Error Correcting Bell Inequalities

Thomas A. Walker, Fiona A. C. Polack, and Samuel L. Braunstein
Computer Science, University of York, York YO10 5DD, United Kingdom
(Received 14 March 2008; published 18 August 2008)

Quantum error-correcting codes can protect multipartite quantum states from errors on some limited number of their subsystems (usually qubits). We construct a family of Bell inequalities which inherit this property from the underlying code and exhibit the violation of local realism, without any quantum information processing (except for the creation of an entangled state). This family shows no reduction in the size of the violation of local realism for arbitrary errors on a limited number of qubits. Our minimal construction requires preparing an 11-qubit entangled state.

DOI: 10.1103/PhysRevLett.101.080501 PACS numbers: 03.67.Pp, 03.65.Ud

In 1964 Bell theoretically demonstrated that quantum mechanics is inconsistent with a fundamental classical concept about nature [1]: that particles carry locally within them all the information necessary for determining detection outcomes (so-called local realism [2]). Although most Bell inequality experiments have now verified this inconsistency, there remain loopholes due to experimental imperfections [3]. Here we construct a family of Bell inequalities which shows no reduction in the size of their locally realistic violation for arbitrary errors on a limited number of qubits. Further, they use only passive detection, mimicking conventional Bell inequalities.

Recently, interest in quantum information theory has produced a number of methods for dealing with decoherence and imperfect devices, of which detector loss is but one example. Without such methods universal quantum computation would be virtually impossible, since the complex states required would become damaged before useful computation could take place. One of the most powerful approaches is based on quantum error correction, where states are encoded into a larger space in such a way that errors on a limited number of particles can be eliminated. Error-correcting codes consist of entangled states. Thus, one might expect them to exhibit violations of local realism. Indeed, a number of states with error-correcting properties have been demonstrated to exhibit such violations [4–6]. However, the idea of using the error correction properties of the code words to recover violations of local realism when information is lost, or when errors occur, has never been explored. Here, we construct Bell inequalities with just this property.

The most direct method of constructing an error-correcting Bell inequality would appear to be to take a standard Bell inequality and encode each of the particles into its own individual quantum error-correcting code before it is transmitted. If these states were now measured in a fault tolerant manner, then the original Bell inequality should be resistant to errors. Since the smallest qubit code that protects against arbitrary one-qubit errors is a five-qubit code, it should be possible to perform such an experiment using 10 qubits on the simplest two-subsystem Bell inequality.

However, such an experiment requires active quantum information processing by receivers at the detection stations, in order to provide the error correction. This increases the complexity of the experiment, since state manipulation needs to take place at a number of different sites. Also any processing is likely to add a delay, opening up a potential locality loophole unless the receivers are separated by sufficient distances. More importantly, this approach would radically change the manner in which Bell inequalities were tested—requiring active quantum information processing at the receiving stations. A much less problematic approach would be to seek a Bell inequality which involves nothing beyond simple measurements for each particle by the receivers; this mimics all conventional Bell inequality tests to date.

A typical Bell inequality may be succinctly written as

$$\langle \mathcal{B} \rangle \leq \mathcal{B}_{\rm lr}, \tag{1}$$

where $\mathcal{B}$ is the (nonlocal) Bell operator [7] and $\mathcal{B}_{\rm lr}$ is the maximum value that the Bell operator can take under any locally realistic model. The locally realistic value is determined by decomposing $\mathcal{B}$ into a sum of tensor products of local operators (such as the Pauli operators X_i, Y_i, and Z_i and the identity $\mathbb{1}$ on each particle). Under local realism each local operator in this expression takes on one of the spectrum of measurable values for that operator. Thus, for a decomposition into local Pauli operators, these would be ± 1. By looking at all combinations of locally realistic values, we may determine the range of values that a locally realistic description of $\mathcal{B}$ can take. Here we shall be interested only in the upper bound to these values, which we call $\mathcal{B}_{\rm lr}$.

