QUASI-CYCLIC CONSTRUCTIONS OF QUANTUM CODES

CARLOS GALINDO, FERNANDO HERNANDO AND RYUTAROH MATSUMOTO

Abstract. We give sufficient conditions for self-orthogonality with respect to symplectic, Euclidean and Hermitian inner products of a wide family of quasi-cyclic codes of index two. We provide lower bounds for the symplectic weight and the minimum distance of the involved codes. Supported in the previous results, we show algebraic constructions of good quantum codes and determine their parameters.

Introduction

Attention to quantum information processing, especially quantum computing, is rapidly growing, as several companies seem to be building quantum computers with many qubits [6]. One of the important theoretical techniques to realize quantum computation is the quantum error correction, which protects quantum memory and quantum computational process from noise.

Quantum error correction was proposed by Shor [22]. Its connection to classical error correction was mainly described in [5, 3, 4, 10, 24]. Afterwards that connection was generalized to the non-binary case (see [20, 2, 1]). Since then, the use of classical (error-correcting) codes has become one of standard methods for constructing quantum codes, see [15] for a survey.

Quasi-cyclic codes (QC codes) are a generalization of classical cyclic codes. It is well-known that there are asymptotically good codes attaining the Gilbert-Varshamov bound among QC codes [14, 19], so it is natural to use QC codes to construct good quantum codes. Hagiwara et al. [12, 13] studied constructions of quantum codes by QC LDPC codes. They focused on long codes and probabilistic constructions.

In this paper, we consider a wide class of QC codes of index 2 (see Subsections 1.2 and 1.3) and give sufficient conditions for their self-orthogonality with respect to symplectic, Euclidean and Hermitian inner products. Sections 2, 3 and 4 are devoted to the symplectic, Euclidean and Hermitian cases, respectively. In addition, we get lower bounds for the symplectic weight and the minimum distance of the involved codes. As a consequence, we provide an algebraic construction of short stabilizer quantum codes coming from the previously introduced QC codes (see Theorems 5, 13 and 16). To testify the interest of our construction, we complete this paper by showing several examples of quantum codes with good parameters. Indeed, we get quantum codes exceeding the Gilbert-Varshamov bounds [8, 9, 20] and/or improving the parameters of those codes which could be obtained by the CSS procedure from the best known linear codes under the assumption of being self-orthogonal.

2010 *Mathematics Subject Classification.* 94B65; 94B15; 81P70.

Key words and phrases. Quasi-cyclic codes; Trace; Symplectic, Hermitian and Euclidean duality; Quantum codes.

Supported by the Spanish Ministry of Economy/FEDER: grants MTM2015-65764-C3-2-P and MTM2015-69138-REDT, the University Jaume I: grant PB1-1B2015-02, and the JPS grant: 26289116.

1. Preliminaries

Throughout the paper, $\mathbb{F}_q$ will denote the finite field with q elements, q being a positive power p^r of a prime number p. Recall than an $[n,k,d]_q$ classical code is a linear space $C \subset \mathbb{F}_q^n$ of dimension k and minimum (Hamming) distance d. For a set $S \subset \mathbb{F}_q^n$, $w(S)$ will denote the minimum of the Hamming weights of those vectors in S.

In this section we review the existing connections between stabilizer quantum codes and classical codes, and the concept of quasi-cyclic (QC) code. We also introduce the class of QC codes we will use. Let us start explaining the mentioned connections.

1.1. **Quantum code constructions from classical linear codes.** 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 [15]. 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 $[[n,k,d]]_q$.

For a linear space $C \subset \mathbb{F}_q^n$, $C^\perp$ denotes its Euclidean dual, that is $\{\vec{x} \in \mathbb{F}_q^n \mid \langle \vec{x}, \vec{y}\rangle = 0, \text{ for all } \vec{y} \in C\}$, where $\langle \vec{x}, \vec{y}\rangle$ denotes the Euclidean (standard) inner product. From two classical linear codes C_1 and C_2 over $\mathbb{F}_q$ and assuming that $C_2 \subset C_1 \subset \mathbb{F}_q^n$, we can construct a stabilizer quantum code with parameters

$$[[n, \dim C_1 - \dim C_2, \min\{w(C_1 \setminus C_2), w(C_2^\perp \setminus C_1^\perp)\}]]_q.$$

This construction was shown in [1, 5, 24].

Stabilizer quantum codes can also be constructed from classical self-orthogonal codes with respect to the Hermitian inner product (see for instance [15, Corollary 16]). Indeed, recall that the Hermitian inner product of two vectors $\vec{x} = (x_1, x_2, \dots x_n)$ and $\vec{y} = (y_1, y_2, \dots y_n)$ in $\mathbb{F}_{q^2}^n$ is defined as

$$\langle \vec{x}, \vec{y}\rangle_h := \sum_{i=1}^{n} x_i^q y_i.$$

Now, if $C \subset \mathbb{F}_{q^2}^n$ is a classical code with parameters $[n,k,d]_{q^2}$ such that

$$C^{\perp_h} := \left\{ \vec{x} \in \mathbb{F}_{q^2}^n \mid \langle \vec{x}, \vec{y}\rangle_h = 0 \right\} \subset C,$$

then, it can be constructed a stabilizer quantum code with parameters $[[n, 2k-n, d]]_q$.

Finally, we have another construction that can be seen in [1]. For $\vec{x}$, $\vec{y} \in \mathbb{F}_q^{2n}$, their *symplectic inner product* is defined as

$$\langle \vec{x}, \vec{y}\rangle_{\mathrm{s}} = \sum_{i=1}^{n} \left(x_i y_{n+i} - x_{n+i} y_i \right).$$

Given a linear space $C \subset \mathbb{F}_q^{2n}$, we denote

$$C^{\perp_{\mathrm{s}}} = \{\vec{x} \in \mathbb{F}_q^{2n} \mid \langle \vec{x}, \vec{y}\rangle_{\mathrm{s}} = 0, \text{ for all } \vec{y} \in C\}.$$

For $\vec{x} \in \mathbb{F}_q^{2n}$, set $w_s(\vec{x}) = \mathrm{card}\{i \mid (x_i,\, x_{n+i}) \neq (0,0)\}$ and for a set $S \subset \mathbb{F}_q^{2n}$, we denote $w_s(S) = \min\{w_s(\vec{x}) \mid \vec{x} \in S\}$. We call w_s as the *symplectic weight.* The result concerning stabilizer codes states that when $C \subset \mathbb{F}_q^{2n}$ is a linear code such that $C \supset C^{\perp_{\mathrm{s}}}$, we can construct an $[[n, \dim C - n, w_s(C \setminus C^{\perp_{\mathrm{s}}})]]_q$ stabilizer quantum code.

Next, we recall the definition and some basic facts concerning quasi-cyclic codes of index 2.

1.2. **Quasi-cyclic codes.** For a vector $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$, we denote

$$\sigma_1(\vec{x}) = (x_n, x_1, \ldots, x_{n-1}).$$

A linear space $C \subset \mathbb{F}_q^n$ is said to be *a cyclic code* if $C = \sigma_1(C)$.

For a vector $\vec{x} \in \mathbb{F}_q^{2n}$, we denote

$$\sigma_2(\vec{x}) = (x_n, x_1, \ldots, x_{n-1}, x_{2n}, x_{n+1}, \ldots, x_{2n-1}).$$

A linear space $C \subset \mathbb{F}_q^{2n}$ is said to be *a quasi-cyclic (QC) code* (of index 2) if $C = \sigma_2(C)$.

