On subsystem codes beating the quantum Hamming or Singleton bound

BY ANDREAS KLAPPENECKER* AND PRADEEP KIRAN SARVEPALLI
Texas A&M University, College Station, Texas, TX 77843, USA

Subsystem codes are a generalization of noiseless subsystems, decoherence-free subspaces and stabilizer codes. We generalize the quantum Singleton bound to $F_q$-linear subsystem codes. It follows that no subsystem code over a prime field can beat the quantum Singleton bound. On the other hand, we show the remarkable fact that there exist impure subsystem codes beating the quantum Hamming bound. A number of open problems concern the comparison in the performance of stabilizer and subsystem codes. One of the open problems suggested by Poulin’s work asks whether a subsystem code can use fewer syndrome measurements than an optimal $F_q$-linear maximum distance separable stabilizer code while encoding the same number of qudits and having the same distance. We prove that linear subsystem codes cannot offer such an improvement under complete decoding.

Keywords: subsystem codes; operator codes; quantum Hamming bound; quantum Singleton bound

1. Introduction

Subsystem codes (sometimes also referred to as operator quantum error-correcting codes) have emerged as an important new discovery in the area of quantum error-correcting codes, unifying the classes of stabilizer codes, decoherence-free subspaces and noiseless subsystems (Kribs et al. 2005, 2006; Poulin 2005; Bacon 2006; Knill 2006; Kribs 2006). This unification permits an understanding of active quantum error correction and passive quantum error correction within a common framework. However, this generalization is more than a theoretical construct. It has important practical implications too in the form of simpler error recovery schemes (Bacon 2006). These potential gains are in part the motivation behind this paper. However, first we recall some facts about quantum codes.

A quantum code $Q$ is a subspace in a finite dimensional Hilbert space, $\mathcal{H} = \mathbb{C}^q^n$. By qudit, we refer to a quantum digit with $q$ levels. A quantum code $Q$ encoding $k$ qudits into $n$ qudits and of distance $d$ is referred to as an $[[n, k, d]]_q$ quantum code. In this case, $Q$ is a $q^k$-dimensional subspace of $\mathcal{H}$. Informally, the generalization to subsystem codes arose when further structure was imposed on the code subspace $Q$. A subsystem code is a quantum code that can be further resolved into a tensor product, i.e. $Q = A \otimes B$. Information is stored in system $A$, while system $B$, referred to as the gauge subsystem or co-subsystem, provides useful additional structure.

* Author for correspondence (klappi@cs.tamu.edu).
some additional redundancy. Errors acting on the co-subsystem $B$ alone can be ignored for the purposes of error correction. Furthermore, in the process of recovery, one need not restore the state of subsystem $B$, which provides a greater degree of flexibility than in the case of stabilizer codes. If $A$ is $q^k$-dimensional and $B$ is $q^r$-dimensional, then we encode $k$ qudits into $n$ qudits with $r$ gauge qudits. The notion of distance also generalizes to subsystem codes as will be seen in §2. We denote the parameters of a subsystem code by $[[n, k, r, d]]_q$, indicating that it is a $q$-ary code with length $n$, encodes $k$ qudits into the subsystem $A$, contains $r$ gauge qudits and has distance $d$.

Perhaps the benefits of subsystem codes are best understood by an example. Consider the first quantum error-correcting code proposed by Shor (1995), which encodes one qubit into nine quantum bits. This code, which is capable of correcting a single error on any of the qubits, requires the measurement of eight syndrome qubits. The Bacon–Shor subsystem code (Bacon 2006), on the other hand, also encodes one qubit into nine but requires only four syndrome measurements, giving a simpler error recovery scheme.

In this context, it becomes crucial to identify when subsystem codes provide gains over the stabilizer codes. It also becomes necessary to compare the stabilizer codes and the subsystem codes fairly and with meaningful criteria. For instance, once again consider the $[[9, 1, 3]]_2$ Shor code requiring $n - k = 9 - 1 = 8$ syndrome measurements. The $[[9, 1, 4, 3]]_2$ Bacon–Shor code, on the other hand, requires $n - k - r = 9 - 1 - 4 = 4$ syndrome measurements. Clearly, this code is better than the Shor’s code. However, the optimal single error-correcting binary quantum code that encodes one qubit is the $[[5, 1, 3]]_2$ code, which also requires only $5 - 1 = 4$ syndrome measurements. So it is apparent that while a given subsystem code can be superior to some stabilizer codes, it is not at all obvious that it is better than the best stabilizer code for the same function, viz., encoding $k$ qubits with a distance $d$.

The first part of our paper seeks to address this issue for $\mathbb{F}_q$-linear Clifford subsystem codes which might perhaps be the most useful class of subsystem codes. In this paper, we generalize the quantum Singleton bound to $\mathbb{F}_q$-linear Clifford subsystem codes. It follows that no Clifford subsystem code over a prime field can beat the quantum Singleton bound. We then show how the quantum Singleton bound can be applied to make the comparison between stabilizer and subsystem codes (focusing on stabilizer codes that are optimal in the sense that they meet the quantum Singleton bound). This bound makes it possible to quantify the gains that subsystem codes can provide in error recovery. In particular, our results show that these gains involve a trade-off between the distance of the subsystem code and the number of information qudits and the gauge qudits. We show that if there exists an $\mathbb{F}_q$-linear maximum distance separable (MDS) stabilizer code, i.e. a code meeting the quantum Singleton bound, then no $\mathbb{F}_q$-linear subsystem code can outperform it in the sense of requiring fewer syndrome measurements for error correction.

Then, we shift our attention to a class of subsystem codes on lattices. Bacon & Casaccino (2006) obtained a subsystem code from two classical codes. We show that this method is a special case of the Euclidean construction for subsystem codes proposed by Aly et al. (2006) and give a coding theoretic analysis of these codes.

Since the early works on quantum error-correcting codes, it has been suspected that impure codes should somehow perform better than the pure codes. However, it was shown that the quantum Singleton bound holds true for both pure and
impure stabilizer codes. However, it was not so clear with respect to the quantum Hamming bound. In fact, it was often conjectured that there might exist impure quantum error-correcting codes beating the quantum Hamming bound, but a proof remained elusive. At least in the case of binary stabilizer codes, there exists some evidence that the conjecture might not be true, as Ashikhmin & Litsyn (1999) showed that asymptotically the quantum Hamming bound was obeyed by impure codes as well, and Gottesman (1997) showed that no single error-correcting binary stabilizer code can beat the quantum Hamming bound. In this context, it is not surprising that questions were raised (Bacon 2006) about whether subsystem codes are any different. Aly et al. (2006) proved the quantum Hamming bound for pure subsystem codes. We show here that impure subsystem codes can indeed beat the quantum Hamming bound for pure subsystem codes. For example, we demonstrate that the lattice subsystem codes can provide examples of impure subsystem codes that beat the quantum Hamming bound.

The paper is structured as follows. We review the necessary background in §2 and then prove the quantum Singleton bound for subsystem codes in §3. The lattice subsystem codes are the focus of attention in §§4 and 5, wherein it is shown that there exist impure subsystem codes that beat the quantum Hamming bound. We conclude with a few open questions on subsystem codes.

2. Background

Let $\mathbb{F}_q$ be a finite field with $q$ elements and characteristic $p$. Let $C \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear classical code denoted by $[n, k, d]_q$, where $k = \dim_{\mathbb{F}_q} C$ and $d$ is the minimum distance of $C$. We define $\text{wt}(C) = \min\{\text{wt}(c) | 0 \neq c \in C\} = d$, where $\text{wt}(c)$ is the Hamming weight of $c$. Sometimes an alternative notation $(n, K, d)_q$ is also used where $K = |C|$. If $C$ is an $\mathbb{F}_q$-linear subspace over $\mathbb{F}_q$, then we say that it is an additive code.

If $x, y \in \mathbb{F}_q^n$, then their Euclidean inner product is defined as $x \cdot y = \sum_i x_i y_i$. The Euclidean dual of a code $C \subseteq \mathbb{F}_q^n$ is defined as $C^\perp = \{y \in \mathbb{F}_q^n | x \cdot y = 0 \text{ for all } x \in C\}$. We say that a code $C$ is self-orthogonal with respect to the Euclidean inner product if $C \subseteq C^\perp$.

