Perfect Quantum Error Correcting Code

Raymond Laflamme,[1] Cesar Miquel,[1,2] Juan Pablo Paz,[1,2] and Wojciech Hubert Zurek[1]
[1]*Theoretical Astrophysics, T-6, MS B288, Los Alamos National Laboratory, Los Alamos, New Mexico 87545*
[2]*Departamento de Física, FCEyN, Pabellón 1, Ciudad Universitaria, 1428 Buenos Aires, Argentina*

(Received 28 February 1996)

We present a quantum error correction code which protects a qubit of information against general one qubit errors. To accomplish this, we encode the original state by distributing quantum information over five qubits, the minimal number required for this task. We describe a circuit which takes the initial state with four extra qubits in the state $|0\rangle$ to the encoded state. It can also be converted into a decoder by running it backward. The original state of the encoded qubit can then be restored by a simple unitary transformation. [S0031-9007(96)00480-2]

PACS numbers: 89.70.+c, 02.70.–c, 03.65.–w, 89.80+h

Quantum computation—which has attracted so much attention as a result of progress in designing efficient quantum algorithms [1,2]—is still far from practical implementation. The biggest difficulty is the fragility of the quantum states required to process information. All the proposed implementations will suffer from the interaction with the environment, and even a weak coupling may result in decoherence [3–5]. Moreover, other sources of errors (i.e., timing of laser pulses in the linear trap computer of Ref. [6]) will add to the problem.

In classical computers, errors can also occur and are handled through various error correcting techniques [7]. However, in the quantum case different error correction techniques are needed to protect quantum superposition and entanglement (which are essential ingredients of quantum computation). The simplest scheme [8] of this sort can be based on a purely quantum watchdog effect. It has been recently demonstrated to show promise [9], but it suffers from an imperfection of being essentially probabilistic; i.e., in principle only some of the correctable errors will actually be corrected by its application. Thus in the terminology of the error correction community, this scheme is not perfect [7].

Shor [10] has championed a different strategy (based on classical schemes using redundancy). The idea is to store quantum information not in a single qubit but in an entanglement of nine qubits. This scheme allows one to correct for any error incurred by any one of the nine qubits. Steane [11] and Calderbank and Shor [12] have proposed a different scheme which uses only seven bits for this purpose and demonstrated that this is the least required for the strategies inspired by the classical coding theory which is based on linear codes [11]. However, these codes are not perfect as they use more bits than is absolutely necessary to correct one-bit errors [7].

In the quantum case at hand, classical coding theory seems to be too restrictive. All classical codes are based on the Hamming distance [13] (the number of different bits between two code words). Efficient quantum codes will have to use a quantum analog of this distance. Below we present a perfect (i.e., capable of correcting all one-bit errors with the minimum number of extra qubits) quantum error correction code using only five qubits (shown to be the smallest possible number). Our code is *not* a classical linear code [11] but a truly quantum code. Some of its mathematical properties are discussed below but others certainly deserve further study. A notable property of our error correction code is that the encoding can be done using a remarkably simple circuit which is itself the central piece of the error correction scheme enabling us to recover from general one-bit errors.

Before presenting our perfect code, let us mention what requirements it must satisfy. An encoding of one qubit into n qubits is a representation of the logical states $|0_L\rangle$ and $|1_L\rangle$ as entangled states in the n-particle Hilbert space

$$|0_L\rangle = \sum_{i=0}^{2^n-1} \mu_i |i\rangle, \qquad |1_L\rangle = \sum_{i=0}^{2^n-1} \nu_i |i\rangle, \tag{1}$$

where the states $|i\rangle = |i_{n-1}, \ldots, i_0\rangle$ form a basis of the n-particle Hilbert space with i_j defining the binary representation of the integer i. To serve as a quantum error correction code Eq. (1) must satisfy certain conditions whose origin is best understood by analyzing the effect of the interaction with the environment. A general interaction between the kth qubit and its environment will lead to an evolution of the form

