J. Opt. B: Quantum Semiclass. Opt. **2** (2000) 225–229. Printed in the UK PII: S1464-4266(00)09599-9

Upper bound on the region of separable states near the maximally mixed state

P Deuar, W J Munro and K Nemoto

Centre for Laser Science, Department of Physics, University of Queensland, QLD 4072, Brisbane, Australia

E-mail: deuar@physics.uq.edu.au

Received 17 November 1999, in final form 31 January 2000

Abstract. A lower bound on the amount of noise that must be added to a GHZ-like entangled state to make it separable (also called the random robustness) is found using the transposition condition. The bound is applicable to arbitrary numbers of subsystems, and dimensions of Hilbert space, and is shown to be exact for qubits. The new bound is compared with previous such bounds on this quantity, and found to be stronger in all cases. It implies that increasing the number of subsystems, rather than increasing their Hilbert space dimension, is a more effective way of increasing entanglement. An explicit decomposition into an ensemble of separable states, when the state is not entangled, is given for the case of qubits.

Keywords: Quantum entanglement, separability, Peres criterion

1. Introduction

A key distinguishing feature of quantum physics from classical physics is the prediction of a new kind of correlation between physical quantities, called entanglement. Quantum entanglement has often been referred to as the inseparability of composite quantum systems. Such an entangled composite system is said to be inseparable because it cannot be prepared by manipulating each subsystem separately, using only measurements and operations local to one subsystem at a time. If a composite quantum mechanical state is specified by some density matrix, how can we tell if the system is entangled?

Much work has been done studying the particular case of two subsystems, with each in a two-dimensional Hilbert space (qubits). There is a good understanding of the entanglement for such systems and in fact a criterion, the partial transposition condition of Peres [1], indicates whether the subsystems are entangled. This, however, is a necessary and sufficient condition only when there are two subsystems, one with Hilbert space dimension two, and the other of dimension two or three, as was shown by Horodecki *et al* [2]. For more complex systems, it only determines whether the state contains distillable entanglement, however there are also some states with bound entanglement, which are lumped together with the separable states by this criterion.

Lewenstein *et al* [3] have used the Peres condition to consider two subsystems, but with each subsystem now in a $(N > 2)$-dimensional Hilbert space. Życzkowski *et al* [4] have, among other results, shown that all the mixed states in a sufficiently small neighbourhood of the maximally mixed state are separable. They also gave a bound on the size of this neighbourhood for small composite systems. Vidal and Tarrach [5] gave a lower bound on the size of this neighbourhood for arbitrary composite states, of any number of subsystems. Schack and Caves [6] gave bounds for composite systems composed of many qubits ($N = 2$).

It has been pointed out by Braunstein *et al* [7] that maximally entangled states of the GHZ type, with noise added, are connected to recent proposals for NMR quantum computing. They are also relevant to fundamental tests of quantum mechanics using Bell inequalities. The separability of such noisy generalized singlet states has been considered by various authors recently, mostly for the case of qubits (subsystems with Hilbert space dimension two). Schack and Caves [6], using the approach of Braunstein *et al* have obtained an exact boundary condition for the Werner states [8] (two qubits), while Caves and Milburn [9] extended the approach to two q-trits (Hilbert space dimension three). Horodecki *et al* [10] gave exact bounds for the case of two subsystems.

In this paper we extend the approach of Peres [1] to consider such noisy generalized singlet states in the general case of D subsystems with each subsystem in a N-dimensional Hilbert space. A parameter ϵ specifies the amount of the pure GHZ-type maximally entangled states present compared with the maximally mixed noise state. We then ask and answer the following question: what is the maximum value of ϵ for this state to be entangled? Another fundamental question is also considered. To create as entangled a state as possible, is it simply better to increase

the dimension of the subsystems or is it better to increase the number of subsystems?