We denote by $(x^n - 1)$ the ideal of the polynomial ring $\mathbb{F}_q[x]$ generated by $x^n - 1$, and by $R = \mathbb{F}_q[x]/(x^n - 1)$ the quotient ring of $\mathbb{F}_q[x]$ modulo $(x^n - 1)$. Given a polynomial $g(x)$ in $\mathbb{F}_q[x]$, by $[g(x)]$ we mean its residue class in R. When studying cyclic codes, a vector $\vec{a} = (a_0, \ldots, a_{n-1})$ is identified with the residue class

$$[a(x)] = [a_0 + a_2 x + a_3 x^2 + \cdots + a_{n-1} x^{n-1}], \tag{1}$$

and $\sigma_1(\vec{a})$ corresponds to the class $[xa(x)]$. Thus, a cyclic code can be identified with an ideal of R via the correspondence (1). Since R is a principal ideal domain, any cyclic code can be generated by a single $[g(x)] \in R$. In the sequel, the minimum Hamming distance of the cyclic code generated by $[g(x)]$ will be denoted by $d([g(x)])$. The expression $g(x)|h(x)$, $g(x), h(x) \in \mathbb{F}_q[x]$ means that $g(x)$ divides $h(x)$. When $g(x)|h(x)$, the cyclic code generated by $[g(x)]$ contains that generated by $[h(x)]$.

A vector $\vec{c} = (a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1})$ in $\mathbb{F}_q^{2n}$ can be identified with $([a(x)], [b(x)]) \in R^2$, where

$$a(x) = a_0 + a_2 x + a_3 x^2 + \cdots + a_{n-1} x^{n-1}, b(x) = b_0 + b_2 x + b_3 x^2 + \cdots + b_{n-1} x^{n-1}.$$

Then $\sigma_2(\vec{c})$ corresponds to the element $([xa(x)], [xb(x)])$ in R^2. By this correspondence, we see that a QC code C can be identified with an R-submodule of R^2.

Note that a QC code generated by m elements in R^2,

$$([f_1(x)], [g_1(x)]), ([f_2(x)], [g_2(x)]), \ldots, ([f_m(x)], [g_m(x)]),$$

can be regarded as the R-module

$$\left\{ \sum_{i=1}^{m} ([a_i(x) f_i(x)], [a_i(x) g_i(x)]) \mid a_i(x) \in \mathbb{F}_q[x] \right\}.$$

We conclude this section by introducing the family of QC codes we are going to use for constructing stabilizer quantum codes.

1.3. **The supporting QC codes.** Recall that p is a prime and $q = p^r$. Fix a positive integer n, consider the polynomial $x^n - 1 \in \mathbb{F}_q[x]$ and assume that the splitting field of that polynomial is $\mathbb{F}_{p^{mr}}$ for some positive integer m.

Let $f(x), g(x)$ and $h(x)$ be monic polynomials in $\mathbb{F}_q[x]$ whose degree is less than n and such that both $f(x)$ and $g(x)$ divide $x^n - 1$. Recall that the class $[f(x)]$ of a polynomial $f(x)$ as above that divides $x^n - 1$ generates a cyclic code of length n and dimension $n - \deg(f)$. Consider the check polynomial $f'(x)$ which satisfies $f(x) \cdot f'(x) = x^n - 1$ and define

$$f^{\perp}(x) := x^{\deg f'} f'\left(\frac{1}{x}\right).$$

Then, it is well-known that $[f^{\perp}(x)]$ generates the dual code of the cyclic code generated by $[f(x)]$. Next we define the mentioned family of QC codes. We will use suitable subfamilies for obtaining our quantum codes.

Definition 1. With the above notation, $Q_q(f,g,h)$ will be the QC code over $\mathbb{F}_q$ of length $2n$ generated by $([f(x)],[h(x)f(x)])$ and $(0,[g(x)])$. When q and the polynomials are clear, we will denote it simply by Q.

Notice that, according to [16, Section 2], the generator set of $Q_q(f,g,h)$ is a Groebner basis for the $\mathbb{F}_q[x]$-submodule $\psi^{-1}(Q_q(f,g,h))$, which is the preimage in $(\mathbb{F}_q[x])^2$ of the R-submodule $Q_q(f,g,h)$ under the class map $\psi:(\mathbb{F}_q[x])^2\to R^2$.

To the best of our knowledge, this is the first family of QC codes of short length giving quantum codes by algebraic techniques. There was a first attempt in [21] but it seems to be wrong because the proposed codes contradict the dimension formula for simple generator QC codes [16]. Indeed, if one considers a QC code generated by a single polynomial vector $([f_1(x)],[f_2(x)],\dots,[f_\ell(x)])$, then $\dim C\leq n$ by [16, Corollary 2.14]. However $C\supset C^{\perp}$ implies $\dim C\geq \ell n/2$, which is not satisfied by the codes in [21].

In our development, attached to polynomials $h(x)\in\mathbb{F}_q[x]$ with degree less than n, we will consider the polynomials $\bar{h}(x)$ defined as

$$\bar{h}(x):=x^n h\left(\frac{1}{x}\right).$$

The coefficients of the polynomial $h(x)$, expressed as $\sum_{i=0}^{n-1}h_ix^i$, determine a vector in $\mathbb{F}_q^n$ whose reversed coordinates correspond to the polynomial $\bar{h}(x)$. These polynomials are instrumental as the following result shows.

Proposition 2. *Let $f(x),g(x)$ and $h(x)$ be monic polynomials in $\mathbb{F}_q[x]$ whose degrees are less than n and consider the vectors in $\mathbb{F}_q^n$ determined by their classes in R as described before Equality (1). Then, the following equality of Euclidean inner products of vectors in $\mathbb{F}_q^n$ holds:*

$$\langle [f(x)g(x)],[h(x)]\rangle=\langle [g(x)],[\overline{f}(x)h(x)]\rangle. \tag{2}$$

Proof. Let $f(x)=f_0+\cdots+f_{n-1}x^{n-1}$. We have

$$\langle [f(x)g(x)],[h(x)]\rangle=\sum_{i=0}^{n-1}f_i\langle [x^ig(x)],[h(x)]\rangle,$$

and

$$\langle [g(x)],[\overline{f}(x)h(x)]\rangle=\sum_{i=0}^{n-1}f_i\langle [g(x)],[x^{n-i}h(x)]\rangle.$$

In order to prove the proposition, it is sufficient to show

$$\langle [x^ig(x)],[h(x)]\rangle=\langle [g(x)],[x^{n-i}h(x)]\rangle. \tag{3}$$

Let $g(x)=g_0+\cdots+g_{n-1}x^{n-1}$ and $h(x)=h_0+\cdots+h_{n-1}x^{n-1}$. Then

$$\langle [x^ig(x)],[h(x)]\rangle=\sum_{j=0}^{n-1}g_{i+j \bmod n}h_j=\sum_{j=0}^{n-1}g_jh_{j+n-i \bmod n},\ \text{ and}$$

$$\langle [g(x)],[x^{n-i}h(x)]\rangle=\sum_{j=0}^{n-1}g_jh_{j+n-i \bmod n},$$

which shows Equality (3). □

The following sections will explain how to get stabilizer quantum codes from suitable QC codes $Q_q(f,g,h)$ and will give information about their parameters.

2. Quasi-cyclic construction of quantum codes with symplectic inner product

In this section we will give conditions on the polynomials f, g and h under which the QC code $Q := Q_q(f,g,h)$ is symplectic self-orthogonal and, according Subsection 1.1, gives rise to a stabilizer quantum code. We start by studying the symplectic dual of our QC code.

