Codeword Stabilized Quantum Codes

Andrew Cross, Graeme Smith, *Member, IEEE*, John A. Smolin, and Bei Zeng

***Abstract*—We present a unifying approach to quantum error correcting code design that encompasses additive (stabilizer) codes, as well as all known examples of nonadditive codes with good parameters. We use this framework to generate new codes with superior parameters to any previously known. In particular, we find $((10,18,3))$ and $((10,20,3))$ codes. We also show how to construct encoding circuits for all codes within our framework.**

***Index Terms*—Nonadditive codes, quantum error correction, stabilizer codes.**

I. Introduction

QUANTUM computers hold the promise of the efficient solution of problems, such as factoring [1] and simulation of quantum systems [2]–[4] that are generally believed to be intractable on a classical computer. Furthermore, as the processor size in state-of-the-art computers continues to scale down and performance begins to be limited by dissipative effects in logical processing, it has become increasingly clear that considering the quantum nature of the components of a classical computer will be essential in the not-too-distant-future. In both of these scenarios—constructing a working quantum computer, or simply continuing to improve the performance of classical computers—quantum error correcting codes and ideas from quantum fault-tolerance [5] will be essential elements in the future computer engineer's toolbox.

Stabilizer codes are an important class of quantum codes developed in [6], [7], and are the quantum analogues of classical additive codes. An $[n,k]$ stabilizer code encodes k logical qubits into n physical qubits, and is described by an abelian subgroup, S, of the Pauli group with size $|S| = 2^{n-k}$. The codespace is the set of simultaneous eigenvectors of S with eigenvalue 1. There is a rich theory of stabilizer codes, and a thorough understanding of their properties.

Nevertheless, such codes are strictly suboptimal in some settings—there exist *nonadditive codes* which encode a larger logical space than possible with a stabilizer code of the same length and capable of tolerating the same number of errors. There are only a handful of such examples [8]–[10], and their constructions have proceeded in an ad hoc fashion, each code working for seemingly different reasons.

In the following we present a framework for code design that includes as special cases stabilizer codes as well as all known nonadditive codes with good parameters. We note that the code of [10] was presented explicitly in the form we describe below and, indeed, served as motivation for our studies of the generality of such a construction. Our codes are fully described by two objects: a single stabilizer state $|S\rangle$, and a classical code that generates the basis vectors of our code from $|S\rangle$. The stabilizer is chosen such that it maps all Pauli errors onto only Z errors, though this may increase their weight. In this way we map the problem of finding a quantum code to that of finding a classical code that corrects an unusual error model. We have thus unified stabilizer and nonadditive codes and rendered both in a form that gives insight into the classical nature of quantum error-correction.

Our approach is related to the description of nonadditive codes given in [11] in terms of Boolean functions. Our codeword operators, codeword stabilizer, and effective classical errors correspond, respectively, to a Boolean function f, a matrix A_f, and the "Cset_f" in the language of that work. Their approach is essentially dual to ours—in the language we use here it amounts to first choosing a classical code and trying to design a stabilizer state whose induced error model is corrected by the chosen code. From this perspective, the approach of [11] seems somewhat unnatural, which is perhaps the reason it has not proved useful for finding new codes. Both approaches are closely related to the work of [12], [13].

We describe codes on n qubits that encode K dimensions with minimum distance d, traditionally written $((n,K,d))$. In this framework we find the original nonadditive $((5,6,2))$ code of [8] and the family it generates, the simple family of minimum distance 2 codes found in [9], the $((9,12,3))$ code of [10], as well as new $((10,18,3))$ and $((10,20,3))$ codes.

II. General Construction and Properties

An $((n,K))$ code will be described by two objects—S, a 2^n element abelian subgroup of the Pauli group not containing minus the identity, which we call the *word stabilizer*, together with a family of Kn-qubit Pauli elements, $W = \{w_l\}_{l=1}^{K}$, which we call the *word operators*. There is a unique state $|S\rangle$ stabilized by S, i.e., $|S\rangle$ satisfies $s|S\rangle = |S\rangle$ for all $s \in S$. Our code will be spanned by basis vectors of the form

$$|w_l\rangle \equiv w_l|S\rangle. \tag{1}$$

Since the code vectors should all be different, at most one w_l can be in S. Typically we will choose $w_1 = I$ and later we will prove this can be done without loss of generality. Note that $|w_l\rangle$

Manuscript received August 14, 2007; revised October 01, 2008. Current version published December 24, 2008. The work of G. Smith was supported in part by the U.K. Engineering and Physical Sciences Research Council. The work of J. A. Smolin was supported by ARO under Contract DAAD19-01-C-0056.

