overline{\mathbf{F}})$ is said to be a *zero* (resp. a *pole*) of f if $\nu_P(f) > 0$ (resp., $\nu_P(f) < 0$). Notice that $(f) = (f)_0 - (f)_\infty$, where $(f)_0 = \sum_{\nu_P(f)>0} \nu_P(f) P$ is the *divisor of zeroes* of f and $(f)_\infty = \sum_{\nu_P(f)<0} \nu_P(f) P$) is the *divisor of poles* of f.

A divisor D as above is *effective* if $n_i > 0$ for all $i = 1, \ldots, r$; we write then $D \geq 0$. Also, given two divisors D and D', the notation $D \geq D'$ means that the divisor $D - D'$ is effective. We also consider the following finite-dimensional $\mathbf{F}$-vector space associated with D:

$$\mathscr{L}(D) := \{f \in \mathbf{F}(\chi) \mid D + (f) \geq 0\} \cup \{0\},$$

where (f) denotes the divisor associated to f.

For a fixed set of $\mathbf{F}$-rational points $\mathscr{P} := \{P_1, P_2, \ldots, P_N\}$ on χ, set $D := P_1 + P_2 + \cdots + P_N$, and let G be another $\mathbf{F}$-rational divisor of χ whose support is disjoint from $\mathscr{P}$. Consider the $\mathbf{F}$-vector space

$$\Omega(D) := \{\omega \in \Omega(\chi) \mid (\omega) \geq D\} \cup \{0\},$$

where $\Omega(\chi)$ is the $\mathbf{F}(\chi)$-vector space of rational differential forms over χ, and (ω) denotes the divisor associated to any $\omega \in \Omega(\chi)$.

Definition 2.1. *The* AG code *associated to the triple* (χ, D, G) *is the linear code* $C(D,G)$ *of length* N *over* $\mathbf{F}$ *given by the image of the linear map*

$$ev_{\mathscr{P}} : \mathscr{L}(G) \to \mathbf{F}^N$$

defined by $ev_{\mathscr{P}}(f) := (f(P_1), f(P_2), \ldots, f(P_N))$.

It can be seen that its dual code, $C(D,G)^\perp$, coincides with the image of the map $\mathrm{res}_{\mathscr{P}} : \Omega(G-D) \to \mathbf{F}^N$ defined by $\mathrm{res}_{\mathscr{P}}(\omega) = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_N}(\omega))$, where $\mathrm{res}_{P_i}(\omega)$ stands for the residue of ω at P_i for all $i = 1, \ldots, N$. Furthermore, if ω is a differential form in $\Omega(\chi)$ with simple poles at P_i and such that $\mathrm{res}_{P_i}(\omega) = 1$ for all $i = 1, \ldots, N$, then it holds that

$$C(D,G)^\perp = C(D, (\omega) + D - G)$$

(see, for instance, [12, Lemma 1.38]). Notice that a differential ω with these conditions does always exist.

Definition 2.2. *The code $C(D,G)$ is said to be* self-orthogonal *if $C(D,G) \subseteq C(D,G)^{\perp}$.*

There is a particular class of curves among those satisfying the definition of AG codes. These are called Castle and weak Castle (pointed) curves, see [36, 35]. A pointed curve is a pair (χ, P), where χ is a curve and $P \in \chi(\mathbf{F})$ is a rational point on χ.

Castle and weak Castle curves are defined taking into consideration the following notion. Let χ be a curve and P an $\mathbf{F}$-rational point on χ, and consider the valuation v_P (attached to the local ring) at P. The set

$$\Gamma(P) := \Big\{ -v_P(f) : f \in \bigcup_{k=0}^{\infty} \mathscr{L}(kP) \Big\}$$

is an additive semigroup of $\mathbb{Z}$ which is called the Weierstraß semigroup at the rational point P of χ. We say that a pointed curve (χ, P) is *Castle* if

(1) $\Gamma(P)$ is symmetric, i.e., $h \in \Gamma(P)$ if and only if $2g-1-h \notin \Gamma(Q)$ for all h.
(2) If $s := \min\{h \in \Gamma(P) : h \neq 0\}$, then $\#\chi(\mathbf{F}) = qs+1$.

If we substitute condition (2) by

(2') There exist a morphism $\varphi : \chi \to \overline{\mathbf{F}} \cup \{\infty\}$ with $(\varphi)_\infty = \ell P$ as well as elements $a_1, a_2, \ldots, a_r \in \mathbf{F}$ such that $\varphi^{-1}(a_i) \subseteq \chi(\mathbf{F})$ and $\#\varphi^{-1}(a_i) = \ell$ for all $i = 1, \ldots, r$,

then the pointed curve (χ, P) is said to be *weak Castle*. Notice that the terminology makes sense, since Castle curves are always weak Castle curves [35].

3. Main results

We start this section with some definitions and conventions. An *affine plane curve over* $\mathbf{F}$ will be a curve C defined by an equation $g(x,y) = 0$, where $g(x,y) \in \mathbf{F}[x,y]$, (x,y) being affine coordinates. Considering projective coordinates $(X : Y : Z)$ such that $x = X/Z$ and $y = Y/Z$, we will denote by χ_C the projectivization of C, and by $\pi_C : \tilde{\chi}_C \to \chi_C$ the associated normalization morphism; in this way $\tilde{\chi}_C$ is a nonsingular model of χ_C.

For every $a \in \mathbf{F}$, L_a (resp., L_∞) will denote the *affine* line over $\mathbf{F}$ defined by the equation $x = a$ (resp., the *projective* line over $\mathbf{F}$, called *line at infinity*, with equation $Z = 0$).

Definition 3.1. An affine plane curve C over $\mathbf{F}$ *is said to have only one place at infinity* if it is geometrically irreducible, there exists an $\mathbf{F}$-rational point Q_∞ such that $\chi_C(\overline{\mathbf{F}}) \cap L_\infty(\overline{\mathbf{F}}) = \{Q_\infty\}$, χ_C has only one branch at Q_∞ and this branch is defined over $\mathbf{F}$. We impose the additional condition that C is not a line.

Notice that, in the situation of Definition 3.1, there exists a unique point $P_\infty \in \tilde{\chi}_C(\overline{\mathbf{F}})$ such that $\pi_C(P_\infty) = Q_\infty$ and, moreover, P_∞ is $\mathbf{F}$-rational. Since $\tilde{\chi}_C \setminus \{P_\infty\}$ and C are isomorphic, we will identify the points of both curves.

If C_1 and C_2 are affine or projective plane curves (with respective equations $A = 0$ and $B = 0$) and Q is any point, then we write $I_Q(C_1, C_2)$ (and also $I_Q(A, B)$) for the intersection multiplicity of C_1 and C_2 at Q, see [27, Def. 2.22]. The intersection multiplicity is positive if and only if Q is a point on both C_1 and C_2.

Definition 3.2. Given two affine plane curves C_1 and C_2 over $\mathbf{F}$, we will say that C_1 and C_2 are *transversal* if $I_Q(C_1, C_2) = 1$ for all $Q \in C_1(\overline{\mathbf{F}}) \cap C_2(\overline{\mathbf{F}})$. Also, we will say that C_1 and C_2 are $\mathbf{F}$-*transversal* if they are transversal and, in addition, all the points in $C_1(\overline{\mathbf{F}}) \cap C_2(\overline{\mathbf{F}})$ are $\mathbf{F}$-rational.

Fixing a curve C, for every subset $\mathscr{A}$ of $\overline{\mathbf{F}}$, we will define $\mathscr{P}_{\mathscr{A}}$ by

$$\mathscr{P}_{\mathscr{A}} := \{(\alpha, \beta) \in C(\overline{\mathbf{F}}) : \alpha \in \mathscr{A}\}$$

and we will be studying the polynomial (where $\mathscr{A}$ is finite)

$$f_{\mathscr{A}}(x) := \prod_{a \in \mathscr{A}} (x - a)$$

and its derivative $f'_{\mathscr{A}}(x)$. We will consider the divisor of zeros of the rational function $f'_{\mathscr{A}}(x)$, and if

$$(f'_{\mathscr{A}}(x))_0 = c_1 Q_1 + \cdots + c_s Q_s + mP_\infty$$

where the Q_i are points in the affine chart and P_∞ is the point at infinity of the curve, then we define a divisor M by $M = c_1 Q_1 + \cdots + c_s Q_s = (f'_{\mathscr{A}}(x))_0 - mP_\infty$. It is easy to show that the divisor M is $\mathbf{F}$-rational. We call M the *divisor of affine zeroes* of the rational function defined by the derivative $f'_{\mathscr{A}}(z)$.

Theorem 3.1. *Let C be a smooth affine plane curve over $\mathbf{F}$ with only one place at infinity. Let g be the genus of $\tilde{\chi}_C$ and let*

$$\mathscr{A} = \{a \in \mathbf{F} \mid C \text{ and } L_a \text{ are } \mathbf{F}\text{-transversal}\}.$$

Let $f_{\mathscr{A}}(z) := \prod_{a \in \mathscr{A}} (z - a) \in \mathbf{F}[z]$. Let M be the divisor of affine zeroes of the rational function of $\tilde{\chi}_C$ defined by the derivative $f'_{\mathscr{A}}(z)$, as defined above.