Proposition 3. *With the above notation, the QC code $Q := Q_q(f,g,h)$ has dimension $2n - \deg(f(x)) - \deg(g(x))$, and its symplectic dual $Q^{\perp_s}$ is quasi-cyclic and generated by $([g^\perp(x)], [\overline{h}(x)g^\perp(x)])$ and $([0], [f^\perp(x)])$.*

Proof. The dimension can be deduced from the shape of the generator matrix of the code Q, which is

$$\begin{pmatrix} G_1 & G_3 \\ 0 & G_2 \end{pmatrix},$$

where G_1 (respectively, G_2) is a generator matrix of the cyclic code generated by $[f(x)]$ (respectively, $[g(x)]$) whose dimension is $n - \deg(f(x))$ (respectively, $n - \deg(g(x))$).

With respect to duality, A vector generated by $([g^\perp(x)], [\overline{h}(x)g^\perp(x)])$ and $(0, [f^\perp(x)])$ has the form $([c(x)g^\perp(x)], [c(x)\overline{h}(x)g^\perp(x) + d(x)f^\perp(x)])$, whose symplectic inner product with $([a(x)f(x)], [a(x)h(x)f(x) + b(x)g(x)])$ is, by Equality (2),

$$\begin{aligned} & \langle [a(x)f(x)], [d(x)f^\perp(x)] \rangle + \langle [a(x)f(x)], [c(x)\overline{h}(x)g^\perp(x)] \rangle \\ & -\langle [a(x)h(x)f(x)], [c(x)g^\perp(x)] \rangle - \langle [b(x)g(x)], [c(x)g^\perp(x)] \rangle \\ = \; & \langle [a(x)f(x)], [c(x)\overline{h}(x)g^\perp(x)] \rangle - \langle [a(x)h(x)f(x)], [c(x)g^\perp(x)] \rangle \\ = \; & \langle [a(x)h(x)f(x)], [c(x)g^\perp(x)] \rangle - \langle [a(x)h(x)f(x)], [c(x)g^\perp(x)] \rangle \\ = \; & 0. \end{aligned}$$

This concludes the proof after taking into account that the dimension of the space generated by $([g^\perp(x)], [\overline{h}(x)g^\perp(x)])$ and $([0], [f^\perp(x)])$ is $2n - \deg(g^\perp(x)) - \deg(f^\perp(x))$. □

The following result provides a lower bound of the symplectic weight of the QC codes $Q_q(f,g,h)$. It holds under certain assumptions on the polynomial h. Later, in this section, we will give some explicit constructions of such polynomials.

Proposition 4. *Consider the QC code $Q := Q_q(f,g,h)$ where we assume that $h(x)$ satisfies that $\gcd(h(x) - \beta, x^n - 1) = 1$ for all non-zero $\beta \in \mathbb{F}_q$. Then, a lower bound on the symplectic weight of Q is the following value*

$$\begin{aligned} & d_q(f,g,h) = \\ & \min\Big\{ d([g(x)]), d\big([(x^n-1)/\gcd(x^n-1, h(x))]\big), d\Big(\big[\mathrm{lcm}\big(f(x), g(x)/\gcd(g(x), h(x))\big)\big]\Big), \\ & \qquad \Big(d([f(x)]) + d([\gcd(h(x)f(x), g(x))]) + (q-1)d([\gcd(f(x), g(x))])\Big)\Big/q \Big\}. \end{aligned}$$

Proof. Consider the symplectic weight

$$w_s = w_s([a(x)f(x)], [a(x)h(x)f(x) + b(x)g(x)]).$$

If $[a(x)] = 0$ then $w_s \geq d(g(x))$.

We are going to use the following relation among symplectic and Hamming weights of vectors $(\vec{u}, \vec{v}) \in \mathbb{F}_q^{2n}$ which was proved in [18, Lemma 2.4].

$$qw_s(\vec{u}, \vec{v}) = w_H(\vec{u}) + w_H(\vec{v}) + \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} w_H(\alpha\vec{u} + \vec{v}). \tag{4}$$

Suppose that $[b(x)] = 0$, $[a(x)] \neq 0$ and $[a(x)h(x)f(x)] \neq 0$. Since $h(x) - \beta$ is a unit modulo $x^n - 1$, $[a(x)(h(x) - \beta)f(x)] \neq 0$ for nonzero β. Then, for $q = 2$, it holds

$$\begin{aligned} w_s &= \Big(w_H([a(x)f(x)]) + w_H([a(x)h(x)f(x)]) + w_H([a(x)(h(x) + 1)f(x)])\Big)\Big/2 \\ &\geq \Big(d([f(x)]) + d([h(x)f(x)]) + d([f(x)])\Big)\Big/2 \\ &\geq \Big(d([f(x)]) + d([\gcd(h(x)f(x), g(x))]) + d([\gcd(f(x), g(x))])\Big)\Big/2. \end{aligned}$$

For $q > 2$, we have

$$\begin{aligned} w_s &= \Big(w_H([a(x)f(x)]) + w_H([a(x)h(x)f(x)]) \\ &\quad + \sum_{0 \neq \beta \in \mathbb{F}_q} w_H([a(x)(h(x) + \beta)f(x)])\Big)\Big/q \\ &\geq \Big(d([f(x)]) + d([\gcd(h(x)f(x), g(x))]) + (q-1)d([\gcd(f(x), g(x))])\Big)\Big/q. \end{aligned}$$

Suppose now that $[b(x)] = 0$, $[a(x)] \neq 0$ and $[a(x)h(x)f(x)] = 0$. Then w_s equals $w_H([a(x)f(x)])$ and $[a(x)f(x)]$ belongs to the cyclic code generated by $[(x^n - 1)/\gcd(x^n - 1, h(x))]$. Thus $w_s \geq d([(x^n - 1)/\gcd(x^n - 1, h(x))])$.

Finally and until the end of the proof, we assume $[a(x)] \neq 0$ and $[b(x)] \neq 0$. Then, we have

$$\begin{aligned} qw_s = w_H([a(x)f(x)]) + w_H([a(x)h(x)f(x) + b(x)g(x)]) \\ + \sum_{0 \neq \beta \in \mathbb{F}_q} w_H([a(x)(h(x) + \beta)f(x) + b(x)g(x)]). \end{aligned} \tag{5}$$

If some summand of the summation in (5) is zero, then $[a(x)(h(x)+\beta)f(x)] = -[b(x)g(x)]$ for some $\beta \in \mathbb{F}_q$, which means that $\operatorname{lcm}(f(x), g(x))|a(x)f(x)$ as $h(x) + \beta$ is a unit. So

$$w_s \geq w_H([a(x)f(x)]) \geq d\big(\operatorname{lcm}(f(x), g(x))\big).$$

In case the second summand in (5) is zero, we get

$$w_s = w_H([a(x)f(x)])$$

and $[a(x)f(x)]$ belongs to the cyclic code generated by $[g(x)/\gcd(g(x), h(x))]$. So

$$w_s \geq d\Big(\big[\operatorname{lcm}\big(f(x), g(x)/\gcd(g(x), h(x))\big)\big]\Big).$$

Otherwise (all summands in (5) are nonzero),

$$w_s \geq \Big(d([f(x)]) + d([\gcd(h(x)f(x), g(x))]) + (q-1)d([\gcd(f(x), g(x))])\Big)\Big/q,$$

which concludes the proof. □

Now we give conditions under which our QC codes are symplectic self-orthogonal, and state the mentioned result about quantum codes coming from these QC codes.

