IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 3, 2020, accepted January 13, 2020, date of publication January 17, 2020, date of current version January 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2967426

Asymmetric Entanglement-Assisted Quantum Error-Correcting Codes and BCH Codes

CARLOS GALINDO[1], FERNANDO HERNANDO[1], RYUTAROH MATSUMOTO[2,3], (Member, IEEE), AND DIEGO RUANO[4]

[1]Departamento de Matemáticas, Instituto Universitario de Matemáticas y Aplicaciones de Castellón, Universitat Jaume I, 12071 Castellón de la Plana, Spain
[2]Department of Information and Communication Engineering, Nagoya University, Nagoya 464-8603, Japan
[3]Department of Mathematical Sciences, Aalborg University, 9100 Aalborg, Denmark
[4]IMUVA-Mathematics Research Institute, University of Valladolid, 47011 Valladolid, Spain

Corresponding author: Ryutaroh Matsumoto (ryutaroh.matsumoto@nagoya-u.jp)

This work was supported in part by the Spanish Government MICINN/FEDER under Grant PGC2018-096446-B-C21, Grant PGC2018-096446-B-C22, and Grant RED2018-102583-T, in part by the Spanish Ministry of Economy and Competitiveness (MINECO) under Grant RYC-2016-20208 (AEI/FSE/UE), in part by the Generalitat Valenciana under Grant AICO-2019-223, in part by the Universitat Jaume I, under Grant P1-1B2018-10, in part by the Japan Society for the Promotion of Science (JSPS), Japan, under Grant 17K06419, and in part by the Junta de CyL, Spain, under Grant VA166G18.

ABSTRACT The concept of asymmetric entanglement-assisted quantum error-correcting code (asymmetric EAQECC) is introduced in this article. Codes of this type take advantage of the asymmetry in quantum errors since phase-shift errors are more probable than qudit-flip errors. Moreover, they use pre-shared entanglement between encoder and decoder to simplify the theory of quantum error correction and increase the communication capacity. Thus, asymmetric EAQECCs can be constructed from any pair of classical linear codes over an arbitrary field. Their parameters are described and a Gilbert-Varshamov bound is presented. Explicit parameters of asymmetric EAQECCs from BCH codes are computed and examples exceeding the introduced Gilbert-Varshamov bound are shown.

INDEX TERMS Asymmetric entanglement-assisted quantum error-correcting codes, asymmetric entanglement-assisted Gilbert-Varshamov bound, BCH codes.

I. INTRODUCTION

In the last decades the interest in quantum computation has grown exponentially, mainly because it transforms some intractable problems into tractable ones as showed the polynomial time algorithms given by Shor for discrete logarithms and prime factorization [41].

The usage of subatomic particles to hold memory and the application of quantum mechanics determine the behavior of quantum computers. These computers (the current implementations) are less reliable than the classical ones and produce more errors. Another inconvenient with this computers is decoherence and, even when one cannot clone quantum information [12], [45], both challenges can be addressed with quantum error correction [42], [43].

The first steps in the construction of quantum error-correcting codes corresponded to the binary case [8], [9], [22] (see also [2], [3], [25]). Afterwards and especially because of their interest in fault-tolerant computation the non-binary case was also studied [28] (some more references are [5], [6], [24], [29], [36]). Most of the quantum error-correcting codes are stabilizer codes where the error group is determined by eigenspaces with eigenvalue 1.

Sufficient (respectively, necessary) conditions for existence of (sometimes pure) quantum codes are given by the Gilbert-Varshamov bounds [13], [17], [28], [37] (respectively, quantum singleton or Hamming bounds [4], [24], [28], [39]).

Unitary operators, usually denoted X and Z, are used to provide quantum (error-correcting) codes and the minimum distance d of such codes indicates that one can correct up to $\lfloor (d-1)/2 \rfloor$ phase-shift and qudit-flip errors. In [27], the authors noticed that phase-shift errors happened more likely than qudit-flip errors, thus it was desirable to construct quantum codes where two minimum distances d_x and d_z, for detecting qudit-flip and phase-shift errors, respectively, were considered and provide results for addressing their behavior. As a consequence, in the last years asymmetric

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

quantum error-correcting codes have been studied giving rise to codes suitable when dephasing occurs more often than relaxation [14]–[16], [31], [32], [40]. Most of the asymmetric quantum codes come from the CSS construction of quantum stabilizer codes and, for them, there is also a Gilbert-Varshamov bound [35]. In addition, the existence of an asymmetric quantum error-correcting code coming from the CSS construction can also be applied to linear ramp secret sharing and communication over wiretap channels of type II [19].

To provide an asymmetric (or symmetric) quantum code requires some type of self-orthogonality of the classical constituent code (or an inclusion of a constituent code into the dual of other constituent one) and, then, many good classical codes cannot be considered for that purpose. For overcoming this restriction and boosting the rate of transmission, it was proposed in [7] (for the symmetric case) to share entanglement between encoder and decoder. Some constructions of this type for binary codes (and also for codes over finite fields $\mathbb{F}_p, p$ prime) can be found in the literature [26], [34], [44]. The case when the codes are supported in an arbitrary finite field has been described in [21].

It seems clear that it remains to consider entanglement-assisted quantum error-correcting codes (EAQECCs) for the asymmetric case. To the best of our knowledge this task had not been performed yet. Section II of this paper is devoted to explain how to construct and which are the parameters of an asymmetric EAQECC obtained from any two linear classical codes. Theorem 3 and Theorem 4 (for nested constituent codes) are the main results in this section. Section III gives a Gilbert-Varshamov bound for asymmetric EAQECCs; we state and prove this bound for both the finite and the asymptotic case. In Section IV we present the explicit computation of the parameters of asymmetric EAQECCs coming from BCH codes, see Theorem 9 and Corollary 10. Finally, our Section VI provides examples of asymmetric EAQECCs which exceed the Gilbert-Varshamov bound before stated. Notice that asymmetric EAQECCs give rise to (symmetric) EAQECCs and in this section we show also examples of EAQECCs obtained with our procedure exceeding the Gilbert-Varshamov bound for EAQECCs.

II. ASYMMETRIC EAQECCS

Let $q = p^r$ a positive power of a prime number p and set $\mathbb{F}_q$ the finite field of order q. A q-ary *stabilizer quantum code* is the linear space of $(\mathbb{C}^q)^n$ given by the intersection of the eigenspaces with eigenvalue 1 corresponding to some subgroup S of the error group G_n generated by the matrices corresponding to a basis of $\mathrm{Hom}\left((\mathbb{C}^q)^{\otimes n}, (\mathbb{C}^q)^{\otimes n}\right)$, that is G_n is determined by the product $X(\mathbf{a})Z(\mathbf{b})$ of tensor products $X(\mathbf{a}) = X(a_1) \otimes X(a_2) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{b}) = Z(b_1) \otimes Z(b_2) \otimes \cdots \otimes Z(b_n)$ of unitary operators X and Z over $\mathbb{C}^q$, where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, $\mathbf{b} = (b_1, b_2, \ldots, b_n)$, and $a_i, b_i \in \mathbb{F}_q$, $1 \leq i \leq n$. It is known [28, Lemma 11] that an error in G_n is detectable by the stabilizer code if and only if it belongs to the group generated by the subgroup S and the center of G_n or the error is not in the centralizer of S in G_n.

