



**HAL**  
open science

# NEW CONSTRUCTIONS OF ENTANGLEMENT-ASSISTED QUANTUM CODES

A Allahmadi, A Alkenani, R Hijazi, N Muthana, F Özbudak, P Solé

► **To cite this version:**

A Allahmadi, A Alkenani, R Hijazi, N Muthana, F Özbudak, et al.. NEW CONSTRUCTIONS OF ENTANGLEMENT-ASSISTED QUANTUM CODES. Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences , In press, 10.1007/s12095-021-00499-7 . hal-03339152

**HAL Id: hal-03339152**

**<https://hal.science/hal-03339152>**

Submitted on 9 Sep 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# NEW CONSTRUCTIONS OF ENTANGLEMENT-ASSISTED QUANTUM CODES

A. ALLAHMADI, A. ALKENANI, R. HIJAZI, N. MUTHANA, F. ÖZBUDAK, P. SOLÉ

ABSTRACT. We present two new constructions of entanglement-assisted quantum error-correcting codes using some fundamental properties of (classical) linear codes in an effective way. The main ideas include linear complementary dual codes and related concatenation constructions. Numerical examples in modest lengths show that our constructions perform better than known constructions in the literature. We also give a proof on a generalization of binary Singleton type bound on entanglement-assisted quantum error-correcting codes to arbitrary  $q$ -ary entanglement-assisted quantum error-correcting codes.

*Keywords:* Entanglement-assisted quantum error correcting codes, Hull of a code, concatenation, isometry codes

AMS MSC(2010): 81P45, 81P70, 94B05

## 1. INTRODUCTION

Quantum error-correcting codes play an important role both in quantum communication and quantum computations. The construction of *quantum error-correcting codes* (or *quantum codes* in short) has been an active research field since the pioneering works in [1], [5], [33], [34]. One of the important developments in the area of quantum error-correction was the introduction of entanglement-assisted quantum error-correction [18]. The entanglement-assisted quantum codes have the advantages of both entanglement-assisted and operator quantum correction. In their theory it is assumed that in addition to the quantum channel, the sender and the receiver share a certain amount of pre-existing entangled qubits. We refer to [18] and [8] for further details.

Recently there has been many results in the literature in constructing new entanglement-assisted quantum error-correcting codes using some properties of (classical) linear codes

---

AA,AA,RH, NM, are with Mathematics Department, King Abdulaziz University, Jeddah, Saudi Arabia; e-mails: adelnife2@yahoo.com, aalke-nani10@hotmail.com,rhijazi@kau.edu.sa,najat\_muthana@hotmail.com.

Ferruh Özbudak is with Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey; e-mail: ozbudak@metu.edu.tr.

Patrick Solé is with I2M, Aix Marseille Univ., Centrale Marseille, CNRS, Marseille, France , e-mail: sole@enst.fr.

[12], [13], [22], [23], [24], [29], [30]. One of the common tools they use is the hull of a linear code. They also use some properties of generator matrices of certain codes and/or some properties of algebraic curves in algebraic geometry codes.

In this paper we present two constructions: Constructions 1 and 2. Construction 1 is very powerful and it works for any field  $\mathbb{F}_q$  with  $q \geq 4$ . Construction 2 uses the idea of isometry codes, which is related to concatenated construction of linear codes and it works for any field  $\mathbb{F}_q$  including  $q \in \{2, 3\}$ . Our constructions are quite simple and clear. Nevertheless we use some fundamental ideas in code constructions (like hull of a code) in a very effective way so that we obtain significant improvements in the parameters of entanglement-assisted quantum error-correcting codes. In particular our constructions use [6] and [7] in an effective way. We also generalize a Singleton type bound from binary entanglement-assisted quantum codes to arbitrary  $q$ -ary entanglement-assisted quantum codes in Appendix A (see also the paragraph before Notation 3.7 below).

The rest of this paper is organized as follows. The next section collects some basic notions and notations. We present Construction 1 in Section 3. Construction 1 uses an algorithm in one of its steps and we explain this algorithm explicitly in Appendix B. We give Construction 2 in Section 4. We also present some important material in Appendix A.

## 2. BACKGROUND MATERIAL

Now we introduce some fundamental notions that we use. Let  $q$  be a prime power and  $\mathbb{F}_q$  denote the finite field with  $q$  elements. For integers  $1 \leq k \leq n$ , let  $G$  be a  $k \times n$  matrix of rank  $k$ . Let  $C$  be the linear code over  $\mathbb{F}_q$  having  $G$  as a generator matrix. We consider the  $\mathbb{F}_q$ -linear space  $\mathbb{F}_q^n$  as an inner product space as well under the Euclidean inner product (or the ordinary inner product) defined as

$$(1) \quad (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) := a_1 b_1 + \dots + a_n b_n$$

(see, [19, page 8]). Using the inner product in (1), let

$$C^\perp := \{(a_1, \dots, a_n) \in \mathbb{F}_q^n : (a_1, \dots, a_n) \cdot (c_1, \dots, c_n) = 0 \text{ for all } (c_1, \dots, c_n) \in C\}$$

be the dual linear code of  $C$ . The Hull of  $C$  is defined as

$$\text{Hull}(C) = C \cap C^\perp.$$

Recall that  $C$  is a linear code of length  $n$ , dimension  $k$  and  $G$  is a generator matrix of  $C$ . One of the fundamental properties we have is

$$(2) \quad \text{rank}(GG^T) + \dim_{\mathbb{F}_q} \text{Hull}(C) = k.$$

If  $C$  is an  $[[n, k, d]]_q$  quantum code with  $c$  entangled qubits, we will write its parameters as an entanglement-assisted quantum error-correcting code as  $[[n, k, d; c]]_q$ .

### 3. A GENERIC CONSTRUCTION FOR $q \geq 4$

In this section we present a construction of entanglement-assisted quantum codes over  $\mathbb{F}_q$  for  $q \geq 4$ . It gives a generic and simple algorithm to construct an  $[[n, k, d; n-k]]_q$  entanglement-assisted quantum code using a generator matrix of a (classical)  $[n, k, d]_q$  code.

We illustrate this algorithm with explicit examples. We study the performance of our construction in terms of the entanglement-assisted quantum Singleton bound (see Notation 3.7 below) of the parameters.

Our construction in this section improves many recent constructions significantly.

We are ready to present our construction in this section.

**Construction 1:** This construction has the following steps:

- 1.1) Let  $q \geq 4$  be a prime power. Let  $G$  be a  $k \times n$  matrix over  $\mathbb{F}_q$ , whose row space is an  $[n, k, d]_q$  code.
- 1.2) Using the algorithm in [6, Section 5A] modify  $G$  to a  $k \times n$  matrix  $G_1$  over  $\mathbb{F}_q$  such that the row space of  $G_1$  is the code  $C_1 \subseteq \mathbb{F}_q^n$  having the properties:  $\text{Hull}(C_1) = \{0\}$  and  $C_1$  is an  $[n, k, d]_q$  code. We refer to Appendix B for an explicit presentation of this step of the algorithm.
- 1.3) Using  $C_1$  and  $C_1^\perp$  (actually only  $C_1^\perp$ ) obtain an  $[[n, k, d; n-k]]_q$  entanglement-assisted quantum code following [9, Theorem 4]. We refer to the proof of Theorem 3.2 below for details.

We will prove that this construction is correct. First we state a useful result due to [37] in its first form. We prefer to state it for arbitrary finite fields and using generator matrices as in [9] (see also [12], [13], [29] and [30]).

**Theorem 3.1.** *Let  $q$  be an arbitrary prime power. Let  $G_1$  and  $G_2$  be generator matrices of  $[n, k_1, d_1]_q$  and  $[n, k_2, d_2]_q$  codes  $C_1$  and  $C_2$  over  $\mathbb{F}_q$ . Put*

$$c = \text{rank}(G_1 G_2^T).$$

*Then we have*

$$(3) \quad c = \dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q} (C_1 \cap C_2^\perp)$$

*and there exists an effective construction of  $[[n, n - k_1 - k_2 + c, d; c]]_q$  entanglement-assisted code  $C$  over  $\mathbb{F}_q$ , where*

$$(4) \quad d = \min \{d_H(C_1^\perp \setminus (C_2 \cap C_1^\perp)), d_H(C_2^\perp \setminus (C_1 \cap C_2^\perp))\}.$$

*Here  $d_H(\cdot)$  is the minimum Hamming distance of the corresponding set.*

Now we are ready to prove that Construction 1 is correct.

**Theorem 3.2.** *Let  $q \geq 4$  be a prime power. If  $G$  is a generator matrix of a  $[n, k, d]_q$  classical code, then Construction 1 gives an  $[[n, k, d; n - k]]_q$  entanglement-assisted quantum code.*

*Proof.* Let  $V$  be the  $\mathbb{F}_q$ -linear code having  $G$  as the generator matrix. Using Step 1.2 in Construction 1 and the algorithm in Appendix B we obtain a  $k \times n$  matrix  $G_1$  over  $\mathbb{F}_q$  such that the  $\mathbb{F}_q$ -linear code  $V_1$  having  $G_1$  as a generator matrix has the following properties:  $V_1$  is an  $[n, k, d]_q$  code and  $\text{Hull}(V_1) = \{0\}$ .

Let  $C_1$  and  $C_2$  be the  $\mathbb{F}_q$ -linear codes of length  $n$  defined as

$$C_1 = C_2 = V_1^\perp.$$

Note that

$$(5) \quad C_1 \cap C_2^\perp = V_1^\perp \cap V_1 = \{0\} \text{ as } \text{Hull}(V_1) = \{0\}.$$

Similarly we have  $C_2 \cap C_1^\perp = V_1^\perp \cap V_1 = \{0\}$  and hence

$$(6) \quad \begin{aligned} d_H(C_1^\perp \setminus (C_2 \cap C_1^\perp)) &= d_H(V_1 \setminus \{0\}) = d \text{ and} \\ d_H(C_2^\perp \setminus (C_1 \cap C_2^\perp)) &= d_H(V_1 \setminus \{0\}) = d. \end{aligned}$$

Applying Theorem 3.1 using  $C_1$  and  $C_2$  we obtain an

$$[[n, k(C), d(C); c]]_q$$

entanglement-assisted quantum code  $C$ . Here using Theorem 3.1, (3) and (5) we get

$$(7) \quad c = \dim_{\mathbb{F}_q} V_1^\perp = n - k.$$

Using Theorem 3.1 and (7) we get

$$(8) \quad k(C) = n - k_1 - k_2 - c = n - (n - k) - (n - k) + (n - k) = k.$$

Using Theorem 3.1, (4) and (6) we get

$$(9) \quad d(C) = \min\{d, d\} = d.$$

Combining (7), (8) and (9) we complete the proof.  $\square$

The following example makes a connection to Appendix B and hence it also illustrates Step 1.2 of Construction 1.

