Entanglement of a Pair of Quantum Bits

Scott Hill and William K. Wootters
Department of Physics, Williams College, Williamstown, Massachusetts 01267
(Received 3 March 1997)

The "entanglement of formation" of a mixed state ρ of a bipartite quantum system can be defined as the minimum number of singlets needed to create an ensemble of pure states that represents ρ. We find an exact formula for the entanglement of formation for all mixed states of two qubits having no more than two nonzero eigenvalues, and we report evidence suggesting that the formula is valid for all states of this system. [S0031-9007(97)03443-1]

PACS numbers: 89.70.+c, 03.65.Bz

Entanglement is the potential of quantum states to exhibit correlations that cannot be accounted for classically. For decades, entanglement has been the focus of much work in the foundations of quantum mechanics, being associated particularly with quantum nonseparability and the violation of Bell's inequalities [1]. In recent years, however, it has begun to be viewed also as a potentially useful resource. The predicted capabilities of a quantum computer, for example, rely crucially on entanglement [2], and a proposed quantum cryptographic scheme converts shared entanglement into a shared secret key [3]. For both theoretical and potentially practical reasons, it has become interesting to quantify entanglement, just as we quantify other resources such as energy and information. In this Letter we adopt a recently proposed quantitative definition of entanglement and derive an explicit formula for the entanglement of a large class of states of a pair of binary quantum systems (qubits).

The simplest kind of entangled system is a pair of qubits in a *pure* but nonfactorizable state. A pair of spin-$\frac{1}{2}$ particles in the singlet state $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ is perhaps the most familiar example, but one can also consider more general states such as $\alpha|\uparrow\downarrow\rangle + \beta|\downarrow\uparrow\rangle$, which may be less entangled. For any bipartite system in a pure state, Bennett *et al.* [4] have shown that it is reasonable to define the entanglement of the system as the von Neumann entropy of either of its two parts. That is, if $|\psi\rangle$ is the state of the whole system, the entanglement can be defined as $E(\psi) = -\mathrm{Tr}\,\rho\log_2\rho$, where ρ is the partial trace of $|\psi\rangle\langle\psi|$ over either of the two subsystems. (It does not matter which subsystem one traces over; the result is the same either way.) What Bennett *et al.* showed specifically is the following. Consider n pairs, each in the state $|\psi\rangle$. Let an observer Alice hold one member of each pair and let Bob, whom we imagine to be spatially separated from Alice, hold the other. Then if $|\psi\rangle$ has E "ebits" of entanglement according to the above definition, the n pairs can be reversibly converted by purely local operations and classical communication into m pairs of qubits in the singlet state, where m/n approaches E for large n and the fidelity of the conversion approaches 100%. This interconvertibility is strong justification for the above definition of E and characterizes it uniquely.

It is somewhat harder to define the entanglement of mixed states [5], though again one can use the singlet as the basic unit of entanglement and relate the given mixed state to singlets. The new feature in the case of mixed states is that the number of singlets required to *create* the state is not necessarily the same as the number of singlets one can *extract* from the state [6]. In this paper we focus on the former quantity, which leads to the following definition of "entanglement of formation" [7]. Given a mixed state ρ of two quantum systems A and B, consider all possible ways of expressing ρ as an ensemble of pure states. That is, we consider states $|\psi_i\rangle$ and associated probabilities p_i such that

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|\,. \tag{1}$$

The entanglement of formation of ρ, $E(\rho)$, is defined as the minimum, over all such ensembles, of the average entanglement of the pure states making up the ensemble

$$E = \min\sum_i p_i E(\psi_i)\,. \tag{2}$$

Entanglement of formation has the satisfying property that it is zero if and only if the state in question can be expressed as a mixture of product states. For ease of expression, we will refer to the entanglement of formation simply as "entanglement."

