Quantum code words contradict local realism

David P. DiVincenzo
IBM Research Division, IBM T. J. Watson Research Center, Yorktown Heights, New York 10598

Asher Peres*
Institute for Theoretical Physics, University of California, Santa Barbara, California 93106

(Received 8 November 1996)

Quantum code words are highly entangled combinations of two-state systems. The standard assumptions of local realism lead to logical contradictions similar to those found by Bell, Kochen, and Specker, Greenberger, Horne and Zeilinger, and Mermin. The new contradictions have some noteworthy features that did not appear in the older ones. [S1050-2947(97)00306-5]

PACS number(s): 03.65.Bz, 89.80.+h, 89.70.+c

Quantum code words are highly entangled combinations of two-state quantum systems (qubits). They are structured in such a way that if one (or sometimes more) of the qubits is perturbed, there remains enough quantum information encoded in the remaining qubits for restoring the original code word unambiguously [1–4]. In this article, we investigate some properties of the five-qubit code words invented by Bennett *et al.* [5] (which are equivalent, up to a change of bases of the individual qubits, to the five-qubit code words of Laflamme *et al.* [2]). The logical 0 is represented by the quantum state

$$\begin{aligned}|0_L\rangle=\frac{1}{4}[&-|00000\rangle-|11000\rangle-|01100\rangle-|00110\rangle\\&-|00011\rangle-|10001\rangle+|10010\rangle+|10100\rangle+|01001\rangle\\&+|01010\rangle+|00101\rangle+|11110\rangle+|11101\rangle\\&+|11011\rangle+|10111\rangle+|01111\rangle],\end{aligned}\tag{1}$$

where, e.g., $|10010\rangle$ means $|1\rangle\otimes|0\rangle\otimes|0\rangle\otimes|1\rangle\otimes|0\rangle$, and $|0\rangle$ and $|1\rangle$ are any two orthogonal states of a physical qubit. The logical 1, denoted by $|1_L\rangle$, is obtained by exchanging all the $|0\rangle$ and $|1\rangle$ in $|0_L\rangle$. These two code words have the useful property of being invariant under cyclic permutations of the physical qubits. This greatly simplifies the calculations below.

Let σ_x, σ_y, and σ_z be the standard Pauli spin matrices, and σ_u denote the unit matrix (the latter will also be denoted by the symbol 1, with no risk of error). It is convenient to introduce the notation

$$\sigma_{abcde}\equiv\sigma_{1a}\sigma_{2b}\sigma_{3c}\sigma_{4d}\sigma_{5e}\equiv\sigma_a\otimes\sigma_b\otimes\sigma_c\otimes\sigma_d\otimes\sigma_e,\tag{2}$$

where the indices $abcde$ may be any combination of u, x, y, and z. It is then readily verified that $|0_L\rangle$ and $|1_L\rangle$ are eigenvectors, with eigenvalue 1, of the 32 following operators: σ_{uuuuu}, $\pm\sigma_{zzzzz}$, and

$$\begin{gathered}\sigma_{xzuzx},\quad\sigma_{yxuxy},\quad\sigma_{zyuyz},\quad\mp\sigma_{uxzxu},\\\mp\sigma_{yuzuy},\quad\pm\sigma_{xyzyx},\end{gathered}\tag{3}$$

and their cyclic permutations. The upper and lower signs refer to $|0_L\rangle$ and $|1_L\rangle$, respectively, (this convention will be followed throughout this article). These 32 operators (with either choice of sign) form an Abelian group; those that are unsigned in Eq. (3) form an invariant subgroup. The existence of such a group associated with this type of quantum error correction codes seems to be quite general. A group-theoretic framework for codes has been extensively developed by Gottesman [6] and by Calderbank *et al.* [7].

