Simple Family of Nonadditive Quantum Codes

John A. Smolin,[1,*] Graeme Smith,[1,2,†] and Stephanie Wehner[3,‡]

[1]*IBM T. J. Watson Research Center, Yorktown Heights, New York 10598, USA*
[2]*Department of Computer Science, University of Bristol, Bristol, BS8 1UB, United Kingdom*
[3]*C.W.I., Kruislaan 413, 1098 SJ Amsterdam, The Netherlands*

(Received 21 March 2007; published 28 September 2007)

Most known quantum codes are additive, meaning the code can be described as the simultaneous eigenspace of an Abelian subgroup of the Pauli group. While in some scenarios such codes are strictly suboptimal, very little is understood about how to construct nonadditive codes with good performance. Here we present a family of distance 2 nonadditive quantum codes for all odd block lengths n, that has a particularly simple form. Our codes detect single qubit errors (or correct single qubit erasures) while encoding a higher dimensional space than is possible with an additive code or, for $n \geq 11$, any previous codes. We exhibit the encoding circuits and automorphism group for our codes as well.

DOI: 10.1103/PhysRevLett.99.130505 PACS numbers: 03.67.Lx

Quantum error correcting codes will be essential if large-scale quantum computers are ever to be built. An error correcting code allows us to encode any quantum state into a larger system, such that errors can be detected. Single qubit errors are modeled by applying one of the Pauli operators X, Z, or Y to a qubit. Since any error can be written as a linear combination of Pauli operators, a code that can correct these errors can correct any error [1]; thus we can confine ourselves to the study of Pauli errors.

Nearly all known quantum codes are stabilizer (or additive) codes, in the framework of [2]. A code is called a stabilizer code, if there exists a set of Pauli operators S such that any code word is in the joint positive eigenspace of S. However, it has been known for some time that nonadditive codes can perform better [3]. Until quite recently this had only been shown for distance 2 quantum codes [4].

The *distance* of a code is the minimum number of errors it takes to change some code word into another. It can be shown that a distance 2 code can correct any single qubit erasure, or alternatively, can be used to detect a single qubit error with unknown location. Particularly in this second capacity, such codes may be quite important in the ancilla preparation phase of fault-tolerant quantum computing [7]. The family of codes presented in this Letter have particularly straightforward encoding circuits and may therefore be well suited to this task and easy to demonstrate experimentally. Furthermore, distance 2 codes promise to shed light on the structure of general quantum codes due to their simplicity. We use the term *code word* to refer to an encoding of a quantum basis state into an error correcting code. The *code space* is the space spanned by the code words.

It is shown in [8] that the best additive distance 2 codes are $[n, n-2, 2]$ for n even and $[n, n-3, 2]$ for n odd, where we have used the notation $[n, k, d]$ to indicate an n qubit additive code with distance d and k encoded qubits. In [9] it was shown that these codes are optimal for even n. For $n = 5$, a $((5, 6, 2))$ nonadditive code was found in [3], where we have used the notation $((n, K, d))$ to indicate a distance d code of size n qubits, protecting a K dimensional code space, in analogy with the standard classical notation of (n, K, d) denoting an n bit code encoding K elements and distance d. This code, together with the family of $((n, 3 \times 2^{n-4}, 2))$ codes it generates [9], gives the only performance improvement from nonadditive codes known for qubits. Here, we present a family of new nonadditive codes that improve on all known constructions. Our codes correct single qubit erasures while encoding a higher dimensional space than is possible with any additive code and, for $n \geq 11$, any nonadditive code known to date. In particular, we show how to construct $((n = 4k + 2l + 3, M_{k,l}, 2))$-codes where $M_{k,l} \approx 2^{n-2}(1 - \sqrt{2/[\pi(n-1)]})$. Our construction is not restricted to qubits, but can be extended to higher dimensional systems.

It is shown in [9] that for odd n the largest code space dimension $K_{\max}$ is bounded by

$$K_{\max} \leq 2^{n-2}\left(1 - \frac{1}{n-1}\right). \tag{1}$$

While we would like to approach this bound, at least for large n, we achieve a more modest goal. Our code is asymptotically almost optimal, but the rate of convergence is weaker due to the square root in $M_{k,l}$.