The above facts can be regarded in terms of additive codes in $\mathbb{F}_q^{2n}$. In order to do this, we introduce the trace-symplectic form for two vectors $(\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \in \mathbb{F}_q^{2n}$ as follows:

$$(\mathbf{a}|\mathbf{b}) \cdot_{ts} (\mathbf{a}'|\mathbf{b}') = \mathrm{tr}_{q|p}(\mathbf{a} \cdot \mathbf{b}' - \mathbf{a}' \cdot \mathbf{b}) \in \mathbb{F}_p,$$

where $\mathrm{tr}_{q|p}$ is the trace map and $\cdot$ the inner product in $\mathbb{F}_q^n$. Then (in the linear case) an $[[n, k, d]]_q$ stabilizer quantum code exists if and only if there is a linear code $C \subseteq \mathbb{F}_q^{2n}$ of dimension $n-k$ such that $C \subseteq C^{\perp_{ts}}$, where $C^{\perp_{ts}}$ stands for the dual code with respect to the $\cdot_{ts}$ product. Here the minimum distance d is determined by the minimum symplectic weight $\mathrm{swt}(C^{\perp_{ts}} \setminus C)$. It is convenient to recall that for $(\mathbf{a}|\mathbf{b})$ as above,

$$\mathrm{swt}(\mathbf{a}|\mathbf{b}) = \#\left\{j \in \{1, 2, \ldots, n\} | (a_j, b_j) \neq (0, 0)\right\},$$

meaning cardinality.

A particular case in the above construction follows from the so-called CSS (Calderbank-Shor-Steane) procedure [9], [43]. Here we need two linear codes C_1 and C_2 in $\mathbb{F}_q^n$ such that $C_2 \subseteq C_1^{\perp}$, $\perp$ means Euclidean duality, and then the code $C = C_1 \times C_2 \subseteq \mathbb{F}_q^{2n}$ provides a stabilizer quantum code whose parameters depend on those of C_1 and C_2. Some classical references are [5], [6], [8]–[10].

The fact that dephasing usually happens much more often that relaxation [27] motivated the study and searching of asymmetric quantum error-correcting codes [14]–[16], [30]–[33]. For this purpose, the most used procedure is the CSS construction because it easily allows us to get parameters d_z and d_x such that our previous stabilizer code detects phase-shift (respectively, qudit-flip) errors up to weight $d_z - 1$ (respectively, $d_x - 1$). The specific result (see [40, Lemma 3.1]) states that

Theorem 1: Let $C_2 \subset C_1^{\perp} \subseteq \mathbb{F}_q^n$ be linear codes. The CSS construction gives rise to an asymmetric quantum code with parameters $[[n, \dim C_1^{\perp} - \dim C_2, d_z/d_x]]_q$, where d_z (respectively, d_x) is the minimum Hamming weight of the set $C_1^{\perp} \setminus (C_2 \cap C_1^{\perp})$ (respectively, $C_2^{\perp} \setminus (C_1 \cap C_2^{\perp})$).

The previously mentioned stabilizer and asymmetric quantum codes require self-orthogonality conditions with respect to trace-symplectic duality and not every classical linear code can be used for providing those quantum codes. The self-orthogonality condition can be bypassed if encoder and decoder share some quantity of entanglement [7] giving rise to the so called entanglement-assisted quantum error-correcting codes (EAQECCs). In the binary case the construction of these codes is described in [26] (third paragraph of Section II). This construction also holds for codes over finite fields of the type $\mathbb{F}_p, p$ being a prime number (see [44, Remark 1] and [34] for a proof). There it is proved that one can obtain an EAQECC from a classical code $C \subseteq \mathbb{F}_p^{2n}$ such that $C \not\subseteq C^{\perp_{ts}}$ and the set of detectable quantum errors is given by

$$\left(C \cap C^{\perp_{ts}}\right) \cup \left(\mathbb{F}_p^{2n} \setminus C^{\perp_{ts}}\right).$$

On $\mathbb{F}_q^{2n}$, $q = p^r$, one can also define a symplectic product:

$$(\mathbf{a}|\mathbf{b}) \cdot_s (\mathbf{a}'|\mathbf{b}') = (\mathbf{a}\cdot\mathbf{b}' - \mathbf{a}'\cdot\mathbf{b}) \in \mathbb{F}_q.$$

Using a suitable basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, an isomorphism of $\mathbb{F}_p$-linear spaces $\phi : \mathbb{F}_p^{2r} \to \mathbb{F}_q^2$ can be given, providing an isomorphism of $\mathbb{F}_p$-linear spaces

$$\phi^E : \left(\mathbb{F}_p^r\right)^n \times \left(\mathbb{F}_p^r\right)^n \to \mathbb{F}_q^{2n}.$$

With the help of ϕ^E, in [21], the results of EAQECCs over $\mathbb{F}_p$ can be extended to $\mathbb{F}_q$ and the product $\cdot_s$ instead of $\cdot_{ts}$. Indeed, the following result holds:

Theorem 2: Let $C \subseteq \mathbb{F}_q^{2n}$ be a linear code over $\mathbb{F}_q$ of dimension $(n-k)$. Denote by $H = (H_X|H_Z)$ a generator matrix for C. Let $C' \subseteq \mathbb{F}_q^{2(n+c)}$ be a linear code over $\mathbb{F}_q$ whose projection to the coordinates $1, 2, \ldots, n, n+c+1, n+c+2, \ldots, 2n+c$ equals C and such that $C' \subseteq (C')^{\perp_s}$, c being the minimum required number of maximally entangled quantum states in $\mathbb{C}^q \otimes \mathbb{C}^q$. Then,

$$\begin{aligned} 2c &= \operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right) \\ &= \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}\left(C \cap C^{\perp_s}\right). \end{aligned}$$

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathbb{C}^q \otimes \cdots (k+c \text{ times}) \cdots \otimes \mathbb{C}^q$ into n physical qudits using c maximally entangled pairs. The minimum distance is

$$\begin{aligned} d &= d_s\left(C^{\perp_s} \setminus (C \cap C^{\perp_s})\right) \\ &= \min\left\{\operatorname{swt}(\mathbf{a}|\mathbf{b}) \mid (\mathbf{a}|\mathbf{b}) \in C^{\perp_s} \setminus (C \cap C^{\perp_s})\right\}. \end{aligned}$$

As a consequence, C provides an $[[n, k+c, d; c]]_q$ EAQECC over the field $\mathbb{F}_q$.

In this paper we are interested in the asymmetric case and we desire to construct asymmetric EAQECCs from two linear codes C_1 and C_2 over an arbitrary finite field $\mathbb{F}_q$. Assume that H_1 (respectively, H_2) is a generator matrix of C_1 (respectively, C_2).

