Subsystem Code Constructions

Salah A. Aly and Andreas Klappenecker
Department of Computer Science
Texas A&M University, College Station, TX 77843-3112, USA
Email: {salah, klappi}@cs.tamu.edu

***Abstract*—Subsystem codes are the most versatile class of quantum error-correcting codes known to date that combine the best features of all known passive and active error-control schemes. The subsystem code is a subspace of the quantum state space that is decomposed into a tensor product of two vector spaces: the subsystem and the co-subsystem. A generic method to derive subsystem codes from existing subsystem codes is given that allows one to trade the dimensions of subsystem and co-subsystem while maintaining or improving the minimum distance. As a consequence, it is shown that all pure MDS subsystem codes are derived from MDS stabilizer codes. The existence of numerous families of MDS subsystem codes is established. Propagation rules are derived that allow one to obtain longer and shorter subsystem codes from given subsystem codes. Furthermore, propagation rules are derived that allow one to construct a new subsystem code by combining two given subsystem codes.**

I. Introduction

Subsystem codes are a relatively new construction of quantum codes that combine the features of decoherence free subspaces [1], noiseless subsystems [2], and quantum error-correcting codes [3], [4]. Such codes promise to offer appealing features, such as simplified syndrome calculation and a wide variety of easily implementable fault-tolerant operations, see [5]–[8].

An $((n,K,R,d))_q$ subsystem code is a KR-dimensional subspace Q of $\mathbb{C}^{q^n}$ that is decomposed into a tensor product $Q = A \otimes B$ of a K-dimensional vector space A and an R-dimensional vector space B such that all errors of weight less than d can be detected by A. The vector spaces A and B are respectively called the subsystem A and the co-subsystem B. For some background on subsystem codes, see for instance [6], [9], [10].

A special feature of subsystem codes is that any classical additive code C can be used to construct a subsystem code. One should contrast this with stabilizer codes, where the classical codes are required to satisfy a self-orthogonality condition.

We assume that the reader is familiar with the relation between classical and quantum stabilizer codes, see [3], [11]. In [6], [9], the authors gave an introduction to subsystem codes, established upper and lower bounds on subsystem code parameters, and provided two methods for constructing subsystem codes. The main results on this paper are as follows:

i) If q is a power of a prime p, then we show that a subsystem code with parameters $((n, K/p, pR, \geq\ d))_q$ can be obtained from a subsystem code with parameters $((n,K,R,d))_q$. Furthermore, we show that the existence of a pure $((n,K,R,d))_q$ subsystem code implies the existence of a pure $((n,pK,R/p,d))_q$ code.

ii) We show that all pure MDS subsystem codes are derived from MDS stabilizer codes. We establish here for the first time the existence of numerous families of MDS subsystem codes.

iii) We derive two propagation rules that yield new subsystem codes by extending or shortening the length existing codes.

iv) We derive two propagation rules that yield a new subsystem code by combining two subsystem codes.

II. Subsystem Code Constructions

First we recall the following fact that is key to most constructions of subsystem codes (see below for notations):

Theorem 1: Let C be a classical additive subcode of $\mathbb{F}_q^{2n}$ 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) $d = \operatorname{swt}((C + C^{\perp_s}) - C) = \operatorname{swt}(D^{\perp_s} - C)$ if $D^{\perp_s} \neq C$;
(b) $d = \operatorname{swt}(D^{\perp_s})$ 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 $\leq \lfloor (d-1)/2 \rfloor$.

Proof: See [9, Theorem 5]. ■

A subsystem code that is derived with the help of the previous theorem is called a Clifford subsystem code. We will assume throughout this paper that all subsystem codes are Clifford subsystem codes. In particular, this means that the existence of an $((n,K,R,d))_q$ subsystem code implies the existence of an additive code $C \leq \mathbb{F}_q^{2n}$ with subcode $D = C \cap C^{\perp_s}$ such that $|C| = q^nR/K$, $|D| = q^n/(KR)$, and $d = \operatorname{swt}(D^{\perp_s} - C)$.

A subsystem code derived from an additive classical code C is called pure to d' if there is no element of symplectic weight less than d' in C. A subsystem code is called pure if it is pure to the minimum distance d. We require that an $((n,1,R,d))_q$ subsystem code must be pure.

