# Generalized concatenated quantum codes

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

| Citation       | Grassl, Markus et al. “Generalized concatenated quantum codes.” Physical Review A 79.5 (2009): 050306. © 2009 The American Physical Society. |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| As Published   | http://dx.doi.org/10.1103/PhysRevA.79.050306                                                                                         |
| Publisher      | American Physical Society                                                                                                           |
| Version        | Final published version                                                                                                             |
| Citable link   | http://hdl.handle.net/1721.1/51860                                                                                                   |
| 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. |
Generalized concatenated quantum codes

Markus Grassl,1 Peter Shor,2 Graeme Smith,3 John Smolin,3 and Bei Zeng3,4

1Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstraße 21a, 6020 Innsbruck, Austria
2Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
3IBM T.J. Watson Research Center, Yorktown Heights, New York 10598, USA
4Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

(Rceived 16 January 2009; published 22 May 2009)

We discuss the concept of generalized concatenated quantum codes. This generalized concatenation method provides a systematic way for constructing good quantum codes, both stabilizer codes and nonadditive codes. Using this method, we construct families of single-error-correcting nonadditive quantum codes, in both binary and nonbinary cases, which not only outperform any stabilizer codes for finite block length but also asymptotically meet the quantum Hamming bound for large block length.

DOI: 10.1103/PhysRevA.79.050306 PACS number(s): 03.67.Pp, 03.67.Lx

I. INTRODUCTION

Quantum error-correcting codes (QECCs) play a vital role in reliable quantum information transmission as well as fault-tolerant quantum computation (FTQC). So far, most good quantum codes constructed are stabilizer codes, which correspond to classical additive codes. There is a rich theory of stabilizer codes and a thorough understanding of their properties [1,2]. However, these codes are suboptimal in certain cases—there exist nonadditive codes which encode a larger logical space than any stabilizer code of the same length that is capable of tolerating the same number of errors [3–5].

The recently introduced codeword stabilized (CWS) quantum codes [6–8] framework, followed by the idea of union of stabilizer codes construction [9,10], provides a unifying way of constructing a large class of quantum codes, both stabilizer codes and nonadditive codes. The CWS framework naturally allows us to search for good quantum codes, and some good nonadditive codes that outperform any stabilizer codes have been found. However, this search algorithm is very inefficient [7], which prevents us from searching for good quantum codes of length $n \approx 10$ in the binary case and even smaller lengths in the nonbinary case.

This Rapid Communication discusses the concept of generalized concatenated quantum codes (GCQCs), which is a systematic way of constructing good QECCs, both stabilizer codes and nonadditive codes. Compared to the usual concatenated quantum code construction, the role of the basis vectors of the inner quantum code is taken on by subspaces of the inner code. The idea of concatenated codes, originally described by Forney in a seminal book in 1966 [11], was introduced to quantum computation community three decades later [1,12–15]. These concatenated quantum codes play a central role in FTQC, as well as the study of constructing good degenerate QECCs.

The classical counterpart of GCQCs, i.e., generalized concatenated codes, was introduced by Blokh and Zyablov [16], followed by Zinoviev [17]. These codes improve the parameters of conventional concatenated codes for short block lengths [17] as well as their asymptotic performance [18]. Many good codes, linear and nonlinear, can be constructed from this method. One may expect that moving to the quantum scenario, the GCQC method should be also a powerful one in making good codes, which we show is the case.

We demonstrate the power of this GCQC method by showing that some good stabilizer quantum codes, such as some quantum Hamming codes, can be constructed this way. We then further construct families of nonadditive single-error-correcting quantum codes, in both binary and nonbinary cases, which outperform any stabilizer codes. This is a systematic construction of these good nonadditive codes, while previous codes were found by exhaustive or random numerical search with no structure to generalize to other cases. We also show that these families of nonadditive codes asymptotically meet the quantum Hamming bound.