Theorem 5. *With the above notation, assume that the polynomial $h(x)$ satisfies that $\gcd(h(x)-\beta, x^n-1)=1$ for all non-zero $\beta \in \mathbb{F}_q$. Assume also that it holds either (i) $f(x)|g^\perp(x)$, $g(x)|f^\perp(x)$ and $h(x)|\overline{h}(x)$, or (ii) $f(x)|g(x)|g^\perp(x)|f^\perp(x)$ -which means that each polynomial in the sequence divides the following ones-.*

Then, the QC code $Q := Q_q(f,g,h)$ is symplectic self-orthogonal and allows us to construct a stabilizer quantum code with parameters $[[n, n-\deg(f(x))-\deg(g(x)), \geq d_q(f,g,h)]]_q$.

Proof. The fact that Q is self-orthogonal follows trivially from Proposition 3 in Case (i). In Case (ii), we have $f^\perp(x)=\alpha_1(x)g^\perp(x)$, $g^\perp(x)=\alpha_2(x)g(x)$ and $g(x)=\alpha_3(x)f(x)$, where $\alpha_i(x)\in\mathbb{F}_q[x]$ for $1\leq i\leq 3$. Now

$$\Big(a(x)g^\perp(x), a(x)\bar{h}(x)g^\perp(x)+b(x)f^\perp(x)\Big)$$
$$= \Big(a(x)\alpha_2(x)\alpha_3(x)f(x), a(x)\alpha_2(x)\alpha_3(x)f(x)+q(x)g(x)\Big),$$

where $q(x)=a(x)\alpha_2(x)(\bar{h}(x)-1)+b(x)\alpha_1(x)\alpha_2(x)$, which again by Proposition 3, proves the self-orthogonality in this case. Now Proposition 4 and Subsection 1.1 conclude the proof. □

To finish this section, we will provide some polynomials $h(x)$ which are suitable for the previous mentioned purposes.

For each set $\{i,j\}$ of positive integers, consider the following trace polynomials:

$$\mathrm{tr}_{ji/i}(x) = x + x^{p^i} + x^{p^{2i}} + \cdots + x^{p^{(j-1)i}}.$$

Proposition 6. *Assume, as above, that the splitting field of $x^n-1\in\mathbb{F}_q[x]$ is $\mathbb{F}_{p^{mr}}$ and consider a positive integer $s<p$ which divides m and is coprime with r. Then the polynomial in $\mathbb{F}_q[x]$*

$$h(x) = (p-s)\mathrm{tr}_{mr/s}(x) + \mathrm{tr}_{mr/1}(x)$$

satisfies that $h(x)+\beta$ is coprime with x^n-1 for all $\beta\in\mathbb{F}_q\setminus\{0\}$.

Proof. In this proof, for the sake of simplicity, we will use the same expression for the involved polynomials and the maps which they define. We are going to prove that the equation $h(x)+\beta=0$ has no solution in $\mathbb{F}_{q^m}$, which is equivalent to $h(a)+\beta\neq 0$ for all $a\in\mathbb{F}_{q^m}$ and $\beta\in\mathbb{F}_q\setminus\{0\}$.

Indeed, observe that $\mathrm{tr}_{ji/i}$ can be regarded as a map $\mathbb{F}_{p^{ji}}\to\mathbb{F}_{p^i}$. In addition, the equality $\mathrm{tr}_{mr/1}=\mathrm{tr}_{s/1}\circ\mathrm{tr}_{mr/s}$, where $\circ$ means maps composition, holds. When $\mathrm{tr}_{mr/s}(a)=b\in\mathbb{F}_p$, we have $\mathrm{tr}_{mr/1}(a)=sb$ and $h(a)=pb=0$. Otherwise we have $\mathrm{tr}_{mr/s}(a)=b'\in\mathbb{F}_{p^s}\setminus\mathbb{F}_p$, which cannot be equal to $-\mathrm{tr}_{mr/1}(a)-\beta\in\mathbb{F}_q$, because our conditions imply that $(\mathbb{F}_{p^s}\setminus\mathbb{F}_p)\cap\mathbb{F}_q=\emptyset$. □

Polynomials $h(x)$ in Proposition 6 need not to be of degree less than n but this condition can be obtained by considering the remainder $h'(x)$ of $h(x)$ by division on x^n-1. The fact that $h'(x)$ satisfies the conclusion of Proposition 6 can be easily proved from Bézout's identity.

Finally we explain when the polynomials $h(x)=x+1$ or $h(x)=x^p-x$ are suitable for our purposes.

$h(x)$	q	n	Result
$h(x) = x + 1$	any	n s.t. $\gcd(q-1, n) = 1$	Lemma 7
$h(x) = x^p - x$	$q = p$ prime	$n = p^m - 1$, m is not a multiple of p	Proposition 8
$h(x)$ as in Proposition 6	any	n s.t. $m = \mathrm{ord}_q(n)$ is a multiple of s, where $s < p$ and $\gcd(s, r) = 1$	Proposition 6

TABLE 1. Parameters (q, n) that guarantee the existence of a suitable polynomial h

Lemma 7. *With the above notation, it holds that* $\gcd(x^n - 1, x + 1 + \beta) = 1$ *for all* $\beta \in \mathbb{F}_q \setminus \{0\}$ *if and only if* $\gcd(q - 1, n) = 1$.

Proof. Assume that $\gcd(x^n - 1, x + 1 + \beta) = x + 1 + \beta = x - \alpha$, $\alpha \in \mathbb{F}_q$, which means that $x^n - 1$ contains a $q - 1$ root of unity and so $\alpha^{q-1} = \alpha^n = 1$. This equality holds if and only if $\gcd(q - 1, n) \neq 1$, which concludes the proof. □

Proposition 8. *The polynomial* $h(x) = x+1 \in \mathbb{F}_2[x]$ *(*$h(x) = x^p - x \in \mathbb{F}_p[x]$*, respectively) satisfies the condition* $\gcd(h(x) - \beta, x^n - 1) = 1$ *for all non-zero* $\beta \in \mathbb{F}_q$*, being* $q = 2$ *(respectively,* $q = p$ *and* p *does not divide* $m = \log_p(n + 1)$*).*

Proof. Lemma 7 proves the case $q = 2$. When $q = p$ is a prime number which does not divide $m = \log_p(n + 1)$, we use the fact that $x^p - x + \beta$ is irreducible over $\mathbb{F}_{p^m}$ if and only if $\mathrm{tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\beta) \neq 0$ [17, Corollary 3.79]. Then $x^p - x + \beta$ is irreducible over $\mathbb{F}_{p^m}$ and therefore $x^p - x + \beta$ is coprime with $x^n - 1$ for $n = p^m - 1$. □

Remark 9. The pairs (q, n), corresponding to the cardinality q of the supporting field and the length n of the quantum codes given by Theorem 5, have some restrictions if one desires to guarantee the existence of some suitable polynomial $h(x)$ by applying some of the above three results. Table 1 contains the pairs (q, n) that can be reached according to the proposed polynomials in Propositions 6 and 8 and Lemma 7. Recall that $\mathrm{ord}_q(n)$ is the smallest positive integer t such that $q^t \equiv 1 \mod n$ and that if $\mathrm{ord}_q(n) = m$, then $\mathbb{F}_{p^{mr}}$ is the splitting field of $x^n - 1 \in \mathbb{F}_q[x]$. Note that, fixed a pair (q, n), one may also attempt to obtain polynomials $h(x)$ through trial and error.