It is well known that, for any entangled state, it is possible to find operators whose correlations violate Bell's inequality [8,9]. However the code word (1) leads to a stronger type of violation, without inequalities [10,11]. In this paper, it will be shown that the code word (1) and its associated operators (3) yield a rich crop of ''quantum paradoxes.'' It appears that these paradoxical properties are inherent to all code words of quantum error correcting codes. In particular, this is obviously true of the nine-qubit code words of Shor [1], since the latter are built from triads of Mermin states [11].

It should be noted that the Mermin states,

$$(|000\rangle\pm|111\rangle)/\sqrt{2},\tag{4}$$

can be used as code words, for correcting a ''bit error'' $(0\leftrightarrow1)$ in any one of the three qubits (but no other type of error). These states are eigenvectors, with eigenvalue $+1$, of an eight-element Abelian group

$$\begin{gathered}\sigma_{uuu},\quad\mp\sigma_{xyy},\quad\mp\sigma_{yxy},\quad\mp\sigma_{yyx},\\\pm\sigma_{xxx},\quad\sigma_{zzu},\quad\sigma_{zuz},\quad\sigma_{uzz}.\end{gathered}\tag{5}$$

To obtain quantum paradoxes for the five-qubit code (1), we note first that for each qubit, each one of σ_x, σ_y, and σ_z is an ''element of reality,'' as defined by Einstein, Podolsky, and Rosen [12]. This is so because the observable value of any one of these operators can be ascertained by measuring only *other* qubits, ''without disturbing in any way'' [12] the element of reality under consideration. For example, if we have prepared the five qubits in the state $|0_L\rangle$, the result of a measurement of σ_{1x} can be predicted with certainty by

*Permanent address: Department of Physics, Technion–Israel Institute of Technology, 32 000 Haifa, Israel.

measuring σ_{2z} and σ_{3x}, because we know that $\sigma_{1x}\sigma_{2z}\sigma_{3x}|0_L\rangle = -|0_L\rangle$. That result will, henceforth, be denoted by $v(\sigma_{1x})$. Note that only the second and third qubits have to be measured in order to determine $v(\sigma_{1x})$ (it is not necessary to measure the fourth and fifth ones). Other ways of determining $v(\sigma_{1x})$ without interacting with the first qubit are to measure $\sigma_{4x}\sigma_{5z}$, or $\sigma_{3x}\sigma_{4y}\sigma_{5y}$, or $\sigma_{2x}\sigma_{3y}\sigma_{4z}\sigma_{5y}$, or $\sigma_{2x}\sigma_{3z}\sigma_{5z}$, or $\sigma_{2y}\sigma_{3y}\sigma_{4x}$, or $\sigma_{2y}\sigma_{3z}\sigma_{4y}\sigma_{5x}$, or $\sigma_{2z}\sigma_{4z}\sigma_{5x}$, as may be seen from the various operators in Eq. (3) and their cyclic permutations.

There are, therefore, eight different ways of determining $v(\sigma_{1x})$ by means of measurements performed on the *other* qubits. However, these measurements cannot all be simultaneously carried out, if each one of the qubits is tested separately, because they involve mutually incompatible, noncommuting one-particle operators (although the eight *products* of operators do commute, however, because their commutators always involve an even number of anticommutations). The notion of ''element of reality'' tacitly implies that these eight different determinations of $v(\sigma_{1x})$ agree with each other. This may be intuitively obvious. However, classical intuition is a notoriously bad guide in the quantum world. There is no way of experimentally verifying that the eight methods agree. (At most, it is possible to verify that for some subsets of these operators, for example, $\sigma_{2z}\sigma_{3x}$ and $\sigma_{4x}\sigma_{5z}$ can be tested simultaneously. There are only five such pairs among the eight operator products listed above.) The assumption that all eight ways of determining $v(\sigma_{1x})$ necessarily agree is manifestly counterfactual. It is an example of the metaphysical hypothesis known as *local realism*. This hypothesis is incompatible with quantum mechanics, and leads to numerous contradictions, as will now be shown.