We also use the bracket notation $[[n,k,r,d]]_q$ to write the parameters of an $((n,q^k,q^r,d))_q$ subsystem code in simpler form. Some authors say that an $[[n,k,r,d]]_q$ subsystem code has r gauge qudits, but this terminology is slightly confusing, as the co-subsystem typically does not correspond to a state space of r qudits except perhaps in trivial cases. We will avoid this misleading terminology. An $((n,K,1,d))_q$ subsystem code is also an $((n,K,d))_q$ stabilizer code and vice versa.

Notation. 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 $(x|y)=(x_1,\ldots,x_n|y_1,\ldots,y_n)$ 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

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

We define $\operatorname{swt}(X)=\min\{\operatorname{swt}(x)\,|\,x\in X, x\neq 0\}$ 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

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

where $x\cdot y$ denotes the dot product and $\operatorname{tr}_{q/p}$ 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

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

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

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

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

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

III. Trading Dimensions of subsystem and co-subsystem codes

In this section we show how one can trade the dimensions of subsystem and co-subsystem to obtain new codes from a 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** 2:* 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 $C\subseteq\mathbb{F}_q^{2n}$ 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 $d=\operatorname{swt}(D^{\perp_s}-C)$ if $C\neq D^{\perp_s}$, otherwise $d=\operatorname{swt}(D^{\perp_s})$ 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 $\mathbb{F}_p$-basis of C of the form

$$C=\operatorname{span}_{\mathbb{F}_p}\{z_1,\ldots,z_s,x_{s+1},z_{s+1},\ldots,x_{s+r},z_{s+r}\}$$

that can be extended to a symplectic basis $\{x_1,z_1,\ldots,x_{nm},z_{nm}\}$ of $\mathbb{F}_q^{2n}$, that is, $\langle x_k\mid x_\ell\rangle_s=0$, $\langle z_k\mid z_\ell\rangle_s=0$, $\langle x_k\mid z_\ell\rangle_s=\delta_{k,\ell}$ for all $1\leq k,\ell\leq nm$, see [12, Theorem 8.10.1].

Define an additive code

$$C_m=\operatorname{span}_{\mathbb{F}_p}\{z_1,\ldots,z_s,x_{s+1},z_{s+1},\ldots,x_{s+r+1},z_{s+r+1}\}.$$

It follows that

$$C_m^{\perp_s}=\operatorname{span}_{\mathbb{F}_p}\{z_1,\ldots,z_s,x_{s+r+2},z_{s+r+2},\ldots,x_{nm},z_{nm}\}$$

and

$$D=C_m\cap C_m^{\perp_s}=\operatorname{span}_{\mathbb{F}_p}\{z_1,\ldots,z_s\}.$$

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 $K_m=q^n/(p^{s+2r+2}p^s)^{1/2}=K/p$ 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 $d_m=\operatorname{swt}(D^{\perp_s}-C_m)\geq\operatorname{swt}(D^{\perp_s}-C)=d$. Since by hypothesis $\operatorname{swt}(D^{\perp_s}-C)=d$ and $\operatorname{swt}(C)\geq d'$, and $D\subseteq C\subset C_m\subseteq D^{\perp_s}$ by construction, we have $\operatorname{swt}(C_m)\geq\min\{d,d'\}$; 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 $d=\operatorname{swt}(D^{\perp_s}-C)=\operatorname{swt}(D^{\perp_s})=d_m$.

This proves the claim. ■

For $\mathbb{F}_q$-linear subsystem codes there exists a variation of the previous theorem which asserts that one can construct the resulting subsystem code such that it is again $\mathbb{F}_q$-linear.

***Theorem** 3:* Let q be a power of a prime p. If there exists an $\mathbb{F}_q$-linear $[[n,k,r,d]]_q$ subsystem code with $k>1$ that is pure to d', then there exists an $\mathbb{F}_q$-linear $[[n,k-1,r+1,\geq d]]_q$ subsystem code that is pure to $\min\{d,d'\}$. If a pure $\mathbb{F}_q$-linear $[[n,1,r,d]]_q$ subsystem code exists, then there exists an $\mathbb{F}_q$-linear $[[n,0,r+1,d]]_q$ subsystem code.