3. Quasi-cyclic construction of stabilizer quantum codes with the Euclidean inner product

Let $Q_q(f, g, h)$ be the QC code over $\mathbb{F}_q$ of length $2n$ generated by $([f(x)], [h(x)f(x)])$ and $(0, [g(x)])$ as introduced in Subsection 1.3. We are going to study the stabilizer quantum codes given by self-orthogonal codes with respect to Euclidean inner product of the form $Q_q(f, g, h)$. This way of obtaining quantum codes is usually known as the CSS construction [5, 23]. For a start, we explain which code is the Euclidean dual of $Q_q(f, g, h)$.

Proposition 10. *The Euclidean dual code of the QC code* $Q_q(f, g, h)$ *over* $\mathbb{F}_q$ *is a QC code generated by the pairs* $([-\overline{h}(x)g^\perp(x)], [g^\perp(x)])$ *and* $([f^\perp(x)], 0)$.

Proof. A codeword in $Q_q(f, g, h)$ can be written as $([a_1(x)f(x)], [a_1(x)h(x)f(x)+a_2(x)g(x)])$. Similarily, a codeword in the code generated by $([-\overline{h}(x)g^\perp(x)], [g^\perp(x)])$ and $([f^\perp(x)], 0)$ can be written as $([-b_1(x)\overline{h}(x)g^\perp(x) + b_2(x)f^\perp(x)], [b_1(x)g^\perp(x)])$. The Euclidean inner

product of the above two codewords is, by Proposition 2,

$$\begin{aligned} & -\langle [a_1(x)f(x)], b_1(x)\overline{h}(x)g^{\perp}(x)\rangle + \underbrace{\langle [a_1(x)f(x)], [b_2(x)f^{\perp}(x)]\rangle}_{=0} \\ & +\langle [a_1(x)h(x)f(x)], [b_1(x)g^{\perp}(x)]\rangle + \underbrace{\langle [a_2(x)g(x)], [b_1(x)g^{\perp}(x)]\rangle}_{=0} \\ = \; & -\langle [a_1(x)f(x)], b_1(x)\overline{h}(x)g^{\perp}(x)\rangle + \langle [a_1(x)h(x)f(x)], [b_1(x)g^{\perp}(x)]\rangle \\ = \; & -\langle [a_1(x)f(x)], b_1(x)\overline{h}(x)g^{\perp}(x)\rangle + \langle [a_1(x)f(x)], [b_1(x)\overline{h}(x)g^{\perp}(x)]\rangle = 0. \end{aligned}$$

We have shown that the Euclidean dual code of $Q_q(f,g,h)$ contains the QC code generated by $([-\overline{h}(x)g^{\perp}(x)], [g^{\perp}(x)])$ and $([f^{\perp}(x)], 0)$. As is Proposition 3, the dimension of $Q_q(f,g,h)$ is $2n - \deg f(x) - \deg g(x)$, and that of the latter is $2n - \deg f^{\perp}(x) - \deg g^{\perp}(x) = \deg f(x) + \deg g(x)$, which completes the proof.

□

Now, we give conditions for self-orthogonality.

Proposition 11. *A sufficient condition for $Q_q(f,g,h)$ to contain its Euclidean dual is*

$$f(x)|g(x)|g^{\perp}(x)|f^{\perp}(x).$$

Proof. It follows from the following two equalities:

$$\begin{aligned} \Big([\overline{h}(x)g^{\perp}(x)], [g^{\perp}(x)]\Big) - \left[\frac{\overline{h}(x)g^{\perp}(x)}{f(x)}\right]([f(x)], [h(x)f(x)]) & \\ = \Big(0, \Big[\big(1 - h(x)\overline{h}(x)\big)\, g^{\perp}(x)\Big]\Big) & \\ = \left[\frac{(1 - h(x)\overline{h}(x))g^{\perp}(x)}{g(x)}\right](0, [g(x)])\,. & \end{aligned}$$

$$\begin{aligned} & \Big([f^{\perp}(x)], 0\Big) \\ & \qquad = \left[\frac{f^{\perp}(x)}{f(x)}\right]([f(x)], [h(x)f(x)]) - \left[\frac{[h(x)f^{\perp}(x)]}{[g(x)]}\right](0, [g(x)])\,. \end{aligned}$$

□

With respect to distance, we can state the following result.

Proposition 12. *The following value*

$$\begin{aligned} & d_q^e(f,g,h) = \\ & \min\Big\{ d([g(x)]), d\big([(x^n-1)/\gcd(x^n-1, h(x))]\big), d\Big(\big[\mathrm{lcm}\big(f(x), g(x)/\gcd(g(x), h(x))\big)\big]\Big), \\ & \qquad\qquad d([f(x)]) + d([\gcd(h(x)f(x), g(x))])\Big\} \end{aligned}$$

is a lower bound for the minimum distance of the QC code $Q_q(f,g,h)$.

Proof. A codeword in $Q_q(f,g,h)$ can be written as $\big([a(x)f(x)], [a(x)h(x)f(x) + b(x)g(x)]\big)$.

If $[b(x)] = 0$ and $[a(x)h(x)f(x)] \neq 0$, then its Hamming weight is at least $d(f(x)) + d(h(x)f(x))$.

If $[b(x)] = 0$ and $[a(x)h(x)f(x)] = 0$, then then $a(x)f(x)$ belongs to the ideal in $\mathbb{F}_q[x]$ generated by $(x^n-1)/\gcd(x^n-1, h(x))$. So $w_H([a(x)h(x)]) \geq d((x^n-1)/\gcd(x^n-1, h(x)))$.

If $[a(x)] = 0$ then the Hamming weight is larger than or equal to $d(g(x))$.

Finally and until the end of proof, we assume $[a(x)] \neq 0$ and $[b(x)] \neq 0$. If $[a(x)h(x)f(x)+b(x)g(x)] = 0$ then $[a(x)f(x)]$ belongs to the cyclic code generated by $[g(x)/\gcd(g(x), h(x))]$. Indeed, set $m(x) = \gcd(g(x), h(x))$ and, as a consequence, $g(x) = m(x)g'(x)$, $h(x) = m(x)h'(x)$ and $\gcd(g'(x), h'(x)) = 1$. Then $[a(x)h(x)f(x) + b(x)g(x)] = 0$ implies

$$a(x)h(x)f(x) \in (g(x))$$

because $g(x)|x^n - 1$. Thus $a(x)m(x)h'(x)f(x) = p(x)m(x)g'(x)$ for some polynomial $p(x)$ which proves that $a(x)f(x)$ belongs to the ideal generated by $g'(x)$. So

$$w_H\left([a(x)f(x)]\right) \geq d\left(\operatorname{lcm}(f(x), g(x)/\gcd(g(x), h(x)))\right).$$

Otherwise ($[a(x)h(x)f(x) + b(x)g(x)] \neq 0$) and then

$$w_H\left(([a(x)f(x)], [a(x)h(x)f(x) + b(x)g(x)]\right) \geq d\left(f(x)\right) + d(\gcd(h(x)f(x), g(x))),$$

which concludes the proof. □

Our next result recalls the above conditions for Euclidean self-orthogonality of our QC codes and gives parameters for the corresponding quantum codes.

