Classical and Quantum Evaluation Codes at the Trace Roots

Carlos Galindo, Fernando Hernando and Diego Ruano

Abstract

We introduce a new class of evaluation linear codes by evaluating polynomials at the roots of a suitable trace function. We give conditions for self-orthogonality of these codes and their subfield-subcodes with respect to the Hermitian inner product. They allow us to construct stabilizer quantum codes over several finite fields which substantially improve the codes in the literature and that are records at [19] for the binary case. Moreover, we obtain several classical linear codes over the field $\mathbb{F}_4$ which are records at [19].

Index Terms

Evaluation Codes, Trace, Subfield-subcodes, Hermitian duality, Quantum codes.

I. Introduction

A stabilizer (quantum) code $\mathcal{C} \neq \{0\}$ is the common eigenspace of a commutative subgroup of the error group generated by a nice error basis on the space $\mathbb{C}^{q^n}$, where $\mathbb{C}$ denotes the complex numbers, q is a positive power of a prime number and n is a positive integer [24]. The code $\mathcal{C}$ has minimum distance d as long as errors with weight less than d can be detected or have no effect on $\mathcal{C}$ but some error with weight d cannot be detected. Furthermore, if $\mathcal{C}$ has dimension q^k as a $\mathbb{C}$-vector space, then we say that the code $\mathcal{C}$ has parameters $[[n, k, d]]_q$.

The importance of quantum computation is beyond doubt after [32], where polynomial time algorithms for prime factorization and discrete logarithms on quantum computers have been given. Quantum error-correcting codes are essential for this type of computation since they protect quantum information from decoherence and quantum noise. Quantum codes were first introduced for the binary case, some references are [3], [4], [6], [7], [8], [18], [20], and, subsequently, for the general case (see for instance [2], [5], [12], [21], [25], [29]). The interest on the general case continues to grow, especially after the realization that these codes are useful for fault-tolerant computation.

Stabilizer codes can be constructed from self-orthogonal classical linear codes:

Theorem 1. *[24], [1] Let C be a linear $[n, k, d]$ error-correcting code over the field $\mathbb{F}_{q^2}$ such that $C^{\perp_h} \subseteq C$. Then, there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code.*

The symbol $\perp_h$ means dual with respect to Hermitian inner product. An analogous result also holds for Euclidean duality when C is defined over $\mathbb{F}_q$, which gives rise to quantum codes obtained from the CSS construction [8], [33]. In this paper, most of our codes will be derived from Theorem 1. Although quantum codes were introduced recently, the literature on this topic is very large. Most papers have addressed the study of quantum MDS, LDCP and BCH codes [31], [11], [1], [25], [27], [23], [35], [26], [22].

In this paper, we introduce a new family of classical linear codes, they are evaluation codes of polynomials in one variable at the set of zeros of a suitable trace map (see Definition 2). The algebraic

Accepted for publication in IEEE Transactions on Information Theory.
This research was supported in part by the Spanish MINECO/FEDER (Grants No. MTM2015-65764-C3-2-P and MTM2015-69138-REDT), in part by the University Jaume I (Grant No. P1-1B2015-02), in part by The Danish Council for Independent Research (Grant No. DFF–4002-00367), and in part by RYC-2016-20208 (AEI/FSE/UE).

C. Galindo and F. Hernando are with Instituto Universitario de Matemáticas y Aplicaciones de Castellón, and with Departamento de Matemáticas, Jaume I University, Spain. e-mail: galindo@mat.uji.es, carrillf@mat.uji.es.

D. Ruano is with IMUVA (Mathematics Research Institute), University of Valladolid, Spain, and with the Department of Mathematical Sciences, Aalborg University, Denmark. e-mail: diego.ruano@uva.es

structure of the set of zeros of the trace map allows us to consider suitable subfield-subcodes, providing a new family of subfield-subcodes different from BCH codes, extended BCH codes or J-affine variety codes [14], [15], [16], [17]. For designing our codes, we will use *consecutive* cyclotomic cosets, the size and number of these cosets will determine a designed minimum distance and a lower bound for the dimension.

Although we are mainly interested in quantum codes, this new family of classical linear codes allows us to obtain 52 linear code records at [19] (see Example 4 in Section V). We construct linear codes with parameters $[128, 85, 16]_4$, $[128, 79, 20]_4$ and $[128, 75, 22]_4$ improving those with the same length and dimension in [19]. The remaining records are obtained by shortening the above three codes.

In Theorem 13, we study the dimension and minimum distance of the subfield-subcodes of this new family of codes and in Theorem 15, we give conditions for their self-orthogonality with respect to Hermitian inner product. In sum, from linear codes over $\mathbb{F}_{p^{2r}}$, p a prime number, we get linear codes over $\mathbb{F}_{p^{2s}}$, s being a positive integer that divides r, which give quantum codes over $\mathbb{F}_{p^s}$ with good parameters, improving those in the literature.

Apart from the introduction, this paper contains four sections. The definition of our classical codes, which evaluate at the roots of a trace function, and conditions for their self-orthogonality with respect to Hermitian inner product are given in Section II. Fundamental results on subfield-codes are presented in Section III, we will follow the approach in [14], [15], [16], [17] for one-variable J-affine variety codes and we will prove that, for some subfamilies of these codes, the operation of obtaining subfield-subcodes commutes with respect to taking Euclidean dual. Namely it holds for the codes we are interested in, which will be studied in Section IV. This section is the core of the paper, where we consider stabilizer codes obtained from the classical codes defined in Section II. We consider codes defined by evaluating at the non-roots of the trace function as well, we will refer to these codes as complementary codes. Finally, Section V is devoted to providing good examples of our codes. Apart from the above mentioned classical linear code records, we also give several examples of binary stabilizer quantum codes improving the records at [19]. In addition, we give tables containing stabilizer codes over $\mathbb{F}_4, \mathbb{F}_5$ and $\mathbb{F}_7$. For comparing our codes, we consider the codes in [25] and show that our codes largely improve them. We also provide new codes with a length that did not exist in the literature and, almost all of them, exceed the quantum Gilbert-Varshamov bounds [30], [13], [24].

II. Evaluation Codes at the Trace Roots

We devote this section to introduce a new class of evaluation linear codes and study their behavior under Hermitian duality. We are mainly interested in quantum codes although it is worthwhile to mention that their subfield-subcodes provide good classical codes as well. Their subfield-subcodes will be treated in Section IV.

Throughout this paper, let p be a prime number and r and s positive integers such that $s|r$. Set $r = s \cdot n$ and $q = p^s$. Our procedure to obtain stabilizer quantum codes over $\mathbb{F}_q = \mathbb{F}_{p^s}$, using Theorem 1, consists of considering subfield-subcodes over $\mathbb{F}_{p^{2s}} = \mathbb{F}_{q^2}$ of classical linear codes over over $\mathbb{F}_{p^{2r}} = \mathbb{F}_{q^{2n}}$.

The *trace polynomial* over $\mathbb{F}_{p^{2r}} = \mathbb{F}_{q^{2n}}$ with respect to $\mathbb{F}_{p^s} = \mathbb{F}_q$ is defined as

$$\mathrm{tr}_{2r}^s(X) = X + X^q + X^{q^2} + \cdots + X^{q^{2n-1}},$$

whose attached polynomial function (*trace map*) will be denoted by $\mathrm{tr}_{2r}^s : \mathbb{F}_{q^{2n}} \to \mathbb{F}_q$.

It is well-known that the trace map is a linear transformation over $\mathbb{F}_q$ and any linear transformation $\mathbb{F}_{q^{2n}} \to \mathbb{F}_q$ is defined by $x \mapsto \mathrm{tr}_{2r}^s(\beta x)$, for some $\beta \in \mathbb{F}_{q^{2n}}$. Another interesting property of the trace map is that

$$\mathrm{card}\left\{\alpha \in \mathbb{F}_{q^{2n}} | \mathrm{tr}_{2r}^s(\alpha) = a\right\}$$

equals q^{2n-1} for all $a \in \mathbb{F}_q$, and therefore, when α runs over $\mathbb{F}_{q^{2n}}$, one has that $\mathrm{tr}_{2r}^s(\alpha)$ takes each value of $\mathbb{F}_q$ exactly q^{2n-1} times. This fact gives rise to the decomposition

$$\mathrm{tr}_{2r}^s(X) - a = \prod_{\alpha \in \mathbb{F}_{q^{2n}}, \mathrm{tr}_{2r}^s(\alpha) = a} (X - \alpha)$$

and, as a consequence,

$$X^{q^{2n}} - X = \prod_{a \in \mathbb{F}_q} \left(\mathrm{tr}_{2r}^s(X) - a\right).$$

Consider now the ideal of the polynomial ring $\mathbb{F}_{q^{2n}}[X]$ generated by $\mathrm{tr}_{2r}^s(X)$, which, by the previous discussion, can also be regarded as the ideal generated by both polynomials $X^{q^{2n}} - X$ and $\mathrm{tr}_{2r}^s(X)$. Consider also

$$Z = \{\alpha \in \mathbb{F}_{q^{2n}} | \mathrm{tr}_{2r}^s(\alpha) = 0\} = \{\alpha_1, \alpha_2, \ldots, \alpha_N\},$$

where $N = q^{2n-1}$.