**Example 3.1.** *Using Construction 1 and Examples B.1, B.2 and B.3 we immediately obtain  $[[23, 7, 12; 16]]_4$ ,  $[[19, 9, 8; 10]]_4$  and  $[[20, 7, 10; 13]]_4$  codes.*

Using Construction 1 and the codes in [15] or [28], we immediately obtain new entanglement-assisted quantum codes:

**Remark 3.3.** We first compare our results with the very recent paper [22]. Construction 1 improves many of the results in [22] significantly. For example in [22] they state that a code with parameters  $[[34, 10, 9; 24]]_4$  is a new entanglement-assisted quantum code in [22, Table 2]. Using Construction 1 and the corresponding code from [15] we immediately obtain a code with parameters  $[[34, 10, 16; 24]]_4$ . The improvement in the minimum distance from 9 to 16 is significant.

As another example in [22] they state that a code  $C$  with parameters  $[[26, 14, 5; 12]]_4$  is a new entanglement-assisted code in [22, Table 5]. Using Construction 1 and [15] we immediately obtain a code  $C$  with parameters  $[[26, 14, 9; 12]]_4$ . The improvement in the minimum distance from 5 to 9 is significant.

We also have improvements compared to the very recent paper [23]. For example in [23] they state that a code with parameters  $[[22, 16, 3; 6]]_9$  is a new entanglement-assisted code in [23, Table 1]. Using Construction 1 and the corresponding code from [15] we immediately obtain a code with parameters  $[[22, 16, 5; 6]]_4$ . The improvement in the minimum distance is from 3 to 5.

Next we study the performance of Construction 1 in terms of the entanglement-assisted quantum Singleton bound. Here we need to introduce some notation.

**Notation 3.4.** Let  $q$  be a prime power. For integers  $1 \leq k \leq n$ , let  $D_q(n, k)$  denote the largest integer  $d$  such that there exists a classical  $[n, k, d]_q$  code. We call  $C$  is *optimal* if  $C$  is a classical  $[n, k, D_q(n, k)]_q$  code. We call  $C$  is *best known* if  $C$  is a classical  $[n, k, D]_q$  code and there is no known code in the literature having parameters  $[n, k, D']_q$  with  $D' > D$ . There is a database and a related command BDLC in Magma.

**Notation 3.5.** Let  $q$  be a prime power. For integers  $1 \leq d \leq n$ , let  $K_q(n, d)$  denote the largest integer  $k$  such that there exists a classical  $[n, k, d]_q$  code. We call  $C$  is *optimal* if  $C$  is a classical  $[n, K_q(n, d), d]_q$  code. We call  $C$  is *best known* if  $C$  is a classical  $[n, K, d]_q$  code and there is no known code in the literature having parameters  $[n, K', d]_q$  with  $K' > K$ . There is a database and a related command BKLC in Magma.

The notions of optimal codes in Notations 3.4, 3.5 are related but different.

**Notation 3.6.** Let  $q$  be a prime power. Let  $C$  be a classical  $[n, k, d]_q$  code. Then the *Singleton defect*  $S(C)$  of  $C$  is the nonnegative integer defined as

$$S(C) = n + 1 - k - d.$$

This is nonnegative due to the Singleton bound (see, for example, [19]). If  $S(C) = 0$ , then  $C$  is called a *maximally distance separable (MDS)* code.

The analog of the Singleton bound for the entanglement-assisted quantum codes is rather intricate. In [4, page 24], the authors stated that if there exists an  $[[n, k, d; c]]_q$

entanglement-assisted quantum code, then

$$(10) \quad 2d \leq n - k + 2 + c.$$

However this bound is invalid for a range. For example in [14], the author constructed an  $[[9, 1, 6; 1]]_2$  entanglement-assisted quantum code, which is a counterexample to the bound in (10). A correct analog of the Singleton bound for the binary entanglement-assisted quantum codes is given in [21] as follows: If there exists an  $[[n, k, d; c]]_2$  entanglement-assisted quantum code, then

$$(11) \quad d \leq \frac{n+2}{2} \Rightarrow 2d \leq n - k + 2 + c.$$

We could not find a proof of the bound in (11) for  $q > 2$  in the literature. Recently in [16], among other results, the authors provide entropic proofs of Singleton bounds for a range of codes.<sup>1</sup> In Appendix A, in Theorem A.5, we generalize the bound in (11) to arbitrary  $q$ -ary entanglement-assisted quantum codes (see also Remarks A.6, A.7 in Appendix A). We call the bound in (11) as the *entanglement-assisted quantum Singleton bound*, which is defined only if  $d \leq \frac{n+2}{2}$ . We note that, unfortunately, there are some incorrect formulations of the entanglement-assisted quantum Singleton bound even in the very recent literature (see, for example, [12, Proposition 2.3], [13, Proposition 4.3], [22, Theorem 2.3], [23, Theorem 2.6], [24, Lemma 12], [29, in the last paragraph in Section 2] and [30, Equation (7) in page 8]).

**Notation 3.7.** Let  $q$  be a prime power. Let  $C$  be an  $[[n, k, d; c]]_q$  entanglement-assisted quantum code. Then the *entanglement-assisted quantum Singleton defect*  $S_q(C)$  of  $C$  is the integer defined as

$$S_q(C) = n + 2 + c - k - 2d.$$

If  $d \leq \frac{n+2}{2}$ , then  $S_q(C)$  is nonnegative due to the entanglement-assisted quantum Singleton bound in (11). If  $d \leq \frac{n+2}{2}$  and  $S_q(C) = 0$ , then we call that  $C$  is a *maximally distance separable (MDS) entanglement-assisted quantum code*.

We presents our results on the performance of Construction 1.

**Corollary 3.1.** *Let  $q \geq 4$  be a prime power. Let  $1 \leq k \leq n$  be integers. For any optimal  $[n, k, D_q(n, k)]_q$  classical code  $C$  with Singleton defect  $S(C)$ , there exists an  $[[n, k, D_q(n, k); n - k]]_q$  entanglement-assisted quantum code  $\hat{C}$  with entanglement-assisted quantum Singleton defect*

$$S_q(\hat{C}) = 2S(C).$$

*In particular if  $C$  is MDS and  $k \geq \frac{n}{2}$ , then  $\hat{C}$  is entanglement-assisted quantum MDS. Also if  $S(C) = 1$  (called near MDS), then  $S_q(\hat{C}) = 2$ .*

---

<sup>1</sup>We note that we were not aware of the results in [16] when we submitted the original and the first revised versions of this paper, which were written before the first version of [16] were made available.

*Proof.* Using Theorem 3.2 we construct  $\hat{C}$  having the parameters  $[[n, k, D_q(n, k); n - k]]_q$ . By definition of  $S_q(\hat{C})$  we get

$$S_q(\hat{C}) = n + 2 + (n - k) - (k - 2D_q(n, k)) = 2(n + 1 - k - D_q(n, k)) = 2S(C).$$

Note that if  $C$  is MDS and  $k \geq \frac{n}{2}$ , then  $D_q(n, k) = n + 1 - k \leq \frac{n+2}{2}$  and  $S_q(\hat{C}) = 0$ . This implies that  $\hat{C}$  is entanglement-assisted quantum MDS by definition.  $\square$

The following is an analogue of Corollary 3.1

**Corollary 3.2.** *Let  $q \geq 4$  be a prime power. Let  $1 \leq d \leq n$  be integers. For any optimal  $[n, K_q(n, d), d]_q$  classical code  $C$  with Singleton defect  $S(C)$ , there exists an  $[[n, K_q(n, d), d; n - K_q(n, d)]]_q$  entanglement-assisted quantum code  $\hat{C}$  with entanglement-assisted quantum Singleton defect*

$$S_q(\hat{C}) = 2S(C).$$

The following results improves Theorems 17 and 18 of [24] significantly. Namely we do not have extra conditions on  $q, n$  and/or  $k$  as in [24, Theorems 17 and 18].

**Theorem 3.8.** *Let  $q \geq 4$  be a prime power. If  $1 \leq k \leq n \leq q+1$ , then using generalized Reed Solomon codes and Construction 1 we immediately obtain  $[[n, k, n + 1 - k; n - k]]_q$  entanglement-assisted quantum code.*

*Proof.* Using generalized Reed Solomon codes we easily construct a  $k \times n$  generator matrix  $G$  over  $\mathbb{F}_q$  such that the linear code  $C$  having  $G$  as a generator matrix is an  $[n, k, n + 1 - k]_q$  code (see, for example [35, Propositions 2.3.2 and 2.3.3]). Then we obtain a  $[[n, k, d; n - k]]_q$  entanglement-assisted quantum code using Construction 1.  $\square$

**Remark 3.9.** Construction 1 also extends some of the results in [29] and [30]. First we need to recall some notation and facts related to algebraic functions fields and algebraic geometry codes, for which we refer, for example, to [35]. For  $q \geq 4$ , and  $g \geq 0$ , let  $N_q(g)$  denote the largest integer  $N$  such that there exists an absolutely irreducible curve  $\chi$  (or equivalently an algebraic function field) over  $\mathbb{F}_q$  of genus  $g$  having  $N$  rational points. Using algebraic geometry codes [11] (see also [35]) if  $n \leq N_q(g)$  and  $1 \leq k \leq n$ , then there exists  $[n, k, d]_q$  code over  $\mathbb{F}_q$  with  $k + d \geq n + 1 - g$ .

It is well known that, due to Hasse-Weil bound we have  $N_q(g) \leq q + 1 + 2gq^{1/2}$  [35]. A curve is called a *maximal curve* if it attains the Hasse-Weil bound.

For any  $q$ , the projective line is a maximal curve of genus 0. If  $g \geq 1$ , then there exists a maximal curve over  $\mathbb{F}_q$  only if

- i)  $q$  is a square, hence put  $q = q_1^2$ , and
- (ii)  $g \leq \frac{q_1(q_1-1)}{2}$ .

