Generalized Concatenation for Quantum Codes

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1109/ISIT.2009.5205592">http://dx.doi.org/10.1109/ISIT.2009.5205592</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Citable link</td>
<td><a href="http://hdl.handle.net/1721.1/59346">http://hdl.handle.net/1721.1/59346</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher’s policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.</td>
</tr>
</tbody>
</table>
Abstract—We show how good quantum error-correcting codes can be constructed using generalized concatenation. The inner codes are quantum codes, the outer codes can be linear or nonlinear classical codes. Many new good codes are found, including both stabilizer codes as well as so-called nonadditive codes.

Index Terms—Generalized concatenated codes, quantum error correction, stabilizer codes, nonadditive codes

I. INTRODUCTION

The idea of concatenated codes, originally described by Forney in a seminal book in 1966 [10], was introduced to quantum computation three decades later [1], [12], [18], [19]. These concatenated quantum codes play a central role in fault tolerant quantum computation (FTQC) as well as in the study of constructing good degenerate quantum codes.

Blokh and Zyablov [3], followed by Zinoviev [25] introduced the concept of generalized concatenated codes. These codes improve the parameters of conventional concatenated codes for short block lengths [25] as well as their asymptotic performance [4]. Many good classical codes, linear and nonlinear, can be constructed using this method.

In [17] we, together with Smith and Smolin, have introduced generalized concatenated quantum codes (GCQC). It is shown that GCQC in its simplest form, i.e., two level concatenation, is already a powerful tool to produce good nonadditive quantum codes which outperform any stabilizer codes.

This paper focuses on the multilevel concatenation for quantum codes. We use the framework of stabilizer codes and the generalization to codeword stabilized (CWS) codes [6], [7] and union stabilizer codes [15], [16]. This allows us to use classical codes as outer codes. We further extend our multilevel concatenation technique to the case of different inner codes, which allows us to construct codes of various lengths.

II. BACKGROUND AND NOTATIONS

A quantum error-correcting code (QECC), denoted by $C = ([n, K, d])_q$, is a $K$-dimension subspace of the Hilbert space $\mathcal{H}_q^n$ of dimension $q^n$ that is the tensor product of $n$ complex Hilbert spaces $\mathcal{H}_q = \mathbb{C}^q$ of dimension $q$. Here we restrict $q = p^m$ to be a prime power. A QECC with minimum distance $d$ allows to correct arbitrary errors that affect at most $(d - 1)/2$ of the $n$ subsystems.

Most of the known QECCs are so-called stabilizer codes introduced independently by Gottesman [11] and Calderbank et al. [5]. The code is defined as the joint eigenspace of a set of commuting operators [11]. Equivalently, the code can be described by a classical additive code $C$ over $GF(q^2)$ that is self-orthogonal with respect to a symplectic inner product [2], [5]. Denoting the symplectic dual code by $C^*$, the minimum distance of the quantum code is given by

$$d = \min \{ \text{wgt}(c) : c \in C^* \setminus C \} \geq d_{\text{min}}(C^*)$$

If $d = d_{\text{min}}(C^*)$, the quantum code is called pure or non-degenerate. The corresponding stabilizer (or additive) code is denoted by $C = ([n, k, d])_q$ and has dimension $K = q^n$.

The first nonadditive code $([5, 6, 2])_2$ which has a higher dimension than any stabilizer code of the same length correcting one erasure can be explained as the union of six locally transformed copies of the stabilizer code $[[5, 0, 3]]_2$ (see [14], [22]). A one-dimensional stabilizer code $[[n, 0, d]]$ can also be described by a graph with $n$ vertices [23]. The corresponding quantum states are referred to as graph states. Combining locally equivalent graph states, the first one-error-correcting nonadditive quantum code $([9, 12, 3])_2$ with higher dimension than any stabilizer code has been found [24]. The theoretical ground for these codeword stabilized (CWS) quantum codes has been laid in [6], [7].

