

Structures and Constructions of Subsystem Codes over Finite Fields

Salah A. Aly

Department of Computer Science

Texas A&M University, College Station, TX 77843-3112, USA

salah@cs.tamu.edu

Abstract—Quantum information processing is a rapidly mounting field that promises to accelerate the speed up of computations. The field utilizes the novel fundamental rules of quantum mechanics such as accelerations. Quantum states carrying quantum information are tempted to noise and decoherence, that's why the field of quantum error control comes. In this paper, we investigate various aspects of the general theory of quantum error control - subsystem codes. Particularly, we first establish two generic methods to derive subsystem codes from classical codes that are defined over finite fields \mathbb{F}_q and \mathbb{F}_{q^2} . Second, we derive cyclic subsystem codes and using our two methods, we derive all classes of subsystem codes. Consequently, we construct two famous families of cyclic subsystem BCH and RS codes. Cyclic subsystem RS codes are turned out to be Optimal and MDS codes saturating the singleton bound with equality. Third, we demonstrate several methods of subsystem code constructions by extending, shortening and combining given subsystem codes. Finally, we present tables of upper and lower bounds on subsystem codes parameters ¹.

I. INTRODUCTION

Quantum information processing as a growing exciting field has attracted researches from different disciplines. It utilizes the laws of quantum mechanical operations to perform physical exponentially speedy computations. In an open system, one might wonder how to perform such computations in the presence of decoherence and noise that disturb quantum states storing quantum information. Providentially, the goals of quantum error-correcting codes are to protect quantum states and to allow recovery of quantum information proceeded in computational operations of a quantum computer. Henceforth, one seeks to design good quantum codes that can be efficiently utilized for these goals.

A well-known approach to derive quantum error-correcting codes from classical self-orthogonal (or dual-containing) codes is called stabilizer codes, which were introduced a decade ago. Stabilizer codes inherit some properties of clifford group theory, i.e., they are stabilized by abelian finite groups. In the seminal paper by Calderbank *at. et* [6], various methods of stabilizer code constructions are given, along with their propagation rules and tables of upper bounds on their parameters. In a similar tactic, we also present subsystem code structures by establishing several methods to derive them easily from

classical codes. Subsystem codes inherit their name from the fact that the quantum codes are decomposed into two systems as explained in Section II. The classes of subsystem codes that we will derive are superior because they can be encoded and decoded using linear shift-register operations.

Subsystem codes as we prefer to call them were mentioned in the unpublished work by Knill [15], [14], in which He attempted to generalize the theory of quantum error-correcting codes into subsystem codes. Such codes with their stabilizer formalism were reintroduced recently [16], [19], [17], [13], [5]

This paper is structured as follows. In section II, we present a brief background on subsystem code structures and present the Euclidean and Hermitian constructions. In section III, we derive cyclic subsystem codes and provide two generic methods of their constructions from classical cyclic codes. Consequently in sections IV and V, we construct families of subsystem BCH and RS codes from classical BCH and RS over \mathbb{F}_q and \mathbb{F}_{q^2} defined using their defining sets. In sections VI and VII, we establish various methods of subsystem code constructions by extending and shortening the code lengths and combining pairs of known codes, in addition, tables of upper bounds on subsystem code parameters are given in section VIII.

Notation. If S is a set, then $|S|$ denotes the cardinality of the set S . Let q be a power of a prime integer p . We denote by \mathbb{F}_q the finite field with q elements. We use the notation $(x|y) = (x_1, \dots, x_n|y_1, \dots, y_n)$ to denote the concatenation of two vectors x and y in \mathbb{F}_q^n . The symplectic weight of $(x|y) \in \mathbb{F}_q^{2n}$ is defined as

$$\text{swt}(x|y) = \{(x_i, y_i) \neq (0, 0) \mid 1 \leq i \leq n\}.$$

We define $\text{swt}(X) = \min\{\text{swt}(x) \mid x \in X, x \neq 0\}$ for any nonempty subset $X \neq \{0\}$ of \mathbb{F}_q^{2n} .

The trace-symplectic product of two vectors $u = (a|b)$ and $v = (a'|b')$ in \mathbb{F}_q^{2n} is defined as

$$\langle u|v \rangle_s = \text{tr}_{q/p}(a' \cdot b - a \cdot b'),$$

where $x \cdot y$ denotes the dot product and $\text{tr}_{q/p}$ denotes the trace from \mathbb{F}_q to the subfield \mathbb{F}_p . The trace-symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as

$$C^{\perp_s} = \{v \in \mathbb{F}_q^{2n} \mid \langle v|w \rangle_s = 0 \text{ for all } w \in C\}.$$

¹This research has been done in Spring '07 and Fall '07 at CS/TAMU, and during Summer '07 at Bell-Labs & Alcatel-Lucent.

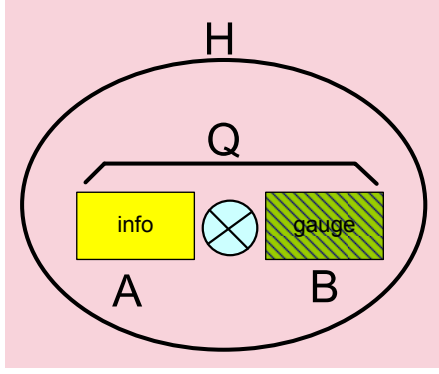


Fig. 1. Stabilizer and subsystem codes based on classical codes

We define the Euclidean inner product $\langle x|y\rangle = \sum_{i=1}^n x_i y_i$ and the Euclidean dual of $C \subseteq \mathbf{F}_q^n$ as

$$C^\perp = \{x \in \mathbf{F}_q^n \mid \langle x|y\rangle = 0 \text{ for all } y \in C\}.$$

We also define the Hermitian inner product for vectors x, y in $\mathbf{F}_{q^2}^n$ as $\langle x|y\rangle_h = \sum_{i=1}^n x_i^q y_i$ and the Hermitian dual of $C \subseteq \mathbf{F}_{q^2}^n$ as

$$C^{\perp_h} = \{x \in \mathbf{F}_{q^2}^n \mid \langle x|y\rangle_h = 0 \text{ for all } y \in C\}.$$

II. SUBSYSTEM CODES BACKGROUND

Let \mathcal{H} be the Hilbert space $C^{q^n} = C^q \otimes C^q \otimes \dots \otimes C^q$. Let $\{|x\rangle \mid x \in \mathbf{F}_q^n\}$ be the vectors of orthonormal basis of C^{q^n} , where the labels $|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$. For $a, b \in \mathbf{F}_q$, we define the unitary operators $X(a)$ and $Z(b)$ in C^q as follows:

$$X(a)|x\rangle = |x+a\rangle, \quad Z(b)|x\rangle = \omega^{\text{tr}(bx)}|x\rangle,$$

where $\omega = \exp(2\pi i/p)$ is a primitive p th root of unity and tr is the trace operation from \mathbf{F}_q to \mathbf{F}_p .

Now, we can define the set of error operators $E = \{X(a)Z(b) \mid a, b \in \mathbf{F}_q\}$ in an error group. Let $\mathbf{a} = (a_1, \dots, a_n) \in \mathbf{F}_q^n$ and $\mathbf{b} = (b_1, \dots, b_n) \in \mathbf{F}_q^n$. Let us denote by

$$X(\mathbf{a}) = X(a_1) \otimes \dots \otimes X(a_n) \text{ and },$$

$$Z(\mathbf{b}) = Z(b_1) \otimes \dots \otimes Z(b_n)$$

the tensor products of n error operators. The set $\mathbf{E} = \{X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n\}$ form an error basis on C^{q^n} . We can define the error group \mathbf{G} as follows

$$\mathbf{G} = \{\omega^c \mathbf{E} = \omega^c X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}.$$

A. Subsystem Codes

Let Q be a quantum code such that $\mathcal{H} = Q \oplus Q^\perp$, where Q^\perp is the orthogonal complement of Q , see 1. Recall definition of the error model acting in qubits as shown in the previous subsection. We can define the subsystem code Q as follows

Definition 1. An $[[n, k, r, d]]_q$ subsystem code is a decomposition of the subspace Q into a tensor product of two vector spaces A and B such that $Q = A \otimes B$, where $\dim A = q^k$ and

$\dim B = q^r$. The code Q is able to detect all errors of weight less than d on subsystem A .

Subsystem codes can be constructed from the classical codes over \mathbf{F}_q and \mathbf{F}_{q^2} , see Fig 2. We recall the Euclidean and Hermitian constructions from [2].

Lemma 2 (Euclidean Construction). *If C is a k' -dimensional \mathbf{F}_q -linear code of length n that has a k'' -dimensional subcode $D = C \cap C^\perp$ and $k' + k'' < n$, then there exists an*

$$[[n, n - (k' + k''), k' - k'', \text{wt}(D^\perp \setminus C)]]_q$$

subsystem code.

Proof: Let us define the code $X = C \times C \subseteq \mathbf{F}_q^{2n}$, therefore $X^{\perp_s} = (C \times C)^{\perp_s} = C^{\perp_s} \times C^{\perp_s}$. Hence $Y = X \cap X^{\perp_s} = (C \times C) \cap (C^{\perp_s} \times C^{\perp_s}) = D \times D$. Thus, $\dim_{\mathbf{F}_q} Y = 2k''$. Hence $|X||Y| = q^{2(k'+k'')}$ and $|X|/|Y| = q^{2(k'-k'')}$. By Theorem [2, Theorem 1], there exists a subsystem code $Q = A \otimes B$ with parameters $[[n, \log_q \dim A, \log_q \dim B, d]]_q$ such that

- i) $\dim A = q^n / (|X||Y|)^{1/2} = q^{n-k'-k'}$.
- ii) $\dim B = (|X|/|Y|)^{1/2} = q^{k'-k'}$.
- iii) $d = \text{swt}(Y^{\perp_s} \setminus X) = \text{wt}(D^\perp \setminus C)$.

Lemma 3 (Hermitian Construction). *If C is a k' -dimensional \mathbf{F}_{q^2} -linear code of length n that has a k'' -dimensional subcode $D = C \cap C^{\perp_h}$ and $k' + k'' < n$, then there exists an*

$$[[n, n - (k' + k''), k' - k'', \text{wt}(D^{\perp_h} \setminus C)]]_q$$

subsystem code.

Proof: See [2, Theorem 5]

III. CYCLIC SUBSYSTEM CODES

In this section we shall derive subsystem codes from classical cyclic codes. We first recall some definitions before embarking on the construction of subsystem codes. For further details concerning cyclic codes see for instance [11] and [18].

Let n be a positive integer and \mathbf{F}_q a finite field with q elements such that $\gcd(n, q) = 1$. Recall that a linear code $C \subseteq \mathbf{F}_q^n$ is called *cyclic* if and only if (c_0, \dots, c_{n-1}) in C implies that $(c_{n-1}, c_0, \dots, c_{n-2})$ in C .

For $g(x)$ in $\mathbf{F}_q[x]$, we write $\langle g(x) \rangle$ to denote the principal ideal generated by $g(x)$ in $\mathbf{F}_q[x]$. Let π denote the vector space isomorphism $\pi: \mathbf{F}_q^n \rightarrow R_n = \mathbf{F}_q[x]/(x^n - 1)$ given by

$$\pi((c_0, \dots, c_{n-1})) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1} + (x^n - 1).$$

A cyclic code $C \subseteq \mathbf{F}_q^n$ is mapped to a principal ideal $\pi(C)$ of the ring R_n . For a cyclic code C , the unique monic polynomial $g(x)$ in $\mathbf{F}_q[x]$ of the least degree such that $\langle g(x) \rangle = \pi(C)$ is called the *generator polynomial* of C . If $C \subseteq \mathbf{F}_q^n$ is a cyclic code with generator polynomial $g(x)$, then

$$\dim_{\mathbf{F}_q} C = n - \deg g(x).$$

Since $\gcd(n, q) = 1$, there exists a primitive n^{th} root of unity α over \mathbf{F}_q ; that is, $\mathbf{F}_q[\alpha]$ is the splitting field of the polynomial $x^n - 1$ over \mathbf{F}_q . Let us henceforth fix this primitive

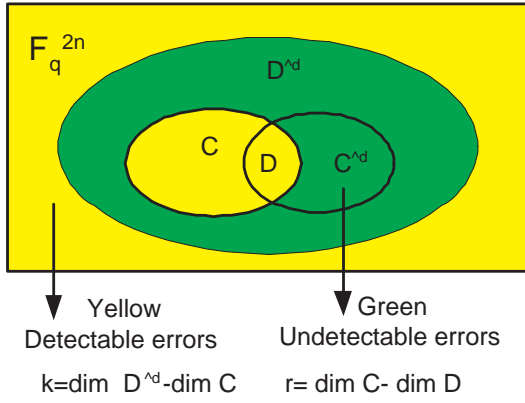


Fig. 2. Stabilizer and subsystem codes based on classical codes

n^{th} primitive root of unity α . Since the generator polynomial $g(x)$ of a cyclic code $C \subseteq \mathbb{F}_q^n$ is of minimal degree, it follows that $g(x)$ divides the polynomial $x^n - 1$ in $\mathbb{F}_q[x]$. Therefore, the generator polynomial $g(x)$ of a cyclic code $C \subseteq \mathbb{F}_q^n$ can be uniquely specified in terms of a subset T of $\{0, \dots, n-1\}$ such that

$$g(x) = \prod_{t \in T} (x - \alpha^t).$$

The set T is called the *defining set* of the cyclic code C (with respect to the primitive n^{th} root of unity α). A defining set is the union of cyclotomic cosets modulo n . The following lemma recalls some well-known and easily proved facts about defining sets (see e.g. [11]).