Note that the Hermitian curve over  $\mathbb{F}_{q_1^2}$  has genus  $\frac{q_1(q_1-1)}{2}$ . We refer to [32] and [35] for the details of these facts.



In [29] and [30] the authors consider only maximal curves of genus 0 if  $q$  is arbitrary, and of genera 1 and  $\frac{q_1(q_1-1)}{2}$  if  $q = q_1^2$ . In their construction they need to control the duality and hence they need explicit and arithmetic conditions on a chosen algebraic curve. However in Construction 1, if  $q \geq 4$ , we do not need to control such arithmetical conditions because of Step 1.2 of the algorithm, which is explained in Appendix B in detail. Hence we can use any suitable algebraic curve over finite fields. There are algebraic curves with  $N_q(g)$  many rational points, which are not maximal. For example consider  $g \geq 1$  and  $q$  is a not a square, or consider  $g > \frac{q_1(q_1-1)}{2}$  if  $q = q_1^2$ . Moreover even if  $q = q_1^2$  and  $1 < g < \frac{q_1(q_1-1)}{2}$ , then there are many different values of  $g$  such that we have a maximal curve over  $\mathbb{F}_q$ , which is not birationally isomorphic to a projective line, elliptic curve or Hermitian curve. Using algebraic geometry codes together with such algebraic curves and Construction 1 we also extend the related results of [29] and [30]. Note that Construction 1 complies also with generalized algebraic geometry codes (see, for example, [26]).

As concrete examples, we have the following extensions. In [29], after [29, Theorem 4] they state to construct a  $[[39, 25, 14; 14]]_{32}$  entanglement-assisted quantum code. In fact [29, Theorem 4] allows to construct an  $[[n, k, n - k; n - k]]_{32}$  entanglement-assisted quantum code for all integers  $1 \leq k < n \leq 42$ , where the upper bound 42 is due to the arithmetical condition  $n + 2 \leq N_{32}(1) = 44$  in [29, Theorem 4]. Here  $N_{32}(1)$  is the largest integer  $N$  such that there exists an absolutely irreducible curve of genus 1 (elliptic curve) having  $N$  rational points (see [36]). Using Construction 1 we relax this condition. Indeed there exist an  $[[n, k, n - k]]_{32}$  code for all integers  $1 \leq k < n$  and  $2 \leq n \leq 44$ , in particular for  $n \in \{43, 44\}$  (see [28]). Hence using Construction 1 we obtain an  $[[n, k, n - k; n - k]]_{32}$  entanglement-assisted quantum code not only for  $1 \leq k < n \leq 42$  but also for  $1 \leq k < n \leq 44$ .

Similarly in [30, Table 2] they present a  $[[15, 10, 6; 5]]_{16}$  entanglement-assisted quantum code. In fact [30, Theorem 5] allows to construct an  $[[n, k, n - k + 1; n - k]]_{16}$  entanglement-assisted quantum code for all integers  $1 \leq k < n \leq 15$ , where the upper bound 15 is due to the arithmetical condition  $n \leq q - 1 = 16 - 1$  in [30, Theorem 5]. Using Corollary 1 and the existence of  $[[n, k, n - k + 1]]_{16}$  MDS codes with  $1 \leq k < n \leq 17$ , we obtain an  $[[n, k, n - k + 1; n - k]]_{16}$  entanglement-assisted quantum code not only for  $1 \leq k < n \leq 15$  but also for  $1 \leq k < n \leq 17$ . We further obtain an  $[[18, 15, 4; 3]]_{16}$  entanglement-assisted quantum code using Construction 1 and the MDS code  $[[18, 15, 4]]_{16}$ , which does not follow from [29] or [30].

In [22] they also use the notion of *net rate* of an  $[[n, k, d; c]]_q$  code as the ratio  $\frac{k-c}{n}$ . Let  $\text{nR}(C) = \frac{k-c}{n}$  denote the net rate of an  $[[n, k, d; c]]_q$  code  $C$ . In [30, Table 4] they present a  $[[26, 15, 6; 5]]_9$  entanglement-assisted quantum code  $C_1$ . Using Construction 1 and [28] we obtain an  $[[26, 19, 6; 7]]_9$  entanglement-assisted quantum code  $\hat{C}_1$ . The net rate of  $\hat{C}_1$  is much better than the net rate of  $C_1$ , which satisfy  $\text{nR}(\hat{C}_1) = \frac{12}{26} > \text{nR}(C_1) = \frac{10}{26}$ .

Note that the length and the minimum distance of  $C_1$  and  $\hat{C}_1$  are the same. Similarly in [30, Table 4] they present a  $[[64, 39, 11; 10]]_{16}$  entanglement-assisted quantum code  $C_2$ . Using Construction 1 and [28] we obtain an  $[[64, 48, 11; 16]]_{16}$  entanglement-assisted quantum code  $\hat{C}_2$ . The net rate of  $\hat{C}_2$  is much better than the net rate of  $C_2$ , which satisfy  $\text{nR}(\hat{C}_2) = \frac{32}{64} > \text{nR}(C_2) = \frac{29}{32}$ . Note that the length and the minimum distance of  $C_2$  and  $\hat{C}_2$  are the same.

**Remark 3.10.** In [12], the authors construct entanglement-assisted quantum codes over  $\mathbb{F}_q$  with parameters  $[[n, k, d; c]]$  only for  $n \leq q + 1$  and with some arithmetical restrictions. Using Construction 1, we cover all of these parameters and we extend their results considerably as we do not have such arithmetical conditions and  $n$  can be larger than  $q + 1$ . In [13], the authors construct further entanglement-assisted quantum codes over  $\mathbb{F}_q$  with parameters  $[[n, k, d; c]]$  only for  $n \leq q + 1$  and with less arithmetical restrictions. Using Construction 1 we also extend these results as we do not have any arithmetical condition and  $n$  can be larger than  $q + 1$ . In our results it is not necessary to use  $\ell$ -intersection pairs of codes as in [13] to get MDS entanglement-assisted quantum codes with the same parameters as in [13].

#### 4. A CONCATENATED TYPE CONSTRUCTION FOR ALL $q$

In this section we present a concatenated type construction of entanglement-assisted quantum codes over  $\mathbb{F}_q$  for all  $q$ . This construction is especially interesting when  $q = 2$  or  $q = 3$ . Nevertheless we prefer to present it for arbitrary  $q$ . This construction also improves several recent results significantly (see Remark 4.5 below).

An important ingredient of our construction in this section is isometry codes, which were introduced in [7]. We first recall its definition. Let  $q$  be an arbitrary prime power and  $k$  be an integer with  $k \geq 2$ . The trace of  $\alpha \in \mathbb{F}_{q^k}$  over  $\mathbb{F}_q$  is defined as

$$\text{tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{k-1} \alpha^{q^i} = \alpha + \alpha^q + \cdots + \alpha^{q^{k-1}}.$$

We also denote  $\text{tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha)$  by  $\text{tr}(\alpha)$  in short for simplicity. Let  $\{e_1, \dots, e_k\} \subseteq \mathbb{F}_{q^k}$ . Assume that  $(e_1, \dots, e_k)$  is an ordered basis of  $\mathbb{F}_{q^k}$  over  $\mathbb{F}_q$ . Recall that  $(e'_1, \dots, e'_k)$  is the dual basis if

$$\text{tr}(e_i e'_j) = \delta_{i,j} := \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

for  $1 \leq i, j \leq k$ . There exists a uniquely determined dual basis for any basis of  $\mathbb{F}_{q^k}$  over  $\mathbb{F}_q$ .

**Definition 4.1.** Let  $2 \leq k \leq n$  be integers. Under notation as above let  $(e_1, \dots, e_k)$  be an ordered basis of  $\mathbb{F}_{q^k}$ . An  $\mathbb{F}_q$ -linear map  $\pi : \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q^n$  is called an *isometry* if

$$\pi(e_i) \cdot \pi(e'_j) = \delta_{i,j}$$

for  $1 \leq i, j \leq k$ , where the inner product is the Euclidean inner product on  $\mathbb{F}_q^n$ . Here  $(e'_1, \dots, e'_k)$  is the dual basis of  $(e_1, \dots, e_k)$ . The image  $\pi(\mathbb{F}_{q^k})$  is called the *isometry code* corresponding to  $\pi$ .

We are ready to present our construction of this section.

**Construction 2:** This construction has the following steps:

- 2.1) Let  $q$  be any prime power. Let  $2 \leq k \leq n$  be integers such that there exists an isometry map  $\pi : \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q^n$ . Let the parameters of the isometry code  $\pi(\mathbb{F}_{q^k})$  be  $[n, k, d]$ . It is useful to choose  $\pi$  so that  $d$  is as large as possible.
- 2.2) Let  $G$  be a  $K \times N$  matrix over  $\mathbb{F}_{q^k}$ , whose row space is an  $[N, K, D]_{q^k}$  code.
- 2.3) Note that  $q^k \geq 4$  as  $k \geq 2$ . Using the algorithm in [6, Section 5A] modify  $G$  to a  $K \times N$  matrix  $G_1$  over  $\mathbb{F}_{q^k}$  such that the row space of  $G_1$  is the code  $C_1$  having the properties:  $\text{Hull}(C_1) = \{0\}$  and  $C_1$  is an  $[N, K, D]_{q^k}$  code.
- 2.4) Using  $C_1$ , the isometry map  $\pi$  and [7, Theorem 3.1] we obtain an  $\mathbb{F}_q$ -linear code  $C_2 \subseteq \mathbb{F}_q^{nN}$  having the properties:  $\text{Hull}(C_2) = \{0\}$  and  $C_2$  is an  $[nN, kK, \geq dD]_q$  code.
- 2.5) Using  $C_2$  and  $C_2^\perp$  obtain an  $[[nN, kK, \geq dD; nN - kK]]_q$  entanglement-assisted quantum code following [9, Theorem 4].

Using the arguments above we conclude the following.

**Theorem 4.2.** *Let  $q$  be an arbitrary prime power. For integers  $2 \leq k \leq n$  assume that there exists an isometry map  $\pi : \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q^n$  such that the isometry code  $\pi(\mathbb{F}_{q^k})$  has parameters  $[n, k, d]$ . If  $G$  is a generator matrix of an  $[N, K, D]_{q^k}$  classical code, then Construction 2 gives an  $[[nN, kK, \geq dD; nN - kK]]_q$  entanglement-assisted quantum code.*

Using [7, Example 2.3] we obtain an isometry  $\pi_2 : \mathbb{F}_4 \rightarrow \mathbb{F}_2^4$  so that the parameters of the isometry code  $\pi_2(\mathbb{F}_4)$  is  $[4, 2, 2]_2$ . Note that this isometry code is optimal. Using this isometry and Construction 2 we obtain the following.