Then the following hold:

(a) *If D is the divisor $\sum_{P \in \mathscr{P}_{\mathscr{A}}} P$, and G is another $\mathbf{F}$-rational divisor such that* $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$, *then*

$$C(D, G)^\perp = C(D, (2g - 2 + \deg(D) - \deg(M))P_\infty + M - G).$$

(b) *If, in addition, $2G \leq (2g - 2 + \deg(D) - \deg(M))P_\infty + M$ then $C(D, G) \subseteq C(D, G)^\perp$.*

Proof. (a) For all $Q = (a, b) \in \mathscr{P}_{\mathscr{A}}$ let $x_Q := x - a$. In view of the choice of $\mathscr{A}$, the image of x_Q at the local ring at Q is a uniformizing parameter. Consider the following differential form of $\tilde{\chi}_C$:

$$\omega = \left(\sum_{a \in \mathscr{A}} \frac{1}{x - a} \right) dx.$$

Clearly, for any $P=(\alpha,\beta)\in\mathscr{P}_{\mathscr{A}}$, we have

$$\omega=\left(\sum_{a\in\mathscr{A}}\frac{1}{x_P+\alpha-a}\right)dx_P=\frac{f'_{\mathscr{A}}(x_P+\alpha)}{\prod_{a\in\mathscr{A}}(x_P+\alpha-a)}dx_P.$$

Therefore ω has poles at the points of $\mathscr{P}_{\mathscr{A}}$, which are of order 1 and have residue 1. Since C and L_a are $\mathbf{F}$-transversal for every root a of $f_{\mathscr{A}}$, the associated divisor to ω is

$$(\omega)=(\deg(D)+2g-2-\deg(M))P_\infty-D+M,$$

and the result now follows from [27, Th. 2.72].

(b) It follows immediately from (a).

□

The following corollary (that is straightforward from Theorem 3.1) concerns AG codes defined from divisors of type $G=mP_\infty$ and yields a range of values of m for which the associated code is self-orthogonal.

Corollary 3.2. *Assume the notation and hypotheses of Theorem 3.1 and suppose that $G=mP_\infty$ with $m\in\mathbb{N}$. Then $C(D,G)\subseteq C(D,G)^\perp$ if $2m\leq 2g-2+\deg(D)-\deg(M)$.*

In the specific case of curves defined by a separable equation $F(y)=H(x)$, the degree of the divisor M mentioned in the statement of Theorem 3.1 can be explicitly computed from the equation of C and the degree of the polynomial $f'_{\mathscr{A}}$:

Corollary 3.3. *Assume the notation and hypotheses of Corollary 3.2 and suppose that C has an equation of the type $F(y)=H(x)$, where F,H are polynomials with coefficients in $\mathbf{F}$. Then* $\deg(M)=\deg(f'_{\mathscr{A}})\cdot\deg(F)$.

Furthermore, $C(D,G)\subseteq C(D,G)^\perp$ if

$$2m\leq 2g-2+\deg(D)-\deg(f'_{\mathscr{A}})\cdot\deg(F).$$

Proof. Let $a_1,\ldots,a_r\in\overline{\mathbf{F}}$ be the distinct roots of the polynomial $f'_{\mathscr{A}}(z)$ and consider the decomposition $f'_{\mathscr{A}}(z)=\delta\sum_{i=1}^r(z-a_i)^{k_i}$, $\delta\in\overline{\mathbf{F}}\setminus\{0\}$. For each $i=1,\ldots,r$, let $b_{1,i},\ldots,b_{s_i,i}$ be the different roots of $F(y)-H(a_i)$ and consider the decomposition

$$F(y)-H(a_i)=\prod_{j=1}^{s_i}(y-b_{j,i})^{\gamma_{j,i}}.$$

Notice that the points in the support of M are those in the set $\{Q_{i,j}:=(a_i,b_{j,i})\}_{1\leq i\leq r;\,1\leq j\leq s_i}$.

The coefficient in M of one of the points $Q_{i,j}$ is $\nu_{Q_{i,j}}(f'_{\mathscr{A}}(x))$, where $\nu_{Q_{i,j}}$ is the valuation defined by the curve C at $Q_{i,j}$; then

$$\nu_{Q_{i,j}}(f'_{\mathscr{A}}(x))=k_i\cdot I_{Q_{i,j}}(F(y)-H(x),f'_{\mathscr{A}}(x))=k_i\cdot\gamma_{j,i}\cdot I_{Q_{i,j}}(y-b_{j,i},x-a_i)=k_i\cdot\gamma_{j,i},$$

therefore

$$\deg(M) = \sum_{i=1}^{r} k_i \sum_{j=1}^{s_i} \gamma_{j,i} = \sum_{i=1}^{r} k_i \deg(F) = \deg(f'_{\mathscr{A}}) \cdot \deg(F).$$

The last part of the statement follows from Corollary 3.2. □

Remark 3.4. In practice, the main difficulty in applying Corollary 3.3 is that the polynomial $f_{\mathscr{A}}(z)$ and its derivative need to be known and can be hard to compute. We give an example of this now.

Example 3.5. *The curve $y^3 - y = x^2 - x^{10}$ has 1215 affine rational points over $\mathbb{F}_{3^6}$. The polynomial $f_{\mathscr{A}}(z)$ can be computed using MAGMA and has degree 405. Furthermore, its derivative has degree 324. Applying Corollary 3.3 gives self-orthogonal curves for m in the range $17 \leq m \leq 129$.*

This is an interesting example because the curve is maximal (recall that a curve defined over $\mathbb{F}_q$ of genus g is maximal over $\mathbb{F}_q$ if the number of projective $\mathbb{F}_q$-rational points is equal to $q+1+2g\sqrt{q}$, see [41]). Maximal curves are desirable in coding theory because the length of the corresponding codes is very good.

We are unable to compute $f_{\mathscr{A}}(z)$ by hand in this example. In the next sections we will give some infinite families of curves where we are able to compute $f_{\mathscr{A}}(z)$ by hand.

Next we present a special case of Corollary 3.3, where the range of values of m for which the codes $C(D, mP_\infty)$ are self-orthogonal depends only on the genus of C and $\deg(F)$. This bound can be used when $f_{\mathscr{A}}(z)$ is not known.

Corollary 3.6. *Assume the notation and hypotheses of Corollary 3.2 and suppose that C has an equation of the type $F(y) = H(x)$, where F, H are polynomials with coefficients in* **F**. *Then $C(D,G) \subseteq C(D,G)^{\perp}$ if*

$$2m \leq 2g - 2 + \deg(F).$$

Proof. First we will prove that $\deg(D) = \#\mathscr{A} \cdot \deg(F)$. Notice that $\deg(D)$ coincides with the cardinality of $\mathscr{P}_{\mathscr{A}}$; hence it is enough to show that $\#\mathscr{P}_{\{a\}} = \deg(F)$ for every $a \in \mathscr{A}$. For this purpose, notice that $I_P(C, L_a) = 1$ for all $P \in \mathscr{P}_{\{a\}}$ because C and L_a are transversal. Then

$$\begin{aligned}
\#\mathscr{P}_{\{a\}} &= \sum_{P \in \mathscr{P}_{\{a\}}} I_P(C, L_a) = \sum_{P \in \mathscr{P}_{\{a\}}} I_P(F(y) - H(x), x - a) \\
&= \sum_{P=(a,b) \in \mathscr{P}_{\{a\}}} I_P(F(y) - H(a), x - a) \\
&= \sum_{P=(a,b) \in \mathscr{P}_{\{a\}}} I_P(y - b, x - a) = \deg(F),
\end{aligned}$$

where the last two equalities are deduced from the fact that C and L_a are **F**-transversal.

Finally, the result follows from

$$\begin{aligned}\deg(M) &= \deg(f'_{\mathscr{A}}) \cdot \deg(F) \\ &\leq (\deg(f_{\mathscr{A}}) - 1) \cdot \deg(F) = (\#\mathscr{A} - 1) \cdot \deg(F) = \deg(D) - \deg(F),\end{aligned}$$

where the first equality is consequence of Corollary 3.3. □

Remark 3.7. There are examples where this bound is tight, in the sense that $C(D,G) \subseteq C(D,G)^{\perp}$ when $2m \leq 2g-2+\deg(F)$, and $C(D,G) \not\subseteq C(D,G)^{\perp}$ for the smallest m with $2m > 2g-2+\deg(F)$. One example is $y^{27}-y=x^2$ over $\mathbb{F}_{3^6}$, the number of rational points is $N = 1431+1$. The derivative $f'_{\mathscr{A}}(z) = 2z^{52}+1$ so it is not constant. The genus is 13 and $\deg(F) = 27$ so $2m \leq 2g-2+\deg(F)$ becomes $m \leq 25$. We confirm with MAGMA that for $1 < m \leq 25$ we have that $C(D,G) \subseteq C(D,G)^{\perp}$ but not for $m = 26$.

To finish this section, we prove that the AG codes coming from Corollary 3.3 arise from weak Castle curves.

Proposition 3.8. *If C is a curve satisfying the hypotheses of Corollary 3.3 then the pointed curve $(\tilde{\chi}_C, P_\infty)$ is weak Castle.*

Proof. Assume the notation of Theorem 3.1 and suppose, without loss of generality, that $0 \in \mathscr{A}$.