We use the notation $(x|y) = (x_1, \ldots, x_n|y_1, \ldots, y_n)$ to denote concatenation of $x, y \in \mathbb{F}_q^n$. Let $u = (a|b)$ and $v = (a'|b')$ be in $\mathbb{F}_q^{2n}$. We define the symplectic weight of $u$ as $\text{swt}(u) = |\{(a_i, b_i) \neq (0, 0) | 1 \leq i \leq n\}|$ and the symplectic weight of a code $C \subseteq \mathbb{F}_q^{2n}$ as $\text{swt}(C) = \min\{\text{swt}(c) | 0 \neq c \in C\}$. For codes over $\mathbb{F}_q^{2n}$, another inner product plays a more important role in the context of quantum codes. The trace-symplectic product between $u$ and $v$ is defined as $\langle u|v \rangle_t = \langle (a|b)|(a'|b') \rangle_t = \text{tr}_{\mathbb{F}_q}(a' \cdot b - a \cdot b')$. The trace-symplectic dual of $C \subseteq \mathbb{F}_q^{2n}$ is defined as $C^{\perp_t} = \{x \in \mathbb{F}_q^{2n} | \langle x|y \rangle_t = 0, \text{ for all } y \in C\}$. If $C \subseteq C^{\perp_t}$, we say that it is self-orthogonal with respect to the trace-symplectic inner product.

(a) Subsystem codes from classical codes

We now briefly review the background on subsystem codes. First, we give a group theoretic description and then an alternate description in terms of classical codes. Further details can be found in Aly et al. (2006) and Klappenecker & Sarvepalli (2006).
Let $q$ be the power of a prime $p$ and $\mathbb{F}_q$ a finite field with $q$ elements. Let $B = \{|x| | x \in \mathbb{F}_q\}$ denote an orthonormal basis for $\mathbb{C}^q$. Let $X(a)$ and $Z(b)$ be unitary operators on $\mathbb{C}^q$ whose action on any element $|x\rangle$ in $B$ is defined as
\[
X(a)|x\rangle = |x + a\rangle \quad \text{and} \quad Z(b)|x\rangle = \omega^{ax/b}|x\rangle,
\]
where $\omega = e^{i2\pi/p}$ is a primitive $p$th root of unity. These operators are a $q$-ary generalization of the well-known Pauli matrices $X$ and $Z$. Their action on an arbitrary element in $\mathbb{C}^q$ is obtained by invoking linearity. Let $\mathcal{H} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q = \mathbb{C}^{q^n}$ and $\mathcal{E}$ be the error group on $\mathcal{H}$, defined as the tensor product of $n$ such error operators, i.e.
\[
\mathcal{E} = \{\omega^c E_1 \otimes \cdots \otimes E_n | E_i = X(a_i)Z(b_i) ; a_i, b_i \in \mathbb{F}_q ; c \in \mathbb{F}_p\}.
\]
The weight of an error $E = \omega^c E_1 \otimes E_2 \otimes \cdots \otimes E_n$ in $\mathcal{E}$ is defined as the number of $E_i$ which are not equal to identity and it is denoted by $\text{wt}(E)$. We can also associate with $E$ a vector $\overline{E} = (a_1, \ldots, a_n b_1, \ldots, b_n) \in \mathbb{F}_q^{2n}$. We define the symplectic weight of $\overline{E}$ as
\[
\text{swt}(\overline{E}) = |\{(a_i, b_i) \neq (0, 0) | 1 \leq i \leq n\}| = \text{wt}(E).
\]
Every nontrivial normal subgroup $N$ in $\mathcal{E}$ defines a subsystem code $Q$. Let $C_\mathcal{E}(N)$ be the centralizer of $N$ in $\mathcal{E}$ and $Z(N)$, the centre of $N$. As a subspace, the subsystem code $Q$ defined by $N$ is precisely the same as the stabilizer code defined by $Z(N)$. By theorem 4 in Klappenecker & Sarvepalli (2006), $Q$ can be decomposed as $A \otimes B$, where $\dim B = |N : Z(N)|^{1/2}$ and
\[
\dim A = |Z(\mathcal{E}) \cap N| |\mathcal{E} : Z(\mathcal{E})|^{1/2} |N : Z(N)|^{1/2} / |N|.
\]
Since information is stored only on subsystem $A$, we need only be concerned with errors that affect $A$. An error $E$ in $\mathcal{E}$ is detectable by subsystem $A$ if and only if $E$ is contained in the set $\mathcal{E} - (NC_\mathcal{E}(N) - N)$. The distance of the code is defined as
\[
d = \min \{\text{wt}(E) | I \neq E \in NC_\mathcal{E}(N) - N\} = \text{wt}(NC_\mathcal{E}(N) - N).
\]
If $NC_\mathcal{E}(N) = N$, then we define the distance of the code to be $\text{wt}(N)$. A distance $d$ subsystem code with $\dim A = K$, $\dim B = R$ is often denoted as $([n, K, R, d])_q$, or $([n, k, r, d])_q$ if $K = q^k$ and $R = q^r$. We say that $N$ is the gauge group of $Q$ and $Z(N)$ its stabilizer. The gauge group acts trivially on $A$.

In Klappenecker & Sarvepalli (2006), we showed that subsystem codes, much like the stabilizer codes, are related to the classical codes over $\mathbb{F}_q^{2n}$ or $\mathbb{F}_q^n$, but with one important difference. We no longer need the associated classical codes to be self-orthogonal, thereby extending the class of quantum codes. The gauge group $N$ can be mapped to a classical code $C$ over $\mathbb{F}_q^{2n}$ and $C_\mathcal{E}(N)$ can be mapped to the trace-symplectic dual of $C$. The following theorem (Klappenecker & Sarvepalli 2006) shows how subsystem codes are related to classical codes.

**Theorem 2.1.** Let $C$ be a classical additive subcode of $\mathbb{F}_q^{2n}$ such that $C \neq \{0\}$ and let $D$ denote its subcode $D = C \cap C^{\perp}$. If $x = |C|$ and $y = |D|$, then there exists an operator quantum error-correcting code $Q = A \otimes B$ such that

(i) $\dim A = q^n / (xy)^{1/2}$,

(ii) $\dim B = (xy)^{1/2}$. The minimum distance of subsystem $A$ is given by

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

(b) $d = \text{swt}(D^{\perp})$ if $D^{\perp} = C$.

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

We call codes constructed using theorem 2.1 as Clifford subsystem codes. Arguably, these codes cover the most important subsystem codes, including the recently proposed Bacon–Shor codes. In this paper, henceforth by a subsystem code, we will mean a Clifford subsystem code.

A further simplification of the above construction is possible, which takes any pair of classical codes to give a subsystem code. We will just recall the result here and study its application in §4.

**Corollary 2.2 (Euclidean construction).** Let \( X_i \subseteq \mathbb{F}_q^n \), be \([n, k, r, d]_q\) linear codes where \( i \in \{1, 2\} \). Then, there exists an \([[n, k, r, d]]_q\) Clifford subsystem code with

\[
\begin{align*}
- k &= n - (k_1 + k_2 + k')/2, \\
- r &= (k_1 + k_2 - k')/2, \text{ and} \\
- d &= \min\{\text{wt}(X_1^\perp \cap X_2), \text{wt}(X_2^\perp \cap X_1^\perp)\}, \text{ where } k' = \dim_{\mathbb{F}_q}(X_1 \cap X_2^\perp) \\
&\quad \times (X_1^\perp \cap X_2).
\end{align*}
\]

The result follows from theorem 2.1 by defining \( C = X_1 \times X_2 \); it follows that \( C^\perp : = X_2^\perp \times X_1 \) and \( D = C \cap C^\perp = (X_1 \cap X_2^\perp) \times (X_2 \cap X_1) \), and the parameters are easily obtained from these definitions (see Aly et al. (2006) for a detailed proof).

\(b\) **Pure and impure subsystem codes**

We can extend the notion of purity to subsystem codes also in a straightforward manner. Let \( N \) be the gauge group of a subsystem code \( Q \) with distance \( d = \text{wt}(C(N) - N) \). We say that \( Q \) is pure to \( d' \) if there is no error of weight less than \( d' \) in \( N \). The code is said to be exactly pure to \( d' \) if \( \text{wt}(N) = d' \) and it is said to be pure if \( d' \geq d \). The code is said to be impure if it is exactly pure to \( d' < d \). This refinement to the notion of purity was made in recognition of certain subtleties that had to be addressed when constructing other subsystem codes from existing subsystem codes (see Aly et al. (2006) for details).