II. BASIC PRINCIPLE

A general quantum code $Q$ of $n$-dimensional systems, encoding $K$ levels, is a $K$-dimensional subspace of the Hilbert space $\mathcal{H}_q^n$. We say $Q$ is of distance $d$ if all $d-1$ errors (i.e., operators acting nontrivially on less than $d$ individual $\mathcal{H}_q$’s) can be detected or have no effect on $Q$, and we denote the parameters of $Q$ by $(n, K, d)$. We may recall that concatenated quantum codes are constructed from two quantum codes: an outer code $A$ and an inner code $B$. If $B$ is an $(n, K, d)\_q$ code with basis vectors $|\varphi_{ij}\rangle_{i=0}^{K-1}$, then the outer code $A$ is taken to be an $(n', K', d')\_K$ code, i.e., a subspace $A \subseteq \mathcal{H}_q^{n'}$. The concatenated code $Q_c$ is constructed in the following way: for any codeword $|\phi\rangle = \sum_{i_1, \ldots, i_n} \alpha_{i_1, \ldots, i_n} |\varphi_{i_1, \ldots, i_n}\rangle$ in $A$, replace each basis vector $|i_j\rangle$ (where $i_j = 0, \ldots, K-1$ for $j=1, \ldots, n'$) by a basis vector $|\varphi_{i_j}\rangle$ in $B$, i.e.,

$$|\phi\rangle \mapsto |\tilde{\phi}\rangle = \sum_{i_1, \ldots, i_n} \alpha_{i_1, \ldots, i_n} |\varphi_{i_1}\rangle \cdots |\varphi_{i_n}\rangle,$$

so the resulting code $Q_c$ is an $((nn', K', d'))\_q$ code and the distance $\delta$ of $Q_c$ is at least $dd'$; for examples, see [1,12].

In its simplest version, a generalized concatenated quantum code is also constructed from two quantum codes: an outer code $A$ and an inner code $B$ which is an $(n, K, d)\_q$ code. The inner code $B$ is further partitioned into $r$ mutually orthogonal subcodes $\{B_r\}_{i=0}^{l-1}$, i.e.,

1050-2947/2009/79(5)/050306(4) 050306-1 ©2009 The American Physical Society
and each $B_i$ is an $((n,K_i,d_i))_q$ code, with basis vectors $\{|\varphi_j,i\rangle\}_{j=0}^{r}$, and $i=0,\ldots,r-1$.

Now choose the outer code $A$ to be an $((n',K',d'))_r$ quantum code in the Hilbert space $\mathcal{H}_{q}^{\otimes n'}$. While for concatenated quantum codes each basis state $|j\rangle$ of the space $\mathcal{H}_q$ is replaced with a basis state $|\varphi_j,i\rangle$ of the inner code, for a generalized concatenated quantum code $Q_{gc}$ the basis state $|j\rangle$ is mapped to the subcode $B_i$ of the inner code. For simplicity we assume that all subcodes $B_i$ are of equal dimension, i.e., $K_1=K_2=\ldots=K_r=R$. Then the resulting dimension of the concatenated code $Q_{gc}$ is $K=K'R^r$, i.e., for each of the $n'$ coordinates of the outer code, the dimension $K$ is increased by the factor $R$. For a codeword $|\phi\rangle = \sum_{i_1,\ldots,i_{n'}} \alpha_{i_1,\ldots,i_{n'}} |\varphi_{i_1,\ldots,i_{n'}}\rangle$ of the outer code and a basis state $|j_{1},\ldots,j_{n'}\rangle$ (where $j_1=0,\ldots,R-1$ for $l=1,\ldots,n'$) of the space $\mathcal{H}_{q}^{\otimes n'}$, the encoding is given by the following mapping:

$$|\phi\rangle|j_{1},\ldots,j_{n'}\rangle \rightarrow \sum_{i_{1},\ldots,i_{n'}} \alpha_{i_{1},\ldots,i_{n'}} |\varphi_{i_{1},i_{1}}\rangle\cdots|\varphi_{i_{n'},i_{n'}}\rangle.$$  \hspace{1cm} (3)

Note that the special case when $R=1$ corresponds to concatenated quantum codes. The resulting code $Q_{gc}$ has parameters $((n',K,R^r))_q$, where the distance $R$ is at least $\min\{dd',d_2\}$. If some of the $K_i$‘s differ, the calculation of the dimension is more involved.