**Corollary 4.1.** *Let  $1 \leq K \leq N$  be integers. Using Construction 2, the isometry  $\pi_2$  given above and an  $\mathbb{F}_4$ -linear code with parameters  $[N, K, D_4(N, K)]_4$ , we obtain a binary entanglement-assisted quantum code with parameters*

$$[[4N, 2K, \geq 2D_4(N, K); 4N - 2K]]_2.$$

*Similarly let  $1 \leq D \leq N$  be integers. Using Construction 2, the isometry  $\pi_2$  given above and an  $\mathbb{F}_4$ -linear code with parameters  $[N, K_4(N, D), D]_4$ , we obtain a binary*

*entanglement-assisted quantum code with parameters*

$$[[4N, 2K_4(N, D), \geq 2D; 4N - 2K_4(N, D)]]_2.$$

**Remark 4.3.** Using another isometry map  $\pi : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2^n$ , it is immediate to get an analogue of Corollary 4.1. For example there exists an isometry map  $\pi : \mathbb{F}_{2^3} \rightarrow \mathbb{F}_{2^5}$  so that the isometry code  $\pi(\mathbb{F}_{2^3})$  has parameters  $[5, 3, 2]_2$ . This allows to construct binary entanglement-assisted quantum codes with parameters

$$[[5N, 3K, \geq 2D_8(N, K); 5N - 3K]]_2 \quad \text{and} \quad [[5N, 3K_8(N, D), \geq 2D; 5N - 3K_8(N, D)]]_2.$$

For ternary codes, it is not difficult to find an isometry  $\pi_3 : \mathbb{F}_9 \rightarrow \mathbb{F}_3^5$  so that the parameters of the isometry code  $\pi_3(\mathbb{F}_9)$  is  $[5, 2, 3]_3$ . Note that this isometry code is optimal. Using this isometry and Construction 2 we obtain the following.

**Corollary 4.2.** *Let  $1 \leq K \leq N$  be integers. Using Construction 2, the isometry  $\pi_3$  given above and an  $\mathbb{F}_9$ -linear code with parameters  $[N, K, D_9(N, K)]_9$ , we obtain a ternary entanglement-assisted quantum code with parameters*

$$[[5N, 2K, \geq 3D_4(N, K); 5N - 2K]]_3.$$

*Similarly let  $1 \leq D \leq N$  be integers. Using Construction 2, the isometry  $\pi_3$  given above and an  $\mathbb{F}_9$ -linear code with parameters  $[N, K_9(N, D), D]_9$ , we obtain a ternary entanglement-assisted quantum code with parameters*

$$[[5N, 2K_9(N, D), \geq 3D; 5N - 2K_9(N, D)]]_3.$$

**Remark 4.4.** As in Remark 4.3, it is immediate to get an analogue of Corollary 4.2 provided we know a good isometry map. For example there exists an isometry map  $\pi : \mathbb{F}_{3^3} \rightarrow \mathbb{F}_3^4$  so that the isometry code  $\pi(\mathbb{F}_{3^3})$  has parameters  $[4, 3, 2]_3$ . This allows to construct ternary entanglement-assisted quantum codes with parameters

$$[[4N, 3K, \geq 2D_{27}(N, K); 4N - 3K]]_3 \quad \text{and} \quad [[4N, 3K_{27}(N, D), \geq 2D; 4N - 3K_{27}(N, D)]]_3.$$

**Remark 4.5.** Construction 2 also improves several recent results significantly. For example in [22] they state that a code  $C_1$  with parameters  $[[90, 28, 10; 62]]_2$  is a new entanglement-assisted quantum code in [22, Table 1]. Using Construction 2, in particular Corollary 4.1 with a  $[22, 14, 6]_4$  code (see [15]), we obtain a  $[[88, 28, 12; 60]]_2$  entanglement-assisted quantum code  $C_2$ . The dimensions of  $C_1$  and  $C_2$  are the same. The other parameters in going from  $C_1$  to  $C_2$  behave as follows:  $n$  decreases,  $d$  increases and  $c$  decreases. These are all in favor of  $C_2$ . Hence  $C_2$  is a better code compared to  $C_1$  in terms of the parameters.

Similarly in [22, Table 1] they state a code  $C_1$  with parameters  $[[30, 6, 5; 24]]_2$  as a new entanglement-assisted quantum code. Using Corollary 4.1 with a  $[7, 3, 4]_4$  code (see [15]), we obtain a  $[[28, 6, 8; 22]]_2$  entanglement-assisted quantum code  $C_2$ . Again

the dimensions of  $C_1$  and  $C_2$  are the same and all the other parameters are in favor of  $C_2$ . Hence  $C_2$  is a better code compared to  $C_1$  in terms of the parameters.

In [31] they state a code  $C_1$  with parameters  $[[132, 12, 30; 120]]_2$  is a new entanglement-assisted quantum code in [31, Table 1]. Using Corollary 4.1 with a  $[33, 6, 20]_4$  code (see [15]), we obtain a  $[[132, 12, 40; 120]]_2$  entanglement-assisted quantum code  $C_2$ . All the parameters of  $C_1$  and  $C_2$  are the same except the minimum distance. The improvement of the minimum distance in  $C_2$  from 30 to 40 is significant.

#### APPENDIX A. APPENDIX A: SINGLETON TYPE BOUND FOR ENTANGLEMENT-ASSISTED QUANTUM CODES

In Appendix A we prove a Singleton type bound for entanglement-assisted quantum codes using methods from [1, 2, 20, 21].

Recall that  $\mathbb{F}_q$  is the finite field with  $q$  elements. Let  $\text{char}(\mathbb{F}_q) = p$  so that  $\mathbb{F}_p \subseteq \mathbb{F}_q$ . Let  $\mathbb{C}$  denote the complex field. We regard  $\mathbb{C}^q$  as a Hilbert space and let  $|x\rangle$  be the (column) vectors of an orthonormal basis of  $\mathbb{C}^q$ , where the labels  $x$  are elements of  $\mathbb{F}_q$ . Let  $\zeta_p = \exp(2\pi\sqrt{-1}/p)$  be a  $p$ -th root of unity in  $\mathbb{C}$ . Let  $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$  be the trace map from  $\mathbb{F}_q$  onto  $\mathbb{F}_p$ .

For  $a, b \in \mathbb{F}_q$ , let  $\mathcal{X}(a)$  and  $\mathcal{Z}(b)$  be the unitary operations on  $\mathbb{C}^q$  defined by

$$\mathcal{X}(a)|x\rangle = |x + a\rangle \text{ and } \mathcal{Z}(b)|x\rangle = \zeta_p^{\text{tr}(bx)}|x\rangle.$$

Let  $\mathbb{C}^{q^n} = (\mathbb{C}^q)^{\otimes n}$  be the  $n$ -th tensor of  $\mathbb{C}^q$ . The coordinate basis is given by

$$|\mathbf{x}\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle.$$

Consider  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ . Let  $\mathcal{X}(\mathbf{a})$  and  $\mathcal{Z}(\mathbf{b})$  be the unitary operations on  $\mathbb{C}^{q^n}$  defined by

$$\mathcal{X}(\mathbf{a})|\mathbf{x}\rangle = |\mathbf{x} + \mathbf{a}\rangle \text{ and } \mathcal{Z}(\mathbf{b})|\mathbf{x}\rangle = \zeta_p^{\text{tr}(\mathbf{b}\cdot\mathbf{x})}|\mathbf{x}\rangle,$$

where  $\mathbf{b} \cdot \mathbf{x} = \sum_{i=1}^n b_i x_i \in \mathbb{F}_q$ .

The set  $\mathcal{E}_n = \{\zeta_p^u \mathcal{X}(\mathbf{a})\mathcal{Z}(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, u \in \mathbb{F}_p\}$  is a finite group of order  $pq^{2n}$ . Let  $\mathbf{E}_n \subseteq \mathcal{E}_n$  be the subset defined as

$$\mathbf{E}_n = \{\mathcal{X}(\mathbf{a})\mathcal{Z}(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}.$$

For  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$  and  $e = \mathcal{X}(\mathbf{a})\mathcal{Z}(\mathbf{b}) \in \mathbf{E}_n$ , let the (quantum) weight  $w_Q(e)$  of  $e$  be the integer

$$w_Q(e) = \#\{1 \leq i \leq n : a_i \neq 0 \text{ or } b_i \neq 0\}.$$

For  $0 \leq i \leq n$ , let  $\mathcal{E}_n[i] \subseteq \mathcal{E}_n$  be the subset defined as

$$\mathcal{E}_n[i] = \{e \in \mathcal{E}_n : w_Q(e) = i\}.$$

**Definition A.1.** A  $q$ -ary quantum code of length  $n$  is a subspace  $Q$  of  $\mathbb{C}^{q^n}$  such that  $\dim_{\mathbb{C}} Q = K \geq 1$ . The *minimum distance* of  $Q$  is the largest integer  $d$  such that for any error  $e \in \mathcal{E}_n[i]$  with  $i < d$  we have

$$|v\rangle, |w\rangle \in Q \text{ are orthogonal vectors} \Rightarrow \langle v|e|w\rangle = 0.$$

Such a code  $Q$  is called an  $((n, K, d))_q$  code.

