Citation	Grassl, M., P.W. Shor, and Bei Zeng. "Generalized concatenation for quantum codes." Information Theory, 2009. ISIT 2009. IEEE International Symposium on. 2009. 953-957. © 2009 IEEE
As Published	http://dx.doi.org/10.1109/ISIT.2009.5205592
Publisher	Institute of Electrical and Electronics Engineers
Version	Final published version
Accessed	Wed Nov 14 13:40:41 EST 2018
Citable Link	http://hdl.handle.net/1721.1/59346
Terms of Use	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.
Detailed Terms	

Generalized Concatenation for Quantum Codes

Markus Grassl[*][†], Peter W. Shor[‡], and Bei Zeng[§]

[*]Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences,
Technikerstraße 21a, 6020 Innsbruck, Austria
[†]Centre for Quantum Technologies, National University of Singapore,
3 Science Drive 2, Singapore 117543, Singapore, Email: Markus.Grassl@nus.edu.sg
[‡]Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, MA 02139, USA, Email: shor@math.mit.edu
[§]Department of Physics, Massachusetts Institute of Technology,
Cambridge, MA 02139, USA, Email: zengbei@mit.edu

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 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 general quantum error-correcting code (QECC), denoted by $C = ((n, K, d))_q$, is a K-dimension subspace of the Hilbert space $\mathcal{H}_q^{\otimes n}$ 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 $\mathcal{C}$ over $GF(q^2)$ that is self-orthogonal with respect to a symplectic inner product [2], [5]. Denoting the symplectic dual code by $\mathcal{C}^*$, the minimum distance of the quantum code is given by

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

If $d = d_{\min}(\mathcal{C}^*)$, 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 $K = q^k$.

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

$$C = \bigoplus_{t \in T_0} t C_0,$$

where $T_0 = \{t_1, \ldots, t_K\}$ is a set of tensor products of (generalized) Pauli matrices such that the spaces $t_i C_0$ are mutually orthogonal. Then the dimension of the union stabilizer code C is $K q^k$, and we will use the notation $\mathcal{C} = ((n, K q^k, d))_q$. Similar to stabilizer codes, a union stabilizer code can be described in terms of classical codes. Given the symplectic dual $\mathcal{C}_0^*$ of the additive code $\mathcal{C}_0$ associated to the stabilizer

code C_0, the union normalizer code is the union of cosets of $\mathcal{C}_0^*$ given by

$$\mathcal{C}^* = \bigcup_{t \in \mathcal{T}_0} \mathcal{C}_0^* + t = \{c + t_j \colon c \in \mathcal{C}_0^*, j = 1, \ldots, K\}. \quad (1)$$

Here $\mathcal{T}_0$ is the set of vectors $t_i \in \mathbb{F}_{q^2}^n$ 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 $\mathcal{C}^*$ is given by

$$d = \min\{\mathrm{wgt}(v) \colon v \in (\mathcal{C}^* - \mathcal{C}^*) \setminus \widetilde{\mathcal{C}}_0\}$$
$$\geq d_{\min}(\mathcal{C}^*)$$
$$= \min\{\mathrm{dist}(c + t_i, c' + t_{i'}) \colon t_i, t_{i'} \in \mathcal{T}_0, c, c' \in \mathcal{C}_0^*$$
$$c + t_i \neq c' + t_{i'}\},$$

where $\mathcal{C}^* - \mathcal{C}^* := \{a - b \colon a, b \in \mathcal{C}^*\}$ denotes the set of all differences of vectors in $\mathcal{C}^*$, and $\widetilde{\mathcal{C}}_0 \leq \mathcal{C}_0$ is the symplectic dual of the additive closure of the (in general nonadditive) union normalizer code $\mathcal{C}^*$.

Hence in order to construct a union stabilizer code with distance d, it suffices to find a large classical code $\mathcal{C}^*$ with minimum distance d that can be decomposed into cosets of an additive code $\mathcal{C}_0^*$ that contains its symplectic dual. Two extremal cases are stabilizer codes where only one coset is used, and CWS codes for which $\mathcal{C}_0^* = \mathcal{C}_0$ 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 $B^{(0)} = ((n, q_1 q_2 \cdots q_r, d_1))_q$ 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 an $((n, q_2 \cdots q_r, d_2))_q$ 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 $((n, q_3 \cdots q_r, d_3))_q$, and so on. Finally, each $B_{i_1 i_2 \ldots i_{r-2}}^{(r-2)}$ is partitioned into q_{r-1} mutually orthogonal subcodes $B_{i_1 i_2 \ldots i_{r-1}}^{(r-1)} = ((n, q_r, d_r))_q$ for $0 \leq i_{r-1} \leq q_{r-1} - 1$. Thus