The code for $n = 5$.—We first describe our construction for $n = 5$ and then show how to extend it to general odd n. We obtain our quantum codes from specific classical codes. Consider the following five five-bit strings:

$$\mathbf{x}^{(j)} \qquad 0 \leq j < 5$$

whose ith bits are given by

$$x_i^{(j)} = \delta_{ij} \qquad 0 \leq i < 5.$$

These, together with their bitwise complements $\bar{\mathbf{x}}^{(j)}$, form a classical (5, 10, 2) code. This can be seen easily as every code word is either weight 1 or weight 4, and single bit errors necessarily change the weight of a code word by 1, taking it out of the code space. In the following, we will

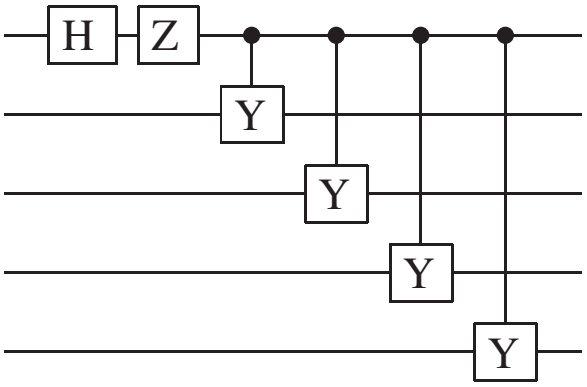

FIG. 1. Encoding circuit for the $n = 5$ code. It involves just four controlled-Y operations and a single Hadamard and Z operator. The circuit for general n has the same structure, just with more qubits.

call a code *self-complementary* if the complement of each code word is also in the code.

A quantum code must detect more than simply bitflips. It must detect the errors

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(''amplitude'' errors, analogous to the classical bitflip),

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(errors in phase) and $Y = XZ$ (when both errors occur) [10]. It will be sufficient to show for our code that any of these errors map code vectors to some vector orthogonal to the code space. The full necessary and sufficient error-correction conditions were derived in [1,11]. We now show how to turn the (5, 10, 2) classical code above into a $((5, 5, 2))$ quantum code. The five basis vectors of our quantum code are related to the classical code by taking superpositions of code words with their complements:

$$|v^{(j)}\rangle = |\mathbf{x}^{(j)}\rangle + |\bar{\mathbf{x}}^{(j)}\rangle \qquad 0 \le j < 5,$$
$$|v^{(0)}\rangle = |10000\rangle + |01111\rangle,$$
$$|v^{(1)}\rangle = |01000\rangle + |10111\rangle,$$
$$|v^{(2)}\rangle = |00100\rangle + |11011\rangle,$$
$$|v^{(3)}\rangle = |00010\rangle + |11101\rangle,$$
$$|v^{(4)}\rangle = |00001\rangle + |11110\rangle.$$

What is the effect of single qubit errors? Let $X_i = (\bigotimes_{j=0}^{i-1} I) \otimes X \otimes (\bigotimes_{j=i+1}^{n-1} I)$ denote an X error on qubit i, and similarly for Y and Z. X_i acts on the code words as

$$X_i|v^{(j)}\rangle = |\mathbf{x}^{(i)} \oplus \mathbf{x}^{(j)}\rangle + |\mathbf{x}^{(i)} \oplus \bar{\mathbf{x}}^{(j)}\rangle, \qquad (2)$$

so that for $i \neq j$ the $X_i|v^{(j)}\rangle$'s are all the ''+'' superpositions of weight two vectors with their weight three complements, while for $i = j$ we always have the state $|00000\rangle + |11111\rangle$, the superposition of the weight zero vector with its weight five complement. These are all orthogonal to the code space since they are constructed entirely of superpositions of weights not in the code words, which is a direct result of having started with a classical distance $d = 2$ code.

Turning our attention to the Z errors, we find

$$Z_i|v^{(j)}\rangle = (-1)^{\delta_{ij}}(|\mathbf{x}^{(j)}\rangle - |\bar{\mathbf{x}}^{(j)}\rangle).$$

These five vectors are the original code vectors but with a ''−'' as relative phase and sometimes an overall phase. They are all orthogonal to the code vectors and to one another, as well as to the X error states of Eq. (2).