The above described construction of stabilizer codes over $\mathbb{F}_p$ following the CSS procedure determines asymmetric EAQECCs coming from any two linear codes $C_1, C_2 \subseteq \mathbb{F}_p^n$. Here the code C over $\mathbb{F}_p^{2n}$ is $C = C_1 \times C_2$ and $C^{\perp_s} = C_2^{\perp} \times C_1^{\perp}$, where $\perp$ denotes the Euclidean dual. Notice that in this case $\cdot_{ts} = \cdot_s$. The set of detectable errors is

$$\begin{aligned} \left((C_1 \cap C_2^{\perp}) \times (C_2 \cap C_1^{\perp})\right) \cup \left(\mathbf{F}_p^{2n} \setminus C_2^{\perp} \times C_1^{\perp}\right) \\ = \left((C_1 \cap C_2^{\perp}) \cup (\mathbf{F}_p^n \setminus C_2^{\perp})\right) \\ \times \left((C_2 \cap C_1^{\perp}) \cup (\mathbf{F}_p^n \setminus C_1^{\perp})\right). \end{aligned}$$

Defining

$$d_z = \operatorname{wt}\left(C_1^{\perp} \setminus (C_2 \cap C_1^{\perp})\right) \text{ and } d_x = \operatorname{wt}\left(C_2^{\perp} \setminus (C_1 \cap C_2^{\perp})\right), \tag{1}$$

where wt means minimum Hamming weight, it is clear we are able to construct an asymmetric EAQECC which can detect up to $d_x - 1$ qudit-flip errors and up to $d_z - 1$ phase-shift errors.

These results can be extended to any finite field $\mathbb{F}_q$ using again the above described isomorphism ϕ^E and [21, Proposition 1] which relates $\cdot_{st}$ and $\cdot_s$. The general result being:

Theorem 3: Consider linear codes $C_i \subseteq \mathbb{F}_q^n$ of dimension k_i and generator matrix H_i, $i = 1, 2$. Set d_x and d_z as in (1).

Then $C_1 \times C_2 \subseteq \mathbb{F}_q^{2n}$ gives rise to an asymmetric EAQECC which encodes $n - k_1 - k_2 + c$ logical qudits into n physical qudits which can correct up to $\lfloor (d_x - 1)/2 \rfloor$ qudit-flip errors and up to $\lfloor (d_z - 1)/2 \rfloor$ phase-shift errors. The minimum required of maximally entangled pairs is

$$c = \operatorname{rank}(H_1 H_2^T) = \dim C_1 - \dim(C_1 \cap C_2^{\perp}).$$

As a consequence, we obtain an

$$[[n, n - k_1 - k_2 + c, d_z/d_x; c]]_q$$

asymmetric EAQECC.

We end this section with a result that assumes that our constituent linear codes are nested. We will see that the asymmetric EAQECC comes from puncturing a code in $\mathbb{F}_q^{2n}$.

Theorem 4: Let C_1 and C_2 be $\mathbb{F}_q$-linear codes such that $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$. Set $k_i = \dim C_i$, $i \in \{1, 2\}$ and $d_1^{\perp}$ (respectively, d_2) the minimum distance of the code $C_1^{\perp}$ (respectively, C_2). Suppose that c is a positive integer such that it satisfies $1 \leq c \leq \min\{d_1^{\perp}, d_2\} - 1$. Then, there exists an asymmetric EAQECC with parameters

$$[[n - c, k_1 - k_2 + c, d_z/d_x; c]]_q,$$

where d_z (respectively, d_x) is the minimum Hamming weight of the elements in the set $C_2^{\perp} \setminus C_1^{\perp}$ (respectively, $C_1 \setminus C_2$).

Proof: Consider the code $C = C_2 \times C_1^{\perp}$, then $C \subseteq C^{\perp_s} = C_1 \times C_2^{\perp}$ and $2c \leq \operatorname{wt}(C \setminus \mathbf{0}) - 1$, and the result follows from [21, Theorem 7] and (1).

Notice that the above asymmetric EAQECC comes from the punctured code defined as

$$P(C) = \left\{ (\operatorname{pr}(\mathbf{a}), \operatorname{pr}(\mathbf{b}) \mid (\mathbf{a}, \mathbf{b}) \in C \right\},$$

pr being the projection to the first $n - c$ coordinates. In fact, according to the proof of [21, Theorem 9]

$$\dim P(C) - \dim\left(P(C) \cap P(C)^{\perp_s}\right) = 2c,$$

which by Theorem 2 shows that c is the number of maximally entangled pairs. □

III. A GILBERT-VARSHAMOV BOUND FOR ASYMMETRIC EAQECCS

We devote this section to provide a finite and an asymptotic Gilbert-Varshamov-type (GV) bound for asymmetric EAQECCs. We start with the finite case.

A. THE FINITE GV BOUND

Let us start with our result.

Theorem 5: Consider positive integer numbers n, k_1, k_2, d_z, d_x and c such that $k_1 \leq n$, $k_2 \leq n$ and

$$k_1 + k_2 - n \leq c \leq \min\{k_1, k_2\},$$

which satisfy the following inequality

$$\frac{q^{n-k_1} - q^{k_2-c}}{q^n - 1} \sum_{i=1}^{d_z-1} \binom{n}{i}(q-1)^i + \frac{q^{n-k_2} - q^{k_1-c}}{q^n - 1} \sum_{i=1}^{d_x-1} \binom{n}{i}(q-1)^i < 1,$$

then there exists an $[[n, n-k_1-k_2+c, d_z/d_x; c]]_q$ asymmetric EAQECC.

Proof: For simplicity sake, in this proof C_2' will be used instead of $C_2^\perp$. Consider integer numbers n, k_1, k_2 and c as in the statement. Define

$$\begin{aligned} A(n, k_1, k_2, c) = \big\{(C_1, C_2') \mid C_1, C_2' \subset \mathbf{F}_q^n, \\ \dim C_1 = k_1, \dim C_2' = n - k_2, \text{ and} \\ c = \dim C_1 - \dim(C_1 \cap C_2')\big\}. \end{aligned}$$

For $\mathbf{v} \in \mathbf{F}_q^n$, define also

$$B_z(\mathbf{v}) = \big\{(C_1, C_2') \in A(n, k_1, k_2, c) \mid \mathbf{v} \in C_1^\perp \setminus (C_2'^\perp \cap C_1^\perp)\big\}$$

and

$$B_x(\mathbf{v}) = \big\{(C_1, C_2') \in A(n, k_1, k_2, c) \mid \mathbf{v} \in C_2' \setminus (C_1 \cap C_2')\big\}.$$

For nonzero $\mathbf{v}_1$ and $\mathbf{v}_2 \in \mathbf{F}_q^n$, we claim that

$$\#B_z(\mathbf{v}_1) = \#B_z(\mathbf{v}_2),$$

where we recall that # means cardinality.