Consider an arbitrary element $a \in \mathscr{A}$ and the divisor $(x-a)$ of the rational function $x-a$. Since L_a and C are $\mathbf{F}$-transversal one has that $\mathscr{P}_{\{a\}} \subseteq \tilde{\chi}_C(\mathbf{F})$ and

$$(x-a) = \sum_{P \in \mathscr{P}_{\{a\}}} P - (\rho - \eta_a) P_\infty,$$

where $\rho := I_{Q_\infty}(L_\infty, \chi_C)$ and, for every $a \in \mathscr{A}$, η_a equals $I_{Q_\infty}(\chi_{L_a}, \chi_C)$ if Q_∞ belongs to χ_{L_a}, and 0 otherwise.

Notice that, independently of $a \in \mathscr{A}$, the point Q_∞ belongs to χ_{L_a} if and only if $Q_\infty = (0:1:0)$; moreover, in this case, $I_{Q_\infty}(\chi_{L_a}, \chi_C)$ equals $\mathrm{mult}_{Q_\infty}(\chi_C)$ (the multiplicity of χ_C at Q_∞) because the line L_a is not tangent to χ_C at Q_∞ (notice that C is not a line). This shows that the value η_a does not depend on a and that $\rho - \eta_a > 0$. Therefore

$$(x-a)_0 = \sum_{P \in \mathscr{P}_{\{a\}}} P \quad \text{and} \quad (x-a)_\infty = (\rho - \eta_0) P_\infty.$$

In particular, $\#\mathscr{P}_{\{a\}} = \rho - \eta_0$.

Now, consider the morphism $f : \tilde{\chi}_C \to \mathbb{P}^1$ associated with the rational function defined by x. From the previous paragraphs, it holds that $(f)_\infty = (\rho - \eta_0) P_\infty$ and, for all $a \in \mathscr{A}$, $f^{-1}(a) = \mathscr{P}_{\{a\}} \subseteq \tilde{\chi}_C(\mathbf{F})$ and $\#f^{-1}(a) = \rho - \eta_0$. Hence, taking into account [36, Prop. 3 (2)], the pointed curve $(\tilde{\chi}_C, P_\infty)$ is weak Castle. □

Remark 3.9. We would like to comment on how our results differ from the results in [36] and [19]. All the families of curves in [36] satisfy the hypotheses of Lemma 2 in that paper. Under the assumptions (and notation) of Theorem 3.1, the pointed curve $(\tilde{\chi}_C, P_\infty)$ satisfies the hypotheses of [36, Lemma 2] if and only if the polynomial $f'_{\mathscr{A}}(z)$ is a nonzero constant (if and only if the divisor M in Theorem 3.1 is the zero divisor). In this paper we will present some families with non-constant derivative, which are the first of this kind as far as we are aware.

To emphasize this point, we partition the curves satisfying the hypotheses of Theorem 3.1 into two types:
Type I: those where $f'_{\mathscr{A}}(z)$ is a nonzero constant.
Type II: those where $f'_{\mathscr{A}}(z)$ is not constant.

The curves in [36] are of Type I and many of the codes introduced in our paper come from curves of Type II. Therefore, we are presenting a new type of code. By Proposition 3.8 both types of curves are weak Castle. Most of the Type II curves in this paper are not Castle, as we will see.

The curves provided in [19] are either of Type I or are not one-point AG codes. All codes in our paper are one-point AG codes, and hence our results and examples are different from [19]. Also, all the sets $\mathscr{A}$ in [19] are multiplicative subgroups after removing 0.

Families of self-orthogonal AG codes. The aim of this subsection is to provide a lemma which will allow us to obtain several families of curves satisfying the hypotheses of Corollary 3.3 and, therefore, to obtain families of self-orthogonal AG codes.

Lemma 3.10. *Let* $\mathbf{F}$ *be a finite field of characteristic* p *and let* C *be an affine plane curve over* $\mathbf{F}$ *with equation*

$$F(y) = H(x),$$

where F *and* H *are polynomials with coefficients in* $\mathbf{F}$ *such that* $F'(y)$ *is a nonzero constant and* $\gcd(\deg(H), p) = 1$. *Then*

(a) C *is smooth.*
(b) *If* $\deg(H) > \deg(F)$ *or* $H(x) = x^\ell$ *with* $\ell \in \mathbb{N}$ *such that* $\ell < \deg(F)$ *and moreover* $\gcd(\deg(F), \ell) = 1$, *then* C *has only one place at infinity.*
(c) *The genus of* $\tilde{\chi}_C$ *is* $\frac{1}{2}(\deg(F)-1)(\deg(H)-1)$.

Proof. Statement (a) is obvious, since the partial derivative with respect to y of the defining equation of C is a nonzero constant. We split the proof of (b) in two cases:

Case 1: $\deg(H) > \deg(F)$. In this case, $(0:1:0)$ is the unique intersection point of χ_C and the line at infinity. Set $L := F(y) - H(x)$, $F_0 := y$, $F_1 := x$, $\delta_0 = d_1 := \deg(H)$, $\delta_1 := \deg_y Res_x(L, F_1)$ and $d_2 := \gcd(\delta_0, \delta_1)$, where $Res_x(L, F_1)$ denotes the resultant (with respect to x) of L and F_1.

It is easily checked that $Res_x(L,F_1) = \pm(F(y) - H(0))$. Therefore, $\delta_1 = \deg(F)$ and $d_2 = 1$. Since $d_2 = 1$ and $\frac{d_1}{d_2}\delta_1$ is a multiple of δ_0, Proposition 3.5 of [11] (see also the original source [1] by Abhyankar) implies that C has only one place at infinity.

Case 2: $H(x) = x^\ell$ with $\ell < \deg(F)$ and $\gcd(\deg(F),\ell) = 1$. In this case, $Q := (1:0:0)$ is the unique intersection point of χ_C and the line at infinity. Setting $m := \deg(F)$ one has that the equation of χ_C (in projective coordinates X, Y and Z) is

$$a_0 Y^m + a_1 Y^{m-1} Z + \cdots + a_1 Y Z^{m-1} + a_m Z^m - X^\ell Z^{m-\ell} = 0,$$

where $a_i \in \mathbf{F}$ for all $i = 0,\ldots,m$ and $a_0 \neq 0$. Taking coordinates $u := Y/X$ and $v := Z/X$ in the affine chart U defined by $X \neq 0$ (to which Q belongs), the equation of the restriction of χ_C to U has the form

$$h(u,v) - v^{m-\ell} = 0,$$

where h is an homogeneous polynomial of degree m such that $h(1,0) \neq 0$ and Q is the origin. Hence, C has a unique tangent at Q (defined by $v = 0$). Performing finitely many successive quadratic transformations we can obtain a resolution of singularities of C at Q (so that, by composition of them, we get the normalization morphism $\pi_C : \tilde{\chi}_C \to \chi_C$); see e.g. [2, Lecture 18]. The quadratic transformation (with center Q) defined by $u = u'$ and $v = u'v'$ gives rise to the following equation of the proper transform C' of C:

$$(u')^\ell h(1,v') - (v')^{m-\ell} = 0.$$

Hence, C' meets the exceptional line at a point that is $\mathbf{F}$-rational. Since $\gcd(\ell, m-\ell) = 1$, it is not difficult to see that all the proper transforms involved in the process meet each exceptional line at a unique $\mathbf{F}$-rational point, and that the last proper transform has multiplicity one at every point. Since the points of $\tilde{\chi}_C$ are in one-to-one correspondence with the branches of χ_C [26, Th. 5.29], it follows that C has only one branch at Q (which is $\mathbf{F}$-rational).

It only remains to prove that χ_C is geometrically irreducible. Indeed, reasoning by contradiction, assume that χ_1 and χ_2 are two different components of χ_C. Then both curves χ_1 and χ_2 must meet at the point Q, which contradicts the conclusion of the preceding paragraph.

Statement (c) follows from [36, Prop. 3]. □

Next, in Sections 4, 5, and 6, we will present some families of curves where our results are applicable. From now on, q will be a power of a prime number p and $N(C,q^n)$ stands for the number of $\mathbb{F}_{q^n}$-rational points of an affine curve C. We will make use of the notion of trace of an element $a \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$: the trace is the sum of the conjugates of a with respect to $\mathbb{F}_q$, i.e.

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} = a + a^q + \cdots + a^{q^{n-1}}.$$

4. CURVES $A_{n,q,\ell}$

Let ℓ and n denote positive integers (not both equal to 1) such that $\gcd(p,\ell)=1$, and let $A_{n,q,\ell}$ be the affine curve (defined over $\mathbb{F}_{q^n}$) with equation

$$y^{q^{n-1}}+y^{q^{n-2}}+\cdots+y=x^{\ell}.$$

The following Proposition refers to the statement of Theorem 3.1.

