QUANTUM CODES FROM AFFINE VARIETY CODES AND THEIR SUBFIELD-SUBCODES

C. GALINDO AND F. HERNANDO

Abstract. We use affine variety codes and their subfield-subcodes to obtain quantum stabilizer codes via the CSS code construction. With this procedure we get codes with good parameters, some of them exceeding the CSS quantum Gilbert-Varshamov bound given by Feng and Ma.

Introduction

Shor's algorithm [30] for factoring integers opens the possibility of breaking some cryptographical systems. This is a clear example of the increasing interest in computers based on the principles of quantum mechanics. The fact that arbitrary quantum states cannot be replicated seemed to suggest that error correction could not be used on quantum mechanical systems [34]. However this is not the case as showed in [31]. Binary stabilizer codes are the most studied quantum error-correcting codes. There is an extensive literature on them, for simplicity we only cite [6, 16] as seminal works.

In this paper, we are interested in general stabilizer codes defined over finite fields and constructed by using a class of linear error-correcting codes called affine variety codes. Let $q = p^r$ be a positive integer power of a prime number p and $\mathbb{C}^q$ the q-dimensional complex vector space representing the states of a quantum mechanical system. Let $|x\rangle$ be the vectors of a distinguished orthonormal basis of $\mathbb{C}^q$, where $x \in \mathbb{F}_q$, $\mathbb{F}_q$ being the finite field with q elements. By definition, a *quantum error-correcting code* is a s-dimensional subspace of $\mathbb{C}^{q^n} = \mathbb{C}^q \otimes \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. Let $a, b \in \mathbb{F}_q$, then the unitary operators on $\mathbb{C}^q$, $X(a)|x\rangle = |x+a\rangle$ and $Z(b)|x\rangle = \beta^{\mathrm{tr}(bx)}|x\rangle$, where $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map and β a primitive pth root of unity, allow us to consider the set $\varepsilon = \{X(a)Z(b)|a, b \in \mathbb{F}_q\}$ of error operators. For $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$, define $X(\mathbf{a}) := X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{a})$ analogously and write $\varepsilon_n = \{X(\mathbf{a})Z(\mathbf{b})|\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ a nice error basis on the complex space $\mathbb{C}^{q^n}$. A *stabilizer code* C is a non-zero subspace of $\mathbb{C}^{q^n}$ such that $C = \cap_{H \in \Delta}\{\mathbf{v} \in \mathbb{C}^{q^n} | H\mathbf{v} = \mathbf{v}\}$, for some subgroup Δ of the group generated by ε_n, G_n.

A stabilizer code C has minimum distance d if, and only if, all errors in G_n with weight less than d can be detected or have no effect on C but some error of weight d cannot be detected, where the weight is the number of nonidentity tensor components. We say that a code C as above is an $((n, s, d))_q$-code. When the code is an $((n, q^k, d))_q$-code, we simply say that it is an $[[n, k, d]]_q$-code. C is said to be *pure to* t whenever the group Δ does not contain non-scalar matrices whose weight is less than t and C is called *pure* whenever it is pure to its minimum distance.

As in the binary case, classical codes can be used to provide quantum codes. The following result gives a first link between them and it can be found in [22, Corollary 19] (see also [6, 5, 2]).

Supported by Spain Ministry of Economy MTM2012-36917-C03-03 and University Jaume I: PB1-1B2012-04. The authors would like to thank three anonymous reviewers for their helpful comments.

Proposition 1. *Assume the existence of an $[n, k, d]$ linear code E over $\mathbb{F}_{q^2}$ such that the dual code of E, $E^{\perp_1}$, with respect to the Hermitian inner product, satisfies $E^{\perp_1} \subseteq E$. Then, there exists an $[[n, 2k-n, \geq d]]_q$-quantum code over $\mathbb{F}_q$ which is pure to d.*

The Hermitian inner product of two vectors $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_{q^2}^n$ is defined as $\mathbf{a} \cdot \mathbf{b}^q$, where $\cdot$ is the standard Euclidean inner product and $\mathbf{b}^q = (b_1^q, b_2^q, \ldots, b_n^q)$ whenever $\mathbf{b} = (b_1, b_2, \ldots, b_n)$. We prefer to use the Euclidean inner product to provide quantum codes. The symbol $\perp$ is used to represent dual spaces with respect to that inner product. So, in this paper we use the so-called CSS code construction after the papers [7] and [32]. We summarize the idea behind it in the next two results, which can be found as Lemma 20 and Corollary 21 in [22].

Theorem 1. *Let C_1 and C_2 be two linear error-correcting block codes with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$ over the field $\mathbb{F}_q$ and such that $C_2^{\perp} \subseteq C_1$. Then, there exists an $[[n, k_1 + k_2 - n, d]]_q$ stabilizer code with minimum distance*

$$d = \min\left\{\mathrm{wt}(c) | c \in (C_1 \setminus C_2^{\perp}) \cup (C_2 \setminus C_1^{\perp})\right\},$$

which is pure to $\min\{d_1, d_2\}$.

For an explanation of how to construct the codes, we refer to [22, Theorem 13] where the additive code $C_1^{\perp} \times C_2^{\perp}$ is used.

Corollary 1. *Let C be a linear $[n, k, d]$ error-correcting block code over $\mathbb{F}_q$ such that $C^{\perp} \subseteq C$. Then, there exists an $[[n, 2k-n, \geq d]]_q$ stabilizer code which is pure to d.*

Quantum codes admit bounds on their parameters as the quantum singleton or, when they are pure, the Hamming bound [28, 3, 17, 12, 22], which give necessary conditions for the existence of arbitrary or pure quantum codes. With the same philosophy of the classical Gilbert-Varshamov bound, a sufficient condition for the existence of pure stabilizer codes is given by Feng and Ma in [12].

Literature contains many quantum codes derived from classical codes. We only cite [5, 22] and other recent papers based on BCH and quasi-cyclic codes [1, 18, 21, 23, 24]. In this paper, we consider affine variety codes to obtain stabilizer codes through the CSS code construction. We use Corollary 1 for this purpose. The direct application of this procedure yields, in general, codes over fields which can be large. Subfield-subcodes [8, 33, 19, 20] are used to decrease them and we consider this type of codes for providing stabilizer codes with good parameters. Our goal consists of finding suitable affine variety codes over a field $\mathbb{F}_{p^r}$ that produce stabilizer codes over $\mathbb{F}_{p^s}$ for some s that divides r. In this way, we get several examples of stabilizer codes improving some of those given in [9] and [24]. In addition, we also provide some stabilizer codes exceeding the Gilbert-Varshamov bound, i.e., they satisfy the opposite inequality in the above mentioned Gilbert-Varshamov sufficient condition.