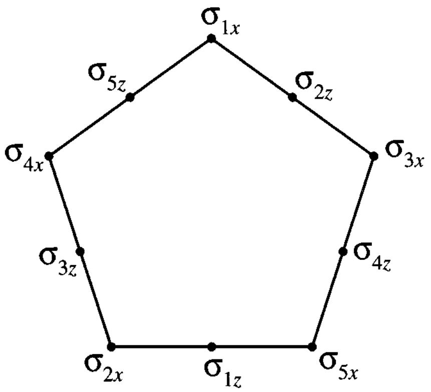

FIG. 1. Each side of the pentagon corresponds to three mutually compatible measurements. The product of the three results is guaranteed to have value ∓ 1, for $|0_L\rangle$ and $|1_L\rangle$, respectively. Moreover, the product of the five σ_z has to be ± 1. There is no consistent set of values for the 12 operators.

As one example, among many, consider the following six operators: $\pm\sigma_{1z}\sigma_{2z}\sigma_{3z}\sigma_{4z}\sigma_{5z}$, and $\mp\sigma_{1x}\sigma_{2z}\sigma_{3x}$ and cyclic permutations of the five qubits. If we measure the values of these six operators for one of the code words, the result is 1, with certainty. If the qubits are widely separated, the easiest way of measuring any one of these operators is to measure separately the physical qubits involved in it, and then to multiply the results. It is therefore tempting to assume that the values of the spin components of *individual* qubits also satisfy

$$v(\sigma_{1z})\, v(\sigma_{2z})\, v(\sigma_{3z})\, v(\sigma_{4z})\, v(\sigma_{5z}) = \pm 1 \tag{6}$$

and

$$v(\sigma_{1x})\, v(\sigma_{2z})\, v(\sigma_{3x}) = \mp 1, \tag{7}$$

and all cyclic permutations of Eq. (7). There are six equalities written above. The product of their right-hand sides is -1. But on the left-hand side each symbol appears twice, and therefore, the product of the left-hand sides is $+1$. We have reached a contradiction, of the same type as in Refs. [10] and [11]. It is graphically illustrated in Fig. 1.

It is also possible to obtain a Bell-Kochen-Specker [13,14] type of contradiction, which does not refer to any particular quantum state, such as Eq. (1). Consider the following array of operators:

$$\begin{array}{ccccccccccc}
\sigma_{1z} & \sigma_{2z} & \sigma_{3z} & \sigma_{4z} & \sigma_{5z} & 1 & 1 & 1 & 1 & 1 & \sigma_{1z}\sigma_{2z}\sigma_{3z}\sigma_{4z}\sigma_{5z} \\
\sigma_{1z} & 1 & 1 & 1 & 1 & 1 & \sigma_{2x} & 1 & 1 & \sigma_{5x} & \sigma_{5x}\sigma_{1z}\sigma_{2x} \\
1 & \sigma_{2z} & 1 & 1 & 1 & \sigma_{1x} & 1 & \sigma_{3x} & 1 & 1 & \sigma_{1x}\sigma_{2z}\sigma_{3x} \\
1 & 1 & \sigma_{3z} & 1 & 1 & 1 & \sigma_{2x} & 1 & \sigma_{4x} & 1 & \sigma_{2x}\sigma_{3z}\sigma_{4x} \\
1 & 1 & 1 & \sigma_{4z} & 1 & 1 & 1 & \sigma_{3x} & 1 & \sigma_{5x} & \sigma_{3x}\sigma_{4z}\sigma_{5x} \\
1 & 1 & 1 & 1 & \sigma_{5z} & \sigma_{1x} & 1 & 1 & \sigma_{4x} & 1 & \sigma_{4x}\sigma_{5z}\sigma_{1x}
\end{array} \tag{8}$$

All the operators in that array have eigenvalues ± 1, and, therefore, each one will yield one of these values, if measured in the standard way. Moreover, all the operators on each row commute, and their product is 1. Therefore, if all the operators on one of the rows are actually measured, the product of the resulting values is 1. Likewise, all the operators in each column commute, and their product is 1, *except those of the last column*, whose product is -1. It is therefore clearly impossible to associate to each operator a definite value ± 1, that is unknown but would be revealed by a measurement of that operator, if such a measurement were actually performed. This is the multiplicative form of the Kochen-Specker contradiction [15,16].