Lemma 4. Let C_i be a cyclic code of length n over \mathbb{F}_q with defining set T_i for $i = 1, 2$. Let $N = \{0, 1, \dots, n-1\}$ and $T_1^a = \{at \pmod n \mid t \in T\}$ for some integer a . Then

- i) $C_1 \cap C_2$ has defining set $T_1 \cup T_2$.
- ii) $C_1 + C_2$ has defining set $T_1 \cap T_2$.
- iii) $C_1 \subseteq C_2$ if and only if $T_2 \subseteq T_1$.
- iv) C_1^\perp has defining set $N \setminus T_1^{-1}$.
- v) $C_1^{\perp h}$ has defining set $N \setminus T_1^{-r}$ provided that $q = r^2$ for some positive integer r .

Notation. If T is a defining set of a cyclic code of length n , then we denote henceforth by T^a the set

$$T^a = \{at \pmod n \mid t \in T\},$$

as in the previous lemma. We use a superscript, since this notation will be frequently used in set differences, and arguably $N \setminus T^{-q}$ is more readable than $N \setminus -qT$.

Now, we shall give a general construction for subsystem cyclic codes. We say that a code C is self-orthogonal if and only if $C \subseteq C^\perp$. We show that if a classical cyclic code is self-orthogonal, then one can easily construct cyclic subsystem codes.

Proposition 5. Let D be a k -dimensional self-orthogonal cyclic code of length n over \mathbb{F}_q . Let T_D and T_{D^\perp} respectively denote the defining sets of D and D^\perp . If T is a subset of $T_D \setminus T_{D^\perp}$, then one can define a cyclic code C of length n over \mathbb{F}_q by the defining set $T_C = T_D \setminus (T \cup T^{-1})$. If $r = |T \cup T^{-1}|$ is in the range $0 \leq r < n - 2k$, and

$d = \min \text{wt}(D^\perp \setminus C)$, then there exists a subsystem code with parameters $[[n, n - 2k - r, r, d]]_q$.

Proof: Since D is a self-orthogonal cyclic code, we have $D \subseteq D^\perp$, whence $T_{D^\perp} \subseteq T_D$ by Lemma 4 iii). Observe that if s is an element of the set $S = T_D \setminus T_{D^\perp} = T_D \setminus (N \setminus T_D^{-1})$, then $-s$ is an element of S as well. In particular, T^{-1} is a subset of $T_D \setminus T_{D^\perp}$.

By definition, the cyclic code C has the defining set $T_C = T_D \setminus (T \cup T^{-1})$; thus, the dual code C^\perp has the defining set

$$T_{C^\perp} = N \setminus T_C^{-1} = T_{D^\perp} \cup (T \cup T^{-1}).$$

Furthermore, we have

$$T_C \cup T_{C^\perp} = (T_D \setminus (T \cup T^{-1})) \cup (T_{D^\perp} \cup T \cup T^{-1}) = T_D;$$

therefore, $C \cap C^\perp = D$ by Lemma 4 i).

Since $n - k = |T_D|$ and $r = |T \cup T^{-1}|$, we have $\dim_{\mathbb{F}_q} D = n - |T_D| = k$ and $\dim_{\mathbb{F}_q} C = n - |T_C| = k + r$. Thus, by Lemma 2 there exists an \mathbb{F}_q -linear subsystem code with parameters $[[n, \kappa, \rho, d]]_q$, where

- i) $\kappa = \dim D^\perp - \dim C = n - k - (k + r) = n - 2k - r$,
- ii) $\rho = \dim C - \dim D = k + r - k = r$,
- iii) $d = \min \text{wt}(D^\perp \setminus C)$,

as claimed. ■

We notice that if $\text{wt}(D) \leq \text{wt}(D^\perp)$, then the constructed cyclic subsystem codes are impure. In addition, if $d = \text{wt}(D^\perp) = \text{wt}(D^\perp \setminus D)$, then the constructed codes are pure up to d . A subsystem code is pure if and only if $\text{wt}(D^\perp \setminus C) = \text{wt}(D^\perp)$. Thus, it is impure if $\text{wt}(D^\perp) < \text{wt}(D^\perp \setminus C)$.

We can also derive subsystem codes from cyclic codes over \mathbb{F}_{q^2} by using cyclic codes that are self-orthogonal with respect to the Hermitian inner product.

Proposition 6. Let D be a cyclic code of length n over \mathbb{F}_{q^2} such that $D \subseteq D^{\perp h}$. Let T_D and $T_{D^{\perp h}}$ respectively be the defining set of D and $D^{\perp h}$. If T is a subset of $T_D \setminus T_{D^{\perp h}}$, then one can define a cyclic code C of length n over \mathbb{F}_{q^2} with defining set $T_C = T_D \setminus (T \cup T^{-q})$. If $n - k = |T_D|$ and $r = |T \cup T^{-q}|$ with $0 \leq r < n - 2k$, and $d = \text{wt}(D^{\perp h} \setminus C)$, then there exists an $[[n, n - 2k - r, r, d]]_q$ subsystem code.

Proof: Since $D \subseteq D^{\perp h}$, their defining sets satisfy $T_{D^{\perp h}} \subseteq T_D$ by Lemma 4 iii). If s is an element of $T_D \setminus T_{D^{\perp h}}$, then one easily verifies that $-qs \pmod n$ is an element of $T_D \setminus T_{D^{\perp h}}$.

Let $N = \{0, 1, \dots, n-1\}$. Since the cyclic code C has the defining set $T_C = T_D \setminus (T \cup T^{-q})$, its dual code $C^{\perp h}$ has the defining set $T_{C^{\perp h}} = N \setminus T_C^{-q} = T_{D^{\perp h}} \cup (T \cup T^{-q})$. We notice that

$$T_C \cup T_{C^{\perp h}} = (T_D \setminus (T \cup T^{-q})) \cup (T_{D^{\perp h}} \cup T \cup T^{-q}) = T_D;$$

thus, $C \cap C^{\perp h} = D$ by Lemma 4 i).

Since $n - k = |T_D|$ and $r = |T \cup T^{-q}|$, we have $\dim D = n - |T_D| = k$ and $\dim C = n - |T_C| = k + r$. Thus, by Lemma 3 there exists an $[[n, \kappa, \rho, d]]_q$ subsystem code with

- i) $\kappa = \dim D^{\perp h} - \dim C = (n - k) - (k + r) = n - 2k - r$,
- ii) $\rho = \dim C - \dim D = k + r - k = r$,
- iii) $d = \min \text{wt}(D^{\perp h} \setminus C)$,

as claimed. ■

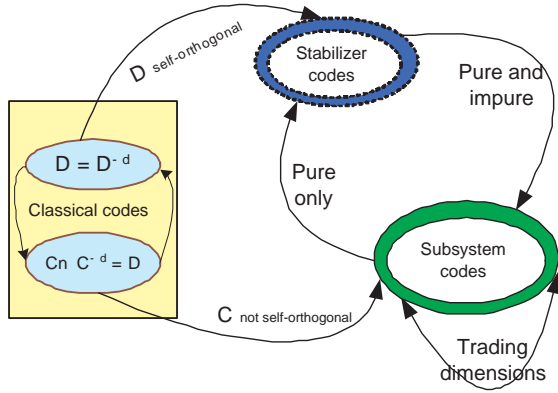


Fig. 3. Stabilizer and subsystem codes based on classical codes

We notice that if $\text{wt}(D) \leq \text{wt}(D^{\perp h})$, then the constructed cyclic subsystem codes are impure. In addition, if $d = \text{wt}(D^{\perp}) = \text{wt}(D^{\perp h} \setminus D)$, then the constructed codes are pure up to d .

The previous two propositions allow one to easily construct subsystem codes from classical cyclic codes. We will illustrate this fact by deriving cyclic subsystem codes from BCH and Reed-Solomon codes.

IV. SUBSYSTEM BCH CODES

In this section we consider an important class of cyclic codes that can be constructed with arbitrary designed distance δ . We will construct families of subsystem BCH codes.

Let n be a positive integer, \mathbf{F}_q be a finite field with q elements, and α is a primitive n th root of unity. A primitive narrow-sense BCH code C of designed distance δ and length n is a cyclic code with generator monic polynomial $g(x)$ over \mathbf{F}_q that has $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ as zeros. c is a codeword in C if and only if $c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{\delta-1}) = 0$. The parity check matrix of this code can be defined as

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(\delta-1)(n-1)} \end{bmatrix} \quad (1)$$

We have shown in [3], [4] that narrow sense BCH codes, primitive and non-primitive, with length n and designed distance δ are Euclidean dual-containing codes if and only if $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}])$. We use this result and [1, Theorem 2] to derive primitive subsystem BCH codes from classical BCH codes over \mathbf{F}_q and \mathbf{F}_{q^2} [2], [4].

For simplicity, we will proceed our work for primitive narrow sense BCH codes, however, the generalization for non-primitive BCH codes is a straightforward.

Lemma 7. *If q is power of a prime, m is a positive integer, and $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$. Then there exists a subsystem BCH code with parameters $[[q^m - 1, n - 2m\lceil(\delta - 1)(1 - 1/q)\rceil - r, r, \geq \delta]]_q$ where $0 \leq r < n - 2m\lceil(\delta - 1)(1 - 1/q)\rceil$.*

Proof: We know that if $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]$, then there exists a stabilizer code with parameters $[[q^m - 1, n - 2m\lceil(\delta - 1)(1 - 1/q)\rceil, \geq \delta]]_q$. Let r be an integer in the range $0 \leq r < n - 2m\lceil(\delta - 1)(1 - 1/q)\rceil$. From [1, Theorem 2], then there must exist a subsystem BCH code with parameters $[[q^m - 1, n - 2m\lceil(\delta - 1)(1 - 1/q)\rceil - r, r, \geq \delta]]_q$. ■

We can also construct subsystem BCH codes from stabilizer codes using the Hermitian constructions.

Lemma 8. *If q is a power of a prime, m is a positive integer, and δ is an integer in the range $2 \leq \delta \leq \delta_{\max} = q^{m+\lceil m \text{ even} \rceil} - 1 - (q^2 - 2)[m \text{ even}]$, then there exists a subsystem code Q with parameters*

$$[[q^{2m} - 1, q^{2m} - 1 - 2m\lceil(\delta - 1)(1 - 1/q^2)\rceil - r, r, d_Q \geq \delta]]_q$$

that is pure up to δ , where $0 \leq r < q^{2m} - 1 - 2m\lceil(\delta - 1)(1 - 1/q^2)\rceil$.

Proof: If $2 \leq \delta \leq \delta_{\max} = q^{m+\lceil m \text{ even} \rceil} - 1 - (q^2 - 2)[m \text{ even}]$, then exists a classical BCH code with parameters $[[q^m - 1, q^m - 1 - m\lceil(\delta - 1)(1 - 1/q)\rceil, \geq \delta]]_q$ which contains its dual code. From [1, Theorem 2], then there must exist a subsystem code with the given parameters. ■

Instead of constructing subsystem codes from stabilizer BCH codes as shown in Lemmas 7, 8, we can also construct subsystem codes from classical BCH codes over \mathbf{F}_q and \mathbf{F}_{q^2} under some restrictions on the designed distance. Let C_i be a cyclotomic coset defined as $\{iq^j \bmod n \mid j \in Z\}$.