Proposition 4.1. (1) *Let $C=A_{n,q,\ell}$ and let $\mathbf{F}=\mathbb{F}_{q^n}$. Then C is smooth over $\mathbf{F}$ and C has only one place at infinity. The set $\mathscr{A}$ in the statement of Theorem 3.1 is equal to the set of all x-coordinates of the $\mathbb{F}_{q^n}$-rational points of C.*

(2) *Moreover, $f_{\mathscr{A}}(z)=z^{e+1}-z$, where $e:=\gcd(\ell(q-1),q^n-1)$, and the number of $\mathbb{F}_{q^n}$-rational points of $A_{n,q,\ell}$ is $N(A_{n,q,\ell},q^n)=q^{n-1}\cdot(e+1)$.*

Proof. (1) By Lemma 3.10, C is a smooth affine curve having one place at infinity with genus $g=(q^{n-1}-1)(\ell-1)/2$. If a is the x-coordinate of an $\mathbb{F}_{q^n}$-rational point of the curve $A_{n,q,\ell}$ then the equation $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y)=a^{\ell}$ has q^{n-1} distinct solutions for y in $\mathbb{F}_{q^n}$. Hence all the points in the intersection $A_{n,q,\ell}(\overline{\mathbb{F}}_{q^n})\cap L_a(\overline{\mathbb{F}}_{q^n})$ are $\mathbb{F}_{q^n}$-rational. Moreover, if $Q=(a,b)$ is one of these points, then

$$I_Q(A_{n,q,\ell},L_a)=I_{(0,b)}(y^{q^{n-1}}+y^{q^{n-2}}+\cdots+y-a^{\ell},x)=1$$

because $y-b$ is a simple factor of $y^{q^{n-1}}+y^{q^{n-2}}+\cdots+y-a^{\ell}$. Therefore the set

$$\{a\in\mathbb{F}_{q^n}\mid \text{ there exists } b\in\mathbb{F}_{q^n} \text{ such that } (a,b)\in A_{n,q,\ell}(\mathbb{F}_{q^n})\}$$

coincides with $\mathscr{A}=\{a\in\mathbb{F}_{q^n}\mid A_{n,q,\ell}$ and L_a are $\mathbb{F}_{q^n}$-transversal$\}$.

(2) Notice that, on the one hand, $0\in\mathscr{A}$. On the other hand, for every $a\in\mathscr{A}\setminus\{0\}$, we have $a^{\ell(q-1)}=1$ and $a^{q^n-1}=1$ and, therefore, a is a root of z^e-1. Then every element of $\mathscr{A}$ is a root of $z^{e+1}-z$.

Conversely, let a be a root of z^e-1. Then $a^{\ell(q-1)}=1$ and, therefore, $a^{\ell}\in\mathbb{F}_q$. Hence $a\in\mathscr{A}$ because the equation $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y)=a^{\ell}$ has solutions in $\mathbb{F}_{q^n}$ (by surjectivity of trace).

Finally, for every $x\in\mathbb{F}_{q^n}$, it holds that $x^{\ell}\in\mathbb{F}_q$ if and only if either $x=0$ or $x^{\ell(q-1)}=1$. Hence, since $y^{q^{n-1}}+y^{q^{n-2}}+\cdots+y$ is the image of y by the trace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we have

$$N(A_{n,q,\ell},q^n)=q^{n-1}\cdot(\gcd(\ell(q-1),q^n-1)+1)\,.$$

□

Proposition 4.1 means that we can apply Corollary 3.3 to the curve $A_{n,q,\ell}$, and we deduce the following result:

Corollary 4.2. *Let $N := N(A_{n,q,\ell}, q^n)$, let $\{P_1, \ldots, P_N\}$ be the set of $\mathbb{F}_{q^n}$-rational points of $A_{n,q,\ell}$, and let $D = P_1 + \cdots + P_N$ be a divisor of $\tilde{\chi}_{A_{n,q,\ell}}$. Then, for any nonnegative integer m, the AG code (defined from $\tilde{\chi}_{A_{n,q,\ell}}$) given by $C(D, mP_\infty)$ is self-orthogonal if*

$$2(m+1) \leq (q^{n-1}-1)(\ell-1) + q^{n-1}(\mu \cdot \gcd(\ell(q-1), q^n-1)+1),$$

where $\mu := 1$ if p divides $\gcd(\ell(q-1), q^n-1)+1$ and $\mu := 0$ otherwise.

Remark 4.3. In [36, Example 2] the authors consider curves $A_{n,q,\ell}$ with $\ell \mid (q^n-1)/(q-1)$ and show that, when $\ell \equiv 1 (\mathrm{mod}\ p)$, the pointed curves $(\tilde{\chi}_{A_{n,q,\ell}}, P_\infty)$ satisfy the hypotheses of Lemma 2 of [36]. Hence, in these cases, this lemma implies that the code $C(D, mP_\infty)$ (defined as in Corollary 4.2) is self-orthogonal if

$$2(m+1) \leq (q^{n-1}-1)(\ell-1) + q^{n-1}(\ell(q-1)+1).$$

Corollary 4.2 gives a larger family of curves $A_{n,q,\ell}$ which do not necessarily satisfy the hypotheses of Lemma 2 of [36] (see Remark 3.9).

Lastly in this section, we show that the pointed curve $(\tilde{\chi}_{A_{n,q,\ell}}, P_\infty)$ is almost never a Castle curve. Proposition 2 of [36] can only be applied to $(\tilde{\chi}_{A_{n,q,\ell}}, P_\infty)$ when the curve is Castle.

Note that we never have $\ell = q^{n-1}$ because ℓ is relatively prime to p.

Proposition 4.4. *(1) If $\ell < q^{n-1}$ the pointed curve $(\tilde{\chi}_{A_{n,q,\ell}}, P_\infty)$ is never a Castle curve.*

(2) If $\ell > q^{n-1}$ the pointed curve $(\tilde{\chi}_{A_{n,q,\ell}}, P_\infty)$ is a Castle curve if and only if $\gcd(\ell, (q^n-1)/(q-1)) = 1$.

Proof. Let s be the smallest nonzero element of the Weierstraß semigroup at P_∞. We know that the number of (affine) points is $q^{n-1}(e+1)$ so the curve is Castle if and only if $s = q^{n-2}(e+1)$.

Notice that e is a multiple of $q-1$, since $e = (q-1)\gcd(\ell, (q^n-1)/(q-1))$.

Proof of (1) : Suppose $\ell < q^{n-1}$. In this case the smallest element of the Weierstraß semigroup is ℓ i.e. $s = \ell$. But we always choose ℓ to be relatively prime to p, so we cannot have $\ell = q^{n-2}(e+1)$ for $n > 2$. Therefore the curve is never Castle in this case.

If $n = 2$ the curve is Castle iff $\ell = e+1$. Then $e = \ell - 1$, but also $e = (q-1)\gcd(\ell, q+1)$. If $\gcd(\ell, q+1) = 1$ then $\ell = q$, which is impossible. If $\gcd(\ell, q+1) > 1$ then there is a divisor of ℓ which is also a divisor of $\ell - 1$, which is impossible.

Proof of (2) : Suppose $\ell > q^{n-1}$ In this case the smallest element of the Weierstraß semigroup is q^{n-1} i.e. $s = q^{n-1}$. The curve is Castle if and only if $q = e+1$. However $e = q-1$ if and only if $\gcd(\ell, (q^n-1)/(q-1)) = 1$, by the definition of e. □

5. CURVES $B_{q,G}$

Let n be a positive integer and consider a polynomial $G(x) \in \mathbb{F}_q[x]$ such that $\deg(G) > q$ and $\gcd(p, \deg(G)) = 1$. Consider the unique polynomial $\mathrm{Tr}_n(G)(z) \in \mathbb{F}_q[z]$ with degree at most $q^n - 1$ such that $\mathrm{Tr}_n(G)(a) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(G(a))$ for all $a \in \mathbb{F}_{q^n}$. We will assume that

(1) $\mathrm{Tr}_n(G)$ is separable, and
(2) all roots of $\mathrm{Tr}_n(G)$ belong to $\mathbb{F}_{q^n}$.

For such G, we define $B_{q,G}$ to be the affine curve (over $\mathbb{F}_q$) with equation $y^q - y = G(x)$. Notice that, by [32, Th. 2.25], the set of $\mathbb{F}_{q^n}$-rational points of $B_{q,G}$ is $\{(a,b) \in \mathbb{F}_{q^n}^2 \mid \mathrm{Tr}_n(G)(a) = 0 \text{ and } b^q - b = G(a)\}$.

The following proposition refers to the statement of Theorem 3.1.

Proposition 5.1. (1) *Let $C = B_{q,G}$ and let $\mathbf{F} = \mathbb{F}_{q^n}$. Then C is smooth over $\mathbf{F}$ and C has only one place at infinity. The set $\mathscr{A}$ in the statement of Theorem 3.1 is equal to the set of all x-coordinates of the $\mathbb{F}_{q^n}$-rational points of C.*

(2) *Moreover*

$$f_{\mathscr{A}}(z) = \gamma \cdot \mathrm{Tr}_n(G)(z)$$

for some $\gamma \in \mathbb{F}_q \setminus \{0\}$, and the number of $\mathbb{F}_{q^n}$-rational points of $B_{q,G}$ is $N(B_{q,G}, q^n) = q \cdot \deg(\mathrm{Tr}_n(G))$.

Proof. (1) First of all, notice that the curve $B_{q,G}$ is smooth and has only one place at infinity by Lemma 3.10.