In coding theoretic terms, this can be translated as follows. Let \( C \) be an additive subcode of \( \mathbb{F}_q^{2n} \) and \( D = C \cap C^\perp \). By theorem 2.1, we can obtain an \([[n, K, R, d]]_q\) subsystem code \( Q \) from \( C \) that has minimum distance \( d = \text{swt}(D^\perp - C) \). If \( d' \leq \text{swt}(C) \), then we say that the associated operator quantum error-correcting code is pure to \( d' \).

Extending these ideas of purity to subsystem codes is useful because it facilitates the analysis of the parameters of the subsystem codes, as will become clear when we derive bounds in §3. If the codes are pure, then it will be very easy to see that the subsystem code with the parameters \([[n, k, r, d]]_q\) satisfies \( k + r \leq n - 2d + 2 \). This is because then the subsystem code can also be viewed as an \([[n, k + r, d]]_q\) stabilizer code (see theorem 11 in Aly et al. (2006) for further details).

### 3. Quantum Singleton upper bound for \( \mathbb{F}_q \)-linear subsystem codes

\(a\) **An upper bound for subsystem codes**

Recall that the quantum Singleton bound states that an \([[n, k, d]]_q\) quantum code satisfies \( 2d \leq n - k + 2 \) (Knill & Laflamme 1997; Rains 1999). In this context, it is natural to ask whether subsystem codes also obey a similar relation.
The usefulness of such a bound is obvious. Apart from establishing the bounds for optimal subsystem codes, they also make it possible to compare stabilizer and subsystem codes, as we shall see subsequently. We prove that the $\mathbb{F}_q$-linear subsystem codes with the parameters $[[n, k, r, d]]_q$ satisfy a quantum Singleton-like bound viz. $k+r \leq n-2d+2$. It will be seen that this reduces to the quantum Singleton bound if $r=0$. More interestingly, this reveals that there is a trade-off in the size of subsystem $A$ and the gauge subsystem. One pays a price for the gains in error recovery. The cost is the reduction in the information to be stored.

Our proof for this result is very straightforward, though the intermediate details are a little involved. First, we show that a linear $[[n, k, r>0, d]]_q$ subsystem code that is exactly pure to 1 can be punctured to an $[[n-1, k, r-1, d]]_q$ code which retains the relationship between $n, k, r, d$. If $d=2$ by repeated puncturing, we arrive at either a pure subsystem code or a stabilizer code, both of which have upper bounds. For $d>2$, two cases can arise: if the code is exactly pure to 1, we simply puncture it to get a smaller code as in $d=2$ case; otherwise, we puncture it to get an $[[n-1, k, r+1, d-1]]_q$ code. By repeatedly shortening, we get either a stabilizer code or a distance 2 code, both of which have an upper bound. Keeping track of the change in the parameters will give us an upper bound on the parameters of the original code.

Let $w = (a_1, a_2, \ldots, a_n|b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^{2n}$. We denote by $\rho(w) \in \mathbb{F}_q^{2n-2}$ the vector obtained by deleting the first and the $n+1$th coordinates of $w$. Thus, we have

$$\rho(w) = (a_2, \ldots, a_n|b_2, \ldots, b_n) \in \mathbb{F}_q^{2n-2}.$$ 

Similarly, given a classical code $C \subseteq \mathbb{F}_q^{2n}$, we denote the puncturing of $C$ in the first and $n+1$ coordinates by $\rho(C)$.

For $\mathbb{F}_q$-linear codes instead of considering the trace symplectic inner product, we can consider the relatively simpler symplectic product. The symplectic product of $u=(a|b)$ and $v=(a'|b')$ in $\mathbb{F}_q^{2n}$ is defined as $\langle u|v \rangle_s = \langle (a|b)|(a'|b') \rangle_s = a' \cdot b - a \cdot b'$. The symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as $C^\perp_s := \{ x \in \mathbb{F}_q^{2n} | \langle x|y \rangle_s = 0, \text{ for all } y \in C \}$. It will be seen that $\langle u|v \rangle_s = \text{tr}_{q/p}(\langle u|v \rangle_s)$.

**Lemma 3.1.** Let $C \subseteq \mathbb{F}_q^{2n}$ be an $\mathbb{F}_q$-linear code with $(a|b) \in C$ and $(a'|b') \in C^\perp_s$. Then $\langle (a|b)|(a'|b') \rangle_s = 0$, if and only if $\langle (a|b)|(a'|b') \rangle_s = a' \cdot b - a \cdot b' = 0$. It follows that $C^\perp_s = C^\perp$.

**Proof.** If $\langle (a|b)|(a'|b') \rangle_s = 0$, then $\text{tr}_{q/p}(a' \cdot b - a \cdot b') = 0$. Since $C$ is linear, $(\alpha a|\alpha b)$ is also orthogonal to $(a'|b')$ for any $\alpha \in \mathbb{F}_q$. Hence, $\text{tr}_{q/p}(\alpha a' \cdot b - \alpha a \cdot b') = 0$. However, $\text{tr}$ is a non-degenerate function. It follows that $a' \cdot b - a \cdot b' = 0$. The converse is straightforward. The equality of $C^\perp_s = C^\perp$ follows immediately from the first part of the statement.

As we shall be concerned with $\mathbb{F}_q$-linear codes in this paper, we will focus only on the symplectic inner product in the rest of the paper.

**Lemma 3.2.** Let $C \subseteq \mathbb{F}_q^{2n}$ be an $\mathbb{F}_q$-linear code. Then, $C$ has an $\mathbb{F}_q$-linear basis of the form

$$B = \{ z_1, \ldots, z_k, z_{k+1}, x_{k+1}, z_{k+2}, x_{k+2}, \ldots, z_{k+r}, x_{k+r} \},$$

where $\langle x_i|z_j \rangle_s = 0 = \langle z_i|x_j \rangle_s$ and $\langle x_i|z_j \rangle_s = \delta_{ij}$.

Proof. First, we choose a basis $B = \{z_1, \ldots, z_k\}$ for a maximal isotropic subspace $C_0$ of $C$. If $C_0 \neq C$, then we can choose a codeword $x_1$ in $C$ that is orthogonal to all of the $z_k$ except one, say $z_1$ (renumbering if necessary). We can scale $x_1$ by an element in $\mathbb{F}_q^\times$ so that $\langle z_1 | x_1 \rangle_s = 1$. If $\langle C_0, x_1 \rangle \neq C$, then we repeat the process until we have a basis of the desired form.

For the remainder of the section, we fix the following notation. By theorem 2.1, we can associate with an $\mathbb{F}_q$-linear $[[n, k, r, d]]_q$ subsystem code two classical $\mathbb{F}_q$-linear codes $C, D \subseteq \mathbb{F}_q^n$ such that $D = C \cap C^\perp$, $|C| = q^{n-k+r}$, $|D| = q^{n-k-r}$ and $\mathrm{swt}(D^\perp \setminus C) = d$. By lemma 3.2, we can also assume that $C$ is generated by

$$C = \langle z_1, \ldots, z_s, z_{s+1}, x_{s+1}, \ldots, z_{s+r}, x_{s+r} \rangle,$$

where $s = n-k-r$ and the vectors $x_i, z_i$ in $\mathbb{F}_q^n$ satisfy the relations $\langle x_i | x_j \rangle_s = 0 = \langle z_i | z_j \rangle_s$ and $\langle x_i | z_j \rangle_s = \delta_{i,j}$. These relations on $x_i, z_i$ imply that

$$C^\perp_s = \langle z_1, \ldots, z_s, z_{s+r+1}, x_{s+r+1}, \ldots, z_{s+r+k}, x_{s+r+k} \rangle,$$

$$D = C \cap C^\perp = \langle z_1, \ldots, z_s \rangle$$

and

$$D^\perp_s = \langle z_1, \ldots, z_s, z_{s+1}, x_{s+1}, \ldots, z_n, x_n \rangle.$$

Lemma 3.3. An $\mathbb{F}_q$-linear $[[n, k, r > 0, d \geq 2]]_q$ Clifford subsystem code exactly pure to 1 can be punctured to an $\mathbb{F}_q$-linear $[[n-1, k, r-1, \geq d]]_q$ code.

Proof. As mentioned above, we can associate with the subsystem code two classical codes $C, D \subseteq \mathbb{F}_q^n$. Two cases arise depending on $\mathrm{swt}(D)$.