Let us see a proof. Denote by $GL(n, q)$ the set of invertible matrices on $\mathbf{F}_q^n$ and for a fixed $(D_1, D_2') \in A(n, k_1, k_2, c)$, a fixed $M_1 \in GL(n, q)$ with $M_1\mathbf{v}_1 = \mathbf{v}_2$ and $M_1' \in GL(n, q)$ with $M_1'\text{span}(\mathbf{v}_1)^\perp = \text{span}(\mathbf{v}_2)^\perp$, where $M_1'\text{span}(\mathbf{v}_1)^\perp$ stands for the linear space given by the products $M_1'\mathbf{w}$ such that $\mathbf{w} \in \text{span}(\mathbf{v}_1)^\perp$. Then we have

$$\begin{aligned} &\#B_z(\mathbf{v}_1) \\ &= \#\big\{(C_1, C_2') \in A(n, k_1, k_2, c) \mid \\ &\quad \mathbf{v}_1 \in C_1^\perp \setminus (C_2'^\perp \cap C_1^\perp)\big\} \\ &= \#\big\{(C_1, C_2') \in A(n, k_1, k_2, c) \mid \text{span}(\mathbf{v}_1)^\perp \supseteq C_1 \\ &\quad \text{and } \text{span}(\mathbf{v}_1)^\perp \not\supseteq C_2'\big\} \\ &= \#\big\{(MD_1, MD_2') \mid \text{span}(\mathbf{v}_1)^\perp \supseteq MD_1 \\ &\quad \text{and } \text{span}(\mathbf{v}_1)^\perp \not\supseteq MD_2', M \in GL(n, q)\big\} \\ &= \#\big\{(M_1'MD_1, M_1'MD_2') \mid M_1'\text{span}(\mathbf{v}_1)^\perp \supseteq M_1'MD_1 \\ &\quad \text{and } M_1'\text{span}(\mathbf{v}_1)^\perp \not\supseteq M_1'MD_2', M \in GL(n, q)\big\} \\ &= \#\big\{(M_1'MD_1, M_1'MD_2') \mid \text{span}(\mathbf{v}_2)^\perp \supseteq M_1'MD_1 \\ &\quad \text{and } \text{span}(\mathbf{v}_2)^\perp \not\supseteq M_1'MD_2', M_1'M \in GL(n, q)\big\} \\ &= \#B_z(\mathbf{v}_2). \end{aligned}$$

We also claim that $\#B_x(\mathbf{v}_1) = \#B_x(\mathbf{v}_2)$. Indeed,

$$\begin{aligned} &\#B_x(\mathbf{v}_1) \\ &= \#\big\{(C_1, C_2') \in A(n, k_1, k_2, c) \mid \mathbf{v}_1 \in C_2' \setminus (C_2' \cap C_1)\big\} \\ &= \#\big\{(MD_1, MD_2') \mid \mathbf{v}_1 \in MD_2' \setminus (MD_2' \cap MD_1), \\ &\quad M \in GL(n, q)\big\} \\ &= \#\big\{(M_1MD_1, M_1MD_2') \mid \\ &\quad M_1\mathbf{v}_1 \in M_1MD_2' \setminus (M_1MD_2' \cap M_1MD_1), \\ &\quad M_1M \in GL(n, q)\big\} \\ &= \#\big\{(MD_1, MD_2') \mid M_1\mathbf{v}_1 \in MD_2' \setminus (MD_2' \cap MD_1), \\ &\quad M \in GL(n, q)\big\} \\ &= \#B_x(\mathbf{v}_2). \end{aligned}$$

Next we will count the quantity of triples $(\mathbf{v}, C_1, C_2')$ such that $\mathbf{v} \in C_1^\perp \setminus (C_2'^\perp \cap C_1^\perp)$ in two different ways. From [21, Proposition 4] and the fact that the rank of a matrix and its transpose coincide, we deduce that

$$c = \dim C_1 - \dim\left(C_1 \cap C_2^\perp\right) = \dim C_2 - \dim\left(C_2 \cap C_1^\perp\right).$$

Then, we observe that

$$\begin{aligned} \dim C_2'^\perp \cap C_1^\perp &= \dim C_2 \cap C_1^\perp \\ &= \dim C_2 - (\dim C_2 - \dim C_2 \cap C_1^\perp) = k_2 - c. \end{aligned}$$

For each pair $(C_1, C_2') \in A(n, k_1, k_2, c)$ there are

$$q^{n-k_1} - q^{k_2-c}$$

vectors $\mathbf{v}$ such that $\mathbf{v} \in C_1^\perp \setminus (C_2'^\perp \cap C_1^\perp)$. Thus the total number of such triples is

$$(q^{n-k_1} - q^{k_2-c})\#A(n, k_1, k_2, c).$$

On the other hand, we can count the total number of triples as

$$\sum_{\mathbf{0} \neq \mathbf{w} \in \mathbf{F}_q^n} \#B_z(\mathbf{w}) = (q^n - 1)\#B_z(\mathbf{v})$$

for any fixed nonzero $\mathbf{v}$. This implies

$$\frac{\#B_z(\mathbf{v})}{\#A(n, k_1, k_2, c)} = \frac{q^{n-k_1} - q^{k_2-c}}{q^n - 1}.$$

A similar argument shows

$$\frac{\#B_x(\mathbf{v})}{\#A(n, k_1, k_2, c)} = \frac{q^{n-k_2} - q^{k_1-c}}{q^n - 1}.$$

If we remove a pair (C_1, C_2') from $A(n, k_1, k_2, c)$ either when $\mathbf{v}_z \in C_1^\perp \setminus (C_2'^\perp \cap C_1^\perp)$ or when $\mathbf{v}_x \in C_2' \setminus (C_2' \cap C_1)$ for $1 \leq \text{wt}(\mathbf{v}_z) \leq d_z - 1$ and for $1 \leq \text{wt}(\mathbf{v}_x) \leq d_x - 1$, then we remove in total

$$\sum_{1 \leq \text{wt}(\mathbf{v}_z) \leq d_z - 1} \#B_z(\mathbf{v}_z) + \sum_{1 \leq \text{wt}(\mathbf{v}_x) \leq d_x - 1} \#B_x(\mathbf{v}_x) \qquad (2)$$

pairs from $A(n, k_1, k_2, c)$.

As a consequence, there exists at least one

$$[[n, n - k_1 - k_2 + c, d_z/d_x; c]]_q$$

asymmetric EAQECC whenever the number (2) is less than $\#A(n, k_1, k_2, c)$ which proves the statement. □

B. THE ASYMPTOTIC GV BOUND

From Theorem 5 and [37], it can be deduced the following asymptotic GV bound.

Theorem 6: Consider positive real numbers $K_1, K_2, \delta_z, \delta_x$ and λ such that

$$K_1 + K_2 - 1 \leq \lambda \leq \min\{K_1, K_2\}.$$

Set $h_q(y) := -y\log_q y - (1-y)\log_q(1-y)$ the q-ary entropy function. If the inequalities

$$h_q(\delta_z) + \delta_z \log_q(q-1) < K_1 \quad \text{and}$$
$$h_q(\delta_x) + \delta_x \log_q(q-1) < K_2$$

hold, then, for sufficiently large n, there exists an asymmetric EAQECC with parameters

$$\left[\left[n, \lfloor n - nK_1 - nK_2 + n\lambda\rfloor, \lfloor n\delta_z\rfloor/\lfloor n\delta_x\rfloor; \lfloor n\lambda\rfloor\right]\right]_q.$$

IV. ASYMMETRIC EAQECCS FROM BCH CODES

The aim of this section is the construction of asymmetric EAQECCs with good parameters by using the results in Section II. To carry it out, we consider specific BCH codes. Instead of the classical way, our BCH codes are regarded as subfield-subcodes of evaluation codes defined by evaluating univariate polynomials [11]. We consider this construction because it can be extended to evaluation by polynomials in several variables [18], [20] which we hope will give better codes in the future.