Next we formally define  $q$ -ary entanglement-assisted quantum error correcting codes. Let  $c$  be a positive integer. For  $|a\rangle \in \mathbb{C}^{q^n}$ ,  $|b\rangle \in \mathbb{C}^{q^c}$ , and  $|\psi\rangle = |a\rangle \otimes |b\rangle \in \mathbb{C}^{q^{n+c}}$  note that  $|a\rangle\langle a|$  is a  $q^n \times q^n$  matrix,  $|b\rangle\langle b|$  is a  $q^c \times q^c$  matrix, and  $|\psi\rangle\langle\psi|$  is a  $q^{n+c} \times q^{n+c}$  matrix. Recall that  $\text{Tr}$  is the trace operation on square matrices and hence  $\text{Tr}(|a\rangle\langle a|)$  is a complex number. Let  $\text{Tr}_A(|\psi\rangle\langle\psi|)$  denote the  $q^c \times q^c$  over  $\mathbb{C}$  defined as

$$\text{Tr}_A(|\psi\rangle\langle\psi|) = \text{Tr}(|a\rangle\langle a|)|b\rangle\langle b|.$$

We extend this definition to  $\mathbb{C}^{q^{n+c}} = \mathbb{C}^{q^n} \otimes \mathbb{C}^{q^c}$  as follows: Let  $|\psi\rangle \in \mathbb{C}^{q^{n+c}}$  be an arbitrary vector. There exist an integers  $s \geq 1$ , vectors  $|a_1\rangle, \dots, |a_s\rangle \in \mathbb{C}^{q^n}$ , vectors  $|b_1\rangle, \dots, |b_s\rangle \in \mathbb{C}^{q^c}$  and complex numbers  $\lambda_1, \dots, \lambda_s \in \mathbb{C}$  such that  $|\psi\rangle = \lambda_1|a_1\rangle \otimes |b_1\rangle + \dots + \lambda_s|a_s\rangle \otimes |b_s\rangle$ . Put  $|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle$  for  $1 \leq i \leq s$ . We further assume without loss of generality that  $\{|a_i\rangle : 1 \leq i \leq s\} \subseteq \mathbb{C}^{q^n}$  is an orthonormal set or  $\{|b_i\rangle : 1 \leq i \leq s\} \subseteq \mathbb{C}^{q^c}$  is an orthonormal set. Note that  $\text{Tr}_a(|\psi_i\rangle\langle\psi_i|)$  is a  $q^c \times q^c$  matrix defined above. Now we define  $\text{Tr}_A(|\psi\rangle\langle\psi|)$  for the arbitrarily chosen vector  $|\psi\rangle \in \mathbb{C}^{q^{n+c}}$  as the  $q^c \times q^c$  matrix given by

$$\text{Tr}_A(|\psi\rangle\langle\psi|) = |\lambda_1|^2 \text{Tr}_A(|\psi_1\rangle\langle\psi_1|) + \dots + |\lambda_s|^2 \text{Tr}_A(|\psi_s\rangle\langle\psi_s|).$$

**Definition A.2.** An  $((n, K, d; c))_q$  *entanglement-assisted  $q$ -ary quantum error correcting code* is a subspace  $Q$  of  $\mathbb{C}^{q^{n+c}}$  such that  $\dim_{\mathbb{C}} Q = K \geq 1$  satisfying the following two properties:

- 1.)  $|\psi\rangle \in Q \Rightarrow \text{Tr}_A(|\psi\rangle\langle\psi|) = \frac{1}{q^c} I_{q^c}$ , where  $I_{q^c}$  is the identity operation on  $\mathbb{C}^{q^c}$ .

- 2.) For integer  $0 \leq i < d$  and each error  $e \in \mathcal{E}_n[i]$  we have:

$$|v'\rangle, |w'\rangle \in Q \text{ are orthogonal vectors} \Rightarrow \langle v'|e'|w'\rangle = 0,$$

where  $e'$  is the error in  $\mathbf{E}_{n+c}$  defined as  $e' = e \otimes I_{q^c}$ .

Let  $\{|\psi_i\rangle : 1 \leq i \leq K\}$  be an orthogonal basis of  $Q$ . Let

$$P = \sum_{i=1}^K |\psi_i\rangle\langle\psi_i|$$

be the orthogonal projection of  $\mathbb{C}^{q^{n+c}}$  onto  $Q$ . For  $1 \leq i \leq n$  and  $1 \leq j \leq c$  be the split weight enumerators of  $Q$  defined by

$$B_{i,j} = \frac{1}{K^2} \sum_{\substack{e \in \mathbf{E}_n[i] \\ e' \in \mathbf{E}_c[j]}} (\text{Tr}((e \otimes e')P))^2,$$

and

$$B_{i,j}^\perp = \frac{1}{K} \sum_{\substack{e \in \mathbf{E}_n[i] \\ e' \in \mathbf{E}_c[j]}} \text{Tr}((e \otimes e')P(e \otimes e')P).$$

We need to recall some notions and properties of Krawtchouk polynomials before the next theorem. We refer to [27, Section 5.7] for details. Let  $m$  be a positive integer. For  $0 \leq i \leq m$ , the  $i$ -th  $q^2$ -ary Krawtchouk polynomial with respect to  $m$  is

$$(12) \quad P_i(x; m) = \sum_{j=0}^i (-1)^j (q^2 - 1)^{i-j} \binom{x}{j} \binom{n-x}{i-j}.$$

In this paper we consider  $q^2$ -ary Krawtchouk polynomials. Note that  $P_i(x; m)$  is a polynomial of degree  $i$  in  $x$  with the leading coefficient  $(-q^2)^i/i!$  and the constant term  $\binom{n}{i}(q-1)^i$ . In particular

$$(13) \quad P_0(x; m) = 1 \text{ and } P_1(x; m) = -q^2x + 1.$$

Let  $0 \leq r, s \leq m$  be integers. Recall that the Kronecker symbol  $\delta_{r,s}$  is given by

$$\delta_{r,s} = \begin{cases} 1 & \text{if } r = s, \\ 0 & \text{if } r \neq s. \end{cases}$$

We have the orthogonality relations (see [27, Section 5.7, Corollary 18]) that

$$(14) \quad \sum_{i=0}^m P_r(i; m) = P_i(s; m) = q^{2m} \delta_{r,s}.$$

Moreover we also have (see [27, Section 5.7, Exercise 41]) that

$$(15) \quad \sum_{i=0}^m \binom{n-r}{n-s} P_r(x; m) = q^{2s} \binom{n-x}{s}.$$

Let  $n, c$  be positive integers. Let  $f(x, y) \in \mathbb{R}[x, y]$  be a polynomial of degree at most  $n$  in  $x$  and at most  $c$  in  $y$ . The properties above imply that there exist uniquely determined coefficients  $f_{u,v} \in \mathbb{R}$  for  $0 \leq u \leq n$  and  $0 \leq v \leq c$  such that

$$(16) \quad f(x, y) = \sum_{u=0}^n \sum_{v=0}^c f_{u,v} P_u(x; n) P_v(y; c).$$

The expansion in (16) is called the Krawtchouk expansion of  $f(x, y)$ . Using (14) we determine the coefficients in the Krawtchouk expansion as

$$(17) \quad f_{i,j} = \frac{1}{q^{2(n+c)}} \sum_{u=0}^n \sum_{v=0}^c f(u, v) P_u(i; n) P_v(j; c)$$

for  $0 \leq i \leq n$  and  $0 \leq j \leq c$ .

Now we are ready for the next theorem. The proof of the following theorem uses the same arguments as in [21, Theorem 2] and hence we skip its proof.

**Theorem A.3.** *Assume that  $Q$  is an  $((n, K, d; c))_q$  entanglement-assisted  $q$ -ary quantum error correcting code with projector  $P$  and split weight enumerators  $B_{i,j}$  and  $B_{i,j}^\perp$  for  $0 \leq i \leq n$ ,  $0 \leq j \leq c$ , respectively. Then the following properties hold:*

- 1.)  $B_{0,0} = B_{0,0}^\perp = 1$ .
- 2.)  $B_{i,j}^\perp \geq B_{i,j} \geq 0$ .
- 3.)  $B_{0,j} = 0$  for  $j = 1, \dots, c$ .
- 4.)  $B_{i,0} = B_{i,0}^\perp$  for  $i = 1, \dots, d-1$ .
- 5.)  $B_{d,0} < B_{d,0}^\perp$ .
- 6.)

$$B_{i,j}^\perp = \frac{K}{q^{n+c}} \sum_{u=0}^n \sum_{v=0}^c B_{u,v} P_i(u; n) P_j(v; c)$$

and

$$B_{i,j} = \frac{1}{q^{n+c} K} \sum_{u=0}^n \sum_{v=0}^c B_{u,v}^\perp P_i(u; n) P_j(v; c).$$

The following theorem is similar to [2, Theorem 4] and [21, Theorem 5].

**Theorem A.4.** *Let  $Q$  be an  $((n, K, d; c))_q$  entanglement-assisted quantum error correcting code. For  $0 \leq i \leq n$  and  $0 \leq j \leq c$  let  $f_{i,j} \in \mathbb{R}$  such that*

$$(18) \quad f_{i,j} \geq 0 \text{ for all } i, j \text{ in this range,}$$

and

$$(19) \quad f_{i,0} > 0 \text{ for } 0 \leq i \leq d-1.$$



Let  $f(x, y) \in \mathbb{R}[x, y]$  be the polynomial defined using the coefficients  $f_{i,j}$  above and the Krawtchouk polynomials in  $x$  and  $y$  variables given by

$$(20) \quad f(x, y) = \sum_{i=0}^n \sum_{j=0}^c f_{i,j} P_i(x; n) P_j(y; c)$$

Assume further that

$$(21) \quad f(\alpha, \beta) \leq 0 \text{ for all integers } d \leq \alpha \leq n \text{ and } 1 \leq \beta \leq c.$$

Then we have

$$K \leq \frac{1}{q^{n+c}} \max_{0 \leq \ell \leq d-1} \frac{f(\ell, 0)}{f_{\ell, 0}}.$$

*Proof.* Let  $B_{i,j}$  and  $B_{i,j}^\perp$  be the split weight enumerators of  $Q$ . Using (18) we obtain

$$(22) \quad LHS := q^{n+c} K \sum_{i=0}^{d-1} f_{i,0} B_{i,0} \leq q^{n+c} K \sum_{i=0}^{d-1} \sum_{j=0}^c f_{i,j} B_{i,j}.$$

It follows from Theorem A.3, item 6) that

$$(23) \quad B_{i,j} = \frac{1}{q^{n+c} K} \sum_{u=0}^n \sum_{v=0}^c B_{u,v}^\perp P_i(u; n) P_j(v; c)$$

for  $0 \leq i \leq d-1$  and  $0 \leq j \leq c$ . Combining (22) and (23) we obtain that

$$(24) \quad \begin{aligned} LHS &\leq \sum_{i=0}^{d-1} \sum_{j=0}^c f_{i,j} \sum_{u=0}^n \sum_{v=0}^c B_{u,v}^\perp P_i(u; n) P_j(v; c) \\ &= \sum_{u=0}^n \sum_{v=0}^c B_{u,v}^\perp f(u, v), \end{aligned}$$

where we use the definition in (20). Using (24) and (21) we get that

$$(25) \quad LHS \leq \sum_{i=0}^{d-1} B_{i,0}^\perp f(i, 0).$$

Combining (25) and Theorem A.3, item 4 we conclude that

$$(26) \quad q^{n+c} K \sum_{i=0}^{d-1} f_{i,0} B_{i,0} \leq \sum_{i=0}^{d-1} f(i, 0) B_{i,0}.$$

It follows from (26) that we have

$$K \leq \frac{1}{q^{n+c}} \frac{\sum_{i=0}^{d-1} f(i, 0) B_{i,0}}{\sum_{i=0}^{d-1} f_{i,0} B_{i,0}} \leq \frac{1}{q^{n+c}} \max_{0 \leq i \leq d-1} \frac{f(i, 0)}{f_{i,0}}.$$

□

The main result of this appendix is the following Singleton type bound for entanglement-assisted quantum error correcting codes.