Peres [8] and Horodecki *et al.* [9] have found elegant characterizations of states with zero and nonzero E, and Bennett *et al.* [7] have determined the value of E for mixtures of Bell states. (These are a particular set of orthogonal, completely entangled states of two qubits; we will refer to other sets of such states as "generalized Bell states.") But the value of E for most states, even of two qubits, is not known, and in fact it has not been evident that one can even express E in closed form as a function of the density matrix. The exact formula we derive in this Letter is proved for all density matrices of two qubits having only two nonzero eigenvalues, but it appears likely that it applies to *all* states of this system.

 0031-9007/97/78(26)/5022(4)$10.00

Our starting point is a curious and useful fact about the pure states of a pair of qubits. For such a system, we define a "magic basis" consisting of the following four states (they are the Bell states with particular phases) [7]:

$$\begin{aligned} |e_1\rangle &= \tfrac{1}{2}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle), \\ |e_2\rangle &= \tfrac{1}{2}i(|\uparrow\uparrow\rangle - |\downarrow\downarrow\rangle), \\ |e_3\rangle &= \tfrac{1}{2}i(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle), \\ |e_4\rangle &= \tfrac{1}{2}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle), \end{aligned} \tag{3}$$

where we have used spin-$\frac{1}{2}$ notation for definiteness. When a pure state $|\psi\rangle$ is written in this particular basis, as $|\psi\rangle = \sum_i \alpha_i |e_i\rangle$, its entanglement can be expressed in a remarkably simple way [7] in terms of the components α_i: Define the function

$$\mathcal{E}(x) = H(\tfrac{1}{2} + \tfrac{1}{2}\sqrt{1 - x^2}) \quad \text{for } 0 \le x \le 1, \tag{4}$$

where H is the binary entropy function $H(x) = -[x \log_2 x + (1 - x)\log_2(1 - x)]$. Then the entanglement of $|\psi\rangle$ is

$$E(\psi) = \mathcal{E}(C(\psi)), \tag{5}$$

where C is defined by

$$C(\psi) = \Big| \sum_i \alpha_i^2 \Big| . \tag{6}$$

The quantity C, like E for this system, ranges from zero to one, and it is monotonically related to E, so that C is a kind of measure of entanglement in its own right. It is sufficiently useful that we give it its own name: *concurrence*. As we look for a pure-state ensemble with minimum *average* entanglement for a given mixed state, our plan will be to look for a set of states that all have the *same* entanglement, which is to say that they all have the same concurrence.

Two other facts about the magic basis are worth highlighting. (i) The set of states whose density matrices are *real* when expressed in the magic basis is the same as the set of mixtures of generalized Bell states (Horodecki *et al.* have called such mixtures "T states" [10]). (ii) The set of unitary transformations that are real when expressed in the magic basis (or real except for an overall phase factor) is the same as the set of transformations that act independently on the two qubits.

It happens that our formula for E is conveniently expressed in terms of a matrix R, which is a function of ρ defined by the equation

$$R(\rho) = \sqrt{\sqrt{\rho}\,\rho^*\sqrt{\rho}}\,. \tag{7}$$

Here ρ^* is the complex conjugate of ρ when it is expressed in the magic basis; that is, $\rho^* = \sum_{ij} |e_i\rangle\langle e_j|\rho|e_i\rangle\langle e_j|$. To get some sense of the meaning of R, note that Tr R, ranging from 0 to 1, is a measure of the "degree of equality" [11] between ρ and ρ^*, which in turn measures how nearly ρ approximates a mixture of generalized Bell states. Note also that the eigenvalues of R are invariant under local unitary transformations of the separate qubits, a fact that makes these eigenvalues particularly eligible to be part of a formula for entanglement, since entanglement must also be invariant under such transformations. We now state our main result.

Theorem.—Let ρ be any density matrix of two qubits having no more than two nonzero eigenvalues. Let $\lambda_{\max}$ be the largest eigenvalue of $R(\rho)$. Then the entanglement of formation of ρ is given by

$$E(\rho) = \mathcal{E}(c); \qquad c = \max(0, 2\lambda_{\max} - \operatorname{Tr} R). \tag{8}$$

[The quantity c can thus be called the concurrence of the density matrix ρ. If ρ is pure, then c reduces to the concurrence defined in Eq. (6).]