Proof: The proof is analogous to the proof of the previous theorem, except that $\mathbb{F}_q$-bases are used instead of $\mathbb{F}_p$-bases. ■

There exists a partial converse of Theorem 2, namely if the subsystem code is pure, then it is possible to increase the dimension of the subsystem and decrease the dimension of the co-subsystem while maintaining the same minimum distance.

***Theorem** 4:* Let q be a power of a prime p. If there exists a pure $((n,K,R,d))_q$ subsystem code with $R>1$, then there exists a pure $((n,pK,R/p,d))_q$ subsystem code.

Proof: Suppose that the $((n,K,R,d))_q$ Clifford subsystem code is associated with a classical additive code

$$C_m=\operatorname{span}_{\mathbb{F}_p}\{z_1,\ldots,z_s,x_{s+1},z_{s+1},\ldots,x_{s+r+1},z_{s+r+1}\}.$$

Let $D=C_m\cap C_m^{\perp_s}$. We have $x=|C_m|=p^{s+2r+2}$, $y=|D|=p^s$, hence $K=q^n/p^{r+s}$ and $R=p^{r+1}$. Furthermore, $d=\operatorname{swt}(D^{\perp_s})$.

The code

$$C=\operatorname{span}_{\mathbb{F}_p}\{z_1,\ldots,z_s,x_{s+1},z_{s+1},\ldots,x_{s+r},z_{s+r}\}$$

has the subcode $D = C \cap C^{\perp_s}$. Since $|C| = |C_m|/p^2$, the parameters of the Clifford subsystem code associated with C are $((n, pK, R/p, d'))_q$. Since $C \subset C_m$, the minimum distance d' satisfies

$$d' = \mathrm{swt}(D^{\perp_s} - C) \leq \mathrm{swt}(D^{\perp_s} - C_m) = \mathrm{swt}(D^{\perp_s}) = d.$$

On the other hand, $d' = \mathrm{swt}(D^{\perp_s} - C) \geq \mathrm{swt}(D^{\perp_s}) = d$, whence $d = d'$. Furthermore, the resulting code is pure since $d = \mathrm{swt}(D^{\perp_s}) = \mathrm{swt}(D^{\perp_s} - C)$. ■

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

***Theorem** 5:* Let q be a power of a prime p. If there exists a pure $\mathbb{F}_q$-linear $[[n, k, r, d]]_q$ subsystem code with $r > 0$, then there exists a pure $\mathbb{F}_q$-linear $[[n, k+1, r-1, d]]_q$ subsystem code.

The purity hypothesis in Theorems 4 and 5 is essential, as the next remark shows.

***Remark** 1:* The Bacon-Shor code is an impure $[[9, 1, 4, 3]]_2$ subsystem code. However, there does not exist any $[[9, 5, 3]]_2$ stabilizer code. Thus, in general one cannot omit the purity assumption from Theorems 4 and 5.

An $[[n, k, d]]_q$ stabilizer code can also be regarded as an $[[n, k, 0, d]]_q$ subsystem code. We record this important special case of the previous theorems in the next corollary.

***Corollary** 6:* If there exists an ($\mathbb{F}_q$-linear) $[[n, k, d]]_q$ stabilizer code that is pure to d', then there exists for all r in the range $0 \leq r < k$ an ($\mathbb{F}_q$-linear) $[[n, k-r, r, \geq d]]_q$ subsystem code that is pure to $\min\{d, d'\}$. If a pure ($\mathbb{F}_q$-linear) $[[n, k, r, d]]_q$ subsystem code exists, then a pure ($\mathbb{F}_q$-linear) $[[n, k+r, d]]_q$ stabilizer code exists.

IV. MDS Subsystem Codes

Recall that an $[[n, k, r, d]]_q$ subsystem code derived from an $\mathbb{F}_q$-linear classical code $C \leq \mathbb{F}_q^{2n}$ satisfies the Singleton bound $k + r \leq n - 2d + 2$, see [13, Theorem 3.6]. A subsystem code attaining the Singleton bound with equality is called an MDS subsystem code.

An important consequence of the previous theorems is the following simple observation which yields an easy construction of subsystem codes that are optimal among the $\mathbb{F}_q$-linear Clifford subsystem codes.

***Theorem** 7:* If there exists an $\mathbb{F}_q$-linear $[[n, k, d]]_q$ MDS stabilizer code, then there exists a pure $\mathbb{F}_q$-linear $[[n, k - r, r, d]]_q$ MDS subsystem code for all r in the range $0 \leq r \leq k$.