Theorem 13. *With the above notation, assume that the polynomials $f(x)$ and $g(x)$ satisfy that $f(x)|g(x)|g^{\perp}(x)|f^{\perp}(x)$, then the QC code $Q_q(f, g, h)$ is self-orthogonal for the Euclidean inner product and, as a consequence, it provides a stabilizer quantum code with parameters*

$$[[2n, 2n - 2\deg(f(x)) - 2\deg(g(x)), \geq d_q^e(f, g, h)]]_q.$$

Proof. It follows from Propositions 10, 11 and 12, and Subsection 1.1. □

4. Quasi-cyclic construction of quantum codes with the Hermitian inner product

In this section the coefficient field for our QC codes and polynomials will be $\mathbb{F}_{q^2}$. This fact will allow us to consider Hermitian inner product instead of Euclidean inner product. Recall that for two vectors $\vec{x}, \vec{y} \in \mathbb{F}_{q^2}^{2n}$, the Hermitian inner product $\langle \vec{x}, \vec{y} \rangle_h$ can be regarded as the Euclidean product $\langle \vec{x}^q, \vec{y} \rangle$, where $\vec{x}^q$ denotes component-wise qth power of the vector $\vec{x}$.

Denote by $Q_{q^2}(f, g, h)$ the QC code in $\mathbb{F}_{q^2}^{2n}$ generated by $([f(x)], [h(x)f(x)])$ and $(0, [g(x)])$. Attached to a polynomial $r(x) = a_0 + a_1x + \cdots + a_mx^m$ of degree $m < n$, we define $r^{[q]}(x) = a_0^q + a_1^q x + \cdots + a_m^q x^m$. If $\vec{x}$ is represented by $[f(x)]$ then $\vec{x}^q$ is represented by $[f^{[q]}(x)]$.

Proposition 14. *The Hermitian dual code of the QC code over $\mathbb{F}_{q^2}$ $Q_{q^2}(f, g, h)$ is a QC code generated by the pairs $([-\overline{h^{[q]}}(x)g^{[q]^{\perp}}(x)], [g^{[q]^{\perp}}(x)])$ and $([f^{[q]^{\perp}}(x)], 0)$.*

Proof. The dimension of the Hermitian dual code of $Q_{q^2}(f, g, h)$ is

$$\deg(f(x)) + \deg(g(x)) = 2n - \deg f^{[q]^{\perp}}(x) - \deg g^{[q]^{\perp}}(x).$$

Therefore, it suffices to check the following chain of equalities:

$$\begin{aligned}\Big\langle ([f(x)],[h(x)f(x)])\,,\Big(\Big[-\overline{h^{[q]}}(x)g^{[q]^\perp}(x)\Big],[g^{[q]^\perp}(x)]\Big)\Big\rangle_h \\ = -\Big\langle [f(x)],\Big[\overline{h^{[q]}}(x)g^{[q]^\perp}(x)\Big]\Big\rangle + \Big\langle [h(x)f(x)],\Big[g^{[q]^\perp}(x)\Big]\Big\rangle_h \\ = -\Big\langle [h(x)f(x)],\Big[g^{[q]^\perp}(x)\Big]\Big\rangle + \Big\langle [h(x)f(x)],\Big[g^{[q]^\perp}(x)\Big]\Big\rangle_h \\ = 0.\end{aligned}$$

□

The following result can be proved with a similar reasoning as that in Proposition 11.

Proposition 15. *A sufficient condition for $Q_{q^2}(f,g,h)$ to contain its Hermitian dual is*

$$f(x)|g(x)|g^{[q]^\perp}(x)|f^{[q]^\perp}(x).$$

As a consequence of the previous results, we obtain the following result providing stabilizer quantum codes.

Theorem 16. *With the above notation, assume that the above polynomials, with coefficients in $\mathbb{F}_{q^2}$, $f(x)$ and $g(x)$ satisfy that $f(x)|g(x)|g^{[q]^\perp}(x)|f^{[q]^\perp}(x)$, then the QC code $Q_{q^2}(f,g,h)$ is self-orthogonal for the Hermitian inner product and, as a consequence, it provides a stabilizer quantum code with parameters*

$$[[2n, 2n-2\deg(f(x))-2\deg(g(x)), \geq d^e_{q^2}(f,g,h)]]_q.$$

Proof. It follows from what we said in Subsection 1.1 with respect to Hermitian duality and the fact that $d^e_{q^2}(f,g,h)$ is a lower bound for the minimum distance of the QC code $Q_{q^2}(f,g,h)$. □

Remark 17. In this remark, we explain why the quantum codes given in this section are, in general, different from those in Section 2. Let (β,β^q) be a normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Let N be a positive integer and ϕ the bijection $\phi:\mathbb{F}_q^{2N}\to\mathbb{F}_{q^2}^N$ defined by $\phi(\vec{u},\vec{v})=\beta\vec{u}+\beta^q\vec{v}$, where $\vec{u},\vec{v}\in\mathbb{F}_q^N$. This map also satisfies that the symplectic weight of the pair $(\vec{u},\vec{v})$ coincides with the Hamming weight of $\phi(\vec{u},\vec{v})$. With the help of ϕ, one can see that the stabilizer codes coming from Hermitian self-orthogonal codes $C\subset\mathbb{F}_{q^2}^N$ can be obtained from the codes $\phi^{-1}(C)\subset\mathbb{F}_q^{2N}$, which are symplectic self-orthogonal [15]. Let us apply this procedure to the codes in this section. Assume that $[f(x)]=\left[\sum_{i=0}^{n-1}f_ix^i\right]$, $[h(x)f(x)]=\left[\sum_{i=0}^{n-1}e_ix^i\right]$, and $[g(x)]=\left[\sum_{i=0}^{n-1}g_ix^i\right]$, where $f_i,e_i,g_i\in\mathbb{F}_{q^2}$, and write $f_i=f_i^1\beta+f_i^2\beta^q$ (respectively, $e_i=e_i^1\beta+e_i^2\beta^q$, $g_i=g_i^1\beta+g_i^2\beta^q$), where f_i^j (respectively, e_i^j, g_i^j) are in $\mathbb{F}_q$ for $j=1,2$. Then the corresponding vectors in $\phi^{-1}(Q_{q^2}(f,g,h))$ will have the shape

$$\big(f_0^1,\ldots,f_{n-1}^1,e_0^1,\ldots,e_{n-1}^1,f_0^2,\ldots,f_{n-1}^2,e_0^2,\ldots,e_{n-1}^2\big),$$

$$\big(0,\ldots,0,g_0^1,\ldots,g_{n-1}^1,0,\ldots,0,g_0^2,\ldots,g_{n-1}^2\big),$$

giving rise, in general cases, to polynomials which have not the shape of those in Section 2.

Remark 18. The QC codes used in this paper can be regarded as an extension of the Plotkin's sum $(u, u+v)$ which could be written as $(u, \varphi(u)+v)$, φ being a suitable linear map. In our case, u, $\varphi(u)$ and v are given by cyclic codes generated by classes of polynomials $[f(x)]$, $[h(x)f(x)]$, and $[g(x)]$. As a referee pointed us, it would be interesting to investigate whether this construction $(u, \varphi(u)+v)$, for other codes and maps, satisfies similar results on duality and minimum distance to ours and gives good codes for quantum correction.

5. Examples

We devote this section to provide some examples of good stabilizer quantum codes coming from our constructions.

The two first examples use symplectic product as explained in Section 2.

Example 1. Set $n = 151$, $q = 2$ and the polynomial $x^{151} - 1 \in \mathbb{F}_2[x]$. The splitting field of $x^{151}-1$ is $\mathbb{F}_{2^{15}}$ and set ζ a primitive element. Taking cyclotomic cosets modulo $n = 151$ with respect to $q = 2$, one can get minimal polynomials of roots of $x^{151} - 1$ which divide that polynomial.