**Theorem A.5.** *Let  $Q$  be an  $((n, K, d; c))_q$  entanglement-assisted quantum error correcting code. If  $d \leq \frac{n+2}{2}$ , then*

$$K \leq q^{n+c-2(d-1)}.$$

*Proof.* Let  $f(x, y) \in \mathbb{R}[x, y]$  be the polynomial

$$(27) \quad f(x, y) = \frac{q^{2(n+c-d+1)}}{(-1)^c c!} \prod_{i=d}^n \left(1 - \frac{x}{i}\right) \prod_{j=1}^c (y - j).$$

For integers  $0 \leq \alpha \leq n$  and  $0 \leq \beta \leq c$  we have

- $f(\alpha, \beta) = 0$  if  $1 \leq \beta \leq c$ , and
- $f(\alpha, 0) = q^{2(n+c-d+1)} \frac{\binom{n-\alpha}{n-d+1}}{\binom{n}{d-1}}$

by definition in (27). Consider the Krawtchouk expansion of  $f(x, y)$

$$f(x, y) = \sum_{u=0}^n \sum_{v=0}^c f_{u,v} P_u(x; n) P_v(y; c),$$

with the coefficients  $f_{u,v} \in \mathbb{R}$ . It follows from (17) that we have

$$f_{u,v} = \frac{1}{q^{2(n+c)}} \sum_{\alpha=0}^n \sum_{\beta=0}^c f(\alpha, \beta) P_\alpha(i; n) P_\beta(j; c).$$

As  $f(\alpha, \beta) = 0$  for  $0 \leq \alpha \leq c$  and  $1 \leq \beta \leq c$  for the function  $f(x, y)$  in (27) and  $P_0(y, c) = 1$  (see (13)) we obtain that

$$(28) \quad \begin{aligned} f_{u,v} &= \frac{1}{q^{2(n+c)}} \sum_{\alpha=0}^n f(\alpha, 0) P_\alpha(u; n) \\ &= \frac{1}{q^{2(n+c)}} \sum_{\alpha=0}^n q^{2(n+c-d+1)} \frac{\binom{n-\alpha}{n-d+1}}{\binom{n}{d-1}} P_\alpha(u; n) \\ &= q^{2(-d+1)} \sum_{\alpha=0}^n \frac{\binom{n-\alpha}{n-d+1}}{\binom{n}{d-1}} P_\alpha(u; n). \end{aligned}$$

It follows from (16) that we have

$$(29) \quad \sum_{\alpha=0}^n \binom{n-\alpha}{n-d+1} P_\alpha(u; n) = q^{2(d-1)} \binom{n-u}{d-1}.$$

Combining (28) and (29) we get

$$(30) \quad f_{u,v} = \frac{\binom{n-u}{d-1}}{\binom{n}{d-1}} \quad \text{for } 0 \leq u \leq n \text{ and } 0 \leq v \leq c.$$

In particular  $f_{u,v}$  is independent from  $v$ .

For  $0 \leq u_1 \leq u_2 \leq d - 1$  we claim that

$$(31) \quad \frac{f(u_1, 0)}{f_{u_1, 0}} \geq \frac{f(u_2, 0)}{f_{u_2, 0}}.$$

Indeed using (30) we get

$$\begin{aligned} \frac{f(u_1, 0)}{f_{u_1, 0}} &= \frac{\binom{n-u_1}{n-d+1}}{\binom{n-u_1}{d-1}} \geq \frac{f(u_2, 0)}{f_{u_2, 0}} = \frac{\binom{n-u_2}{n-d+1}}{\binom{n-u_2}{d-1}} && \iff \\ \frac{\frac{(n-u_1)!}{(n-d+1)!(n-u_1-n+d-1)!}}{\frac{(n-u_1)!}{(d-1)!(n-u_1-d+1)!}} &\geq \frac{\frac{(n-u_2)!}{(n-d+1)!(n-u_2-n+d-1)!}}{\frac{(n-u_2)!}{(d-1)!(n-u_2-d+1)!}} && \iff \\ \frac{(n-u_1-d+1)!}{(d-u_1-1)!} &\geq \frac{(n-u_2-d+1)!}{(d-u_2-1)!} && \iff \\ \frac{(n-u_1-d+1)!}{(n-u_2-d+1)!} &\geq \frac{(d-u_1-1)!}{(d-u_2-1)!} && \iff \\ (n-u_1-d+1) \cdots (n-u_2-d+2) &\geq (d-u_1-1) \cdots (d-u_2) && \stackrel{(*)}{\iff} \\ n-u_1-d+1 &\geq d-u_1-1 && \iff \\ d &\leq \frac{n+2}{2}, \end{aligned}$$

where in the step (\*) above we use the observation that both sides are the products of  $u_2 - u_1$  consecutive integers such that the left hand side ends at  $n - u_1 - d + 1$  and the right hand side ends at  $d - u_1 - 1$ . As  $d \leq \frac{n+2}{2}$  by assumption, this completes the proof of the claim in (31).

We apply Theorem A.4 using  $f(x, y)$  in (27). Note that the assumptions of Theorem A.4 hold. Using Theorem A.4 and the claim in(31) we conclude that

$$\begin{aligned} K &\leq \frac{1}{q^{n+c}} \frac{f(0, 0)}{f_{0, 0}} \\ &= \frac{1}{q^{n+c}} f(0, 0) \\ &= \frac{1}{q^{n+c}} \frac{q^{2(n+c-d+1)}}{(-1)^c c!} (-1)^c c! \\ &= q^{n+c-2(d-1)}. \end{aligned}$$

□

**Remark A.6.** If  $q = 2$ , then Theorem A.5 corresponds to [21, Theorem 6]. It is clear from the proof of Theorem A.5 that the factor  $\frac{1}{(-1)^{c!}}$  is necessary in the definition of  $f(x, y)$  in (27) in the proof of Theorem A.5. However this factor is forgotten in the proof of [21, Theorem 6] in [21]. Hence we also present this small correction in our detailed proof.

**Remark A.7.** Let  $S$  be an abelian subgroup of  $\mathcal{E}_n$ . If  $S$  satisfies some commutation relations given in [25] (see also [9] and [21]), then

$$C = \{|\psi\rangle \in \mathbb{C}^{q^{n+c}} : g|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}.$$

is called an entanglement-assisted  $q$ -ary quantum error correcting *stabilizer* code. We refer to [25], [9] and [21] for further details on entanglement-assisted quantum stabilizer codes. In particular  $C$  is a subspace of  $\mathbb{C}^{q^{n+c}}$  and  $C$  is an entanglement-assisted  $q$ -ary quantum error correcting code in the sense of Definition A.2. If the parameters of  $C$  are shown as  $((n, K, d; c))_q$ , then we call  $C$  as an  $[[n, K, d; c]]_q$  throughout this paper in order to emphasize that  $C$  is a stabilizer code. Note that [9, Theorem 4] is a construction of stabilizer codes. As our constructions are based on [9, Theorem 4], the quantum codes in all sections except the appendices are quantum stabilizer codes and denoted using  $[[\cdot]]_q$ . It is clear that Theorem A.5 holds for quantum stabilizer codes as well.

## APPENDIX B. APPENDIX B: THE ALGORITHM OF CARLET ET. AL. [6]

In Appendix B, we explain an important step in detail of our Construction 1. Recall that we present Construction 1 in Section 3.

Let  $q \geq 4$  be a prime power. Let  $G$  be a  $k \times n$  matrix over  $\mathbb{F}_q$ , which is a generator matrix of an  $[n, k, d]_q$  code  $C$ . We observe that [6] gives an algorithm in order to modify  $G$  to a  $k \times n$  matrix  $G'$  over  $\mathbb{F}_q$  such that the linear code  $C'$  having  $G'$  as a generator matrix has the following properties:  $C'$  is an  $[n, k, d]_q$  over  $\mathbb{F}_q$  (same parameters as  $C$ ) and  $\text{Hull}(C') = \{0\}$  (while  $\text{Hull}(C)$  is not necessarily  $\{0\}$ ).

In this appendix we explain this algorithm in detail.

First we find a  $n \times n$  permutation matrix  $P$  over  $\mathbb{F}_q$  such that  $G_1 = GP$  is in the systematic form. Namely

$$G_1 = [I_k \quad A],$$

where  $I_k$  is the  $k \times k$  identity matrix and  $A$  is a  $k \times (n - k)$  matrix over  $\mathbb{F}_q$ . For example using Gaussian elimination we can find the row reduced echelon form of  $G$ . This indicates the pivot columns in the row reduced echelon form of  $G$ . Changing the pivot columns to the first  $k$  columns gives a method to find such a permutation matrix  $P$ .

Let  $C_1$  be the  $\mathbb{F}_q$ -linear code having  $G_1$  as a generator matrix. Note that  $C_1$  is permutation equivalent to  $C$  and hence  $C_1$  is again an  $[n, k, d]_q$  code.

Here we need to introduce a notation. For a symmetric  $k \times k$  matrix  $M$  and a subset  $I \subseteq \{1, 2, \dots, k\}$  with  $\#I = t$ , let  $M_I$  denote the  $(k-t) \times (k-t)$  symmetric submatrix of  $M$  obtained by removing the  $i$ -th column and  $i$ -th row of  $M$  for each  $i \in I$ . Note that  $M_I = M$  if  $I = \emptyset$ . We denote  $M_I = 0$  if  $I = \{1, 2, \dots, k\}$  by convention (see Remark B.1).