III. CWS-GQC

From now on we restrict ourselves in constructing some special kind of quantum codes, namely, CWS codes. CWS codes include all the stabilizer codes and many good nonadditive codes [6], so it is a large class of quantum codes. The advantage of the CWS framework is that the problem of constructing quantum codes is reduced to the construction of some classical codes correcting certain error patterns induced by a graph. So the point of view of constructing these codes could be fully classical. For simplicity we only consider nondegenerate codes here.

A nondegenerate $((n,K,d))_q$ CWS codes $Q_{cw}$ is fully characterized by a graph $G$ and a classical code $C_{G}$ [6–8], and for simplicity we only consider $q$ as a prime power. For any graph $G$ of $n$ vertices, there exists a unique stabilizer code $((n,1,d_G))$ defined by $G$ (called the graph state of $G$). We call the distance $d_G$ the graph distance of $G$. For constructing a nondegenerate CWS code, we require that the distance of the code be $\leq d_G$. Then any quantum error $E$ acting on $Q_{cw}$ can be transformed into a classical error by a mapping $C_{G}(E)$ whose image is an $n$-bit string. The nondegenerate code $Q_{cw}$ detects the error set $E$ if and only if $C$ detects $C_{G}(E)$ [6–8].

We take the inner code $B$ to be an $((n,K,d))_q$ nondegenerate CWS code, constructed by a graph $G$ and a classical code $B$. Furthermore, we decompose $B$ as $B=\bigoplus_{i=0}^{r} B_i$ such that each $B_i$ is an $((n,K_i,d_i))_q$ CWS code constructed from $G$. The basis vectors of each $B_i$ can be represented by classical codewords of a code $B_i=(b_0^{K_i})_{j=0}^{r}$. Then consequently, the classical code $B$ has a partition $B=\bigcup_{i=0}^{r} B_i$.

Now we take the outer code $A$ to be an $((n',K',d'=1))_r$ code in the Hilbert space $\mathcal{H}_{q}^{\otimes n'}$, which is constructed from a classical $((n',K',d))_r$ code $A$ over an alphabet of size $r$, of length $n'$, of size $K'$, and of distance $d'$, in the following way: the basis vector $|\psi_{i_1,\ldots,i_r}\rangle$ of $A$ is given by $|\psi_{i_1,\ldots,i_r}\rangle = |i_1\ldots i_r\rangle$, $\forall \ (i_1\ldots i_r) \in A^{n'}$. (4)

Denote the generalized concatenated code obtained from $A$ and $B$ by $Q_{gc}$. It is straightforward to see $Q_{gc}$ is also a CWS code, where the corresponding graph is given by $n'$ disjoint copies of the graph $G$. The corresponding classical code $C_{gc}$ is a classical generalized concatenated code with inner code $B=\bigcup_{i=0}^{r} B_i$ and outer code $A$. The minimum distance of $Q_{gc}$ is at least $\min\{d,d_1,d_2\}$. However, the following statement provides an improved lower bound:

Main result: the minimum distance of $Q_{gc}$ is given by $\min\{dd_1,dd_2,d_2\}$.

We will not give a technical detailed proof of this result here. Instead, since the proof idea can be illustrated clearly with a simple example, we will analyze such an example, which also illustrates a systematic method of constructing good nonadditive quantum codes that outperform the best stabilizer codes.

IV. GOOD NONADDITIVE CODES

We start taking the subcode $B_0$ of the inner code $B$ to be the well-known $((5,2,3))_2$ code, the shortest one-error-correcting quantum code. As a CWS code, this code can be constructed by a pentagon graph as well as a classical code $B_0=\{00000,11111\}$. Further details can be found in [6]; here we just focus on the classical error patterns given by the mapping $C_G$. Since the pentagon graph has a distance of 3, the CWS code $B_0$ has a distance of at least 3 if $B_0$ detects up to two errors with the error patterns induced by the pentagon. The induced error patterns are given by the following strings:

$$Z:\{10000,01000,00100,00010,00001\},$$
$$X:\{01001,10100,01010,00101,10010\},$$
$$Y:\{11001,11100,01110,00111,11011\}.$$

It is straightforward to check that $B_0$ indeed detects two of these errors.