Now the advantage of focusing on this nonlocal Bell operator $\mathcal{B}$ is that its quantum expectation value is the same whether we compute it directly on the nonlocal operator as in Eq. (1), or on each term in its sum individually, as in an experimental implementation of the Bell inequality test [7]. Theoretically, then, the properties of this single operator summarize the size of the expected violation of local realism that can be attained.

The spectral properties of $\mathcal{B}$ can illuminate the behavior of the associated Bell inequality under errors. We aim to design a Bell operator such that, for some specific quantum state, the spectrum of eigenvalues will form a degenerate subspace with correctable errors merely mapping between states within this subspace. Under these circumstances, the size of the violation of the Bell inequality will not change for arbitrary errors on a limited number of particles q (corresponding to the set of correctable errors). Since there is still a chance of seeing an error on more than q particles simultaneously, for a simple error model where the error rate ϵ is independent for each particle, the size of the violation will decrease as $O(\epsilon^{q+1})$, from the noiseless, loss-free case.

A starting point for our work on error-correcting Bell inequalities is the construction of a Mermin–Greenberger-Horne-Zeilinger–like (Mermin-GHZ-like) argument [4,5] by DiVincenzo and Peres [6] showing the inconsistency between quantum mechanics and local realism in the ideal noise-free case. DiVincenzo and Peres considered a specific five-qubit quantum error-correcting code code word $|0_L\rangle$ stabilized by elements of the Pauli group [8]: four basis elements $\hat{S}_1$, $\hat{S}_2$, $\hat{S}_3$, and $\hat{S}_4$ defining the code subspace and in addition $\hat{S}_5 = \hat{Z} = ZZZZZ$ specifically stabilizing the logical zero state $|0_L\rangle$ within the encoded subspace. These five operators then form a basis for all the elements of the Pauli subgroup $\mathbb{S}$ that completely stabilizes $|0_L\rangle$. The DiVincenzo and Peres argument boils down to the fact that if any basis for the elements that stabilize $|0_L\rangle$ takes on the locally realistic value $+1$ then at least one other element in the stabilizing group $\mathbb{S}$ must take on a locally realistic value of -1—contradicting the quantum mechanical stabilizing property where all 32 elements $\hat{S}_i$ of the stabilizer group $\mathbb{S}$ should actually have the value $+1$.

Let us now consider a very simple Bell inequality based on the DiVincenzo-Peres argument which may be described by the Bell operator

$$\mathcal{B}_{\text{simple}} = \sum_{\hat{S}_i \in \mathbb{S}} \hat{S}_i, \tag{2}$$

where we sum over all $|\mathbb{S}| = 32$ elements of the stabilizer group $\mathbb{S}$ for $|0_L\rangle$. By the DiVincenzo and Peres argument, under local realism $\mathcal{B}_{\text{simple}}$ will take a value less than 32, since at least one term will take on the locally realistic value of -1 (for any locally realistic assignment of x_i, y_i, $z_i = \pm 1$ for the Pauli operators X_i, Y_i, and Z_i). By exhaustively checking all 8^5 possible local-realistic configurations one can show that for the specific five-qubit code studied [6] $\mathcal{B}_{\text{simple,lr}} = 20$. By contrast, $\langle 0_L|\mathcal{B}_{\text{simple}}|0_L\rangle = 32$ (trivially corresponding to the maximum eigenvalue of $\mathcal{B}_{\text{simple}}$). So ideally the "size" for the violation in the absence of errors is $\langle \mathcal{B}_{\text{simple}}\rangle - \mathcal{B}_{\text{simple,lr}} = 12 > 0$. How does this violation respond to single-qubit errors? This can be seen by writing the Bell operator as the products of projectors on to the basis stabilizers as