$$\begin{aligned} |e\rangle|0_k\rangle &\rightarrow |e_0\rangle|0_k\rangle + |e_0^B\rangle|1_k\rangle, \\ |e\rangle|1_k\rangle &\rightarrow |e_1\rangle|1_k\rangle + |e_1^B\rangle|0_k\rangle, \end{aligned} \tag{2}$$

where $|e\rangle$, $|e_{0,1}\rangle$, $|e_{0,1}^B\rangle$ are states of the environment which will remain arbitrary throughout this paper [apart from the obvious orthogonality and normalization constraints imposed by unitarity of the evolution in Eq. (2)]. The effect of the interaction given by Eq. (2) upon the logical states $|0_L\rangle$ and $|1_L\rangle$ is easily calculated,

$$|e\rangle \begin{matrix} |0_L\rangle \\ |1_L\rangle \end{matrix} \rightarrow (|e_+\rangle I + |e_-\rangle\sigma_z^k + |e_+^B\rangle\sigma_x^k - |e_-^B\rangle i\sigma_y^k) \begin{matrix} |0_L\rangle \\ |1_L\rangle \end{matrix}, \tag{3}$$

where σ_i^k are the Pauli matrices acting on the kth bit. The states of the environment appearing in Eq. (3) are

$|e_\pm\rangle = (|e_0\rangle \pm |e_1\rangle)/2$ and $|e^B_\pm\rangle = (|e^B_0\rangle \pm |e^B_1\rangle)/2$. Four types of outcome due to interaction with the environment exhaust all possibilities. First, the state may remain unchanged (the operator I is proportional to the identity). Second, the state of the system may pick a minus sign in front of all the states with a 1 in the kth qubit (thus corresponding to action of the operator σ_z^k). This alternative is correlated with the environment $|e_-\rangle$. Third, the state of the system may be altered by flipping the kth bit (through the operator σ_x^k) getting correlated with the states $|e^B_+\rangle$. Fourth, and finally, the system may get a bit flip in the kth bit together with a sign flip for which the operator is $-i\sigma_y^k$, an option correlated with $|e^B_-\rangle$. The second operation is denoted by S_k (for *sign* flip), the third by B_k (for *bit* flip), and the fourth one by BS_k (which is self-explanatory). Note that the same state of the environment is coupled to the respective states of $|0_L\rangle$ and $|1_L\rangle$. This is essential in what follows.

A sufficient property to define a quantum error correction code Eq. (1) is the following: the original two-dimensional Hilbert space spanned by $|0_L\rangle$ and $|1_L\rangle$ must be mapped coherently into orthogonal two-dimensional Hilbert spaces corresponding to each of the different environment-induced errors (denoted by S_k, B_k, and BS_k). This is sufficient to recover from a one-qubit error since it is possible to measure in which 2D Hilbert space the system is without destroying the relevant coherence. After the measurement it is possible to restore the original quantum state by means of simple unitary transformations (which depend upon the result of the measurement).

Orthogonality of the subspaces corresponding to the different errors imposes a rather stringent constraint on the dimension of the Hilbert space which must be large enough to accommodate so many orthogonal subspaces. How big should this space be? Orthogonality requires a subspace for each of the three errors every qubit can suffer and another one for the unperturbed logical state. This makes a total of $3n + 1$. We must double this to have enough space to accommodate both logical states and their erroneous descendants. Thus, the number of subspaces is $2(3n + 1)$. To have enough room in the Hilbert space the condition

$$2(3n + 1) \leq 2^n \tag{4}$$

must be satisfied. Both Shor's $n = 9$ code and Steane's $n = 7$ code satisfy this constraint while $n = 5$ is the number which saturates Eq. (4). The code we present has 5 bits.