In [15], [16], the framework of union stabilizer codes has been introduced. Starting with a stabilizer code $C_0 = [[n, k, d_0]]_q$, a union stabilizer code is given by

$$C = \bigoplus_{t \in T_0} tC_0,$$

where $T_0 = \{t_1, \ldots, t_K\}$ is a set of tensor products of (generalized) Pauli matrices such that the spaces $t_tC_0$ are mutually orthogonal. Then the dimension of the union stabilizer code $C$ is $Kq^K$, and we will use the notation $C = ([n, Kq^K, d])_q$.

Similar to stabilizer codes, a union stabilizer code can be described in terms of classical codes. Given the symplectic dual $C_0^*$ of the additive code $C_0$ associated to the stabilizer...
code $C_0$, the union normalizer code is the union of cosets of $C_0^*$ given by
\[ C^* = \bigcup_{t \in T_0} C_0^* + t = \{ c + t_j : c \in C_0^*, j = 1, \ldots, K \}. \]  

(1)

Here $T_0$ is the set of vectors $t_i \in \mathbb{F}_{q_1^2}$ corresponding to the generalized Pauli matrices $t_i \in T_0$.

Proposition 1 (cf. [16]): The minimum distance of a union stabilizer code with union normalizer code $C^*$ is given by
\[ d = \min \{ \text{wt}(v) : v \in (C^* - C^*) \setminus \bar{C}_0 \} \]
\[ \geq \min \{ \text{dist}(c + t_i, c' + t_i') : t_i, t_i' \in T_0, c, c' \in C_0^*, c + t_i \neq c' + t_i' \}, \]

where $C^* - C^* := \{ a - b : a, b \in C^* \}$ denotes the set of all differences of vectors in $C^*$, and $\bar{C}_0 \subseteq C_0$ is the symplectic dual of the additive closure of the (in general nonadditive) union normalizer code $C^*$. Hence in order to construct a union stabilizer code with distance $d$, it suffices to find a large classical code $C^*$ with minimum distance $d$ that can be decomposed into cosets of an additive code $C_0^*$ that contains its symplectic dual. Two extremal cases are stabilizer codes where only one coset is used, and CWS codes for which $C_0^* = C_0$ is a symplectic self-dual code.

III. GENERALIZED CONCATENATION

The basic idea of generalized concatenated quantum codes [17] uses just two levels of concatenation. Here we first present multilevel concatenation for quantum codes. Then we discuss a special case that can be described by classical codes only.

A. Multilevel Concatenation for Quantum Codes

The inner quantum code $B^{(0)} = (n, q_1 q_2 \cdots q_r, \nu q_1 d_1)_q$ is first partitioned into $q_1$ mutually orthogonal subcodes $B_{i_1}^{(1)} (0 \leq i_1 \leq q_1 - 1)$, where each $B_{i_1}^{(1)}$ is a $(n, q_2 \cdots q_r, d_2 q_2 q_3)_q$ code. Then each $B_{i_1}^{(1)}$ is partitioned into $q_2$ mutually orthogonal subcodes $B_{i_1,i_2}^{(2)} (0 \leq i_2 \leq q_2 - 1)$, where $B_{i_1,i_2}^{(2)}$ has parameters $(n, q_3 \cdots q_r, d_3 q_2^2 q_3)_q$, and so on. Finally, each $B_{i_1,i_2,\ldots,i_r}^{(r-2)}$ is partitioned into $q_r$ mutually orthogonal subcodes $B_{i_1,i_2,\ldots,i_r}^{(r-1)} = (n, q_r, d_r)_q$ for $0 \leq i_r - 1 \leq q_r - 1$.