The classical code $B_0$ is linear, so we can choose 15 disjoint proper cosets, e.g., $B_1=\{00001,11110\}$ and $B_{15}=\{01111,10000\}$. Combining these classical codes with the pentagon gives us the CWS codes $B_i$, each of which is a $((5,2,3))_2$ quantum code. The union $B=\bigcup_{i=1}^{15} B_i$ of all cosets is a classical $(5,32,1)_2$ code which consists of all five-bit strings. Combining $B$ with a pentagon gives us the CWS quantum inner code $B$ which is a $(5,32,1)_2$ quantum code. It can be decomposed as $B=\bigoplus_{i=0}^{15} B_i$.

For the outer code we take a quantum code $A$ which corresponds to a classical code $A=\{(3,16,3)_{16}\}$, i.e., a distance three code over $GF(16)$ of length 3. Hence the basis of $A$ is given by $|i_1i_2i_3\rangle$, where $(i_1i_2i_3)$ is one of the 16 codewords of
{000, 111, ..., aaa, ..., fff} of A. Here we use the hexadecimal notation to denote the 16 symbols of the alphabet GF(16).

Now we construct the GCQC \( G^{[15]}_{\text{gc}} \) of length 15 from A and B in the following way: first, from the product state form of the basis of A, we choose the corresponding graph \( G^{[15]} \) to be three disjoint pentagons, as shown in Fig. 1. We denote this graph by \( G^{[15]} \). The distance of the graph state corresponding to \( G^{[15]} \) is still 3. So from these three pentagons we can obtain a nondegenerate CWS quantum code whose distance is at most 3. The error patterns induced by the mapping \( CL_{g^{[15]}} \) given by this 15-vertex graph are simply the strings from Eq. (5) on the coordinates 1–5 (or 6–10 or 11–15) and zeros on the other coordinates. For instance, 10000 in Eq. (5) gives rise to three strings of length 15 which are 100000000000000, 000001000000000, and 000000000000010000. In total there are 45 strings in the induced error set of three pentagons corresponding to the 45 single-qubit errors on 15 qubits.

Now we need to figure out what the corresponding classical code \( C^{[15]}_{\text{gc}} \) is. We know that it is the generalized concatenated code with inner code \( B = \bigcup_1^{[15]} \), and outer code A. To see how this works explicitly, consider the first codeword \( a_0 = \text{000} \) of A. Each of the three zeros is replaced with the code \( B_0 = \{00000, 11111\} \), i.e., \( a_0 = (j_1, j_2, j_3) \) (where \( j_i = 0,1 \)) will be mapped to one of the eight codewords of \( C^{[15]} \), which are strings of length 15, given by 0000000000000, 0000000000111, 000000111100000, 000000111111111, 0111110000000, 0111111111111. Similarly, any other codeword \( a_i \) of A will be mapped to \( 2^3 \) codewords in \( C^{[15]}_{\text{gc}} \) obtained by concatenating three codewords of \( B_i \). The size of \( C^{[15]}_{\text{gc}} \) is then \( 2^3 \times 16 = 2^7 \).

We now show that the distance of \( Q^{[15]}_{\text{gc}} \) is 3. To see this, we only need to show that \( C^{[15]}_{\text{gc}} \) detects up to two errors of the error patterns induced by three pentagons. This is clear via the following two observation: (i) \( c_1, c_2 \in C^{[15]}_{\text{gc}} \) correspond to different codewords of the outer code \( A \); since the pentagons are disjoint, and A has a distance of 3, at least three strings in the induced error patterns are needed to transform \( c_1 \) to \( c_2 \). (ii) \( c_1, c_2 \in C^{[15]}_{\text{gc}} \) correspond to the same codewords of the outer code \( A \); since at least three strings in the induced error patterns are needed to transform codewords in \( B_i \), at least three strings in the induced error patterns are needed to transform \( c_1 \) to \( c_2 \).

Now one can generalize the construction of \( Q^{[15]}_{\text{gc}} \) to the case of more than three pentagons. Suppose we use \( n \) pentagons to construct single-error-correcting CWS codes, then we observe the following.