A. Cross is with the Department of Electrical Engineering, Massachusetts Institute of Technology, Cambridge MA 02139 USA and also with the IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA (e-mail: awcross@mit.edu).

G. Smith and J. A. Smolin are with the IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA (e-mail: gsbsmith@gmail.com; smolin@watson.ibm.com).

B. Zeng is with the Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

Communicated by A. Winter, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2008.2008136

is an eigenvector of all $s \in S$ with eigenvalue $\lambda_s = \pm 1$, but $|w_l\rangle$ is not stabilized by S unless $w_l \in S$. Each $|w_l\rangle$ is stabilized by a different stabilizer $w_l S w_l^\dagger$.

We would now like to understand the error correction capabilities of such a *codeword stabilized* (CWS) code. An $((n, K, d))$ code is an $((n, K))$ code capable of detecting Pauli errors of weight up to $d-1$, but not d, and is said to have minimum distance d (we will often use "distance" as shorthand for "minimum distance" when referring to codes). A distance d code can also be used to correct errors up to weight $\lfloor (d-1)/2 \rfloor$. The conditions for error correction were found in [14], [15]. The error correction conditions for a general code with basis vectors $|w_l\rangle$ are that, in order to detect errors from a set $\mathcal{E}$, it is necessary and sufficient to have

$$\langle w_i | E | w_j \rangle = c_E \delta_{ij} \tag{2}$$

for all $E \in \mathcal{E}$ where c_E is a constant depending only on E. For a code of the form described above, this becomes

$$\langle S | w_i^\dagger E w_j | S \rangle = c_E \delta_{ij}. \tag{3}$$

To correct errors on a fixed number of qubits, it is sufficient to study errors of the form $Z^{\mathbf{v}} X^{\mathbf{u}}$ with bounded weight since these form a basis [14]. This leads to the *necessary and sufficient conditions* for detecting errors in $\mathcal{E}$ that for all $E \in \mathcal{E}$

$$\forall i \neq j \; w_i^\dagger E w_j \notin \pm S \tag{4}$$

and

$$\left(\forall i \; w_i^\dagger E w_i \notin \pm S\right) \text{ or} \tag{5}$$

$$\left(\forall i \; w_i^\dagger E w_i \in S\right) \text{ or} \tag{6}$$

$$\left(\forall i \; w_i^\dagger E w_i \in -S\right) \tag{7}$$

Equation (4) is the condition that two codewords should not be confused after an error, while the final three conditions express that each error must either be detected (5), or the code must be "immune" to it—i.e., the code is *degenerate*.

Theorem 1: An $((n, K))$ codeword stabilized code with word operators $W = \{w_l\}_{l=1}^K$ and codeword stabilizer S is locally Clifford-equivalent to a codeword stabilized code with word operators $w_l' = Z^{\mathbf{c}_l}$ and codeword stabilizer S' generated by

$$S_i' = X_i Z^{\mathbf{r}_i} \tag{8}$$

for some choice of classical bitstrings $\{\mathbf{c}_l\}_{l=1}^K$ and $\{\mathbf{r}_i\}_{i=1}^n$. In other words, any CWS code is locally equivalent to a CWS code with a graph-state stabilizer and word operators consisting only of Zs. The set of $\mathbf{r}_i$s forms the adjacency matrix of the graph. Moreover, the word operators can always be chosen to include the identity. We call this **standard form**.

Proof: First note that S is local-Clifford equivalent to a graph state due to [16]–[18] so there is some local-Clifford unitary $C = \bigotimes_{i=1}^n C_i$ that maps S to S' of the form (8). In the new basis the word operators are $C w_l C^\dagger = \pm Z^{\mathbf{a}_l} X^{\mathbf{b}_l}$, and we have

$$C w_l C^\dagger \prod_i (S_i')^{(\mathbf{b}_l)_i} = \pm Z^{\mathbf{c}_l} \tag{9}$$

so that, letting $w_l' = Z^{\mathbf{c}_l}$, we have

$$\begin{aligned} Z^{\mathbf{c}_l} |S'\rangle &= \pm C w_l C^\dagger s' |S'\rangle \\ &= \pm C w_l C^\dagger |S'\rangle = \pm C w_l |S\rangle. \end{aligned}$$

Since C consists of local Clifford elements, we see that the CWS code defined by S' and w' is locally Clifford equivalent to the original code.