Note that  $G_1 G_1^T = (GP)(P^T G^T) = GG^T$  as  $PP^T = I_n$ . Let  $0 \leq t \leq k$  be the integer such that  $\text{rank}(GG^T) = k - t$ . It follows from (2) that  $\dim_{\mathbb{F}_q} \text{Hull}(C) = t$ . Hence there exists a subset  $I \subseteq \{1, \dots, k\}$  such that  $(GG^T)_I$  is invertible (see also [?]). In fact there is a deterministic way to choose such  $I$  as follows: Let  $J$  be the subset of  $\{1, 2, \dots, k\}$  such that  $j \in J$  if and only if the  $j$ -th column is a pivot in the reduced row echelon form of  $GG^T$ . Put  $I = \{1, 2, \dots, k\} \setminus J$ .

For  $1 \leq i \leq k$ , let  $\alpha_i \in \mathbb{F}_q$  be chosen as follows:

$$(32) \quad \alpha_i \in \begin{cases} \mathbb{F}_q \setminus \{0, 1, -1\} & \text{if } i \in I, \\ \{1\} & \text{if } i \notin I. \end{cases}$$

Let  $D$  be the  $n \times n$  diagonal matrix having entries  $\alpha_1, \alpha_2, \dots, \alpha_k, 1, \dots, 1$  in order, namely  $D = \text{Diag}(\alpha_1, \alpha_2, \dots, \alpha_k, 1, \dots, 1)$ . Let  $G_2$  be the  $k \times n$  matrix obtained from  $G_1$  as

$$G_2 = G_1 D.$$

Let  $C_2$  be the  $\mathbb{F}_q$ -linear code having  $G_2$  as a generator matrix. Recall that a square matrix  $M$  is called a monomial matrix if there exists exactly one nonzero entry in each row and column of  $M$  (see, [19, page 24]). Moreover if  $G$  is a  $k \times n$  generator matrix of a code  $C$  and  $M$  is an  $n \times n$  monomial matrix, then the code having  $GM$  as a generator matrix is called monomially equivalent to  $C$  (see, [19, page 469]). Here  $D$  is a monomial matrix and  $C_2$  is monomially equivalent to  $C_1$ . In particular  $C_2$  is an  $[n, k, d]_q$  code, having the same parameters as  $C_1$ .

Let  $D_1$  be the  $k \times k$  diagonal matrix given by  $D_1 = \text{Diag}(\alpha_1, \alpha_2, \dots, \alpha_k)$ . Note that

$$G_2 = [I_k \quad A] \begin{bmatrix} D_1 & 0 \\ 0 & I_{n-k} \end{bmatrix} = [D_1 \quad A]$$

and hence

$$(33) \quad \begin{aligned} G_2 G_2^T &= D_1^2 + AA^T = I_k + AA^T + \text{Diag}(\alpha_1^2 - 1, \dots, \alpha_k^2 - 1) \\ &= G_1 G_1^T + \text{Diag}(\alpha_1^2 - 1, \dots, \alpha_k^2 - 1). \end{aligned}$$

Recall that  $\text{rank}(G_1 G_1^T) = k - t$  and  $\alpha_1, \dots, \alpha_k \in \mathbb{F}_q$  are chosen as in (32). Hence using (33) and [6, Lemma 9] we conclude that

$$(34) \quad \det(G_2 G_2^T) = \left( \prod_{i \in I} (\alpha_i^2 - 1) \right) \det(G G^T)_I \neq 0,$$

where  $\det(G G^T)_I = 1$  if  $I = \{1, 2, \dots, k\}$  by convention (see Remark B.1). Therefore  $\text{Hull}(C_2) = \{0\}$ .

**Remark B.1.** If  $G$  is self-orthogonal, then  $G G^T = 0$  and hence  $t = k$ . In this degenerate case it is necessary to choose  $I = \{1, 2, \dots, k\}$ . We have the conventions that  $(G G^T)_I = 0$  and  $\det(G G^T)_I = 1$  when  $I = \{1, 2, \dots, k\}$ . Indeed in this degenerate case (33) becomes

$$G_2 G_2^T = 0 + \text{Diag}(\alpha_1^2 - 1, \dots, \alpha_k^2 - 1)$$

and hence we use the convention  $(G G^T)_I = 0$ . Again in this degenerate case (34) becomes

$$\det(G_2 G_2^T) = \left( \prod_{i \in I} (\alpha_i^2 - 1) \right)$$

and hence we use the convention  $\det(G G^T)_I = 1$ . We need to use the convention that  $\det(G G^T)_I = 1$  if  $I = \{1, 2, \dots, k\}$ . The convention  $(G G^T)_I = 0$  is not essential as it appears only in the background.

In summary we obtain the following algorithm:

Input: For integers  $1 \leq k \leq n$ , let  $G$  is a  $k \times n$  matrix of rank  $k$  over  $\mathbb{F}_q$ . Let  $C$  be the  $\mathbb{F}_q$  linear code having  $G$  as a generator matrix. Let  $C$  be an  $[n, k, d]_q$  code.

Output:  $G'$  is a  $k \times n$  matrix of rank  $k$  over  $\mathbb{F}_q$ . Let  $C'$  be the  $\mathbb{F}_q$  linear code having  $G'$  as a generator matrix. We obtain that  $C'$  is an  $[n, k, d]_q$  code with  $\text{Hull}(C') = \{0\}$ .

i) Find an  $n \times n$  permutation matrix  $P$  such that  $GP$  is in the systematic form so that  $GP = [I_k \quad A]$ .

ii) Let  $\text{rank}(G G^T) = k - t$ , Find a subset  $I \subseteq \{1, \dots, k\}$  such that  $\#I = t$  and  $(G G^T)_I$  is invertible.

iii) For  $1 \leq i \leq k$ , let  $\alpha_i \in \mathbb{F}_q$  be chosen as follows:

$$(35) \quad \alpha_i \in \begin{cases} \mathbb{F}_q \setminus \{0, 1, -1\} & \text{if } i \in I, \\ \{1\} & \text{if } i \notin I. \end{cases}$$

iv) Put  $G' = GP \text{Diag}(\alpha_1, \dots, \alpha_k, 1, \dots, 1)$ .

**Remark B.2.** In many cases for a starting code  $[n, k, d]_q$  code  $C$  we know a generator matrix  $G$  in systematic form. In such a case we take  $P = I_n$  and we skip step i) in the algorithm.

In the following examples we illustrate this algorithm. In these algorithms the generators matrices in the input are in systematic form and hence we take  $P = I_n$  as explained in Remark B.2.

**Example B.1.** Let  $q = 4$  and  $w \in \mathbb{F}_4$  be an element satisfying  $w^2 + w + 1 = 0$ . Note that  $w$  is a primitive element of  $\mathbb{F}_4$ . Let  $G$  be the  $7 \times 23$  matrix over  $\mathbb{F}_4$  given by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w^2 & 0 & w^2 & w & 1 & w & 1 & w^2 & w^2 & 0 & 0 & w & 1 & 0 & w \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w & 0 & 1 & w & 0 & 0 & w^2 & w^2 & 1 & w & 1 & w & w^2 & 0 & w^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & w^2 & w^2 & w & w^2 & 1 & w & w & 0 & 0 & w^2 & 0 & w & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & w & w & 1 & w^2 & 1 & w^2 & 0 & 1 & 1 & w^2 & w^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & w^2 & 0 & w^2 & w & w & 0 & 0 & w & 0 & w^2 & 1 & w^2 & w^2 & w^2 & w \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 0 & 1 & w & 0 & w^2 & 1 & w & 0 & 1 & w & w^2 & w & w & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 0 & 1 & w & 0 & w^2 & 1 & w & 0 & 1 & w & w^2 & w & w \end{bmatrix}.$$

Let  $C$  be the  $\mathbb{F}_4$ -linear code having  $G$  as a generator matrix. In fact  $C$  is a code in the database of Magma [3]. Using the Magma command  $\text{BKLC}(\mathbb{F}_4, 23, 7)$  (or  $\text{BDLC}(\mathbb{F}_4, 23, 12)$ ) we immediately obtain  $C$  and the matrix  $G$  above. Then  $C$  is an  $[23, 7, 12]_4$  code. Moreover  $C$  is an optimal code in both of the senses in Notation 3.4 and Notation 3.5 below. We refer to the online table [15] for the optimality.

We observe that  $\text{rank}(GG^T) = 6$  and hence  $\dim_{\mathbb{F}_4} \text{Hull}(C) = 1$ . Using the algorithm explained in this appendix, let  $I = \{7\} \subseteq \{1, 2, \dots, 7\}$ ,

$$D_1 = \text{Diag}(\underbrace{1, \dots, 1}_{6 \text{ times}}, w, \underbrace{1, \dots, 1}_{16 \text{ times}})$$

and  $G_1 = GD_1$ . Moreover let  $C_1$  be the  $\mathbb{F}_4$ -linear code having  $G_1$  as a generator matrix. We obtain that  $C_1$  is an  $[23, 7, 12]_4$  code and  $\text{Hull}(C_1) = \{0\}$ .

**Example B.2.** Let  $q = 4$  and  $w \in \mathbb{F}_4$  be an element satisfying  $w^2 + w + 1 = 0$ . Let  $G$  be the  $9 \times 19$  matrix over  $\mathbb{F}_4$  given by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & w^2 & w & w & 0 & 1 & 0 & w^2 & w^2 & w \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w & 0 & 0 & 1 & w & w & 1 & 1 & w & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w & 0 & 0 & 1 & w & w & 1 & 1 & w \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & 1 & 1 & w^2 & 0 & w^2 & w & w^2 & 0 & w \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & w & w^2 & w & w & w^2 & w & w^2 & w^2 & w & w^2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & w^2 & 0 & w & w^2 & w & 0 & w & 1 & 1 & w^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w^2 & 1 & 1 & w^2 & w^2 & 1 & 0 & 0 & w^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w^2 & 1 & 1 & w^2 & w^2 & 1 & 0 & 0 & w^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & w^2 & w & w & 0 & 1 & 0 & w^2 & w^2 & w & 1 \end{bmatrix}.$$

Let  $C$  be the  $\mathbb{F}_4$ -linear code having  $G$  as a generator matrix. Using the Magma command  $\text{BDLC}(\mathbb{F}_4, 19, 8)$  we immediately obtain  $C$  and the matrix  $G$  above. Then  $C$  is an  $[19, 9, 8]_4$  code. Note that  $C$  is a best known code in the sense of Notation 4.5 (see [15]).