2. Generalized Werner states

The states considered here consist of a mixture of the maximally mixed noise states, and the GHZ-type entangled states, where the number D of subsystems over which entanglement occurs, and the Hilbert space dimension N of each subsystem (equal for all D subsystems) can take on any values $N > 1$, $D > 1$. The relative proportion of GHZ-type states is controlled by the parameter ε, where $\varepsilon = 1$ corresponds to a pure GHZ-type state, while $\varepsilon = 0$ corresponds to the maximally mixed state. Explicitly, the state is given by the density operator

$$\hat{\rho} = (1-\varepsilon)\hat{\rho}_n + \varepsilon\hat{\rho}_e, \tag{1a}$$

$$\hat{\rho}_n = \frac{1}{N^D}\sum_{i_1,i_2,\ldots,i_D=1}^{N} |i_1 i_2 \ldots i_D\rangle\langle i_1 i_2 \ldots i_D|, \tag{1b}$$

$$\hat{\rho}_e = \frac{1}{N}\sum_{n,m=1}^{N} |nn\ldots n\rangle\langle mm\ldots m|, \tag{1c}$$

where

$$|i_1 i_2 \ldots i_D\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_D\rangle. \tag{2}$$

Here $|i_k\rangle$ represents one of N complete orthogonal basis states for the kth subsystem, while $\hat{\rho}_n$ is the density operator for the maximally mixed state, and $\hat{\rho}_e$ for the GHZ-like state.

The Werner state [8], consisting of a singlet state and some noise, is the simplest $D = N = 2$ case, hence we call these generalized Werner states. The state $\hat{\rho}$ can be viewed as a generalized singlet state $\hat{\rho}_e$ after it has emerged from a depolarizing channel.

3. Separability

The separability of particular cases of the state (1), and of more general states, has been considered previously by a number of authors [4–12]. Firstly, it was shown [11, 12] that for the two-qubit ($N = 2$, $D = 2$) case (the Werner state), $\hat{\rho}$ is separable for $\varepsilon \leqslant \frac{1}{3}$, and entangled otherwise, whereas for three qubits ($N = 2$, $D = 3$), Schack and Caves [6] found the state to be separable for $\varepsilon \leqslant \frac{1}{5}$. Soon after, Horodecki and Horodecki [10] found the exact result for arbitrary numbers of qubits:

$$\varepsilon_{\text{separable}} \leqslant \frac{1}{1+N}. \tag{3}$$

Schack and Caves also found bounds on the size of the separable neighbourhood around the maximally mixed state for totally general states of many qubits ($N = 2$). For $D = 4$ and $D = 5$ these are $\varepsilon \leqslant \frac{1}{33}$ and $\varepsilon \leqslant \frac{1}{243}$ respectively, and for higher D are given by

$$\varepsilon_{\text{separable}} \leqslant \begin{cases} 1/(1+2^D+2^{2D-2}) & \text{if} \quad D \text{ even} \\ 1/(1-2^D+2^{2D-2}) & \text{if} \quad D \text{ odd.} \end{cases} \tag{4}$$

What about the more general case when N and D are arbitrary? For what values of ε is the state given by (1) separable? Vidal and Tarrach [5] gave a maximum bound for the random robustness R of arbitrary multi-component states. For the states considered here, the critical value of ε at which the states change from being entangled to separable is $\varepsilon_c = 1/(1+R(\hat{\rho}_e||\hat{\rho}_n))$ (in the notation of [5]). So, according to that bound,

$$\varepsilon_{\text{entangled}} > \frac{1}{(1+N/2)^{D-1}}. \tag{5}$$

We will prove in section 4 that the states given by (1) are always entangled if

$$\varepsilon_{\text{entangled}} > \frac{1}{N^{D-1}+1}. \tag{6}$$

That this bound is strong for qubits ($N = 2$) is shown in the appendix, and an explicit decomposition into product states is given for the case of separable $\hat{\rho}$.