(i) If $\mathrm{swt}(D) = 1$, then without loss of generality we can assume that $\mathrm{swt}(z_1) = 1$. Further, $z_1$ can be taken to be of the form $(1, 0, \ldots, 0, a, 0, \ldots, 0)$, and for $i \neq 1$, owing to the $\mathbb{F}_q$-linearity of the codes we can choose every $x_i, z_i$ to be of the form $(0, a_2, \ldots, a_n | b_1, b_2, \ldots, b_n)$. Further, as $x_i, z_i$ must satisfy the orthogonality relations with $z_1$ viz. $\langle z_1 | z_i \rangle_s = 0 = \langle z_1 | x_i \rangle_s$, for $i > 1$ we can choose $x_i, z_i$ to be of the form $(0, a_2, \ldots, a_n | 0, b_2, \ldots, b_n)$. It follows that owing to the form of $x_i$ and $z_i$ puncturing the first and $n+1$th coordinate will not alter these orthogonality relations, in particular $\langle \rho(x_i) | \rho(z_i) \rangle_s \neq 0$ for $s+1 \leq i \leq n$.

Letting $\rho(x_i) = x'_i$, $\rho(z_i) = z'_i$ and observing that $\rho(z_1) = (0, \ldots, 0 | 0, \ldots, 0)$, we see that the code $\rho(C) = \langle z'_2, \ldots, z'_s, z'_{s+1}, x'_{s+1}, \ldots, z'_{s+r}, x'_{s+r} \rangle$. Denoting by $D_p = \rho(C) \cap \rho(C)^\perp$, it is immediate that $D_p$ is generated by $\{z'_2, \ldots, z'_s\}$ while $D_p^\perp_s = \langle z'_2, \ldots, z'_s, z'_{s+1}, x'_{s+1}, \ldots, z'_n, x'_n \rangle$. Hence, $\rho(C)$ defines an $[[n-1, k, r, \mathrm{swt}(D^\perp_s \setminus \rho(C))]_q$ code.

Next we show that $\mathrm{swt}(D^\perp_s \setminus \rho(C)) \geq d$. Let $u = (a_2, \ldots, a_n | b_2, \ldots, b_n)$ be in $D^\perp_s \setminus \rho(C)$, then we can easily verify that $(0, a_2, \ldots, a_n | 0, b_2, \ldots, b_n)$ is orthogonal to all $z_i$, $1 \leq i \leq s$ and hence it is in $D^\perp_s$. It cannot be in $C$ as that would imply that $u$ is in $\rho(C)$. However, $\mathrm{swt}(D^\perp_s \setminus C) \geq d$. Therefore, $\mathrm{swt}(u) \geq d$, and $\rho(C)$ defines an $[[n-1, k, r, \geq d]]_q$ code. By choosing $C' = \langle z'_2, \ldots, z'_s, z'_{s+1}, x'_{s+1}, \ldots, z'_{s+r}, x'_{s+r} \rangle$, we can conclude that there exists an $[[n-1, k, r-1, \geq d]]_q$ code. Alternatively, apply theorem 16 in Aly et al. (2006).

(ii) If $\mathrm{swt}(D) > 1$, then we can assume that $\mathrm{swt}(z_{s+1}) = 1$ and form the code $C' = \langle z_1, \ldots, z_s, z_{s+1}, x_{s+2}, \ldots, z_{s+r}, x_{s+r} \rangle$. It is clear that $C'$ defines an $[[n,k,r-1,d]]_q$ code that is pure to 1 with $\mathrm{swt}(C' \cap C'^\perp) = 1$. However, this is just the previous case, from which we can conclude that there exists an $[[n-1, k, r-1, \geq d]]_q$ code.
Lemma 3.3 allows us to establish a bound for distance 2 codes which can then be used to prove the bound for arbitrary distances.

**Lemma 3.4.** An impure $\mathbb{F}_q$-linear $[[n, k, r, d=2]]_q$ Clifford subsystem code satisfies
\[
k + r \leq n - 2d + 2.
\]

**Proof.** Suppose that there exists an $\mathbb{F}_q$-linear $[[n,k,r,d=2]]$ impure subsystem code such that $k + r > n - 2d + 2$; in particular, this code must be pure to 1. By lemma 3.3, it can be punctured to give an $[[n-1, k, r-1, \geq d]]_2$ subsystem code. If this code is pure, then $k + r - 1 \leq n - 1 - 2d + 2$ holds, contradicting our assumption $k + r > n - 2d + 2$; hence, the resulting code is once again impure and pure to 1.

Now we repeatedly apply lemma 3.3 to puncture the shortened codes until we get an $[[n-r, k, 0, \geq d]]_q$ subsystem code. However, this is a stabilizer code that must obey the Singleton bound $k \leq n - r - 2d + 2$, contradicting our initial assumption $k + r > n - 2d + 2$. Therefore, we can conclude that $k + r \leq n - 2d + 2$.

If the codes are of distance greater than 2, then we puncture the code until either it has distance 2 or it is a pure code. The following result tells us how the parameters of the subsystem codes vary on puncturing.

**Lemma 3.5.** An impure $\mathbb{F}_q$-linear $[[n, k, r, d \geq 3]]_q$ Clifford subsystem code exactly pure to $d' \geq 2$ implies the existence of an $\mathbb{F}_q$-linear $[[n-1, k, r+1, \geq d-1]]_q$ subsystem code.

**Proof.** Recall that the existence of an $[[n, k, r, d \geq 3]]_q$ subsystem code implies the existence of $\mathbb{F}_q$-linear codes $C$ and $D$ such that
\[
C = \langle z_1, \ldots, z_s, z_{s+1}, x_{s+1}, \ldots, z_{s+r}, x_{s+r} \rangle,
\]
with $s = n - k - r$, and $D = C \cap C^\perp$ (see above).

The stabilizer code defined by $D$ satisfies $k + r = n - s \leq n - 2d' + 2$, or equivalently $s \geq 2d' - 2$; it follows that $s \geq 2$, since $d > d' \geq 2$. Without loss of generality, we can take $z_1$ to be of the form $(1, a_2, \ldots, a_n | b_1, b_2, \ldots, b_n)$ for if no such codeword exists in $D$, then $(0, 0, \ldots, 0 | 1, 0, \ldots, 0)$ is contained in $D^\perp$, contradicting the fact that $\text{swt}(D^\perp) \geq 2$. Consequently, we can choose $z_2$ in $D$ to be of the form $(0, c_2, \ldots, c_n | 1, d_2, \ldots, d_n)$, and we may further assume that $b_1 = 0$ in $z_1$.

The form of $z_1$ and $z_2$ allows us to assume that any remaining generator of $C$ is of the form $(0, u_2, \ldots, u_n | 0, v_2, \ldots, v_n)$.

Let $\rho$ be the map defined by puncturing the first and $(n+1)$th coordinate of a vector in $C$. Define for all $i$ the punctured vectors $x'_i = \rho(x_i)$ and $z'_i = \rho(z_i)$. Then one easily checks that $\langle \rho(x_i) | \rho(x_j) \rangle s = 0 = \langle \rho(z_i) | \rho(z_j) \rangle s$ for all indices $i$ and $j$, and $\langle \rho(x_i) | \rho(z_j) \rangle s = \delta_{i,j}$ if $i \geq s + 1$ or $j \geq 3$, and that $\langle \rho(z_1) | \rho(z_2) \rangle s = -1$.

Let us look at the punctured code $\rho(C)$,
\[
\rho(C) = \langle z'_3, \ldots, z'_s, z'_{s+1}, x'_{s+1}, \ldots, z'_{s+r}, x'_{s+r} | z'_1, z'_2 \rangle.
\]

Since $\langle \rho(z_1) | \rho(z_2) \rangle s = -1$ we have $D_\rho = \rho(C) \cap \rho(C)^\perp = \langle z'_3, \ldots, z'_s \rangle$, whence $|D_\rho| = |D|/q^2$. As $\text{swt}(C) \geq 2$, it follows that $|\rho(C)| = |C|$. Thus, $\rho(C)$ defines an $[[n-1, k, r+1, \text{swt}(D_\rho) \backslash \rho(C)]]_q$ subsystem code.
Recall that the code $D$ is generated by $s \geq 2$ vectors; we will next show that our assumptions actually force $s \geq 3$. Indeed, if $s = 2$, then $|D| = q^2$ and $|D^\perp| = q^{2n-2}$. Under the assumption $\text{swt}(D^\perp) \geq 2$, it follows that $|\rho(D^\perp)| = |D^\perp| = q^{2n-2}$.