Second, if a is the x-coordinate of an $\mathbb{F}_{q^n}$-rational point of $B_{q,G}$, then the equation $y^q - y = G(a)$ has q distinct solutions in $\mathbb{F}_{q^n}$. Indeed, since $y^q - y = G(a)$ has, at least, one solution $b \in \mathbb{F}_{q^n}$, it is obvious that the set of all solutions is $\{b + \alpha \mid \alpha \in \mathbb{F}_q\}$. Hence, an analogous reasoning as in the proof of Theorem 3.1 shows that L_a and $B_{q,G}$ are $\mathbb{F}_{q^n}$ transversal.

(2) This follows from part (1) because $\mathrm{Tr}_n(G)$ is a separable polynomial and all its roots belong to $\mathbb{F}_{q^n}$. Finally, the counting of $\mathbb{F}_{q^n}$-rational points is easy to check. □

Using Proposition 5.1 we can apply Corollary 3.3 to the curve $B_{q,G}$ and deduce the following result:

Corollary 5.2. *Let $N := N(B_{q,G}, q^n)$, let $\{P_1, \ldots, P_N\}$ be the set of $\mathbb{F}_{q^n}$-rational points of $B_{q,G}$, and let $D = P_1 + \cdots + P_N$ be a divisor of $\tilde{\chi}_{B_{q,G}}$.*

Then, for any nonnegative integer m, the AG code (defined from $\tilde{\chi}_{B_{q,G}}$) given by $C(D, mP_\infty)$ is self-orthogonal if

$$2(m+1) \leq (q-1)(\deg(G) - 1) + q \cdot (\deg(\mathrm{Tr}_n(G)) - \deg(\mathrm{Tr}_n(G)')).$$

For the rest of this section we will consider the special case that $G(x) = H_k(x)$ where $H_k(x) := x^{q^k+1} + x$, and $n = 2k$, and $\gcd(n, p) = 1$. First we must verify the conditions on H_k in order to apply Corollary 5.2.

Lemma 5.3. *Assume q is odd, let k be a positive integer such that $\gcd(p, 2k) = 1$, and let $n = 2k$. Then (1) $\mathrm{Tr}_n(H_k)$ is separable, and (2) all roots of $\mathrm{Tr}_n(H_k)$ belong to $\mathbb{F}_{q^n}$.*

Proof. Notice that, for all $a \in \mathbb{F}_{q^n}$, it holds that

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(H_k(a)) &= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a^{q^k+1}) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) \\ &= 2(a^{q^k+1} + a^{q^{k+1}+q} + a^{q^{k+2}+q^2} + \cdots + a^{q^{2k-1}+q^{k-1}}) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a).\end{aligned}$$

Therefore:

$$\mathrm{Tr}_n(H_k)(z) = 2(z^{q^k+1} + z^{q^{k+1}+q} + z^{q^{k+2}+q^2} + \cdots + z^{q^{2k-1}+q^{k-1}}) + (z + z^q + z^{q^2} + \cdots + z^{q^{n-1}})$$

and we can see that the degree of $\mathrm{Tr}_n(H_k)(z)$ is $q^{n-1} + q^{k-1}$. Computing the derivative we have

$$\mathrm{Tr}_n(H_k)'(z) = 2z^{q^k} + 1 = 2(z + 1/2)^{q^k}.$$

Notice that $\mathrm{Tr}_n(H_k)'$ has only one root (namely $-1/2$) which has multiplicity q^k. Moreover $H_k(-1/2) = -1/4$; so $\mathrm{Tr}_n(H_k)(-1/2) = -n/4$, which is not zero because p does not divide n. Hence $\mathrm{Tr}_n(H_k)$ is separable because it is relatively prime to its derivative. This proves (1).

The number of $\mathbb{F}_{q^n}$-rational points of B_{q,H_k} is

$$N(B_{q,H_k}, q^n) = q^n + q^k$$

which is proved in [34, Thm 20]. It then follows from the degree calculation above that

$$N(B_{q,H_k}, q^n) = q \cdot \deg(\mathrm{Tr}_n(H_k)).$$

Hence all the roots of $\mathrm{Tr}_n(H_k)$ belong to $\mathbb{F}_{q^n}$. This proves (2). □

Assume then that q is odd, let k be a positive integer such that $\gcd(p, 2k) = 1$ and consider the curve B_{q,H_k} over the field $\mathbb{F}_{q^n}$ where $n := 2k$. The curve B_{q,H_k} satisfies the hypotheses of Corollary 5.2; and in addition we have shown that

$$f_{\mathscr{A}}(z) = \frac{1}{2}\mathrm{Tr}(H_k)(z) \quad \text{and} \quad f'_{\mathscr{A}}(z) = (z + 1/2)^{q^k}.$$

As a consequence we may apply Corollary 5.2 to the curves $B_{q,H_k} : y^q - y = x^{q^k+1} + x$. We get that, for any positive integer m, the associated AG code $C(D, mP_\infty)$ (with D as in Corollary 5.2) is self-orthogonal if

$$2(m+1) \leq q^n. \tag{5.1}$$

Remark 5.4. Notice that none of the pointed curves B_{q,H_k} discussed here satisfies Lemma 2 of [36] (see Remark 3.9). None of the curves B_{q,H_k} is Castle either, because the smallest element of the Weierstraß semigroup is q, and the number of (affine) rational points is not equal to q^2. Hence [36, Prop. 2] cannot be applied.

6. CURVES $C_{q,\ell}$

Let ℓ be a positive integer such that $\gcd(p,\ell)=1$. Let $C_{q^s,\ell}$ be the affine plane curve defined by the equation $y^{q^s}-y=x^\ell$. We consider the curve over $\mathbb{F}_{q^n}$.

We consider two special cases here, firstly when $s=1$ and $n=2$, and secondly for arbitrary $s>1$ and n with an extra hypothesis.

6.1. *Curves $C_{q,\ell}$.* Assume that q is odd and $2\gcd(\ell,q+1)$ divides $q+1$. Let $C_{q,\ell}$ be the affine plane curve defined by the equation $y^q-y=x^\ell$. We consider the curve over $\mathbb{F}_{q^2}$.

The following Proposition refers to the statement of Theorem 3.1.

Proposition 6.1. (1) *Let $C=C_{q,\ell}$ and $\mathbf{F}=\mathbb{F}_{q^2}$. Then C is smooth over $\mathbf{F}$ and C has only one place at infinity. The set $\mathscr{A}$ in the statement of Theorem 3.1 is equal to the set of all x-coordinates of the $\mathbb{F}_{q^2}$-rational points of C.*

(2) *Moreover, $f_{\mathscr{A}}(z)=z^{e+1}-z$, where $e:=\gcd(\ell(q-1),q^2-1)$, and the number of $\mathbb{F}_{q^2}$-rational points of C is $N(C_{q,\ell},q^2)=q\cdot(e+1)$.*

Proof. By Lemma 3.10 it holds that $C_{q,\ell}$ is smooth, it has only one place at infinity, and the genus of $\tilde{\chi}_{C_{q,\ell}}$ is $(q-1)(\ell-1)/2$. The set of $\mathbb{F}_{q^2}$-rational points of $C_{q,\ell}$ is

$$\{(a,b)\in\mathbb{F}_{q^2}\mid b^q-b=a^\ell\}$$

which implies $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a^\ell)=0$. For each a with $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a^\ell)=0$ there are q solutions for b. Then $a^\ell+a^{\ell q}=0$ which implies $a=0$ or $a^{\ell(q-1)}=-1$. If $a\neq 0$, the assumption $2\gcd(\ell,q+1)$ divides $q+1$ implies that there are e solutions for a, where $e:=\gcd(\ell(q-1),q^2-1)$. So $N(C_{q,\ell},q^2)=q(e+1)$.

Similar arguments to those given in Section 4 for $A_{n,q,\ell}$ show that the curve $C_{q,\ell}$ satisfies the hypotheses of Theorem 3.1 for $\mathbf{F}=\mathbb{F}_{q^2}$, and that the set $\mathscr{A}$ consists of the x-coordinates of the $\mathbb{F}_{q^2}$-rational points. Moreover, it is easy to check that

$$f_{\mathscr{A}}(z)=z^{e+1}-z.$$

□

Proposition 6.1 means that we can apply Corollary 3.3 to the curve $C_{q,\ell}$, and we deduce the following result:

Corollary 6.2. *Let $N := N(C_{q,\ell}, q^2)$, let $\{P_1, \ldots, P_N\}$ be the set of $\mathbb{F}_{q^2}$-rational points of $C_{q,\ell}$, and let $D = P_1 + \cdots + P_N$ be a divisor of $\tilde{\chi}_{C_{q,\ell}}$.*

Then, for any nonnegative integer m, the AG code (defined from $\tilde{\chi}_{C_{q,\ell}}$) given by $C(D, mP_\infty)$ is self-orthogonal if

$$2(m+1) \leq (q-1)(\ell-1) + q(e+1) - \mu \cdot eq$$

where $\mu := 0$ if p divides $e+1$ and $\mu := 1$ otherwise.

Remark 6.3. Notice that the derivative $f'_{\mathscr{A}}(z)$ is constant if and only if p divides $e+1$. Lemma 2 of [36] (see Remark 3.9) can only be applied if p divides $e+1$. Our result includes the case that p does not divide $e+1$.