4. Outline of the proof of (6)

Peres [1] has shown that a necessary condition for a state consisting of two subsystems to be separable is that the partial transpose of the density matrix over one of the subsystems, and the partial transpose over the other subsystem, have positive eigenvalues. However, this is a necessary and sufficient condition only when one of the subsystems has Hilbert space dimension two or three, and the other dimension two, as was shown by Horodecki *et al* [2]. That paper went on to give a necessary and sufficient condition for a state to be separable. Nevertheless, the Peres condition is just what is needed for an upper bound on ε for separable states: i.e., any states which break the condition are entangled, although some which satisfy it may also be, but do not have to be, entangled. It is worth noting that any states which satisfy the Peres condition but are entangled are said to contain only 'bound' entanglement, as it cannot be used for teleportation, nor distilled by the process of entanglement distillation.

Firstly, note that the Peres condition is easily extended to more than two entangled subsystems. If there are D subsystems, one simply chooses some group of $M < D$ original subsystems to be called half-system number 1, and the remaining subsystems to be called half-system number 2. If for any such group of subsystems, an eigenvalue of the partial transpose of $\hat{\rho}$ over half-system number 1 (say) is negative, then $\hat{\rho}$ is entangled. Thus to use the Peres condition to full advantage, one must consider all such groups of subsystems.

The state (1) is convenient in this respect because it is unchanged under relabelling of the subsystems (evident by inspection). Thus the eigenvalues of ρ_α^T, the partial transpose of $\hat{\rho}$ over the set α of subsystems, need only be looked at for $D/2$ (rounded down) sets of subsystems to extract the maximum benefit from the Peres condition. In particular, a choice of sets of subsystems can be $\alpha_M = \{1, 2, \ldots, M\}$ where $M = 1, 2, \ldots, D/2$, and α_M contains the labels of the subsystems to be considered as members of the Mth half-system.

Firstly let us consider $M = 1$, i.e. the first subsystem's entanglement with the remaining $D-1$ of them. The partially transposed density matrix is

$$\rho_1^T = (1-\varepsilon)\rho_n^T + \varepsilon\rho_e^T, \tag{7a}$$

$$\rho_n^T = \frac{1}{N^D} \sum_{i_1,i_2,\ldots,i_D=1}^{N} |i_1 i_2 \ldots i_D\rangle\langle i_1 i_2 \ldots i_D|, \qquad (7b)$$

$$\rho_e^T = \frac{1}{N} \sum_{n,m=1}^{N} |mn \ldots n\rangle\langle nm \ldots m|. \qquad (7c)$$

Since all of the elements of $\hat{\rho}$ (hence ρ_1^T) are finite, the eigenvalues of ρ_1^T must also be finite. Now, exploiting the general continuity property of eigenvalues of $\hat{\rho}_1^T$, we conclude that at the value of $\varepsilon = \varepsilon_o$ above which the Peres condition indicates the state is entangled, one or more eigenvalues of ρ_1^T must be zero, since they are all positive for $\varepsilon < \varepsilon_o$, and at least one is negative for $\varepsilon > \varepsilon_o$, i.e. for some nonzero eigenvector

$$|\psi\rangle = \sum_{j_1,j_2,\ldots,j_D=1}^{N} \psi_{j_1 j_2 \ldots j_D} |j_1 j_2 \ldots j_D\rangle \neq 0 \qquad (8)$$

we must have $\rho_1^T(\varepsilon_o)|\psi\rangle = 0$. Expanded, this gives

$$\frac{1-\varepsilon_o}{N^D} \sum_{i_1,i_2,\ldots,i_D=1}^{N} \psi_{i_1 i_2 \ldots i_D} |i_1 i_2 \ldots i_D\rangle + \frac{\varepsilon_o}{N} \sum_{n,m=1}^{N} \psi_{nm\ldots m} |mn \ldots n\rangle = 0. \qquad (9)$$