However, as $\rho(D^\perp) \subseteq \mathbb{F}_q^{2n-2}$ this implies that $\rho(D^\perp) = \mathbb{F}_q^{2n-2}$. Since $\mathbb{F}_q^{2n-2}$ has $2n-2$ independent codewords of symplectic weight 1, $D^\perp$ must have $2n-2$ independent codewords of symplectic weight 2. However, this contradicts our assumptions on the minimum distance of the subsystem code.

(i) If $C$ is a proper subspace of $D^\perp$, then the minimum distance $d$ is given by $d = \text{swt}(D^\perp \setminus C) \geq 3$; thus, the weight 2 vectors must all be contained in $C$, which shows that $|C| = q^{2n-3} = |D|$, contradicting $|C| < |D^\perp|$.

(ii) If $C = D^\perp$, then the minimum distance is given by $d = \text{swt}(D^\perp) = 2$, contradicting our assumption that $d \geq 3$.

Thus, from now on, we can assume that $s \geq 3$.

Before bounding the minimum distance of the punctured subsystem code, we are going to show that $D^\perp_{\rho} = \rho(D^\perp)$. Let $w = (u_1, u_2, \ldots, u_n|v_1, v_2, \ldots, v_n)$ be a vector in $D^\perp$. For $3 \leq i \leq s$, the vectors $z_i$ are of the form $v = (0, a_2, \ldots, a_n, 0, b_2, \ldots, b_n)$; thus, it follows from $\langle w|z_i \rangle_s = 0$ that $\langle \rho(w)|z_i \rangle_s = 0$. Hence $\rho(w)$ is in $D^\perp_{\rho}$, which implies $\rho(D^\perp) \subseteq D^\perp_{\rho}$. We have $|D^\perp_{\rho}| = q^{2n-2}/|D_p| = q^r/|D| = |D^\perp|$, and we note that $|D^\perp_{\rho}| = |\rho(D^\perp)|$, because $\text{swt}(D^\perp) \geq 2$; hence, $D^\perp_{\rho} = \rho(D^\perp)$.

Let $w' = (u_2, \ldots, u_n|v_2, \ldots, v_n)$ be an arbitrary vector in $\rho(D^\perp) \setminus \rho(C)$. It follows that there exist some $\alpha, \beta$ in $\mathbb{F}_q$ such that $w = (\alpha, u_2, \ldots, u_n|\beta, v_2, \ldots, v_n)$ is in $D^\perp$; it is clear that $w$ cannot be in $C$, since then $\rho(w) = w'$ would be in $\rho(C)$; hence, $\text{swt}(w) \geq d$. It immediately follows that $\text{swt}(D^\perp_{\rho} \setminus \rho(C)) \geq d - 1$. Hence $\rho(C)$ defines an $[[n-1, k, r+1, \geq d-1]] q$ subsystem code.

Now we are ready to prove the upper bound for an arbitrary subsystem code. Essentially, we reduce it to a pure code or distance 2 code by repeated puncturing and bound the parameters by carefully tracing the changes.

**Theorem 3.6.** An $\mathbb{F}_q$-linear $[[n, k, r, d \geq 2]] q$ Clifford subsystem code satisfies

$$k + r \leq n-2d + 2. \quad (3.1)$$

**Proof.** The bound holds for all pure codes (see Aly et al. 2006). So assume that the code is impure. If $d=2$, then the relation holds by lemma 3.4; so let $d \geq 3$. If the code is exactly pure to 1, then it can be punctured using lemma 3.3 to give an $[[n-1, k, r-1, d' = d]] q$ code, otherwise it can be punctured using lemma 3.5 to obtain an $[[n-1, k, r+1, d' \geq d-1]] q$ code. If the punctured code is pure, then it follows that either $k + r - 1 \leq n - 1 - 2d + 2$ or $k + r + 1 \leq n - 1 - 2d' + 2 \leq n - 1 - 2(d-1) + 2$ holds; in both cases, these inequalities imply that $k + r \leq n - 2d + 2$.

If the resulting code is impure, then if it is exactly pure to 1, we puncture the code again using lemma 3.3, if not we puncture using lemma 3.5, until we get a pure code or a code with distance 2. Assume that we punctured $i$ times using lemma 3.3 and $j$ times using lemma 3.5, then the resulting code is an $[[n-i-j, k, r+j-i, d' \geq d-j]] q$ subsystem code. Since pure subsystem codes
and distance 2 subsystem codes satisfy
\[ k + r + j - i \leq n - i - j - 2d' + 2 \leq n - i - j - 2(d - j) + 2, \]
it follows that \( k + r \leq n - 2d + 2 \) holds.

When the subsystem codes are over a prime alphabet, this bound holds for all codes over that alphabet. In the more general case where the code is not linear, numerical evidence indicates that it is unlikely that the additive subsystem codes have a different bound. We have shown that a large class of impure codes already satisfied this bound. This prompts the following conjecture.

**Conjecture 3.7.** Any \( [[n, k, r, d]]_q \) Clifford subsystem code satisfies \( k + r \leq n - 2d + 2 \).

(b) **Can subsystem codes improve upon MDS stabilizer codes?**

In this subsection, we compare stabilizer codes with subsystem codes. We first need to establish the criteria for the comparison, since subsystem codes cannot be universally better than stabilizer codes. For example, it is known that a subsystem code can be converted to a stabilizer code (Poulin 2005; Kribs et al. 2006). See also lemma 10 in Aly et al. (2006) for a simple proof to convert an \( [[n, k, r, d]]_q \) code to an \( [[n, k, d]]_q \) code. This implies that no \( [[n, k, r, d]]_q \) subsystem code can beat an optimal \( [[n, k, d']]_q \) stabilizer code in terms of minimum distance, as \( d' \geq d \). One of the attractive features of subsystem codes is a potential reduction of the number of syndrome measurements, and we use this criterion as the basis for our comparison.

First, we must highlight a subtle point on the required number of syndrome bits for an \( \mathbb{F}_q \)-linear \( [[n, k, d]]_q \) code. A complete decoder will require \( n - k \) syndrome bits. Complete decoders are also optimal decoders. A bounded distance decoder, on the other hand, can potentially decode with fewer syndrome bits. Bounded distance decoders typically decode up to \( \lfloor (d - 1)/2 \rfloor \). However, to the best of our knowledge, except for the lookup table decoding method, all bounded distance decoders also require \( n - k \) syndrome bits. As the complexity of decoding using a lookup table increases exponentially in \( n - k \), it is highly impractical for long lengths. We therefore assume that for practical purposes we need \( n - k \) syndrome bits.

Similarly, for an \( \mathbb{F}_q \)-linear \( [[n, k, r, d]]_q \) subsystem code, a complete decoder will require \( n - k - r \) syndrome measurements, as is shown in appendix A. We are not aware of any quantum code, stabilizer or subsystem, for which there exists a bounded distance decoder that uses less than \( n - k - r \) syndrome measurements to perform bounded distance decoding. The work by Poulin (2005) prompts the following question: given an optimal \( [[k + 2d - 2, k, d]]_q \) MDS stabilizer code, is it possible to find an \( [[n, k, r, d]]_q \) subsystem code that uses fewer syndrome measurements?

There exist numerous known examples of subsystem codes that improve upon non-optimal stabilizer codes. The fact that the stabilizer code is assumed to be optimal makes this question interesting. The Singleton bound \( k + r \leq n - 2d + 2 \) of an \( \mathbb{F}_q \)-linear \( [[n, k, r, d]]_q \) subsystem code implies that the number \( n - k - r \) of syndrome measurements is bounded by \( n - k - r \geq 2d - 2 \); thus, for fixed minimum distance \( d \), there exists a trade-off between the dimension \( k \) and the difference \( n - r \) between the length and number of gauge qudits.
Corollary 3.8. Under complete decoding, an $\mathbb{F}_q$-linear $[[n, k, r, d \geq 2]]_q$ Clifford subsystem code cannot use fewer syndrome measurements than an $\mathbb{F}_q$-linear $[[k + 2d - 2, k, d]]_q$ stabilizer code.