Finally, to ensure the codeword operators include the identity we can choose $\tilde{W} = \{\tilde{w}_l = w_l' w_1'\}$ which always has $\tilde{w}_1 = \mathrm{Identity}$. This can be seen by commuting the w_1' through the E in the error-correction conditions ((4)–(7)) which can at worst pick up a sign depending only on E. The two conditions with $\pm S$ on the right are insensitive to this and the other two conditions at most change places. □

This structure theorem gives rise to the following lemma, which is at the heart of our construction.

Lemma 2: A single qubit Pauli error Z, X or $Y = ZX$ acting on a codeword $w|S\rangle$ of a CWS code in standard form is equivalent up to a sign to another (possibly multi-qubit) error consisting only of Zs.

Proof: Let the error E_i act only on the ith qubit. If it is a Z error the result is immediate. Otherwise use the fact that $E_i w |S\rangle = \pm E_i S_i w |S\rangle$, and take S_i to be the generator having X on bit i. Then since $E_i = Z_i^{\{0,1\}} X_i$ the X in E_i cancels with the X from S_i and we are left with the Zs from S_i as well as a Z_i if E_i was $Z_i X_i$. □

Lemma 2 allows us to construct CWS codes with a satisfying interpretation: X errors on any qubit are "pushed" outwards along the edges of the graph and transformed into Zs. This is illustrated in Fig. 1. Similarly Y errors are pushed along the edges, but also leave a Z behind at their original locations. Since all errors become Zs, we can think of the error model as classical, albeit consisting of strange multi-bit errors. We mathematically codify this translation to classical errors by defining the function $\mathrm{Cl}_S(E \in \mathcal{E}) \to \{0,1\}^n$

$$\mathrm{Cl}_S(E = \pm Z^{\mathbf{v}} X^{\mathbf{u}}) = \mathbf{v} \oplus \bigoplus_{i=1}^n (\mathbf{u})_i \mathbf{r}_i \tag{10}$$

with length n bitstrings $\mathbf{u}, \mathbf{v}$ and where $\mathbf{r}_i$ is the ith row of the stabilizer's adjacency matrix (recall from (8) $S_i = X_i Z^{\mathbf{r}_i}$ defines $\mathbf{r}_i$). The codeword operators $w_l = Z^{\mathbf{c}_l}$ will be chosen to so that the $\mathbf{c}_l$s are a classical code for this error model.

Theorem 3: A CWS code in standard form with stabilizer S and codeword operators $\{Z_{\mathbf{i}}^{\mathbf{c}}\}_{\mathbf{c_i} \in \mathcal{C}}$ detects errors from $\mathcal{E}$ if and only if there exists a classical code $\mathcal{C}$ which detects errors from $\mathrm{Cl}_S(\mathcal{E})$ and in addition we have for each E

$$\mathrm{Cl}_S(E) \neq 0 \tag{11}$$

$$\text{or } \forall i \; Z^{\mathbf{c}_i} E = E Z^{\mathbf{c}_i}. \tag{12}$$

Thus, any CWS code is completely specified by a graph state stabilizer S and a classical code $\mathcal{C}$.

Proof: When $i \neq j, w_i^\dagger E w_j \notin \pm S$ is satisfied exactly when $Z^{\mathbf{c}_i} E Z^{\mathbf{c}_j} \notin \pm S$, which is in turn equivalent to $Z^{\mathbf{c}_i} Z^{\mathrm{Cl}_S(E)} Z^{\mathbf{c}_j} \notin \pm S$. In standard form, the only element

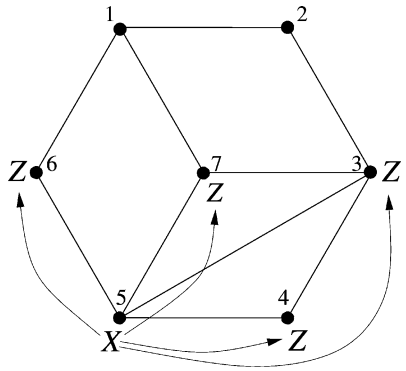

Fig. 1. Example of the induced error on a graph state: The state has stabilizer generators $XZIIIZZ, ZXZIIII, IZXZIIZ, IIZXZII, IIZZXZZ, ZIIIZXI$, and $ZIZIZIX$. An X error applied to node 5 in the lower-left is translated by multiplying with the stabilizer element $IIZZXZZ$ and turns into Z errors on the nodes indicated.

of S without any X is the identity, so that this is satisfied exactly when $\mathbf{c}_i \oplus \mathrm{Cl}_S(E) \neq \mathbf{c}_j$. This is explicitly the classical error-detection condition.