Let ℓ be a positive integer such that r divides ℓ and consider a positive integer N such that $N-1$ divides $p^\ell - 1$. In this section, we use classes of univariate polynomials in the quotient ring $\mathbb{F}_{p^\ell}[X]/I$, where I is the ideal of $\mathbb{F}_{p^\ell}[X]$ generated by $X^{N-1} - 1$. If $Z = \{P_1, P_2, \ldots, P_n\}$, where $n = N-1$, is the zero set of I in $\mathbb{F}_{p^\ell}$, we define the evaluation map

$$\mathrm{ev} : \mathbb{F}_{p^\ell}[X]/I \to \mathbb{F}_{p^\ell}^n \quad \mathrm{ev}(f) = (f(P_1), f(P_2), \ldots, f(P_n)).$$

Assume that Δ is a subset of $\mathcal{H} := \{0, 1, \ldots, N-2\}$, then we write E_Δ the code in $\mathbb{F}_{p^\ell}^n$ generated by the vectors

$$\left\{\mathrm{ev}\left(X^i\right) \mid i \in \Delta\right\}.$$

Within the congruence ring $\mathbb{Z}_{N-1}$, we consider minimal cyclotomic cosets with respect to $q = p^r$; minimal means that it contains exactly the elements of the form $aq^t, t \geq 0$ in $\mathbb{Z}_{N-1}$ for some fixed element $a \in \mathbb{Z}_{N-1}$ under the identification $\mathbb{Z}_{N-1} = \mathcal{H}$. Pick a representative a (the least one) of each minimal cyclotomic coset which we denote $\mathfrak{I}_a$. Then $\{\mathfrak{I}_a\}_{a\in\mathcal{A}}$ is the set of minimal cyclotomic cosets with respect to q, $\mathcal{A}$ being the set of representatives above mentioned. In addition set $i_a := \#(\mathfrak{I}_a)$. For convenience, we will write

$$\mathcal{A} = \{a_0 = 0 < a_1 < a_2 < \cdots\} = \{a_j\}_{j=0}^z.$$

We will use the following two results which can be found in [18], [20].

Proposition 7: Set $\Delta = \cup_{j=t'}^t \mathfrak{I}_{a_j}$, $t' < t$. Then the subfield-subcode of E_Δ over $\mathbb{F}_q$,

$$E_\Delta|_{\mathbb{F}_q} := E_\Delta \cap (\mathbb{F}_q)^n,$$

has dimension $\sum_{j=t'}^t i_{a_j}$.

Proposition 8: The minimum distance of the (Euclidean) dual of the subfield-subcode $E_\Delta|_{\mathbb{F}_q}$, where $\Delta = \cup_{j=0}^t \mathfrak{I}_{a_j}$ is larger than or equal to $a_{t+1} + 1$ (BCH bound).

Next we state the main result in this section.

Theorem 9: With the above notation consider two different indices $s, t \in \{0, 1, \ldots, z\}$ and assume that $s < t$. Then we can construct an asymmetric EAQECC with parameters

$$\left[\left[n, n - \sum_{j=0}^t i_{a_j}, (a_{t+1} + 1/a_{s+1} + 1); \sum_{j=0}^s i_{a_j}\right]\right]_q.$$

Proof: Consider the linear codes $C_i = E_{\Delta_i}|_{\mathbb{F}_q}$, $i = 1, 2$, where $\Delta_1 = \bigcup_{j=0}^t \mathfrak{I}_{a_j}$ and $\Delta_2 = \bigcup_{j=0}^s \mathfrak{I}_{a'_j}$, a'_j being the representative of the minimal cyclotomic coset containing $N - 1 - a_j$. Taking into account that $\#\mathfrak{I}_{a'_j} = \#\mathfrak{I}_{a_j}$, by Proposition 7 it holds that $k_1 := \dim C_1 = \sum_{j=0}^t i_{a_j}$ and $k_2 := \dim C_2 = \sum_{j=0}^s i_{a_j}$.

Now $C_2^\perp = E_{\Delta'}|_{\mathbb{F}_q}$, where $\Delta' = \mathcal{H} \setminus \bigcup_{j=0}^s \mathfrak{I}_{a_j}$ [18]. Hence, the minimum required of maximally entangled pairs is

$$\begin{aligned} c &= \dim C_1 - \dim(C_1 \cap C_2^\perp) \\ &= \sum_{j=0}^t i_{a_j} - \sum_{j=s+1}^t i_{a_j} = \sum_{j=0}^s i_{a_j}. \end{aligned}$$

The minimum distance of the dual codes satisfies $d(C_1^\perp) \geq a_{t+1} + 1$ (by Proposition 8) and $d(C_2^\perp) \geq a_{s+1} + 1$ because C_2 contains $s+1$ consecutive cyclotomic cosets and it is equivalent to a code as in Proposition 8.

Finally, applying Theorem 3, we get an asymmetric EAQECC with parameters as in the statement. □

From the previous result, we can deduce the following one.

Corollary 10: Keeping the above notation where $q = p^r$, assume that

$$\left(p^r\right)^{\lfloor \frac{\ell}{2r}\rfloor} < n \leq p^\ell - 1 \tag{3}$$

and pick and index t such that

$$2 \leq a_{t+1} \leq \min\left\{\frac{n\,(p^r)^{\lfloor \frac{\ell}{2r}\rfloor}}{p^\ell - 1}, n\right\}. \tag{4}$$

Let $s \in \{0, 1, \ldots, z\}$ such that $s < t$. Then we can construct an asymmetric EAQECC with parameters

$$\left[\left[n, n - \frac{\ell}{r}\left\lceil\left(a_{t+1} - 1\right)\left(1 - \frac{1}{q}\right)\right\rceil - 1,\right.\right.$$
$$\left.\left.(a_{t+1} + 1/a_{s+1} + 1); \frac{\ell}{r}\left\lceil\left(a_{s+1} - 1\right)\left(1 - \frac{1}{q}\right)\right\rceil + 1\right]\right]_q.$$

Proof: It follows from the proof of [1, Theorem 10] where it is showed that if Inequalities (3) and (4) hold, then the number t of non-zero cyclotomic cosets considered is

$$\left\lceil (a_{t+1} - 1)(1 - \frac{1}{q}) \right\rceil$$

and all of them have cardinality ℓ/r. □

TABLE 1. Asymmetric EAQECC coming from Theorem 9.