It is also worth mentioning that affine variety codes are, in some cases, a particular case of multivariable abelian codes. These codes have been studied in [26], where for the case $q = 4$, self-orthogonal and self-dual codes with respect to the trace inner product are characterized.

Our manuscript is structured as follows. Section 1 introduces affine variety codes over a finite field $\mathbb{F}_{p^r}$, where p is a prime number and r a positive integer. The codes are obtained by evaluating polynomials in several variables belonging to vector spaces generated by monomials whose exponents are in some subsets U of the cartesian product

$$\{0, 1, \ldots, N_1 - 1\} \times \{0, 1, \ldots, N_2 - 1\} \times \cdots \times \{0, 1, \ldots, N_m - 1\},$$

where the integer N_i divides $p^r - 1$ for all i, $1 \leq i \leq m$. We also devote Section 1 to show that good choices of sets U give rise to stabilizer codes over $\mathbb{F}_{p^r}$. However, the ground field of these codes is, in general, large. To reduce the size of the field, in Section 2 we introduce and study subfield-subcodes of our affine variety codes providing, in Theorem 3, a basis for the vector space of polynomials associated with affine variety codes but evaluating to a subfield $\mathbb{F}_{p^s}$ of $\mathbb{F}_{p^r}$. Dual codes of the above mentioned subfield-subcodes are treated in Section 3. They are useful for proving our main result, Theorem 6, which gives conditions on the above sets U for obtaining good stabilizer codes and their parameters. Finally, Section 4 shows parameters of stabilizer codes constructed with our procedure. These codes improve some of the quantum codes included in [9] and [24, Tables I and II], and several of them exceed the Gilbert-Varshamov bound.

1. Affine variety codes

We devote this section to introduce the class of classical error-correcting codes that we will use to yield stabilizer codes via the CSS code construction. Consider a finite field $\mathbb{F}_{p^r}$ where r is a positive integer. Set $\mathbb{F}_{p^r}[X_1, X_2, \ldots, X_m]$ the ring of polynomials in m variables over the field $\mathbb{F}_{p^r}$ and pick m positive integer numbers $N_1, N_2, \ldots, N_m$ such that $N_i \mid p^r - 1$ for $i = 1, 2, \ldots, m$. Consider the ideal of $\mathbb{F}_{p^r}[X_1, X_2, \ldots, X_m]$ generated by the set of polynomials $\{X_1^{N_1} - 1, X_2^{N_2} - 1, \ldots, X_m^{N_m} - 1\}$, which will be denoted by I. Let $Z(I)$ be the set of zeroes of I, its cardinality is $n := \mathrm{card}(Z(I))$, and we set $Z(I) = \{P_1, P_2, \ldots, P_n\}$. Now, write $R := \mathbb{F}_{p^r}[X_1, X_2, \ldots, X_m]/I$ and consider the evaluation map $\mathrm{ev} : R \to \mathbb{F}_{p^r}^n$ which maps any function $f \in R$ to $\mathrm{ev}(f) = (f(P_1), f(P_2), \ldots, f(P_n))$, where f also denotes any representative of its class.

The family of codes that we are going to define will be determined by certain linear subspaces of R. Since the polynomials $X_i^{N_i} - 1$ have no multiple roots, our codes are of semi-simple type [27].

It is worthwhile to mention that $G = \{X_1^{N_1} - 1, X_2^{N_2} - 1, \ldots, X^{N_m} - 1\}$ is a Gröbner basis of the ideal I with respect to (say, some fixed) lexicographical ordering. Hence, we can choose a *canonical representative* of each class given by a polynomial f which will be its reduction module G. Frequently, we will use the same notation for expressing a class in R and its canonical representative. The following result will be useful.

Proposition 2. *The above introduced evaluation map,* ev*, is an isomorphism of $\mathbb{F}_{p^r}$-vector spaces.*

Proof. It follows from the fact that R and $\mathbb{F}_{p^r}^n$ have the same cardinality and the evaluation map is surjective. □

Throughout this paper $\mathcal{H}$ denotes the hypercube

$$\mathcal{H} := \{0, 1, \ldots, N_1 - 1\} \times \{0, 1, \ldots, N_2 - 1\} \times \cdots \times \{0, 1, \ldots, N_m - 1\}$$

and our codes are defined by suitable subsets U of $\mathcal{H}$. Each U gives rise to the set $\{X_1^{u_1} X_2^{u_2} \cdots X_m^{u_m} | (u_1, u_2, \ldots, u_m) \in U\}$ of monomials in $\mathbb{F}_{p^r}[X_1, X_2, \ldots, X_m]$. This set provides elements in R which generate a vector space over $\mathbb{F}_{p^r}$ that is denoted by $\mathbb{F}_{p^r}^U$. In particular $R = \mathbb{F}_{p^r}^{\mathcal{H}}$ as vector spaces. Now we introduce the concept of affine variety codes. For a more general definition see [13] or [14].

Definition 1. *Let U be a set as above. The image of the restriction of the evaluation map* ev *to $\mathbb{F}_{p^r}^U$ is denoted by C_U and constitutes the affine variety code associated to U over $\mathbb{F}_{p^r}$.*

As a consequence of the previous proposition and with the above notation for the set $Z(I)$, it holds that the restriction map of ev to $\mathbb{F}_{p^r}^U$,

$$\mathrm{ev}|_{\mathbb{F}_{p^r}^U} : \mathbb{F}_{p^r}^U \to \mathbb{F}_{p^r}^n, \quad f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)),$$

is injective and therefore $\dim(C_U) = \mathrm{card}(U)$.

Consider an element $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathcal{H}$ and set $\hat{\mathbf{u}} \in \mathcal{H}$ the element $\hat{\mathbf{u}} := (\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_n)$ defined by $\hat{u}_i = 0$ if $u_i = 0$ and $\hat{u}_i = N_i - u_i$ otherwise. The next result generalizes a similar result for toric codes. It can be found in [4] and [29].

Proposition 3. *Let C_U be the affine variety code defined by $U \subset \mathcal{H}$, then $C_U^\perp$ is the affine variety code defined by $U^\perp = \mathcal{H} \setminus \{\hat{\mathbf{u}} | \mathbf{u} \in U\}$.*

The following result is useful for obtaining stabilizer (quantum) codes.

Theorem 2. *With the above notations, the inclusion $C_U \subset C_U^\perp$ happens if, and only if, $\hat{\mathbf{u}} \notin U$ for all $\mathbf{u} \in U$.*

Proof. Proposition 3 shows that the code $C_U^\perp$ is the evaluation by ev of $\mathbb{F}_{p^r}^{U^\perp}$, where $U^\perp = \mathcal{H} \setminus \{\hat{\mathbf{u}} | \mathbf{u} \in U\}$, hence $U \subset U^\perp$ if and only if $\hat{\mathbf{u}} \notin U$ for all $\mathbf{u} \in U$, what concludes the proof. □

By using the CSS code construction, one can deduce the following result.