Lemma 9. *If q is a power of a prime, m is a positive integer, and $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]$. Let D be a BCH code with length $n = q^m - 1$ and defining set $T_D = \{C_0, C_1, \dots, C_{n-\delta}\}$, such that $\gcd(n, q) = 1$. Let $T \subseteq \{0\} \cup \{C_\delta, \dots, C_{n-\delta}\}$ be a nonempty set. Assume $C \subseteq \mathbf{F}_q^n$ be a BCH code with the defining set $T_C = \{C_0, C_1, \dots, C_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then there exists a subsystem BCH code with the parameters $[[n, n - 2k - r, r, \geq \delta]]_q$, where $k = m\lceil(\delta - 1)(1 - 1/q)\rceil$ and $r = |T \cup T^{-1}|$.*

Proof: The proof can be divide into the following parts:

- i) We know that $T_D = \{C_0, C_1, \dots, C_{n-\delta}\}$ and $T \subseteq \{0\} \cup \{C_\delta, \dots, C_{n-\delta}\}$ be a nonempty set. Hence $T_D^\perp = \{C_1, \dots, C_{\delta-1}\}$. Furthermore, if $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]$, then $D \subseteq D^\perp$. Furthermore, let $k = m\lceil(\delta - 1)(1 - 1/q)\rceil$, then $\dim D^\perp = n - k$ and $\dim D = k$.
- ii) We know that $C \in \mathbf{F}_q^n$ is a BCH code with defining set $T_C = T_D \setminus (T \cup T^{-1}) = \{C_0, C_1, \dots, C_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then the dual code C^\perp has defining set $T_C^\perp = \{C_1, \dots, C_{\delta-1}\} \cup T \cup T^{-1} = T_{D^\perp} \cup T \cup T^{-1}$. We can compute the union set T_D as $T_C \cup T_C^\perp = \{C_0, C_1, \dots, C_{n-\delta}\} = T_D$. By Lemma 4, therefore, $C \cap C^\perp = D$. Furthermore, if $r = |T \cup T^{-1}|$, then $\dim C = k + r$.
- iii) From step (i) and (ii), and for $0 \leq r < n - 2k$, and by Lemma 2, there exists a subsystem code with parameters $[[n, \dim D - \dim C, \dim C - \dim D, d]]_q = [[n, n - 2k - r, r, d]]_q$, $d = \min \text{wt}(D^\perp - C) \geq \delta$.

Also, we can derive subsystem BCH codes from classical BCH codes over \mathbf{F}_{q^2} as shown in the following Lemma, see [4], [3].

Lemma 10. *If q is a power of a prime, n, m are positive integers, and $\gcd(n, q) = 1$. Let $n = (q^2)^m - 1$, $2 \leq \delta \leq q^m - 1 - (q - 2)[m \text{ odd}]$ and $T \subseteq \{0\} \cup \{C_\delta, \dots, C_{n-\delta}\}$. Let $C \subseteq \mathbf{F}_{q^2}^n$ be a cyclic code with the defining set $T_C = \{C_0, C_1, \dots, C_{n-\delta}\} \setminus (T \cup T^{-q})$ where $T^{-q} = \{-qt \bmod n \mid t \in T\}$. Then there exists a cyclic subsystem code with the parameters $[[n, n - 2k - r, r, \geq \delta]]_q$, where $k = m[(\delta - 1)(1 - 1/q^2)]$ and $0 \leq r = |T \cup T^{-q}| < n - 2k$.*

Proof:

Taking in consideration that the classical BCH codes are over \mathbf{F}_{q^2} , we can proceed the proof as follows.

- i) We know that the BCH code contains its Hermitian dual code if $2 \leq \delta \leq q^m - 1 - (q - 2)[m \text{ odd}]$. Let $n = (q^2)^m - 1$ and $D^{\perp_h} \subseteq \mathbf{F}_{q^2}^n$ be a BCH code defined with a designed distance δ . The dual code D^{\perp_h} has defining set $T_{D^{\perp_h}} = \{C_1, \dots, C_{\delta-1}\}$. Consequently, the code D has defining set $\{C_0, C_1, \dots, C_{n-\delta}\}$ and it is self-orthogonal, i.e., $D \subseteq D^{\perp_h}$. Furthermore, if $k = m[(\delta - 1)(1 - 1/q^2)]$, then $\dim D^{\perp_h} = n - k$ and $\dim D = k$.
- ii) We know that $C \subseteq \mathbf{F}_{q^2}^n$ is a BCH code with defining set $T_C = \{C_0, C_1, \dots, C_{n-\delta}\} \setminus (T \cup T^{-q})$ where $T^{-q} = \{-qt \bmod n \mid t \in T\}$. Then the dual code C^{\perp_h} has defining set $T_{C^{\perp_h}} = \{C_1, \dots, C_{\delta-1}\} \cup T \cup T^{-q}$. We can compute the union set T_D as $T_C \cup T_{C^{\perp_h}} = \{C_0, C_1, \dots, C_{n-\delta}\}$. Therefore, $C \cap C^{\perp_h} = D$. Assume $r = |T \cup T^{-q}|$, then $\dim C = k + r$.
- iii) From step (i) and (ii), and by Lemma 3 for $0 \leq r < n - 2k$, there exists a subsystem code with parameters $[[n, n - 2k - r, r, d]]_q$, where $k = m[(\delta - 1)(1 - 1/q^2)]$ and $0 \leq r = |T \cup T^{-q}| < n - 2k$, $d = \min wt(D^{\perp} - C) \geq \delta$.

Table II shows some families of subsystem BCH codes derived from classical BCH codes. The subsystem code $[[21, 18, 1, 2]]_2$ constructed using BCH codes, but the stabilizer code $[[21, 19, 2]]_2$ does not exist using the linear programming bound [6].

It may be useful to end up this section with an example

Example 11. *Consider a BCH code D^{\perp} with designed distance $d = 5$ and length $n = 2^5 - 1$ over \mathbf{F}_4 . Then $C_1 = \{1, 2, 4, 8, 16\}$, $C_2 = \{3, 6, 12, 24, 17\}$, and $C_5 = \{5, 10, 20, 9, 18\}$. Then $T_{D^{\perp_h}} = C_1 \cup C_3$. Hence $\dim D = 10$ and $\dim D^{\perp_h} = 21$. Now, let $T = C_5$, so, $T^{-q} = C_{11} = \{11, 13, 21, 22, 26\}$ and $T_{C^{\perp_h}} = T_{D^{\perp_h}} \cup T \cup T^{-q}$. We have $|T_{C^{\perp_h}}| = 20$, therefore $\dim C = 20$. Consequently, there exists a subsystem BCH codes with parameters $[[n, \dim D^{\perp_h} - \dim C, \dim C - \dim D, \geq \delta]]_q = [[31, 1, 10, \geq 5]]_2$. Some subsystem BCH codes are shown in Table II.*

V. SUBSYSTEM RS CODES

In this section we will derive cyclic subsystem codes based on Reed-Solomon codes. Also, we show that given optimal

TABLE I
SUBSYSTEM BCH CODES USING THE EUCLIDEAN CONSTRUCTION

Subsystem Code	Parent BCH Code	Designed distance
$[[15, 4, 3, 3]]_2$	$[15, 7, 5]_2$	4
$[[15, 6, 1, 3]]_2$	$[15, 5, 7]_2$	6
$[[31, 10, 1, 5]]_2$	$[31, 11, 11]_2$	8
$[[31, 20, 1, 3]]_2$	$[31, 6, 15]_2$	12
$[[63, 6, 21, 7]]_2$	$[63, 39, 9]_2$	8
$[[63, 6, 15, 7]]_2$	$[63, 36, 11]_2$	10
$[[63, 6, 3, 7]]_2$	$[63, 30, 13]_2$	12
$[[63, 18, 3, 7]]_2$	$[63, 24, 15]_2$	14
$[[63, 30, 3, 5]]_2$	$[63, 18, 21]_2$	16
$[[63, 32, 1, 5]]_2$	$[63, 16, 23]_2$	22
$[[63, 44, 1, 3]]_2$	$[63, 10, 27]_2$	24
$[[63, 50, 1, 3]]_2$	$[63, 7, 31]_2$	28
$[[15, 2, 5, 3]]_4$	$[15, 9, 5]_4$	4
$[[15, 2, 3, 3]]_4$	$[15, 8, 6]_4$	6
$[[15, 4, 1, 3]]_4$	$[15, 6, 7]_4$	7
$[[15, 8, 1, 3]]_4$	$[15, 4, 10]_4$	8
$[[31, 10, 1, 5]]_4$	$[31, 11, 11]_4$	8
$[[31, 20, 1, 3]]_4$	$[31, 6, 15]_4$	12
$[[63, 12, 9, 7]]_4$	$[63, 30, 15]_4$	15
$[[63, 18, 9, 7]]_4$	$[63, 27, 21]_4$	16
$[[63, 18, 7, 7]]_4$	$[63, 26, 22]_4$	22

* punctured code
+ Extended code

TABLE II
SUBSYSTEM BCH CODES USING HERMITIAN CONSTRUCTIONS

Subsystem Code	Parent BCH Code	Designed distance
$[[14, 1, 3, 4]]_2$	$[14, 8, 5]_{2^2}$	6*
$[[15, 1, 2, 5]]_2$	$[15, 8, 6]_{2^2}$	6
$[[15, 5, 2, 3]]_2$	$[15, 6, 7]_{2^2}$	7
$[[16, 5, 2, 3]]_2$	$[16, 6, 7]_{2^2}$	7+
$[[17, 8, 1, 4]]_2$	$[17, 5, 9]_{2^2}$	4
$[[21, 6, 3, 3]]_2$	$[21, 9, 7]_{2^2}$	6
$[[21, 7, 2, 3]]_2$	$[21, 8, 9]_{2^2}$	8
$[[31, 10, 1, 5]]_2$	$[31, 11, 11]_{2^2}$	8
$[[31, 20, 1, 3]]_2$	$[31, 6, 15]_{2^2}$	12
$[[32, 10, 1, 5]]_2$	$[32, 11, 11]_{2^2}$	8+
$[[32, 20, 1, 3]]_2$	$[32, 6, 15]_{2^2}$	12+
$[[25, 12, 3, 3]]_3$	$[25, 8, 12]_{3^2}$	9*
$[[26, 6, 2, 5]]_3$	$[26, 11, 8]_{3^2}$	8
$[[26, 12, 2, 4]]_3$	$[26, 8, 13]_{3^2}$	9
$[[26, 13, 1, 4]]_3$	$[26, 7, 14]_{3^2}$	14
$[[80, 1, 17, 20]]_3$	$[80, 48, 21]_{3^2}$	21
$[[80, 5, 17, 17]]_3$	$[80, 46, 22]_{3^2}$	22

* punctured code
+ Extended code

stabilizer codes, one can construct optimal subsystem codes. Recall that a Reed-Solomon code over \mathbf{F}_q is a BCH code with length $n = q - 1$ and minimum distance equals to its designed distance δ . Therefore, the RS code C with designed distance δ has defining set T with size $\delta - 1$. This can be seen as all roots lie in different cyclotomic cosets. The dimension of a RS code is given by $n - \delta + 1$. RS codes are an important class of optimal cyclic codes. They are MDS codes, in which Singleton bound is satisfied with equality.

Grassl *et al.* in [9] showed that optimal stabilizer codes with maximal minimum distance exist with parameters $[[n, n - 2d + 2, d]]_q$ over \mathbf{F}_q for $3 \leq n \leq q$ and $1 \leq d \leq n/2 + 1$. Also,

optimal stabilizer codes exist with parameters $[[q^2, q^2 - 2d + 2, d]]_q$ for $1 \leq d \leq q$ over \mathbf{F}_q , see [9, Theorems 9, 10]. These codes satisfy the quantum Singleton bound $k + 2d = n + 2$. The following subsystem codes are optimal since they obey the singleton bound $k + r + 2d = n + 2$ as shown in [2, Theorem 21].

Lemma 12 (Reed-Solomon Subsystem codes). *Let q be power of a prime.*

- i) If $0 \leq \delta < (q-1)/2$ there exist subsystem codes with parameters $[[q-1, q-2\delta-1-r, r, \delta+1]]_q$ and $[[q, q-2\delta-2-r, r, \delta+2]]_q$.
- ii) If $0 \leq \delta < q-1$ there exist subsystem codes with parameters $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$.

Proof:

- i) We know that if $0 \leq \delta < (q-1)/2$, then there are stabilizer codes with parameters $[[q-1, q-2\delta-1, \delta+1]]_q$ and $[[q, q-2\delta-2, \delta+2]]_q$, see [9, Theorem 9]. Now, let $0 \leq r < q-2\delta-1$, then using [1, Corollary 6], there are subsystem codes with parameters $[[q-1, q-2\delta-1-r, r, \delta+1]]_q$ and $[[q, q-2\delta-2-r, r, \delta+2]]_q$.
- ii) Similarly, if $0 \leq \delta < q-1$, then from [9, Theorem 10], there exist stabilizer codes with parameters $[[q^2-1, q^2-2\delta-1, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$. Assuming $0 \leq r < q^2-2\delta-1$, then from [1, Corollary 6], there exist subsystem codes with parameters $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$. ■

Instead of extending the subsystem code that we constructed, one can start with a subsystem code with length $n = q$ and shorten it to a subsystem code with length $n = q-1$. These subsystem codes are all \mathbf{F}_{q^2} -linear. Therefore they satisfy $k + r = n - 2d + 2$. As a consequence the subsystem codes in Lemma 12 are optimal. The subsystem codes that we derive are not necessarily cyclic. In order to derive cyclic codes we need to make further restrictions on the codes. The following lemma gives an explicit construction for cyclic subsystem codes based on the Reed-Solomon codes over \mathbf{F}_q .

