A Nonadditive Quantum Code

Eric M. Rains, R. H. Hardin, Peter W. Shor, and N. J. A. Sloane
AT&T Research, 600 Mountain Ave., Murray Hill, NJ 07974, USA
(March 3, 1997)

Up to now every good quantum error-correcting code discovered has had the structure of an eigenspace of an Abelian group generated by tensor products of Pauli matrices; such codes are known as *stabilizer* or *additive* codes. In this letter we present the first example of a code that is better than any code of this type. It encodes six states in five qubits and can correct the erasure of any single qubit.

Most present models for quantum computers require quantum error-correcting codes [1–4] for their operations. Many recent papers have been devoted to the construction of these codes [5–9]. Up to now all good codes known have fallen into the class of what have been called "stabilizer" or "additive" codes [7,9]. These are not the most general quantum codes, however, and it was an open question as to whether more general codes could be more powerful. In the present letter we present a code which is not a stabilizer code, and which is strictly better than any code of this type.

Stabilizer codes are defined as follows. Let the extraspecial group E be generated by all tensor products $M_1 \otimes M_2 \otimes \ldots \otimes M_n$, where each M_i is one of $\{I, \sigma_x, \sigma_y, \sigma_z\}$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

σ_x, σ_y, σ_z being the Pauli matrices. Then a *stabilizer* code is a joint eigenspace of an Abelian subgroup of E.

The new code. Since a quantum code is a subspace of the Hilbert space $\mathbb{C}^{2^n}$, we may define it by giving the orthogonal projection matrix onto this subspace. Since the Pauli matrices together with I form a basis for the space of 2×2 Hermitian matrices, we may write the projection as a linear combination of elements of E. In this form, the new code Q is defined by the projection matrix

$$\begin{aligned} P = 1/16 \, [\; & 3 \;\; I \otimes I \otimes I \otimes I \otimes I \\ & + \;\; (I \otimes \sigma_z \otimes \sigma_y \otimes \sigma_y \otimes \sigma_z)_{\mathrm{cyc}} \\ & + \;\; (I \otimes \sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x)_{\mathrm{cyc}} \\ & - \;\; (I \otimes \sigma_y \otimes \sigma_x \otimes \sigma_x \otimes \sigma_y)_{\mathrm{cyc}} \\ & + 2\,(\sigma_z \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x)_{\mathrm{cyc}} \\ & - 2 \;\; \sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z], \end{aligned}$$

where the subscript "cyc" indicates that all five cyclic shifts occur. It is straightforward to verify that $P^2 = P$ and $\mathrm{Trace}(P) = 6$, so that the eigenvalues of P are 1 (6 times) and 0 (26 times). Thus P projects onto a six-dimensional space.

It remains to verify that the code has minimum distance 2, that is, that it can correct one erasure. For a code to correct one erasure it suffices for it to be orthogonal to its image under any single qubit error. Since Q is cyclic, it is enough to consider an error in the first qubit. There are thus three cases to check: conjugation of P by $\eta = M \otimes I \otimes I \otimes I \otimes I \otimes I$ where M is one of σ_x, σ_y, σ_z, obtaining $P' = \eta P \eta$. We verify in each case that $PP' = 0$. Thus Q is a ((5,6,2)) code, as claimed.

Further properties of the code. Since the code is cyclic, we label the qubits by $0, 1, \ldots, 4$ (mod 5). The code also has the symmetry defined by

$$k \to 2k \text{ (mod 5)}, \;\; \sigma_x \to \sigma_y, \;\; \sigma_y \to -\sigma_x. \tag{1}$$

There are further symmetries that do not permute the qubits, for example conjugation by the element

$$\sigma_z \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x \tag{2}$$

of E, or any of its cyclic shifts. These five elements generate a subgroup of E of size 32, which we call H. Moreover, since this group is Abelian, it has 32 one-dimensional eigenspaces, and Q is the span of six of them. (Each of these eigenspaces is a ((5,1,3)) stabilizer quantum code.) This gives an explicit basis for our code, namely:

$$|00000\rangle - (|00011\rangle)_{\mathrm{cyc}} + (|00101\rangle)_{\mathrm{cyc}} - (|01111\rangle)_{\mathrm{cyc}} \tag{3}$$

together with all five cyclic shifts of

$$\begin{aligned} & |00001\rangle - |00010\rangle - |00100\rangle - |01000\rangle - |10000\rangle \\ & + |00111\rangle - |01110\rangle - |11100\rangle + |11001\rangle + |10011\rangle \\ & - |01011\rangle + |10110\rangle - |01101\rangle + |11010\rangle - |10101\rangle \\ & - |11111\rangle \end{aligned} \tag{4}$$

By examining how single bit errors act on these 32 eigenspaces, one can again see that the image of Q under such an error is orthogonal to Q, by noting that the six new eigenspaces are disjoint from the original six.