Thus
\[ B^{(0)} = \bigoplus_{i_1 = 0}^{q_1-1} B_{i_1}^{(1)}, \quad B_{i_1}^{(1)} = \bigoplus_{i_2 = 0}^{q_2-1} B_{i_1,i_2}^{(2)}, \ldots, \]  

(2)

and $d_1 \leq d_2 \leq \ldots \leq d_r$. A typical basis vector of $B^{(0)}$ will be denoted by $| \varphi_{i_1,i_2,\ldots,i_r} \rangle (0 \leq i_1 \leq q_1 - 1, \ldots, 0 \leq i_r - 1 \leq q_r - 1)$, with subscripts chosen such that $| \varphi_{i_1,i_2,\ldots,i_r} \rangle$ is a basis vector of all $B_{i_1}^{(1)}, B_{i_1,i_2}^{(2)}, \ldots, B_{i_1,i_2,\ldots,i_r}^{(r-1)}$.

In addition, we take as outer codes a collection of r quantum codes $A_1, \ldots, A_r$ where $A_j$ is an $(N_j, M_j, \delta_j,q_j)_q$ code over the Hilbert space $\mathcal{H}^{\otimes N}$. Denote the standard basis of each $\mathcal{H}^{\otimes N}$ by
\[ \{|i_1^{(j)}\rangle \otimes \cdots \otimes |i_N^{(j)}\rangle : 0 \leq i_j^{(j)} \leq q_j - 1, 1 \leq \nu \leq N \} \]

(where $j$ runs from 1 to $r$), and the bases of the codes $A_j$ are denoted by $\{ |\phi_{i_1^{(j)}}\rangle : 0 \leq i_j \leq M_j - 1 \}$. Expanding the basis vectors of $A_j$ with respect to the standard basis of $\mathcal{H}^{\otimes N}$ we obtain
\[ |\phi_{i_1^{(j)}}\rangle = \sum_{i_2^{(j)},i_3^{(j)},\ldots,i_N^{(j)}} \alpha_{i_1^{(j)},i_2^{(j)},\ldots,i_N^{(j)}}^{(j)} |i_2^{(j)}\rangle \otimes \cdots \otimes |i_N^{(j)}\rangle. \]  

(3)

The basis vectors of the tensor product of all outer codes are given by
\[ |\phi_{i_1^{(1)}}\rangle \otimes |\phi_{i_2^{(2)}}\rangle \otimes \cdots \otimes |\phi_{i_r^{(r)}}\rangle, \]

where $i_j$ runs from 0 to $M_j - 1$. Expanding these basis vectors with respect to the standard bases we obtain
\[ |\phi_{i_1^{(1)}}\rangle \otimes |\phi_{i_2^{(2)}}\rangle \otimes \cdots \otimes |\phi_{i_r^{(r)}}\rangle = \sum_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}} \alpha_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}}^{(r)} |i_1^{(1)}\rangle \otimes |i_2^{(2)}\rangle \otimes \cdots \otimes |i_N^{(r)}\rangle. \]  

(4)

The basis of the resulting generalized concatenated quantum code $Q$ is given by replacing the basis vectors in Eq. (4) using the mapping
\[ |i_{\nu}^{(1)}\rangle \otimes |i_{\nu}^{(2)}\rangle \otimes \cdots \otimes |i_{\nu}^{(r)}\rangle \rightarrow |\varphi_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}}\rangle \]

for $1 \leq \nu \leq N$. Hence the basis of $Q$ is given by
\[ |\psi_{i_1,i_2,\ldots,i_r}\rangle = \sum_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}} \alpha_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}}^{(r)} |\varphi_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}}\rangle \otimes \cdots \otimes |\varphi_{i_1^{(1)},i_2^{(2)},\ldots,i_N^{(r)}}\rangle. \]

So $Q$ is a quantum code in the Hilbert space $\mathcal{H}^{\otimes N}$ of dimension $M = M_1 M_2 \cdots M_r$. As already mentioned, the construction given in [17] is a two-level construction with $r = 2$, while the concatenation of quantum codes used in the context of fault tolerant quantum computation (cf. [1], [12], [18], [19]) is a one-level construction, i.e. $r = 1$.