Lemma 13. *Let q be a prime power, and $n = q-1$, $2 \leq \delta < (q-1)/2$ and $T \subseteq \{0\} \cup \{\delta, \dots, n-\delta\}$. Let $C \subseteq \mathbf{F}_q^n$ be a cyclic code with the defining set $T_C = \{0, 1, \dots, n-\delta\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then there exists a cyclic subsystem RS code with the parameters $[[n, n-2\delta+2-r, r, \geq \delta]]_q$, where $0 \leq r = |T \cup T^{-1}| < n-2(\delta+1)$.*

Proof: We divide the proof to the following parts

- i) We know that if $2 \leq \delta < (q-1)/2$, then there exists classical cyclic code D^\perp that contains its dual code D , i.e., $D \subseteq D^\perp$. The code D^\perp has defining set $T_{D^\perp} = \{1, 2, \dots, \delta-1\}$. Therefore the defining set of D is given by $T_D = \{0\} \cup \{1, \dots, n-\delta\}$ and $D = C \cap D^\perp$. Also, $\dim D^\perp = n - (\delta-1)$ and $\dim D = \delta-1$.
- ii) Let $T \subseteq T_D$ be a nonempty set and $T^{-1} = \{-t \bmod n \mid t \in T\}$. Let $C \subseteq \mathbf{F}_q^n$ be a cyclic code with the defining set $T_C = T_D \setminus (T \cup T^{-1})$. We can actually compute the

defining set of the dual code C^\perp as $T_{C^\perp} = T_{D^\perp} \cup T \cup T^{-1}$. We notice that $T_C \cup T_{C^\perp} = \{1, 2, \dots, n-\delta\} \cup \{0\} = T_D$. Let $k = \delta-1$ and $0 \leq r = |T \cup T^{-1}| < n-2k$.

- iii) From steps (i), (ii) and by using Lemma 2, there is a subsystem code with $[[n, k, r, \geq \delta]]_q$, where $k = n-2\delta+2-r$ and $0 \leq r = |T \cup T^{-1}| < n-2(\delta-1)$. ■

Also, cyclic subsystem codes, based on RS codes over \mathbf{F}_{q^2} , can be derived as shown in the following lemma. Some codes are shown in Table III.

Lemma 14. *Let q be a prime power, $n = q^2-1$, and $2 \leq \delta < (q-1)$. Let $T \subseteq \{0\} \cup \{q\delta, \dots, q(n-\delta)\}$ be a nonempty set. Let $C \subseteq \mathbf{F}_{q^2}^n$ be a cyclic code with the defining set $T_C = \{0, q, \dots, q(n-\delta)\} \setminus (T \cup T^{-q})$ where $T^{-q} = \{-qt \bmod n \mid t \in T\}$. Then there exists a cyclic subsystem RS code with the parameters $[[n, n-2(\delta-1)-r, r, \geq \delta]]_q$, where $0 \leq r = |T \cup T^{-q}| < n-2(\delta-1)$.*

Proof: The proof is a direct consequence as shown in the previous lemmas.

We know that if $2 \leq \delta < (q-1)$, then there exists a cyclic code D^\perp over \mathbf{F}_{q^2} that contains its dual code D . The code D^\perp has length n , and minimum distance δ . The defining set of the code D is given by $T_D = \{q, 2q, \dots, q(n-\delta)\} \cup \{0\}$

We just notice that the defining set of the dual code $C^{\perp h}$ is given by $T_{C^{\perp h}} = \{q, 2q, \dots, q(\delta-1)\} \cup T \cup T^{-q}$. Furthermore, $T_C \cup T_{C^{\perp h}} = \{q, 2q, \dots, q(n-\delta)\} \cup \{0\} = T_D$. Hence, $D \subseteq C$, $D \subseteq C^{\perp h}$, and $D = C \cap C^{\perp h}$. From Lemma 3, there must exist a cyclic subsystem RS code with parameters $[[n, k, r, \geq \delta]]_q$, where $k = n-2(\delta-1)-r$ and $0 \leq r = |T \cup T^{-q}| < n-2(\delta+1)$. ■

TABLE III
OPTIMAL PURE SUBSYSTEM CODES

Subsystem Codes	Parent Code (RS Code)
$[[8, 1, 5, 2]]_3$	$[8, 6, 3]_{3^2}$
$[[8, 4, 2, 2]]_3$	$[8, 3, 6]_{3^2}$
$[[8, 5, 1, 2]]_3$	$[8, 2, 7]_{3^2}$
$[[9, 1, 4, 3]]_3$	$[9, 6, 4]_{3^2}^\dagger, \delta = 3$
$[[9, 4, 1, 3]]_3$	$[9, 3, 7]_{3^2}^\dagger, \delta = 6$
$[[15, 1, 10, 3]]_4$	$[15, 12, 4]_{4^2}$
$[[15, 9, 2, 3]]_4$	$[15, 4, 12]_{4^2}$
$[[15, 10, 1, 3]]_4$	$[15, 3, 13]_{4^2}$
$[[16, 1, 9, 4]]_4$	$[16, 12, 5]_{4^2}^\dagger, \delta = 4$
$[[24, 1, 17, 4]]_5$	$[24, 20, 5]_{5^2}$
$[[24, 16, 2, 4]]_5$	$[24, 5, 20]_{5^2}$
$[[24, 17, 1, 4]]_5$	$[24, 4, 21]_{5^2}$
$[[24, 19, 1, 3]]_5$	$[24, 3, 22]_{5^2}$
$[[24, 21, 1, 2]]_5$	$[24, 2, 23]_{5^2}$
$[[23, 1, 18, 3]]_5$	$[23, 20, 4]_{5^2}^*, \delta = 5$
$[[23, 16, 3, 3]]_5$	$[23, 5, 19]_{5^2}^*, \delta = 20$
$[[48, 1, 37, 6]]_7$	$[48, 42, 7]_{7^2}$

* Punctured code
† Extended code

In table III we show various optimal subsystem codes derived from RS codes. Some of these codes have been derived by puncture existing subsystem codes. It is also possible to derive some optimal impure subsystem codes. For instance $[[9, 1, 4, 3]]_2$ is an optimal impure subsystem codes.

a) *Puncture Subsystem Codes:* The MDS subsystem codes constructed from RS codes can also be punctured to other subsystem codes. Recall that if there is a subsystem code with parameters $[[n, k, r, d]]_q$ then there is a subsystem code with parameters $[[n-1, k, r, \geq d-1]]_q$. This is known as the propagation rules of quantum code constructions.

We end up this section by presenting two examples to illustrate the previous construction.

Example 15. Let C be a RS code with length $n = q - 1 = 6$ over \mathbf{F}_q . Define $N = \{0, 1, 2, 3, 4, 5\}$. We can construct subsystem code from RS codes with parameters $[6, 4, 3]_7$. This code is a subcode-subfield in BCH codes with deigned distance $\delta = 3$. So, $T_{D^\perp} = \{1, 2\}$, $T_D = \{0, 1, 2, 3\}$, $T_C = \{1, 2, 3\}$ and $T_{C^\perp} = \{0, 1, 2\}$. We notice that $T_D = T_C \cup T_{C^\perp}$ and $\dim C = 3$, $\dim D = 2$ and $\dim D^\perp = 4$. So, we have $k=4-3=1$ and $r=3-2=1$. Consequently, there exists a subsystem code with parameters $[6, 1, 1, 3]$ over \mathbf{F}_7

The previous example shows the shortest subsystem codes with length $n = 6$. However, it is not necessarily that this code exists only over \mathbf{F}_7 . In fact, as we were able to show that there exists a subsystem code with length $n = 6$ over \mathbf{F}_3 .

Example 16. Let F_{13} be the finite field with $q = 13$ elements. Let D^\perp be the narrow-sense Reed-Solomon code of length $n = 12$ and designed distance $\delta = 5$ over F_{13} . So, D^\perp has defining set $T_{D^\perp} = \{1, 2, 3, 4\}$. Therefore, D^\perp is an MDS code with parameters $[12, 8, 5]$. The dual of D^\perp is a RS code D with defining set $T_D = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Also, D is an MDS code with parameters $[12, 4, 9]$. Clearly, from our construction,

$$D \subseteq D^\perp \iff T_{D^\perp} \subseteq T_D$$

Now, let us define the code C by choosing a defining set $T_C = \{1, 2, 3, 4, 7\}$. So, $D \subseteq C \iff T_C \subseteq T_D$. Also compute the defining set of C^\perp as $T_{C^\perp} = \{0, 1, 2, 3, 4, 6, 7\}$. So, $D \subseteq C^\perp \iff T_{C^\perp} \subseteq T_D$. We see from our construction of these codes that

$$C \cap C^\perp = D \iff T_C \cup T_{C^\perp} = T_D.$$

Hence, we can compute the parameters of the subsystem code as follows. The minimum distance is given by $d_{\min} = D^\perp \setminus C = 5$, dimension $k = \dim D^\perp - \dim C = 8 - 7 = 1$, and gauge qubits $r = \dim C - \dim D = 7 - 4 = 3$. Therefore, we have a subsystem code with parameters $[[12, 1, 3, 5]]$, which is also an MDS code obeying Singleton bound $k+r+2d = n+2$.

Actually, if we choose the defining set of C to be $T_C = \{1, 2, 3, 4, 6, 7\}$, then the defining set of C^\perp is $T_{C^\perp} = \{0, 1, 2, 3, 4, 7\}$, then we get a subsystem code with parameters $d_{\min} = D^\perp \setminus C = 5$, $k = \dim D^\perp - \dim C = 8 - 6 = 2$, $r = \dim C - \dim D = 6 - 4 = 2$. Therefore, we have a subsystem code with parameters $[[12, 2, 2, 5]]$, which is also an MDS code. Some of subsystem RS codes are listed in Table IV.

VI. TRADING DIMENSIONS OF SUBSYSTEM CODES

In this section we show how one can trade the dimensions of subsystem and co-subsystem to obtain new codes from a

TABLE IV
REED-SOLOMON(RS) SUBSYSTEM CODES

Subsystem Codes	Parent RS Code
$[[15, 1, 10, 3]]_4$	$[15, 12, 4]_{4^2}$
$[[15, 1, 8, 3]]_4$	$[15, 11, 5]_{4^2}$
$[[15, 1, 6, 3]]_4$	$[15, 10, 6]_{4^2}$
$[[15, 2, 5, 3]]_4$	$[15, 9, 7]_{4^2}$
$[[24, 1, 17, 4]]_5$	$[24, 20, 5]_{5^2}$
$[[24, 2, 10, 4]]_5$	$[24, 16, 9]_{5^2}$
$[[24, 4, 10, 4]]_5$	$[24, 15, 10]_{5^2}$
$[[24, 16, 2, 4]]_5$	$[24, 5, 20]_{5^2}$
$[[24, 17, 1, 4]]_5$	$[24, 4, 21]_{5^2}$
$[[24, 19, 1, 3]]_5$	$[24, 3, 22]_{5^2}$
$[[48, 1, 37, 6]]_7$	$[48, 42, 7]_{7^2}$
$[[48, 2, 26, 6]]_7$	$[48, 36, 13]_{7^2}$

given subsystem or stabilizer code. The results are obtained by exploiting the symplectic geometry of the space. A remarkable consequence is that nearly any stabilizer code yields a series of subsystem codes.

Our first result shows that one can decrease the dimension of the subsystem and increase at the same time the dimension of the co-subsystem while keeping or increasing the minimum distance of the subsystem code.

Theorem 17. Let q be a power of a prime p . If there exists an $((n, K, R, d))_q$ subsystem code with $K > p$ that is pure to d' , then there exists an $((n, K/p, pR, \geq d))_q$ subsystem code that is pure to $\min\{d, d'\}$. If a pure $((n, p, R, d))_q$ subsystem code exists, then there exists a $((n, 1, pR, d))_q$ subsystem code.

Proof: By definition, an $((n, K, R, d))_q$ Clifford subsystem code is associated with a classical additive code $C \subseteq \mathbf{F}_q^{2n}$ and its subcode $D = C \cap C^{\perp_s}$ such that $x = |C|$, $y = |D|$, $K = q^n/(xy)^{1/2}$, $R = (x/y)^{1/2}$, and $d = \text{swt}(D^{\perp_s} - C)$ if $C \neq D^{\perp_s}$, otherwise $d = \text{swt}(D^{\perp_s})$ if $D^{\perp_s} = C$.