Corollary 2. *Let $N_1, N_2, \ldots, N_m$ be positive integers such that N_i divides $p^r - 1$ for all index i, p being a prime number and r a positive integer. Let U be a nonempty subset of the hypercube $\mathcal{H}$ satisfying that $\hat{\mathbf{u}} \notin U$ for all $\mathbf{u} \in U$. Then, from the affine variety code C_U, a stabilizer code can be obtained. The parameters for this code are $[[n, k, \geq d]]_{p^r}$, where $n = N_1 N_2 \cdots N_m$, $k = n - 2\,\mathrm{card}(U)$ and $d = d(C_U^\perp)$.*

Example 1. With the above notation, set R the ring $\mathbb{F}_4[x, y, z]/ < x^3 - 1, y^3 - 1, z^3 - 1 >$. This means that the corresponding codes will have length $n = 27$. Our set U will be

$$U = \{(0,0,1), (1,1,0), (0,1,1), (1,1,1), (1,2,0)(1,0,2), (0,1,2), (1,1,2), (1,2,1), (2,1,1)\}.$$

Since U satisfies the conditions in Corollary 2, U yields a $[[27, 7, 6]]_4$ stabilizer code. The distance has been computed with the computational algebra system Magma [25].

Example 2. Let us show another example. Consider the ring $R = \mathbb{F}_8[x, y]/ < x^7 - 1, y^7 - 1 >$ and the set $U = \{(1,3), (4,4), (1,6), (5,0), (1,2)\}$. This gives a $[[49, 39, 4]]_8$ stabilizer code.

Codes in the above examples are only samples. The next section is devoted to show that new codes with algebraic structure and good parameters can be obtained by considering subfield-subcodes.

2. Subfield-Subcodes of Affine variety Codes

As above, we write $R = \mathbb{F}_{p^r}[X_1, X_2, \ldots, X_m]/I$, where I is the ideal of the polynomial ring $\mathbb{F}_{p^r}[X_1, X_2, \ldots, X_m]$ generated by the set of polynomials $\{X_1^{N_1} - 1, X_2^{N_2} - 1, \ldots, X^{N_m} - 1\}$. In addition, we consider a positive integer s which divides r. We say that an element $f \in R$ evaluates to $\mathbb{F}_{p^s}$ whenever $f(\boldsymbol{\alpha}) \in \mathbb{F}_{p^s}$ for all $\boldsymbol{\alpha} \in Z(I)$. Now, define $\mathcal{T} : R \to R$ the map given by $\mathcal{T}(f) = f + f^{p^s} + \cdots + f^{p^{s(\frac{r}{s}-1)}}$. Also, set $\mathrm{tr}_r^s : \mathbb{F}_{p^r} \to \mathbb{F}_{p^s}$ given by $\mathrm{tr}_r^s(x) = x + x^{p^s} + \cdots + x^{p^{s(\frac{r}{s}-1)}}$ and extend it to $\mathbf{tr} : \mathbb{F}_{p^r}^n \to \mathbb{F}_{p^s}^n$ by applying tr_r^s coordinatewise. Afterwards, we will need the following results.

Proposition 4. *With the above notations and for any $f \in R$, it holds:*

(1) $\mathcal{T}(af) = a\mathcal{T}(f)$, *for all element* $a \in \mathbb{F}_{p^s}$.
(2) $\mathcal{T}(f)^{p^s} = \mathcal{T}(f^{p^s}) = \mathcal{T}(f)$.
(3) $\mathrm{ev}(\mathcal{T}(f)) = \mathbf{tr}(\mathrm{ev}(f))$.
(4) $\mathrm{ev}(\mathcal{T}(f)) = \mathbf{0}$ *happens if, and only if,* $\mathcal{T}(f) = 0$.

Proof. Items (1), (2) and (3) follow from the definition of $\mathcal{T}$, properties of finite fields and the fact that we are working modulo I. Item (4) holds because the map ev is an isomorphism. □

Proposition 5. *Let $g \in R$. Then, the following statements are equivalent.*

(1) $g = \mathcal{T}(h)$ *for some* $h \in R$.
(2) $g^{p^s} = g$.
(3) g *evaluates to* $\mathbb{F}_{p^s}$.

Proof. First suppose that for some $h \in R$, $g = \mathcal{T}(h)$. Then

$$g^{p^s} = \mathcal{T}(h)^{p^s} = \mathcal{T}(h) = g,$$

where the second equality follows from Proposition 4. If $g^{p^s} = g$, then for any $\boldsymbol{\alpha} \in \mathbb{F}_{p^r}^m$, $g(\boldsymbol{\alpha})^{p^s} = g(\boldsymbol{\alpha})$ and so $g(\boldsymbol{\alpha}) \in \mathbb{F}_{p^s}$. Lastly suppose that, for every $\boldsymbol{\alpha} \in \mathbb{F}_{p^r}^m$, $g(\boldsymbol{\alpha}) \in \mathbb{F}_{p^s}$. Since $\mathbf{tr}$ is surjective, we can consider $\mathbf{y} \in \mathbb{F}_{p^r}^n$ such that $\mathbf{tr}(\mathbf{y}) = \mathrm{ev}(g)$. Now, consider the class h of a interpolating polynomial satisfying $\mathrm{ev}(h) = \mathbf{y}$, then,

$$\mathrm{ev}(\mathcal{T}(h)) = \mathbf{tr}(\mathrm{ev}(h)) = \mathrm{ev}(g)$$

and the proof is concluded since ev is an isomorphism. □

Given a positive integer t, $\mathbb{Z}_t$ will stand for the quotient ring $\mathbb{Z}/t\mathbb{Z}$.

Definition 2. *A subset $\mathfrak{I}$ of the cartesian product $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_m}$ is called to be a cyclotomic set if $\mathfrak{I} = p \cdot \mathfrak{I} := \{p \cdot \boldsymbol{\alpha} \mid \boldsymbol{\alpha} \in \mathfrak{I}\}$. $\mathfrak{I}$ will be a minimal cyclotomic set if there is $\boldsymbol{\alpha} \in \mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_m}$ such that every element of $\mathfrak{I}$ can be written $p^{si} \cdot \boldsymbol{\alpha}$ for some integer i.*

Fix a monomial ordering on $\mathbb{F}_{p^r}[X_1, X_2, \cdots, X_m]$ and its corresponding ordering $\succ$ on $\mathbb{Z}_{\geq 0}^m$, where $\mathbb{Z}_{\geq 0}$ denotes the nonnegative integers. A minimal cyclotomic set $\mathfrak{I}$ will be represented by that element $\mathbf{a} \in \mathfrak{I}$ with smallest coordinates with respect to the above fixed ordering $\succ$. Notice that we use the ordering $\succ$ for determining a unique representative of the set $\mathfrak{I}$ and the monomial ordering in the proof of Theorem 3. Thus, we will set $\mathfrak{I}_{\mathbf{a}} := \mathfrak{I}$ and $i_{\mathbf{a}} := \mathrm{card}(\mathfrak{I}_{\mathbf{a}})$. Finally, the set of elements $\mathbf{a}$ representing minimal cyclotomic sets is denoted by $\mathcal{A}$.