Proof: An MDS stabilizer code must be pure, see [11, Theorem 2] or [14, Corollary 60]. By Corollary 6, a pure $\mathbb{F}_q$-linear $[[n, k, d]]_q$ stabilizer code implies the existence of an $\mathbb{F}_q$-linear $[[n, k-r, r, d_r \geq d]]_q$ subsystem code that is pure to d for any r in the range $0 \leq r \leq k$. Since the stabilizer code is MDS, we have $k = n - 2d + 2$. By the Singleton bound, the parameters of the resulting $\mathbb{F}_q$-linear $[[n, n-2d+2-r, r, d_r]]_q$ subsystem codes must satisfy $(n-2d+2-r)+r \leq n-2d_r+2$, which shows that the minimum distance $d_r = d$, as claimed. ■

***Remark** 2:* We conjecture that $\mathbb{F}_q$-linear MDS subsystem codes are actually optimal among all subsystem codes, but a proof that the Singleton bound holds for general subsystem codes remains elusive.

In the next lemma, we give a few examples of MDS subsystem codes that can be obtained from Theorem 7. These are the first families of MDS subsystem codes (though sporadic examples of MDS subsystem codes have been established before, see e.g. [6], [7]).

***Lemma** 8:*

i) An $\mathbb{F}_q$-linear pure $[[n, n-2d+2-r, r, d]]_q$ MDS subsystem code exists for all n, d, and r such that $3 \leq n \leq q$, $1 \leq d \leq n/2+1$, and $0 \leq r \leq n-2d+1$.

ii) An $\mathbb{F}_q$-linear pure $[[(\nu+1)q, (\nu+1)q-2\nu-2-r, r, \nu+2]]_q$ MDS subsystem code exists for all ν and r such that $0 \leq \nu \leq q-2$ and $0 \leq r \leq (\nu+1)q-2\nu-3$.

iii) An $\mathbb{F}_q$-linear pure $[[q-1, q-1-2\delta-r, r, \delta+1]]_q$ MDS subsystem code exists for all δ and r such that $0 \leq \delta < (q-1)/2$ and $0 \leq r \leq q-2\delta-1$.

iv) An $\mathbb{F}_q$-linear pure $[[q, q-2\delta-2-r', r', \delta+2]]_q$ MDS subsystem code exists for all $0 \leq \delta < (q-1)/2$ and $0 \leq r' < q-2\delta-2$.

v) An $\mathbb{F}_q$-linear pure $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$ MDS subsystem code exists for all δ and r in the range $0 \leq \delta < q-1$ and $0 \leq r < q^2-2\delta-1$.

vi) An $\mathbb{F}_q$-linear pure $[[q^2, q^2-2\delta-2-r', r', \delta+2]]_q$ MDS subsystem code exists for all δ and r' in the range $0 \leq \delta < q-1$ and $0 \leq r' < q^2-2\delta-2$.

Proof: i) By [15, Theorem 14], there exist $\mathbb{F}_q$-linear $[[n, n-2d+2, d]]_q$ stabilizer codes for all n and d such that $3 \leq n \leq q$ and $1 \leq d \leq n/2+1$. The claim follows from Theorem 7.
ii) By [16, Theorem 5], there exist a $[[(\nu+1)q, (\nu+1)q - 2\nu-2, \nu+2]]_q$ stabilizer code. In this case, the code is derived from an $\mathbb{F}_{q^2}$-linear code X of length n over $\mathbb{F}_{q^2}$ such that $X \subseteq X^{\perp_h}$. The claim follows from Lemma 15 and Theorem 7.
iii),iv) There exist $\mathbb{F}_q$-linear stabilizer codes with parameters $[[q-1, q-2\delta-1, \delta+1]]_q$ and $[[q, q-2\delta-2, \delta+2]]_q$ for $0 \leq \delta < (q-1)/2$, see [15, Theorem 9]. Theorem 7 yields the claim.
v),vi) There exist $\mathbb{F}_q$-linear stabilizer codes with parameters $[[q^2-1, q^2-2\delta-1, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2, \delta+2]]_q$. for $0 \leq \delta < q-1$ by [15, Theorem 10]. The claim follows from Theorem 7. ■

The existence of the codes in i) are merely established by a non-constructive Gilbert-Varshamov type counting argument. However, the result is interesting, as it asserts that there exist for example $[[6, 1, 1, 3]]_q$ subsystem codes for all prime powers $q \geq 7$, $[[7, 1, 2, 3]]_q$ subsystem codes for all prime powers $q \geq 7$, and other short subsystem codes that one should compare with a $[[5, 1, 3]]_q$ stabilizer code. If the syndrome calculation is simpler, then such subsystem codes could be of practical value.