We have $q = p^m$ for some positive integer m . Since K and R are positive integers, we have $x = p^{s+2r}$ and $y = p^s$ for some integers $r \geq 1$, and $s \geq 0$. There exists an \mathbf{F}_p -basis of C of the form

$$C = \text{span}_{\mathbf{F}_p} \{z_1, \dots, z_s, x_{s+1}, z_{s+1}, \dots, x_{s+r}, z_{s+r}\}$$

that can be extended to a symplectic basis $\{x_1, z_1, \dots, x_{nm}, z_{nm}\}$ of \mathbf{F}_q^{2n} , that is, $\langle x_k | x_\ell \rangle_s = 0$, $\langle z_k | z_\ell \rangle_s = 0$, $\langle x_k | z_\ell \rangle_s = \delta_{k,\ell}$ for all $1 \leq k, \ell \leq nm$, see [7, Theorem 8.10.1].

Define an additive code

$$C_m = \text{span}_{\mathbf{F}_p} \{z_1, \dots, z_s, x_{s+1}, z_{s+1}, \dots, x_{s+r+1}, z_{s+r+1}\}.$$

It follows that

$$C_m^{\perp_s} = \text{span}_{\mathbf{F}_p} \{z_1, \dots, z_s, x_{s+r+2}, z_{s+r+2}, \dots, x_{nm}, z_{nm}\}$$

and

$$D = C_m \cap C_m^{\perp_s} = \text{span}_{\mathbf{F}_p} \{z_1, \dots, z_s\}.$$

By definition, the code C is a subset of C_m .

The subsystem code defined by C_m has the parameters (n, K_m, R_m, d_m) , where $K_m = q^n/(p^{s+2r+2}p^s)^{1/2} = K/p$

Family	Stabilizer $[[n, k, d]]_q$	Subsystem $[[n, k - r, r, d]]_q, k > r \geq 0$
Short MDS	$[[n, n - 2d + 2, d]]_q$	$[[n, n - 2d + 2 - r, r, d]]_q$
Hermitian Hamming	$[[n, n - 2m, 3]]_q$	$m \geq 2, [[n, n - 2m - r, r, 3]]_q$
Euclidean Hamming	$[[n, n - 2m, 3]]_q$	$[[n, n - 2m - r, r, 3]]_q$
Melias	$[[n, n - 2m, \geq 3]]_q$	$[[n, n - 2m - r, r, \geq 3]]_q$
Euclidean BCH	$[[n, n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil, \geq \delta]]_q$	$[[n, n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil - r, r, \geq \delta]]_q$
Hermitian BCH	$[[n, n - 2m \lceil (\delta - 1)(1 - 1/q^2) \rceil, \geq \delta]]_q$	$[[n, n - 2m \lceil (\delta - 1)(1 - 1/q^2) \rceil - r, r, \geq \delta]]_q$
Punctured MDS	$[[q^2 - q\alpha, q^2 - q\alpha - 2\nu - 2, \nu + 2]]_q$	$[[q^2 - q\alpha, q^2 - q\alpha - 2\nu - 2 - r, r, \nu + 2]]_q$
Euclidean MDS	$[[n, n - 2d + 2]]_q$	$[[n, n - 2d + 2 - r, r]]_q$
Hermitian MDS	$[[q^2 - s, q^2 - s - 2d + 2, d]]_q$	$[[q^2 - s, q^2 - s - 2d + 2 - r, r, d]]_q$
Twisted	$[[q^r, q^r - r - 2, 3]]_q$	$[[q^r, q^r - r - 2 - r, r, 3]]_q$
Extended twisted	$[[q^2 + 1, q^2 - 3, 3]]_q$	$[[q^2 + 1, q^2 - 3 - r, r, 3]]_q$
Perfect	$[[n, n - s - 2, 3]]_q$ $[[n, n - s - 2, 3]]_q$	$[[n, n - s - 2 - r, r, 3]]_q$ $[[n, n - s - 2 - r, r, 3]]_q$

Fig. 4. Families of subsystem codes from stabilizer codes

and $R_m = (p^{s+2r+2}/p^s)^{1/2} = pR$. For the claims concerning minimum distance and purity, we distinguish two cases:

- (a) If $C_m \neq D^{\perp s}$, then $K > p$ and $d_m = \text{swt}(D^{\perp s} - C_m) \geq \text{swt}(D^{\perp s} - C) = d$. Since by hypothesis $\text{swt}(D^{\perp s} - C) = d$ and $\text{swt}(C) \geq d'$, and $D \subseteq C \subset C_m \subseteq D^{\perp s}$ by construction, we have $\text{swt}(C_m) \geq \min\{d, d'\}$; thus, the subsystem code is pure to $\min\{d, d'\}$.
- (b) If $C_m = D^{\perp s}$, then $K_m = 1 = K/p$, that is, $K = p$; it follows from the assumed purity that $d = \text{swt}(D^{\perp s} - C) = \text{swt}(D^{\perp s}) = d_m$.

This proves the claim. \blacksquare

Theorem 18. *Let q be a power of a prime p . If there exists an \mathbf{F}_q -linear $[[n, k, r, d]]_q$ subsystem code with $k > 1$ that is pure to d' , then there exists an \mathbf{F}_q -linear $[[n, k - 1, r + 1, \geq d]]_q$ subsystem code that is pure to $\min\{d, d'\}$. If a pure \mathbf{F}_q -linear $[[n, 1, r, d]]_q$ subsystem code exists, then there exists an \mathbf{F}_q -linear $[[n, 0, r + 1, d]]_q$ subsystem code.*

Replacing \mathbf{F}_p -bases by \mathbf{F}_q -bases in the proof of the previous theorem yields the following variation of the previous theorem for \mathbf{F}_q -linear subsystem codes.

Theorem 19. *Let q be a power of a prime p . If there exists a pure \mathbf{F}_q -linear $[[n, k, r, d]]_q$ subsystem code with $r > 0$, then there exists a pure \mathbf{F}_q -linear $[[n, k + 1, r - 1, d]]_q$ subsystem code.*

VII. PROPAGATION RULES

We derive propagation rules of subsystem code constructions.

Let $C_1 \leq \mathbf{F}_q^n$ and $C_2 \mathbf{F}_q^n$ be two classical codes defined over \mathbf{F}_q . The direct sum of C_1 and C_2 is a code $C \leq \mathbf{F}_q^{2n}$ defined as follows

$$C = C_1 \oplus C_2 = \{uv \mid u \in C_1, v \in C_2\}. \quad (2)$$

In a matrix form the code C can be described as

$$C = \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix}$$

An $[[n, k_1, d_1]]_q$ classical code C_1 is a subcode in an $[[c, k_2, d_2]]_q$ if every codeword v in C_1 is also a codeword in

C_2 , hence $k_1 \leq k_2$. We say that an $[[n, k_1, r_1, d_1]]_q$ subsystem code Q_1 is a subcode in an $[[n, k_2, r_2, d_2]]_q$ subsystem code Q_2 if every codeword $|v\rangle$ in Q_1 is also a codeword in Q_2 and $k_1 + r_1 \leq k_2 + r_1$.

Notation. Let q be a power of a prime integer p . We denote by \mathbf{F}_q the finite field with q elements. We use the notation $(x|y) = (x_1, \dots, x_n | y_1, \dots, y_n)$ to denote the concatenation of two vectors x and y in \mathbf{F}_q^n . The symplectic weight of $(x|y) \in \mathbf{F}_q^{2n}$ is defined as

$$\text{swt}(x|y) = \{(x_i, y_i) \neq (0, 0) \mid 1 \leq i \leq n\}.$$

We define $\text{swt}(X) = \min\{\text{swt}(x) \mid x \in X, x \neq 0\}$ for any nonempty subset $X \neq \{0\}$ of \mathbf{F}_q^{2n} .

The trace-symplectic product of two vectors $u = (a|b)$ and $v = (a'|b')$ in \mathbf{F}_q^{2n} is defined as

$$\langle u|v \rangle_s = \text{tr}_{q/p}(a' \cdot b - a \cdot b'),$$

where $x \cdot y$ denotes the dot product and $\text{tr}_{q/p}$ denotes the trace from \mathbf{F}_q to the subfield \mathbf{F}_p . The trace-symplectic dual of a code $C \subseteq \mathbf{F}_q^{2n}$ is defined as

$$C^{\perp_s} = \{v \in \mathbf{F}_q^{2n} \mid \langle v|w \rangle_s = 0 \text{ for all } w \in C\}.$$

We define the Euclidean inner product $\langle x|y \rangle = \sum_{i=1}^n x_i y_i$ and the Euclidean dual of $C \subseteq \mathbf{F}_q^n$ as

$$C^{\perp} = \{x \in \mathbf{F}_q^n \mid \langle x|y \rangle = 0 \text{ for all } y \in C\}.$$

We also define the Hermitian inner product for vectors x, y in $\mathbf{F}_{q^2}^n$ as $\langle x|y \rangle_h = \sum_{i=1}^n x_i^q y_i$ and the Hermitian dual of $C \subseteq \mathbf{F}_{q^2}^n$ as

$$C^{\perp_h} = \{x \in \mathbf{F}_{q^2}^n \mid \langle x|y \rangle_h = 0 \text{ for all } y \in C\}.$$

Theorem 20. *Let C be a classical additive subcode of \mathbf{F}_q^{2n} such that $C \neq \{0\}$ and let D denote its subcode $D = C \cap C^{\perp_s}$. If $x = |C|$ and $y = |D|$, then there exists a subsystem code $Q = A \otimes B$ such that*

- i) $\dim A = q^n / (xy)^{1/2}$,
- ii) $\dim B = (x/y)^{1/2}$.

The minimum distance of subsystem A is given by

- (a) $d = \text{swt}((C + C^{\perp_s}) - C) = \text{swt}(D^{\perp_s} - C)$ if $D^{\perp_s} \neq C$;
- (b) $d = \text{swt}(D^{\perp_s})$ if $D^{\perp_s} = C$.

Thus, the subsystem A can detect all errors in E of weight less than d , and can correct all errors in E of weight $\leq \lfloor (d-1)/2 \rfloor$.

Extending Subsystem Codes. We derive new subsystem codes from known ones by extending and shortening the length of the code.

Theorem 21. *If there exists an $((n, K, R, d))_q$ Clifford subsystem code with $K > 1$, then there exists an $((n+1, K, R, \geq d))_q$ subsystem code that is pure to 1.*

Proof: We first note that for any additive subcode $X \leq \mathbf{F}_q^{2n}$, we can define an additive code $X' \leq \mathbf{F}_q^{2n+2}$ by

$$X' = \{(a\alpha|b0) \mid (a|b) \in X, \alpha \in \mathbf{F}_q\}.$$

We have $|X'| = q|X|$. Furthermore, if $(c|e) \in X^{\perp_s}$, then $(c\alpha|e0)$ is contained in $(X')^{\perp_s}$ for all α in \mathbf{F}_q , whence $(X^{\perp_s})' \subseteq (X')^{\perp_s}$. By comparing cardinalities we find that equality must hold; in other words, we have

$$(X^{\perp_s})' = (X')^{\perp_s}.$$

By Theorem 20, there are two additive codes C and D associated with an $((n, K, R, d))_q$ Clifford subsystem code such that

$$|C| = q^n R/K$$

and

$$|D| = |C \cap C^{\perp_s}| = q^n / (KR).$$

We can derive from the code C two new additive codes of length $2n+2$ over \mathbf{F}_q , namely C' and $D' = C' \cap (C')^{\perp_s}$. The codes C' and D' determine a $((n+1, K', R', d'))_q$ Clifford subsystem code. Since

$$\begin{aligned} D' &= C' \cap (C')^{\perp_s} = C' \cap (C^{\perp_s})' \\ &= (C \cap C^{\perp_s})', \end{aligned}$$

we have $|D'| = q|D|$. Furthermore, we have $|C'| = q|C|$. It follows from Theorem 20 that

- (i) $K' = q^{n+1} / \sqrt{|C'| |D'|} = q^n / \sqrt{|C| |D|} = K$,
- (ii) $R' = (|C'| / |D'|)^{1/2} = (|C| / |D|)^{1/2} = R$,
- (iii) $d' = \text{swt}((D')^{\perp_s} \setminus C') \geq \text{swt}((D^{\perp_s} \setminus C)') = d$.

Since C' contains a vector $(0\alpha|00)$ of weight 1, the resulting subsystem code is pure to 1. ■

Corollary 22. *If there exists an $[[n, k, r, d]]_q$ subsystem code with $k > 0$ and $0 \leq r < k$, then there exists an $[[n+1, k, r, \geq d]]_q$ subsystem code that is pure to 1.*

Shortening Subsystem Codes. We can also shorten the length of a subsystem code and still trade the dimensions of the new subsystem code and its co-subsystem code as shown in the following Lemma.