q	n	k_1	k_2	c	$d_z = d(C_1^\perp)$	$d_x = d(C_2^\perp)$	$(\mathfrak{d}_z, \mathfrak{d}_x)$	Cyclotomic Cosets Defining C_1	Cyclotomic Cosets Defining C_2
4	15	3	1	1	3	2	(2,1)	$\{0,1\}$	$\{0\}$
5	24	5	3	3	4	3	(2,2)	$\{0,1,2\}$	$\{0,23\}$
7	19	7	4	4	5	3	(4,2)	$\{0,1,2\}$	$\{0,18\}$
7	19	13	10	10	9	6	(8,6)	$\{0,1,2,4,5\}$	$\{0,15,17,18\}$
8	63	7	1	1	5	2	(3,1)	$\{0,1,2,3\}$	$\{0\}$
8	63	11	3	3	7	3	(5,2)	$\{0,1,2,3,4,5\}$	$\{0,62\}$
9	40	10	5	5	7	4	(5,3)	$\{0,1,2,3,4,5\}$	$\{0,38,39\}$
9	40	12	3	3	8	3	(6,2)	$\{0,1,2,3,4,5,6\}$	$\{0,39\}$
9	40	12	7	7	8	5	(6,3)	$\{0,1,2,3,4,5,6\}$	$\{0,37,38,39\}$
16	51	9	3	3	6	3	(5,2)	$\{0,1,2,3,4\}$	$\{0,50\}$
16	51	11	1	1	7	2	(6,1)	$\{0,1,2,3,4\}$	$\{0,50\}$
16	51	11	3	3	7	3	(6,2)	$\{0,1,2,3,4,5\}$	$\{0,50\}$
16	51	17	5	5	10	4	(10,3)	$\{0,1,2,3,4,5,6,7,8\}$	$\{0,49,50\}$
16	51	19	5	5	12	4	(11,3)	$\{0,1,2,3,4,5,6,7,8,9\}$	$\{0,49,50\}$
16	51	23	3	3	15	3	(14,2)	$\{0,1,2,3,4,5,6,7,8,9,11,12\}$	$\{0,50\}$
16	51	23	9	9	15	6	(14,5)	$\{0,1,2,3,4,5,6,7,8,9,11,12\}$	$\{0,47,48,49,50\}$
16	51	27	5	5	18	4	(17,3)	$\{0,1,2,3,4,5,6,7,8,9,11,12,14,15\}$	$\{0,49,50\}$
25	48	6	4	4	5	4	(4,2)	$\{0,1,2,3\}$	$\{0,46,47\}$
25	48	10	4	4	8	4	(6,2)	$\{0,1,2,3,4,5,6\}$	$\{0,46,47\}$
25	48	10	7	7	8	6	(6,4)	$\{0,1,2,3,4,5,6\}$	$\{0,44,45,46,47\}$
25	48	12	3	3	9	3	(7,2)	$\{0,1,2,3,4,5,6,7\}$	$\{0,47\}$
25	48	12	6	6	9	5	(7,4)	$\{0,1,2,3,4,5,6,7\}$	$\{0,45,46,47\}$

Remark 11: Notice that the parameters of the asymmetric EAQECC given in Corollary 10 can be written as follows:

$$\left[\left[n, n-\frac{\ell}{r}t-1, (a_{t+1}+1/a_{s+1}+1); \frac{\ell}{r}s+1\right]\right]_q.$$

V. ENTANGLEMENT AND MINIMUM DISTANCES

Assume that C is a (standard) asymmetric quantum code over a field $\mathbb{F}_q$ coming from the CSS construction with parameters $[[n, k, d_z/d_x]]_q$. Considering entanglement and a suitable extension of constituent codes, it is possible to increase the value of d_z (or d_x) keeping the length and information rate. Therefore, one may increase the asymmetry ratio (the ratio between d_z and d_x). Indeed, for both the standard case and the entanglement-assisted case, one considers two linear codes C_1 and C_2 and it holds that $d_z = \mathrm{wt}(C_1^\perp \setminus (C_2 \cap C_1^\perp))$ and $d_x = \mathrm{wt}(C_2^\perp \setminus (C_1 \cap C_2^\perp))$. However, for the standard case it must be imposed that $C_2 \subseteq C_1^\perp$. Thus, given a pair of codes C_1, C_2 such that $C_2 \subseteq C_1^\perp$, we may consider a new pair of linear codes, C_1' and C_2', by enlarging C_1 or C_2, in such a way that either $C_2' \subseteq (C_1')^\perp$ or $C_1' \subseteq C_2^\perp$ do not hold any more, but this new pair gives an asymmetric EAQECC with better parameters. Hence, taking into account that $c = \dim C_1' - \dim\left(C_1' \cap (C_2')^\perp\right) = \dim C_2' - \dim\left(C_2' \cap (C_1')^\perp\right)$, the information rate is kept, one of the minimum distances is the same and the other one increases.

Let us illustrate the above technique with a small example. Keep the notation as in Section IV and assume that $\ell = r$, that is we do not consider subfield-subcodes in this example. Let C_i be the code E_{Δ_i}, for $1 \leq i \leq 2$, where $\Delta_1 = \{2\}$ and $\Delta_2 = \{0, n-1\}$. Set $C_1' = E_{\Delta_1'}$ with $\Delta_1' = \{1, 2\}$. Then $C_2 \subseteq C_1^\perp = E_{\Delta_1^\perp}$, with $\Delta_1^\perp = \{0, 1, \ldots, n-3, n-1\}$. Now setting $C_2' = C_2$, we deduce that the value d_x for the standard case (C_1, C_2) and the entanglement-assisted case (C_1', C_2') is the same. However, in the standard case,

$$d_z = \mathrm{wt}(C_1^\perp \setminus (C_2 \cap C_1^\perp)) = 2,$$

because the cardinality of Δ_1 is one. But

$$(C_1')^\perp \setminus \left(C_2' \cap (C_1')^\perp\right) \subseteq \left(C_1'\right)^\perp$$

and then, when one considers entanglement,

$$d_z = \mathrm{wt}\left((C_1')^\perp \setminus \left(C_2' \cap (C_1')^\perp\right)\right) \geq 3$$

by the BCH bound. As a consequence, to share entanglement allows us to increase the value d_z and therefore the asymmetry ratio.

VI. EXAMPLES OF EAQECCS

Table 1 shows the different values involved in the construction of asymmetric EAQECCs, over several finite fields, constructed as in Theorem 9. The last two columns display the representatives of the cyclotomic cosets used to define the codes C_1 and C_2. Notice that the parameters of our asymmetric EAQECCs follow immediately from Theorem 3 and are $[[n, n-k_1, d_z/d_x; c]]_q$. All these codes exceed the asymmetric Gilbert-Varshamov bound proved in Theorem 5. In addition, for fixed values (q, n, k_1, k_2, c), we consider the set P of pairs (d_1, d_2) of Z-minimum and X-minimum distances of asymmetric EAQECCs such that (d_1, d_2) does not exceed the bound in Theorem 5 but either (d_1+1, d_2) or (d_1, d_2+1) beat it; we have noticed that frequently the cardinality of P is one. Let $(\mathfrak{d}_z, \mathfrak{d}_x)$ be the maximum of P with respect to the lexicographical order where $(1,0) > (0,1)$. Table 1 displays the threshold $(\mathfrak{d}_z, \mathfrak{d}_x)$ as well. Note that many times our codes exceed both values $\mathfrak{d}_z$ and $\mathfrak{d}_x$ by one or two units.