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

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

In addition, we take as outer codes a collection of r quantum codes $A_1, \ldots, A_r$, where A_j is an $((N, M_j, \delta_j))_{q_j}$ code over the Hilbert space $\mathcal{H}_{q_j}^{\otimes N}$. Denote the standard basis of each $\mathcal{H}_{q_j}^{\otimes N}$ by

$$\{|i_1^{(j)}\rangle \otimes \ldots \otimes |i_N^{(j)}\rangle \colon 0 \leq i_\nu^{(j)} \leq q_j - 1, 1 \leq \nu \leq N\}$$

(where j runs from 1 to r), and the bases of the codes A_j are denoted by $\{|\phi_{l_j}^{(j)}\rangle \colon 0 \leq l_j \leq M_j - 1\}$. Expanding the basis vectors of A_j with respect to the standard basis of $\mathcal{H}_j^{\otimes N}$ we obtain

$$|\phi_{l_j}^{(j)}\rangle = \sum_{i_1^{(j)} i_2^{(j)} \ldots i_N^{(j)}} \alpha_{l_j, i_1^{(j)} i_2^{(j)} \ldots i_N^{(j)}}^{(j)} |i_1^{(j)}\rangle \otimes |i_2^{(j)}\rangle \otimes \ldots \otimes |i_N^{(j)}\rangle. \quad (3)$$

The basis vectors of the tensor product of all outer codes are given by

$$|\phi_{l_1}^{(1)}\rangle \otimes |\phi_{l_2}^{(2)}\rangle \otimes \ldots \otimes |\phi_{l_r}^{(r)}\rangle,$$

where l_j runs from 0 to $M_j - 1$. Expanding these basis vectors with respect to the standard bases we obtain

$$|\phi_{l_1}^{(1)}\rangle \otimes |\phi_{l_2}^{(2)}\rangle \otimes \cdots \otimes |\phi_{l_r}^{(r)}\rangle =$$
$$\left(\sum_{i_1^{(1)} i_2^{(1)} \ldots i_N^{(1)}} \alpha_{l_1, i_1^{(1)} i_2^{(1)} \ldots i_N^{(1)}}^{(1)} |i_1^{(1)}\rangle \otimes |i_2^{(1)}\rangle \otimes \ldots \otimes |i_N^{(1)}\rangle \right)$$
$$\otimes \left(\sum_{i_1^{(2)} i_2^{(2)} \ldots i_N^{(2)}} \alpha_{l_2, i_1^{(2)} i_2^{(2)} \ldots i_N^{(2)}}^{(2)} |i_1^{(2)}\rangle \otimes |i_2^{(2)}\rangle \otimes \ldots \otimes |i_N^{(2)}\rangle \right)$$
$$\ldots$$
$$\otimes \left(\sum_{i_1^{(r)} i_2^{(r)} \ldots i_N^{(r)}} \alpha_{l_r, i_1^{(r)} i_2^{(r)} \ldots i_N^{(r)}}^{(r)} |i_1^{(r)}\rangle \otimes |i_2^{(r)}\rangle \otimes \ldots \otimes |i_N^{(r)}\rangle \right). \quad (4)$$

The basis of the resulting generalized concatenated quantum code Q is given by replacing the basis vectors in Eq. (4) using the mapping

$$|i_\nu^{(1)}\rangle \otimes |i_\nu^{(2)}\rangle \otimes \ldots \otimes |i_\nu^{(r)}\rangle \mapsto |\varphi_{i_\nu^{(1)} i_\nu^{(2)} \ldots i_\nu^{(r)}}\rangle$$

for $1 \leq \nu \leq N$. Hence the basis of Q is given by

$$|\psi_{l_1 l_2 \ldots l_r}\rangle = \sum \alpha_{l_1, i_1^{(1)} i_2^{(1)} \ldots i_N^{(1)}}^{(1)} \cdots \alpha_{l_r, i_1^{(r)} i_2^{(r)} \ldots i_N^{(r)}}^{(r)}$$
$$|\varphi_{i_1^{(1)} i_1^{(2)} \ldots i_1^{(r)}}\rangle \otimes \ldots \otimes |\varphi_{i_N^{(1)} i_N^{(2)} \ldots i_N^{(r)}}\rangle.$$