Similarly, when $i = j$, we must satisfy (5), (6), and (7), whose three possibilities translate directly to

$$\forall \mathbf{c}\ Z^{\mathbf{c}} E Z^{\mathbf{c}} \notin \pm S \tag{13}$$

$$\text{or } \forall \mathbf{c}\ Z^{\mathbf{c}} E Z^{\mathbf{c}} \in S \tag{14}$$

$$\text{or } \forall \mathbf{c}\ Z^{\mathbf{c}} E Z^{\mathbf{c}} \in -S. \tag{15}$$

Since $Z^{\mathbf{c}} = I$ for the $\mathbf{c} = 0$ codeword, (13) is equivalent to $E \notin \pm S$ and therefore to (11). If (11) (and therefore (13)) is not satisfied, $E \in \pm S$. If any $Z^{\mathbf{c}}$ anticommutes with E we have also $E \in \mp S$. Since no $s \in S$ is also in $-S$ this readily implies the equivalence of (12) to (14) and (15). □

Remark: A classical code expressed in quantum terms would traditionally comprise computational basis vectors that are eigenstates of Z, and therefore the operators mapping one codeword to another would be of the form $X^{\mathbf{c}}$ as these are the only errors that have any effect. It then might seem odd that standard form for CWS codes, the intuition of which is to make everything classical, would employ word operators and effective errors consisting only of Zs. This choice is arbitrary (one could exchange Z and X and nothing in the formalism would be affected) and is made since the usual form of a graph state stabilizer is to have one X and some number of Zs rather than the reverse. We hope this historical accident does not cause too much confusion going forward. □

A. Relation to Stabilizer Codes

The CWS framework includes stabilizer codes, and allows them to be understood in a new way. We now show that any stabilizer code is a CWS code, and give a method for determining if a CWS code is also a stabilizer code.

Theorem 4: An $[n, k]$ stabilizer code with stabilizer generators $S_1, \ldots, S_{n-k}$ and logical operations $\bar{X}_1 \cdots \bar{X}_k$ and $\bar{Z}_1 \cdots \bar{Z}_k$, is equivalent to the CWS code defined by

$$S = \langle S_1 \cdots S_{n-k}, \bar{Z}_1 \cdots \bar{Z}_k \rangle \tag{16}$$

and word operators

$$w_{\mathbf{v}} = \bar{X}_1^{(\mathbf{v})_1} \otimes \cdots \otimes \bar{X}_k^{(\mathbf{v})_k} \tag{17}$$

where $\mathbf{v}$ is a k-bit string.

Proof: To see that this CWS code describes the original code, note that the stabilizer state associated with S is $|\bar{0} \cdots \bar{0}\rangle$, while the codeword generated by $W_{\mathbf{v}}$ acting on $|\bar{0} \cdots \bar{0}\rangle$ is $|(\bar{\mathbf{v}})_1 \cdots (\bar{\mathbf{v}})_k\rangle$.

Theorem 5: If the word operators of an $((n, K))$ CWS code are an abelian group W (not containing $-I$), then the code is an $[n, k = \log_2 K]$ stabilizer code.

Proof: The stabilizer S of the CWS code is a maximal abelian subgroup of the Pauli group (not containing $-I$) therefore it is isomorphic to the group $S' = \langle X_1 \ldots X_n \rangle$ and the mapping from S to S' is a Clifford operation C (not necessarily local). This follows from the definition of the Clifford group as the automorphisms of the Pauli group. Because this automorphism group allows one to achieve any bijective mapping that preserves commutation relations (see Chapter 4 of [6]), the map can further be chosen to map W to $W' = \langle Z_1 \ldots Z_k \rangle$. Here we have made use of the facts that all $w \in W$ anticommute with at least one $s \in S$ (which implies $S \cap W = \{I\}$) and that S' is maximal, which allows us to choose for W' any order K group made only of Zs we like (since *all* products of X's are in S'). Note that this nonlocal Clifford mapping is not the same as the conversion to Zs used in Theorem 1.