$$\mathcal{B}_{\text{simple}} = \sum_{\hat{S}_i \in \mathbb{S}} \hat{S}_i = \prod_{\hat{S}_i \in \text{basis}} (\mathbb{1} + \hat{S}_i), \tag{3}$$

for any basis for $\mathbb{S}$, e.g., $\{\hat{S}_1, \hat{S}_2, \hat{S}_3, \hat{S}_4, \hat{S}_5\}$. If the error that has occurred (say X_1) commutes with a stabilizer (e.g., $\hat{S}_1$) then the effect is to just multiply the state by a factor of 2 since $(\mathbb{1} + \hat{S}_1)X_1|0_L\rangle = X_1(|0_L\rangle + \hat{S}_1|0_L\rangle) = 2X_1|0_L\rangle$. On the other hand if the error anticommutes with the stabilizer (e.g., $\hat{S}_4$) then $(\mathbb{1} + \hat{S}_4)X_1|0_L\rangle = X_1|0_L\rangle - X_1\hat{S}_4|0_L\rangle \equiv 0$. Since the $\{\hat{S}_1, \hat{S}_2, \hat{S}_3, \hat{S}_4, \hat{S}_5\}$ form a basis for all stabilizers of this codeword any single-qubit Pauli operator will anticommute with at least one of these basis elements and the measurement of $\mathcal{B}_{\text{simple}}$ will yield zero. Thus, the inequality formed from this Bell operator (2) is very sensitive to Pauli errors. Indeed, this behavior is exactly the opposite of what we desire.

To construct an error-correcting Bell inequality we must start by constructing a suitable Bell operator that will be insensitive to errors. Let $\mathbb{S}$ denote the Pauli subgroup (of dimension 2^n) that completely stabilizes some n-qubit codeword denoted $|0_L\rangle$ from an $[[n, k, d]]$ quantum error-correcting code. The code has a quantum Hamming distance d, so it can correct arbitrary errors on up to $\lfloor\frac{d-1}{2}\rfloor$ qubits; similarly, it can detect errors on up to $d - 1$ qubits. We construct the Bell operator

$$\mathcal{B} = \sum_{E_k \in \mathbb{E}^*} E_k \mathcal{B}_{\text{simple}} E_k^{\dagger}, \tag{4}$$

where $\mathcal{B}_{\text{simple}}$ is the simple Bell operator (3) for the new Pauli subgroup $\mathbb{S}$, $\mathbb{E}$ is the set of Pauli errors [8] on up to $q \leq \lfloor\frac{d-1}{2}\rfloor$ qubits, and $\mathbb{E}^*$ is a nondegenerate reduction of $\mathbb{E}$, where degenerate errors are treated as duplicates of each other and all but one of the duplicates is removed.

Now if an error $E_j \in \mathbb{E}$ occurs the state becomes transformed to $E_j|0_L\rangle$ and the Bell operator of Eq. (4) has expectation value (for this state $E_j|0_L\rangle$)

$$\langle \mathcal{B}\rangle = \sum_{E_k \in \mathbb{E}^*} \langle 0_L|E_j^{\dagger} E_k \mathcal{B}_{\text{simple}} E_k^{\dagger} E_j|0_L\rangle = \langle 0_L|\mathcal{B}_{\text{simple}}|0_L\rangle. \tag{5}$$

The last step here relies on the fact that the error-correcting code described by $\mathbb{S}$ can *detect* up to $d - 1 \geq 2q$ errors so at least one of the basis stabilizers must flip in $\mathcal{B}_{\text{simple}} = \prod_{\hat{S}_i \in \text{basis}}(1 + \hat{S}_i)$ yielding exactly zero except for terms in the sum where $E_k = E_j$ (modulo degeneracy). If an error were a superposition of Pauli errors then it is easy to see that the cross terms vanish, so the above result still holds.