So Q is a quantum code in the Hilbert space $\mathcal{H}_q^{\otimes Nn}$ 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 $((n, Kq^k, d_1))_q$ nondegenerate union stabilizer code, given by a classical symplectic self-orthogonal additive code $\mathcal{C}_0 \subset \mathcal{C}_0^* = (n, q^{n+k}, d_r)_{q^2}$ and

a set $\mathcal{T}^{(0)}$ of $K = q_1 q_2 \cdots q_{r-1}$ coset representatives. The corresponding classical union normalizer code is

$$\mathcal{C}^* = \mathcal{B}^{*(0)} = \bigcup_{t \in \mathcal{T}^{(0)}} \mathcal{C}_0^* + t.$$

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 $\mathcal{B}^{*(0)}$ that is obtained by partitioning the coset representatives

$$\mathcal{T}^{(0)} = \bigcup_{i_1=0}^{q_1-1} \mathcal{T}_{i_1}^{(1)}, \quad \mathcal{T}_{i_1}^{(1)} = \bigcup_{i_2=0}^{q_2-1} \mathcal{T}_{i_1 i_2}^{(2)}, \quad \cdots$$

This defines union normalizer codes $\mathcal{B}^{*(j)}$ given by

$$\mathcal{B}_{i_1 i_2 \ldots i_{j-1}}^{*(j)} = \bigcup_{t \in \mathcal{T}_{i_1 i_2 \ldots i_{j-1}}^{(j)}} \mathcal{C}_0^* + t.$$

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

Here $\mathcal{B}^{*(0)}$ is a classical code over $GF(q^2)$ with parameters $(n, q_1 q_2 \cdots q_{r-1} q^{n+k}, d_1)_{q^2}$ that is the union of q_1 disjoint codes $\mathcal{B}_{i_1}^{*(1)} = (n, q_2 \cdots q_{r-1} q^{n+k}, d_2)_{q^2}$, and so on. Finally, each $\mathcal{B}_{i_1 i_2 \ldots i_{r-2}}^{*(r-2)}$ is the union of q_{r-1} disjoint codes $\mathcal{B}_{i_1 i_2 \ldots i_{r-1}}^{*(r-1)} = (n, q^{n+k}, d_r)_{q^2}$, each of which is a single coset of the additive code $\mathcal{C}_0^*$.

In total we use r classical outer codes. For the first $r-1$ outer codes we take $\mathcal{A}_i = (N, M_i, \delta_i)_{q_i}$, a classical code over an alphabet of size q_i with length N, size M_i, and distance δ_i. The code $\mathcal{A}_r$ is a trivial code $\mathcal{A}_r = [N, N, 1]_{q_r}$ where $q_r = |\mathcal{C}_0^*| = q^{n+k}$.

Next we show how to construct the classical generalized concatenated code using the inner code $\mathcal{B}^{*(0)}$ and the outer codes $\mathcal{A}_1, \ldots, \mathcal{A}_r$. What follows is an adaption of [20, Ch. 18, §8.2]. The trivial classical code $\mathcal{A}_r = [N, N, 1]_{q_r}$ on level r is concatenated with the additive normalizer code $\mathcal{C}_0^*$, resulting in the additive code $(\mathcal{C}_0^*)^N$ which contains its symplectic dual $\mathcal{C}_0^N$. Note that this corresponds to concatenating a trivial quantum code $A_r = [[N, N, 1]]_{q^k}$ with the stabilizer code C_0. As a technicality we note that the alphabet size of the trivial classical outer code $\mathcal{A}_r$ is q^{n+k}, while the trivial outer quantum code A_r 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

$$\begin{bmatrix} a_1^{(1)} & a_1^{(2)} & \cdots & a_1^{(r-1)} \\ a_2^{(1)} & a_2^{(2)} & \cdots & a_2^{(r-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_N^{(1)} & a_N^{(2)} & \cdots & a_N^{(r-1)} \end{bmatrix},$$

where the first column is a codeword of $\mathcal{A}_1$, the second is in $\mathcal{A}_2$, 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_i by the numbers $0, 1, \ldots, q_i - 1$ 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

$$\mathcal{C}_{\mathrm{gc}}^* = \bigcup_{(T_1, \ldots, T_N)} (\mathcal{C}_0^* \times \ldots \times \mathcal{C}_0^*) + (T_1, \ldots, T_N). \quad (5)$$