We can now choose $T', \bar{X}'$ and $\bar{Z}'$ as follows:

$$\bar{X}' = W' = \langle Z_1 \ldots Z_k \rangle \tag{18}$$

$$\bar{Z}' = \langle X_1 \ldots X_k \rangle \tag{19}$$

$$T' = \langle X_{k+1} \ldots X_n \rangle \tag{20}$$

The inverse Clifford operation $C^\dagger$ maps these to our stabilizer code with stabilizer T, and logical operations $\bar{X} = W$ and $\bar{Z}$.

It remains to show this is the same as the CWS code we started with. T is by construction a subgroup of S (T' is explicitly generated by a subset of the generators of S') and therefore stabilizes $|S\rangle$. T also stabilizes all $\bar{x}|S\rangle, \bar{x} \in \bar{X}$, since T and $\bar{X}$ commute. Using $\bar{X} = W$ we see these states are exactly the basis states of the CWS code.

III. Examples

We now give some examples of our construction and including all known nonadditive codes with good parameters.

A. The $[5, 1, 3]$ Code

The celebrated $[5, 1, 3]$ quantum code [14], [15] can be written as a CWS code using (16) and (17) but another way of writing it demonstrates the power of the CWS framework. Take generators corresponding to a ring graph:

$$S_i = ZXZII \quad \text{and cyclic shifts.} \tag{21}$$

This induces effective errors as follows. Letting $|\mathrm{R}5\rangle$ be the graph state corresponding to the unique simultaneous $+1$ eigenvector of these generators, we have

$$Z_i|\mathrm{R}5\rangle = Z_i|\mathrm{R}5\rangle$$

$$X_i|\mathrm{R5}\rangle = Z_{i-1}Z_{i+1}|\mathrm{R5}\rangle$$
$$Y_i|\mathrm{R5}\rangle = Z_{i-1}Z_iZ_{i+1}|\mathrm{R5}\rangle \quad (22)$$

where all additions and subtractions are taken modulo 5. The corresponding 15 classical errors are

$$\begin{array}{lccccc} Z: & 10000 & 01000 & 00100 & 00010 & 00001 \\ X: & 01001 & 10100 & 01010 & 00101 & 10010. \\ Y: & 11001 & 11100 & 01110 & 00111 & 10011 \end{array} \quad (23)$$

We then must choose $w_l = Z^{\mathbf{c}_l}$ where the $\mathbf{c}_l$s form a classical code capable of detecting pairs of these errors. Since no pair of these errors produces 11111 the codewords $\mathbf{c}_0 = 00000$ and $\mathbf{c}_1 = 11111$ will serve, and together with the stabilizer (21) completely define the code. Since the $((5,2,3))$ code is known to be unique we need not otherwise check that our construction is equivalent to the traditional presentation of this code. We note also that for $n \geq 7$ a ring code with codeword operators I and $\otimes_{l=1}^{n} Z_l$ gives a $[n,2,3]$ code.

B. The $((5,6,2))$ Code

The first nonadditive quantum code was found in [8], and encodes a six-dimensional space into five qubits with a minimum distance of two. This outperforms the best additive five qubit distance two code, which can have an encoded dimension of at most four. The code was originally found as follows: It was known that the linear programming upper bound was exactly 6 for a blocklength 5 distance 2 code, and in fact it was possible to completely determine what the weight enumerator [19] of a code meeting this bound must be. The authors of [8] then performed a numerical search for such a code, and managed to find one. The structure of the resulting code was mysterious, and generating larger codes in a similar fashion seemed intractable (though [20] showed how to construct a $((5+2l, 2^{2l+1}3, 2))$ code from this code).

As a CWS code the $((5,6,2))$ code of [8] becomes simple. We again use the ring stabilizer (21) and will have to detect the induced errors (23), but since we are seeking a distance-2 code we need only consider single errors rather than pairs. The classical codewords $\mathbf{c}_l, l = 0 \ldots 5$, are

$$00000 \quad 11010 \quad 01101 \quad 10110 \quad 01011 \quad 10101 \quad (24)$$

and the code generated by $|c^{\mathrm{RS}}\rangle$ and $W_l = Z^{\mathbf{c}_l}$ is locally Clifford equivalent to the $((5,6,2))$ code of [8]. The $((5+2l, 2^{2l+1}3, 2))$ codes of [20] are also CWS codes whose graph state is the union of the ring graph and l Bell pair graphs, and whose classical codewords can be derived straightforwardly from the $((5,6,2))$ classical codewords.