Next, we define the evaluation map that supports our codes:

$$\begin{array}{rl} \mathrm{ev}_{\mathrm{tr}_{2r}^s}: & \mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^s(X)\rangle \longrightarrow \mathbb{F}_{q^{2n}}^N \\ & f \longmapsto (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_N)), \end{array} \tag{1}$$

where f denotes both the class in $\mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^s(X)\rangle$ and a polynomial in $\mathbb{F}_{q^{2n}}[X]$ representing that class. Notice that we have proved that the map $\mathrm{ev}_{\mathrm{tr}_{2r}^s}$ is well-defined.

Our codes will take advantage from the existing relations in the ring $\mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^s(X)\rangle$ (see Remark 14) and we will only need to evaluate monomials of degree less than q^{2n-1}.

Definition 2. Let $\mathcal{H} = \{0, 1, \ldots, q^{2n} - 2\}$ and for any non-empty subset $\Delta \subseteq \mathcal{H}$, we define the evaluation code $E_{\Delta, \mathrm{tr}_{2r}^s}$ in $\mathbb{F}_{q^{2n}}^N$, as the linear code generated by the set of vectors $\{\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^a) | a \in \Delta\}$.

We have considered such a set $\mathcal{H}$ because we will evaluate classes of polynomials of degree less than $q^{2n} - 1$ in our Theorems 8 and 15 when we consider the Hermitian inner product.

Proposition 3. *Assume that $\Delta \subseteq \{0, 1, \ldots, q^{2n-1} - 1\}$. Then the dimension of the code $E_{\Delta, \mathrm{tr}_{2r}^s}$ coincides with the cardinality of the set Δ.*

Proof. A generator matrix of the code consists of some rows of a Vandermonde matrix over the field $\mathbb{F}_{q^{2n}}$. These rows are linearly independent because q^{2n-1} is the degree of the polynomial $\mathrm{tr}_{2r}^s(X)$ and $q^{2n-1} - 1$ is the maximum degree of the involved monomials. □

Stabilizer quantum codes can be constructed from classical self-orthogonal codes with respect to the Hermitian inner product. Since, in this section, we are getting quantum codes over $\mathbb{F}_{q^n}$ from linear codes over $\mathbb{F}_{q^{2n}}$, we will consider the Hermitian inner product of two vectors $\mathbf{a} = (a_1, a_2, \ldots a_N)$ and $\mathbf{b} = (b_1, b_2, \ldots b_N)$ in $\mathbb{F}_{q^{2n}}^N$ defined as

$$\mathbf{a} \cdot_h \mathbf{b} := \sum_{j=1}^{N} a_j b_j^{q^n}.$$

Hence, we will look for self-orthogonal codes $E_{\Delta, \mathrm{tr}_{2r}^s}$ with respect to this inner product, that is codes which satisfy

$$E_{\Delta, \mathrm{tr}_{2r}^s} \subseteq \left(E_{\Delta, \mathrm{tr}_{2r}^s}\right)^{\perp_h},$$

where $(E_{\Delta, \mathrm{tr}_{2r}^s})^{\perp_h} = \{\mathbf{b} \in \mathbb{F}_{q^{2n}}^N | \mathbf{a} \cdot_h \mathbf{b} = 0, \ \forall\ \mathbf{a} \in E_{\Delta, \mathrm{tr}_{2r}^s}\}$.

The Euclidean inner product will be used in our development as well. For $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_{q^{2n}}^N$, it is defined as $\mathbf{a} \cdot \mathbf{b} := \sum_{j=1}^{N} a_j b_j$. We start with a lemma which will allow us to derive the first result on the orthogonality of the generators of our codes.

Lemma 4. *Let f be a polynomial in $\mathbb{F}_{q^{2n}}[X]$ of degree m, $f = \sum_{j=1}^{m} a_j X^j$ with $a_m = 1$. Assume that f has m roots $\{x_1, x_2, \ldots, x_m\}$ in $\mathbb{F}_{q^{2n}}$. Denote by s_k, $1 \leq k \leq m$, the power sum $s_k = \sum_{j=1}^{m} x_j^k$. Then*

$$\left(\sum_{j=0}^{i-1} a_{m-j} s_{i-j}\right) + i a_{m-i} = 0, \tag{2}$$

when $i \leq m$. Otherwise ($i > m$), it holds

$$\sum_{j=0}^{m-1} a_{m-j} s_{i-j} = 0.$$

Proof. It suffices to consider that the elementary symmetric elements σ_k, $1 \leq k \leq m$:

$$\sigma_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$$

and the Newton identities [9, proof of Theorem 8 in Chapter 7, Section 1] prove that

$$s_k + \sum_{i=1}^{k-1} (-1)^i \sigma_i s_{k-i} + (-1)^k k \sigma_k = 0,$$

when $1 \leq k \leq m$. Moreover, for $k > m$,

$$s_k + \sum_{i=1}^{m} (-1)^i \sigma_i s_{k-i} = 0.$$

Finally, the result holds since $a_j = (-1)^{m-j} \sigma_{m-j}$ [9, Problem 4 in Chapter 7, Section 1]. □

We desire to study the metric structure of our codes. As we will see in Theorem 8, to characterize when the inner product of the evaluation of two monomials vanishes, it is sufficient to study the product of the evaluation of one monomial and the all ones vector. Thus, we consider the following two propositions. The first one for the classes of monomials in $\mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^s(X) \rangle$, and the second one, for those that arise when one considers the Hermitian inner product.

Proposition 5. *With the above notations, recall that $p^{2r} = q^{2n}$, one has that the map in (1) satisfies*

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^k) \cdot \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^0) = 0,$$

for $1 \leq k < q^{2n-1} - 1$ and

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^{q^{2n-1}-1}) \cdot \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^0) \neq 0.$$

Proof. This result is a consequence of Lemma 4. Namely, notice that, with the notation as in Lemma 4, $\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^k) \cdot \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^0) = s_k$, where one will consider the polynomial $\mathrm{ev}_{\mathrm{tr}_{2r}^s}$ instead of f and N instead of m. In addition, all the coefficients a_j are equal to zero, but $a_1, a_q, a_{q^2}, \ldots, a_{q^{2n-1}}$ which are equal to 1. Now Formula (2) with $i = 1$ proves that $s_1 = -a_{N-1} = 0$; with $i = 2$, $s_2 = -2a_{N-2} = 0$, and iterating the same argument for consecutive values, one has that $s_k = 0$ for indices $1 \leq k < q^{2n-1} - q^{2n-2}$. Again Formula (2), for $i = q^{2n-1} - q^{2n-2}$, proves that $s_{q^{2n-1}-q^{2n-2}} = 0$ since we work over a field of characteristic p. It is clear that the same procedure proves that $s_k = 0$ for $1 \leq k < q^{2n-1} - 1$.

Finally $s_{q^{2n-1}-1} \neq 0$, because Formula (2) for $i = q^{2n-1} - 1$ shows that

$$s_{q^{2n-1}-1} + a_{q^{2n-1}-1} s_{q^{2n-1}-2} + \cdots + a_1(q^{2n-1} - 1) = 0,$$

and then $s_{q^{2n-1}-1} = -(q^{2n-1} - 1) = 1 \neq 0$, which concludes the proof. □

The map $\mathrm{ev}_{\mathrm{tr}_{2r}^s}$ is defined for elements in $\mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^s(X) \rangle$ which have as class representatives, polynomials of degree lower than q^{2n-1}. Proposition 5 shows that the evaluation by $\mathrm{ev}_{\mathrm{tr}_{2r}^s}$ of a (class of a) polynomial f in $\mathbb{F}_{q^{2n}}[X]$ is Euclidean orthogonal to $\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^0)$ if and only if the mentioned representative does not contain the monomial $X^{q^{2n-1}-1}$. This proves the following result which complements Proposition 5.