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

Theorem 2: The minimum distance of the union normalizer code

$$C_{\mathrm{gc}} = ((nN, M_1 M_2 \cdots M_{r-1} q^{kN}, d))_q,$$

corresponding to $\mathcal{C}_{\mathrm{gc}}^*$ given in (5) is

$$d \ge \min\{\delta_1 d_1, \ldots, \delta_{r-1} d_{r-1}, d_r\}.$$

Proof: Let c and $\tilde{c}$ be two distinct codewords of $\mathcal{C}_{\mathrm{gc}}^*$. If they belong to the same coset, then $c - \tilde{c} \in (\mathcal{C}_0^*)^N$. Hence their distance is at least d_r. Now assume that c and $\tilde{c}$ lie in different cosets given by the arrays $(a_j^{(i)})$ and $(\tilde{a}_j^{(i)})$. If the arrays differ in the νth column then they differ in at least δ_ν places in the νth column. By definition $t_{i_1 i_2 \ldots i_{\nu-1} \alpha \ldots}$ and $t_{i_1 i_2 \ldots i_{\nu-1} \beta \ldots}$ (with $\alpha \ne \beta$) both belong to $\mathcal{T}_{i_1 i_2 \ldots i_{\nu-1}}^{(\nu-1)}$. Therefore the corresponding codewords of $\mathcal{B}_{i_1 i_2 \ldots i_{\nu-1}}^{*(\nu-1)}$ differ in at least d_ν places. Hence c and $\tilde{c}$ differ in at least $\delta_\nu d_\nu$ places. ∎

C. Additivity Properties

We know that if $\mathcal{C}_{\mathrm{gc}}^*$ is an additive code, then the corresponding quantum code C_{gc} 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., $\mathbb{F}_p$-linear, outer codes $\mathcal{A}_1, \ldots, \mathcal{A}_{r-1}$ and an additive inner code $\mathcal{B}$, the resulting generalized concatenated code is additive if the mapping

$$(a_i^{(1)}, a_i^{(2)}, \ldots, a_i^{(r-1)}) \mapsto t_{a_i^{(1)}, a_i^{(2)}, \ldots, a_i^{(r-1)}} \quad (6)$$

is $\mathbb{F}_p$-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

$$B^{(0)} = [[n, k_0, d_1]]_q \supset B^{(1)} = [[n, k_1, d_2]]_q \supset \ldots$$
$$\ldots \supset B^{(r-1)} = [[n, k_{r-1}, d_r]]_q$$

be a sequence of nested nondegenerate stabilizer codes. This defines a decomposition of the inner code $B^{(0)}$. Using $r-1$ additive outer codes $\mathcal{A}_i = (N, M_i, \delta_i)_{q_i}$ where $q_i = q^{k_{i-1}-k_i}$ together with the trivial code $\mathcal{A}_r = [N, N, 1]_{q_r}$ where $q_r = q^{n+k_{r-1}}$, by generalized concatenation we obtain a stabilizer code with parameters $[[nN, K, d]]_q$ where

$$d \ge \min\{\delta_1 d_1, \delta_2 d_2, \ldots, \delta_{r-1} d_{r-1}, d_r\}$$

and

$$K = k_r^N \log_q(M_1 M_2 \cdots M_{r-1}).$$

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

$$\mathcal{A}_1 = [6,3,4]_4 \quad \text{and} \quad \mathcal{A}_2 = [6,5,2]_{16},$$

together with $\mathcal{A}_3 = [6,6,1]_{2^6}$. The dimension of the resulting code is $|\mathcal{A}_1| \times |\mathcal{A}_2| = 4^3 16^5 = 2^6 2^{20} = 2^{26}$, and the minimum distance is at least $\min\{4 \times 1, 2 \times 2, 4\} = 4$. Taking an additive map (6), we obtain a stabilizer code. As all inner codes are $GF(4)$-linear, we can even chose 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 $[[36,26,d]]_2$ 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 $\mathcal{A}_i$ of different lengths n_i as well as different inner codes $B_j^{(0)}$.

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 $\mathcal{A}_1 = [65,63,3]_{2^6}$, as well as the trivial code $\mathcal{A}_2 = [65,65,1]_{2^{21+15}}$. 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 $B_j^{(1)} = [[n_j, n_j - 6, 3]]_2$ with $n_j \in \{7, \ldots, 17, 21\}$. Note that now the trivial outer code $\mathcal{A}_2$ 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 $B_j^{(1)}$. 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 $\mathcal{A}_1 = (18, \lceil \frac{16^{18}}{17^2} \rceil, 3)_{16}$ over $GF(16)$ using Proposition 7. The resulting generalized concatenated quantum code has parameters $((90, 2^{81.825}, 3))_2$, 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 $2^{6-3} = 8$ and distance two, as well as a trivial code. We take the nonlinear code $\mathcal{A}_1 = (6, \lceil 4^6/5^2 \rceil, 3)_4$ derived from the linear MDS code $[6,4,3]_5$ over $GF(5)$, the linear code $\mathcal{A}_2 = [6,5,2]_8$ over $GF(8)$, and the linear code $\mathcal{A}_3 = [6,6,1]_{2^{8+3}}$. The dimension of the generalized concatenated quantum code is $|\mathcal{A}_1| \times |\mathcal{A}_2| \times \dim(B^{(2)})^6 = 164 \times 8^5 \times 2^{3 \times 6}$. Hence we get a nonadditive code $((48, 2^{40.356}, 3))_2$, 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 $B^{(r)}$ 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

REFERENCES

[1] D. Aharonov and M. Ben-Or, "Fault-Tolerant Quantum Computation with Constant Error," in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*. Association for Computing Machinery, 1997, pp. 176–188, preprint quant-ph/9611025.