The symmetries discussed above generate a group of order 640. There is an additional symmetry, which can be described as follows: First, permute the columns as $k \to k^3$, that is, exchange the qubits 2 and 3. Next, for each qubit, negate one of the Pauli matrices and exchange the other two, where the Pauli matrices negated are σ_z, σ_y, σ_x, σ_x, σ_y, respectively. This increases the size of the symmetry group to 3840. The group acts as the permutation group S_5 on the qubits. This is the full group of symmetries of the code, that is, the full subgroup of the semidirect product of S_5 and $PSU(2)^5$ that preserves the code [12].

In principal one can construct other codes in a similar manner, e.g. as the spans of translates of self-dual stabilizer codes. Let C_0 be a self-dual additive code of length n with associated stabilizer quantum code Q_0 and let C be the union of K cosets of C_0. If C has minimum distance d, then there exists an $((n, K, d))$ quantum code. This code is obtained as the span of the translates of Q_0 under the operators in C. For our code, for instance, C_0 is the $[[5, 0, 3]]$ additive code H and C is $C_0 + (\sigma C_0)_{\rm cyc}$, where

$$\sigma = \sigma_x \otimes \sigma_z \otimes I \otimes I \otimes I.$$

Thus, for example, we have

$$P = P_0 + (\sigma P_0 \sigma^{-1})_{\rm cyc}, \tag{5}$$

where P_0 is $|x\rangle\langle x|$ and $|x\rangle$ is given by Eq. (3).

We remark that the only stabilizer code that contains Q is the trivial code consisting of the entire Hilbert space.

How the code was discovered. Investigation of the linear programming bound for quantum codes (cf. [8,10,11]) revealed that for a length 5 code of minimum distance 2 the dimension $K = 6$ is extremal. In fact, the inequalities cannot even be satisfied for any *real* $K > 6$. This suggested a ((5,6,2)) code as a natural place to look. Further, the weight enumerator of any such code is uniquely determined by linear programming; with the normalization used in [11], it is

$$A(u, v) = 36u^5 + 60uv^4 + 96v^5. \tag{6}$$

The best stabilizer code of this length and distance has dimension $K = 4$ [8, Table III].

Rather than look for a projection matrix with this weight enumerator, we decided to look for a matrix with this weight enumerator that happened to be a projection. We describe a near projection matrix M as a linear combination of elements of E. Beginning with a random matrix M, we first scaled the contribution from the terms of each weight so as to force the desired weight enumerator. We then replaced M by $M' = 2M^2 - M^4$. (This moves small eigenvalues of M closer to 0 and large eigenvalues closer to 1.) We then iterated these two steps. On our first attempt, the algorithm converged to a (complex) projection matrix. Since the algorithm preserves symmetry, by choosing our initial guess to be real, we obtained a real code equivalent to the code described above. We omit the details of transforming the computer output into the above form. Note that we did not choose our initial guess to be cyclic, but nonetheless obtained a code equivalent to one with cyclic symmetry.

Acknowledgement. We thank Rob Calderbank for helpful discussions concerning the description of the code in terms of cosets.

---

[1] P. W. Shor, Scheme for reducing decoherence in quantum memory, Phys. Rev. A. **52,** 2493 (1995).

[2] A. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. **77,** 793 (1996).

[3] A. Ekert and C. Macchiavello, Error correction in quantum communication, Phys. Rev. Lett. **77,** 2585 (1996).

[4] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A **55,** 900 (1997).

[5] A. Steane, Multiple particle interference and quantum error correction, Proc. R. Soc. London A **452,** 2551 (1996). Also LANL e-print quant-ph/9512032.

[6] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A **54,** 1098 (1996).

[7] D. Gottesman, A class of quantum error-correcting codes saturating the quantum Hamming bound, Phys. Rev. A **54,** 1844 (1996).

[8] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, Phys. Rev. Lett. **78,** 405 (1997). Also LANL e-print quant-ph/9608006.

[9] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), LANL e-print quant-ph/9608006.

[10] E. M. Rains, Quantum codes of minumum distance two, LANL e-print quant-ph/9704043.

[11] P. W. Shor and R. A. Laflamme, Quantum analog of the MacWilliams identities in classical coding theory, Phys. Rev. Lett., **78,** 1600 (1997), also LANL e-print quant-ph/9610040.

[12] E. M. Rains, Quantum shadow enumerators, LANL e-print quant-ph/9611001.