Proposition 6.4. *(1) If $\ell < q$ the pointed curve $(\tilde{\chi}_{C_{q,\ell}}, P_\infty)$ is never a Castle curve.*

(2) If $\ell > q$ the pointed curve $(\tilde{\chi}_{C_{q,\ell}}, P_\infty)$ is a Castle curve if and only if $\gcd(\ell, q+1) = 1$.

Proof. The curve is Castle if and only if $s = e+1$ where s is the smallest nonzero element of the Weierstraß semigroup. Also note that $e = (q-1)\gcd(\ell, q+1)$.

(1) If $\ell < q$ then $s = \ell$, so the curve is Castle if and only if $e = \ell - 1$ which is impossible.

(2) If $\ell > q$ then $s = q$, so the curve is Castle if and only if $e = q-1$, which happens if and only if $\gcd(\ell, q+1) = 1$. □

Proposition 2 of [36] cannot be applied to $(\tilde{\chi}_{C_{q,\ell}}, P_\infty)$ if the curve is not Castle, however our result applies in all cases.

6.2. *Curves $C_{q^s,\ell}$.* Let s and n be positive integers such that n is a multiple of s and n/n_ℓ^s is a multiple of p, where n_ℓ^s denotes the cardinality of the cyclotomic coset of ℓ with respect to q^s, that is, the cardinality of the set $\{\ell q^{js} \bmod (q^n-1) \mid j = 0, \ldots, n-1\}$.

The key fact in this case is that $\mathrm{Tr}_{q^n/q^s}(x^\ell) = \frac{n}{n_\ell^s}(x^\ell + x^{\ell \cdot q^s} + \cdots + x^{\ell \cdot q^{(n_\ell^s - 1)s}})$, and this is always 0 because $\frac{n}{n_\ell^s} \equiv 0 \pmod{p}$. Therefore any element of $\mathbb{F}_{q^n}$ has trace equal to zero. So following same arguments as in previous subsections we have the following result.

Proposition 6.5. *Let $C = C_{q^s,\ell}$ and $\mathbf{F} = \mathbb{F}_{q^n}$. If $\frac{n}{n_\ell^s}$ is divisible by p then*

(1) C is smooth over $\mathbf{F}$ and C has only one place at infinity. The set $\mathscr{A}$ in the statement of Theorem 3.1 is equal to the set of all x-coordinates of the $\mathbb{F}_{q^n}$-rational points of C.

(2) Moreover, $\mathscr{A} = \mathbb{F}_{q^n}$ and $f_{\mathscr{A}}(z) = z^{q^n} - z$, and the number of $\mathbb{F}_{q^n}$-rational points of C is $N(C_{q^s,\ell}, q^n) = q^{n+s}$.

Hence, applying Corollary 3.3 we have that the code over $\mathbb{F}_{q^n}$ given by $C(D, mP_\infty)$ (with D as in Corollary 3.2) is self-orthogonal if

$$2(m+1) \leq (q-1)(\ell-1).$$

We note that these codes are of Type I, that is, the derivative of $f_{\mathscr{A}}(z)$ is constant.

7. Application to quantum codes

In this section we will use the results of the previous sections to construct new quantum error-correcting codes. We point out that the number of rational points on our curves is always greater than the field size. We will show that our curves beat the Gilbert-Varshamov bound.

Recall that the Hermitian inner product of any two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_N)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_N)$ in the vector space $\mathbb{F}_{q^2}^N$ is defined as $\mathbf{x} \cdot_h \mathbf{y} = \sum x_i y_i^q$ and the Euclidean inner product of $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^N$ as $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$. Given a linear code $\mathscr{C}$ in $\mathbb{F}_{q^2}^N$ (respectively, $\mathbb{F}_q^N$), the Hermitian (respectively, Euclidean) dual space is denoted by $\mathscr{C}^{\perp_h}$ (respectively, $\mathscr{C}^{\perp}$).

In [10] the following key theorem is stated and in [29] is generalized over any field.

Theorem 7.1. *The following two statements hold.*

(1) Let $\mathscr{C}$ be a linear $[N,k,d]$ error-correcting code over $\mathbb{F}_q$ such that $\mathscr{C} \subseteq \mathscr{C}^{\perp}$. Then, there exists an $[[N, N-2k, \geq d^{\perp}]]_q$ stabilizer quantum code, where $d^{\perp}$ denotes the minimum distance of $\mathscr{C}^{\perp}$. If the minimum weight of $\mathscr{C}^{\perp} \setminus \mathscr{C}$ is equal to $d^{\perp}$, then the stabilizer code is pure and has minimum distance $d^{\perp}$.

(2) Let $\mathscr{C}$ be a linear $[N,k,d]$ error-correcting code over $\mathbb{F}_{q^2}$ such that $\mathscr{C} \subseteq \mathscr{C}^{\perp_h}$. Then, there exists an $[[N, N-2k, \geq d^{\perp_h}]]_q$ stabilizer quantum code, where $d^{\perp_h}$ denotes the minimum distance of $\mathscr{C}^{\perp_h}$. If the minimum weight of $\mathscr{C}^{\perp_h} \setminus \mathscr{C}$ is equal to $d^{\perp_h}$, then the stabilizer code is pure and has minimum distance $d^{\perp_h}$.

Recall that the stabilizer quantum code associated to $\mathscr{C}$, as in the previous theorem, is pure if the minimum distance of $\mathscr{C}^{\perp}$ (or $\mathscr{C}^{\perp_h}$) coincides with the minimum Hamming weight of $\mathscr{C}^{\perp} \setminus \mathscr{C}$ (or $\mathscr{C}^{\perp_h} \setminus \mathscr{C}$).

Corollary 7.2. *The following statements hold:*

(1) *Let $\mathscr{C}$ be a linear $[N,k,d]$ error-correcting code over $\mathbb{F}_q$ such that $\mathscr{C} \subseteq \mathscr{C}^{\perp}$. If $d > k+1$ then there exists an $[[N, N-2k, \geq d^{\perp}]]_q$ stabilizer quantum code which is pure.*

(2) *Let $\mathscr{C}$ be a linear $[N,k,d]$ error-correcting code over $\mathbb{F}_{q^2}$ such that $\mathscr{C} \subseteq \mathscr{C}^{\perp_h}$. If $d > k+1$ then there exists an $[[N, N-2k, \geq d^{\perp_h}]]_q$ stabilizer quantum code which is pure.*

Proof. The result follows from Theorem 7.1 and the fact $d^{\perp} \leq k+1$ (resp., $d^{\perp_h} \leq k+1$) by the Singleton bound.

□

7.1. *Euclidean Inner Product.* Now we are going to consider codes within the framework of Theorem 3.1, that is, codes $C(D,G)$ associated to curves with equation of the type $F(y) = H(x)$ such that $D = P_1 + \cdots + P_N$ and $G = mP_\infty$, with $2g-2 < m < N$ and $P_1, \ldots, P_N, P_\infty$ being rational points of the curve. The parameters of $C(D,G)$ are $[N, m-g+1, \geq N-m]$ (see [27]).

Moreover the dual code $C(D,G)^\perp = C(D, (2g-2+\deg(D)-\deg(M))P_\infty + M - G)$ has parameters

$$[N, N-m+g-1, \geq m-2g+2] \tag{7.1}$$

Assuming self-orthogonality, Theorem 7.1 provides a quantum code with parameters

$$[[N, N-2(m-g+1), \geq m-2g+2]]. \tag{7.2}$$

Notice that, by Corollary 7.2, this code is pure if

$$N > 2m-g+2. \tag{7.3}$$

We notice here that all the forthcoming examples satisfy the above condition (7.3) and, therefore, they are pure.

With the same philosophy of the classical Gilbert-Varshamov bound, a sufficient condition for the existence of pure stabilizer codes with parameters $[[N,k,d]]_q$ is given by Feng and Ma in [14]. Assuming $N > k \geq 2$, $d \geq 2$ and $N \equiv k \pmod 2$, this condition reads

$$\sum_{i=1}^{d-1} (q^2-1)^{i-1} \binom{N}{i} < \frac{q^{N-k+2}-1}{q^2-1}. \tag{7.4}$$

In case N odd and $k=1$, the condition is

$$q^N + 1 > \sum_{i=1}^{d-1} \binom{N}{i} [q(q^2-1)^{i-1} + (-1)^{i+1}(q+1)^{i-1}]$$

and there exists a similar formula for the case N even and $k=0$.

We will use this bound as a measure of goodness of our codes. We will only consider codes exceeding this bound, i.e., cases in which the parameters q, N, k and d satisfy

$$\sum_{i=1}^{d-1} (q^2-1)^{i-1} \binom{N}{i} \geq \frac{q^{N-k+2}-1}{q^2-1}. \tag{7.5}$$

We will say that an $[[N,k,d]]_q$ quantum code is GV if it fulfills this inequality.