Proposition 6. *With the above notation, for $k \in \mathcal{H}$, the Euclidean inner product*

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^k) \cdot \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^0) = 0$$

if and only if the polynomial of degree less than q^{2n-1} representing the class $X^k + \langle \mathrm{tr}_{2r}^s(X) \rangle$ does not contain the monomial $X^{q^{2n-1}-1}$.

Next, we give a condition, whose proof can be found in Appendix A, implying that some classes as above do not contain $X^{q^{2n-1}-1}$ in their representatives.

Proposition 7. *With the above notation, let i, j be integers such that $(i, j) \neq (0, 0)$ and*

$$0 \leq i, j < q^n - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{n-1} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1.$$

Then, for $0 < m \leq n$, the representative of the class $X^{i+jq^m} + \langle \mathrm{tr}_{2r}^s(X) \rangle$ of degree less than q^{2n-1} does not contain the monomial $X^{q^{2n-1}-1}$.

We conclude this section with a result which gives the parameters of the quantum codes constructed from Hermitian duals of certain codes $E_{\Delta, \mathrm{tr}_{2r}^s}$. These codes are MDS quantum codes and they were also found in [28], [31].

Theorem 8. *Let p be a prime number, r and s positive integers such that $r = s \cdot n$, $n \geq 1$ and set $q = p^s$. Let t be a nonnegative integer such that*

$$t < q^n - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{n-1} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1$$

and write $\Delta(t) = \{a \in \mathbb{Z} \mid 0 \leq a \leq t\}$. Then, the following inclusion holds:

$$E_{\Delta(t), \mathrm{tr}_{2r}^s} \subseteq \left(E_{\Delta(t), \mathrm{tr}_{2r}^s} \right)^{\perp_h}.$$

As a consequence, we are able to construct a stabilizer (quantum) MDS code with parameters $[[N, N - 2t - 2, t + 2]]_{q^n}$.

Proof. Propositions 6 and 7 for $m = n$ show that

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^i) \cdot_h \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^j) = \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^{i+jq^n}) \cdot \mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^0) = 0,$$

where the monomials X^i and X^j are representatives of classes in $\mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^s(X) \rangle$ and $i, j \in \Delta(t)$. This proves the codes' inclusion. The dimension of the stabilizer code is clear from Proposition 3 and Theorem 1. Finally, we use Theorem 1 again for bounding the distance of the stabilizer code. Indeed, by Proposition 5 the code $\left(E_{\Delta(t), \mathrm{tr}_{2r}^s} \right)^{\perp}$ contains the image by $\mathrm{ev}_{\mathrm{tr}_{2r}^s}$ of consecutive monomials X^j, $0 \leq j \leq (N-1) - (t+1)$, because $E_{\Delta(t), \mathrm{tr}_{2r}^s}$ is the code generated by $\mathrm{ev}_{\mathrm{tr}_{2r}^s}(X^i)$, $0 \leq i \leq t$. Thus, the minimum distance of the code is at least $t + 2$ but it cannot be larger than the Singleton bound. This concludes the proof after noticing that Hermitian and Euclidean dual codes are isometric, which can be deduced from the fact that, in our case, the Euclidean dual of a code coincides with the q^nth power of its Hermitian dual. □

III. Subfield-subcodes of evaluation codes

In this section, we will consider subfield subcodes of one-variable J-affine variety codes with $J = \emptyset$. J-affine variety codes have been introduced and used in [14], [15], [16], [17] to provide quantum codes. We refer the reader to these references for further details.

We recall that p is a prime number, r and s are positive integers such that $s | r$, $r = s \cdot n$ and $q = p^s$. Let $M = p^{2r} = q^{2n}$ and consider the map

$$\mathrm{ev}' : \mathbb{F}_{q^{2n}}[X]/\langle X^M - X \rangle \longrightarrow \mathbb{F}_{q^{2n}}^M$$

defined by

$$\mathrm{ev}'(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_M)),$$

where $\{\alpha_1, \alpha_2, \ldots, \alpha_M\}$ is the set of zeros of the polynomial $X^M - X$ in $\mathbb{F}_{q^{2n}}$. Note that $Z \subset \mathbb{F}_{q^{2n}}$ by Section II. Let $\Delta \subseteq \{0, 1, \ldots, M-1\}$, we define the evaluation code $D_\Delta \subseteq \mathbb{F}_{q^{2n}}^M$ as the linear space generated by the vectors $\{\mathrm{ev}'(X^a) \mid a \in \Delta\}$. For $\Delta = \{0, 1, \ldots, k-1\}$ we have a Reed-Solomon code with length q^{2n} and dimension k. In general, the dimension of D_Δ is equal to the cardinality of the set Δ.

Let $\mathcal{H}^T = \{0\} \cup \{1, 2, \ldots, M-1\}$, where $\{1, 2, \ldots, M-1\}$ is regarded as a set of representatives of the congruence ring $\mathbb{Z}_{M-1} = \mathbb{Z}/(M-1)\mathbb{Z}$, and consider cyclotomic cosets with respect to q^2 defined as subsets $\mathfrak{I} \subseteq \mathcal{H}^T$ such that $q^2 a \in \mathfrak{I}$ for all $a \in \mathfrak{I}$. A cyclotomic coset $\mathfrak{I}$ as above is said to be *minimal* whenever its elements are those that can be expressed as aq^{2i}, for some nonnegative integer i and some fixed element $a \in \mathfrak{I}$. We represent each minimal cyclotomic coset $\mathfrak{I}$ by that element a in $\mathcal{H}^T$ which is the minimum in $\mathfrak{I}$ and then we write $\mathfrak{I} = \mathfrak{I}_a$. This set of representatives will be denoted by $\mathcal{A}$ and so $\{\mathfrak{I}_a\}_{a \in \mathcal{A}}$ is the family of minimal cyclotomic cosets in $\mathcal{H}^T$.

Next, we consider a different trace map,

$$\mathrm{tr}_{2r}^{2s} : \mathbb{F}_{p^{2r}} (:= \mathbb{F}_{q^{2n}}) \longrightarrow \mathbb{F}_{p^{2s}} (:= \mathbb{F}_{q^2}),$$

defined as

$$\mathrm{tr}_{2r}^{2s}(x) = x + x^{q^2} + \cdots + x^{q^{2(n-1)}},$$

and let

$$\mathcal{T} : \mathbb{F}_{q^{2n}}[X]/\langle X^M - X\rangle \to \mathbb{F}_{q^{2n}}[X]/\langle X^M - X\rangle$$

be the map given by $\mathcal{T}(f) = f + f^{q^2} + \cdots + f^{q^{2(n-1)}}$. This last map satisfies the following result whose proof is identical to that of [14, Proposition 5].

Proposition 9. *Let f be an element in $\mathbb{F}_{q^{2n}}[X]/\langle X^M - X\rangle$. Then, the following conditions are equivalent:*

1) *$f = \mathcal{T}(h)$ for some $h \in \mathbb{F}_{q^{2n}}[X]/\langle X^M - X\rangle$.*
2) *$f^{q^2} = f$.*
3) *f evaluates to $\mathbb{F}_{q^2}$, that is $\mathrm{ev}'(f) \in (\mathbb{F}_{q^2})^M$.*

The above result shows that one can get codes of length M over $\mathbb{F}_{q^2}$ from the images $\mathrm{ev}'(\mathcal{T}(h))$ of classes of polynomials $h \in \mathbb{F}_{q^{2n}}[X]$.

Now, we are going to consider *subfield-subcodes* E^σ over the field $\mathbb{F}_{q^2}$ of evaluation codes E of certain length $\mathcal{N}$ over $\mathbb{F}_{q^{2n}}$. Recall that E^σ is the set of elements in E whose coordinates belong to $\mathbb{F}_{q^2}$, that is $E^\sigma = E \cap (\mathbb{F}_{q^2})^{\mathcal{N}}$. Our first result holds for any linear code E as above.