Next, we must determine the locally realistic bound $\mathcal{B}_{\text{lr}}$ for the expression for $\mathcal{B}$ when it is expanded out as a sum of elements from the Pauli group. A mechanical procedure for obtaining this bound is to replace each Pauli operator X_i, Y_i, and Z_i in the expanded expression with the locally-realistic c numbers x_i, y_i, and z_i, respectively. By searching through all 8^n configurations $x_i, y_i, z_i = \pm 1$ we may find the maximal value $\mathcal{B}_{\rm lr}$. Since this procedure involves searching through every possible locally realistic configuration, any error that simply maps one configuration into another will not change the value of $\mathcal{B}_{\rm lr}$. In general, it will be too difficult to determine $\mathcal{B}_{\rm lr}$ exactly, but it is often good enough to obtain an upper bound to it. For the Bell operator of Eq. (4), therefore, in the worst case

$$\mathcal{B}_{\rm lr} \leq \sum_{E_k \in \mathbb{E}^*} \mathcal{B}_{\rm simple,lr} = |\mathbb{E}^*|\mathcal{B}_{\rm simple,lr} \leq |\mathbb{E}|\mathcal{B}_{\rm simple,lr} = \sum_{e=0}^{q} 3^e \binom{n}{e} \mathcal{B}_{\rm simple,lr}, \tag{6}$$

where we use the fact that the set of correctable errors $\mathbb{E}$ consists of Pauli errors on up to q qubits at a time.

Finally, it is often found that as the number of qubits increases the size of any locally realistic violation in typical multiparticle Bell inequalities increases exponentially. We might then expect the Bell inequality of Eq. (4) to yield a violation of local realism, which does not deteriorate under correctable errors for a sufficiently large quantum error-correcting code (i.e., for sufficiently many qubits). Indeed, we show below that precisely this happens for the many qubit generalization of the Shor code.

Shor's 9-qubit code [9] can be viewed as a specific instance of a more general code with code words

$$|0_L\rangle = \frac{1}{\sqrt{2}^m}(|00\ldots 0\rangle + |11\ldots 1\rangle)^{\otimes m}, \quad |1_L\rangle = \frac{1}{\sqrt{2}^m}(|00\ldots 0\rangle - |11\ldots 1\rangle)^{\otimes m}, \tag{7}$$

where there are m blocks each consisting of m qubits—this describes an $[[n = m^2, k = 1, d = m]]$ quantum error-correcting code. The $|0_L\rangle$ code word consists of m copies, or blocks, of the m-qubit GHZ-like state $\frac{1}{\sqrt{2}}(|00\ldots 0\rangle + |11\ldots 1\rangle)$. This m-qubit block is stabilized by a basis consisting of all pairs of Z operators on adjacent qubits and one of X operators on all qubits

$$\begin{array}{cccccc} Z & Z & \mathbb{1} & \mathbb{1} & \ldots & \mathbb{1} \\ \mathbb{1} & Z & Z & \mathbb{1} & \ldots & \mathbb{1} \\ & & & \vdots & & \\ \mathbb{1} & \mathbb{1} & \ldots & \mathbb{1} & Z & Z \\ X & X & \ldots & & X & X, \end{array} \tag{8}$$

corresponding to a total of m basis operators.

The sum over all stabilizers on each block of m qubits may then be written as

$$\mathcal{B}^{\rm block}_{\rm simple} = \prod_{j=1}^{m-1}(\mathbb{1} + Z_j Z_{j+1}) + {\rm Re}\Big[\prod_{j=1}^{m}(X_j + iY_j)\Big], \tag{9}$$

where the second term may be recognized as just the Mermin Bell operator for a GHZ-like state without its complex phase factor [5].