The original, additive form of the Kochen-Specker theorem can also be obtained from the above array. In its original formulation, that theorem asserted that there exist finite sets of projection operators, such that it is impossible to attribute to each one of the operators a bit value, ‘‘true’’ or ‘‘false,’’ subject to the two following constraints:

(i) (KS1) two orthogonal projection operators cannot both be true.

(ii) (KS2) if a subset of orthogonal projection operators is complete (i.e., it has a sum equal to the unit operator), one of these projection operators is true.

In the physical interpretation of the Kochen-Specker theorem, orthogonal projectors correspond to mutually compatible quantum measurements, whose results are arbitrarily labeled 1 and 0, or ‘‘yes’’ and ‘‘no.’’ The theorem asserts that there exist sets of n yes-no questions, such that none of the 2^n possible answers is compatible with the sum rules of quantum mechanics. This implies that there can be no subquantum physics, with hidden variables that would ascribe definite outcomes to the n yes-no tests (provided that the hidden variables are not ‘‘contextual,’’ namely, that the answer to each question is unique, and does not depend on the choice of other questions being asked).

A set of Kochen-Specker projectors can now be obtained from the above array of operators as follows.

(a) There is one complete set of eigenvectors that are common to all the operators in the first row: it is the ‘‘classical’’ basis $|00000\rangle, |00001\rangle, \ldots, |11111\rangle$. The 32 projectors on these vectors form a complete orthogonal set.

(b) There is one complete set of eigenvectors that are common to all the operators in the last column of the array. These are the codewords $|0_L\rangle$ and $|1_L\rangle$, and the 15 mutations of each one of them, obtained by letting one of the Pauli matrices act on one of the physical qubits. The 32 projectors on these orthonormal vectors form another complete set. Each one is moreover orthogonal to 16 vectors of the ‘‘classical’’ basis, and vice versa.

(c) Each one of the five other rows in array (8) generates eight mutually orthogonal four-dimensional subspaces, that form a complete set. For example, the subspaces that correspond to the third row are the tensor products of the eigenvectors of σ_{1x}, σ_{2z}, σ_{3x}, and the complete subspaces of the two other qubits. The products of the three eigenvectors are

$$\tfrac{1}{2}(|0\rangle\pm|1\rangle)\otimes(|0\rangle \quad\text{or}\quad |1\rangle)\otimes(|0\rangle\pm|1\rangle), \tag{9}$$

or

$$\begin{aligned}&\tfrac{1}{2}(|000\rangle+n\ |001\rangle+m\ |100\rangle+mn\ |101\rangle) \quad\text{for}\quad \langle\sigma_{2z}\rangle=1,\\ &\tfrac{1}{2}(|010\rangle+n\ |011\rangle+m\ |110\rangle+mn\ |111\rangle) \quad\text{for}\quad \langle\sigma_{2z}\rangle=-1,\end{aligned} \tag{10}$$

where $m=\langle\sigma_{1x}\rangle$ and $n=\langle\sigma_{3x}\rangle$. The eight corresponding projection operators thus are

$$\begin{aligned}&\tfrac{1}{4}\,(|000\rangle+n|001\rangle+m|100\rangle+mn|101\rangle)\\ &\quad\times(\langle000|+n\langle001|+m\langle100|+mn\langle101|)\otimes1\otimes1,\end{aligned} \tag{11}$$

and

$$\begin{aligned}&\tfrac{1}{4}\,(|010\rangle+n|011\rangle+m|110\rangle+mn|111\rangle)\\ &\quad\times(\langle010|+n\langle011|+m\langle110|+mn\langle111|)\otimes1\otimes1,\end{aligned} \tag{12}$$

respectively. There are, therefore, 40 projectors of rank 4. They satisfy many mutual orthogonality relations, for example, any projector with $\langle\sigma_{1x}\rangle=1$ in the third row of array (8) is orthogonal to any projector with $\langle\sigma_{1x}\rangle=-1$ in the sixth row.