For every $\mathbf{a} = (a_1, a_2, \ldots, a_m) \in \mathcal{A}$, $i_{\mathbf{a}}$ is a divisor of r and it holds that $a_i p^{si_{\mathbf{a}}} \equiv a_i \pmod{N_i}$, $1 \leq i \leq m$. In addition, every cyclotomic set is a union of minimal cyclotomic sets and the minimal cyclotomic sets constitute a partition of $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_m}$. Recall that we denote by f an element in R and its canonical representative and we set $\mathrm{supp}(f)$ the support of the canonical representative. Then, any element $f \in R$ may be decomposed in a unique way as a sum of classes of polynomials with support included in minimal cyclotomic sets. That is to say, $f = \sum_{\mathbf{a} \in \mathcal{A}} f_{\mathbf{a}}$, where $\mathrm{supp}(f_{\mathbf{a}}) \subseteq \mathfrak{I}_{\mathbf{a}}$. We also notice that $\mathrm{supp}(\mathcal{T}(f_{\mathbf{a}})) \subseteq \mathfrak{I}_{\mathbf{a}}$.

Now define the function $\mathcal{T}_{\mathbf{a}} : R \to R$ as $\mathcal{T}_{\mathbf{a}}(f) = f + f^{p^s} + \cdots + f^{p^{s(i_{\mathbf{a}}-1)}}$ and set $X^{\mathbf{a}} = X_1^{a_1} X_2^{a_2} \cdots X_m^{a_m}$. Then we are ready to state and prove Theorem 3, which gives a basis for the vector space of elements in R evaluating to the field $\mathbb{F}_{p^s}$. First, we provide two results that help us in our purpose.

Proposition 6. *Let f be an element in R that evaluates to $\mathbb{F}_{p^s}$ with $\mathrm{supp}(f) \subseteq \mathfrak{I}_{\mathbf{a}}$ and consider a primitive element β of $\mathbb{F}_{p^{si_{\mathbf{a}}}}$. Then, f can be expressed as a linear combination with coefficients in $\mathbb{F}_{p^s}$ of the elements in R given by $\mathcal{S}_{\mathbf{a}}^{\beta} := \left\{\mathcal{T}_{\mathbf{a}}(X^{\mathbf{a}}), \mathcal{T}_{\mathbf{a}}(\beta X^{\mathbf{a}}), \ldots, \mathcal{T}_{\mathbf{a}}(\beta^{i_{\mathbf{a}}-1} X^{\mathbf{a}})\right\}$.*

Proof. Since $\mathrm{supp}(f) \subseteq \mathfrak{I}_{\mathbf{a}}$ and $f^{p^s} = f$, there is some $\alpha \in \mathbb{F}_{p^r}$ such that $f = \sum_{j=0}^{i_{\mathbf{a}}-1} (\alpha X^{\mathbf{a}})^{p^{js}}$. Moreover $\alpha^{p^{si_{\mathbf{a}}}} = \alpha$, which implies that $\alpha \in \mathbb{F}_{p^{si_{\mathbf{a}}}}$.

We know that $\{1, \beta, \ldots, \beta^{i_{\mathbf{a}}-1}\}$ is a basis of $\mathbb{F}_{p^{si_{\mathbf{a}}}}$ over $\mathbb{F}_{p^s}$, so $\alpha = a_0 + a_1\beta + \cdots + a_{i_{\mathbf{a}}-1}\beta^{i_{\mathbf{a}}-1}$, with $a_i \in \mathbb{F}_{p^s}$ for all i. Therefore,

$$f = \sum_{j=0}^{i_{\mathbf{a}}-1} \alpha^{p^{js}} X^{p^{js}\mathbf{a}} = \sum_{j=0}^{i_{\mathbf{a}}-1} X^{p^{js}\mathbf{a}} \left(\sum_{l=0}^{i_{\mathbf{a}}-1} a_l \beta^l\right)^{p^{js}}$$
$$= \sum_{l=0}^{i_{\mathbf{a}}-1} a_l \left(\sum_{j=0}^{i_{\mathbf{a}}-1} \beta^{lp^{js}} X^{p^{js}\mathbf{a}}\right) = \sum_{l=0}^{i_{\mathbf{a}}-1} a_l \mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}}).$$

□

Proposition 7. *The polynomials in the previously considered set $\mathcal{S}_{\mathbf{a}}^{\beta}$ are linearly independent over $\mathbb{F}_{p^s}$.*

Proof. Reasoning by contradiction, assume that $\sum_{l=0}^{i_{\mathbf{a}}-1} a_l \mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}}) = 0$. Then, the term whose attached monomial is $X^{\mathbf{a}}$ and appears in the left hand side of the above equality is $(a_0 + a_1\beta + \cdots + a_{i_{\mathbf{a}}-1}\beta^{i_{\mathbf{a}}-1})X^{\mathbf{a}}$ and it must vanish. This is true only if β is a root of the univariate polynomial $a_0 + a_1 Z + \cdots + a_{i_{\mathbf{a}}-1} Z^{i_{\mathbf{a}}-1}$. This gives the desired contradiction because the minimal polynomial of β has degree $i_{\mathbf{a}}$. □

Next, we state the above mentioned theorem.

Theorem 3. *The following set*

$$\Omega_s^R := \bigcup_{\mathbf{a}\in\mathcal{A}} \left\{\mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}}) \mid 0 \leq l \leq i_{\mathbf{a}} - 1 \text{ and } \beta \text{ is a primitive element of } \mathbb{F}_{p^{si_{\mathbf{a}}}}\right\}$$

constitutes a basis for the vector space over $\mathbb{F}_{p^s}$ of elements in R evaluating to $\mathbb{F}_{p^s}$.

Proof. We start by proving that the classes in Ω_s^R are linearly independent. This holds, on the one hand, because there is no linear dependence among the elements in Ω_s^R supported on different minimal cyclotomic sets. Indeed, any monomial of any element supported on $\mathfrak{I}_{\mathbf{a}}$ is different from that of any other supported on $\mathfrak{I}_{\mathbf{a}'}$ with $\mathbf{a} \neq \mathbf{a}'$. On the other hand, Proposition 7 proves the independence of the elements supported on the same set $\mathfrak{I}_{\mathbf{a}}$, which shows our statement.