We would like to add that our construction from BCH codes (regarded as in Section IV), using Theorem 3, may produce good symmetric EAQECCs as well. We use the fact that an asymmetric EAQECC provides a symmetric EAQECC with the same parameters but its minimum distance, which is the minimum of the two minimum distances d_x and d_z. In all our examples, both minimum distances are equal. Thus,

TABLE 2. Symmetric EAQECC coming from Theorem 9.

q	n	k_1	k_2	c	$d_z = d(C_1^{\perp})$	$d_x = d(C_2^{\perp})$	$\mathfrak{d}$	Cyclotomic Cosets Defining C_1	Cyclotomic Cosets Defining C_2
2	15	11	11	11	8	8	6	$\{0,1,3,5\}$	$\{0,1,3,5,7\}$
2	15	10	10	10	7	7	6	$\{1,3,5\}$	$\{3,5,7\}$
2	15	9	9	9	6	6	5	$\{0,1,3\}$	$\{0,3,7\}$
2	15	7	5	1	4	4	3	$\{0,1,5\}$	$\{0,1\}$
2	15	10	10	6	7	7	6	$\{1,3,5\}$	$\{1,3,5\}$
2	15	14	14	14	15	15	11	$\{1,3,5,7\}$	$\{1,3,5,7\}$
2	15	13	13	13	10	10	9	$\{0,1,3,7\}$	$\{0,1,3,7\}$
2	31	6	6	6	4	4	2	$\{0,1\}$	$\{0,15\}$
2	31	11	11	1	6	6	5	$\{0,1,3\}$	$\{0,1,3\}$
2	31	5	5	5	3	3	2	$\{1\}$	$\{15\}$
2	31	21	21	16	12	12	11	$\{0,1,5,7,15\}$	$\{0,3,7,11,15\}$
2	31	20	20	15	11	11	10	$\{1,5,7,15\}$	$\{3,7,11,15\}$
2	31	10	10	10	5	5	4	$\{1,3\}$	$\{7,15\}$
2	63	7	7	7	4	4	2	$\{0,1\}$	$\{0,31\}$
2	63	13	13	13	6	6	5	$\{0,1,3\}$	$\{0,15,31\}$
2	63	9	7	7	4	4	3	$\{0,1,21\}$	$\{0,31\}$
2	63	10	7	7	4	4	3	$\{0,1,9\}$	$\{0,31\}$
2	63	15	13	13	6	6	5	$\{0,1,3,21\}$	$\{0,15,31\}$
2	63	19	19	19	8	8	7	$\{0,1,3,5\}$	$\{0,15,23,31\}$
3	26	7	7	1	5	5	4	$\{0,1,2\}$	$\{0,7,14\}$
3	26	18	18	18	13	13	12	$\{1,2,4,5,7,8\}$	$\{2,5,7,8,14,17\}$
4	15	4	4	1	4	4	3	$\{0,1,5\}$	$\{0,1,5\}$
4	15	8	8	3	7	7	6	$\{0,1,2,3,5\}$	$\{0,1,2,3,5\}$
4	15	11	11	9	10	10	9	$\{1,2,3,5,6,7\}$	$\{1,2,3,6,10,11\}$
4	17	4	4	4	4	4	3	$\{6\}$	$\{6\}$
4	17	8	8	4	7	7	5	$\{1,3\}$	$\{1,6\}$
4	17	13	13	13	12	12	10	$\{0,1,2,3\}$	$\{0,1,2,3\}$
4	17	16	16	16	17	17	14	$\{1,2,3,6\}$	$\{1,2,3,6\}$
4	17	9	8	8	7	7	6	$\{0,1,3\}$	$\{1,3\}$
5	24	4	4	4	4	4	3	$\{0,1,6\}$	$\{0,18,19\}$
5	24	4	4	1	4	4	3	$\{0,1,6\}$	$\{12,13,18\}$
5	24	10	10	4	8	8	7	$\{0,1,2,3,4,6\}$	$\{2,6,8,9,12,19\}$
5	24	5	4	4	4	4	3	$\{0,1,6,12\}$	$\{0,18,19\}$
5	24	20	20	20	18	18	16	$\{0,1,2,3,4,7,8,9,13,14,18\}$	$\{0,2,3,4,6,7,8,9,13,14,19\}$

Table 2 displays values of codes coming from our construction, giving rise to symmetric EAQECCs whose parameters are $[[n, k = n - k_1 - k_2 + c, d = d_z = d_x; c]]_q$. We have used the Hartmann-Tzeng bound [38] in our computations. All codes in this table exceed the Gilbert-Varshamov bound for symmetric EAQECCs [21]. Table 2 also contains, for each code C, the minimum distance $\mathfrak{d}$ of a symmetric EAQECC with the same parameters (q, n, k, c) as C and such that $\mathfrak{d}$ does not beat the above mentioned symmetric Gilbert-Varshamov bound but $\mathfrak{d} + 1$ does. In several cases, our codes exceed the value $\mathfrak{d}$ by more than one unit.

We conclude this section by showing another sign of the goodness of our codes and from the advantages of considering entanglement. Table 1 provides two asymmetric EAQECCs with parameters $[[24, 19, 4/3; c = 3]]_5$, and $[[15, 12, 3/2; c = 1]]_4$, which (using entanglement) have better parameters that the optimal (non entanglement-assisted) asymmetric QECCs $[[24, 17, 4/3]]_5$ and $[[15, 11, 3/2]]_4$ given in [15]. Finally, Table 2 shows two binary symmetric EAQECCs with parameters $[[15, 4, 8; c = 8]]_2$ and $[[31, 25, 4; c = 6]]_2$ with better parameters than the best (non entanglement-assisted) QECCs $[[15, 4, 4]]_2$ and $[[31, 25, 2]]_2$ given in [23].

VII. CONCLUSION

In this article we show how to construct asymmetric EAQECCs. That is, entanglement-assisted quantum error-correcting codes designed for the case when phase-shift errors happen more likely than qudit-flip errors, as it is with the combined amplitude damping and dephasing channel. Moreover, they can be constructed from any pair of classical linear codes since the encoder and decoder may share entanglement. Following our framework, a concrete construction using BCH codes is proposed and we expect further families of asymmetric EAQECCs to be proposed. In particular, we will extend the BCH construction by considering evaluation of polynomials in several variables which will hopefully give better results and a larger constellation of codes. The Gilbert-Varshamov-type bound provided in this article will allow researchers to check the goodness of the parameters of codes of this type.

ACKNOWLEDGEMENT

We would like to thank the reviewers for their insightful comments.

REFERENCES

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

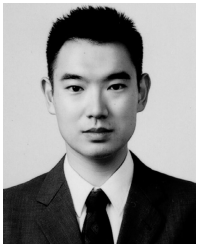
[2] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, "Quantum error detection. I. Statement of the problem," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 778–788, May 2000.

[3] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn, "Quantum error detection. II. Bounds," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 789–800, May 2000.