B. Classical Outer Codes

From now on we restrict ourselves in constructing union stabilizer codes. For simplicity we consider only nondegenerate codes here.

We take the inner code $B^{(0)}$ to be an $(n, K q^k, d_1)_q$ nondegenerate union stabilizer code, given by a classical symplectic self-orthogonal additive code $C_0 \subset C_0 = (n, q^{n+k}, d_1)_q$ and

954
a set \( T^{(0)} \) of \( K = q_1 q_2 \cdots q_r \) coset representatives. The corresponding classical union normalizer code is
\[
C^* = B^*(0) = \bigcup_{t \in T^{(0)}} C_0^* + t.
\]

The decomposition (2) of the inner quantum code \( B^{(0)} \) into mutually orthogonal union stabilizer codes is based on the decomposition of the union normalizer code \( B^{(0)} \) that is obtained by partitioning the coset representatives
\[
T^{(0)} = \bigcup_{i_2=0}^{q_2-1} T^{(2)}_{i_1}, \quad T^{(1)}_{i_1} = \bigcup_{i_2=0}^{q_2-1} T^{(2)}_{i_1 i_2}, \ldots
\]

This defines union normalizer codes \( B^{*(j)} \) given by
\[
B^{*(j)}_{i_1 \cdots i_{j-1}} = \bigcup_{t \in T^{(j)}_{i_1 \cdots i_{j-1}}} C_0^* + t.
\]

The coset representatives in \( T^{(0)} \) will be denoted by \( t_{i_1 \cdots i_r} \) with \( 0 \leq i_1 \leq q_1 - 1, \ldots, 0 \leq i_r \leq q_r - 1 \). The indices are chosen such that \( t_{i_1 \cdots i_r} \) belongs to all \( T^{(1)}_{i_1}, T^{(2)}_{i_1 i_2}, \ldots, T^{(r-2)}_{i_1 \cdots i_{r-2}} \).

Here \( B^{(0)} \) is a classical code over GF\((q^2)\) with parameters \((n, q_1 q_2 \cdots q_r - q^{n+k}, d_1)q^2\) that is the union of \( q_1 \) disjoint codes \( B^{(1)}_{i_1} = (n, q_2 \cdots q_r - q^{n+k}, d_2)q^2 \), and so on. Finally, each \( B^{(r-1)}_{i_1 \cdots i_{r-2}} \) is the union of \( q_1 \) disjoint codes \( B_{i_1 \cdots i_{r-2}}^{(r-1)} = (n, q^{n+k}, d_r)q^2 \), each of which is a single coset of the additive code \( C_0^* \).

In total we use \( r \) classical outer codes. For the first \( r-1 \) outer codes we take \( A_j = (N, M_j, \delta_j)q_0 \), a classical code over an alphabet of size \( q_0 \) with length \( N \), size \( M_j \), and distance \( \delta_j \). The code \( A_j \) is a trivial code \( A_j = [N, N, 1]_{q_0} \) where \( q_0 = |C_0^*| = q^{n+k} \).

Next we show how to construct the classical generalized concatenated code using the inner code \( B^{(0)} \) and the outer codes \( A_1, \ldots, A_r \). What follows is an adaption of [20, Ch. 18, §8.2]. The trivial classical code \( A_j = [N, N, 1]_{q_0} \) on level \( r \) is concatenated with the additive normalizer code \( C_0^* \), resulting in the additive code \( (C_0^*)^N \) which contains its symplectic dual \( C_0^* \). Note that this corresponds to concatenating a trivial quantum code \( A_j = [[N, N, 1]_{q_0}]_q \) with the stabilizer code \( C_0^* \). As a technicality we note that the alphabet size of the trivial classical outer code \( A_j \) is \( q^{n+k} \), while the trivial outer quantum code \( A_j \) is over quantum systems of dimension \( q^k \).