Proof. Seeking a contradiction, we assume that there exists an $[[n, k, r, d]]_q$ subsystem code that requires fewer syndrome measurements than the optimal $[[k + 2d - 2, k, d]]_q$ MDS stabilizer code. In other words, the number of syndrome measurements yields the inequality $k + 2d - 2 - k > n - k - r$, which is equivalent to $k + r > n - 2d + 2$, but this contradicts the Singleton bound.

Poulin (2005) showed by exhaustive computer search that a $[[5, 1, r > 0, 3]]_2$ subsystem code does not exist. The above result confirms his computer search and shows further that not even allowing longer lengths and more gauge qudits can help in reducing the number of syndrome measurements. In fact, we conjecture that corollary 3.8 holds for bounded distance decoders also.

We wish to caution the reader that gains in error recovery cannot be quantified purely by the number of syndrome measurements. In practice, more complex measures such as the simplicity of the decoding algorithm or the resulting threshold in fault-tolerant quantum computing are more relevant. The drawback is that the comparison of large classes of codes becomes unwieldy when such complex criteria are used.

4. Subsystem codes on a lattice

Bacon (2006) gave the first family of subsystem codes generalizing the ideas of Shor’s $[[9, 1, 3]]_2$ code. Recently, he and Casaccino gave another construction that generalizes this further by considering a pair of classical codes (Bacon & Casaccino 2006). We show that this method is a special case of theorem 2.1. Since this construction is not limited to binary codes and our proofs remain essentially the same, we will immediately discuss a generalization to non-binary alphabets.

Theorem 4.1. For $i \in \{1, 2\}$, let $C_i \subseteq \mathbb{F}_q^{n_i}$ be $\mathbb{F}_q$-linear codes with the parameters $[n_i, k_i, d_i]_q$. Then there exists a Clifford subsystem code with the parameters

$$[[n_1 n_2, k_1 k_2, (n_1 - k_1)(n_2 - k_2), \min\{d_1, d_2\}]]_q,$$

that is pure to $d_q = \min\{d_1^\perp, d_2^\perp\}$, where $d_i^\perp$ denotes the minimum distance of $C_i^\perp$.

Proof. Let $C$ be the classical linear code given by $C = (\mathbb{F}_q^{n_1} \otimes C_2^\perp) \times (C_1^\perp \otimes \mathbb{F}_q^{n_2})$. Then $\dim C = n_1(n_2 - k_2) + n_2(n_1 - k_1)$ and $\swt(C \setminus \{0\}) \geq \min\{d_1^\perp, d_2^\perp\}$. The symplectic dual of $C$ is given by

$$C^\perp = (C_1^\perp \otimes \mathbb{F}_q^{n_2}) \perp \times (\mathbb{F}_q^{n_1} \otimes C_2^\perp) \perp = (C_1 \otimes \mathbb{F}_q^{n_2}) \times (\mathbb{F}_q^{n_1} \otimes C_2).$$

We have $\dim C^\perp = n_1 n_2 + n_1 k_2$. The code $D = C \cap C^\perp$ is given by

$$D = (\left(\mathbb{F}_q^{n_1} \otimes C_2^\perp\right) \times (C_1^\perp \otimes \mathbb{F}_q^{n_2})) \cap ((C_1 \otimes \mathbb{F}_q^{n_2}) \times (\mathbb{F}_q^{n_1} \otimes C_2))$$

$$= \left((\mathbb{F}_q^{n_1} \otimes C_2^\perp) \times (C_1 \otimes \mathbb{F}_q^{n_2})\right) \times ((C_1^\perp \otimes \mathbb{F}_q^{n_2}) \cap (\mathbb{F}_q^{n_1} \otimes C_2))$$

$$= (C_1 \otimes C_2^\perp) \times (C_1^\perp \otimes C_2).$$

and \( \dim D = k_1(n_2 - k_2) + k_2(n_1 - k_1) \). It follows that \( \dim C - \dim D = 2(n_1 - k_1)(n_2 - k_2) \) and \( \dim C^\perp - \dim D = 2k_1k_2 \). Using corollary 2.2, we can get a subsystem code with the parameters

\[
[[n_1n_2, k_1k_2, (n_1 - k_1)(n_2 - k_2), \quad d = \text{swt}(D^\perp \backslash C)]],
\]

that is pure to \( d_p = \min\{d_1^+, d_2^+\} \). It remains to show that \( d = \min\{d_1, d_2\} \).

Since \( D = (C_1 \otimes C_2^\perp) \times (C_1^\perp \otimes C_2) \), we have

\[
D^\perp, = \left( (C_1 \otimes F_q^{n_1}) \oplus (F_q^{n_1} \otimes C_2^\perp) \right) \times \left( (F_q^{n_1} \otimes C_2) \oplus (C_1^\perp \otimes F_q^{n_2}) \right).
\]

In the last equality, we used the fact that vectors \( u_1 \otimes u_2 \) and \( v_1 \otimes v_2 \) are orthogonal if and only if \( u_1 \perp v_1 \) or \( u_2 \perp v_2 \).

For \( i \in \{1,2\} \), let \( G_i \) and \( H_i \), respectively, denote the generator and parity check matrix of the code \( C_i \). Without loss of generality, we may assume that these matrices are in standard form

\[
H_i = \begin{bmatrix} I_{n_i-ki} & P_i \end{bmatrix} \quad \text{and} \quad G_i = \begin{bmatrix} -P_i^t & I_{ki} \end{bmatrix},
\]

where \( P_i^t \) is the transpose of \( P_i \). Let \( H_i^f = [0 \quad I_{ki}] \). Using these notations, the generator matrices of \( C \) and \( D^\perp, \) can be written as

\[
G_C = \begin{bmatrix} I_{n_1} \otimes H_2 & 0 \\ 0 & H_1 \otimes I_{n_2} \end{bmatrix} \quad \text{and} \quad G_{D^\perp,} = \begin{bmatrix} G_1 \otimes H_2^f & 0 \\ I_{n_1} \otimes H_2 & 0 \\ 0 & H_1^f \otimes G_2 \end{bmatrix}.
\]

It follows that the minimum distance \( d \) is given by

\[
\text{swt}(D^\perp \backslash C) = \min\left\{ \text{wt}\left( \begin{bmatrix} G_1 \otimes H_2^f \\ H_1 \otimes I_{n_2} \end{bmatrix} \right) \right\}, \text{wt}\left( \begin{bmatrix} H_1^f \otimes G_2 \\ H_1 \otimes I_{n_2} \end{bmatrix} \right)\}
\]

Let us compute

\[
\text{wt}\left( \begin{bmatrix} H_1^f \otimes G_2 \\ H_1 \otimes I_{n_2} \end{bmatrix} \right)\).
\]

If minimum weight codeword is present in \( D^\perp \backslash C \), it must be expressed as a linear combination of at least one row from \( [H_1^f \otimes G_2] \), otherwise the codeword is entirely in \( C \). Recall that \( H_1 = [I_{n_1-ki} \quad P_i] \) and \( H_1^f = [0 \quad I_{ki}] \). Letting \( P_1 = (p_{ij}) \), we
can write

\[
\begin{pmatrix}
H_1^c \otimes G_2 \\
H_1 \otimes I_{n_2}
\end{pmatrix} = \begin{bmatrix}
0 & 0 & \ldots & 0 & G_2 & 0 \\
0 & 0 & \ldots & 0 & 0 & G_2 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0 & 0 & \ldots & \ldots & G_2 \\
I_{n_2} & 0 & \ldots & 0 & p_{11}I_{n_2} & \ldots & \ldots & p_{1k_1}I_{n_2} \\
0 & I_{n_2} & \ldots & p_{21}I_{n_2} & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & I_{n_2} & p_{(n_1-k_1)1}I_{n_2} & \ldots & \ldots & \ldots & p_{(n_1-k_1)k_1}I_{n_2}
\end{bmatrix}
\]

Now observe that any row below the line in the above matrix can have a weight of only one in each of the last \( k_1 \) blocks of size \( n_2 \). And any linear combination of them involving less than \( d_2 \) and at least one generator from the rows above must have a weight \( \geq d_2 \). On the other hand, if there are more than \( d_2 \) rows involved, then the first \( n_2(n_1-k_1) \) columns will have a weight \( \geq d_2 \). Thus, in either case, the weight of an element that involves a generator from \([H_1^c \otimes G_2]\) must have a weight \( \geq d_2 \). On the other hand, the minimum weight of the span of \([H_1^c \otimes G_2]\) is \( \text{wt}(C_2) = d_2 \), from which we can conclude that

\[
\text{wt}\left(\langle H_1^c \otimes G_2 \rangle \setminus \langle H_1 \otimes I_{n_2} \rangle\right) = d_2.
\]