7.1.1. *Curves $A_{n,q,\ell}$.* Let ℓ and n be positive integers (not both equal to 1) such that $\gcd(p,\ell) = 1$ and let $A_{n,q,\ell}$ be the curve defined in Section 4. From Corollary 4.2 and (7.2) it is deduced the following result:

Theorem 7.3. *Let $C(D,mP_\infty)$ be the code coming from the curve $\tilde{\chi}_{A_{n,q,\ell}}$ over $\mathbb{F}_{q^n}$ as in Section 4. Assume that*

$$2(m+1) \leq (q^{n-1}-1)(\ell-1)+q^{n-1}(\mu\cdot\gcd(\ell(q-1),q^n-1)+1),$$

where $\mu := 1$ if p divides $\gcd(\ell(q-1),q^n-1)+1$ and $\mu := 0$ otherwise. Then there exists a quantum code with parameters

$$[[N, N-2m+2g-2, \geq m-2g+2]]_{q^n},$$

where $N = N(A_{n,q,\ell},q^n) = q^{n-1}\cdot(e+1)$, $g = (q^{n-1}-1)(\ell-1)/2$ and $e := \gcd(\ell(q-1),q^n-1)$.

Notice that, under the hypotheses of the above theorem, $2g-2 < m < N$ only if $\mu = 1$, and these cases satisfy the hypotheses of [36, Lemma 2] (they correspond to Type I of Remark 3.9).

First we give an example where $\mu = 0$.

Example 7.4. *Consider the curve $A_{2,9,8}$, with equation $y^9+2x^8z+yz^8=0$. For $m=9<2g-2=54$, the quantum code obtained from Theorem 7.3 has parameters $[[153,147,3]]_{3^4}$. The dimension of $C(D,G)$ and the distance of its dual have been computed using MAGMA.*

Next we give an example where $\mu = 1$.

Example 7.5. *Consider the curve $A_{2,9,10}$, with equation $y^9z+2x^{10}+yz^9=0$. For $j=0,\ldots,381-194$ we have quantum codes with parameters*

$$[[729, 413-2j, 123+j]]_{3^4},$$

which correspond to $194 \leq m \leq 381$. By (7.3) these codes are pure. Moreover they are GV.

7.1.2. *Curves $B_{q,x^{q^k+1}+x}$.* From Section 5 and Eq. (7.2) we get the following:

Theorem 7.6. *Asume that $\gcd(p,2k)=1$ and $n=2k$. Consider the curve B_{q,H_k}, with equation $y^q-y=H_k(x)=x^{q^k+1}+x$, and the code $C(D,mP_\infty)$ coming from $\tilde{\chi}_{B_{q,H_k}}$ (over $\mathbb{F}_{q^n}$), as defined in Section 5. Assume that*

$$2(m+1) \leq q^n.$$

Then there exists a quantum code with parameters

$$[[q^n+q^k, q^n+q^k-2m+2g-2, \geq m-(q-1)q^k+2]]_{q^n}.$$

Now we include some examples of quantum codes coming from the above theorem.

Example 7.7. *Consider $q = 3$, $n = 8$, $k = 4$. For $j = 0, \ldots, 3279 - 538$ we have quantum codes with parameters*

$$[[6642, 5726 - 2j, 378 + j]]_{3^8},$$

which correspond to $538 \leq m \leq 3279$. By (7.3) these codes are pure. Moreover they are GV.

Example 7.8. *Consider $q = 5$, $n = 6$, $k = 3$. For $j = 0, \ldots, 7811 - 1955$ we have quantum codes with parameters*

$$[[15750, 12338 - 2j, 1457 + j]]_{5^6},$$

which correspond to $1955 \leq m \leq 7811$. By (7.3) these codes are pure. Moreover they are GV.

7.1.3. *Curves $C_{q,\ell}$.* From Corollary 6.2 and Eq. (7.2) we obtain the following result concerning codes coming from curves in the family given in Section 6.1.

Theorem 7.9. *Consider the code $C(D, mP_\infty)$ coming from the curve $\tilde{\chi}_{C_{q,\ell}}$ over $\mathbb{F}_{q^2}$ under the assumptions and hypotheses of Corollary 6.2. If*

$$2(m+1) \leq (q-1)(\ell-1) + q(e+1) - \mu \cdot qe,$$

where $\mu = 0$ if p divides $e+1$ and $\mu = 1$ otherwise, then there exists a quantum code with parameters

$$[[N, N - 2m + 2g - 2, \geq m - (q-1)(\ell-1) + 2]]_q,$$

where $N = N(C_{q,\ell}, q^2) = q(e+1)$ and $e = \gcd(\ell(q-1), q^2 - 1)$.

If $\mu = 0$ then the value for m is less than $2g-2$ so we have to compute the dimension and the minimum distance using MAGMA.

Example 7.10. *Consider $p = 3$, $n = 4$, $q = p^2$ and $\ell = 5$. We choose $m = 9$ and so we consider the code $\mathscr{C} = C(D, 9P_\infty)$. Using MAGMA we compute that $N = 369$ (thus the curve is maximal) and $\dim(\mathscr{C}) = 3$ and $d(\mathscr{C}^\perp) = 3$, so there exists a quantum code with parameters $[[369, 363, \geq 3]]_{3^4}$.*

We present now an example where $\mu = 1$; notice that this satisfies the hypothesis of [36, Lemma 2].

Example 7.11. *Consider $p = 3$, $n = 6$, $q = p^3$ and $\ell = 7$. For $j = 0, \ldots, 2508 - 313$, there exist quantum codes with parameters*

$$[[4941, 4469 - 2j, 159 + j]]_{3^6}$$

which correspond to $313 \leq m \leq 2508$. By (7.3) these codes are pure. Moreover they are GV.

7.2. *Hermitian Inner Product.* Let $\mathbf{F} = \mathbb{F}_{q^2}$, q being a power of a prime number. Within this framework, the results of Section 3 can be applied to obtain quantum codes by using Hermitian inner product instead of Euclidean inner product.

Notice that $\mathbf{x} \cdot_h \mathbf{y} = 0$ if and only if $\mathbf{x} \cdot \mathbf{y}^q = 0$. For any linear code $\mathscr{C}$ we have therefore that $\mathscr{C} \subseteq \mathscr{C}^{\perp_h}$ if and only if $\mathscr{C}^q \subseteq \mathscr{C}^{\perp}$. For AG codes we have that $C(D,G)^q \subseteq C(D,qG)$. Hence if $C(D,qG) \subseteq C(D,G)^{\perp}$ then

$$C(D,G)^q \subseteq C(D,qG) \subseteq C(D,G)^{\perp}$$

and, therefore, $C(D,G) \subseteq C(D,G)^{\perp_h}$. So we can trivially extend previous results (Theorem 3.1 and Corollaries 3.2, 3.3, and 3.6) using the latter observation.

Theorem 7.12. *Let* $\mathbf{F}$ *be as before and let C, g,* $\mathscr{A}$*,* $f'_{\mathscr{A}}$*, M, D and G be as in Theorem 3.1. Then:*

(a) *If* $(q+1)G \leq (2g-2+\deg(D)-\deg(M))P_\infty + M$ *then* $C(D,G) \subseteq C(D,G)^{\perp_h}$.
(b) *If* $G = mP_\infty$*, with* $m \in \mathbb{N}$*, and* $(q+1)m \leq 2g-2+\deg(D)-\deg(M)$ *then* $C(D,G) \subseteq C(D,G)^{\perp_h}$.
(c) *If* $G = mP_\infty$*, with* $m \in \mathbb{N}$*, the curve C has an equation of the type* $F(y) = G(x)$*, where* F, G *are polynomials with coefficients in* $\mathbf{F}$*, and*

$$(q+1)m \leq 2g-2+\deg(D)-\deg(f'_{\mathscr{A}})\deg(F) \text{ or } (q+1)m \leq 2g-2+\deg(F),$$

then $C(D,G) \subseteq C(D,G)^{\perp_h}$.

Notice that the values m satisfying parts (b) and (c) of Theorem 7.12 are not bigger than $2g-2$. Hence, in practice, we are forced to compute the minimum distance of associated quantum codes with MAGMA. Finally we provide two examples applying Theorem 7.12.

Example 7.13. *Applying Theorem 7.12 to the code of Example 7.4 we can produce a quantum code with parameters* $[[153,147,3]]_{3^2}$*. By* (7.3) *these codes are pure. Moreover they are GV.*

Example 7.14. *Similarly, considering the curve* $C_{9,5}$ *from Section 6 (with equation* $y^9 + 2x^5z^4 + 2yz^8 = 0$*), with* $q = 9$*,* $n = 4$*,* $\ell = 5$*, for* $m = 9 < 2g-2 = 30$ *we have the quantum code* $[[369,363,3]]_{3^2}$*. By* (7.3) *these codes are pure. Moreover they are GV.*

7.3. *Comparison with other papers.* As we already mentioned in this paper, we obtain new results for any curve where the divisor M in Theorem 3.1 is not equal to zero. All the examples in [36] are the special case of our results when $M = 0$.

Jin and Xing have the following interesting result in [28]: If

$$deg(G) < \frac{N}{2}(1 - \frac{1}{N} + log_q(1 - \frac{1}{q}) - log_q(2)).$$

and q is even then there exists an equivalent code to $C(D,G)$ over $\mathbb{F}_q$ which is Euclidean Self-Orthogonal.

We compare some curves and codes with this result in the case $G = mP_\infty$. We now present some examples of curves that satisfy the hypotheses of Theorem 3.1 and where the divisor M is nonzero (checked with Magma).