Under local realism, each of the X_i, Y_i, Z_i corresponds to an element of reality with definite value $x_i, y_i, z_i = \pm 1$. Thus, the locally realistic value for this sum will be

$$\prod_{j=1}^{m-1}(1 + z_j z_{j+1}) + {\rm Re}\Big[\prod_{j=1}^{m}(x_j + iy_j)\Big], \tag{10}$$

for some particular combination of values $x_i, y_i, z_i = \pm 1$. The first product in (10) has value 0 or 2^{m-1} since if all of the z_j take the same value then each term in the product will be 2; however, if some of the z_j take different values then at least one of the terms $1 + z_j z_{j+1}$ will be zero. The second product is bounded by

$$\Big|{\rm Re}\Big[\prod_{j=1}^{m}(x_j + iy_j)\Big]\Big| \leq \begin{cases} 2^{m/2}, & m \text{ even} \\ 2^{(m-1)/2}, & m \text{ odd,} \end{cases} \tag{11}$$

since for each term $|x_j + iy_j| = \sqrt{2}$. Thus the sum of stabilizers for an individual block $\mathcal{B}^{\rm block}_{\rm simple,lr}$ is bounded by

$$\mathcal{B}^{\rm block}_{\rm simple,lr} \leq \begin{cases} 2^{m-1} + 2^{m/2}, & m \text{ even} \\ 2^{m-1} + 2^{(m-1)/2}, & m \text{ odd.} \end{cases} \tag{12}$$

Further, since the individual blocks are separate, the sum over all m^2 stabilizers of the full m^2-qubit state $|0_L\rangle$ can be written

$$\mathcal{B}_{\rm simple} = \prod_{k=1}^{m}\Big\{\prod_{j=m(k-1)+1}^{mk-1}(\mathbb{1} + Z_j Z_{j+1}) + {\rm Re}\Big[\prod_{j=m(k-1)+1}^{mk}(X_j + iY_j)\Big]\Big\}. \tag{13}$$

That this operator takes this product form can most readily be seen by recalling that each $\mathcal{B}^{\rm block}_{\rm simple}$ may be written as a product of projectors over the relevant stabilizer basis. Under local realism, this simple Bell operator may be bounded using Eq. (12) by

$$\mathcal{B}_{\rm simple,lr} \leq 2^{m^2-m}(1 + \sqrt{2}^{-(m-1)})^m, \tag{14}$$

where without loss of generality we focus on the case of odd m. By comparison the expectation of $\mathcal{B}_{\rm simple}$ for $|0_L\rangle$ is 2^{m^2}; thus their ratio is

$$\frac{\langle \mathcal{B}_{\rm simple}\rangle}{\mathcal{B}_{\rm simple,lr}} \geq \frac{2^m}{[1 + \sqrt{2}^{-(m-1)}]^m}. \tag{15}$$

For all (odd) $m \geq 2$ the quantity $1 + \sqrt{2}^{-(m-1)}$ will be less than 2; thus, the size of the violation grows exponentially in m which is the square root of the number of qubits used in the code. For any fixed number of qubits q subject to errors this quantum expectation will grow faster than $|\mathbb{E}|\mathcal{B}_{\rm simple,lr}$. Thus, from Eqs. (5) and (6), for sufficiently large m the

Bell operator

$$\mathcal{B} = \sum_{E_k \in \mathbb{E}^*} E_k \mathcal{B}_{\text{simple}} E_k^\dagger, \quad (16)$$

where $\mathcal{B}_{\text{simple}}$ is given explicitly by Eq. (13), yields a violation of local realism whose size is not degraded by arbitrary errors on up to q qubits. For an error model consisting of some probability ϵ of independent errors or loss on each particle, our result shows that a Bell inequality may be constructed such that the size of the violation of local realism diminishes from the ideal noiseless and loss-free value by $O(\epsilon^{q+1})$ for any q we wish to choose. For the generalized Shor codes, Eqs. (6), (15), and (16), then give $\langle \mathcal{B} \rangle / \mathcal{B}_{\text{lr}} \geq 2^{(m-1)}/[q 3^q \binom{m^2}{q}] + O(\epsilon^{q+1})$.