C. The SSW Codes

A family of distance two codes was found in [9], which outperforms the family of [20] for odd blocklengths of eleven or larger. The codes were originally described in terms of their codewords as follows. If $n = 1 \bmod 4$, a basis of our code consists of vectors of the form

$$|\mathbf{x}\rangle + |\bar{\mathbf{x}}\rangle \quad (25)$$

where $\mathbf{x}$ ranges over all n-bit vectors of odd weight less than $(n-1)/2$ and $\bar{\mathbf{x}}$ is the complement of $\mathbf{x}$, while if $n = 3 \bmod 4$, we let $\mathbf{x}$ range over even weight vectors of weight less than $(n-1)/2$, leading to an encoded dimension of $2^{n-2}(1 - \frac{\binom{n-1}{(n-1)/2}}{2^{n-1}})$.

We now show that these are actually CWS codes. Indeed, the codeword stabilizer of this code will be generated by

$$\langle X_1Z_2\cdots Z_n, Z_1X_2, Z_1X_3, \ldots, Z_1X_n\rangle, \quad (26)$$

with the corresponding stabilizer state being equivalent to a GHZ state, $(|0\rangle|+\rangle^{\otimes n-1} + |1\rangle|-\rangle^{\otimes n-1})/\sqrt{2}$. The codeword operators are simply $W_{\mathbf{x}} = X^{(\mathbf{x})_1}Z^{((\mathbf{x})_2,\ldots(\mathbf{x})_n)}$ for each allowed $\mathbf{x}$, which can immediately be seen to generate, up to local unitaries, the same codewords as (25). Putting the stabilizer into standard form, we find that the graph state it describes corresponds to a star graph.

D. The $((9,12,3))$ Code

Like the $((5,6,2))$ code, the codeword stabilizer is of the form

$$S_i = ZXZIIIIII \text{ and cyclic shifts.} \quad (27)$$

The associated classical code correcting the induced errors is

$$\begin{array}{cccc} 000000000 & 100100100 & 010001100 & 110101000 \\ 000110001 & 100010101 & 011001010 & 111101110. \\ 001010011 & 101110111 & 011111111 & 111011011 \end{array} \quad (28)$$

IV. New Codes

A. Ring Codes: $((10,18,3))$

In light of the excellent performance of ring-stabilizers for CWS codes—the $((5,6,2))$ and $((9,12,3))$ are both of this form—we have studied larger blocklength codes based on this stabilizer. This leads to a new code that outperforms stabilizer codes for blocklength 10.

The blocklength ten code has a codeword stabilizer generated by $\langle Z_{i-1}X_iZ_{i+1}\rangle$ and has 18 word operators of the form $Z^{\mathbf{c}_l}$, with $\mathbf{c}_l$ taken from the list

$$\begin{array}{ccc} 0000000000 & 1101001100 & 0011001010 \\ 0000011111 & 0010001001 & 1111100000 \\ 1000111110 & 1100100101 & 0101101101 \\ 0001000110 & 1010010010 & 0100110100 \\ 1001010111 & 1011010001 & 0110111000 \\ 0101110010 & 1110100011 & 0111111011. \end{array} \quad (29)$$

That this code satisfies the required error correction conditions can be shown by the straightforward (if tedious) technique

of verifying that the associated classical code corrects the classical noise model induced by the ring stabilizer.

B. A $((10, 20, 3))$ Double Ring Code

We now consider a CWS code with a codeword stabilizer that is not of the ring form. In particular, our stabilizer will correspond to the double ring, with generators

$$\begin{array}{llll} S_1 = & XZIIZZIIII & S_6 = & ZIIIIXZIIZ \\ S_2 = & ZXZIIIZIII & S_7 = & IZIIIZXZII \\ S_3 = & IZXZIIIZII & S_8 = & IIZIIIZXZI \\ S_4 = & IIZXZIIIZI & S_9 = & IIIZIIIZXZ \\ S_5 = & ZIIZXIIIIZ & S_{10} = & IIIIZZIIZX. \end{array} \tag{30}$$

This leads to a $|S\rangle$ that is a $[10, 0, 4]$ stabilizer state. Our classical code $\mathcal{C}$ giving the codeword s operators is

0000000000	1100101101	1100000100	0010010010
1001100100	0111011011	1101111110	0010111011
1001101111	0111010000	1111000101	1011010100
0101100000	1011011111	0101101011	0011000001
0000101001	1110010110	0001111010	1110111111.