Owing to the symmetry in the code, we can argue that

\[
\text{wt}\left(\langle I_{n_1} \otimes H_2 \rangle \setminus \langle G_1 \otimes H_2^c \rangle\right) = d_1
\]

and consequently \( d = \min\{d_1, d_2\} \), which proves the theorem.

\[(a)\] \textit{Bacon–Shor codes}

Bacon (2006) proposed one of the first families of subsystem codes based on square lattices. A trivial modification using rectangular lattices instead of square ones gives the following codes (see also Bacon & Casacino 2006). The relevance of these codes will be seen later in §5. Using the same notation as in theorem 4.1, let \( G_i = [1, \ldots, 1]_{1 \times i} \) and \( H_i \) be the matrix defined as

\[
H_i = \begin{bmatrix}
1 & 1 \\
1 & 1 \\
\vdots & \vdots \\
1 & 1 \\
1 & 1
\end{bmatrix}_{i-1 \times i}
\]
and $C$, the additive code generated by the following matrix.

$$G = \begin{bmatrix}
I_{n_1} \otimes H_{n_2} & 0 \\
0 & H_{n_1} \otimes I_{n_2}
\end{bmatrix}.$$ 

Observe that $G_i$ generates an $[i,1,i]_q$ code with distance $i$. By theorem 4.1, $G_{n_1}$ and $G_{n_2}$ will give us the following family of codes.

**Corollary 4.2.** There exist $[[n_1 n_2, 1, (n_1 - 1)(n_2 - 1), \min\{n_1, n_2\}]]_q$ Clifford subsystem codes.

### 5. Subsystem codes and packing

We investigate whether subsystem codes lead to better codes with respect to the quantum Hamming bound. Since the early days of quantum codes, it has been recognized that the degeneracy of quantum codes could lead to a more efficient quantum code and allow for a much more compact packing of the subspaces in the Hilbert space. However, so far it has not been shown for stabilizer codes. We can derive a similar bound for subsystem codes. Aly et al. (2006) showed the following theorem for pure subsystem codes.

**Theorem 5.1.** A pure $((n, K, R, d))_q$ Clifford subsystem code satisfies

$$\sum_{j=0}^{[(d-1)/2]} \binom{n}{j} (q^2 - 1)^j \leq q^n / KR.$$  (5.1)

It is natural to ask whether impure subsystem codes also satisfy this bound. We show that they do not do so by giving an explicit counterexample. This counterexample comes from the codes proposed by Bacon (2006). Recall that the Bacon–Shor codes are $[[n^2, 1, (n-1)^2, n]]_2$ subsystem codes. The $[[9, 1, 4, 3]]_2$ is an interesting code. We can check whether it satisfies the Singleton bound for subsystem codes as

$$k + r = 1 + 4 = n - 2d + 2 = 9 - 6 + 2.$$ 

So it is an optimal code. More interestingly, substituting the parameters of the $[[9, 1, 4, 3]]_2$ Bacon–Shor code in the above inequality, we get

$$\sum_{j=0}^{1} \binom{9}{j} 3^j = 28 > 2^9 - 5 = 16.$$ 

Therefore, the $[[9, 1, 4, 3]]_2$ Bacon–Shor code beats the quantum Hamming bound for the pure subsystem codes proving the following result.

**Theorem 5.2.** There exist impure $((n, K, R, d))_q$ Clifford subsystem codes that do not satisfy

$$\sum_{j=0}^{[(d-1)/2]} \binom{n}{j} (q^2 - 1)^j \leq q^n / KR.$$
An obvious question is why some impure codes can pack more efficiently than the pure codes. Let us understand this by looking at the $[[9, 1, 4, 3]]_2$ code a little more closely. This code encodes information into a subspace $Q$ where $\dim Q = 2^{k+r} = 2^5$. As it is a subsystem code, $Q$ can be decomposed as $Q = A \otimes B$, with $\dim A = 2^k = 2$ and $\dim B = 2^r = 2^4$. In a pure single error-correcting code, all single errors must take the code space into orthogonal subspaces. In an impure code this is not required; two or more distinct errors can take the code space to the same orthogonal space. In the Bacon–Shor code, a phase flip error on any of the first three qubits will take the code space to the same orthogonal subspace and owing to this we cannot distinguish between these errors. However, it is not a problem because we can restore the code space with respect to $A$, even though we cannot restore $B$. Thus, instead of requiring nine orthogonal subspaces as in a pure code, we only require three orthogonal subspaces to correct for any single phase flip error. Considering the bit flip errors and the combinations, we need only nine orthogonal subspaces. Thus, with the original code space, this means we need to pack ten $2^5$-dimensional subspaces in the $2^n = 2^9$ dimensional ambient space, which is achievable as $10 \cdot 2^5 < 2^9$.

More generally, in a sense, degeneracy allows distinct errors to share the same orthogonal subspace and thus pack more efficiently. It must be pointed out though that this better packing is attained at the cost of $r$ gauge qudits compared with a stabilizer code.

In fact, there exists another code among the Bacon–Shor codes which also beats the Hamming bound for the subsystem codes. This is the $[[16, 1, 9, 4]]_2$ code. The family of codes given in corollary 4.2 provides us with $[[[12, 1, 6, 3]]_2$ yet another example of a code that beats the quantum Hamming bound like the $[[9, 1, 4, 3]]_2$ code. We can check that

$$\sum_{j=0}^{1} \binom{12}{j} 3^j = 37 > 2^{12-1-6} = 2^5 = 32.$$  

However, note that unlike $[[9, 1, 4, 3]]_2$ this code does not meet the Singleton bound for pure subsystem codes as $6 + 1 < 12 - 6 + 2$. Naturally, we can ask whether there is a systematic method to construct codes that beat the quantum Hamming bound. At the moment we do not know. It appears unlikely that there exist long codes that beat the quantum Hamming bound.

6. Conclusion

We have proved that any $\mathbb{F}_q$-linear $[[n, k, r, d]]_q$ Clifford subsystem code obeys the Singleton bound $k + r \leq n - 2d + 2$. Furthermore, we have shown earlier that pure Clifford subsystem codes satisfy this bound as well. Our results provide much evidence for the conjecture that the Singleton bound holds for arbitrary subsystem codes.

Pure Clifford subsystem codes obey the Hamming (or sphere packing) bound. In this paper, we have shown the amazing fact that there exist impure Clifford subsystem codes beating the Hamming bound. This is the first illustration of a case when impure codes pack more efficiently than their pure counterparts. One example of a code beating the Hamming bound is provided by the $[[9, 1, 4, 3]]_2$ code.
Bacon–Shor code; this remarkable example also illustrates the following noteworthy facts.

(i) The [[9, 1, 4, 3]]\textsubscript{2} code requires 9−1−4=4 syndrome measurements just like the perfect [[5, 1, 3]]\textsubscript{2} code.

(ii) Since $k+r \leq n−2d+2$ for all prime alphabet codes, [[9, 1, 4, 3]]\textsubscript{2} code is also an optimal subsystem code. This is interesting because the underlying classical codes are not MDS. In MDS stabilizer codes, the underlying classical codes are required to be MDS codes.

(iii) The Bacon–Shor code is also impure. So unlike MDS stabilizer codes that must be pure, MDS subsystem codes can be impure.

(iv) The maximal length of a $q$-ary stabilizer MDS code is $2q^2−2$ (Ketkar et al. 2006), whereas for subsystem codes it is larger as the [[9, 1, 4, 3]]\textsubscript{2} code indicates.

The implication of (ii)–(iv) is that optimal subsystem codes can be derived from suboptimal classical codes, unlike stabilizer codes.

We conclude with a few open questions that seem to be interesting.

(i) Do arbitrary [[n, k, r, d]]\textsubscript{q} subsystem codes also satisfy $k+r \leq n−2d+2$?

(ii) Is the Hamming bound for subsystem codes obeyed asymptotically?

(iii) What is the maximal length of MDS subsystem codes?

The second question is motivated by the fact that binary stabilizer codes obey the quantum Hamming bound asymptotically (see corollary 2 in Ashikhmin & Litsyn (1999)).