The first \( r-1 \) outer codes are used to define a set of coset representatives. For this, form an \( N \times (r-1) \) array
\[
\begin{bmatrix}
q_1 (a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(r-1)}) \\
q_2 (a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{(r-1)}) \\
\vdots \\
q_n (a_n^{(1)}, a_n^{(2)}, \ldots, a_n^{(r-1)})
\end{bmatrix},
\]

where the first column is a codeword of \( A_1 \), the second is in \( A_2 \), etc. Then replace each row \( a_j^{(1)}, a_j^{(2)}, \ldots, a_j^{(r-1)} \) by the coset representative \( t_{a_j^{(1)}, a_j^{(2)}, \ldots, a_j^{(r-1)}} = T_j \). For this, label the elements of the alphabet of size \( q_0 \) by the numbers 0, 1, \ldots, \( q_0 - 1 \) in some arbitrary, but fixed way.) The resulting \( N \times n \) arrays \( T = (T_1, \ldots, T_N) \) (considered as vectors of length \( Nn \)) form the new set of coset representatives of the generalized concatenated code
\[
C^*_g = \bigcup_{(T_1, \ldots, T_N)} (C_0^* \times \cdots \times C_0^*) + (T_1, \ldots, T_N). \quad (5)
\]

Clearly, this code \( C^*_g \) has the form of a union normalizer code as specified in (1). Hence \( C^*_g \) defines a QECC. The properties of this code are given by the following theorem.

**Theorem 2:** The minimum distance of the union normalizer code
\[
C^*_g = ([nN, M_1 M_2 \cdots M_r q^k N, d_j]_q),
\]
corresponding to \( C^*_g \) given in (5) is
\[
d \geq \min \{\delta_1 d_1, \ldots, \delta_{r-1} d_{r-1}, d_r\}.
\]

**Proof:** Let \( c \) and \( \tilde{c} \) be two distinct codewords of \( C^*_g \). If they belong to the same coset, then \( c - \tilde{c} \in (C_0^*)^N \). Hence their distance is at least \( d_r \). Now assume that \( c \) and \( \tilde{c} \) lie in different cosets given by the arrays \((a_j^{(1)}, a_j^{(2)})\) and \((\tilde{a}_j^{(1)}, \tilde{a}_j^{(2)})\). If the arrays differ in the \( j^{th} \) column then they differ in at least \( \delta_j \) places in the \( j^{th} \) column. By definition \( t_{a_j^{(1)}, a_j^{(2)}, \ldots, a_j^{(r-1)}} - \delta_j \) and \( t_{\tilde{a}_j^{(1)}, \tilde{a}_j^{(2)}, \ldots, \tilde{a}_j^{(r-1)}} \) both belong to \( T_{(r-1)} \). Therefore the corresponding coset codewords of \( B^{(r-1)}_{a_j^{(1)}, \ldots, a_j^{(r-1)}} \) differ in at least \( \delta_j d_r \) places. Hence \( c \) and \( \tilde{c} \) differ in at least \( \delta_j d_r \) places.

**C. Additivity Properties**

We know that if \( C^*_g \) is an additive code, then the corresponding quantum code \( C^*_g \) is a stabilizer code. So the question is when does generalized concatenation yield an additive code. The following is an adaption of a result from [9].

**Proposition 3:** Given additive, i.e., \( F_q \)-linear, outer codes \( A_1, \ldots, A_{r-1} \) and an additive inner code \( B \), the resulting generalized concatenated code is additive if the mapping
\[
(a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(r-1)}) \mapsto t_{a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(r-1)}} (6)
\]
is \( F_q \)-linear.

Hence we can construct stabilizer codes from a sequence of nested stabilizer codes yielding a decomposition of the inner code and classical linear outer codes.