V. Encoding Circuits

Thus far, we have focused on the existence and structure of CWS codes. We now address a question of fundamental importance: *What is the complexity of encoding a CWS code?* The answer we find is perhaps the strongest one could hope for: a CWS code will have an encoding circuit of the same complexity as the classical encoding circuit for the classical code $\mathcal{C}$.

We will use the fact [22] that a graph state $|S\rangle$ whose graph has edges E is equal to $\prod_{(j,k)\in E} P_{(j,k)} H^{\otimes n} |0\rangle^{\otimes n}$, where $P_{(j,k)}$ is the two qubit controlled phase gate, acting on qubits j and $k : P|x\rangle|y\rangle = (-1)^{xy}|x\rangle|y\rangle$.

Theorem 6: Let S and $\mathcal{C}$ define CWS code $\mathcal{Q}, C$ be a unitary encoding circuit for the classical code $\mathcal{C}$, and Q be the unitary mapping $|0\rangle^{\otimes n}$ to $|S\rangle$. Then

$$U_{(\mathcal{Q},\mathcal{C})} = QC \tag{31}$$

is an encoder for $\mathcal{Q}$. In particular, since Q has complexity no more than n^2, if C has complexity $f(n)$, the complexity of our encoder is $\max(n^2, f(n))$.

Proof: The ith quantum codeword $|\mathbf{c}_i\rangle$ is given by $C|i\rangle$ where $\mathbf{c}_i$ is the ith codeword of $\mathcal{C}$. So

$$QC|i\rangle = \prod_{(j,k)\in E} P_{(j,k)} H^{\otimes n} X^{\mathbf{c}_i} |0\rangle^{\otimes n} \tag{32}$$

$$= Z^{\mathbf{c}_i} \prod_{(j,k)\in E} P_{(j,k)} H^{\otimes n} |0\rangle^{\otimes n} \tag{33}$$

$$= Z^{\mathbf{c}_i} |S\rangle \tag{34}$$

□

VI. Discussion

We have presented a new framework for quantum codes and shown how it encompasses stabilizer codes, elucidates the structure of the known good nonadditive codes, as well as generates new nonadditive codes with excellent performance. It should be noted, however, that there do exist quantum codes outside of our framework, for example those of [21].

Our codeword stabilized codes are described by two objects as follows. First, the codeword stabilizer that without loss of generality can be taken to describe a graph state, and which transforms the quantum errors to be corrected into effectively classical errors. And second, a classical code capable of correcting the induced classical error model. With a fixed stabilizer state, finding a quantum code is reduced to finding a classical code that corrects the (perhaps rather exotic) induced error model. We also show that CWS codes include all stabilizer codes. This new way of thinking of stabilizer codes may help to find new codes with good properties. In fact, this method has since been used [23] to systematically categorize all codes of $n \leq 8$ and to find a $((10, 24, 3))$ code as well as slightly better distance-2 codes.

In a future work we hope to expand our work in several new areas. We will give algorithms for finding codes (some of which were employed to find the new codes presented here) as well as bounds on the computational complexity of the algorithms. We also hope to find more new codes, especially of distance higher than three. These have proven elusive as we have so far developed little intuition regarding which graphs to use to build good codes other than searching them all.

References

[1] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Found. Comput. Sci.*, pp. 124–134, 1994.

[2] R. Feynman, "Simulating physics with computers," *Int. J. Theoret. Phys.*, vol. 21, pp. 467–488, 1982.

[3] R. Feynman, "Quantum mechanical computers," *Found. Phys.*, vol. 16, no. 6, pp. 507–531, 1986.

[4] S. Lloyd, "Universal quantum simulators," *Science*, no. 273, p. 1073, 1996.

[5] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error," in *Proc. Twenty-Ninth Annu. ACM Symp. Theory Comput.*, 1997, pp. 176–188.