Theorem 23. *If an $((n, K, R, d))_q$ pure subsystem code Q exists, then there is a pure subsystem code Q_p with parameters $((n-1, qK, R, \geq d-1))_q$.*

Proof: We know that existence of the pure subsystem code Q with parameters $((n, K, R, d))_q$ implies existence of a pure stabilizer code with parameters $((n, KR, \geq d))_q$ for $n \geq 2$ and $d \geq 2$ from [1, Theorem 2.]. By [12, Theorem 70], there

exist a pure stabilizer code with parameters $((n-1, qKR, \geq d-1))_q$. This stabilizer code can be seen as $((n-1, qKR, 0, \geq d-1))_q$ subsystem code. By using [1, Theorem 2.], there exists a pure \mathbf{F}_q -linear subsystem code with parameters $((n-1, qK, R, \geq d-1))_q$ that proves the claim. ■

Analogue of the previous Theorem is the following Lemma.

Lemma 24. *If an \mathbf{F}_q -linear $[[n, k, r, d]]_q$ pure subsystem code Q exists, then there is a pure subsystem code Q_p with parameters $[[n-1, k+1, r, \geq d-1]]_q$.*

Proof: We know that existence of the pure subsystem code Q implies existence of a pure stabilizer code with parameters $[[n, k+r, \geq d]]_q$ for $n \geq 2$ and $d \geq 2$ by using [1, Theorem 2. and Theorem 5.]. By [12, Theorem 70], there exist a pure stabilizer code with parameters $[[n-1, k+r+1, \geq d-1]]_q$. This stabilizer code can be seen as an $[[n-1, k+r+1, 0, \geq d-1]]_q$ subsystem code. By using [1, Theorem 3.], there exists a pure \mathbf{F}_q -linear subsystem code with parameters $[[n-1, k+1, r, \geq d-1]]_q$ that proves the claim. ■

We can also prove the previous Theorem by defining a new code C_p from the code C as follows.

Theorem 25. *If there exists a pure subsystem code $Q = A \otimes B$ with parameters $((n, K, R, d))_q$ with $n \geq 2$ and $d \geq 2$, then there is a subsystem code Q_p with parameters $((n-1, K, qR, \geq d-1))_q$.*

Proof: By Theorem 20, if an $((n, K, R, d))_q$ subsystem code Q exists for $K > 1$ and $1 \leq R < K$, then there exists an additive code $C \in \mathbf{F}_q^{2n}$ and its subcode $D \leq \mathbf{F}_q^{2n}$ such that $|C| = q^n R/K$ and $|D| = |C \cap C^{\perp_s}| = q^n / KR$. Furthermore, $d = \min \text{swt}(D^{\perp_s} \setminus C)$. Let $w = (w_1, w_2, \dots, w_n)$ and $u = (u_1, u_2, \dots, u_n)$ be two vectors in \mathbf{F}_q^n . W.l.g., we can assume that the code D^{\perp_s} is defined as

$$D^{\perp_s} = \{(u|w) \in \mathbf{F}_q^{2n} \mid w, u \in \mathbf{F}_q^n\}.$$

Let $w_{-1} = (w_1, w_2, \dots, w_{n-1})$ and $u_{-1} = (u_1, u_2, \dots, u_{n-1})$ be two vectors in \mathbf{F}_q^{n-1} . Also, let $D_p^{\perp_s}$ be the code obtained by puncturing the first coordinate of D^{\perp_s} , hence

$$D_p^{\perp_s} = \{(u_{-1}|w_{-1}) \in \mathbf{F}_q^{2n-2} \mid w_{-1}, u_{-1} \in \mathbf{F}_q^{n-1}\}.$$

since the minimum distance of D^{\perp_s} is at least 2, it follows that $|D_p^{\perp_s}| = |D^{\perp_s}| = K^2 |C| = K^2 q^n R/K = q^n RK$ and the minimum distance of $D_p^{\perp_s}$ is at least $d-1$. Now, let us construct the dual code of $D_p^{\perp_s}$ as follows.

$$\begin{aligned} (D_p^{\perp_s})^{\perp_s} &= \{(u_{-1}|w_{-1}) \in \mathbf{F}_q^{2n-2} \mid \\ &\quad (0u_{-1}|0w_{-1}) \in D, w_{-1}, u_{-1} \in \mathbf{F}_q^{n-1}\}. \end{aligned}$$

Furthermore, if $(u_{-1}|w_{-1}) \in D_p$, then $(0u_{-1}|0w_{-1}) \in D$. Therefore, D_p is a self-orthogonal code and it has size given by

$$|D_p| = q^{2n-2} / |D_p^{\perp_s}| = q^{n-2} / RK.$$

We can also puncture the code C to the code C_p at the first coordinate, hence

$$\begin{aligned} C_p &= \{(u_{-1}|w_{-1}) \in \mathbf{F}_q^{2n-2} \mid w_{-1}, u_{-1} \in \mathbf{F}_q^{n-1}, \\ &\quad (aw_{-1}|bu_{-1}) \in C, a, b \in \mathbf{F}_q\}. \end{aligned}$$

Clearly, $D \subseteq C$ and if $a = b = 0$, then the vector $(0u_{-1}|0w_{-1}) \in D$, therefore, $(u_{-1}, w_{-1}) \in D_p$. This gives us that $D_p \subseteq C_p$. Furthermore, hence $|C| = |C_p|$. The dual code $C_p^{\perp_s}$ can be defined as

$$C_p^{\perp_s} = \{(u_{-1}|w_{-1}) \in \mathbf{F}_q^{2n-2} \mid w_{-1}, u_{-1} \in \mathbf{F}_q^{n-1}, \\ (ew_{-1}|fu_{-1}) \in C^{\perp_s}, e, f \in \mathbf{F}_q\}.$$

Also, if $e = f = 0$, then $D_p \subseteq C_p^{\perp_s}$, furthermore,

$$D_p^{\perp_s} = C_p \cup C_p^{\perp_s} = \{(u_{-1}|w_{-1}) \in \mathbf{F}_q^{2n-2} \mid \\ (0u_{-1}|0w_{-1}) \in D\} \quad (3)$$

$$(4)$$

Therefore there exists a subsystem code $Q_p = A_p \otimes B_p$. Also, the code $D_p^{\perp_s}$ is pure and has minimum distance at least $d - 1$. We can proceed and compute the dimension of subsystem A_p and co-subsystem B_p from Theorem 20 as follows.

- (i) $K_p = \frac{q^{n-1}/\sqrt{|C_p||D_p|}}{q^{n-1}/\sqrt{(q^n R/K)(q^{n-2}/RK)}} = K$,
- (ii) $R_p = (|C_p|/|D_p|)^{1/2} = ((q^n R/K)/(q^{n-2}/RK))^{1/2} = qR$,
- (iii) $d_p = \text{swt}((D_p)^{\perp_s} \setminus C_p) = \text{swt}((D^{\perp_s} \setminus C_p)) \geq d - 1$.

Therefore, there exists a subsystem code with parameters $((n - 1, K, qR, \geq d - 1))_q$.

The minimum distance condition follows since the code Q has $d = \min \text{swt}(D^{\perp_s} \setminus C)$ and the code Q_p has minimum distance as Q reduced by one. So, the minimum weight of $D_p^{\perp_s} \setminus C_p$ is at least the minimum weight of $(D^{\perp_s} \setminus C) - 1$

$$d_p = \min \text{swt}(D_p^{\perp_s} \setminus C_p) \\ \geq \min \text{swt}(D^{\perp_s} \setminus C) - 1 = d - 1$$

If the code Q is pure, then $\min \text{swt}(D^{\perp_s}) = d$, therefore, the new code Q_p is pure since $d_p = \min \text{swt}(D_p^{\perp_s}) \geq d$.

We conclude that if there is a subsystem code with parameters $((n - 1, K, qR, \geq d - 1))_q$, using [1, Theorem 2.], there exists a code with parameters $((n - 1, qK, R, \geq d - 1))_q$. ■

Reducing Dimension. We also can reduce dimension of the subsystem code for fixed length n and minimum distance d , and still obtain a new subsystem code with improved minimum distance as shown in the following results.

Theorem 26. *If a (pure) \mathbf{F}_q -linear $[[n, k, r, d]]_q$ subsystem code Q exists for $d \geq 2$, then there exists an \mathbf{F}_q -linear $[[n, k - 1, r, d_e]]_q$ subsystem code Q_e (pure to d) such that $d_e \geq d$.*

Proof: Existence of the $[[n, k, r, d]]_q$ subsystem code Q , implies existence of two additive codes $C \leq \mathbf{F}_q^{2n}$ and $D \leq \mathbf{F}_q^{2n}$ such that $|C| = q^{n-k+r}$ and $|D| = |C \cap C^{\perp_s}| = q^{n-k-r}$. Furthermore, $d = \min \text{swt}(D^{\perp_s} \setminus C)$ and $D \subseteq D^{\perp_s}$.

The idea of the proof comes by extending the code D by some vectors from $D^{\perp_s} \setminus (C \cup C^{\perp_s})$. Let us choose a code D_e of size $|q^{n+1-r-k}| = q|D|$. We also ensure that the code D_e is self-orthogonal. Clearly extending the code D to D_e will extend both the codes C and C^{\perp_s} to C_e and $C_e^{\perp_s}$, respectively. Hence $C_e = q|C| = q^{n+1+r-k}$ and $D_e = C_e \cap C_e^{\perp_s}$.

There exists a subsystem code Q_e stabilized by the code C_e . The result follows by computing parameters of the subsystem code $Q_e = A_e \otimes B_e$.

- (i) $K_e = \frac{q^n/\sqrt{|C_e||D_e|}}{q^n/((q^{n+1+r-k})(q^{n+1-k-r}))^{1/2}} = q^{k-1}$,
- (ii) $R_e = \frac{(|C_e|/|D_e|)^{1/2}}{((q^{n+1}R/K)/(q^{n+1}/RK))^{1/2}} = q^r$,
- (iii) $d_e = \text{swt}((D_e)^{\perp_s} \setminus C_e) \geq \text{swt}((D^{\perp_s} \setminus C_e)) = d$. If the inequality holds, then the code is pure to d .

Arguably, It follows that the set $(D_e^{\perp_s} \setminus C_e)$ is a subset of the set $D^{\perp_s} \setminus C$ because $C \leq C_e$, hence the minimum weight d_e is at least d . ■

Lemma 27. *Suppose an $[[n, k, r, d]]_q$ linear pure subsystem code Q exists generated by the two codes $C, D \leq \mathbf{F}_q^{2n}$. Then there exist linear $[[n - m, k', r', d']]_q$ and $[[n - m, k' + r' - r'', r'', d'']]_q$ subsystem codes with $k' \geq k - m$, $r' \geq r$, $0 \leq r'' < k' + r'$, and $d' \geq d$ for any integer m such that there exists a codeword of weight m in $(D^{\perp_s} \setminus C)$.*

Proof: [Sketch] This lemma 27 can be proved easily by mapping the subsystem code Q into a stabilizer code. By using [6, Theorem 7.], and the new resulting stabilizer code can be mapped again to a subsystem code with the required parameters. ■

Combining Subsystem Codes We can also construct new subsystem codes from given two subsystem codes. The following theorem shows that two subsystem codes can be merged together into one subsystem code with possibly improved distance or dimension.

Theorem 28. *Let Q_1 and Q_2 be two pure subsystem codes with parameters $[[n_1, k_1, r_1, d_1]]_2$ and $[[n_2, k_2, r_2, d_2]]_2$ for $k_2 + r_2 \leq n_1$, respectively. Then there exists a subsystem code with parameters $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1 - r, r, d]]_2$, where $d \geq \min\{d_1, d_1 + d_2 - k_2 - r_2\}$ and $0 \leq r < k_1 + r_1$.*

Proof: Existence of an $[[n_i, k_i, r_i, d_i]]_2$ pure subsystem code Q_i for $i \in \{1, 2\}$, implies existence of a pure stabilizer code S_i with parameters $[[n_i, k_i + r_i, d_i]]_2$ with $k_2 + r_2 \leq n_1$, see [1]. Therefore, by [6, Theorem 8.], there exists a stabilizer code with parameters $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1, d]]_2$, $d \geq \min\{d_1, d_1 + d_2 - k_2 - r_2\}$. But this code gives us a subsystem code with parameters $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1 - r, r, \geq d]]_2$ with $k_2 + r_2 \leq n_1$ and $0 \leq r < k_1 + r_1$ that proves the claim. ■

Theorem 29. *Let Q_1 and Q_2 be two pure subsystem codes with parameters $[[n, k_1, r_1, d_1]]_q$ and $[[n, k_2, r_2, d_2]]_q$, respectively. If $Q_2 \subseteq Q_1$, then there exists an $[[2n, k_1 + k_2 + r_1 + r_2 - r, r, d]]_q$ pure subsystem code with minimum distance $d \geq \min\{d_1, 2d_2\}$ and $0 \leq r < k_1 + k_2 + r_1 + r_2$.*

Proof: Existence of a pure subsystem code with parameters $[[n, k_i, r_i, d_i]]_q$ implies existence of a pure stabilizer code with parameters $[[n, k_i + r_i, d_i]]_q$ using [1, Theorem 4.]. But by using [12, Lemma 74.], there exists a pure stabilizer code with parameters $[[2n, k_1 + k_2 + r_1 + r_2, d]]_q$ with $d \geq \min\{2d_2, d_1\}$. By [1, Theorem 2., Corollary 6.], there must exist a pure subsystem code with parameters $[[2n, k_1 + k_2 + r_1 + r_2 - r, r, d]]_q$ where $d \geq \min\{2d_2, d_1\}$ and $0 \leq r < k_1 + k_2 + r_1 + r_2$, which proves the claim. ■

We can recall the trace alternative product between two codewords of a classical code and the proof of Theorem 29

can be stated as follows.