The orthogonality conditions can be written as algebraic constraints on the coefficients μ_i and ν_i which define the encoding. For the sake of space and time we will not write them all explicitly but just mention the following simple subset:

$$\sum_{\substack{k\text{ even}\\ l\text{ even}}} |\mu_i|^2 = \sum_{\substack{k\text{ even}\\ l\text{ odd}}} |\mu_i|^2 = \sum_{\substack{k\text{ odd}\\ l\text{ even}}} |\mu_i|^2 = \sum_{\substack{k\text{ odd}\\ l\text{ odd}}} |\mu_i|^2, \tag{5}$$

for all $k, l = 1, \ldots, 5$ (and a similar condition for ν_i). The sums are over k even and k odd numbers: k even (k odd) numbers are those with a 0 (1) in the kth bit. If we restrict ourselves to encodings satisfying $|\mu_i| = |\nu_i| = 1$, an assumption based on simplicity, the above condition implies that we need at least eight states in the superposition. Thus, five bits and eight states in the superposition seem to be the minimum required by the orthogonality conditions (and the simplicity assumption). Moreover, it is easily shown that it is impossible to satisfy all the constraints by using only positive numbers for μ's or ν's ($+1$ in our case) so either phases or minus signs are essential.

The conditions of Eq. (5), while still incomplete, are nevertheless extremely restrictive: In fact, one can prove that they essentially determine (up to permutations between bits) what are the eight states $|i\rangle$ allowed in the superposition of Eq. (1). This determines the encoding of each of the logical states, thus defining the support of the code. It is interesting to note that the solution can be guessed from Steane's encoding [11] by dropping any two of its qubits. The only remaining freedom is in the sign distribution between states, which can be found by solving simple algebraic equations. This is how we have arrived at the class of possible encodings exemplified by the following perfect five-bit code:

$$\begin{aligned} |0_L\rangle = &- |00000\rangle + |01111\rangle - |10011\rangle + |11100\rangle \\ &+ |00110\rangle + |01001\rangle + |10101\rangle + |11010\rangle, \\ |1_L\rangle = &- |11111\rangle + |10000\rangle + |01100\rangle - |00011\rangle \\ &+ |11001\rangle + |10110\rangle - |01010\rangle - |00101\rangle \end{aligned} \tag{6}$$

(up to the obvious normalization). Other allowed codes can be found from Eq. (6) by permutations of bits and coordinated sign changes. Thus, all the allowed codes have the same sign pattern, with two minus signs in one of the logical states and four in the other (these results will be proven in detail elsewhere). The mathematical structure behind this sign distribution (which, as we said before, is the only freedom we have, save for the "gauge transformation" in the form of sign and coordinated bit flips) still lies beyond our present understanding.

The encoding Eq. (6) can be implemented by using the circuit depicted in Fig. 1(a). The original information carrier is the qubit $|Q\rangle$ which may be in a general state $|Q\rangle = \alpha|0\rangle + \beta|1\rangle$. After the action of the encoding circuit, and when the other input states are all set to $|0\rangle$, the output state will always be given by $\alpha|0_L\rangle + \beta|1_L\rangle$. This circuit is just a combination of quantum logic gates (controlled not, controlled rotations, etc.) which can be implemented (at least *in principle*) in various physical settings.

Until now we exhibited a quantum code and a quantum circuit which acts as encoder. However, the error correction method would not be complete without the circuit for actually *correcting* all the possible one-bit errors. The