Lemma 10. *Let E be a linear code over $\mathbb{F}_{q^{2n}}$ and E^σ its subfield-subcode over $\mathbb{F}_{q^2}$. Then $(E^\sigma)^\perp = \left(E^\perp\right)^\sigma$ if and only if, E has a basis whose vectors have coordinates in $\mathbb{F}_{q^2}$.*

Proof. Assume first that E has a basis whose coordinates are in $\mathbb{F}_{q^2}$. By [34, Lemma 1], this fact is equivalent to the invariance of E by the action of the Galois group of $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_{q^2}$ and, also, to the invariance of the dual code $E^\perp$ by the action of the same group. Delsarte Theorem [10] proves that

$$(E^\sigma)^\perp = \mathbf{tr}_{2r}^{2s}\left(E^\perp\right),$$

where $\mathbf{tr}_{2r}^{2s}$ consists of applying tr_{2r}^{2s} componentwise. It is clear that $\mathbf{tr}_{2r}^{2s}\left(E^\perp\right) \supseteq \left(E^\perp\right)^\sigma$. Hence, it remains to prove the opposite inclusion. As we have said, we can pick a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k\}$ of $E^\perp$ whose coordinates are in $\mathbb{F}_{q^2}$. Let $\mathbf{a} \in E^\perp$, then $\mathbf{a} = \sum_{i=1}^k \alpha_i \mathbf{a}_i$ with $\alpha_i \in \mathbb{F}_{q^{2n}}$ and

$$\mathbf{tr}_{2r}^{2s}(\mathbf{a}) = \sum_{i=1}^{k} \mathrm{tr}_{2r}^{2s}(\alpha_i)\mathbf{a}_i,$$

which holds because the trace is additive and linear over $\mathbb{F}_{q^2}$. This concludes the proof because $\mathrm{tr}_{2r}^{2s}(\alpha_i) \in \mathbb{F}_{q^2}$ and the coordinates of each vector $\mathbf{a}_i$, $1 \le i \le k$, are also in $\mathbb{F}_{q^2}$.

For the converse, suppose that $(E^\sigma)^\perp = \left(E^\perp\right)^\sigma$, which means by Delsarte Theorem that

$$\mathbf{tr}_{2r}^{2s}\left(E^\perp\right) = \left(E^\perp\right)^\sigma \subseteq E^\perp.$$

Now $\dim \mathbf{tr}_{2r}^{2s}\left(E^\perp\right) = \dim E^\perp$. Indeed, it suffices to prove that $\dim \mathbf{tr}_{2r}^{2s}\left(E^\perp\right) \geq \dim E^\perp$ and to do it, consider $\alpha \in \mathbb{F}_{q^{2n}}$ such that $\mathrm{tr}_{2r}^{2s}(\alpha) = 1$ and a basis B of $E^\perp$ obtained by considering α times each vector of a standard basis of $E^\perp$. Then applying $\mathbf{tr}_{2r}^{2s}$ to each vector in B one obtains a set of linearly independent vectors in $\mathbf{tr}_{2r}^{2s}\left(E^\perp\right)$. As a consequence, we get a basis of $\mathbf{tr}_{2r}^{2s}\left(E^\perp\right)$ which is also a basis of $E^\perp$ and, thus, has coordinates in $\mathbb{F}_{q^2}$. This concludes the proof because the same holds for E by [34, Lemma 1]. □

The classical codes we will use in this paper satisfy the conditions in the above lemma. For a start we need the following notation: i_a denotes the cardinality of the minimal cyclotomic coset $\mathfrak{I}_a$ and, since i_a divides n, the mapping for polynomials f with support on a cyclotomic coset $\mathfrak{I}_a$

$$\mathcal{T}_a(f) = f + f^{q^2} + \cdots + f^{q^{2(i_a-1)}},$$

evaluates to $\mathbb{F}_{q^2}$.

Let D_Δ^σ be the subfield subcode of D_Δ over $\mathbb{F}_{q^2}$, i.e.

$$D_\Delta^\sigma := D_\Delta \cap \left(\mathbb{F}_{q^2}\right)^M.$$

Let $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 \cdots < a_z\}$ the above mentioned set of representatives of minimal cyclotomic sets of $\mathcal{H}^T$ with respect to q^2. For $t \leq z$, define

$$\Delta^\sigma(t) := \mathfrak{I}_{a_0} \cup \mathfrak{I}_{a_1} \cup \cdots \cup \mathfrak{I}_{a_t}.$$

Then,

Proposition 11. *With the above notations, one has that*

$$\left(D_{\Delta^\sigma(t)}^\sigma\right)^\perp = \left(D_{\Delta^\sigma(t)}^\perp\right)^\sigma.$$

Proof. By Lemma 10, it suffices to prove that $D_{\Delta^\sigma(t)}$ has a basis with coordinates in $\mathbb{F}_{q^2}$. Recall that $D_{\Delta^\sigma(t)}$ is generated, as a $\mathbb{F}_{q^{2n}}$ vector space, by $\mathrm{ev}'(\mathcal{A})$, where $\mathcal{A}$ is the following set of monomials

$$\mathcal{A} = \bigcup_{i=0}^{t} \left\{X^{a_i}, X^{a_i q^2}, \ldots, X^{a_i q^{2(i_{a_i}-1)}}\right\}.$$

We are going to give another set of polynomials $\mathcal{B}$, with the same cardinality as $\mathcal{A}$, that are linearly independent over the field $\mathbb{F}_{q^2}$ which, by Proposition 9, will evaluate to $\mathbb{F}_{q^2}$. As a consequence, we get a basis of $D_{\Delta^\sigma(t)}$ whose vectors are in $\left(\mathbb{F}_{q^2}\right)^M$ and the proof is concluded.

Consider defining elements β_i, $0 \leq i \leq t$, of the field $\mathbb{F}_{q^{2i_{a_i}}}$ over $\mathbb{F}_{q^2}$ (i.e., elements such that $\{1, \beta_i, \ldots, \beta_i^{i_{a_i}-1}\}$ is a basis of $\mathbb{F}_{q^{2i_{a_i}}}$ over $\mathbb{F}_{q^2}$) and set

$$\mathcal{B} = \bigcup_{i=0}^{t} \left\{\mathcal{T}_{a_i}(X^{a_i}), \mathcal{T}_{a_i}(\beta_i X^{a_i}), \ldots, \mathcal{T}_{a_i}(\beta_i^{i_{a_i}-1} X^{a_i})\right\}.$$

To prove the independence over $\mathbb{F}_{q^2}$ of the vectors in $\mathcal{B}$, it suffices to check it for each subset attached to an index i. Now, set, for simplicity, $a_i = a$ and $\beta_i = \beta$, and, by contradiction, suppose $\sum_{\ell=0}^{i_a-1} \alpha_\ell \mathcal{T}_a(\beta^\ell X^a) = 0$ for some elements $\alpha_\ell \in \mathbb{F}_{q^2}$ which are not all zero. Then the term corresponding to the monomial X^a has $\alpha_0 + \alpha_1\beta + \cdots + \alpha_{i_a-1}\beta^{i_a-1}$ as a coefficient and then β is a root of a polynomial with coefficients in $\mathbb{F}_{q^2}$ of degree $i_a - 1$, which is a contradiction because the minimal polynomial of β has degree i_a. □

Notice that as a consequence of Proposition 11, the minimum distance of the dual code of $D_{\Delta^\sigma(t)}^\sigma$, is greater than or equal to $a_{t+1} + 1$ (BCH bound).

Example 1. Let $p = 2$, $s = 1$ and $r = 4$. Hence, we will consider codes over $\mathbb{F}_{2^8}$ and subfield-subcodes over $\mathbb{F}_{2^2}$ with length $M = 256$. The first eight minimal cyclotomic cosets are $\mathfrak{I}_0 = \{0\}$, $\mathfrak{I}_1 = \{1, 4, 16, 64\}$, $\mathfrak{I}_2 = \{2, 8, 32, 128\}$, $\mathfrak{I}_3 = \{3, 12, 48, 192\}$, $\mathfrak{I}_5 = \{5, 20, 65, 80\}$, $\mathfrak{I}_6 = \{6, 24, 12, 129\}$, $\mathfrak{I}_7 = \{7, 28, 112, 193\}$ and $\mathfrak{I}_9 = \{9, 36, 66, 144\}$. Hence we have that $a_0 = 0$, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 5$, $a_5 = 6$, $a_6 = 7$, $a_7 = 9$.

Consider $\Delta^\sigma(6) = \mathfrak{I}_{a_0} \cup \mathfrak{I}_{a_1} \cup \cdots \cup \mathfrak{I}_{a_6}$. Then, the dual code of $D^\sigma_{\Delta^\sigma(t)}$ has parameters

$$\begin{aligned}\left[M, M - \sum_{l=0}^{6} i_{a_l}, \geq a_7 + 1\right]_4 &= [256, 256 - 25, \geq 10]_4 \\ &= [256, 231, \geq 10]_4.\end{aligned}$$

IV. Stabilizer codes obtained from subfield-subcodes of Evaluation Codes at the Trace Roots

The aim of this section is to study subfield-subcodes over $\mathbb{F}_{q^2}$ of some codes introduced in Section II and determine the parameters for their attached stabilizer quantum codes over $\mathbb{F}_q$. Keep the notation as in that section.