The subsystem codes given in ii)-vi) of the previous lemma are constructively established. The subsystem codes in ii) are derived from Reed-Muller codes, and in iii)-vi) from Reed-Solomon codes. There exists an overlap between the parameters given in ii) and in iv), but we list here both, since each code construction has its own merits.

***Remark** 3:* By Theorem 5, pure MDS subsystem codes can always be derived from MDS stabilizer codes, see Table I.

TABLE I
OPTIMAL PURE SUBSYSTEM CODES

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

* Punctured code
† Extended code

Therefore, one can derive in fact all possible parameter sets of pure MDS subsystem codes with the help of Theorem 7.

Remark *4:* In the case of stabilizer codes, all MDS codes must be pure. For subsystem codes this is not true, as the $[[9,1,4,3]]_2$ subsystem code shows. Finding such impure $\mathbb{F}_q$-linear $[[n,k,r,d]]_q$ MDS subsystem codes with $k+r=n-2d+2$ is a particularly interesting challenge.

Recall that a pure subsystem code is called perfect if and only if it attains the Hamming bound with equality. We conclude this section with the following consequence of Theorem 7:

Corollary *9:* If there exists an $\mathbb{F}_q$-linear pure $[[n,k,d]]_q$ stabilizer code that is perfect, then there exists a pure $\mathbb{F}_q$-linear $[[n,k-r,r,d]]_q$ perfect subsystem code for all r in the range $0 \leq r \leq k$.

V. EXTENDING AND SHORTENING SUBSYSTEM CODES

In Section III, we showed how one can derive new subsystem codes from known ones by modifying the dimension of the subsystem and co-subsystem. In this section, we derive new subsystem codes from known ones by extending and shortening the length of the code.

Theorem *10:* 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 $X \leq \mathbb{F}_q^{2n}$, we can define an additive code $X' \leq \mathbb{F}_q^{2n+2}$ by

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

We have $|X'| = q|X|$. Furthermore, if $(c|d) \in X^{\perp_s}$, then $(c\alpha|d0)$ is contained in $(X')^{\perp_s}$ for all α in $\mathbb{F}_q$, 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 1, 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 $\mathbb{F}_q$, 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 1 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) $d' = \operatorname{swt}((D')^{\perp_s} \setminus C') \geq \operatorname{swt}((D^{\perp_s} \setminus C)') = d$.

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

Corollary *11:* 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.

We can also shorten the length of a subsystem code in a simple way as shown in the following Theorem.

Theorem *12:* If a pure $((n,K,R,d))_q$ subsystem code exists, then there exists a pure $((n-1,qK,R,d-1))_q$ subsystem code.

Proof: By [6, Lemma 10], the existence of a pure Clifford subsystem code with parameters $((n,K,R,d))_q$ implies the existence of a pure $((n,KR,d))_q$ stabilizer code. It follows from [14, Lemma 70] that there exist a pure $((n-1,qKR,d-1))_q$ stabilizer code, which can be regarded as a pure $((n-1,qKR,1,d-1))_q$ subsystem code. Thus, there exists a pure $((n-1,qK,R,d-1))_q$ subsystem code by Theorem 4, which proves the claim. ■

In bracket notation, the previous theorem states that the existence of a pure $[[n,k,r,d]]_q$ subsystem code implies the existence of a pure $[[n-1,k+1,r,d-1]]_q$ subsystem code.

VI. COMBINING SUBSYSTEM CODES

In this section, we show how one can obtain a new subsystem code by combining two given subsystem codes in various ways.

Theorem *13:* If there exists a pure $[[n_1,k_1,r_1,d_1]]_2$ subsystem code and a pure $[[n_2,k_2,r_2,d_2]]_2$ subsystem code such that $k_2+r_2 \leq n_1$, then there exist subsystem codes with parameters

$$[[n_1+n_2-k_2-r_2, k_1+r_1-r, r, d]]_2$$

for all r in the range $0 \leq r < k_1+r_1$, where the minimum distance $d \geq \min\{d_1, d_1+d_2-k_2-r_2\}$.