We observe that  $\text{rank}(GG^T) = 0$  and hence  $\dim_{\mathbb{F}_4} \text{Hull}(C) = 9$ . Using the algorithm explained in this appendix, let  $I = \{1, 2, \dots, 9\} \subseteq \{1, 2, \dots, 9\}$ ,

$$D_1 = \text{Diag}(\underbrace{(w, \dots, w)}_{9 \text{ times}}, \underbrace{(1, \dots, 1)}_{10 \text{ times}})$$

and  $G_1 = GD_1$ . Moreover let  $C_1$  be the  $\mathbb{F}_4$ -linear code having  $G_1$  as a generator matrix. We obtain that  $C_1$  is an  $[19, 9, 8]_4$  code and  $\text{Hull}(C_1) = \{0\}$ .

**Example B.3.** Let  $q = 4$  and  $w \in \mathbb{F}_4$  be an element satisfying  $w^2 + w + 1 = 0$ . Let  $G$  be the  $7 \times 20$  matrix over  $\mathbb{F}_4$  given by

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & w^2 & 0 & 0 & 1 & w & w^2 & 1 & w & 0 & w & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & w^2 & 1 & 0 & w^2 & w^2 & 0 & w & 1 & w^2 & 0 & w \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & w^2 & w & w^2 & 0 & 1 & 1 & w & w^2 & 0 & w & w & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & w^2 & w^2 & w & w & w & w & 0 & 0 & w^2 & w & w^2 & w^2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & w & 0 & w^2 & w^2 & w^2 & w & 1 & 0 & w & w^2 & w & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & w & w & 0 & w & 1 & 1 & 1 & w^2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & w & 1 & 0 & 1 & w^2 & w & 1 & 0 & 1 & 0 & 0 & w^2 & w \end{bmatrix}.$$

Let  $C$  be the  $\mathbb{F}_4$ -linear code having  $G$  as a generator matrix. Using the Magma command  $\text{BKLC}(\mathbb{F}_4, 20, 7)$  we immediately obtain  $C$  and the matrix  $G$  above. Then  $C$  is an  $[20, 7, 10]_4$  code. Note that  $C$  is a best known code in the sense of Notation 3.4 (see [15]).

We observe that  $\text{rank}(GG^T) = 6$  and hence  $\dim_{\mathbb{F}_4} \text{Hull}(C) = 1$ . Using the algorithm explained in this appendix, let  $I = \{7\} \subseteq \{1, 2, \dots, 7\}$ ,

$$D_1 = \text{Diag}(\underbrace{(1, \dots, 1)}_{6 \text{ times}}, w, \underbrace{(1, \dots, 1)}_{13 \text{ times}})$$

and  $G_1 = GD_1$ . Moreover let  $C_1$  be the  $\mathbb{F}_4$ -linear code having  $G_1$  as a generator matrix. We obtain that  $C_1$  is an  $[20, 7, 10]_4$  code and  $\text{Hull}(C_1) = \{0\}$ .

#### ACKNOWLEDGMENTS

The authors extend thanks to the anonymous reviewers for their valuable comments and suggestions, which improved the quality and presentation of the manuscript.



## REFERENCES

- [1] A. Ashikhmin, E. Knill : *Nonbinary quantum stabilizer codes*, IEEE Trans. Inf. Theory **47** (2001), no. 7, pp. 3065–3072.
- [2] A. Ashikhmin, S. Litsyn : *Upper bounds on the size of quantum codes*, IEEE Trans. Inf. Theory **45** (1999), no. 4, pp. 1206–1215.
- [3] W. Bosma, J. Cannon, C. Playoust : *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), no. 3, pp. 235–265.
- [4] T. Brun, I. Devetak, M.-H. Hsieh : *Catalytic quantum error correction*, arXiv:quant-ph/0608027.
- [5] A.R. Calderbank, E. Rains, M.P.W. Shor, N.J.A. Sloane : *Quantum error correction via codes over GF(4)*, IEEE Trans. Inform. Theory **44** (1998), pp. 1369–1387.
- [6] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan : *Linear codes over are equivalent to LCD Codes for  $q > 3$* , IEEE Trans. Inform. Theory **64** (2018), no. 4, pp. 3010–3017.
- [7] C. Carlet, C. Güneri, F. Özbudak, P. Solé : *A new concatenated type construction for LCD codes and isometry codes*, Discrete Mathematics **341** (2018), no. 3, pp. 830–835.
- [8] Y. Fujiwara, D. Clark, P. Vandendriessche, V.D. Tonchev: *Entanglement-assisted quantum low-density parity-check codes*, Phys. Rev. A. **82** (2010), no. 4, 042338.
- [9] C. Galindo, F. Hernando, R. Matsumoto, D. Ruano: *Entanglement-assisted quantum error-correcting codes over arbitrary finite fields*, Quantum Information Processing **18** (2019), no. 4, Art. 116, 18 pp.
- [10] A. Garcia, H. Stichtenoth and C. Xing: *On subfields of the Hermitian function field*, Compos. Math. **120** (2000), no. 2, pp. 137–170.
- [11] V. D. Goppa: *Codes on algebraic curves* (in Russian), Dokl. Akad. Nauk SSSR **259** (1981), pp. 1289–1290.
- [12] K. Guenda, S. Jitman, T. A. Gulliver: *Constructions of good entanglement-assisted quantum error correcting codes*, Des. Codes Cryptogr. **86** (2018), no. 1, pp. 121–136.
- [13] K. Guenda, T. A. Gulliver, S. Jitman, S. Thipworawimon: *Linear  $\ell$ -intersection pairs of codes and their applications*, Des. Codes Cryptogr. **88** (2020), no. 1, pp. 133–152.
- [14] M. Grassl: *Entanglement-asisted quantum communication beating the quantum Singleton bound*, 16-th Asian Quantum Information Science Conference, August 28- September 2, 2016, Academia Sinica, Taipei, Taiwan, Online available at [http://aqis-conf.org/2016/wp-content/uploads/2015/12/03.GRASSL\\_EntanglementAssistedCommunication.pdf](http://aqis-conf.org/2016/wp-content/uploads/2015/12/03.GRASSL_EntanglementAssistedCommunication.pdf) . Accessed on 2020-09-20.
- [15] M. Grassl: *Bounds on the minimum distance of linear codes and quantum codes*, Online available at <http://www.codetables.de>. Accessed on 2020-09-20.
- [16] M. Grassl, F. Huber, A. Winter: *Entropic proofs of Singleton bounds for quantum error-correcting codes*, arXiv[quant-ph]:2010.07902v2, 2021-02-03 (first version is on 2020-10-15).
- [17] T. Brun, I. Devetak, M. H. Hsieh: *Correcting quantum errors with entanglement*, Science **314** (2006), Oct., pp. 436–439.
- [18] M. H. Hsieh, I. Devetak, T. Brun: *General entanglement-assisted quantum error-correcting codes*, Phys. Rev. A, Gen. Phys. **76** (2007), no. 6, Art. no. 062313.
- [19] W.C. Huffman, V. Pless: *Fundamentals of Error Correcting Codes*, Cambridge University Press (2003).
- [20] C. Hu, S. Yang, S. S.-T. Yau: *Weight enumerators for nonbinary asymmetric quantum codes and their applications*, Adv. in Appl. Math. **121** (2020), 102085, <https://doi.org/10.1016/j.aam.2020.102085>.

- [21] C.-Y. Lai, A. Ashikhmin : *Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators*, IEEE Trans. Inf. Theory **64** (2018), no. 1, pp. 622–639.
- [22] H. Liu, X. Liu: *New EAQEC codes from cyclic codes over  $\mathbb{F}_q + u\mathbb{F}_q$* , Quantum Information Processing **19** (2020) 85 <https://doi.org/10.1007/s11128-020-2580-3>.
- [23] X. Liu, L. Yu, P. Hu: *New entanglement-assisted quantum codes from  $k$ -Galois dual codes*, Finite Fields Appl. **55** (2019), no. 5, pp. 21–32.
- [24] G. Luo, X. Cao, X. Chen: *MDS codes with hulls of arbitrary dimensions and their quantum error correction*, IEEE Trans. Information Theory **65** (2019), no. 5, pp. 2944–2952.
- [25] L. Luo, Z. Ma, Z. Wei, R. Leng: *Non-binary entanglement-assisted quantum stabilizer codes*, Sci. China Inf. Sci. **60** (2017), no. 4, 42501, <https://doi.org/10.1007/s11432-015-0932-y>.
- [26] F. Özbudak, H. Stichtenoth: *Constructing codes from algebraic curves*, IEEE Trans. Information Theory **45** (1999), no. 7, pp. 2502–2505.
- [27] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, (1977).
- [28] MinT: Database for optimal parameters of  $(t,m,s)$ -nets,  $(t,s)$ -sequences, orthogonal arrays, linear codes and OAs. <http://mint.sbg.ac.at/index.php> . Accessed on 2020-09-21.
- [29] F. R. F. Pereira, R. Pellikaan, G. G. La Guardia, F. M. de Assis: *Application of complementary dual AG codes to entanglement-assisted quantum codes*, IEEE ISIT 2019 (IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019): pp. 1559–2563.
- [30] F. R. F. Pereira, R. Pellikaan, G. G. La Guardia, F. M. de Assis: *Entanglement-assisted quantum codes from algebraic geometry codes*, arXiv:1907.06357v2[cs.IT].
- [31] J. Qian, L. Zhang: *Entanglement-assisted quantum codes from arbitrary binary linear codes*, Des. Codes Cryptogr. **77** (2015), pp. 193–202.
- [32] H.-G. Rück, H. Stichtenoth: *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), pp. 185–188.
- [33] P.W. Shor: *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A. **52** (1995), no. 4, pp. 2493–2496.
- [34] A.M. Steane: *Simple quantum error correcting codes*, Phys. Rev. A. **54** (1996), pp. 4741–4751.
- [35] H. Stichtenoth: *Algebraic Function Fields and Codes*, Springer GTM, New York, **254** (2009).
- [36] G. van der Geer, E. W. Howe, K. Lauter, C. Ritzenthaler: *Tables of Curves with Many Points*, (2009) Online available at <http://www.manypoints.org>. Accessed on 2020-09-21.
- [37] M. M. Wilde and T. A. Brun: *Optimal entanglement formulas for entanglement-assisted quantum coding*, Phys. Rev. A, Gen. Phys. **77** (2008), no. 6, Art. no. 064302.