Equation (9) can explicitly be written out as N^D equations

$$(1-\varepsilon_o)\psi_{i_1 i_2 \ldots i_D} + \varepsilon_o N^{D-1} \delta_{i_2 i_3} \delta_{i_2 i_4} \ldots \delta_{i_2 i_D} \psi_{i_2 i_1 \ldots i_1} = 0, \qquad (10)$$

where $\delta_{ab} = 1$ if $a = b$, 0 otherwise. Now if one or more of the $i_a : a = 3, \ldots, D$ does not equal i_2, then that equation is satisfied only if $\varepsilon = 1$ or $\psi_{i_1 i_2 \ldots i_D} = 0$. The first case is not of interest here, as $\varepsilon = 1$ corresponds to our maximally entangled GHZ-like states, so we choose $\psi_{i_1, i_2 \ldots i_D} = 0$.

The rest of the equations where $i_2 = i_3 = \cdots = i_D$, separate into $N(N-1)/2$ coupled sets of two equations of the identical form

$$(1-\varepsilon_o)\psi_{ab\ldots b} + \varepsilon_o N^{D-1} \psi_{ba\ldots a} = 0, \qquad (11)$$

$$(1-\varepsilon_o)\psi_{ba\ldots a} + \varepsilon_o N^{D-1} \psi_{ab\ldots b} = 0. \qquad (12)$$

These have solutions if $\psi_{ab\ldots b} = \psi_{ba\ldots a} = 0$, but this would imply $|\phi\rangle = 0$, which was specifically excluded in (8). Otherwise, these coupled two equations are only satisfied if

$$\varepsilon_o = \frac{1}{N^{D-1}+1}. \qquad (13)$$

So for $|\psi\rangle \neq 0$, at least one such coupled set of two equations leads to the expression (13). This is the only candidate for the point where the Peres condition becomes satisfied.

Now it can be easily seen that in the total-noise case $\varepsilon = 0$, $\rho_1^T = \hat{\rho}$ and all the eigenvalues of ρ_1^T are $1/(N^D)$. In the no-noise case ($\varepsilon = 1$), proceeding in similar fashion to before, the eigenvalues λ of ρ_1^T must satisfy

$$\frac{1}{N} \sum_{n,m=1}^{N} \psi_{nm\ldots m} |mn \ldots n\rangle = \lambda \sum_{i_1,i_2,\ldots,i_D=1}^{N} \psi_{i_1 i_2 \ldots i_D} |i_1 i_2 \ldots i_D\rangle. \qquad (14)$$

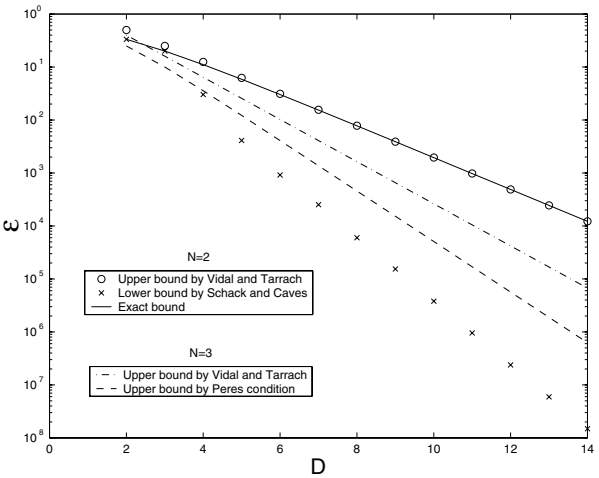

Figure 1. Bounds on the value of ε for which the states (1) become separable or entangled, for the qubit ($N = 2$) and q-trit ($N = 3$) cases, shown on the same plot. When ε is above the upper bounds or the exact bound, $\hat{\rho}$ is entangled, and when ε is below the lower bound or the exact bound, $\hat{\rho}$ is always separable. When ε is below an upper bound, $\hat{\rho}$ may be separable or bound entangled.