To conclude the proof, we are going to show that the set Ω_s^R generates the vector space of elements f in R evaluating to $\mathbb{F}_{p^s}$. Recall that we are using canonical polynomials for representing their corresponding classes in R. Consider the term in f with smallest order for the above mentioned monomial ordering associated with the order $\succ$ on $\mathbb{Z}_{\geq 0}^m$, say $\beta^{k_1} X^{\mathbf{a}_1}$, then $\mathcal{T}_{\mathbf{a}_1}(\beta^{k_1} X^{\mathbf{a}_1}) = \sum_{l=0}^{i_{\mathbf{a}_1}-1} (\beta^{k_1} X^{\mathbf{a}_1})^{p^{ls}}$ must appear in f because it evaluates to $\mathbb{F}_{p^s}$. Since $\beta^{k_1} X^{\mathbf{a}_1}$ has the smallest order in f, $\mathbf{a}_1$ must be one of the elements in $\mathcal{A}$. Assume, without loss of generality, that these elements are $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_t\}$. Set $f_1 = f - \mathcal{T}_{\mathbf{a}_1}(\beta^{k_1} X^{\mathbf{a}_1})$ and pick its monomial with smallest order, say $\beta^{k_2} X^{\mathbf{a}_2}$. Again the polynomial $\mathcal{T}_{\mathbf{a}_2}(\beta^{k_2} X^{\mathbf{a}_2})$ must appear in f_1. We can repeat the above procedure and consider $f_2 = f_1 - \mathcal{T}_{\mathbf{a}_2}(\beta^{k_2} X^{\mathbf{a}_2})$. We will finish in t steps and this will provide the desired expression of f as a linear combination of elements in Ω_s^R, which concludes the proof. □

We have just provided a constructive way of obtaining all classes in R that evaluate to $\mathbb{F}_{p^s}$. In particular, if we restrict to those with support in U, we have a formula for the dimension of an affine variety subfield-subcode.

Theorem 4. *Let U be a subset of $\{0,1,\ldots,N_1-1\}\times\{0,1,\ldots,N_2-1\}\times\cdots\times\{0,1,\ldots,N_m-1\}$, $n=N_1N_2\cdots N_m$ and define $C_U^s := C_U\cap\mathbb{F}_{p^s}^n$. Then,*

$$C_U^s = \mathrm{ev}\ \left(\mathcal{T}(\mathbb{F}_{p^r}^{\mathcal{H}})\cap\mathbb{F}_{p^r}^U\right),$$

C_U^s is generated by the images under the evaluation map ev *of the following elements in R*

$$\bigcup_{\mathfrak{I}_{\mathbf{a}}|\mathfrak{I}_{\mathbf{a}}\subseteq U}\left\{\mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}})\mid 0\le l\le i_{\mathbf{a}}-1 \text{ and } \beta \text{ is a primitive element of } \mathbb{F}_{p^{si_{\mathbf{a}}}}\right\}$$

and

$$\dim C_U^s = \sum_{\mathfrak{I}_{\mathbf{a}}|\mathfrak{I}_{\mathbf{a}}\subseteq U} i_{\mathbf{a}}.$$

3. Quantum codes from subfield-subcodes of affine variety codes

We devote this section to explain which of our affine variety subfield-subcodes yield stabilizer codes. Notice that our quantum codes will be defined over a *small* field $\mathbb{F}_{p^s}$ but the original code is defined over a *large* field $\mathbb{F}_{p^r}$.

Prior to stating our main result, we will need to describe dual codes of subfield-subcodes. From Proposition 3, we know that $C_U^{\perp}$ is the affine variety code defined by $U^{\perp}$. Then, we get

$$(C_U^s)^{\perp} = \mathbf{tr}\,(C_{U^{\perp}}) = \mathbf{tr}\left(\mathrm{ev}(\mathbb{F}_{p^r}^{U^{\perp}})\right) = \mathrm{ev}\left(\mathcal{T}(\mathbb{F}_{p^r}^{U^{\perp}})\right),$$

where the first equality follows from Delsarte's Theorem [8] and the last one from the fact that, by Proposition 5, the following map composition equality $\mathrm{ev}\circ\mathcal{T}=\mathbf{tr}\circ\mathrm{ev}$ holds. Notice that, as above, we are identifying classes in R with canonical representatives. Now, $\mathcal{T}(\mathbb{F}_{p^r}^{U^{\perp}})$ is generated by $\mathcal{T}(\gamma X^{\mathbf{a}})$ for $\mathbf{a}\in U^{\perp}$ and $\gamma\in\mathbb{F}_{p^r}$. If one fixes $\mathbf{a}$ and varies γ over the field, then the set $\{\mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}})\}_{0\le l\le i_{\mathbf{a}}-1}$, β primitive, is obtained. Thus we have proved the following result.

Theorem 5. *Let $U\subseteq\mathcal{H}$ be as in Section 1. The dual code $(C_U^s)^{\perp}$ of the code C_U^s is generated by the image by* ev *of the following elements in R:*

$$\bigcup_{\mathfrak{I}_{\mathbf{a}}|\mathfrak{I}_{\mathbf{a}}\cap U^{\perp}\neq\emptyset}\left\{\mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}})\mid 0\le l\le i_{\mathbf{a}}-1 \text{ and } \beta \text{ is a primitive element of } \mathbb{F}_{p^{si_{\mathbf{a}}}}\right\}.$$

As a consequence, it holds that

$$\dim(C_U^s)^{\perp} = \sum_{\mathfrak{I}_{\mathbf{a}}|\mathfrak{I}_{\mathbf{a}}\cap U^{\perp}\neq\emptyset} i_{\mathbf{a}}.$$

We conclude this section with our main result which allows us to construct good stabilizer codes. Given a minimal cyclotomic set $\mathfrak{I}_{\mathbf{a}}$, the subset of $\mathbb{Z}_{N_1}\times\mathbb{Z}_{N_2}\times\cdots\times\mathbb{Z}_{N_m}$ defined as $\hat{\mathfrak{I}_{\mathbf{a}}} := \{\hat{\mathbf{u}}\mid \mathbf{u}\in\mathfrak{I}_{\mathbf{a}}\}$ will be called the complementary set of $\mathfrak{I}_{\mathbf{a}}$.