**Theorem 4:** Let
\[
B^{(0)} = [[n, k_0, d_1]_q] \supset B^{(1)} = [[n, k_1, d_2]_q] \supset \cdots \supset B^{(r-1)} = [[n, k_{r-1}, d_r]_q]
\]
be a sequence of nested nondegenerate stabilizer codes. This defines a decomposition of the inner code \( B^{(0)} \). Using \( r-1 \) additive outer codes \( A_j = (N, M_j, \delta_j)q_0 \) where \( q_0 = q^{n+k} \), together with the trivial code \( A_r = [N, N, 1]_{q_0} \) where \( q_r = q^{n+k} \), by generalized concatenation we obtain a stabilizer code with parameters \([nN, K, d]\)
\[
d \geq \min \{\delta_1 d_1, \delta_2 d_2, \ldots, \delta_{r-1} d_{r-1}, d_r\}
\]
Examples for this theorem are given in the next section.

IV. EXAMPLES

A. Stabilizer Codes

Example 5: Consider the following sequence of nested stabilizer codes:

\[ B^{(0)} = [6, 6, 1]_2 \supset B^{(1)} = [6, 4, 2]_2 \supset B^{(2)} = [6, 0, 4]_2. \]

The largest code \( B^{(0)} \) can be decomposed into four mutually orthogonal subspaces, each of which is a code \([6, 4, 2]_2\). Then each of these codes \( B^{(1)} \) is decomposed into 16 one-dimensional spaces \([6, 0, 4]_2\). Hence we need nontrivial outer codes with alphabet sizes 4 and 16, which we chose to be

\[ A_1 = [6, 3, 4]_4 \text{ and } A_2 = [6, 5, 2]_{16}, \]

together with \( A_3 = [6, 6, 1]_2 \). The dimension of the resulting code is \( |A_1| \times |A_2| = 4^3 \times 15^5 = 2^9 \cdot 2^{20} = 2^{26} \), and the minimum distance is at least \( \min\{4 \times 1, 2 \times 2, 4\} = 4 \). Taking an additive map \( (6) \) to obtain a stabilizer code. As all inner codes are \( GF(4) \)-linear, we can even choose the mapping \( (6) \) to be \( GF(4) \)-linear, resulting in a \( GF(4) \)-linear code \([36, 26, 4]_2\). This code improves the lower bound on the minimum distance of a stabilizer code \([36, 26, 6]_2\) given in [13].

Our construction allows to adopt most of the known variations of generalized concatenation for classical codes. In [8] a modified generalized concatenation has been introduced which uses outer code \( A_i \) of different lengths \( n_i \) as well as different inner codes \( B_j^{(s)} \).

Example 6: Using the stabilizer code \( B^{(1)} = [21, 15, 3]_2 \), we can decompose the full space \( B^{(0)} = [21, 21, 1]_2 \) into 64 mutually orthogonal codes \([21, 15, 3]_2\). In order to construct a generalized concatenated quantum code of distance three, we need a classical distance-three code over an alphabet of size 64, e.g., the classical MDS code \( A_1 = [65, 63, 3]_2 \), as well as the trivial code \( A_2 = [65, 65, 1]_{2^{1+1}} \). Then by generalized concatenation one obtains a perfect quantum code \([1365, 1353, 3]_2\). Instead of taking 65 copies of the inner code of length 21, we can use any combination of inner codes \( B_j^{(s)} = [n_j, n_j - 6, 3]_2 \) with \( n_j \in \{7, \ldots, 17, 21\} \). Note that now the trivial outer code \( A_2 \) has to be modified in such a way that by concatenation we get the normalizer code of the direct product of the various inner codes \( B_j^{(s)} \). Overall we obtain quantum codes with parameters \([n, n - 12, 3]_2\) for \( n = 455, \ldots, 1361 \) and \( n = 1365 \).

Note that for quantum codes, the existence of a code \([n, k, d]_q \) does not necessarily imply the existence of a shortened code \([n - s, k - s, d]_q \). In general, one would have to analyze the weight structure of an auxiliary code, the so-called puncture code, introduced in [21]. Varying the length of the inner quantum codes, we can directly construct shorter codes.