Lemma 30. *Let Q_1 and Q_2 be two pure subsystem codes with parameters $[[n, k_1, r_1, d_1]]_q$ and $[[n, k_2, r_2, d_2]]_q$, respectively. If $Q_2 \subseteq Q_1$, then there exists an $[[2n, k_1+k_2, r_1+r_2, d]]_q$ pure subsystem code with minimum distance $d \geq \min\{d_1, 2d_2\}$.*

Proof: Existence of the code Q_i with parameters $[[n, K_i, R_i, d_i]]_q$ implies existence of two additive codes C_i and D_i for $i \in \{1, 2\}$ such that $|C_i| = q^n R_i / K_i$ and $|D_i| = |C \cup C^{\perp_s}| = q^n / R_i K_i$.

We know that there exist additive linear codes $D_i \subseteq D_i^{\perp_a}$, $D_i \subseteq C_i$, and $D_i \subseteq C_i^{\perp_a}$. Furthermore, $D_i = C_i \cap C_i^{\perp_a}$ and $d_i = wt(D_i^{\perp_a} \setminus C_i)$. Also, $C_i = q^{n+r_i-k_i}$ and $|D_i| = q^{n-r_i-k_i}$.

Using the direct sum definition between to linear codes, let us construct a code D based on D_1 and D_2 as

$$D = \{(u, u+v) \mid u \in D_1, v \in D_2\} \leq \mathbf{F}_q^{2n}.$$

The code D has size of $|D| = q^{2n-(r_1+r_2+k_1+k_2)=|D_1||D_2|}$. Also, we can define the code C based on the codes C_1 and C_2 as

$$C = \{(a, a+b) \mid a \in C_1, b \in C_2\} \leq \mathbf{F}_q^{2n}.$$

The code C is of size $|C| = |C_1||C_2| = q^{2n+r_1+r_2-k_1-k_2}$. But the trace-alternating dual of the code D is

$$D^{\perp_a} = \{(u' + v', v') \mid u' \in D_1^{\perp_a}, v' \in D_2^{\perp_a}\}.$$

We notice that $(u' + v', v')$ is orthogonal to $(u, u+v)$ because, from properties of the product,

$$\begin{aligned} \langle (u, u+v) \mid (u' + v', v') \rangle_a &= \langle u \mid u' + v' \rangle_a + \langle u+v \mid v' \rangle_a \\ &= 0 \end{aligned}$$

holds for $u \in D_1, v \in D_2, u' \in D_1^{\perp_a}$, and $v' \in D_2^{\perp_a}$.

Therefore, $D \subseteq D^{\perp_a}$ is a self-orthogonal code with respect to the trace alternating product. Furthermore, $C^{\perp_a} = \{(a' + b', b') \mid a' \in C_1^{\perp_a}, b' \in C_2^{\perp_a}\}$. Hence, $C \cap C^{\perp_a} = \{(a, a+b) \cap (aa + b', b')\} = D$. Therefore, there exists an \mathbf{F}_q -linear subsystem code $Q = A \otimes B$ with the following parameters.

i)

$$\begin{aligned} K &= |A| = q^{2n}/(|C||D|)^{1/2} \\ &= \frac{q^{2n}}{\sqrt{(q^{2n} R_1 R_2 / K_1 K_2)(q^{2n} / K_1 K_2 R_1 R_2)}} \\ &= \frac{q^{2n}}{\sqrt{q^{2n+r_1+r_2-k_1-k_2} q^{2n-r_1-r_2-k_1-k_2}}} \\ &= q^{k_1 k_2} = K_1 K_2. \end{aligned}$$

ii) $R = \left(\frac{|C|}{|D|}\right)^{1/2} = R_1 R_2$.

iii) the minimum distance is a direct consequence. ■

Theorem 31. *If there exist two pure subsystem quantum codes Q_1 and Q_2 with parameters $[[n_1, k_1, r_1, d_1]]_q$ and $[[n_2, k_2, r_2, d_2]]_q$, respectively. Then there exists a pure subsystem code Q' with parameters $[[n_1+n_2, k_1+k_2+r_1+r_2-r, r, \geq \min(d_1, d_2)]]_q$.*

Proof: This Lemma can be proved easily from [1, Theorem 5.] and [12, Lemma 73.]. The idea is to map a pure subsystem code to a pure stabilizer code, and once again map the pure stabilizer code to a pure subsystem code. ■

Theorem 32. *If there exist two pure subsystem quantum codes Q_1 and Q_2 with parameters $[[n_1, k_1, r_1, d_1]]_q$ and $[[n_2, k_2, r_2, d_2]]_q$, respectively. Then there exists a pure subsystem code Q' with parameters $[[n_1+n_2, k_1+k_2, r_1+r_2, \geq \min(d_1, d_2)]]_q$.*

Proof: Existence of the code Q_i with parameters $[[n, K_i, R_i, d_i]]_q$ implies existence of two additive codes C_i and D_i for $i \in \{1, 2\}$ such that $|C_i| = q^n R_i / K_i$ and $|D_i| = |C \cup C^{\perp_s}| = q^n / R_i K_i$.

Let us choose the codes C and D as follows.

$$C = C_1 \oplus C_2 = \{uv \mid v \in C_1, v \in C_2\},$$

and

$$D = D_1 \oplus D_2 = \{ab \mid a \in D_1, b \in D_2\},$$

respectively. From this construction, and since D_1 and D_2 are self-orthogonal codes, it follows that D is also a self-orthogonal code. Furthermore, $D_1 \subseteq C_1$ and $D_2 \subseteq C_2$, then

$$D_1 \oplus D_2 \subseteq C_1 \oplus C_2,$$

hence $D \subseteq C$. The code C is of size

$$\begin{aligned} |C| &= |C_1||C_2| = q^{(n_1+n_2)-(k_1+k_2)+(r_1+r_2)} \\ &= q^{n_1} q^{n_2} R_1 R_2 / K_1 K_2 \end{aligned}$$

and D is of size

$$\begin{aligned} |D| &= |D_1||D_2| = q^{(n_1+n_2)-(k_1+k_2)-(r_1+r_2)} \\ &= q^{n_1} q^{n_2} / R_1 R_2 K_1 K_2. \end{aligned}$$

On the other hand,

$$C^{\perp_s} = (C_1 \oplus C_2)^{\perp_s} = C_2^{\perp_s} \oplus C_1^{\perp_s} \supseteq D_2 \oplus D_1.$$

Furthermore, $C \cap C^{\perp_s} = (C_1 \oplus C_2) \cap (C_2^{\perp_s} \cap C_1^{\perp_s}) = D$.

Therefore, there exists a subsystem code $Q = A \otimes B$ with the following parameters.

i)

$$\begin{aligned} K &= |A| = q^{n_1+n_2}/(|C||D|)^{1/2} \\ &= \frac{q^{n_1+n_2}}{\sqrt{(q^{n_1+n_2} R_1 R_2 / K_1 K_2)(q^{n_1+n_2} / K_1 K_2 R_1 R_2)}} \\ &= \frac{q^{n_1+n_2}}{\sqrt{q^{n_1+n_2+r_1+r_2-k_1-k_2} q^{n_1+n_2-r_1-r_2-k_1-k_2}}} \\ &= q^{k_1 k_2} = K_1 K_2 = |A_1||A_2|. \end{aligned}$$

ii)

$$\begin{aligned} R &= \left(\frac{|C|}{|D|}\right)^{1/2} = \sqrt{\frac{q^{n_1} q^{n_2} R_1 R_2 / K_1 K_2}{q^{n_1} q^{n_2} / R_1 R_2 K_1 K_2}} \\ &= R_1 R_2 = |B_1||B_2|. \end{aligned}$$

iii) the minimum weight of $D_1^{\perp s} \setminus C$ is at least the minimum weight of $D_1^{\perp s} \setminus C_1$ or $D_2^{\perp s} \setminus C_2$.

$$\begin{aligned} d &= \min\{\text{swt}(D_1^{\perp s} \setminus C_1), (D_2^{\perp s} \setminus C_2)\} \\ &\geq \min\{d_1, d_2\}. \end{aligned}$$

Theorem 33. *Given two pure subsystem codes Q_1 and Q_2 with parameters $[[n_1, k_1, r_1, d_1]]_q$ and $[[n_2, k_2, r_2, d_2]]_q$, respectively, with $k_2 \leq n_1$. An $[[n_1 + n_2 - k_2, k_1 + r_1 + r_2 - r, r, d]]_q$ subsystem code exists such that $d \geq \min\{d_1, d_1 + d_2 - k_2\}$ and $0 \leq r < k_1 + r_1 + r_2$.*

Proof: The proof is a direct consequence as shown in the previous theorems. ■

Theorem 34. *If an $((n, K, R, d))_{q^m}$ pure subsystem code exists, then there exists a pure subsystem code with parameters $((nm, K, R, \geq d))_q$. Consequently, if a pure subsystem code with parameters $((nm, K, R, \geq d))_q$ exists, then there exist a subsystem code with parameters $((n, K, R, \geq \lfloor d/m \rfloor))_{q^m}$.*

Proof: Existence of a pure subsystem code with parameters $((n, K, R, d))_{q^m}$ implies existence of a pure stabilizer code with parameters $((n, KR, d))_{q^m}$ using [1, Theorem 5.]. By [12, Lemma 76.], there exists a stabilizer code with parameters $((nm, KR, \geq d))_q$. From [1, Theorem 2,5.], there exists a pure subsystem code with parameters $((nm, K, R, \geq d))_q$ that proves the first claim. By [12, Lemma 76.] and [1, Theorem 2,5.], and repeating the same proof, the second claim is a consequence. ■

$n \setminus k$	$k-1$	k	$k+1$
$n-1$	$[r, \leq d]_q$	$[\leq r-1, d]_q$	$[r, d-1]_q$
n	$[\geq r, d]_q, [r, \geq d]_q$	$[r, d]_q \rightarrow [\leq r, \geq d]_q$ $\rightarrow [\geq r, \leq d]_q$	$[\leq r, d]_q$
$n+1$	$[\geq r, \geq d]_q$	$[\geq r, d]_q, [r, \geq d]_q$	

TABLE V
EXISTENCE OF SUBSYSTEM PROPAGATION RULES

VIII. TABLES OF UPPER BOUNDS

In this section we investigate tables of upper bounds on subsystem code parameters.

IX. SPECIAL AND SHORT SUBSYSTEM CODES $[[8, 1, 2, 3]]_2$ AND $[[6, 1, 1, 3]]_3$

In this section we present the shortest subsystem codes over \mathbf{F}_2 and \mathbf{F}_3 fields. Corollary ?? implies that a stabilizer code with parameters $[[n, k, d]]_q$ gives subsystem codes with parameters $[[n, k-r, r, d]]_q$, see Tables II, III, IV, 4.

Consider a stabilizer code with parameters $[[8, 3, 3]]_2$. This code can be used to derive $[[8, 2, 1, 3]]_2$ and $[[8, 1, 2, 3]]_2$ subsystem codes. We give an explicit construction of these codes. Further, we claim that $[[8, 1, 2, 3]]_2$ and $[[8, 2, 1, 3]]_2$ are the shortest nontrivial binary subsystem codes. We obtain these codes using MAGMA computer algebra search. It remains to study properties of these codes and whether they have nice error correction capabilities. We show the stabilizer and

normalizer matrices for these codes. Also, we prove their minimum distances using the weight enumeration of these codes. It was known that the $[[9, 1, 4, 3]]_2$ Becan-Shor code is the shortest subsystem code constructed via graphs, in which it tolerates 4 gauge qubits. We present two codes with less length, however we can not tolerate more than 2 gauge qubits. The following example shows $[[8, 1, 2, 3]]$ short subsystem code over \mathbf{F}_2 .