Definition 12. Let $\emptyset \neq \Delta \subseteq \mathcal{H}$, the subfield-subcode over $\mathbb{F}_{q^2}$ of the code $E_{\Delta,\mathrm{tr}^s_{2r}}$ is defined as

$$E^\sigma_{\Delta,\mathrm{tr}^s_{2r}} := E_{\Delta,\mathrm{tr}^s_{2r}} \cap \mathbb{F}^N_{q^2}.$$

The same reasoning that proves Proposition 9 shows that the map $\mathrm{ev}_{\mathrm{tr}^s_{2r}}$ applied to classes of polynomials $\mathcal{T}(f)$ (and $\mathcal{T}_a(f)$) evaluates to $\mathbb{F}_{q^2}$, where $N = q^{2n-1} = p^{2r-s}$. Moreover, considering subfield subcodes of codes defined by the above sets $\Delta^\sigma(t)$, we can bound their parameters. Recall that $\mathcal{A} = \{a_0 = 0 < a_1 < a_2 \cdots < a_z\}$ and, for $t \leq z$,

$$\Delta^\sigma(t) := \mathfrak{I}_{a_0} \cup \mathfrak{I}_{a_1} \cup \cdots \cup \mathfrak{I}_{a_t}.$$

Then,

Theorem 13. *The dimension of $E^\sigma_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}}$ and the minimum distance of its Hermitian dual code satisfy the following bounds:*

$$\dim\left(E^\sigma_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}}\right) \leq \sum_{l=0}^{t} i_{a_l},$$

$$d\left(E^\sigma_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}}\right)^{\perp_h} \geq a_{t+1} + 1.$$

Proof. By the proof of Proposition 11, we have that $\dim\left(D^\sigma_{\Delta^\sigma(t)}\right) = \sum_{l=0}^{t} i_{a_l}$. Since we only evaluate at the zeros of the polynomial $\mathrm{tr}^s_{2r}(X)$ ($Z \subset \mathbb{F}_M$), the first inequality holds.

With respect to the last inequality, setting $A = \{0, 1, \ldots, a_{t+1} - 1\}$, it holds that $A \subseteq \Delta^\sigma(t)$ and then one gets the inclusion of codes in $\mathbb{F}_{q^{2n}}$: $E_{A,\mathrm{tr}^s_{2r}} \subseteq E_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}}$. Thus, the Euclidean dual of both codes satisfy

$$(E_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}})^\perp \subseteq (E_{A,\mathrm{tr}^s_{2r}})^\perp.$$

Therefore,

$$d\left((E_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}})^\perp\right) \geq d\left(E^\perp_{A,\mathrm{tr}^s_{2r}}\right) \geq a_{t+1} + 1,$$

because the parity check matrix of $E^\perp_{A,\mathrm{tr}^s_{2r}}$ corresponds with the generator matrix of $E_{A,\mathrm{tr}^s_{2r}}$, which is a Vandermonde matrix. Considering subfield-subcodes over $\mathbb{F}_{q^2}$ and by Lemma 10 and the proof of Proposition 11, we have that

$$\left(E^\sigma_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}}\right)^\perp = \left(E^\perp_{\Delta^\sigma(t),\mathrm{tr}^s_{2r}}\right)^\sigma \subseteq \left(E^\perp_{A,\mathrm{tr}^s_{2r}}\right)^\sigma.$$

Then,

$$\begin{aligned} d\left(E^{\sigma}_{\Delta^{\sigma}(t),\mathrm{tr}^s_{2r}}\right)^{\perp} &= d\left(E^{\perp}_{\Delta^{\sigma}(t),\mathrm{tr}^s_{2r}}\right)^{\sigma} \\ &\geq d\left(E^{\perp}_{A,\mathrm{tr}^s_{2r}}\right)^{\sigma} \geq a_{t+1}+1. \end{aligned}$$

This concludes the proof because the Euclidean and Hermitian dual of our codes are isometric. □

Example 2. Let $p=2$, $s=1$ and $r=4$, that is $q=2$ and $n=4$. We will consider a code over $\mathbb{F}_{2^8}$ and a subfield-subcode over $\mathbb{F}_{2^2}$ as in Example 1. We have that $N=128$ and consider again $\Delta^{\sigma}(6)=\mathfrak{I}_{a_0}\cup\mathfrak{I}_{a_1}\cup\cdots\cup\mathfrak{I}_{a_6}$. The code $\left(E^{\sigma}_{\Delta^{\sigma}(6),\mathrm{tr}^s_{2r}}\right)^{\perp_h}$ has parameters

$$\begin{aligned} \left[N, \geq N-\sum_{l=0}^{6} i_{a_l}, \geq a_7+1\right]_4 &= [128, \geq 128-25, \geq 10]_4 \\ &= [128, \geq 103, \geq 10]_4. \end{aligned}$$

Moreover, we know that the dimension is strictly greater than 103 since $\mathcal{T}_1(X)$ and $\mathcal{T}_2(X)$ are equal modulo $\mathrm{tr}^1_8(X)$, because $\mathcal{T}_1(X)=X+X^4+X^{16}+X^{64}$, $\mathcal{T}_2(X)=X^2+X^8+X^{32}+X^{128}$, and $\mathrm{tr}^1_8(X)=X+X^2+X^4+X^8+X^{16}+X^{32}+X^{64}+X^{128}$. Actually one can prove that the code $\left(E^{\sigma}_{\Delta^{\sigma}(6),\mathrm{tr}^s_{2r}}\right)^{\perp_h}$ has parameters $[128,104,10]_4$.

Remark 14. Examples 1 and 2 help to illustrate how to compare the codes obtained in the previous section –extended BCH codes (or subfield-subcodes of J-affine variety codes with $J=\emptyset$)– with subfield-subcodes of evaluation codes at the trace roots. When considering dual codes, the advantage of the last code can be observed from the difference between the length and dimension since both codes have the same designed minimum distance. First observe that such a difference is equal to $\sum_{l=0}^{t} i_{a_l}$ in both cases (25 in our examples), however for the evaluation codes at the trace roots we have an advantage: their dimension may be strictly greater than the designed dimension $N-\sum_{l=0}^{t} i_{a_l}$, as the previous example shows. This will allow us to get classical and quantum codes with excellent parameters. In general, there may be several relations modulo $\mathrm{tr}^s_{2r}(X)$ among the polynomials in the set $\mathcal{B}$ in the proof of Proposition 11, which increase the dimension of $\left(E^{\sigma}_{\Delta^{\sigma}(t),\mathrm{tr}^s_{2r}}\right)^{\perp_h}$.

We conclude this section with our main result that shows how to construct stabilizer codes from subfield-subcodes over $\mathbb{F}_{p^{2s}}$. Recall that $\mathbb{F}_{q^2}=\mathbb{F}_{p^{2s}}$.

Theorem 15. *Let $N=q^{2n-1}$ the degree of the polynomial $\mathrm{tr}^s_{2r}(X)$, $M=q^{2n}$ and $\mathcal{A}=\{a_0=0<a_1<a_2\cdots<a_z\}$ the set of representatives of the minimal cyclotomic sets $\mathfrak{I}_{a_i}$, $0\leq i\leq z$, of $\mathcal{H}^T$ with respect to q^2. Let $t\leq z$ be an index such that*

$$a_t < q^n - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{n-1} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1.$$

Then, with the notation as above, the following inclusion holds

$$E^{\sigma}_{\Delta^{\sigma}(t),\mathrm{tr}^s_{2r}} \subseteq \left(E^{\sigma}_{\Delta^{\sigma}(t),\mathrm{tr}^s_{2r}}\right)^{\perp_h}, \tag{3}$$

where $\Delta^{\sigma}(t)=\mathfrak{I}_{a_0}\cup\mathfrak{I}_{a_1}\cup\cdots\cup\mathfrak{I}_{a_t}$.