Theorem 6. *Let p be a prime number and r and s positive integers such that $s|r$. Let*

$$\mathcal{H} := \{0,1,\ldots,N_1-1\}\times\{0,1,\ldots,N_2-1\}\times\cdots\times\{0,1,\ldots,N_m-1\}$$

be the hypercube defined in Section 1, where N_i divides p^r-1 for all index i, and consider a nonempty subset U of $\mathcal{H}$. Then,

(1) *The codes' inclusion* $C_U^s \subseteq (C_U^s)^\perp$ *happens if, and only if,* $\hat{\mathfrak{I}_{\mathbf{a}}}$ *is not contained in* U *whenever* $\mathfrak{I}_{\mathbf{a}}$ *is.*
(2) *Assume that* U *satisfies the conditions in the previous item. Then, from the affine variety code* C_U^s *a stabilizer code can be obtained. The parameters for that code are* $[[n, k, \geq d]]_{p^s}$*, where* $n = N_1 N_2 \cdots N_m$*,* $k = n - 2\sum_{\mathfrak{I}_{\mathbf{a}} | \mathfrak{I}_{\mathbf{a}} \subseteq U} i_{\mathbf{a}}$ *and* $d = d\left((C_U^s)^\perp\right)$*.*

Proof. Theorem 5 proves that the dual code $(C_U^s)^\perp$ is given by the evaluation of the elements $\mathcal{T}_{\mathbf{a}}(\beta^l X^{\mathbf{a}})$, where $0 \leq l \leq i_{\mathbf{a}} - 1$ and β is a primitive element of $\mathbb{F}_{p^{si_{\mathbf{a}}}}$, whenever $\mathfrak{I}_{\mathbf{a}} \cap U^\perp \neq \emptyset$. Therefore, $C_U^s \subseteq (C_U^s)^\perp$ if and only if $\mathfrak{I}_{\mathbf{a}} \cap U^\perp \neq \emptyset$ when $\mathfrak{I}_{\mathbf{a}} \subseteq U$ and this happens if, and only if, the complementary set of $\mathfrak{I}_{\mathbf{a}}$ satisfies $\hat{\mathfrak{I}_{\mathbf{a}}} \not\subseteq U$ for all minimal cyclotomic set $\mathfrak{I}_{\mathbf{a}} \subseteq U$. This proves our first assertion. The second one follows from the CSS construction. □

Remark 1. One of the best known classes of affine variety codes are those where the ring R (it could be more general than that in this paper) admits a weight function. This function takes values in an ordered semigroup and gives a suitable nested sequence of vector spaces in R, $L_1 \subset L_2 \subset \cdots \subset L_r$, whose dimensions increase in one unit. The evaluation of these spaces provides a nested family of primary codes $C_1 \subset C_2 \subset \cdots \subset C_r$ and their corresponding dual ones $(C_r)^\perp \subset (C_{r-1})^\perp \subset \cdots \subset (C_1)^\perp$. The weight function allows us to define the so-called Feng-Rao bound on the minimum distance of the previous codes. In this paper, from the point of view of classical codes and despite not having a weight function, we show a way of getting suitable sets $U_i \subset \mathcal{H}$, $1 \leq i \leq r$, to obtain nested sequences of codes $C_{U_1} \subset C_{U_2} \subset \cdots \subset C_{U_r}$ (respectively, $C_{U_1}^s \subset C_{U_2}^s \subset \cdots \subset C_{U_r}^s$) such that $C_{U_r} \subset C_{U_r}^\perp$ (respectively, $C_{U_r}^s \subset (C_{U_r}^s)^\perp$) and therefore $(C_{U_r})^\perp \subset (C_{U_{r-1}})^\perp \subset \cdots \subset (C_{U_1})^\perp$ (respectively, $(C_{U_r}^s)^\perp \subset (C_{U_{r-1}}^s)^\perp \subset \cdots \subset (C_{U_1}^s)^\perp$). Our main result is to determine the dimensions of the above mentioned codes.

It would be interesting to know an explicit formula or tight bound for the value $d((C_U^s)^\perp)$, $U \subset \mathcal{H}$. Reasoning as in Theorem 6, when the inclusion $(C_U^s)^\perp \subseteq C_U^s$ holds, one can get an $[[n, k, \geq d]]_{p^s}$ code where n is as above, $k = 2\sum_{\mathfrak{I}_{\mathbf{a}} | \mathfrak{I}_{\mathbf{a}} \subseteq U} i_{\mathbf{a}} - n$ and $d = d(C_U^s)$. In this case a lower bound for the distance d can be described. Indeed, $d(C_U^s) \geq d(C_U)$ and a lower bound for the distance of the code C_U can be computed following the procedure given in [15]. It should be noted that this procedure is not easy to implement computationally and the bound seems not to be sharp.

Codes in this paper are constructed by applying the CSS code construction to suitable linear codes. However, to get quantum codes, one can also use other bilinear pairings as the trace alternating inner product. As a referee of this paper pointed out, to relate our codes with those obtained with respect to different bilinear pairings is an interesting future work. Notice that in terms of the CSS construction as well as in the more general context of asymmetric quantum codes, this last topic has been explored in [11, 10] by using the so-called functional approach.

4. Examples

In this section we provide some sets U with associated codes C_U^s giving rise to CSS stabilizer codes and compute their quantum parameters. We impose the condition that a minimal cyclotomic set $\mathfrak{I}_{\mathbf{a}}$ is contained in U whenever any of its elements is in U. First we give a table containing the parameters and the field where are defined. Notice that, by Corollary 1, the value d in the table needs not to be the true minimum distance but a lower bound and that our codes are pure to d. These codes either improve or add new

parameters with respect to those ones given in [9]. In addition, some of them have a symbol GV which means that we have checked that they are pure and exceed the quantum Gilbert-Varshamov bound [12, Theorem 1.4 and Corollary 2.3]. Finally, codes with a symbol L improve the parameters of some codes in [24, Tables I and II]. Computations has been done by writing a Magma [25] function. After the table, as announced earlier, the reader can find, also in tabular form, those *subsets* U and *values* N_i, p, r and s providing the codes. For simplicity, a code given by U is also called U. Based on [10, Table IV, entry 18], within the family of CSS codes, the code U_{23} is optimal.