\textbf{Fact 1.} Choose the inner code as \( B = U_1^{[15]} \), with each \( B_i \) a \((5, 2, 3)\) quantum code and the outer code \( A \) corresponding to the classical code \( A \) with parameters \((n', K', 3)_{16}\), then the resulting GCQC \( Q^{[15]}_{\text{gc}} \) is a \((5n', 2^n', K', 3)_{16}\) binary quantum code.

This indicates that if we have a good classical code over GF(16) of distance 3, then we may systematically construct good quantum codes via the generalized concatenation method described above.

\textbf{Example 1.} Using the quantum code corresponding to the classical Hamming code with parameters \((17, 165, 3)_{16}\) as the outer code, then by Fact 1 we get a quantum code with parameters \((85, 277, 3)_{16}\), which is a quantum Hamming code [2]. If we properly choose the labeling of the subcodes \( B_i \) by elements of GF(16), the corresponding classical code is linear [19], and hence this quantum code is a stabilizer code [6].

If we take a quantum code corresponding to a good non-linear classical code as the outer code, then we can construct a good nonadditive quantum code [6]. Here we give examples of such a good quantum codes which are constructed using a good nonlinear classical codes. Those nonlinear codes are obtained via the following classical construction, called “subcode over subalphabet” (see [19], Lemma 3.1).

\textbf{Fact 2.} If there exists an \((n, K, d)\) code, then for any \( s < q \), there exists an \((n', K', d)\) code with size at least \( K(s/q)^n\).

\textbf{Example 2.} It is known that there is a classical Hamming code with parameters \((18, 176, 3)_{17}\). Therefore, Fact 2 is there a \((18, 176, 3)_{16}\) code. Then the resulting quantum code has parameters \((90, 2^8, 8, 3)\). For a binary quantum code with \( n = 90 \) and \( d = 3 \), the quantum Hamming bound \( K = q^n/((q^2 - 1)n + 1) \) see [2]) gives \( K < 2^{81.918} \), and the linear programming bound (see [2]) gives \( K < 2^{81.879} \). So the best stabilizer quantum code can only be \((90, 2^8, 3)\). Hence our simple construction gives a nonadditive single-error-correcting quantum code which outperforms any possible stabilizer codes. This is an example given by construction, not by numerical search.

\textbf{Example 3.} The similar CWS-GCQC idea works also for the nonbinary case using the nonbinary CWS construction [8]. Take the inner code to be a union of 81 mutually orthogonal \((10, 729, 3)\) codes that is constructed from a graph that is a ring of ten vertices [20]. Choose the outer code as the quantum code corresponding to the classical \((84, 512, 8)_{10}\), which is obtained from the Hamming code \((84, 832, 3)_{83}\). Then the resulting quantum code has parameters \((840, 3^8, 3)\). For a ternary quantum code with \( n = 840 \) and \( d = 3 \), the Hamming bound gives \( K < 3^{831.978} \), and the linear programming bound gives \( K < 3^{831.978} \), so the best stabilizer code can only be \((840, 3^8, 3)\). This is a nonbinary nonadditive code which outperforms any stabilizer codes.

It is straightforward to generalize the above construction for binary and ternary codes to build good nonadditive quantum codes in Hilbert space \( H_q^n \) for any prime power \( q \). For this, we take the inner code \( B_0 \) as the perfect quantum Hamming code \((q^2, q, q^2 - 2, 3)\) in \( H_q^3 \) of length \( n_q = (q^2 - 1) / (q^2 - 1) \). The full space \( B = (n_q, q^2, 1) \) can be decomposed as the sum of \( q^2 \) orthogonal translates of \( B_0 \).
The outer quantum code is then corresponding to a classical code over an alphabet of size $Q = q^2$ given by Fact 2, i.e., the classical code is obtained from the $P$-ary Hamming code $[L_i, L_i -1, 3]_P$, where $P$ is the least prime power exceeding $Q$ and $L_i = (P^i -1)/(P-1)$. The result is the code $V_{si} = (N_{si}, M_{si}, 3)$, with length $N_{si} = L_i P_i = (P^i -1)(Q-1)/(q^2-1)(P-1)$ and dimension $M_{si} = q^{N_{si}}/P^i$.