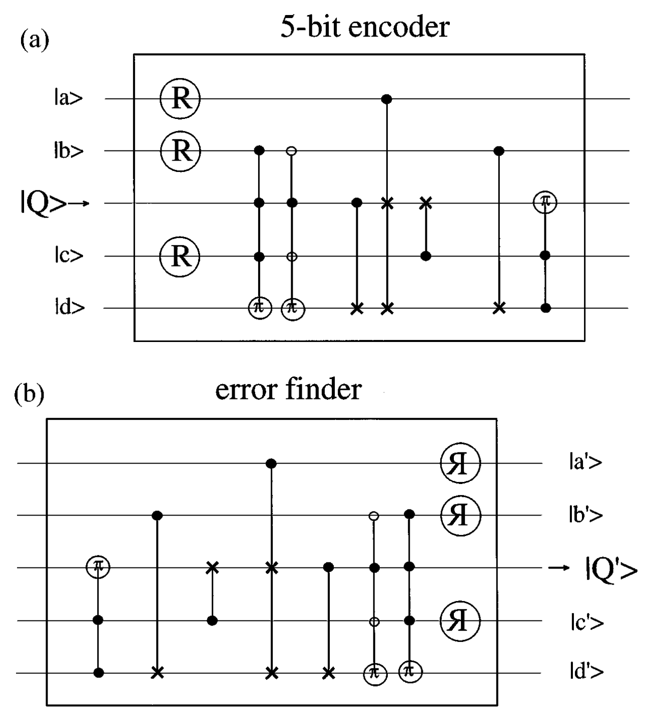

FIG. 1. (a) Circuit for the encoding of the states described in Eq. (6). R describes the rotation $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$. The element with an × corresponds to a control not (with control on the filled circle); if the control is $|1\rangle$ then the state at × is flipped. The element including π corresponds to a conditional rotation by a phase π, where the condition is satisfied when the state has the bit in the 0 state for the empty circle and 1 for the filled one. (b) Circuit of (a) run in the opposite way. The state $|a', b', c', d'\rangle$ gives the syndromes of Table I. A unitary transformation brings back $|Q'\rangle$ to $|Q\rangle$, which can be reencoded using the circuit of (a).

most remarkable feature of our method is that the circuit for this is *exactly the same as the one for encoding but run backwards* [see Fig. 1(b)]. This is in contrast with all previous schemes discussed in the literature where a different decoding or correction circuit was necessary.

A heuristic argument has guided us in searching for this circuit. The fact that we are using exactly $n = 5$ bits allows us *in principle* to have a circuit like the one we found. To distinguish the 16 different error syndromes (the "no error alternative" plus the 15 ones corresponding to five errors of each type S_k, B_k, and BS_k) we would need to make four binary tests (which would provide us with 16 results). This is precisely what the circuit does: when any one of the sixteen possible states inputs the encoder from the right, the states $|a'\rangle$, $|b'\rangle$, $|c'\rangle$, and $|d'\rangle$ uniquely identify the input and allow us to know what the state of the qubit $|Q'\rangle$ is. All possibilities are exhibited in Table I. Some of them are easily understood. For example, the trivial case $|a'\rangle = |b'\rangle = |c'\rangle = |d'\rangle = |0\rangle$ corresponds to the "no error" alternative (since in that case the input in the left is identical to the one used for encoding). Other alternatives, such as the one corresponding to the S_1 syndrome (an error in the first bit), can be easily identified by looking at the circuit from the left to the right: In fact, if the input to the encoder is not $|a\rangle = |b\rangle = |c\rangle = |d\rangle = |0\rangle$ but $|a\rangle = |1\rangle$, $|b\rangle = |c\rangle = |d\rangle = |0\rangle$, the output state is easily seen to be the one corresponding to the S_1 error (since the first rotation would produce a state with a minus sign in front of the $|1\rangle$ state). Other alternatives are less obvious but they all work in the same way.

Thus, after using the encoding circuit in backwards direction we have a precise diagnosis of what went wrong (if anything) with our quantum bit. The state of the qubit $|Q'\rangle$ may be easily restored to the original $\alpha|0\rangle + \beta|1\rangle$ by a unitary transformation which depends upon the measurement of the states $|a'\rangle$, $|b'\rangle$, $|c'\rangle$, and $|d'\rangle$ [14].