Moreover, any rank 4 projector is orthogonal to many of the 64 projectors of rank 1, listed above. For example, all the projectors in Eq. (12), for any m and n, are orthogonal to all the ‘‘classical’’ vectors $|a0cde\rangle$. All the projectors in Eq. (12) with $m=n$ (so that $\langle\sigma_{1x}\sigma_{2z}\sigma_{3x}\rangle=-1$) are orthogonal to $|1_L\rangle$ and to all its mutations of type $\sigma_{4d}\sigma_{5e}|1_L\rangle$, and to some others. They are also orthogonal to the various mutations of $|0_L\rangle$, generated by σ_{1y}, σ_{1z}, σ_{2x}, σ_{2y}, σ_{3y}, σ_{3z}, or any odd number of the latter. (Not all these vectors are distinct, however.)

These numerous orthogonality relations have as a consequence that the constraints KS1 and KS2 cannot both be satisfied: there is no way of assigning to all these projection operators numerical values 1 (‘‘true’’) and 0 (‘‘false’’), that are compatible with all the orthogonality and completeness relations. The easiest way to see that is to note that if this were possible, all the operators in array (8) would acquire definite values, and we have already seen that this is impossible. The novel features in this Kochen-Specker contradiction is that projectors of rank 4 are used, and that the total number of projectors involved is remarkably low, when compared to the number of dimensions: 104/32=3.25, while a similar construction in four dimensions requires 24 vectors [17], and in eight dimensions, 40 vectors are involved [18].

We have likewise investigated the seven-qubit code words of Steane [3]. They are simultaneous eigenvectors of 128 matrices of order 128, which are direct products of three to seven Pauli matrices, and form an Abelian group. There are subsets of ten group elements with properties similar to those listed in Eqs. (6) and (7): each Pauli matrix corresponds to a local ‘‘element of reality,’’ because the result of its measurement can be predicted with certainty by examining only *other* qubits. However, if it is assumed, in accordance with local realism, that each one of the local Pauli matrices is associated with a definite numerical value, ±1, an algebraic contradiction appears.

We are grateful for the hospitality of the Program on Quantum Computers and Quantum Coherence at the Institute for Theoretical Physics, University of California at Santa Barbara, where this work was completed and was supported in part by the National Science Foundation under Grant No. PHY94-07194. D.P.D.V. acknowledges support from the Program on the Comparative Analysis of Quantum Computer Implementations of the U. S. Army Research Office.

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

[2] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

[3] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996); Proc. R. Soc. (London) A **452**, 2551 (1996).

[4] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[6] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997); Report No. quant-ph/9608006.

[8] V. Capasso, D. Fortunato, and F. Selleri, Int. J. Theor. Phys. **7**, 319 (1973).

[9] N. Gisin and A. Peres, Phys. Lett. A **162**, 15 (1992).

[10] D. M. Greenberger, M. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), p. 69.

[11] N. D. Mermin, Phys. Today **43** (6), 9 (1990); Am. J. Phys. **58**, 731 (1990).

[12] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[13] J. S. Bell, Rev. Mod. Phys. **38**, 447 (1966).

[14] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).

[15] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993), p. 189.

[16] N. D. Mermin, Rev. Mod. Phys. **65**, 803 (1993).

[17] A. Peres, J. Phys. A **24**, L175 (1991).

[18] M. Kernaghan and A. Peres, Phys. Lett. A **198**, 1 (1995).