This gives $\psi_{i_1 i_2 \ldots i_D} = 0$ if for some $a = 3, 4, \ldots, D$, $i_2 \neq i_a$, and leads to sets of two coupled equations of the form

$$\psi_{ab\ldots b} = \lambda N \psi_{ba\ldots a}, \qquad (15)$$

$$\psi_{ba\ldots a} = \lambda N \psi_{ab\ldots b}. \qquad (16)$$

These have the solutions $\psi_{ab\ldots b} = \psi_{ba\ldots a} = 0$ or

$$\lambda = \pm \frac{1}{N^2}. \qquad (17)$$

As before, for nonzero eigenvectors, the first cannot be true. So, finally, for the no-noise state, at least one eigenvalue of ρ_1^T must be negative, and equal to

$$\lambda = -\frac{1}{N^2}. \qquad (18)$$

Thus, finally, since ε_o is the only value of ε where an eigenvalue of ρ_1^T is zero, all eigenvalues are positive for $\varepsilon = 0$, and an eigenvalue is negative for $\varepsilon = 1$, there must be at least one negative eigenvalue for $\varepsilon > \varepsilon_o$ given by (13).

When one proceeds in the same fashion when $M = 2, 3, \ldots, D/2$, one always gets coupled sets of two equations identical in form to (11), as can be seen by inspection, so nothing new is found. Thus the result of section 2 is indicated.

5. Comparison to known bounds

For the qubit case ($N = 2$), as seen in figure 1, equation (6) gives an exact bound on the values of ε that divide separable from entangled states of the form (1). One sees that the upper bound (5) derived from the work of Vidal and Tarrach comes very close to the exact value for the qubit case. This exact bound is also greater than those lower bounds previously found by Schack and Caves [6], as expected.

For the two-subsystem ($D = 2$) case, the bound (6) agrees with the exact one found by Horodecki *et al* [10].

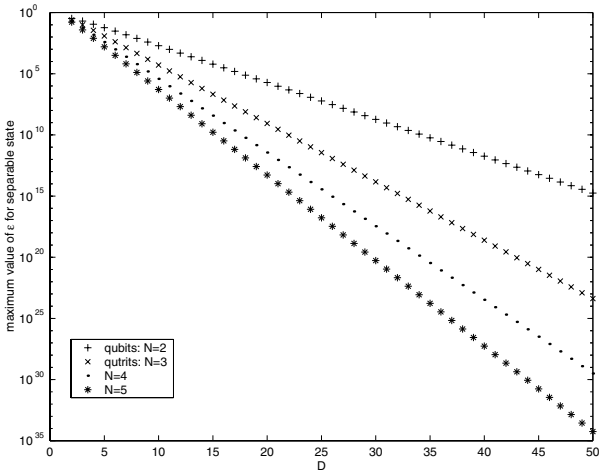

Figure 2. Upper bounds on ε for separable states of the form (1) on a logarithmic scale. Variation with subsystem Hilbert-space dimension N is shown.

For other values of D and N, the results on random robustness by Vidal and Tarrach lead to an upper bound which is considerably weaker than the upper bound (6) given by the partial transposition condition. The upper bound found here actually gives a stronger bound on the random robustness of entanglement of states given by (1):

$$R(\hat{\rho}_e||\hat{\rho}_n) \leqslant N^{D-1}. \tag{19}$$

It is interesting to note that in the border cases when $N = 2$ or $D = 2$, the bound (6) is in fact an exact bound. This is despite the fact that the Peres condition does not necessarily give a strong bound for such states. This leads one to the tentative conjecture that for noisy GHZ-type states of the form (1), the Peres condition may in general give a strong upper bound.

Looking at figure 2, one sees that as the Hilbert space dimension of the subsystems increases, the upper bound on ε rapidly decreases, indicating that the entanglement becomes stronger.

As bound (6) is completely general in N and D, it does provide some answers to the question of what raises entanglement more: creating more entangled subsystems, or increasing their dimension? Since the bound on ε decreases exponentially with D, but only polynomially with N, one concludes that increasing the number of subsystems is a more effective way of increasing the entanglement.