Code	Symbol	n	k	d	$q = p^s$	Code	Symbol	n	k	d	$q = p^s$
U_1		147	123	4	2	U_2		147	105	6	2
U_3	GV	23	1	7	2	U_4		189	147	5	2
U_5		189	141	6	2	U_6		189	129	7	2
U_7		217	171	6	2	U_8		245	209	4	2
U_9		245	179	6	2	U_{10}		441	411	4	2
U_{11}		45	25	6	4	U_{12}		225	199	5	4
U_{13}		189	165	5	4	U_{14}		189	153	6	4
U_{15}	GV	225	211	4	4	U_{16}	L	73	55	6	8
U_{17}		21	9	5	8	U_{18}	L	73	43	8	8
U_{19}		147	135	4	8	U_{20}		147	127	5	8
U_{21}		64	48	4	3	U_{22}		64	52	3	3
U_{23}	GV, L	11	1	5	3	U_{24}	L	71	51	5	5
U_{25}	L	31	13	6	5	U_{26}		71	41	8	5
U_{27}		96	88	3	5	U_{28}		96	84	4	5
U_{29}	GV	200	184	4	3	U_{30}		36	26	4	7

Code / Subset	p	r	s	N_1	N_2	N_3
$U_1 = \{(6,2,2),(5,4,1),(3,1,2),(6,2,1),(5,4,2),(3,1,1),$ $(2,3,0),(4,6,0),(1,5,0),(6,0,0),(5,0,0),(3,0,0)\}$	2	6	1	7	7	3
$U_2 = \{(2,4,0),(4,1,0),(1,2,0),(6,0,2),(5,0,1),(3,0,2),$ $(6,0,1),(5,0,2),(3,0,1),(6,2,0),(5,4,0),(3,1,0),$ $(0,6,2),(0,5,1),(0,3,2),(0,6,1),(0,5,2),(0,3,1),$ $(2,0,0),(4,0,0),(1,0,0)\}$	2	6	1	7	7	3

Code / Subset	p	r	s	N_1	N_2	N_3
$U_3 = \{2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1\}$	2	11	1	23	-	-
$U_4 = \{(0,2,0),(0,4,0),(0,1,0),(0,6,2),(0,5,1),(0,3,2),$ $(0,6,1),(0,5,2),(0,3,1),(2,6,2),(4,5,1),(8,3,2),$ $(7,6,1),(5,5,2),(1,3,1),(2,1,0),(4,2,0),(8,4,0),$ $(7,1,0),(5,2,0),(1,4,0)\}$	2	6	1	9	7	3
$U_5 = \{(2,4,1),(4,1,2),(8,2,1),(7,4,2),(5,1,1),(1,2,2),$ $(0,6,2),(0,5,1),(0,3,2),(0,6,1),(0,5,2),(0,3,1),$ $(2,6,2),(4,5,1),(8,3,2),(7,6,1),(5,5,2),(1,3,1),$ $(2,2,0),(4,4,0),(8,1,0),(7,2,0),(5,4,0),(1,1,0)\}$	2	6	1	9	7	3
$U_6 = \{(2,3,0),(4,6,0),(8,5,0),(7,3,0),(5,6,0),(1,5,0),$ $(6,6,0),(3,5,0),(6,3,0),(3,6,0),(6,5,0),(3,3,0),$ $(2,3,1),(4,6,2),(8,5,1),(7,3,2),(5,6,1),(1,5,2),$ $(2,4,2),(4,1,1),(8,2,2),(7,4,1),(5,1,2),(1,2,1),$ $(6,2,2),(3,4,1),(6,1,2),(3,2,1),(6,4,2),(3,1,1)\}$	2	6	1	9	7	3
$U_7 = \{(0,2),(0,4),(0,1),(14,0),(28,0),(25,0),(19,0),$ $(7,0),(22,6),(13,5),(26,3),(21,6),(11,5),(22,3),(13,6),$ $(26,5),(21,3),(11,6),(22,5),(13,3),(26,6),(21,5),(11,3)\}$	2	15	1	31	7	-
$U_8 = \{(2,4,0),(4,1,0),(1,2,0),(6,0,2),(5,0,4),(3,0,3),$ $(6,0,1),(5,0,2),(3,0,4),(6,0,3),(5,0,1),(3,0,2),$ $(6,0,4),(5,0,3),(3,0,1),(2,0,0),(4,0,0),(1,0,0)\}$	2	12	1	7	7	5

Code / Subset	p	r	s	N_1	N_2	N_3
$U_9 = \{(2,4,2),(4,1,4),(1,2,3),(2,4,1),(4,1,2),(1,2,4),$ $(2,4,3),(4,1,1),(1,2,2),(2,4,4),(4,1,3),(1,2,1),$ $(6,2,0),(5,4,0),(3,1,0),(6,4,2),(5,1,4),(3,2,3),$ $(6,4,1),(5,1,2),(3,2,4),(6,4,3),(5,1,1),(3,2,2),$ $(6,4,4),(5,1,3),(3,2,1),(6,6,0),(5,5,0),(3,3,0),$ $(6,0,0),(5,0,0),(3,0,0)\}$	2	12	1	7	7	5
$U_{10} = \{(0,6,2),(0,5,4),(0,3,1),(6,2,2),(3,4,4),(6,1,1),$ $(3,2,2),(6,4,4),(3,1,1),(2,2,3),(4,4,6),(8,1,5),$ $(7,2,3),(5,4,6),(1,1,5)\}$	2	12	1	9	7	7
$U_{11} = \{(3,1,1),(2,1,1),(0,0,2),(4,1,2),(1,1,2),(4,2,0),$ $(0,2,2),(3,0,1),(2,0,1),(1,2,0)\}$	2	4	2	5	3	3
$U_{12} = \{(10,0),(0,10),(10,5),(10,13),(10,7)(8,5),(2,5),$ $(4,3),(1,12),(12,1),(3,4)(8,3),(2,12)\}$	2	4	2	15	15	-
$U_{13} = \{(8,5),(5,20),(2,17),(4,9),(7,15),(1,18),(3,0),$ $(6,7),(6,14),(8,6),(5,3),(2,12)\}$	2	6	2	9	21	-
$U_{14} = \{(8,5),(5,20),(2,17),(4,9),(7,15),(1,18),(3,0),$ $(6,7),(6,14),(8,6),(5,3),(2,12),(0,4),(0,16),$ $(0,1),(0,19),(0,13),(0,10)\}$	2	6	2	9	21	-
$U_{15} = \{(10,0),(14,14),(11,11),(5,9),(5,6),(0,10),(10,5)\}$	2	4	2	15	15	-