As a consequence, we are able to construct a stabilizer code with parameters

$$\left[\left[N, \geq N-2\sum_{a=0}^{t} i_a, \geq a_{t+1}+1\right]\right]_q.$$

Proof. By Theorem 13, it suffices to prove the inclusion in (3). We shall show that

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(\mathcal{T}_{a_i}(\beta_i^{k_i}X^{a_i})\right)\cdot_h \mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(\mathcal{T}_{a_j}(\beta_j^{k_j}X^{a_j})\right)=0, \tag{4}$$

for β_i (respectively, β_j) a defining element of $\mathbb{F}_{q^{2i_{a_i}}}$ (respectively, in $\mathbb{F}_{q^{2i_{a_j}}}$) over $\mathbb{F}_{q^2}$, for $0\leq k_i\leq i_{a_i}-1$ (respectively, $0\leq k_j\leq i_{a_j}-1$) and $i,j\in\{0,1,\ldots,t\}$. This will conclude the proof by Proposition 11.

Our codes are over $\mathbb{F}_{q^2}$ and in this case $\mathbf{a}\cdot_h\mathbf{b}=\sum_{i=1}^N a_ib_i^q$. Then, the left hand side in (4) is a summation, up to constants that depend on β_i and β_j, of Euclidean products of the form

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{aq^l+bqq^m}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right), \tag{5}$$

where, for simplicity's sake, we write a,b for the corresponding representatives in $\mathcal{A}$. By hypothesis,

$$a,b<q^n-\lfloor\frac{(q-1)}{2}\rfloor q^{n-1}-\cdots-\lfloor\frac{(q-1)}{2}\rfloor q-1$$

and from the definition of $\mathcal{T}_a$ and $\mathcal{T}_b$, $l,m\in\{0,1,\ldots,2n-1\}$.

We claim that each product of the form given in (5) equals zero, which proves Equality (4). Indeed, without loss of generality, we may assume that $m\geq l$ and divide the proof in two parts.

First, suppose that $m-l\leq n-1$. Then

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{aq^l+bqq^m}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right)=$$
$$\left(\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{a+bq^{m-l+1}}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right)\right)^{q^l}, \tag{6}$$

because of the characteristic of the field. Now, Proposition 7 proves that the right hand side of Equality (6) is equal to zero since $m-l+1\leq n$, which concludes the first part.

Finally, assume that $m-l\geq n$, then

$$l\leq m-n\leq(2n-1)-n=n-1$$

and $m=n+n_1\leq 2n-1$, thus $n_1<n$. In addition, Formula (5) is equal to zero if and only if

$$\left(\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{aq^l+bqq^{n+n_1}}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right)\right)^{q^n}$$

is equal to zero. This last expression can also be written as

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{aq^{l+n}+bq^{2n+n_1+1}}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right).$$

Since we are evaluating elements in the field $\mathbb{F}_{p^{2r}}=\mathbb{F}_{q^{2n}}$, it suffices to prove

$$\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{aq^{l+n}+bq^{n_1+2}}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right)=0, \tag{7}$$

which holds whenever

$$\left(\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^{aq^{l+n-n_1-2}+b}\right)\cdot\mathrm{ev}_{\mathrm{tr}_{2r}^s}\left(X^0\right)\right)^{q^{n_1+2}}$$

is equal to zero. Note that this holds by Proposition 7 since $l+n-n_1-2<n$. In fact, $n+n_1-l>n>n-1$ and then $l-n_1-1<0$. This concludes the proof. □

Example 3. Let $p=2$, $s=1$, $r=4$, $n=4$ and $q=2$. Consider the classical subfield-subcode over $\mathbb{F}_4$, $E^{\sigma}_{\Delta^{\sigma}(6),\mathrm{tr}_{2r}^s}$, given in Example 2. Since

$$\begin{aligned}a_6 &= 7 < 15 = 2^4-1\\ &= q^n-\left\lfloor\frac{(q-1)}{2}\right\rfloor q^{n-1}-\cdots-\left\lfloor\frac{(q-1)}{2}\right\rfloor q-1,\end{aligned}$$

we can apply Theorem 15 and therefore it is self-orthogonal with respect to the Hermitian inner product. Its Hermitian dual has parameters $[128, 104, 10]_4$, therefore, by Theorem 1, we obtain a stabilizer code with parameters $[[128, 2 \cdot 104 - 128, 10]]_2 = [[128, 80, 10]]_2$. This code is a record at [19] as we will see in Example 4 in Section V.

To end this section, we consider another construction of linear codes: we have shown that $\mathrm{ev}_{\mathrm{tr}_{2r}^s}$ evaluates at the points in Z, which is a subset of the zero-set of $X^{q^{2n}} - X$. By [16, Proposition 1], Proposition 6 also holds for the map ev' defined at Section III when, as above,

$$k < q^n - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{n-1} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1.$$

Since the set Z defined in Section II is included in $\mathbb{F}_{q^{2n}}$, considering the set $\mathbb{F}_{q^{2n}} \setminus Z = \{\gamma_1, \gamma_2, \ldots, \gamma_{N^C}\}$, where $N^C = M - N$, and the evaluation map

$$\mathrm{ev}^C : \frac{\mathbb{F}_{q^{2n}}[X]}{\langle (X^M - X)/\mathrm{tr}_{2r}^s(X) \rangle} \longrightarrow \mathbb{F}_{q^{2n}}^{N^C},$$

given by $\mathrm{ev}^C(f) = f(\gamma_1, \gamma_2, \ldots, \gamma_{N^C})$, one gets that, with the same reasoning, our results hold for these linear and stabilizer quantum codes as well. We will refer to these linear codes (respectively, their subfield-subcodes and the corresponding stabilizer codes) as *complementary codes* (respectively, their subfield-subcodes and the stabilizer codes obtained from them).

V. Examples

In this section we give the parameters of a number of stabilizer codes obtained or derived from our development. First, we recall that Theorem 15 shows how to use subfield-subcodes for constructing stabilizer codes over $\mathbb{F}_q$ with length $N = q^{2n-1}$, for $q = p^s$, where p is a prime number and s and n are positive integers. The same reasoning gives rise to codes of length $N - 1$, simply by not evaluating at the first element in the set Z in Section II (that is, at $\alpha_1 = 0$ or by not considering the coset $\mathfrak{I}_0$).

In addition, we emphasize that Theorem 15 determines stabilizer quantum codes with designed distance, and gives a lower bound for their dimension. In a large number of cases, the dimension of our codes is strictly larger than the bound given in Theorem 15. Note that, in contrast with the minimum distance, the computation of the dimension of a linear code is not computationally intense and can be easily performed.

In the first two examples, we will detail the different values of p, q, n and the considered length. However, for the sake of brevity and since it is straightforward to deduce them from the parameters of the codes, we do not give further details in the remaining examples. In Example 4, we obtain codes, both classical and quantum, that are records in [19]. For the rest of the examples there is no table of codes available to compare parameters (the previous table only contains binary stabilizer codes) and we indicate which codes exceed the quantum Gilbert-Varshamov bounds (QGVB, for short) [30], [13], [24].

Example 4. We consider the same setting as in examples 1, 2 and 3. Let $p = 2$, $s = 1$, $n = 4$. We obtain codes with length $q^{2n-1} = 2^7 = 128$ over $q^{2s} = 4$. As a consequence, we are able to get 52 linear codes over $\mathbb{F}_4$ improving the parameters in [19]. In fact, we obtain two linear codes with parameters $[128, 79, 20]_4$ and $[128, 75, 22]_4$ improving the previous best known linear codes $[128, 79, 19]_4$ and $[128, 75, 21]_4$. We are also able to construct a $[128, 85, 16]_4$ code (no construction was known for such parameters in [19]). Then, by shortening the above codes, we obtain 49 additional linear codes over $\mathbb{F}_4$ which are records at [19]. Their parameters can be found in Table I. For the sake of brevity we only display some of them because their parameters are clear from their construction.