6. Conclusion

The results presented here based on the Peres condition provide a lower bound on the parameters ε in (1) above which the generalized Werner states are always entangled. Furthermore, it gives an exact bound on this parameter for the case of many qubits. An explicit simple expression is derived that depends on D, the number of subsystems over which entanglement occurs, and N the Hilbert space dimension of each subsystem. Apart from the few cases ($D = 2$; $N = 2$ and $D = 3$) where this bound was known exactly previously, the new bounds are stronger than previously known ones.

This work also sheds light on the question of whether to increase quantum entanglement in a system, it is better to create more entangled subsystems, or to increase the dimension of the existing subsystem. As the bound on ε decreases exponentially with N, but only polynomially with D, increasing the number of subsystems is a much more effective way of increasing entanglement.

To conclude, the Peres partial transposition condition has provided a good upper bound for determining the separability of a generalized N, D Werner state. However for other systems it is known that this transposition condition fails to give strong results, thus when this condition is useful, and when it is not, remains an interesting question.

Acknowledgments

We are grateful to Gerard Milburn for discussion about entanglement and separability. WJM acknowledges the support of the Australian Research Council.

Appendix. Proof that (6) is exact for qubits

We wish to show that the bound (6) is exact for qubits ($N = 2$), and to find the product states which combine to give the state when it is separable.

Beginning similarly to Schack and Caves [6], the D-subsystem generalization of the Werner state ((1) with $N = 2$) can be written in terms of Pauli matrices:

$$\hat{\rho}(\varepsilon) = \frac{1}{2^D}\left\{(1-\varepsilon)I^{\otimes D} + \frac{\varepsilon}{2}\hat{E}\right\}, \tag{A1a}$$

where

$$\hat{E} = (I+\sigma_3)^{\otimes D} + (I-\sigma_3)^{\otimes D} + (\sigma_1+\mathrm{i}\sigma_2)^{\otimes D} + (\sigma_1-\mathrm{i}\sigma_2)^{\otimes D}, \tag{A1b}$$

and σ_i are the Pauli matrices, I is the two-dimensional identity matrix, and for conciseness, the following notation is used:

$$(A)^{\otimes D} = (A)\otimes\cdots\otimes(A) \qquad D \text{ times.} \tag{A2}$$

To show that (6) is actually a strong bound, is suffices to find an expansion of ρ in terms of a positive sum of direct tensor products of density matrices for this value of

$$\varepsilon = \varepsilon_c = \frac{1}{2^{D-1}+1}. \tag{A3}$$

By analogy with the results of Schack and Caves [6], it has been guessed that an expansion of $\rho(\varepsilon_c)$ in terms of the density matrices

$$P_{\pm i} = \tfrac{1}{2}(I \pm \sigma_i) \qquad (i = 1, 2, 3), \tag{A4}$$

is given by the following:

$$\hat{\rho}_g = \frac{\varepsilon_c}{2}(P_3^{\otimes D} + P_{-3}^{\otimes D}) + \frac{\varepsilon_c}{2^{D-1}}\sum P_{x_1}\otimes P_{x_2}\otimes\cdots\otimes P_{x_D}. \tag{A5}$$

Here the sum is over all permutations of D indices $x_1, x_2, \ldots, x_D$ satisfying the following conditions:

(1) $x_i \in \{1, -1, 2, -2\}$.

(2) The number of $x_i \in \{2, -2\}$ is even (or zero).
(3) If the number of $x_i \in \{2, -2\}$ is a multiple of four (or is zero), then the number of $x_i \in \{-1, -2\}$ is even (or zero).
(4) If the number of $x_i \in \{2, -2\}$ is not a multiple of four, then the number of $x_i \in \{-1, -2\}$ is odd.

The proof of this proceeds by starting with the above guess, and showing that it is a correct one. As it turns out, the hard work is in actually writing down the guess mathematically, so let us begin with this.