Consider the cyclotomic coset

$$\{[2, 4, 8, 16, 32, 64, 128, 105, 59, 118, 85, 19, 38, 76, 1]\},$$

and the attached polynomial $f(x) = (x - \zeta^2)(x - \zeta^4)\cdots(x - \zeta)$ which belongs to $\mathbb{F}_2[x]$ and divides $x^{151} - 1$. Analogously, let $g(x) \in \mathbb{F}_2[x]$ be the polynomial defined by the next two cyclotomic cosets:

$$\big\{[2, 4, 8, 16, 32, 64, 128, 105, 59, 118, 85, 19, 38, 76, 1],$$

$$[10, 20, 40, 80, 9, 18, 36, 72, 144, 137, 123, 95, 39, 78, 5]\big\}.$$

If now $h(x) = x+1$, using the QC code $Q_2(f, g, h)$ and Theorem 5 we are able to construct a *stabilizer quantum code with parameters* $[[151, 106, 8]]_2$.

To testify the goodness of this code, we note that [7] only gives a quantum code with parameters $[[151, 106, 6]]_2$. In addition, according to [11], a code with parameters $[151, 128, 8]_2$ is the best known binary linear code with length 151 and minimum distance 8. In the unlikely case it were self-orthogonal for the Euclidean inner product, by using the CSS construction, we would get a $[[151, 105, 8]]_2$ code, with one unit less of dimension than our code.

Example 2. In this example we use again Theorem 5 for providing a stabilizer quantum code with good parameters.

Set $n = 73$ and $q = 2^3$. The splitting field of $x^{73}-1$ is $\mathbb{F}_{2^9}$. As in Example 1, considering a primitive element of this field, we consider the polynomial $f(x)$ (respectively, $g(x)$) in $\mathbb{F}_8[x]$ defined by the cyclotomic cosets

$$\{[8, 64, 1], [16, 55, 2], [24, 46, 3]\}$$

(respectively,

$$\{[8, 64, 1], [16, 55, 2], [24, 46, 3], [56, 10, 7]\}).$$

Taking $h(x) = x+1$, from $Q_2(f, g, h)$ we obtain a *stabilizer quantum code with parameters* $[[73, 52, 7]]_8$. A code with parameters $[73, 63, 7]_8$ is the best known binary linear code with length 73 and minimum distance 7 [11]. In the unlikely case it were self-orthogonal for the Euclidean inner product, by using the CSS construction, we would get a $[[73, 53, 7]]_8$ code, which has only one unit more of dimension than ours.

Now we are going to give a couple of binary quantum codes obtained from the procedure described in Section 3.

Example 3. Let $n = 73$ and consider the following polynomials in $\mathbb{F}_2[x]$: $f(x) = 1$, $h(x) = x^5 + x^4 + x^2 + x + 1$ and $g_i(x) = h(x)f_i(x)$, $1 \leq i \leq 3$, where

$$f_1(x) = x^9 + x^7 + x^4 + x^3 + 1,$$
$$f_2(x) = x^{18} + x^{16} + x^{12} + x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + x + 1 \quad \text{and}$$
$$f_3(x) = x^{27} + x^{26} + x^{25} + x^{24} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1.$$

The polynomials $f_1(x)$, $f_2(x)$ and $f_3(x)$ are determined, respectively, by cyclotomic cosets $\mathcal{I}_1$, $\mathcal{I}_2$ and $\mathcal{I}_3$, with respect to 2 modulo $n = 73$, such that $\mathcal{I}_1 \subset \mathcal{I}_2 \subset \mathcal{I}_3$. They provide linear codes with parameters $[73, 64, 3]_2, [73, 55, 5]_2$ and $[73, 46, 9]_2$.

Consider the QC codes $Q_i := Q_2(f, g_i, h)$, $1 \leq i \leq 3$. By construction of the polynomials $g_i(x)$ and by Proposition 11, it holds that

$$Q_1^\perp \subseteq Q_2^\perp \subseteq Q_3^\perp \subseteq Q_3 \subseteq Q_2 \subseteq Q_1.$$

Therefore, using the CSS procedure, we get binary stabilizer quantum codes C_1, C_2 and C_3 with parameters $[[146, 128, 3]]_2$, $[[146, 110, 5]]_2$ and $[[146, 74, 8]]_2$. Now, the Steane's enlargement applied to (the QC codes giving rise to) the codes C_1 and C_2 [25] provides a *binary stabilizer quantum code with parameters* $[[146, 119, 5]]_2$ which is better than one of the previous ones and exceeds the Gilbert-Varshamov bounds [8, 9, 20]. Analogously, the Steane's enlargement for C_2 and C_3 produces another stabilizer quantum code with parameters $[[146, 92, 8]]_2$.

Our next example is obtained by applying Theorem 16 where Hermitian inner product is used.

Example 4. Write $n = 80$, $q = 3$ and consider the following polynomials in $\mathbb{F}_9[x]$, which involve a primitive element ζ of $\mathbb{F}_9$, $f(x) = x + \zeta^5$, $h(x) = x^2 + \zeta^7 x + \zeta$ and

$$g(x) = x^9 + 2x^8 + \zeta^2 x^6 + 2x^5 + \zeta^5 x^4 + \zeta x^3 + \zeta^3 x^2 + \zeta^2.$$

These polynomials satisfy the requirements of Theorem 16 and, as a consequence, we get a *stabilizer quantum code with parameters* $[[160, 140, 5]]_3$.

Notice that this code exceeds the Gilbert-Varshamov bounds [8, 9, 20]. In addition, according to [11], a linear code with parameters $[160, 149, 5]_3$ is the best known linear ternary code with length $n = 160$ and minimum distance $d = 5$. In the unlikely case, it were self-orthogonal, the CSS procedure would give a quantum code with parameters $[[160, 138, 5]]_3$, which is worse than ours. We conclude by observing that we cannot reproduce this last procedure for self-orthogonality with respect to Hermitian duality because examples of length 160 over $\mathbb{F}_9$ are not provided in [11].

The polynomials $f, g \in \mathbb{F}_q[x]$ considered in Section 3 must divide the polynomial $x^n - 1$ which also divides $x^{q^m-1} - 1$, where $\mathbb{F}_{q^m}$ is the splitting field of $x^n - 1 \in \mathbb{F}_q[x]$. The polynomials f and g are also in $\mathbb{F}_{q^2}[x]$ and they could be used for obtaining stabilizer quantum codes as described in Section 4, however we should operate in a larger field without getting any improvement. Notice also that the above positive integer m has to be even if we desire to use the construction in Section 4 (where $x^n - 1 \in \mathbb{F}_{q^2}[x]$) and polynomials f or g with coefficients in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Some comments about comparison between the codes introduced in Section 3 and those given in Section 4 are included in our next,

and last, example. It should be interesting to compare the parameters of the quantum codes which can be obtained from Section 2 with those coming from Sections 3 and 4. This is not an easy problem since we need to consider different polynomials over distinct fields. Although we leave this question as an open problem for future research, we show some cases in the mentioned last example.

Example 5. One expects that, for reachable lengths and when comparison is possible, the quantum codes coming from Section 4 are better than those from Section 3. However CSS codes, as in Section 3, can sometimes be enlarged by the Steane's procedure [25] improving the initial codes as we showed in Example 3.

Let us see some comparative examples of our procedures and assume first that we look for quantum binary codes.