Code / Subset	p	r	s	N_1	N_2	N_3
$U_{16} = \{16, 55, 2, 32, 37, 4, 53, 59, 34\}$	2	9	3	73	-	-
$U_{17} = \{(5,2), (5,1), (1,2), (1,1), (2,0), (4,0)\}$	2	6	3	7	3	-
$U_{18} = \{(23, 38, 12, 22, 30, 21, 54, 67, 25, 56, 10, 7, 15, 47, 11\}$	2	9	3	73	-	-
$U_{19} = \{(2,2,0), (3,2,2), (3,2,1), (4,1,0), (5,3,0), (3,1,0)\}$	2	6	3	7	7	3
$U_{20} = \{(2,2,0), (3,2,2), (3,2,1), (4,1,0), (5,3,0), (3,1,0), (4,2,2), (4,2,1), (3,4,2), (3,4,1)\}$	2	6	3	7	7	3
$U_{21} = \{(3,2), (1,6), (0,3), (0,1), (7,0), (5,0), (7,3), (5,1)\}$	3	2	1	8	8	-
$U_{22} = \{(3,0), (1,0), (6,5), (2,7), (7,7), (5,5)\}$	3	2	1	8	8	-
$U_{23} = \{(3, 9, 5, 4, 1\}$	3	5	1	11	-	-
$U_{24} = \{39, 53, 52, 47, 22, 65, 41, 63, 31, 13\}$	5	5	1	71	-	-
$U_{25} = \{15, 13, 3, 20, 7, 4, 29, 21, 12\}$	5	3	1	31	-	-
$U_{26} = \{64, 36, 38, 48, 27, 15, 4, 20, 29, 3, 45, 12, 60, 16, 9\}$	5	5	1	71	-	-
$U_{27} = \{(18,1), (17,0), (13,0), (6,0)\}$	5	2	1	24	4	-
$U_{28} = \{(23,3), (19,3), (11,2), (7,2), (18,0), (12,3)\}$	5	2	1	24	4	-
$U_{29} = \{(3,3,3), (4,4,1), (2,2,3), (1,1,1), (3,0,6), (4,0,2), (2,0,6), (1,0,2)\}$	3	4	1	5	5	8
$U_{30} = \{(2,0), (2,2), (0,5), (1,1), (1,2)\}$	7	2	1	6	6	-

References

[1] Aly, S.A., Klappenecker, A., Sarpevally, P.K. On quantum and classical BCH codes, *IEEE Trans. Inf. Theory* **53** (2007) 1183-1188.

[2] Ashikhmin, A., Knill, E. Non-binary quantum stabilizer codes, *IEEE Trans. Inf. Theory* **47** (2001) 3065-3072.

[3] Ashikhmin, A., Litsyn, S. Upper bounds on the size of quantum codes, *IEEE Trans. Inf. Theory* **45** (1999) 1206-1215.

[4] Bras-Amorós, M., O'Sullivan, M.E. Duality for some families of correction capability optimized evaluation codes, *Adv. Math. Commun.* **2** (2008) 15-33.

[5] Bierbrauer, J., Edel, Y. Quantum twisted codes, *J. Comb. Designs* **8** (2000) 174-188.

[6] Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A. Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory* **44** (1998) 1369-1387.

[7] Calderbank A.R., Shor, P. Good quantum error-correcting codes exist, *Phys. Rev. A* **54** (1996) 1098-1105.

[8] Delsarte, P. On subfield subcodes of modified Reed-Solomon codes, *IEEE Trans. Inform. Theory* **IT-21** (1975) 575-576.

[9] Edel, Y. *Some good quantum twisted codes.* Online available at `http://www.mathi.uni-heidelberg.de/ yves/Matritzen/QTBCH/QTBCHIndex.html`. Based in reference [5].

[10] Ezerman, M.F., Jitman, S., Ling, S., Pasechnik, D.V. CSS-like constructions of asymmetric quantum codes, *IEEE Trans. Inf. Theory* **59** (2013) 6732-6754.

[11] Feng, K., Ling, S., Xing, C. Asymptotic bounds on quantum codes from algebraic geometry codes, *IEEE Trans. Inf. Theory* **52** (2006) 986-991.

[12] Feng, K., Ma, Z. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes, *IEEE Trans. Inf. Theory* **50** (2004) 3323-3325.

[13] Fitzgerald, J., Lax, R.F. Decoding affine variety codes using Gröbner bases, *Des. Codes Cryptogr.* **13** (1998) 147-158.

[14] Geil, O. *Evaluation codes from an affine variety code perspective.* Advances in algebraic geometry codes, Ser. Coding Theory Cryptol. 5 (2008) 153-180. World Sci. Publ., Hackensack, NJ. Eds.: E. Martinez-Moro, C. Munuera, D. Ruano.

[15] Geil, O., Martin, S. An improvement of the Feng-Rao bound for primary codes, arXiv:1307.3107.

[16] Gottesman, D. A class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* **54** (1996) 1862-1868.

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

[18] Hagiwara, M., Imai, H., Quantum quasi-cyclic LDPC codes. Information Theory Proc. (ISIT) 2007, 806-810.

[19] Hernando, F., Marshall, K., O'Sullivan, M.E. The dimension of subcode-subfields of shortened generalized Reed-Solomon codes, *Des. Codes Cryptogr.* **69** (2013) 131-142.
[20] Hernando, F., O'Sullivan, M.E., Popovici, E., Srivastava, S. Subfield-subcodes of generalized toric codes. Information Theory Proc. (ISIT) 2010, 1125-1129.
[21] Kasai, K., Hagiwara, M., Imai, H., Sakaniwa, K. Non-binary quasi-cyclic quantum LDPC codes. Information Theory Proc. (ISIT) 2011, 653-657.
[22] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K. Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inform. Theory* **52** (2006) 4892-4914.
[23] La Guardia, G.G. Construction of new families of nonbinary quantum codes, *Phys. Rev. A* **80** (2009) 042331-1-042331-11.
[24] La Guardia, G.G. On the construction of nonbinary quantum BCH codes, *IEEE Trans. Inf. Theory* **60** (2014) 1528-1535.
[25] Magma Computational Algebra System. `http://magma.maths.usyd.edu.au/magma/`.
[26] Martínez-Moro, E., Piñera-Nicolás A., Rúa. I.F. Additive semisimple multivariable codes over $\mathbb{F}_4$, *Des. Codes Cryptogr.* **69** (2013) 161-180.
[27] Martínez-Moro, E. On semisimple algebra codes: generator theory, *Algebra Discr. Math.* **3** (2007) 99-112.
[28] Rains, E.M. Nonbinary quantum codes, *IEEE Trans. Inf. Theory* **45** (1999) 1827-1832.
[29] Ruano, D. On the structure of generalized toric codes, *J. Symbolic Comput.* **44** (2009) 499-506.
[30] Shor, P.W. Algorithms for quantum computation: discrete logarithm and factoring, in Proc. 35th Ann. Symp. Foundations of Computer Science, *IEEE Computer Society Press* 1994, 124-134.
[31] Shor, P.W. Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* **52** (1995) 2493-2496.
[32] Steane, A.M. Simple quantum error correcting codes, *Phys. Rev. Lett.* **77** (1966) 793-797.
[33] Stichtenoth, H. On the dimension of subfield subcodes, *IEEE Trans. Inf. Theory* **36** (1990) 90-93.
[34] Wootters W.K., Zurek, W.H. A single quantum cannot be cloned, *Nature*, **299** (1982) 802-803.

Current address: `Carlos Galindo and Fernando Hernando:` Instituto Universitario de Matemáticas y Aplicaciones de Castellón and Departamento de Matemáticas, Universitat Jaume I, Campus de Riu Sec. 12071 Castelló (Spain).

E-mail address: Galindo: `galindo@mat.uji.es;` Hernando: `carrillf@mat.uji.es`