Part of this paper was presented at the BIRS workshop Operator Structures in Quantum Information Theory, Banff, Canada, 2007 and at the I^2Lab Workshop: Frontiers in Quantum and Biological Information Processing, Orlando, Florida 2006. We thank the organizers, particularly David Kribs, Mary Beth Ruskai and Pawel Wocjan, for inviting us to these fruitful workshops. We thank the referees for their comments which helped improve the presentation of the paper. This research was supported by NSF CAREER award CCF 0347310 and NSF grant CCF 0622201.

Appendix A. Syndrome measurement for non-binary $\mathbb{F}_q$-linear codes.

Decoding of non-binary quantum codes has not been studied as well as binary codes. Encoding of $\mathbb{F}_q$-linear non-binary quantum codes was investigated in Grassl et al. (2003). The authors suggest that the decoder is simply the encoder running backwards. While that may be reasonable in quantum communication, it is not preferable in the case of quantum computation.

Here, we give a method that allows us to measure the syndrome for $\mathbb{F}_q$-linear non-binary quantum codes. We also show that an $\mathbb{F}_q$-linear [[n, k, r, d]]\textsubscript{q} code requires $n−k−r$ syndrome measurements. However, first we need the definition of the following non-binary gates (see Grassl et al. (2003)).

(i) $X(a)|x⟩ = |x+a⟩$

(ii) $Z(b)|x⟩ = ω^{tr_{q/p}(b)}|x⟩$, $ω = e^{2π/p}$

(iii) $M(c)|x⟩ = |cx⟩$, $c ∈ \mathbb{F}_q^∗$

(iv) \( F|x\rangle = (1/\sqrt{q}) \sum_{y \in \mathbb{F}_q} \omega^{1 \epsilon_{xy}(xy)} |y\rangle \) and

(v) \( A|x\rangle |y\rangle = |x\rangle |x+y\rangle \).

Graphically, these gates are represented below.

\[
\begin{array}{c}
\begin{array}{c}
X(a) \\
\hline
Z(b)
\end{array} \\
\hline
\begin{array}{c}
F \\
\hline
\end{array}
\end{array}
\]

(i) (ii) (iii) (iv) (v)

Consider the following circuit.

\[
\begin{array}{c}
|a\rangle \\
\hline
|y\rangle \\
\hline
\begin{array}{c}
g_x^{-1} \oplus \ \ g_x
\end{array}
\end{array}
\]

\[|y + ag_z\rangle\]

Alternatively, this circuit maps \(|a\rangle |x\rangle\) to \(|a\rangle X(\alpha g_z) |y\rangle\). Observe that this circuit effectively applies \(X(\alpha g_z)\) on the second qudit. Using the linearity, we can analyse the following circuit. The normalization constants are ignored in the following discussion.

\[
\begin{array}{c}
|0\rangle \\
\hline
|y\rangle \\
\hline
\begin{array}{c}
g_x^{-1} \oplus \ \ g_x
\end{array}
\end{array}
\]

\[\sum_{\alpha \in \mathbb{F}_q} |\alpha\rangle |y + \alpha g_z\rangle\]

The above circuit maps \(|0\rangle |y\rangle\) to \(\sum_{\alpha \in \mathbb{F}_q} |\alpha\rangle X(\alpha g_z) |y\rangle\). Using the fact that \(FX(b)F^\dagger = Z(b)\), we can show that the following circuit maps \(|b\rangle |y\rangle\) to \(|b\rangle Z(bg_z) |y\rangle\).

\[
\begin{array}{c}
|b\rangle \\
\hline
|y\rangle \\
\hline
\begin{array}{c}
F^\dagger \\
\hline
\begin{array}{c}
g_x^{-1} \oplus \ \ g_x
\end{array}
\end{array} \\
\hline
\begin{array}{c}
F \\
\hline
\end{array}
\end{array}
\]

\[Z(bg_z) |y\rangle\]

If we wanted to apply a general operator \(X(\alpha g_z)Z(\alpha g_z)\) to the second qudit conditioned on the first one, then we can combine the previous circuits as follows.

\[
\begin{array}{c}
|a\rangle \\
\hline
|y\rangle \\
\hline
\begin{array}{c}
g_x^{-1} \oplus \ \ g_x
\end{array} \\
\hline
\begin{array}{c}
F \\
\hline
\begin{array}{c}
g_x^{-1} \oplus \ \ g_x
\end{array}
\end{array}
\end{array}
\]

\[X(\alpha g_z)Z(\alpha g_z) |y\rangle\]

The above implementation is not optimal in terms of gates, but it will suffice for our purposes. Consider an \([[n, k, r, d]]_q\) code. Let \(E\) be an error in \(E\). If \(E\) is detectable, then \(E\) does not commute with some element(s) in the stabilizer of the code. Let

\[
g = (g_x|g_z) = (0, \ldots, 0, a_j, \ldots, a_n|0, \ldots, 0, b_j, \ldots, b_n) \in \mathbb{F}_q^{2n},
\]

where \((a_j, b_j) \neq (0, 0)\), be a generator of the stabilizer. Then, for all detectable errors that do not commute with a multiple of \(g\), the following circuit gives a
Let $X(g_z)Z(g_z)E = \omega^{tr_{q/\rho}(t)} EX(g_z)Z(g_z)$, where $X(g_z)Z(g_z)$ is a corresponding matrix representation of $g$. Then, we have $X(a g_z)Z(\alpha g_z)E = \omega^{tr_{q/\rho}(\alpha t)} EX(a g_z)Z(\alpha g_z)$, by lemma 5 in Ketkar et al. (2006). Thus, we can write

$$
\sum_{\alpha \in \mathbb{F}_q} \langle \alpha \rangle X(a g_z)Z(\alpha g_z)E|\psi\rangle = \sum_{\alpha \in \mathbb{F}_q} |\alpha\rangle \omega^{tr_{q/\rho}(\alpha t)} EX(a g_z)Z(\alpha g_z)|\psi\rangle
$$

where we have made use of the fact that $X(a g_z)Z(\alpha g_z)|\psi\rangle = |\psi\rangle$ as $X(a g_z)Z(\alpha g_z)$ is in the stabilizer. The final state is given by

$$
\sum_{\alpha \in \mathbb{F}_q} F^\dagger|\alpha\rangle X(a g_z)Z(\alpha g_z)E|\psi\rangle = \sum_{\alpha \in \mathbb{F}_q} F^\dagger|\alpha\rangle \omega^{tr_{q/\rho}(\alpha t)} E|\psi\rangle
$$

where the last equality follows from the property of the characters of $\mathbb{F}_q$. Next we observe that the error $\alpha E$, where $\alpha \in \mathbb{F}_q$ gives $|\alpha t\rangle$ on measurement. Strictly speaking, we refer to the preimage of $\alpha E$ in $E$. Hence, the syndrome qudit can take $q$ different values. Since every detectable error does not commute with some $\mathbb{F}_q$-multiple of a stabilizer generator, we have the following lemma on the necessary and sufficient number of syndrome measurements.

**Lemma A.1.** Given an $\mathbb{F}_q$-linear $[[n, k, r, d]]_q$ Clifford subsystem code, $n-k-r$ syndrome measurements are required for decoding it completely.

**Proof.** Let $g$ be a generator of the stabilizer of the subsystem code. By theorem 2.1 and lemma 3.2, for every generator $g$ there exists at least one detectable error that does not commute with $g$ but commutes with all the other generators. This error can
be detected only by measuring \( g \). Thus we need to measure all the generators of the stabilizer, equivalently \( n-k-r \) syndrome measurements must be performed.

Every correctable error takes the code space into a \( q^{k+r} \)-dimensional orthogonal subspace in the \( q^n \)-dimensional ambient space (see §2). Each of these errors will give a distinct syndrome. This implies that we can have \( q^{n-k-r} \) distinct syndromes. Since each syndrome measurement can have \( q \) possible outcomes and there are \( n-k-r \) generators, these measurements are sufficient for performing error correction.

This parallels the classical case where an \([n, k, d]_q\) code requires \( n-k \) syndrome bits. A subtle caveat must be issued to the reader. If we choose to perform bounded distance decoding, then it may be possible that the set of correctable errors can be distinguished by a smaller number of syndrome measurements. However, even in the case of (classical) bounded distance decoding, it is often the case that we need to measure all the syndrome bits.

**References**