By Theorem 1 these linear codes give rise to stabilizer quantum codes over $\mathbb{F}_2$, which are also records in the table [19]. We get stabilizer codes with parameters $[[128, 80, 10]]_2$ improving $[[128, 80, 9]]_2$; $[[128, 72, 11]]_2$ improving $[[128, 72, 10]]_2$; $[[128, 66, 12]]_2$ improving $[[128, 66, 11]]_2$ and $[[128, 58, 14]]_2$ improving $[[128, 58, 12]]_2$. Either puncturing or taking subcodes of the previous codes, we obtain binary stabilizer codes with parameters as in Table II.

n	k	d	n	k	d	n	k	d
127	78	20	126	77	20	125	76	20
124	75	20	$\cdots$	$\cdots$	$\cdots$	105	56	20
127	74	22	126	73	22	125	72	22
124	71	22	$\cdots$	$\cdots$	$\cdots$	108	55	22
127	84	16	126	83	16	125	82	16
124	81	16	123	80	16	122	79	16

TABLE I
LINEAR CODES OVER $\mathbb{F}_4$, OBTAINED BY SHORTENING, WHICH ARE RECORDS

n	k	d	n	k	d	n	k	d
128	79	10	127	80	9	128	71	11
128	65	12	128	64	12	128	63	12
128	57	14	128	56	14	128	55	14
127	58	13	127	57	13	127	56	13

TABLE II
QUANTUM CODES OVER $\mathbb{F}_2$ WHICH ARE RECORDS

Example 5. In this example, let $p = s = n = 2$. We get stabilizer (quantum) codes over $\mathbb{F}_4$. Some of these stabilizer codes with length $N = 64$, all of them with parameters that exceed the QGVB, are displayed in Table III.

n	k	d	n	k	d	n	k	d	n	k	d
64	58	3	64	54	4	64	50	5	64	48	6
64	44	7	64	40	8	64	36	9	64	34	10
64	30	11	64	26	12	64	22	13	64	20	14

TABLE III
STABILIZER CODES OVER $\mathbb{F}_4$ OF LENGTH 64

In the case where we do not evaluate at zero, their length is 63 and we get stabilizer codes over $\mathbb{F}_4$ with parameters as in Table IV. Again, all the parameters of the presented codes exceed the QGVB.

n	k	d	n	k	d	n	k	d	n	k	d
63	59	3	63	55	4	63	51	5	63	49	6
63	45	7	63	41	8	63	37	9	63	35	10
63	31	11	63	27	12	63	23	13	63	21	14

TABLE IV
STABILIZER CODES OVER $\mathbb{F}_4$ OF LENGTH 63

Notice that we get a large improvement with respect to the codes in [25, Table III], and larger minimum distances (10 is the largest minimum distance in [25, Table III]).

We may consider quantum codes coming from complementary codes as well. Their length is $N^C = M - N = q^{2n} - q^{2n-1} = 256 - 64 = 192$. The parameters of some codes exceeding the QGVB are displayed in Table V. We have not found better codes over $\mathbb{F}_4$ with this length in the literature.

Example 6. Table VI contains some stabilizer codes over $\mathbb{F}_3$ obtained with our procedure with length 242, 243 and 486. Our codes with length 242 and distance 5, 6, 10 and 11 exceed the the QGVB. Every code we give with length 243, but those with distance 15, 16 or 17, exceed the QGVB. Finally all codes with length 486 exceed that bound.

Example 7. Some stabilizer codes over $\mathbb{F}_5$ obtained with our procedure with length 124, 125 and 500 can be found in Table VII. Our codes exceed the QGVB, excepting those with length 124 and distance 5 or 15. Notice that, again, we obtain a great improvement with respect to the codes with length 124 in [25, Table III]. In addition, the minimum distance of our codes can be much larger than in [25].

n	k	d	n	k	d	n	k	d
192	186	3	192	182	4	192	178	5
192	174	6	192	170	7	192	166	8
192	162	9	192	158	10	192	154	11
192	150	12	192	146	13	192	121	14

TABLE V
STABILIZER CODES OVER $\mathbb{F}_4$ OF LENGTH 192

n	k	d	n	k	d	n	k	d
242	220	5	242	214	6	242	208	7
242	202	8	242	196	10	242	190	11
242	184	12	242	178	13	242	172	14
242	166	15	242	160	16	242	154	17
243	225	5	243	219	6	243	213	7
243	207	8	243	201	9	243	195	11
243	189	12	243	183	13	243	177	14
243	171	15	243	165	16	243	159	17
486	466	5	486	460	6	486	454	7
486	448	8	486	442	9	486	436	11
486	430	12	486	424	13	486	418	14
486	412	15	486	406	16	486	400	17

TABLE VI
STABILIZER CODES OVER $\mathbb{F}_3$ OF LENGTHS 242, 243 AND 486

Example 8. Finally, we display Table VIII containing stabilizer codes with length 342 and 2058 (from complementary codes) over $\mathbb{F}_7$. All the codes exceed the QGVB. Moreover, those with length 342 provide a great improvement with respect to the codes given in [25, Table III]. And as before, the minimum distance of our codes can be much larger than in [25].

Remark 16. We have not performed an exhaustive search of good codes. We expect that more records can be found following this construction. For instance, Markus Grassl, with the setting as in Example 4, has found record complementary codes with the following parameters: $[127, 39, 44]_4$, $[127, 40, 43]_4$, $[127, 41, 42]_4$, $[128, 75, 22]_4$, $[128, 79, 20]_4$, $[128, 93, 14]_4$.

APPENDIX A
PROOF OF PROPOSITION 7

Proof. Write $\delta = q - \lfloor \frac{(q-1)}{2} \rfloor$ and notice that $\delta = \frac{(q+1)}{2}$ if q is odd and it equals $\frac{(q+2)}{2}$ otherwise. Thus, the bound $q^n - \lfloor \frac{(q-1)}{2} \rfloor q^{n-1} - \cdots - \lfloor \frac{(q-1)}{2} \rfloor q - 1$ can be expressed as

$$\delta q^{n-1} - \left\lfloor \frac{(q-1)}{2} \right\rfloor q^{n-2} - \cdots - \left\lfloor \frac{(q-1)}{2} \right\rfloor q - 1. \tag{8}$$

Now, consider the q-adic expansion of i and j:

$$i = \sum_{k=0}^{n-1} a_k q^k, \quad j = \sum_{k=0}^{n-1} b_k q^k.$$

For i (and analogously for j), the expression in (8) shows that:

- *When q is even*, $a_{n-1} \leq \delta - 1$ and when $a_{n-1} = \delta - 1$, then $a_{n-2} \leq \delta - 1$, fact that we can iterate and claim that $a_0 \leq \delta - 1$, whenever $a_1 = a_2 = \cdots = a_{n-1} = \delta - 1$. There exists an exception for $q = 2$, in this case $\delta = 2$ and $a_0 = 0$, whenever $a_1 = a_2 = \cdots = a_{n-1} = 1$.
- *Otherwise (q is odd)*, one also has that $a_{n-1} \leq \delta - 1$. If $a_{n-1} = \delta - 1$, then $a_{n-2} \leq \delta - 1$ and, as above, this argument can be repeated and one gets that $a_0 \leq \delta$, when $a_1 = a_2 = \cdots = a_{n-1} = \delta - 1$.

We divide our reasoning in two cases:

n	k	d	n	k	d	n	k	d
124	108	5	124	106	6	124	102	7
124	98	8	124	94	9	124	90	10
124	88	11	124	84	12	124	80	13
124	76	14	124	72	15	124	70	16
125	111	5	125	107	6	125	105	7
125	101	8	125	97	9	125	93	10
125	89	11	125	87	12	125	83	13
125	79	14	125	75	15	125	71	16
500	462	11	500	458	12	500	454	12
500	450	14	500	446	15	500	442	16
500	438	17	500	434	18	500	430	19
500	426	20	500	422	21	500	418	22

TABLE VII
STABILIZER CODES OVER $\mathbb{F}_5$ OF LENGTHS 124, 125 AND 500

n	k	d	n	k	d	n	k	d
342	326	5	342	322	6	342	318	7
342	316	8	342	312	9	342	308	10
342	304	11	342	300	12	342	296	13
342	292	14	342	290	15	342	286	16
342	282	17	342	278	18	342	274	19
342	270	20						
2058	2020	11	2058	2016	12	2058	2012	12
2058	2008	14	2058	2004	15	2058	2000	16
2058	1996	17	2058	1992	18	2058	1988	19
2058	1984	20	2058	1980	21	2058	1976	22
2058	1972	23	2058	1968	24	2058	1964	25
2058	1960	26						

TABLE VIII
STABILIZER CODES OVER $\mathbb{F}_7$ OF LENGTHS 324 AND 2058

Case 1, $m < n$*:* then $n-1 = m + m_1$, where $m_1 \geq 0$. Then

$$\begin{aligned} i + jq^m &= a_0 + a_1 q + \cdots + (a_m + b_0)q^m \\ &\quad + \cdots + (a_{n-1} + b_{m_1})q^{n-1} + \\ &\quad b_{m_1+1}q^n + \cdots + b_{n-1}q^{n+m-1} \\ &\leq 2q^n + b_{m_1+1}q^n + \cdots + b_{n-1}q^{n+m-1} \\ &\leq (b_{n-1}+1)q^{n+m-1} \\ &< q^{2n-1} - 1, \end{aligned}$$

the last inequality holds because otherwise $m = n-1$ (notice that $m < n$) and $b_{n-1} + 1 = q$ and then

$$i + jq^m = a_0 + \cdots + (a_{n-1} + b_0)q^{n-1} + b_1 q^n + \cdots + b_{n-1}q^{2n-2}.$$

The last expression is equal to $q^{2n-1} - 1$ only when all the coefficients are exactly equal to $q-1$, which gives a contradiction because $a_0 \leq \delta$ as we indicated previously.