Proof: Since there exist pure $[[n_1,k_1,r_1,d_1]]_2$ and $[[n_2,k_2,r_2,d_2]]_2$ subsystem codes with $k_2+r_2 \leq n_1$, it follows from Theorem 4 that there exist stabilizer codes with the parameters $[[n_1, k_1 + r_1, d_1]]_2$ and $[[n_2, k_2 + r_2, d_2]]_2$ such that $k_2 + r_2 \leq n_1$. Therefore, there exists an $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1, d]]_2$ stabilizer code with minimum distance $d \geq \min\{d_1, d_1 + d_2 - k_2 - r_2\}$ by [3, Theorem 8]. It follows from Theorem 2 that there exists $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1 - r, r, \geq d]]_2$ subsystem codes for all r in the range $0 \leq r < k_1 + r_1$. ■

***Theorem** 14:* 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 pure subsystem codes with parameters

$$[[2n, k_1 + k_2 + r_1 + r_2 - r, r, d]]_q$$

for all r in the range $0 \leq r \leq k_1 + k_2 + r_1 + r_2$, where the minimum distance $d \geq \min\{d_1, 2d_2\}$.

Proof: By assumption, there exists a pure $[[n, k_i, r_i, d_i]]_q$ subsystem code, which implies the existence of a pure $[[n, k_i + r_i, d_i]]_q$ stabilizer code by Theorem 4, where $i \in \{1, 2\}$. By [14, Lemma 74], there exists a pure stabilizer code with parameters $[[2n, k_1 + k_2 + r_1 + r_2, d]]_q$ such that $d \geq \min\{2d_2, d_1\}$. By Theorem 2, there exist a pure subsystem code with parameters $[[2n, k_1 + k_2 + r_1 + r_2 - r, r, d]]_q$ for all r in the range $0 \leq r \leq k_1 + k_2 + r_1 + r_2$, which proves the claim. ■

VII. Conclusions and Open Problems

Subsystem codes – or operator quantum error-correcting codes as some authors prefer to called them – are among the most versatile tools in quantum error-correction, since they allow one to combine the passive error-correction found in decoherence free subspaces and noiseless subsystems with the active error-control methods of quantum error-correcting codes. The subclass of Clifford subsystem codes that was studied in this paper is of particular interest because of the close connection to classical error-correcting codes.

In this paper, we showed that any $\mathbb{F}_q$-linear MDS stabilizer code yields a series of pure $\mathbb{F}_q$-linear MDS subsystem codes. These codes are known to be optimal among the $\mathbb{F}_q$-linear Clifford subsystem codes. We conjecture that the Singleton bound holds in general for subsystem codes.

We have established a number of subsystem code constructions. In particular, we have shown how one can derive subsystem codes from stabilizer codes. In combination with the propagation rules that we have derived, one can easily create tables with the best known subsystem codes. Further propagation rules and examples of such tables will be given in an expanded version of this paper that is not limited by space constraints.

VIII. ACKNOWLEDGMENTS

This research was supported by NSF grant CCF-0622201 and NSF CAREER award CCF-0347310. We thank Daniel Lidar for providing us with references on DFS and noiseless subsystems. S.A.A. thanks the organizers of the first international conference on quantum error correction (held at the USC campus, December 17-21, 2007) for their hospitality.

Appendix

We recall that the Hermitian construction of stabilizer codes yields $\mathbb{F}_q$-linear stabilizer codes, as can be seen from the following reformulation of [15, Corollary 2].

***Lemma** 15 ([15]):* If there exists an $\mathbb{F}_{q^2}$-linear code $X \subseteq \mathbb{F}_{q^2}^n$ such that $X \subseteq X^{\perp_h}$, then there exists an $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_q^{2n}$ such that $C \subseteq C^{\perp_s}$, $|C| = |X|$, $\mathrm{swt}(C^{\perp_s} - C) = \mathrm{wt}(X^{\perp_h} - X)$ and $\mathrm{swt}(C) = \mathrm{wt}(X)$.