[2] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001, preprint quant-ph/0005008.

[3] E. L. Blokh and V. V. Zyablov, "Coding of Generalized Concatenated Codes," *Problemy Peredachi Informatsii*, vol. 10, no. 3, pp. 45–50, 1974.

[4] ——, *Linear Concatenated Codes*. Moscow: Nauka, 1982, (in Russian).

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum Error Correction Via Codes over $GF(4)$," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998, preprint quant-ph/9608006.

[6] X. Chen, B. Zeng, and I. L. Chuang, "Nonbinary Codeword Stabilized Quantum Codes," *Physical Review A*, vol. 78, p. 062315, Dec. 2008, preprint arXiv:0808.3086 [quant-ph].

[7] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, "Codeword Stabilized Quantum Codes," *IEEE Transactions on Information Theory*, vol. 55, no. 1, pp. 433–438, Jan. 2009, preprint arXiv:0801.1021v4 [quant-ph].

[8] U. Dettmar, Y. Gao, and U. K. Sorger, "Modified Generalized Concatenated Codes and their Application to the Construction and Decoding of LUEP Codes," *IEEE Transactions on Information Theory*, vol. 41, no. 5, pp. 1499–1503, Sep. 1995.

[9] I. Dumer, "Concatenated Codes and Their Multilevel Generalizations," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier, 1998, ch. 23, pp. 1911–1988.

[10] G. D. Forney, Jr., *Concatenated Codes*. Cambridge, MA: M.I.T. Press, 1966.

[11] D. Gottesman, "A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound," *Physical Review A*, vol. 54, no. 3, pp. 1862–1868, Sep. 1996, preprint quant-ph/9604038.

[12] ——, "Stabilizer Codes and Quantum Error Correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997.

[13] M. Grassl, "Bounds on the minimum distance of quantum codes," Online available at http://www.codetables.de, 2007, accessed on 2009-01-10.

[14] M. Grassl and T. Beth, "A Note on Non-Additive Quantum Codes," 1997, preprint quant-ph/9703016.

[15] M. Grassl and M. Rötteler, "Non-Additive Quantum Codes from Goethals and Preparata Codes," in *Proceedings IEEE Information Theory Workshop 2008 (ITW 2008)*, Porto, May 2008, pp. 396–400, preprint arXiv:0801.2144v1 [quant-ph].

[16] ——, "Quantum Goethals-Preparata Codes," in *Proceedings 2008 IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Jul. 2008, pp. 300–304, preprint arXiv:0801.2150v1 [quant-ph].

[17] M. Grassl, P. W. Shor, G. Smith, J. A. Smolin, and B. Zeng, "Generalized Concatenated Quantum Codes," *Physical Review A*, 2009 (to appear), preprint arXiv:0901.1319v1 [quant-ph].

[18] E. Knill, R. Laflamme, and W. Zurek, "Accuracy Threshold for Quantum Computation," Oct. 1996, preprint quant-ph/9610011.

[19] ——, "Resilient Quantum Computation: Error Models and Thresholds," *Proceedings of the Royal Society A*, vol. 454, no. 1969, pp. 365–384, Jan. 1998, preprint quant-ph/9702058.

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[21] E. M. Rains, "Nonbinary Quantum Codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1827–1832, Sep. 1999, preprint quant-ph/9703048.

[22] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "Nonadditive Quantum Code," *Physical Review Letters*, vol. 79, no. 5, pp. 953–954, Aug. 1997, preprint quant-ph/9703002.

[23] D. Schlingemann and R. F. Werner, "Quantum Error-Correcting Codes Associated with Graphs," *Physical Review A*, vol. 65, no. 012308, 2002, preprint quant-ph/0012111.

[24] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, "Nonadditive Quantum Error-Correcting Code," *Physical Review Letters*, vol. 101, p. 090501, 2008, arXiv:0704.2122v1 [quant-ph].

[25] V. A. Zinoviev, "Generalized Concatenated Codes," *Problemy Peredachi Informatsii*, vol. 12, no. 1, pp. 5–15, 1976.