To begin with, note that

$$\mathcal{T}_0 = (P_1 + P_2 + P_{-1} + P_{-2})^{\otimes D} = \sum P_{x_1} \otimes P_{x_2} \otimes \cdots \otimes P_{x_D}, \tag{A6}$$

where the sum is over *all* permutations of D indices $x_1, x_2, \ldots, x_N \in \{1, 2, -1, -2\}$. Also note that

$$\mathcal{S}_0 = (P_1 + P_2 - P_{-1} - P_{-2})^{\otimes D} \tag{A7}$$

will give a sum over all these permutations, except that all terms which have an odd number of indices in $\{-1, -2\}$ will be subtracted rather than added like in $\mathcal{T}_0$. Thus one can see that

$$\mathcal{R}_0^e = \tfrac{1}{2}[\mathcal{T}_0 + \mathcal{S}_0] \tag{A8a}$$

will give a sum over permutations of D indices, like $\mathcal{T}_0$, except that only terms where the number of indices in $\{-1, -2\}$ is even will be included. Similarly,

$$\mathcal{R}_0^o = \tfrac{1}{2}[\mathcal{T}_0 - \mathcal{S}_0] \tag{A8b}$$

will give a sum over only those terms in which the number of indices in $\{-1, -2\}$ is odd.

Now consider some more similar expressions.

$$\mathcal{T}_1 = (P_1 - P_2 + P_{-1} - P_{-2})^{\otimes D}. \tag{A9}$$

$\mathcal{T}_1$ will give a sum over all index permutations, except that all terms which have an odd number of indices in $\{2, -2\}$ will be subtracted rather than added like for $\mathcal{T}_0$.

$$\mathcal{T}_2 = (P_1 + \mathrm{i}P_2 + P_{-1} + \mathrm{i}P_{-2})^{\otimes D}. \tag{A10}$$

$\mathcal{T}_2$ will give a similar sum over all permutations, but terms in which the number of indices in $\{2, -2\}$ is a multiple of four (or is zero) will be added, terms in which this number is even, but not a multiple of four, will be subtracted, terms in which this number is one more than a multiple of four will be added and multiplied by i, and terms for which this number is one less than a multiple of four will be subtracted and multiplied by i:

$$\mathcal{T}_3 = (P_1 - \mathrm{i}P_2 + P_{-1} - \mathrm{i}P_{-2})^{\otimes D}. \tag{A11}$$

$\mathcal{T}_3$ is the complex conjugate of $\mathcal{T}_2$. It can be seen (after a little thought) that $\frac{1}{4}[\mathcal{T}_0 + \mathcal{T}_1 + \mathcal{T}_2 + \mathcal{T}_3]$ will give a sum over only those terms in which the number of indices in $\{2, -2\}$ is a multiple of four (or is zero). Similarly, $\frac{1}{4}[\mathcal{T}_0 + \mathcal{T}_1 - \mathcal{T}_2 - \mathcal{T}_3]$ will give a sum over only those terms in which the number of indices in $\{2, -2\}$ is even, but not a multiple of four.

Analogously to equation (A7) define

$$\mathcal{S}_1 = (P_1 - P_2 - P_{-1} + P_{-2})^{\otimes D}, \tag{A12a}$$

$$\mathcal{S}_2 = (P_1 + \mathrm{i}P_2 - P_{-1} - \mathrm{i}P_{-2})^{\otimes D}, \tag{A12b}$$

$$\mathcal{S}_3 = (P_1 - \mathrm{i}P_2 - P_{-1} + \mathrm{i}P_{-2})^{\otimes D}, \tag{A12c}$$

and one can define expressions for $\mathcal{R}_i^e$ and $\mathcal{R}_i^o$ for $i = 0, 1, 2, 3$ analogously to equations (A8*b*). So following the same reasoning as previously, the sum of all terms in which the number of indices in $\{2, -2\}$ is a multiple of four, and the number of indices in $\{-1, -2\}$ is even is given by

$$\tfrac{1}{4}[\mathcal{R}_0^e + \mathcal{R}_1^e + \mathcal{R}_2^e + \mathcal{R}_3^e]. \tag{A13}$$