The above demonstration of the efficacy of our approach relied on the asymptotic behavior of the quantum expectation of an error-correcting Bell operator $\langle \mathcal{B} \rangle = 2^n$ (for an n-qubit code) and a loose bound on the locally realistic maximum $\mathcal{B}_{\text{lr}}$. For single-qubit errors the results show that a violation of local realism can be attained using the generalized Shor code construction for a block size of $m = 7$ corresponding to $n = 49$ qubits. We now investigate a broader set of quantum error correction codes in order to seek a more compact (smaller total number of qubits) error-correcting Bell inequality.

Candidate error-correcting Bell inequalities may be constructed from any stabilizer $[[n, k, d]]$ quantum error-correcting code. Therefore, we performed a systematic search for the codes listed in Grassl's public database of quantum error-correcting codes [10]. In each case, we took the set of allowable errors $\mathbb{E}$ to correspond to single-qubit errors. Using a brute-force search through all locally realistic configurations, the smallest local-realism-violating error-correcting Bell inequality we found involved 11 qubits and was already at the extreme end of easily accessible computational power (requiring roughly 6 months equivalent time on a desktop computer; each added qubit increases the CPU time by a factor of 8 or more). The stabilizers for this $[[11, 0, 5]]$ code are [10]

$$\begin{matrix}
X & I & I & I & I & Z & Z & Y & I & Z & Z \\
I & X & I & I & I & Z & Z & X & Y & I & Y \\
I & I & X & I & I & Z & Z & Z & Z & X & I \\
I & I & I & X & I & Z & Z & Z & I & I & X \\
I & I & I & I & X & Z & I & Z & X & Y & I \\
I & I & Z & I & I & X & Z & Z & Y & Y & Y \\
I & I & I & I & I & I & X & Z & Z & Z & Z \\
I & I & Z & Z & I & I & Z & X & X & Z & X \\
Z & I & I & Z & I & I & I & I & X & Y & Z \\
Z & I & I & I & Z & I & I & Z & I & X & X \\
I & Z & I & I & Z & I & Z & Z & Z & I & X,
\end{matrix} \quad (17)$$

and a brute-force search showed that $\mathcal{B}_{\text{lr}} = 1760$ whereas the quantum expectation is simply $\langle \mathcal{B} \rangle = 2^{11} = 2048$, demonstrating a clear violation of the associated Bell inequality, yet with single-error correcting properties.

Now Bell inequalities provide an alternative strategy for formulating quantum key distribution [11]—they have several practical advantages despite the added overhead of entanglement. Our work potentially extends this by allowing error-correcting capabilities to be built into the entanglement. This is particularly interesting in a cryptographic scenario where individual parties would have access only to passive detection and would be unable to further share quantum information among different parties to perform active quantum error correction. In a multiparty cryptographic network setting conventional quantum error correction could not obviously be used, but our passive scheme would be available.

Error-correcting Bell inequalities can provide a robust violation of local realism; the size of the violation decays only as a second-order or higher effect from errors or data loss, such as would arise from finite-efficiency detectors. Our scheme uses only passive detection; no quantum processing is needed at the detection stations. Our minimal construction requires preparing an 11-qubit entangled state, whereas using conventional error correction would require at least 10 qubits and active decoding at the detection stations. We do not rule out the possibility of an alternate construction, say based on qudits, yielding more efficient passive error-correcting Bell inequalities.

[1] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).

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

[3] L. E. Ballentine, Am. J. Phys. **55**, 785 (1987); A. Peres, Found. Phys. **29**, 589 (1999); L. Vaidman, Phys. Lett. A **286**, 241 (2001).

[4] 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), pp. 69–72.

[5] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

[6] D. P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997).

[7] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

[8] Consisting of simple tensor products of the identity, the Pauli operators, and the prefactors ± 1 and $\pm i$.

[9] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[10] M. Grassl, http://iaks-www.ira.uka.de/home/grassl/QECC/

[11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).