B. Nonadditive Codes

In our construction, we can also use classical nonlinear codes as outer codes. Good nonlinear codes can be obtained as subcodes of a linear code over a larger alphabet (or one of its cosets) by taking only those codewords whose symbols are taken from a subset of the alphabet. The following result can be found in [9, Lemma 3.1]:

Proposition 7: If there exists an \((n, K, d)_q \) code, then for any \( s < q \), there exists an \((n', K', d)_s \) code with size at least \( K(s/q)^n \).

Example 8 (cf. [17]): We start with the sequence of inner codes

\[ B^{(0)} = [[5, 5, 1]]_2 \supset B^{(1)} = [[5, 1, 3]]_2. \]

For the nontrivial outer code we take a code over an alphabet of size \( 2^{5-1} = 16 \) and distance three. From the linear MDS code \([18, 16, 3]_17 \) over \( GF(17) \) we can derive a nonlinear code \( A_1 = (18, [10^{18}, 1, 3]_16 \) over \( GF(16) \) using Proposition 7. The resulting generalized concatenated quantum code has parameters \(([90, 2^{81} \times 2^{25}, 9])_2 \), while the best stabilizer code has parameters \(([90, 81, 3])_2 \).

In the final example, we use three levels of concatenation and a nonlinear classical outer code.

Example 9: Decompose the code \( B^{(0)} = [[8, 8, 1]]_2 \) using the sequence of nested stabilizer codes

\[ B^{(0)} = [[8, 8, 1]]_2 \supset B^{(1)} = [[8, 6, 2]]_2 \supset B^{(2)} = [[8, 3, 3]]_2. \]

As outer codes we need a code with alphabet size \( 2^{8-6} = 4 \) and distance three, a code with alphabet size \( 2^{9-3} = 8 \) and distance two, as well as a trivial code. We take the nonlinear code \( A_1 = (6, [4^0/5^2], 3)_4 \) derived from the linear MDS code \([6, 4, 3]_5 \) over \( GF(5) \), the linear code \( A_2 = [6, 5, 2]_8 \) over \( GF(8) \), and the linear code \( A_3 = [6, 6, 1]_{2^8+2} \). The dimension of the generalized concatenated quantum code is \([A_1] \times [A_2] \times \dim(B^{(2)})^6 = 164 \times 85 \times 2^{3\times 6} \). Hence we get a nonadditive code \(([48, 2^{40} \times 356, 3])_2 \), which has a higher dimension than the best possible additive code \(([48, 40, 3])_2 \).

V. DECODING

One of the advantages of concatenated codes as well as generalized concatenated codes is that decoding can be based on decoding algorithms for the constituent codes [9], [10]. For quantum codes, however, it is not possible to directly measure the “code symbols”. Instead, decoding is based on measuring an error syndrome.

For stabilizer codes, the error syndrome is obtained by measuring the eigenvalues of generators of the stabilizer group. The error syndrome can be defined in such a way that it corresponds to the error syndrome of the underlying classical code, and hence a classical decoding algorithm can be used.

For generalized concatenated quantum codes derived from a sequence of nested stabilizer codes as in Theorem 4, the corresponding stabilizer groups are nested as well, with the stabilizer of the smallest code \( B^{(1)} \) being the largest. It is possible to choose its generators in such a way that stabilizers of the larger codes are generated by appropriate subsets. Hence
the components of the syndrome vector reflect the nested structure of the inner code.

Again, we may not directly measure the syndromes of the $N$ copies of the inner code. Instead, we compute the eigenvalues using some auxiliary quantum systems. Then we derive syndromes for the outer codes which will be measured.

Details of the quantum circuits for syndrome measurement and iterative decoding algorithms are left to further work.

ACKNOWLEDGMENT

The authors would like to thank Panos Aliferis, Salman Beigi, Sergey Bravyi, G. David Forney, Martin Rötteler, Graeme Smith, and John Smolin for helpful discussions.

Centre for Quantum Technologies is a Research Centre of Excellence funded by Ministry of Education and National Research Foundation of Singapore.

REFERENCES