[6] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," Caltech Ph.D. dissertation, Psadena, CA, ArXiv:quant-ph/9705052v1.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. Sloane, "Quantum error correction via codes over gf(4)," *IEEE Trans. Inf. Theory*, vol. 44, p. 1369, 1387, 1998, arXiv:quant-ph/9608006.

[8] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "A nonadditive quantum code," *Phys. Rev. Lett.*, vol. 79, pp. 953–954, 1997, arXiv:quant-ph/9703002.

[9] J. A. Smolin, G. Smith, and S. Wehner, A Simple Family of Nonadditive Quantum Codes arXiv:quant-ph/0701065.

[10] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, "Nonadditive quantum error-correcting code," *Phys. Rev. Lett.*, vol. 99, p. 130505, 2007.

[11] V. Aggarwal and A. R. Calderbank, "Boolean functions, projections operators, and quantum error correcting codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1700–1707, Apr. 2008.

[12] V. Arvind, P. Kurur, and K. Parthasarathy, Nonstabilizer Quantum Codes From Abelian Subgroups of the Error Group arXiv:quant-ph/0210097.

[13] M. Grassl and T. Beth, A Note on Non-Additive Quantum Codes arXiv:quant-ph/9703016.

[14] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A.*, vol. 54, pp. 3824–3851, 1996, arXiv:quant-ph/9604024.

[15] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A.*, vol. 55, no. 2, pp. 900–911, 1997.

[16] D. Schlingermann, "Stabilizer codes can be realized as graph codes," *Quantum Inf. Comput.*, vol. 2, no. 4, pp. 307–323, 2002, arXiv:quant-ph/0111080.

[17] M. Grassl, A. Klappenecker, and M. Rötteler, "Graphs, quadratic form, and quantum codes," in *Proc. 2002 IEEE Int. Symp. Inf. Theory (ISIT)*, 2002, p. 45.

[18] M. Van den Nest, J. Dehaene, and B. DE Moor, "Graphical description of the action of local clifford transformations on graph states," *Phys. Rev. A.*, vol. 69, no. 022316, 2004.
[19] E. Rains, "Quantum shadow enumerators," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2361–2366, 1999, arXiv:quant-ph/9611001.
[20] E. Rains, "Quantum codes of minimum distance two," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 266–271, 1999, arXiv:quant-ph/9704043.
[21] H. Pollatsek and M. B. Ruskai, "Permutationally invariant codes for quantum error correction," *Lin. Alg. Appl.*, vol. 392, pp. 255–258, 2004, arXiv:quant-ph/0304153.
[22] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation with cluster states," *Phys. Rev. A.*, vol. 68, p. 022312, 2003.
[23] S. Yu, Q. Chen, and C. H. Oh, Graphical Quantum Error-Correcting Codes arXiv:0709.1780.

Andrew Cross is from Chardon, OH, and received the B.Sc. degree in electrical engineering from Case Western Reserve University, Cleveland, OH, in 2002 and the S.M. and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology, Cambridge, MA, in 2005 and 2008.

He currently works at the Science Applications International Corporation in the Washington, DC area. His interests include quantum computation, coding, and information theory.

Graeme Smith (M'04) received the B.Sc. degree in physics from the University of Toronto, Toronto, ON, Canada, in 2001 and the M.S. and Ph.D. degrees in physics from the California Institute of Technology, Pasadena in 2004 and 2006, respectively.

He is currently a Postdoctoral Fellow at the IBM T.J. Watson Research Center, Yorktown Heights, NY, working on quantum information theory, coding theory, and cryptography.

John A. Smolin received the S.B. degree in physics from the Massachusetts Institute of Technology (MIT), Cambridge, in 1989 and the Ph.D. degree, also in physics from the University of California, Los Angeles, in 1996.

Since receiving the Ph.D. degree, he has been at IBM T.J. Watson Research Center, Yorktown Heights, NY, first as a postdoc and subsequently as a Research Staff Member. He, together with Charles Bennett built the first quantum cryptography apparatus at IBM in 1989. His current research interests are in quantum information theory, coding theory, and quantum computation, with the occasional misguided foray into the foundations of quantum mechanics.

Bei Zeng received the B.Sc. degree in physics and mathematics and M.Sc. degree in physics from Tsinghua University, Beijing, China, in 2002 and 2004, respectively.

She is currently a Ph.D. candidate in department of physics, Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts, working on quantum information theory, quantum computation, coding theory, foundations of quantum mechanics, and mathematical physics.