Let $n = 85$ and consider the following polynomials in $\mathbb{F}_2[x]$:

$$f(x) = 1, \;\; g(x) = x^8 + x^6 + x^5 + x^4 + x^2 + x + 1,$$

$$g_1(x) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x + 1, \text{ and } h(x) = x^6 + x^5 + x^3 + x^2 + 1.$$

The polynomials $f(x), g(x), h(x)$ (respectively, $f(x), g_1(x), h(x)$) satisfy the requirements in Theorem 13 and produce stabilizer quantum codes with parameters $[[170, 154, 3]]_2$ (respectively, $[[170, 138, 5]]_2$). One can apply the Steane's enlargement procedure to the above considered codes, giving rise to a quantum stabilizer code with parameters $[[170, 146, 5]]_2$. Consider now the following polynomials in $\mathbb{F}_4[x]$, where ζ is a primitive element of $\mathbb{F}_4$:

$$f(x) = 1, \;\; g(x) = x^{12} + \zeta x^{11} + \zeta x^{10} + \zeta^2 x^9 + x^8 + x^7 + \zeta^2 x^6 + \zeta x^5 + x^4 + x^3 + \zeta x^2 + x + 1,$$

$$\text{and} \quad h(x) = x^6 + x^5 + x^3 + x^2 + 1.$$

These polynomials satisfy the required conditions in Theorem 16 providing a quantum code whose parameters are $[[170, 146, 5]]_2$. As expected, one of the codes obtained from the construction in Section 3 is worse than that from Section 4, but with the construction in Section 3 and after applying the Steane's enlargement procedure, working in a smaller field, we obtain the same parameters. Notice also that we have got a good code which exceeds the Gilbert-Varshamov bounds [8, 9, 20].

We can choose many different polynomials to apply our results and, for the moment, to compare the codes coming from Section 2 with those from Sections 3 and 4 is an open problem. We tend to think that, generally speaking, quantum stabilizer codes from Section 2 might be better because they use a more general procedure as showed in [15], however this is not always true. Indeed, if we desire to construct a binary quantum code of length 170 using symplectic inner product and our quasi-cyclic codes, we need to use polynomials that divide the polynomial $x^{170} - 1$ which coincides with $(x^{85} - 1)^2$. Then our polynomials have to divide $x^{85} - 1$ but their corresponding cyclic codes are ideals of the ring $\mathbb{F}_2[x]/(x^{170} - 1)$, which seems to get worse the code. In fact, if we consider the above polynomials $f(x), g_1(x)$ and $h(x)$ in $\mathbb{F}_2[x]$ and apply Theorem 5, we obtain a stabilizer quantum code with parameters $[[170, 154, 2]]_2$, which is poor.

Finally, we show examples of ternary stabilizer quantum codes, obtained from the constructions in the paper, and where the best one corresponds to that obtained as described in Section 2. Consider the following polynomials in $\mathbb{F}_3[x]$:

$$f(x) = 1, \;\; g(x) = x^6 + x^3 + x^2 + 1,$$

$$g_1(x) = x^{12} + 2x^{10} + 2x^9 + 2x^8 + x^7 + 2x^6 + 2x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1,$$

$$\text{and} \quad h(x) = x^3 + x^2 + 2.$$

By Theorem 13 we obtain stabilizer quantum codes with parameters $[[182, 170, 3]]_3$ and $[[182, 158, 4]]_3$ which are suitable for applying the Steane's enlargement procedure which gives a $[[182, 164, 4]]_3$ quantum code.

If now we choose the following polynomials in $\mathbb{F}_9[x]$, where ζ is a primitive element of $\mathbb{F}_9$:

$$f(x) = 1, \;\; g(x) = x^9 + \zeta^6 x^8 + 2x^7 + \zeta^5 x^5 + \zeta^3 x^4 + 2x^3 + \zeta^3 x^2 + 2x + 2,$$
$$\text{and} \quad h(x) = x^3 + x^2 + 2,$$

then we obtain also a $[[182, 164, 4]]_3$ quantum code.

To finish, considering the polynomials in $\mathbb{F}_3[x]$:

$$f(x) = 1, \;\; g(x) = x^{12} + 2x^{11} + 2x^{10} + 2x^9 + x^7 + 2x^6 + 2x^4 + 2x^3 + x^2 + 1, \;\; \text{and}$$

$$h(x) = x^{15} + 2x^{14} + 2x^{13} + x^{12} + 2x^{11} + 2x^{10} + 2x^9 + x^8 + 2x^7 + 2x^6 + x^4 + 2x^3 + x^2 + x + 1,$$

and applying Theorem 5, we obtain a $[[182, 170, 4]]_3$ quantum code which exceeds the Gilbert-Varshamov bounds [8, 9, 20], while the above given ternary codes do not.

References

[1] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory* 47(7):3065–3072, Nov. 2001.

[2] A. Ashikhmin, S. Litsyn and M. A. Tsfasman. Asymptotically good quantum codes. *Phys. Rev. A* 63(3):032311, Mar. 2001.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* 78(3):405–408, Jan. 1997.

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

[5] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A* 54(2):1098–1105, Aug. 1996.

[6] D. Castelvecchi. Quantum computers ready to leap out of the lab in 2017. *Nature* 541(7635):9–10, Jan. 2017.

[7] Y. Edel Some good quantum twisted codes. Available at https://www.mathi.uni-heidelberg.de/ yves/.

[8] A. Ekert and C. Macchiavello. Quantum Error Correction for Communication. *Phys. Rev. Lett.* 77:2585-2588, Sept. 1996.

[9] K. Feng and Z. Ma. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inform. Theory* 50:3323-3325, Dec. 2004.

[10] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* 54(3):1862–1868, Sept. 1996.

[11] M. Grassl. Codetables. available at http://www.codetables.de/.

[12] M. Hagiwara and H. Imai. Quantum quasi-cyclic ldpc codes. In *Proc. 2007 IEEE ISIT*, pages 806–810, Nice, France, June 2007.

[13] M. Hagiwara, K. Kasai, H. Imai and K. Sakaniwa. Spacially-coupled quasi-cyclic quantum ldpc codes. In *Proc. 2011 IEEE ISIT*, pages 638–642, Nice, France, June 2007.

[14] T. Kasami. A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2. *IEEE Trans. Inform. Theory* 20:679, Sept. 1974.

[15] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inform. Theory* 52: 4892-4914, Nov 2006.

[16] K. Lally and P. Fitzpatrick. Algebraic structure of quasicyclic codes. *Discrete Appl. Math.* 11:157–175, July 2001.

[17] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 2nd edition, 2008.

[18] S. Ling, J. Luo and C. Xing. Generalization of Steane's enlargement construction of quantum codes and applications. *IEEE Trans. Inform. Theory* 56(8):4080–4084, Aug. 2010.

[19] S. Ling and P. Solé. Good self-dual quasi-cyclic codes exist. *IEEE Trans. Inform. Theory* 49(4):1052–1053, Apr. 2003.

[20] R. Matsumoto and T. Uyematsu. Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes. *IEICE Trans. Fundamentals* E83-A(10):1878–1883, Oct. 2000.

[21] J. Qian, W. Ma and X. Wang. Quantum error-correcting codes from quasi-cyclic codes. *Int. J. Quantum Inf.* 6(6):1263–1269, Dec. 2008.

[22] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* 52(4):2493–2496, Oct. 1995.

[23] A. M. Steane. Simple quantum error correcting codes *Phys. Rev. Lett.* 77(1954):793–797, Dec. 1996.

[24] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. Roy. Soc. London Ser. A* 452:2551–2577, Nov. 1996.
[25] A. M. Steane. Enlargement of Calderbank-Shor-Steane quantum codes. *IEEE Trans. Inform. Theory* 45:2492-2495, Dec. 1999.

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), `Ryutaroh Matsumoto:` Department of Information and Communication Engineering, Nagoya University, Nagoya, 464-8603 Japan.

E-mail address: `galindo@uji.es; carrillf@uji.es; ryutaroh.matsumoto@nagoya-u.jp`