[4] A. Ashikhmin and S. Litsyu, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206–1215, May 1999.
[5] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.
[6] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Combinat. Des.*, vol. 8, no. 3, pp. 174–188, 2000.
[7] T. Brun, I. Devetak, and M. H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, Oct. 2006.
[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, no. 3, pp. 405–408, Jul. 2002.
[9] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[10] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Jul. 2002.
[11] I. Cascudo, "On squares of cyclic codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 1034–1047, Feb. 2019.
[12] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.
[13] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett.*, vol. 77, no. 12, p. 2585, 1996.
[14] M. F. Ezerman, S. Jitman, H. M. Kiah, and S. Ling, "Pure asymmetric quantum MDS codes from CSS construction: A complete characterization," *Int. J. Quantum Inform.*, vol. 11, no. 3, Apr. 2013, Art. no. 1350027.
[15] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, "CSS-like constructions of asymmetric quantum codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6732–6754, Oct. 2013.
[16] M. F. Ezerman, S. Ling, and P. Sole, "Additive asymmetric quantum codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5536–5550, Aug. 2011.
[17] K. Feng and Z. Ma, "A Finite Gilbert–Varshamov bound for pure stabilizer quantum codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3323–3325, Dec. 2004.
[18] C. Galindo, O. Geil, F. Hernando, and D. Ruano, "On the distance of stabilizer quantum codes from J-affine variety codes," *Quantum Inf. Process.*, vol. 16, no. 4, p. 111, 2017.
[19] C. Galindo, O. Geil, F. Hernando, and D. Ruano, "Improved constructions of nested code pairs," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2444–2459, Sep. 2018.
[20] C. Galindo and F. Hernando, "Quantum codes from affine variety codes and their subfield-subcodes," *Des., Codes Cryptogr.*, vol. 76, no. 1, pp. 89–100, Jul. 2015.
[21] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," *Quantum Inf. Process.* vol. 18, no. 4, p. 116, 2019.
[22] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 3, pp. 1862–1868, Sep. 1996.
[23] M. Grassl. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Dec. 22, 2019. [Online]. Available: http://www.codetables.de
[24] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 02, no. 01, pp. 55–64, Mar. 2004.
[25] M. Grassl and M. Rötteler, "Quantum BCH codes," in *Proc. 10th Int. Symp. Theor. Elect. Eng. Germany*, 1999, pp. 207–212.
[26] M.-H. Hsieh, I. Devetak, and T. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 6, 2007, Art. no. 062313.
[27] L. Ioffe and M. Mézart, "Asymmetric quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 3, 2007, Art. no. 032345.
[28] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892–4924, Oct. 2006.
[29] G. G. La Guardia, "Constructions of new families of nonbinary quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 80, no. 4, 2009, Art. no. 042331.
[30] G. G. La Guardia, "Asymmetric quantum product codes," *Int. J. Quantum Inf.*, vol. 10, no. 1, Feb. 2012, Art. no. 1250005.
[31] G. G. La Guardia, "Asymmetric quantum Reed–Solomon and generalized Reed–Solomon codes," *Quantum Inf. Process.*, vol. 11, no. 2, pp. 591–604, Apr. 2012.
[32] G. G. La Guardia, "Asymmetric quantum codes: New codes from old," *Quantum Inf Process*, vol. 12, no. 8, pp. 2771–2790, Aug. 2013.
[33] G. G. La Guardia, "On the construction of asymmetric quantum codes," *Int. J. Theor. Phys.*, vol. 53, no. 7, pp. 2312–2322, 2014.
[34] L. Luo, Z. Ma, Z. Wei, and R. Leng, "Non-binary entanglement-assisted quantum stabilizer codes," *Sci. China Inf. Sci.*, vol. 60, no. 4, p. 42501, 2017.
[35] R. Matsumoto, "Two Gilbert–Varshamov type existential bounds for asymmetric quantum error correcting bounds," *Quantum Inf. Process.*, vol. 16, no. 12, p. 285, 2017.
[36] R. Matsumoto and T. Uyematsu, "Constructing quantum error correcting codes for p^m state systems from classical error correcting codes," *IEICE Trans. Fundam.*, vol. E83-A, no. 10, pp. 1878–1883, 2000.
[37] R. Matsumoto and T. Uyematsu, "Lower bound for the quantum capacity of a discrete memoryless quantum channel," *J. Math. Phys.*, vol. 43, no. 9, pp. 4391–4403, 2002.
[38] R. Pellikaan, "The shift bound for cyclic, Reed–Müller and geometric Goppa codes," in *Arithmetic, Geometry, and Coding Theory*. Berlin, Germany: Walter de Gruyter, 1996.
[39] E. Rains, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.
[40] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: Constructions, bounds and performance," *Proc. R. Soc. London A, Math. Phys. Eng. Sci.*, vol. 465, no. 2105, pp. 1645–1672, May 2009.
[41] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
[42] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, no. 4, pp. R2493–R2496, Jul. 2002.
[43] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. Lett.*, vol. 77, no. 6, pp. 793–797, 1996.
[44] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 6, 2008, Art. no. 064302.
[45] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

CARLOS GALINDO was born in Valladolid, Spain, in October 1962. He received the M.S. and Ph.D. degrees in mathematics from the University of Valladolid, Spain, in 1985 and 1991, respectively. He is currently a Professor with University Jaume I, Spain. His research interests include quantum and classical coding theory, algebraic geometry, ordinary differential equations, and their interactions.

FERNANDO HERNANDO was born in Burgos, Spain, in October 1976. He received the M.S. degrees in mathematics from the University of Valladolid, Spain, and the University of Kaiserslautern, Germany, in 2001 and 2002, respectively, and the Ph.D. degree in mathematics from the University of Valladolid, in 2007. He was a Postdoctoral Researcher with the University of Cork, in 2007, and was a Postdoctoral Fellow with San Diego State University, in 2010. He was an Assistant Professor, from 2011 to 2016 and has been an Associate Professor, since 2016 with the Department of Mathematical, Universitat Jaume I, Spain. His research interests include quantum and classical coding theory, computer algebra, and singularity theory.



RYUTAROH MATSUMOTO (Member, IEEE) was born in Nagoya, Japan, in November 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering from the Tokyo Institute of Technology, Japan, in 1996, 1998 and 2001, respectively. He was an Assistant Professor from 2001 to 2004, and had been an Associate Professor from 2004 to 2017 with the Department of Information and Communications Engineering, Tokyo Institute of Technology, Japan. Since 2017, he has been an Associate Professor with the Department of Information and Communication Engineering, Nagoya University, Japan. He also served as a Velux Visiting Professor with the Department of Mathematical Sciences, Aalborg University, Denmark, in 2011 and 2014. His research interests include error-correcting codes, quantum information theory, information theoretic security, and communication theory. He received the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan, in 2001. He received the Best Paper Awards from IEICE, in 2001, 2008, 2011, and 2014.

DIEGO RUANO was born in Valladolid, Spain, in 1980. He received the M.S. degrees in mathematics from the University of Valladolid, Spain, and the University of Kaiserslautern, Germany, in 2002 and 2003, respectively, and the Ph.D. degree in mathematics from the University of Valladolid, in 2007. He was a Postdoctoral Researcher with the University of Kaiserslautern, in 2007, and a H.C. Ørsted Postdoctoral Fellow with the Technical University of Denmark, in 2008. He was an Assistant Professor from 2009 to 2012, and an Associate Professor from 2013 to 2018 with Aalborg University, Denmark. He is currently a Ramón-y-Cajal Fellow with the IMUVA-Mathematics Research Institute, University of Valladolid, Spain. His research interests include classical and quantum coding theory, secret sharing, network codes, computer algebra, and algebraic geometry.