Finally, Y errors act on the code words according to

$$Y_i|v^{(j)}\rangle = (-1)^{\delta_{ij}}(|\mathbf{x}^{(i)} \oplus \mathbf{x}^{(j)}\rangle - |\mathbf{x}^{(i)} \oplus \bar{\mathbf{x}}^{(j)}\rangle).$$

These are again orthogonal to the code space as they consist of superpositions of weights not included in the original code, and also to the image of the code under X and Z errors (the X's due to the relative phase, and the Z's due to being made of the wrong weight strings).

We emphasize that this code is not a subcode of the $((5, 6, 2))$ code in [3]. Indeed, it is not a subcode of *any* $((5, 6, 2))$ code, since there are no vectors orthogonal to the code space with distance 2 to all five vectors. To see this, observe that the set of vectors obtained by single qubit errors on the code vectors spans the entire space orthogonal to the code space. Since every vector outside the code space might be mistaken for a single error on some state in the code, no such vector can be added to our code while maintaining a minimum distance of 2.

The code for ODD n.—We now show how to extend our construction to any odd n. The method we have used is quite general, and is summarized in the following lemma, whose proof follows immediately from the reasoning above:

Lemma 1.—Any self-complementary $(n, K, d > 1)$ classical code leads to a $((n, K/2, 2))$ quantum code by pairing up codewords with their complements in superposition. □

Our construction again starts from a classical code, which is obtained as follows: We choose all code words of even weight or odd weight up to $(n - 1)/2 - 1$ and their complements. The choice of even or odd weights corresponds to whether $(n - 1)/2 - 1$ is even or odd. This ensures that all the classical code words are separated by at least distance 2. Formally: Choose an ordering of the weight i bit strings of length n and let $\mathbf{w}^{(i,j,n)}$ be the jth such string, where $0 \le j < \binom{n}{i}$. Letting $n = 4k + 2l + 3$ for $k \ge 0$, $l = 0, 1$, we consider the classical distance-2 codes indexed by (k, l) whose code words [indexed by (i, j)] are

$$\mathbf{v}_{(k,l)}^{(i,j)} = \mathbf{w}^{(2i+l,j,4k+2l+3)} \qquad 0 \le i \le k, \qquad 0 \le j < \binom{4k+2l+3}{2i+l} \tag{3}$$

together with their complements $\bar{\mathbf{v}}_{(k,l)}^{(i,j)}$. Note that our (5, 10, 2) code is the special case of (3) with $k = 0$, $l = 1$, giving us the stated $((5, 5, 2))$ quantum code.

Using Lemma 1, we now turn this code into an $((n = 4k + 2l + 3, M_{(k,l)}, 2))$ quantum code, spanned by

$$|\psi_{(k,l)}^{(i,j)}\rangle = |\mathbf{v}_{(k,l)}^{(i,j)}\rangle + |\bar{\mathbf{v}}_{(k,l)}^{(i,j)}\rangle \qquad 0 \le i \le k, \qquad 0 \le j < \binom{4k+2l+3}{2i+l}.$$

Let C_n denote our code.

It remains for us to count $M_{(k,l)}$, the total number of code vectors. We have for $l \in \{0, 1\}$ that

$$M_{(k,l)} = \sum_{i=0}^{k} \binom{4k+2l+3}{2i+l} = 2^{4k+2l+1} - \frac{1}{2}\binom{4k+2l+2}{2k+l+1},$$

where we have evaluated the sum using Pascal's first identity $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ [12].

As mentioned above, $((n, 3 \times 2^{n-4}, 2))$ codes were constructed in [9]. For $n \le 9$, these codes encode more elements than ours, while for $n \ge 11$ our codes have a larger code space. Evaluating $M_{(k,l)}$ as $n \to \infty$ gives

$$M_{(k,l)} = 2^{n-2}\left(1 - \frac{\binom{n-1}{\frac{n-1}{2}}}{2^{n-1}}\right) \approx 2^{n-2}\left(1 - \sqrt{\frac{2}{\pi(n-1)}}\right),$$

allowing us to asymptotically encode $n - 2 - \frac{1}{\ln 2}\sqrt{\frac{2}{\pi(n-1)}}$ qubits. While the rate of convergence to may be suboptimal [$O(\frac{1}{\sqrt{n}})$ vs $O(\frac{1}{n})$], in light of Eq. (1) the resulting limit of $n - 2$ encoded qubits cannot be surpassed and our code is asymptotically optimal.