Proof.—Let $|v_1\rangle$ and $|v_2\rangle$ be the two eigenvectors of ρ corresponding to its two nonzero eigenvalues. Define the 2×2 matrix τ such that $\tau_{ij} = v_i \cdot v_j$, where the dot product is taken in the magic basis with no complex conjugation: $v_i \cdot v_j \equiv \sum_k \langle e_k \mid v_i\rangle \langle e_k \mid v_j\rangle$. Consider an arbitrary pure state $|\psi\rangle$ that can be written in the form $|\psi\rangle = a|v_1\rangle + b|v_2\rangle$. If $|\psi\rangle$ is expressed as a four-vector in the magic basis, we can rewrite Eq. (6) as $C(\psi) = |\psi \cdot \psi|$, and

$$C^2(\psi) = (\psi \cdot \psi)(\psi \cdot \psi)^* = \operatorname{Tr}[s^*\tau s\tau^*], \tag{9}$$

where $s = \binom{a}{b}(a \;\; b)^*$ is the density matrix of $|\psi\rangle$ in the (v_1, v_2) basis.

Let us define the function

$$f(\omega) = \operatorname{Tr}[\omega^*\tau\omega\tau^*] \tag{10}$$

for any density matrix ω expressed in the (v_1, v_2) basis. From Eq. (9), $f(\omega) = C^2(\omega)$ if ω represents a pure state. Now, ω is a 2×2 density matrix, and as such can be written as a real linear combination of Pauli matrices: $\omega = \frac{1}{2}(I + \vec{r} \cdot \vec{\sigma})$ where $r_j = \operatorname{Tr}[\sigma_j \omega]$. Substituting this form into Eq. (10) gives us an expression

$$f(\omega) = \tfrac{1}{4}\operatorname{Tr}[\tau^*\tau] + \sum_j r_j L_j + \sum_{i,j} r_i r_j M_{ij}, \tag{11}$$

with

$$L_j = \tfrac{1}{2}\operatorname{Tr}[\sigma_j \tau^* \tau] \tag{12}$$

and

$$M_{ij} = \tfrac{1}{4}\operatorname{Tr}[\sigma_i^* \tau \sigma_j \tau^*]. \tag{13}$$

Thus f is defined on the surface and interior of a unit sphere in three dimensions, the domain of $\vec{r}$.

M is a real, symmetric matrix with eigenvalues $\pm\frac{1}{2}|\det\tau|$ and $\frac{1}{4}\operatorname{Tr}[\tau^*\tau]$, and L is the eigenvector of M corresponding to the eigenvalue $\frac{1}{4}\operatorname{Tr}[\tau^*\tau]$. Since M has two positive eigenvalues and one negative eigenvalue, $f(\omega)$ is convex along two directions and concave along a third. For the purpose of this proof, we would like to have a function that is equal to $f(s)$ for pure states s, but convex in all directions. With this in mind we define

$$g(\omega) = f(\omega) + \tfrac{1}{2}|\det\tau|(|\vec{r}|^2 - 1), \tag{14}$$

which is identical to f for pure states ($|\vec{r}| = 1$). The extra term added to $f(\omega)$ in effect adds a constant to f and a multiple of the identity matrix to M. If we define a matrix