Assuming that the interaction affected at most one bit in any way, we have shown that there exists a five-qubit code which corrects perfectly, i.e., has perfect fidelity [15]. It is not difficult to convince yourself that if the probability of an error in only one qubit is p, the fidelity of the code where the restriction to only one error is lifted will be $1 - cp^2 + \cdots$, for some constant c. This is an improvement on the uncorrected evolution of a single qubit which has fidelity $1 - p$ as long as $c < 1/p$.

The support of our code is unique under the conditions (i) that the coefficients of the codewords have unit modulus and (ii) that under error due to the interaction with the environment the logical states would go to mutually orthogonal states [16].

We would like to thank E. Knill and B. Schumacher for many useful comments concerning classical and quantum error correction codes as well as R. Hughes for general comments about quantum computation. We are also

TABLE I. Error with corresponding syndromes and states for the decoder shown in Fig. 1. B, S, and BS correspond to a bit, a sign, or a bit and a sign flipped with the following number which identifies the bit. To recover the initial state, 5 different unitary operations must be performed consisting of bit and sign flips on the state $|Q'\rangle$.

Error	Syndrome $\lvert a'b'c'd'\rangle$	Resulting state $\lvert Q'\rangle$
None	0000	$\alpha\lvert 0\rangle + \beta\lvert 1\rangle$
$BS3$	1101	$-\alpha\lvert 1\rangle + \beta\lvert 0\rangle$
$BS5$	1111	$-\alpha\lvert 0\rangle + \beta\lvert 1\rangle$
$B2$	0001	$\alpha\lvert 0\rangle - \beta\lvert 1\rangle$
$S3$	1010	
$S5$	1100	
$BS2$	0101	
$B5$	0011	$-\alpha\lvert 0\rangle - \beta\lvert 1\rangle$
$S1$	1000	
$S2$	0100	
$S4$	0010	
$B1$	0110	$-\alpha\lvert 1\rangle - \beta\lvert 0\rangle$
$B3$	0111	
$B4$	1011	
$BS1$	1110	
$BS4$	1001	

grateful to A. Ekert for discussions on the size of error correcting codes.

Note added.—After completion of this work the IBM group [17] let us know that they also found a five-bit code. Their code is a "gauge transformation" of our code.

[1] For reviews see D. P. DiVincenzo, Science **270**, 255 (1995); S. Lloyd, Sci. Am. **273**, No. 4, 140 (1995); A. Ekert and R. Jozsa, Rev. Mod. Phys. (to be published).

[2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* edited by S. Goldwasser (IEEE Computer Society Press, New York, 1994), pp. 124–134.

[3] W. H. Zurek, Phys. Today **44**, No. 10, 36 (1991).

[4] W. G. Unruh, Phys. Rev. A **51**, 992 (1995).

[5] I. Chuang, R. Laflamme, P. Shor, and W. H. Zurek, Science **270**, 1633 (1995).

[6] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[7] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Publishing Company, New York, 1977).

[8] W. H. Zurek, Phys. Rev. Lett. **53**, 391 (1984).

[9] C. Miquel, J. P. Paz, and R. Perazzo, Report No. quant-ph/9601021.

[10] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).

[11] A. Steane, Report No. quant-ph/9601029 (to be published).

[12] A. R. Calderbank and P. W. Shor, Report No. quant-ph/9512032.

[13] E. A. Lee and D. G. Messerschmitt, *Digital Communication* (Kluwer Academic Publishers, Dordrecht, 1988).

[14] This last unitary transformation can be omitted if we redefine the meaning of logical 0 and 1 in the quantum program.

[15] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[16] This last condition is sufficient for the code to operate properly but is not necessary. It is possible to find codes such that some errors are mapped to the same 2D subspace. This alternative, which is now under investigation, does not allow less than five qubits but might allow one to detect or even correct more than the one-qubit errors (E. Knill and R. Laflamme, Report No. quant-ph/9604034).

[17] C. H. Bennett and D. DiVincenzo (private communication). See also C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Report No. quant-ph/9604006.