Example 7.15. *Here $q = 2$ and $n = 6$. The curve is defined by $F(y) = H(x)$ where*

$F(y) = y^{16} + y^4 + y$

$H(x) = x^{17} + x^{13} + x^6 + x^4 + x^3 + x + 1.$

The Jin-Xing bound implies that there exists a self-orthogonal code (from some curve) for $m \leq 66.27$, and our bound in Theorem 3.1 implies that there exists a self-orthogonal code (from this curve) for $m \leq 135.5$.

There is something of additional interest in the previous example; our bound is tight. We confirmed with Magma that the AG code is self-orthogonal for $m \leq 135$ and NOT self-orthogonal for $m = 136$. This shows that, in some sense, our bound cannot be improved.

Example 7.16. *$q = 2$, $n = 7$*

$F(y) = y^8 + y^4 + y$

$H(x) = x^{29} + x^{17} + x^{15} + x^{13} + x^{12} + x^{11} + x^9 + x^4 + x + 1,$

See Table 1 for the range of values for m.

Example 7.17. *$q = 2$, $n = 8$*

$F(y) = y^{64} + y^{16} + y^4 + y$

$H(x) = x^{67} + x^{63} + x^{61} + x^{58} + x^{56} + x^{54} + x^{53} + x^{52} + x^{50} + x^{49} + x^{48} + x^{46} + x^{45} + x^{44} + x^{39} + x^{37} + x^{36} + x^{35} + x^{34} + x^{33} + x^{31} + x^{29} + x^{23} + x^{20} + x^{16} + x^{15} + x^{14} + x^{10} + x^8 + x^4 + x^3 + 1,$

See Table 1 for the range of values for m.

	[28]	This paper
Example 3.5	nothing for q odd	$17 \leq m \leq 129$
Example 7.15	$m \leq 66$	$m \leq 135$
Example 7.16	$m \leq 78$	$m \leq 101$
Example 7.17	$m \leq 1902$	$m \leq 2398$
Example 7.7	nothing for q odd	$m \leq 3279$
Example 7.8	nothing for q odd	$m \leq 7811$
Example 7.10	nothing for q odd	$m \leq 2508$

Table 1

Any example with q odd will improve on [28] because the bound in that paper for Euclidean codes is not valid when q is odd. From our infinite families we list three examples

in the table. They do not appear in [36] because the divisor M is nonzero, as we proved in the earlier sections.

Acknowledgements We thank J.I. Farrán and C. Munuera for helpful conversations.

REFERENCES

[1] Abhyankar, S.S.: Irreducibility criterion for germs of analytic functions of two complex variables. Adv. Math. **74**, 190–257 (1989)
[2] Abhyankar, S.S.: Algebraic Geometry for scientists and engineers. Mathematical Surveys and Monographs, Am. Math. Soc. (1990)
[3] Ashikhmin, A., Barg, A., Knill, E., Litsyn, S.: Quantum error-detection I: Statement of the problem. IEEE Trans. Inf. Theory **46**, 778–788 (2000)
[4] Ashikhmin, A., Barg, A., Knill, E., Litsyn, S.: Quantum error-detection II: Bounds. IEEE Trans. Inf. Theory **46**, 789–800 (2000)
[5] Ashikhmin, A., Knill, E.: Non-binary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**, 3065–3072 (2001)
[6] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
[7] Bierbrauer, J., Edel, Y.: Quantum twisted codes. J. Comb. Designs **8**, 174–188 (2000)
[8] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **76**, 405–409 (1997)
[9] Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**, 1098–1105 (1996)
[10] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inform. Theory **44**(4), 1369–1387 (1998)
[11] Campillo, A., Farrán, J.I.: Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models. Finite Fields Appl. **6**, 71–92 (2000)
[12] Duursma, I.M.: Algebraic geometry codes: general theory. In: Advances in Algebraic Geometry Codes, Series of Coding Theory and Cryptology, vol. 5. World Scientific, Singapore (2008)
[13] Feng, K. Quantum error correcting codes. In Coding Theory and Cryptology, Word Scientific, 2002, 91–142.
[14] Feng, K., Ma, Z.: A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. IEEE Trans. Inf. Theory **50**, 3323–3325 (2004)
[15] Galindo, C., Geil, O., Hernando, F., Ruano, D.: On the distance of stabilizer quantum codes from J-affine variety codes. Quantum Inf. Process **16**, 111 (2017)
[16] Galindo, C., Hernando, F., Matsumoto, R.: Quasi-Cyclic Construction of Quantum Codes. Finite Fields Appl. **52**, 261–280 (2018)
[17] Galindo, C., Hernando, F., Ruano, D.: Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. Quantum Inf. Process **14**, 3211–3231 (2015)
[18] Galindo, C., Hernando, F., Ruano, D.: Classical and Quantum Evaluation Codes at the Trace Roots. IEEE Transaction on Information Theory **16**, 2593–2602 (2019)
[19] Garcia, A.: On AG codes and Artin-Schreier extensions. Comm. Alg. **20**(12), 3683–3689 (1992)
[20] Goppa, V.D.: Geometry and codes. Mathematics and its Applications 24, Kluwer, Dordrecht (1991)
[21] Goppa, V.D.: Codes associated with divisors. Problems Inform. Transmission **13**, 22–26 (1977)
[22] Gottesman, D.: A class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A **54**, 1862–1868 (1996)

[23] Grassl, M., Rötteler, M. Quantum BCH codes. In: Proc. X Int. Symp. Theor. Elec. Eng. Germany pp. 207–212 (1999)

[24] Grassl, M., Beth, T., Rötteler, M.: On optimal quantum codes. Int. J. Quantum Inform. **2**, 757–775 (2004)

[25] He, X., Xu, L., Chen. H.: New q-ary quantum MDS codes with distances bigger than $q/2$. Quantum Inf. Process. **15**(7), 2745–2758 (2016).

[26] Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic curves over a finite field. Princeton Series in Applied Mathematics, Princeton (2008)

[27] Høholdt, T., van Lint, J., Pellikaan, R.: Algebraic geometry codes. In: Handbook of Coding Theory, vol. 1, pp. 871–961 (1998)

[28] Jin, L., Xing, C.: Euclidean and Hermitian Self-Orthogonal Algebraic Geometry Codes and Their Application to Quantum Codes. IEEE Trans. Inform. Theory **58**, 5484–4489 (2012)

[29] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inform. Theory **52**, 4892–4924 (2006)

[30] La Guardia, G.G.: Construction of new families of nonbinary quantum BCH codes. Phys. Rev. A **80**, 042331 (2009)

[31] La Guardia, G.G.: On the construction of nonbinary quantum BCH codes. IEEE Trans. Inform. Theory **60**, 1528–1535 (2014)

[32] Lidl, R., Niederreiter, H.: Introduction to finite Fields and their applications. Cambridge University Press, Cambridge (1994)

[33] Matsumoto, R., Uyematsu, T.: Constructing quantum error correcting codes for p^m state systems from classical error correcting codes. IEICE Trans. Fund. **E83-A**, 1878–1883 (2000)

[34] McGuire, G., Yılmaz, E.S.: Divisibility of L-Polynomials for a Family of Artin-Schreier Curves. J. Pure Appl. Alg. **223**(8), 3341–3358 (2019)

[35] Munuera, C., Sepúlveda, A., Torres, F.: Castle curves and codes, Adv. Math. Commun. **3**, 399–408 (2009)

[36] Munuera, C., Tenório, W., Torres, F.: Quantum error-correcting codes from algebraic geometry codes of Castle Type. Quant. Inf. Process. **15**, 4071–4088 (2016)

[37] Pellikaan, R., Shen, B.Z., van Wee, G. J. M.: Which linear codes are Algebraic-Geometric. IEEE Trans. Inform. Theory **37**, 583–602 (1991)

[38] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In: Proc. 35th ann. symp. found. comp. sc. IEEE Comp. Soc. Press, pp. 124–134 (1994)

[39] Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52** R2493 (1995).

[40] Steane, A.M.: Multiple-particle interference and quantum error correction. Proc. R. Soc. Lond. Ser. A **452**, 2551–2557 (1996)

[41] Stichtenoth, H.: Algebraic Function Fields and Codes. Springer-Verlag, Berlin-Heidelberg (2009)

[42] Tsfasman, M.A., Vlăduţ, S.G., Zink, T.: Modular Curves, Shimura Curves and AG Codes, better than Varshamov-Gilbert bound. Math. Nachr. **109**, 21–28 (1982)

UNIVERSITAT JAUME I (UJI), CAMPUS DE RIU SEC, INSTITUT UNIVERSITARI DE MATEMÀTIQUES I APLICACIONS DE CASTELLÓ, 12071 CASTELLÓN DE LA PLANA, SPAIN.

Email address: carrillf@uji.es

UCD SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY COLLEGE DUBLIN, DUBLIN 4 (IRELAND).

Email address: gary.mcguire@ucd.ie

INSTITUTO UNIVERSITARIO DE MATEMÁTICA PURA Y APLICADA, UNIVERSIDAD POLITÉCNICA DE VALENCIA, CAMINO DE VERA S/N, 46022 VALENCIA (SPAIN).

Email address: framonde@mat.upv.es

UNIVERSITAT JAUME I (UJI), CAMPUS DE RIU SEC, INSTITUT UNIVERSITARI DE MATEMÀTIQUES I APLICACIONS DE CASTELLÓ , 12071 CASTELLÓN DE LA PLANA, SPAIN.

Email address: moyano@uji.es