$$N = M + \tfrac{1}{2}|\det\tau|I \tag{15}$$

and a constant

$$K = \tfrac{1}{4}\mathrm{Tr}[\tau^*\tau] - \tfrac{1}{2}|\det\tau|, \tag{16}$$

then we can write

$$g(\omega) = K + \sum_j r_j L_j + \sum_{i,j} r_i r_j N_{ij}. \tag{17}$$

The added term in Eq. (15) makes all the eigenvalues of N non-negative, one of them being zero. Thus g is a convex function. Since L is an eigenvector of N associated with a positive eigenvalue, and is orthogonal to the eigenvector with zero eigenvalue, the function g is constant along the latter direction. We can imagine the function g (suppressing one dimension) as a sheet of paper curved upward into a parabolic shape; it achieves its minimum value along a straight line. Moreover, one can show by direct calculation that the minimum value of g is zero. In Fig. 1, we indicate surfaces along which g is constant, for a generic choice of $|v_1\rangle$ and $|v_2\rangle$. The surfaces appear as cylinders with elliptical cross sections. The mixed state ρ that we are considering lies on one of these cylinders and can be decomposed into two pure states lying on the same cylinder; that is, having the same value of g. (These two states are connected to ρ by a straight line parallel to the cylinders' axis.) The next two paragraphs show that no other decomposition of ρ has a smaller average entanglement than this one.

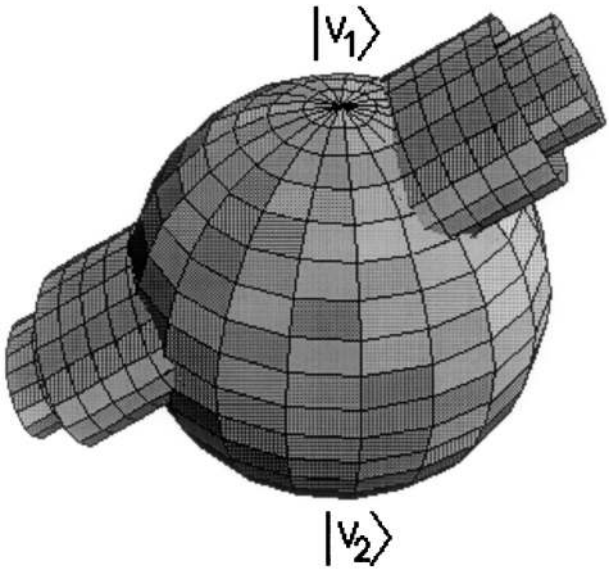

FIG. 1. The surface of the sphere represents the set of all pure superpositions of $|v_1\rangle$ and $|v_2\rangle$, the eigenvectors of ρ. The interior represents all mixed states formed from such superpositions. The elliptical cylinders are surfaces of constant g, and their intersections with the spherical surface are therefore curves of constant entanglement. ρ itself lies on the vertical axis, between $|v_1\rangle$ and $|v_2\rangle$ which are at the poles. Its minimum-entanglement decomposition consists of two pure states lying on the same cylinder as ρ.

Any decomposition of ρ into pure states can be viewed as a collection of weighted points on the surface of the sphere in Fig. 1 whose "center of mass" is the point representing ρ. The average entanglement of such an ensemble is the average of $\mathcal{E}(\sqrt{g(s)})$ over the ensemble, since $\mathcal{E}(\sqrt{g(s)})$ is equal to entanglement for pure states s. If we can show that $\mathcal{E}(\sqrt{g(\omega)})$, regarded as a function of ω, is convex over the interior of the sphere, then it will follow that this average cannot be less than $\mathcal{E}(\sqrt{g(\rho)})$. But we have just seen that ρ can be decomposed into two pure states s for which $g(s)$ is the same as $g(\rho)$, so this will prove that the entanglement of ρ is *equal* to $\mathcal{E}(\sqrt{g(\rho)})$.

In fact it is not hard to prove the desired convexity. The function $g(\omega)$ is parabolic with minimum value zero. Its square root is therefore a kind of cone and is also convex. The function $\mathcal{E}(x)$ is a convex and monotonically increasing function of x. It follows, then, from the transitive property of convex functions [12] that $\mathcal{E}(\sqrt{g(\omega)})$ is a convex function of ω.