The encoding circuit.—In order to actually use an $((n, K, d))$ code whose code space dimension K is not a power 2 it is necessary to define what the bare (unencoded) data look like. One option is to use a number of qubits r such that $K < 2^r$ and not use the entire Hilbert space available. Instead we choose to use n qubits, even for the bare data, and let the unencoded states be indexed by (i, j) be $|ij\rangle = |v_{(k,l)}^{(i,j)}\rangle$ where i, j, k, l and $|v_{(k,l)}^{(i,j)}\rangle$ are as in Eq. (3).

This is particularly nice in the case of $n = 5$ where one can think of the unencoded basis states as, for example, five cavities, one of which contains a single photon. For other values of n the states will involve multiple photons, but only ever occupying the zero or one photon modes in each cavity. The encoder's job is then to take the input state and superpose it with its complement (i.e., photons in all cavities where they were not in the input state). A circuit which achieves this is shown in Fig. 1. For our $((5, 5, 2))$ code, for example, where $k = 0$ and $l = 1$, the unencoded states that are given as input to the circuit are simply $|10000\rangle$, $|01000\rangle$, $|00100\rangle$, $|00010\rangle$, and $|00001\rangle$. The great economy of this circuit and of the bare states should allow these codes be used in experiment fairly easily.

The automorphism group.—The automorphism group of a code is the group of unitaries that map the code space to itself and consist of the composition of local unitaries on each qubit and a permutation of qubits. The automorphisms of a code characterize the code's symmetries. Since they correspond to the logical operations that can be applied transversely, they are relevant for fault-tolerant quantum computation. The following lemma gives the automorphism group of our code.

Lemma 2.—The automorphisms of C_n are exactly

$$(X^{\otimes n})^b Z^{\mathbf{f}} \circ \pi_n \equiv (X^{\otimes n})^b \left(\bigotimes_{l=1}^{n} Z^{f_l}\right) \circ \pi_n, \tag{5}$$

with $|\mathbf{f}|$ even, $b \in \{0, 1\}$ and $\pi_n \in S_n$ is a permutation.

This is most easily proved as a consequence of the following characterization of the projector onto C_n.

Lemma 3.—The projector onto C_n is given by

$$P_{C_n} = \frac{1}{2^n}(I^{\otimes n} + X^{\otimes n}) \sum_{s=0}^{\frac{n-1}{2}} K^{(2s)} \left(\sum_{|\mathbf{x}|=2s} Z^{\mathbf{x}}\right), \tag{6}$$

where we have let $K^{(2s)} = \sum_{i=0}^{k} K_{2i+l}^{(2s)}$, as well as $K_{2i+l}^{(2s)} = 2\sum_{t=0}^{2i+l}\binom{2s}{t} - \binom{n-2s}{2i+l-t}(s-t)$ for $s > 0$ and $K_{2i+l}^{(0)} = \binom{n}{2i+l}$.

Proof.—Letting $P_{2i+l} = \sum_j |\psi_{(k,l)}^{(i,j)}\rangle\langle\psi_{(k,l)}^{(i,j)}|$, we have

$$P_{2i+l} = \frac{1}{2} \sum_{|\mathbf{w}|=2i+l} \sum_{b_1 b_2=0}^{1} (X^{\otimes n})^{b_1} |\mathbf{w}\rangle\langle\mathbf{w}| (X^{\otimes n})^{b_2}, \tag{7}$$

which, using the fact that $|\mathbf{w}\rangle\langle\mathbf{w}| = \bigotimes_{l=1}^{n} (\frac{I + (-1)^{w_l} Z}{2})$, is equal to

$$\frac{1}{2^n} \sum_{|\mathbf{x}|\text{even}} \left(\sum_{|\mathbf{w}|=2i+l} (-1)^{\mathbf{x}\cdot\mathbf{w}}\right)(I^{\otimes n} + X^{\otimes n}) Z^{\mathbf{x}} = \frac{1}{2^n} \sum_{s=0}^{\frac{n-1}{2}} K_{2i+l}^{(2s)} (I^{\otimes n} + X^{\otimes n}) \left(\sum_{|\mathbf{x}|=2s} Z^{\mathbf{x}}\right).$$