Proof: Let $\{1, \beta\}$ be a basis of $\mathbb{F}_{q^2}/\mathbb{F}_q$. Then $\mathrm{tr}_{q^2/q}(\beta) = \beta + \beta^q$ is an element β_0 of $\mathbb{F}_q$; hence, $\beta^q = -\beta + \beta_0$. Let

$$C = \{(u|v) \mid u, v \in \mathbb{F}_q^n, u + \beta v \in X\}.$$

It follows from this definition that $|X| = |C|$ and that $\mathrm{wt}(X) = \mathrm{swt}(C)$. Furthermore, if $u + \beta v$ and $u' + \beta v'$ are elements of X with u, v, u', v' in $\mathbb{F}_q^n$, then

$$\begin{array}{rcl} 0 & = & (u + \beta v)^q \cdot (u' + \beta v') \\ & = & u \cdot u' + \beta^{q+1} v \cdot v' + \beta_0 v \cdot u' + \beta(u \cdot v' - v \cdot u'). \end{array}$$

On the right hand side, all terms but the last are in $\mathbb{F}_q$; hence we must have $(u \cdot v' - v \cdot u') = 0$, which shows that $(u|v) \perp_s (u'|v')$, whence $C \subseteq C^{\perp_s}$. Expanding $X^{\perp_h}$ in the basis $\{1 \beta\}$ yields a code $C' \subseteq C^{\perp_s}$, and we must have equality by a dimension argument. Since the basis expansion is isometric, it follows that $\mathrm{swt}(C^{\perp_s} - C) = \mathrm{wt}(X^{\perp_h} - X)$. The $\mathbb{F}_q$-linearity of C is a direct consequence of the definition of C. ■

References

[1] D. Lidar, I. Chuang, and K. Whaley, “Decoherence-free subspaces for quantum-computation,” *Phys. Rev. Letters*, vol. 81, pp. 2594–2597, 1998.

[2] P. Zanardi and M. Rasetti, “Noiseless quantum codes,” *Phys. Rev. Lett.*, vol. 79, p. 3306, 1997.

[3] A. Calderbank, E. Rains, P. Shor, and N. Sloane, “Quantum error correction via codes over GF(4),” *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, 1998.

[4] D. Gottesman, “A class of quantum error-correcting codes saturating the quantum Hamming bound,” *Phys. Rev. A*, vol. 54, pp. 1862–1868, 1996.

[5] P. Aliferis and A. W. Cross, “Sub-system fault tolerance with the Bacon-Shor code,” *Phys. Rev. Lett.*, vol. 98, p. 220502, 2007.

[6] S. Aly, A. Klappenecker, and P. Sarvepalli, “Subsystem codes,” in *44th Annual Allerton Conference on Communication, Control, and Computing, Monticello, Illinois, September, 2006*, 2006.

[7] D. Bacon, “Operator quantum error correcting subsystems for self-correcting quantum memories,” *Phys. Rev. A*, vol. 73, no. 012340, 2006.

[8] D. W. Kribs, R. Laflamme, and D. Poulin, “Unified and generalized approach to quantum error correction,” *Phys. Rev. Lett.*, vol. 94, no. 180501, 2005.

[9] A. Klappenecker and P. Sarvepalli, “Clifford code constructions of operator quantum error correcting codes.” arXiv:quant-ph/0604161, 2006.

[10] D. Poulin, “Stabilizer formalism for operator quantum error correction,” *Phys. Rev. Lett.*, vol. 95, no. 230504, 2005.

[11] E. Rains, “Nonbinary quantum codes,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 1827–1832, 1999.

[12] P. Cohn, *Basic Algebra – Groups, Rings, and Fields*. Springer, 2005.

[13] A. Klappenecker and P. Sarvepalli, “On subsystem codes beating the Hamming or Singleton bound,” *Proc. Royal Soc. Series A*, vol. 463, no. 2087, pp. 2887–2905, 2007.

[14] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.

[15] M. Grassl, T. Beth, and M. Rötteler, “On optimal quantum codes,” *Internat. J. Quantum Information*, vol. 2, no. 1, pp. 757–775, 2004.

[16] P. Sarvepalli and A. Klappenecker, “Nonbinary quantum Reed-Muller codes,” in *Proc. 2005 IEEE International Symposium on Information Theory, Adelaide, Australia*, pp. 1023–1027, 2005.