We have thus found the entanglement of ρ and need only express it in a simpler form. Replacing ω with ρ in Eq. (10) and using the fact that ρ is diagonal in the (v_1, v_2) basis, we obtain

$$f(\rho) = \mathrm{Tr}(R^2) = \lambda_1^2 + \lambda_2^2, \tag{18}$$

where λ_1 and λ_2 are the nonzero eigenvalues of R [Eq. (7)]. Similarly, one finds that for the other term in Eq. (14),

$$\tfrac{1}{2}|\det\tau|(|\vec{r}|^2 - 1) = -2\lambda_1\lambda_2, \tag{19}$$

so that $g(\rho) = \lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2$. Taking the square root, we arrive at the result

$$E(\rho) = \mathcal{E}(c); \qquad c = |\lambda_1 - \lambda_2|. \tag{20}$$

The expression (20) is equivalent to Eq. (8) for the case of two nonzero eigenvalues. This completes the proof of the theorem.

Although we have proved our result only for density matrices with just two nonzero eigenvalues, we can report three pieces of evidence suggesting that the formula (8) may hold quite generally for a system of two qubits.

(1) For a mixture of Bell states, mixed with probabilities $p_1, \ldots, p_4$, Bennett *et al.* [7] have shown that the entanglement is equal to $\mathcal{E}(c)$, with c given by $\max(0, 2p_{\max} - 1)$. But in this case R is equal to ρ, so that our expression is equal to theirs. Thus our formula applies also to this class of density matrices, most of which are not covered by the above theorem.

(2) Peres [8] and Horodecki *et al.* [9] have provided a test, based on partial transposition, for determining whether a given state of two qubits has zero or nonzero E. We have applied both the Peres-Horodecki test and our own formula to several thousand randomly chosen density matrices and have found agreement between them in every case. That is, Eq. (8) gave $E > 0$ if and only if the Peres-Horodecki test indicated the presence of entanglement, which happened in roughly one-third of the cases.

(3) For each of 25 randomly chosen density matrices with nonzero entanglement, we have explored the space of all decompositions of the density matrix into pure states, limiting ourselves to ensembles of four states. (The example of Bell mixtures [7] suggests that four-state ensembles may be sufficient.) In each case, the result of numerically minimizing the average entanglement of the ensemble agrees with the result predicted by our formula.

If the formula turns out to be correct for all states, it will considerably simplify studies of entanglement. Questions such as whether the "distillable entanglement" is equal to the entanglement of formation [6,7], that is, whether one can extract as much entanglement as one puts into the state, will presumably be easier to answer if there is an explicit formula for the latter quantity. It is also conceivable that our result can be generalized to systems with larger state-spaces, such as an entangled pair of n-level atoms, though it is not clear whether there is any structure in such spaces that would play quite the same role that the magic basis plays in the two-qubit case. In imagining possible generalizations, it is interesting to note that the form of R has much in common with the "mixed-state fidelity" [11] of Bures, Uhlmann, and Jozsa, which is in no way special to two-qubit systems.

We would like to thank Charles Bennett, David DiVincenzo, and John Smolin for helpful and stimulating discussions.

[1] For a guide to some of the literature, see L. E. Ballentine, Am. J. Phys. **55**, 785 (1986).

[2] See, for example, D. P. DiVincenzo, Science **270**, 255 (1995).

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[4] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[5] Some alternatives to the definition we adopt, based on other criteria, are given in V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); A. Peres, Phys. Rev. A **54**, 2685 (1996); D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997); see Ref. [7].

[7] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996). The interpretation of Eq. (2) in terms of the number of singlets required is actually rather subtle. It depends, for example, on whether $E(\rho \otimes \rho)$ is always equal to $2E(\rho)$, a question whose answer is not yet known. In this Letter we take Eq. (2) as the definition of E and focus only on its evaluation.

[8] A. Peres, Phys. Rev. Lett. **76**, 1413 (1996).

[9] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[10] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996); R. Horodecki, M. Horodecki, and P. Horodecki, Phys. Lett. A **222**, 21 (1996).

[11] D. Bures, Trans. Am. Math. Soc. **135**, 199 (1969); A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976); R. Jozsa, J. Mod. Optics **41**, 2315 (1994).

[12] See, for example, A. W. Roberts and D. E. Varberg, *Convex Functions* (Academic Press, New York, 1973), p. 16.