And thus finally, the sum in the second term of the guess ρ_g (equation (A5)) can be written as

$$\tfrac{1}{4}[\mathcal{R}_0^e + \mathcal{R}_1^e + \mathcal{R}_2^e + \mathcal{R}_3^e] + \tfrac{1}{4}[\mathcal{R}_0^o + \mathcal{R}_1^o - \mathcal{R}_2^o - \mathcal{R}_3^o] = \tfrac{1}{4}[\mathcal{T}_0 + \mathcal{T}_1 + \mathcal{S}_2 + \mathcal{S}_3]. \tag{A14}$$

So the guess that has been made (i.e. equation (A5)) can be rewritten:

$$\rho_g = \frac{\varepsilon_c}{2}(P_3^{\otimes N} + P_{-3}^{\otimes N}) + \frac{\varepsilon_c}{2^{N+1}}[\mathcal{T}_0 + \mathcal{T}_1 + \mathcal{S}_2 + \mathcal{S}_3], \tag{A15}$$

which is explicitly (via the expressions (A6), (A7), (A9), (A12*c*)) a positive sum of direct tensor products of density matrices, and thus is separable. The only question that remains is whether $\rho_g = \rho(\varepsilon_c)$.

This is the easy part. It is seen using expression (A4) that

$$\mathcal{T}_0 = (2I)^{\otimes N} = 2^N I^{\otimes N}, \tag{A16a}$$

$$\mathcal{T}_1 = 0, \tag{A16b}$$

$$\mathcal{S}_2 = (\sigma_1 + \mathrm{i}\sigma_2)^{\otimes N}, \tag{A16c}$$

$$\mathcal{S}_3 = (\sigma_1 - \mathrm{i}\sigma_2)^{\otimes N}, \tag{A16d}$$

$$P_3^{\otimes N} = 2^{-N}(I + \sigma_3)^{\otimes N}, \tag{A16e}$$

$$P_{-3}^{\otimes N} = 2^{-N}(I - \sigma_3)^{\otimes N}, \tag{A16f}$$

so

$$\rho_g = \frac{\varepsilon_c}{2} I^{\otimes N} + \frac{\varepsilon_c}{2^{N+1}} \hat{E}, \tag{A17}$$

which only seemingly differs from equation (6) by the first term, but using the expression for ε_c (A3), one finds that these first terms are equal also.

$$\frac{1 - \varepsilon_c}{2^N} = \frac{\varepsilon_c}{2}, \tag{A18}$$

so $\rho_g = \rho$, the guess was correct, and thus the bound ε_c is strong.

References

[1] Peres A 1996 *Phys. Rev. Lett.* **77** 1413
[2] Horodecki M, Horodecki P and Horodecki R 1996 *Phys. Lett.* A **223** 1
(Horodecki M, Horodecki P and Horodecki R 1996 *Preprint* quant-ph/9605038)
[3] Lewenstein M, Cirac J I and Karnas S 1999 *Preprint* quant-ph/9903012
[4] Życzkowski K, Horodecki P, Sanpera A and Lewenstein M 1998 *Phys. Rev.* A **58** 883
[5] Vidal G and Tarrach R 1999 *Phys. Rev.* A **59** 141
[6] Schack R and Caves C M 2000 *J. Mod. Opt* **47** 387
[7] Braunstein S L, Caves C M, Jozsa R, Linden N, Popescu S and Schack R 1999 *Phys. Rev. Lett.* **83** 1054
[8] Werner R F 1989 *Phys. Rev.* A **40** 4277
[9] Caves C M and Milburn G J 1999 *Preprint* quant-ph/9910001
[10] Horodecki M and Horodecki P 1999 *Phys. Rev.* A **59** 4206
[11] Murao M, Plenio M B, Popescu S, Vedral V and Knight P L 1998 *Phys. Rev.* A **57** R4075
[12] Horodecki R and Horodecki M 1996 *Phys. Rev.* A **54** 1838