Summing over $i = 0 \ldots k$ proves the claim. □

Proof (of Lemma 2).—Since our code is permutation invariant, we only need to show that the unitaries of the form $\bigotimes_{l=1}^{n} U_l$ leaving C_n invariant are exactly of the form $Z^{\mathbf{f}}$ or $X^{\otimes n} Z^{\mathbf{f}}$ with $|\mathbf{f}|$ even. To see this, note that Eq. (6) has terms of

two types: those of weight (the number of nonidentity Pauli operators) less than n, namely,

$$\frac{1}{2^n}\sum_{s=0}^{\frac{n-1}{2}} K^{(2s)}\Big(\sum_{|\mathbf{x}|=2s} Z^{\mathbf{x}}\Big), \tag{9}$$

and those of weight n. Since conjugation by local unitaries does not change the weight of a Pauli operator (and indeed, acts trivially on identity factors), if we wish P_{C_n} to be invariant under conjugation by $\bigotimes_{l=1}^n U_l$, we must have

$$\Big(\bigotimes_{l=1}^n U_l\Big) Z^{\mathbf{x}} \Big(\bigotimes_{l=1}^n U_l^\dagger\Big) = Z^{\mathbf{x}} \tag{10}$$

whenever $|\mathbf{x}|$ is even. In other words, $\bigotimes_{l=1}^n U_l$ must commute with $Z^{\mathbf{x}}$ for all even weight $\mathbf{x}$. This implies $\bigotimes_{l=1}^n U_l = (X^{\otimes n})^b Z^{\mathbf{f}}$ for $b \in \{0, 1\}$. To see that we must have $|\mathbf{f}|$ even, note that $(X^{\otimes n})^b Z^{\mathbf{f}}$ commutes with $\frac{1}{2^n} \times \sum_{s=0}^{\frac{n-1}{2}} K^{(2s)}(\sum_{|\mathbf{x}|=2s} Z^{\mathbf{x}})$, so that to commute with P_{C_n} it must also commute with $X^{\otimes n}$. □

Conclusion.—Our family of codes can be extended to Heisenberg-Weyl type errors on higher dimensions than qubits with exactly the same counting as before. The errors from this group—the natural generalization of the Pauli group—are generated by the D-dimensional operators defined by

$$X|j\rangle = |(j+1) \bmod D\rangle, \tag{11}$$

$$Z|j\rangle = e^{2\pi j i/D}|j\rangle. \tag{12}$$

Instead of using classical code words paired with their complements, one uses code words of the form

$$|\mathbf{v}\rangle + X^{\otimes n}|\mathbf{v}\rangle + (X^{\otimes n})^2|\mathbf{v}\rangle \ldots (X^{\otimes n})^{D-1}|\mathbf{v}\rangle. \tag{13}$$

The same classical code words $\mathbf{v}$ of Eq. (3) generate quantum $((4k + 2l + 3,\ M_{(k,l)}, 2))$-codes with $M_{(k,l)}$ as before.

So far we have not been able to find similar constructions for higher distances as Lemma 1 is specific to distance 2, but we are hopeful our work will inspire new thinking on nonadditive codes.

Thanks to A. W. Cross and S. Bravyi for helpful discussions. J. A. S. thanks ARO Contract No. DAAD19-01-C-0056 and G. S. thanks the UK Engineering and Physical Sciences Research Council. S. W. thanks IBM Watson for their hospitality, and the NWO vici grant No. 2004-2009 and EU project QAP (No. IST-2005-15848) for support.

*smolin@watson.ibm.com
†gsbsmith@gmail.com
‡wehner@cwi.nl

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[2] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[3] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **79**, 953 (1997).
[4] A $((9, 12, 3))$ quantum code was demonstrated in [5] and $((10, 18, 3))$, $((10, 20, 3))$, and $((11, 48, 3))$ codes have be since been found [6].
[5] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, arXiv:0704.2122.
[6] A. W. Cross, G. Smith, J. A. Smolin, and B. Zeng (to be published).
[7] E. Knill, Nature (London) **434**, 39 (2005).
[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[9] E. M. Rains, IEEE Trans. Inf. Theory **45**, 266 (1999).
[10] We omit factors of $\sqrt{-1}$ in the Pauli matrices.
[11] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[12] B. Pascal, Traité du triangle arithmétique, 1654.