The number of different errors we want to deal with is $(q^2 -1)N_{si} +1 > Q^e = q^{si}$ for $Q > Q^e$ and $i > 1$. By the quantum Hamming bound $K < q^{N_{si}}/[(q^2 -1)N_{si} +1] < q^{N_{si}}/Q^e$, the dimension of any stabilizer code (including degenerate codes) is upper bounded by $K < q^{N_{si} - 2i -1}$. Hence for any prime power $P$ with $Q^e < P^e < qQ^e$, the dimension $M_{si}$ is strictly larger than $q^{N_{si} - 2i -1}$, i.e., our codes are better than any stabilizer codes. Moreover, we have $q^{N_{si}}/P^e < M_{si} < q^{N_{si}}/Q^e$. Since $Q^e/P^e \rightarrow 1$ for $s \rightarrow \infty$ [19], these families of nonadditive codes asymptotically meet the quantum Hamming bound.

V. DISCUSSION

We have discussed the concept of GCQC, which is a systematic construction of good QECCs, both stabilizer codes and nonadditive codes. One way of generalizing the concatenation of Eq. (3) is to put some constraints on the additional degrees of freedom $|j_1 \cdots j_n\rangle$ by using a second outer code. Additionally, one can recursively decompose the codes $B_i$ in decomposition (2) of the inner code, which leads to a more general construction of GCQC with which more good quantum codes can be constructed (see [21]). While the nonadditive codes of this communication tighten the gap between lower and upper bounds for the dimension of the codes, we believe that in general the GCQC construction gives a promising way for further constructing new quantum codes of good performance, and we hope that this generalized concatenation technique will also shed light on improvements of fault-tolerant protocols.

[1] D. Gottesman, Ph.D. thesis, Caltech, 1997.
[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory 44, 1369 (1998).
[3] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. 79, 953 (1997).
[4] J. A. Smolin, G. Smith, and S. Wehner, Phys. Rev. Lett. 99, 130505 (2007).
[5] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, Phys. Rev. Lett. 101, 090501 (2008).
[6] A. Cross, G. Smith, J. Smolin, and B. Zeng, IEEE Trans. Inf. Theory 55, 433 (2009).
[7] I. Chuang, A. Cross, G. Smith, J. Smolin, and B. Zeng, J. Math. Phys. 50, 042109 (2009).
[8] X. Chen, B. Zeng, and I. L. Chuang, Phys. Rev. A 78, 062315 (2008).
[9] M. Grassl and M. Rötteler, e-print arXiv:0801.2150.
[10] M. Grassl and M. Rötteler, e-print arXiv:0801.2144.
[11] G. D. Forney, Jr., Concatenated Codes (MIT Press, Cambridge, MA, 1966).
[12] E. Knill and R. Laflamme, e-print arXiv:quant-ph/9608012.
[13] E. Knill, R. Laflamme, and W. Zurek, e-print arXiv:quant-ph/9610011; e-print arXiv:quant-ph/9702058.
[14] C. Zalka, e-print arXiv:quant-ph/9612028.
[15] D. Aharonov and M. Ben-Or, Proceedings of the 29th Annual ACM Symposium on Theory of Computing, 1997, pp. 176–188; e-print arXiv:quant-ph/9611025.
[16] E. L. Blokh and V. V. Zyablov, Probl. Peredachi Inf. 10, 45 (1974).
[17] V. A. Zinoviev, Probl. Peredachi Inf. 12, 5 (1976).
[18] E. L. Blokh and V. V. Zyablov, Linear Concatenated Codes (Nauka, Moscow, 1982) (in Russian).
[19] I. Dumer, in Handbook of Coding Theory, edited by V. S. Pless and W. C. Huffman (Elsevier Science, Amsterdam, 1998), Chap. 23, pp. 191–1988.
[20] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A 78, 042303 (2008).
[21] M. Grassl, P. W. Shor, and B. Zeng, e-print arXiv:0905.0428.