Case 2, $m = n$*:* then,

$$\begin{aligned} i + jq^m &= i + jq^n \\ &= a_0 + a_1 q + \cdots + a_{n-1}q^{n-1} + \\ &\quad b_0 q^n + b_1 q^{n+1} + \cdots + b_{n-1}q^{2n-1}. \end{aligned}$$

This expression is the exponent of a term in X which can be written as

$$X^{a_0 + a_1 q + \cdots + b_{n-2}q^{2n-2}} (X^{q^{2n-1}})^{b_{n-1}}. \tag{9}$$

Since we are considering the class of the term in $\mathbb{F}_{q^{2n}}[X]/\langle \mathrm{tr}_{2r}^{s}(X)\rangle$, we can replace the monomial $X^{q^{2n-1}}$ with the polynomial $-X - X^q - \cdots - X^{q^{2n-2}}$. The multinomial theorem shows that the expression in (9) can be expressed as a sum of terms where the exponents of the attached monomials are of the form

$$a_0 + a_1 q + \cdots + a_{n-1}q^{n-1} + b_0 q^n + \cdots + b_{n-2}q^{2n-2} + \sum_{k=0}^{2n-2} c_k q^k.$$

Notice that $\sum_{k=0}^{2n-2} c_k q^k$ is the q-adic expansion of the exponent of some monomial in

$$(-X - X^q - \cdots - X^{q^{2n-2}})^{b_{n-1}} \tag{10}$$

and therefore $\sum_{k=0}^{2n-2} c_k = b_{n-1} \leq \delta - 1$. As a consequence, we get terms whose exponents (of the corresponding monomials) are

$$\sum_{k=0}^{n-1}(a_k + c_k)q^k + \sum_{k=0}^{n-2}(b_k + c_{k+n})q^{k+n}. \tag{11}$$

Consider first the case when q is odd. Then, for having a term whose monomial is $X^{q^{2n-1}-1}$, every coefficient in the q-adic expansion of (11) should be equal to $q-1$. As b_k and c_k are lower than $\delta = (q+1)/2$, it holds that $b_k + c_{k+n} \leq q-1$. However, $b_{n-2} + c_{2n-2}$ is the coefficient of q^{2n-2} and it equals $q-1$ only when $b_{n-1} = (q-1)/2$ and uniquely for one monomial obtained from (10), but in this case $c_{2n-3} = 0$, and thus not all coefficients in (11) are equal to $q-1$.

Finally, when q is even, $\delta = (q+2)/2 = q/2+1$ and then the sums $a_k + c_k$, $0 \leq k \leq n-1$ and $b_k + c_{k+n}$, $0 \leq k \leq n-2$, may reach the values $q-1$ or q. However, this is not the case for $a_0 + c_0$ because c_0 is either 0 or 1 depending on either $b_{n-1} > 1$ or $b_{n-1} = 1$. When either $a_k + c_k$, for $0 \leq k \leq n-1$, or $b_k + c_{k+n}$, for $0 \leq k \leq n-2$, is equal to q, the q-adic expansion of (11) is obtained by adding one unit to the next power of q, and when $b_{n-2} + c_{2n-2} = q$, again one must use the fact that $X^{q^{2n-1}} = -X - X^q - \cdots - X^{q^{2n-2}}$. Taking into account that the power $(X^{q^{2n-1}})^i$ with $i = 1$ can appear only once, we deduce that the q-adic expansion $\sum_{k=0}^{2n-2} d_k q^k$ of the expression (11) satisfies $d_k < (\delta - 1) + 1 = (q+2)/2 < q-1$ and not every coefficient of the mentioned q-adic expansion is equal to $q-1$. □

ACKNOWLEDGMENT

The authors thank Markus Grassl for pleasant discussions and for providing the codes in Remark 16.

REFERENCES

[1] Aly, S.A., Klappenecker, A., Kumar, S., Sarvepalli, 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., Barg, A., Knill, E., Litsyn, S. Quantum error-detection I: Statement of the problem, *IEEE Trans. Inf. Theory* **46** (2000) 778-788.

[4] Ashikhmin, A., Barg, A., Knill, E., Litsyn, S. Quantum error-detection II: Bounds, *IEEE Trans. Inf. Theory* **46** (2000) 789-800.

[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 and orthogonal geometry, *Phys. Rev. Lett.* **76** (1997) 405-409.

[7] 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.

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

[9] Cox, D. Little, J., O'Shea, D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Second Edition. Springer, 1998.

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

[11] Edel, Y. *Some good quantum twisted codes*. Online available at https://www.mathi.uni-heidelberg.de/~yves/Matritzen/QTBCH/QTBCHIndex.html

[12] Feng, K. Quantum error correcting codes. In Coding Theory and Cryptology, Word Scientific, 2002, 91-142.

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

[14] Galindo, C., Hernando, F. Quantum codes from affine variety codes and their subfield subcodes, *Des. Codes Cryptogr.* **76** (2015) 89-100.
[15] Galindo, C., Hernando, F., Ruano, D. New quantum codes from evaluation and matrix-product codes, *Finite Fields Appl.* **36** (2015) 98-120.
[16] Galindo, C., Hernando, F., Ruano, D. Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement, *Quantum Inf. Process.* **14** (2015) 3211-3231.
[17] Galindo, C., Geil, O., Hernando, F., Ruano, D. On the distance of stabilizer quantum codes from J-affine variety codes, *Quantum Inf. Process.* **16** (2017) 111.
[18] Gottesman, D. A class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* **54** (1996) 1862-1868.
[19] Grassl, M. *Bounds on the minimum distance of linear codes*. Online available at http://www.codetables.de, accessed on 4th October 2017.
[20] Grassl, M., Rötteler, M. Quantum BCH codes. In Proc. X Int. Symp. Theor. elec. Eng. Germany 1999, 207-212.
[21] Grassl, M., Beth, T., Rötteler, M. On optimal quantum codes, *Int. J. Quantum Inf.* **2** (2004) 757-775.
[22] He, X., Xu, L., Chen. H. New q-ary quantum MDS codes with distances bigger than $q/2$. *Quantum Inf. Process.* **15** (2016) 2745-2758.
[23] Jin, L., Ling, S., Luo, J., Xing, C. Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes, *IEEE Trans. Inf. Theory* **56** (2010) 4735-4740.
[24] Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K. Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inf. Theory* **52** (2006) 4892-4914.
[25] La Guardia, G.G. Construction of new families of nonbinary quantum BCH codes, *Phys. Rev. A* **80** (2009) 042331.
[26] La Guardia, G.G. On the construction of nonbinary quantum BCH codes, *IEEE Trans. Inf. Theory* **60** (2014) 1528-1535.
[27] La Guardia, G.G., Palazzo, R. Constructions of new families of nonbinary CSS codes, *Discrete Math.* **310** (2010) 2935-2945.
[28] Li, Z., Xing, L.J., Wang, X.M. Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes, *Phys. Rev. A* **77** (2008) 012308.
[29] Matsumoto, R., Uyematsu, T. Constructing quantum error correcting codes for p^m state systems from classical error correcting codes. *IEICE Trans. Fund.* **E83-A** (2000) 1878-1883.
[30] Matsumoto, R., Uyematsu, T. Lower bound for the quantum capacity of a discrete memoryless quantum channel, *J. Math. Phys* **43** (2002) 4391-4403.
[31] Sarvepalli, P.K., Klappenecker, A. Nonbinary quantum Reed-Muller codes. In Proc. 2005 Int. Symp. Inf. Theory, 1023-1027.
[32] 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* 1994, 124-134.
[33] Steane, A.M. Simple quantum error correcting codes, *Phys. Rev. Lett.* **77** (1996) 793-797.
[34] Stichtenoth, H. On the dimension of subfield subcodes, *IEEE Trans. Inf. Theory* **36** (1990) 90-93.
[35] Yu, S. Bierbrauer, J., Dong, Y., Chen, Q., Oh, C.H. All the stabilizer codes of distance 3, *IEEE Trans. Inf. Theory* **59** (2013) 5179-5185.