Example 35.

$$D_S = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \end{bmatrix} \quad (5)$$

$$D_S^\perp = \begin{bmatrix} X & I & I & I & I & I & Z & Y \\ Y & I & I & I & I & Y & X & X \\ I & X & I & I & I & Y & Y & X \\ I & Y & I & I & I & I & X & Z \\ I & I & X & I & I & Y & Z & I \\ I & I & Y & I & I & I & Z & X \\ I & I & I & X & I & Y & I & Z \\ I & I & I & Y & I & Y & Y & Y \\ I & I & I & I & X & I & Y & Z \\ I & I & I & I & Y & Y & Z & Z \\ I & I & I & I & I & Z & X & Y \end{bmatrix} \quad (6)$$

$$C_S = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \\ \hline Y & I & I & I & I & Y & X & X \\ I & X & I & I & I & Y & Y & X \end{bmatrix} \quad (7)$$

$$C_S^\perp = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \\ \hline X & I & I & I & I & I & Z & Y \\ I & I & I & Y & I & Y & Y & Y \end{bmatrix} \quad (8)$$

We notice that the matrix D_S generates the code $D = C \cap C^{\perp s}$. Furthermore, dimensions of the subsystems A and B are given by $k = \dim D^{\perp s} - \dim C = (11 - 7)/2 = 2$ and $r = \dim C - \dim D = (7 - 5)/2 = 1$. Hence we have $[[8, 2, 1, 3]]_2$ and $[[8, 1, 2, 3]]_2$ subsystem codes.

We show that the subsystem codes $[[8, 1, 2, 3]]_2$ is not better than the stabilizer code $[[8, 3, 3]]_2$ in terms of syndrome measurement. The reason is that the former needs $8 - 1 - 2 = 5$ syndrome measurements, while the later needs also $8 - 3 = 5$ measurements. This is an obvious example where subsystem codes have no superiority in terms of syndrome measurements.

We post an open question regarding the threshold value and fault tolerant gate operations for this code. We do not know at this time if the code $[[8, 1, 2, 3]]_2$ has better threshold value

and less fault-tolerant operations. Also, does the subsystem code with parameters $[[8, 1, 3, 3]]_2$ exist?

No nontrivial $[[7, 1, 1, 3]]_2$ exists. There exists a trivial $[[7, 1, 1, 3]]_2$ code obtained by simply extending the $[[5, 1, 3]]_2$ code as the $[[5, 1, 3]]_2$ code. We show the smallest subsystem code with length 7 must have at most minimum weight equals to 2. Since $[[7, 2, 2]]_2$ exists, then we can construct the stabilizer and normalizer matrices as follows.

$$D_S = \begin{bmatrix} X & X & X & X & I & I & I \\ Y & Y & Y & Y & I & I & I \\ I & I & I & I & X & I & I \\ I & I & I & I & I & X & I \\ I & I & I & I & I & I & X \end{bmatrix} \quad (9)$$

$$D_S^\perp = \begin{bmatrix} X & I & I & X & I & I & I \\ Y & I & I & Y & I & I & I \\ I & X & I & X & I & I & I \\ I & Y & I & Y & I & I & I \\ I & I & X & X & I & I & I \\ I & I & Y & Y & I & I & I \\ I & I & I & I & X & I & I \\ I & I & I & I & I & X & I \\ I & I & I & I & I & I & X \end{bmatrix} \quad (10)$$

Clearly, from our construction and using Corollary ??, there must exist a subsystem code with parameters k and r given as follows. $\dim D^{\perp_s} = 9/2$ and $\dim C = 7/2$. Also, $\dim D = 5/2$ and $\min(D^{\perp_s} \setminus C) = 2$. Therefore, $k = (9 - 7)/2 = 1$ and $r = (7 - 5)/2 = 1$. Consequently, the parameters of the subsystem code are $[[7, 1, 1, 2]]_2$.

This example shows $[[6, 1, 1, 3]]$ short subsystem code over \mathbf{F}_3 .

Example 36. We give a nontrivial short subsystem code over \mathbf{F}_3 . This is derived from the $[[6, 2, 3]]_3$ graph quantum code, see [8] for existence results and [10] for a method to construct the code. Also, we showed an example earlier for an $[[6, 1, 1, 3]]$ subsystem code over \mathbf{F}_7 . Consider the field \mathbf{F}_3 and let $C \subseteq \mathbf{F}_3^{12}$ be a linear code defined by the following generator matrix.

$$C = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 & 0 & 2 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array} \right] = \left[\begin{array}{c} S \\ X_1 \\ Z_1 \end{array} \right]$$

Let the symplectic inner product $\langle (a|b)|(c|d) \rangle_s = a \cdot d - b \cdot c$. Then the symplectic dual of C is generated by

$$C^{\perp_s} = \left[\begin{array}{c} S \\ X_2 \\ Z_2 \end{array} \right],$$

where $X_2 = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 2 \ 0 \ 0 \ 0]$ and

$Z_2 = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1]$. The matrix S generates the code $D = C \cap C^{\perp_s}$. Now D defines a

$[[6, 2, 3]]_3$ stabilizer code [8, Theorem 3.1] and [10, Theorem 1 and Equation (15)]. Therefore, $\text{swt}(D^{\perp_s} \setminus D) = 3$. It follows that $\text{swt}(D^{\perp_s} \setminus C) \geq \text{swt}(D^{\perp_s}) = 3$. By [2, Theorem 4], we have a $[[6, (\dim D^{\perp_s} - \dim C)/2, (\dim C - \dim D)/2, 3]]_3$ viz. a $[[6, 1, 1, 3]]_3$ subsystem code.

We can also have a trivial $[[6, 1, 1, 3]]_2$ code. This trivial extension seems to argue against the usefulness of subsystem codes and if they will really lead to improvement in performance. An obvious open question is if there exist nontrivial $[[6, 1, 1, 3]]_2$ or $[[7, 1, 1, 3]]_2$ subsystem codes.

X. ACKNOWLEDGMENTS

"Sharing knowledge, in which we all born knowing nothing, is better than proving or canceling it. S.A.A."

REFERENCES

- [1] S. A. Aly and A. Klappenecker. Subsystem code constructions. In *Proc. 2008 IEEE International Symposium on Information Theory, Toronto, Canada*, Submitted, 2008.
- [2] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Subsystem codes. In *44th Annual Allerton Conference on Communication, Control, and Computing, Monticello, Illinois, September, 2006*, 2006.
- [3] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. *IEEE Trans. Inform. Theory*, 53(2):1183–1188, 2007.
- [4] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Primitive qutnum BCH codes over finite fields. In *Proc. 2006 IEEE International Symposium on Information Theory, Seattle, USA*, pages 1114 – 1118, July 2006.
- [5] D. Bacon. Operator quantum error correcting subsystems for self-correcting quantum memories. *Phys. Rev. A*, 73(012340), 2006.
- [6] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.
- [7] P.M. Cohn. *Basic Algebra – Groups, Rings, and Fields*. Springer, 2005.
- [8] K. Feng. Quantum codes $[[6, 2, 3]]_p$, $[[7, 3, 3]]_p$ ($p \geq 3$) exist. *IEEE Trans. Inform. Theory*, 48(8):2384–2391, 2002.
- [9] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *Internat. J. Quantum Information*, 2(1):757–775, 2004.
- [10] M. Grassl, A. Klappenecker, and M. Rötteler. Graphs, quadratic forms, and quantum codes. In *Proc. 2002 IEEE Intl. Symp. Inform. Theory, Lausanne, Switzerland*, page 45. IEEE, 2002.
- [11] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. University Press, Cambridge, 2003.
- [12] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.
- [13] A. Klappenecker and P. K. Sarvepalli. Clifford code constructions of operator quantum error correcting codes. arXiv:quant-ph/0604161, 2006.
- [14] E. Knill. Group representations, error bases and quantum codes. Los Alamos National Laboratory Report LAUR-96-2807, 1996.
- [15] E. Knill. On protected realizations of quantum information. Eprint: quant-ph/0603252, 2006.
- [16] D. W. Kribs, R. Laflamme, and D. Poulin. Unified and generalized approach to quantum error correction. *Phys. Rev. Lett.*, 94(180501), 2005.
- [17] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky. Operator quantum error correction. Eprint: quant-ph/0504189, 2005.
- [18] F. J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [19] D. Poulin. Stabilizer formalism for operator quantum error correction. *Phys. Rev. Lett.*, 95(230504), 2005.

TABLE VI. Upper bounds on subsystem code parameters using linear programming, $q = 2$

n/k	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
n=5	(3,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)								
n=6	(1,3), (4,2), (5,1)	(3,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)							
n=7	(3,3), (5,2), (6,1)	(4,2), (5,1)	(3,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)						
n=8	(4,3), (6,2), (7,1)	(3,3), (5,2), (6,1)	(4,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)					
n=9	(2,4), (6,3), (7,2), (8,1)	(4,3), (6,2), (7,1)	(2,3), (5,2), (6,1)	(4,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)				
n=10	(4,4), (7,3), (8,2), (9,1)	(2,4), (6,3), (7,2), (8,1)	(4,3), (6,2), (7,1)	(1,3), (5,2), (6,1)	(4,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)			
n=11	(2,5), (5,4), (8,3), (9,2), (10,1)	(4,4), (7,3), (8,2), (9,1)	(2,4), (5,3), (7,2), (8,1)	(3,3), (6,2), (7,1)	(1,3), (5,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)		
n=12	(3,5), (7,4), (9,3), (10,2), (11,1)	(1,5), (6,4), (8,3), (9,2), (10,1)	(4,4), (7,3), (8,2), (9,1)	(1,4), (5,3), (7,2), (8,1)	(3,3), (6,2), (7,1)	(1,3), (5,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)	
n=13	(1,6), (5,5), (8,4), (10,3), (11,2), (12,1)	(3,5), (7,4), (9,3), (10,2), (11,1)	(5,4), (8,3), (9,2), (10,1)	(3,4), (6,3), (8,2), (9,1)	(1,4), (4,3), (7,2), (8,1)	(3,3), (6,2), (7,1)	(5,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)
n=14	(3,6), (6,5), (9,4), (11,3), (12,2), (13,1)	(8,4), (10,3), (11,2), (12,1)	(6,4), (9,3), (10,2), (11,1)	(5,4), (7,3), (9,2), (10,1)	(3,4), (6,3), (8,2), (9,1)	(4,3), (7,2), (8,1)	(2,3), (6,2), (7,1)	(5,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)
n=15	(5,6), (8,5), (10,4), (12,3), (13,2), (14,1)	(3,6), (7,5), (9,4), (11,3), (12,2), (13,1)	(4,5), (8,4), (10,3), (11,2), (12,1)	(2,5), (6,4), (9,3), (10,2), (11,1)	(4,4), (7,3), (9,2), (10,1)	(2,4), (6,3), (8,2), (9,1)	(4,3), (7,2), (8,1)	(2,3), (6,2), (7,1)	(4,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)

TABLE VII. Upper bounds on subsystem code parameters using linear programming, $q = 3$

n/k	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
n=5	(3,2) (4,1)	(2,2) (3,1)	(2,1)									
n=6	(2,3) (4,2) (5,1)	(3,2) (4,1)	(1,2) (3,1)	(2,1)								
n=7	(4,3) (5,2) (4,1)	(2,3) (3,2) (4,1)	(2,2) (4,1)	(1,2) (3,1)	(2,1)							
n=8	(3,4) (5,3) (6,2) (5,1)	(2,3) (5,2) (5,1)	(2,3) (4,2) (5,1)	(3,2) (4,1)	(1,2) (3,1)	(2,1)	(1,1)					
n=9	(4,4) (6,3) (7,2) (6,1)	(2,4) (4,3) (6,2) (5,1)	(3,3) (5,2) (6,1)	(1,3) (4,2) (4,1)	(3,2) (4,1)	(1,2) (3,1)	(1,1)					
n=10	(3,5) (6,4) (7,3) (8,2) (9,1)	(4,4) (5,3) (7,2) (8,1)	(2,4) (5,3) (6,2) (7,1)	(3,3) (5,2) (6,1)	(1,3) (4,2) (5,1)	(2,2) (4,1)	(1,2) (3,1)	(2,1)	(1,1)			
n=11	(5,5) (7,4) (8,3) (9,2) (10,1)	(2,5) (6,4) (7,3) (8,2) (9,1)	(4,4) (6,3) (7,2) (7,1)	(1,4) (4,3) (6,2) (7,1)	(3,3) (5,2) (6,1)	(1,3) (4,2) (5,1)	(1,2) (4,1)	(1,2) (2,1)	(2,1)			
n=12	(3,6) (6,5) (8,4) (10,3) (8,2) (10,1)	(4,5) (7,4) (9,3) (6,2) (9,1)	(2,5) (5,4) (7,3) (8,2) (9,1)	(3,4) (6,3) (7,2) (8,1)	(1,4) (3,3) (6,2) (7,1)	(2,3) (5,2) (6,1)	(4,2) (5,1)	(2,2)	(1,2) (3,1)			