Entangled Quantum States and the Kronecker Product

Willi-Hans Steeb and Yorick Hardy

International School for Scientific Computing, Rand Afrikaans University, P.O. Box 524, Auckland Park 2006, South Africa

Reprint requests to Prof. W.-H. S.; E-mail: whs@na.rau.ac.za

Z. Naturforsch. **57 a,** 689–691 (2002); received March 25, 2002

Entangled quantum states are an important component of quantum computing techniques such as quantum error-correction, dense coding and quantum teleportation. We determine the requirements for a state in the Hilbert space $\mathbf{C}^m \otimes \mathbf{C}^n$ for $m, n \in \mathbf{N}$ to be entangled and a solution to the corresponding "factorization" problem if this is not the case. We consider the implications of these criteria for computer algebra applications.

Key words: Entangled States; Quantum Computing; Computer Algebra; Hilbert Space.

1. Entanglement

Entanglement is the characteristic trait of quantum mechanics which enforces its entire departure from classical lines of thought [1 - 6]. We consider entanglement of pure states. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two finite dimensional Hilbert spaces. Thus a basic question in quantum computing is as follows: given a normalized state $|z\rangle$ in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, can two normalized states $|x\rangle$ and $|y\rangle$ in the Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively be found such that

$$|x\rangle \otimes |y\rangle = |z\rangle. \quad (1)$$

In other words, what is the condition on $|z\rangle$ such that $|x\rangle$ and $|y\rangle$ exist? If no such $|x\rangle$ and $|y\rangle$ exist then $|z\rangle$ is said to be *entangled*. The measure for entanglement for pure states $E(|u\rangle\langle u|)$ is defined as follows [6]:

$$E(|u\rangle\langle u|) := S_{\dim(\mathcal{H}_1)}(\rho_{\mathcal{H}_1}) = S_{\dim(\mathcal{H}_2)}(\rho_{\mathcal{H}_2}), \quad (2)$$

where the density operators are defined as

$$\rho_{\mathcal{H}_1} := \mathrm{Tr}_{\mathcal{H}_2}|u\rangle\langle u|, \ \rho_{\mathcal{H}_2} := \mathrm{Tr}_{\mathcal{H}_1}|u\rangle\langle u| \quad (3)$$

and

$$S_b(\rho) := -\mathrm{Tr}\rho \log_b \rho. \quad (4)$$

Tr denotes the trace and $\mathrm{Tr}_{\mathcal{H}_1}$ denotes the partial trace over $\mathcal{H}_1$. We use the base b for the logarithm $\log_b$. We have $0 \log_b 0 = 0$ and $1 \log_b 1 = 0$. Thus $0 \leq E \leq 1$. If $E = 1$ we call the pure state maximally entangled. If $E = 0$, the pure state is not entangled. We note that

$$S_b(\rho) = -\sum_{j=1}^{k} \lambda_j \log_b \lambda_j, \quad (5)$$

where $\{ \lambda_j, \ j = 1, \ldots, k \}$ are the eigenvalues of ρ, and ρ is an operator on a k dimensional Hilbert space.

Next we describe the relation between conditions for entanglement and the measure of entanglement introduced above. The cases $m = n = 2$ and $m = n = 3$ have been discussed by Steeb and Hardy [3, 4]. We prove that, if $|z\rangle$ can be written as the Kronecker product $|x\rangle \otimes |y\rangle$ then $E(|z\rangle\langle z|) = 0$, and conversely, if $E(|z\rangle\langle z|) = 0$ it follows that $|z\rangle$ can be written as $|x\rangle \otimes |y\rangle$.

2. Conditions for Separability

Let $m := \dim(\mathcal{H}_1)$, $n := \dim(\mathcal{H}_2)$,

$$\{ |j\rangle_{\mathcal{H}_1}, j = 0, 1, \ldots, m-1 \} \quad (6)$$

be an orthonormal basis for $\mathcal{H}_1$, and

$$\{ |j\rangle_{\mathcal{H}_2}, j = 0, 1, \ldots, n-1 \} \quad (7)$$

be an orthonormal basis for $\mathcal{H}_2$. Thus

$$\{ |j\rangle_{\mathcal{H}_1} \otimes |k\rangle_{\mathcal{H}_2}, j = 0, 1, \ldots, m-1, \quad k = 0, 1, \ldots, n-1 \} \quad (8)$$

is an orthonormal basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$. We consider arbitrary normalized states $|x\rangle$, $|y\rangle$ and $|z\rangle$ in the Hilbert spaces $\mathcal{H}_1$, $\mathcal{H}_2$ and $\mathcal{H}_1 \otimes \mathcal{H}_2$ respectively. We can identify these states with the vectors $(x_0, x_1, \ldots, x_{m-1})^T \in \mathbf{C}^m$, $(y_0, y_1, \ldots, y_{m-1})^T \in \mathbf{C}^n$ and $(z_0, z_1, \ldots, z_{nm-1})^T \in \mathbf{C}^{mn}$ as follows:

$$|x\rangle := \sum_{j=0}^{m-1} x_j |j\rangle_{\mathcal{H}_1} \; |y\rangle := \sum_{j=0}^{n-1} y_j |j\rangle_{\mathcal{H}_2}, \qquad (9)$$

$$|z\rangle := \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} z_{in+j} |i\rangle_{\mathcal{H}_1} \otimes |j\rangle_{\mathcal{H}_2} \qquad (10)$$

$$\sum_{j=0}^{m-1} |x_j|^2 = 1, \; \sum_{j=0}^{n-1} |y_j|^2 = 1, \; \sum_{j=0}^{nm-1} |z_j|^2 = 1. \qquad (11)$$

Thus we see that the tensor product is equivalent to considering the Kronecker product [7]. To ensure that $|z\rangle$ is the product state of $|x\rangle$ and $|y\rangle$ we must have

$$\forall i \in \{0, 1, \ldots, m-1\},\; j \in \{0, 1, \ldots, n-1\}:$$

$$x_i y_j = z_{in+j}. \qquad (12)$$

Thus

$$x_i y_j x_k y_l = z_{in+j} z_{kn+l} = z_{in+l} z_{kn+j}, \qquad (13)$$

$$i = 0, 1, \ldots, m-1,\; j = 0, 1, \ldots, n-1, \qquad (14)$$

$$k = i+1, i+2, \ldots, m-1, l = j+1, j+2, \ldots, n-1. \qquad (15)$$

There are

$$\Big(\sum_{i=0}^{m-1}(m-1-i)\Big)\Big(\sum_{j=0}^{n-1}(n-1-j)\Big) \qquad (16)$$

$$= \frac{mn(m-1)(n-1)}{4}$$

such equations. Supposing equations (13) hold, then a "factorization" is given by

$$x_j = \Big(\sum_{k=0}^{n-1} |z_{jn+k}|^2\Big)^{\frac{1}{2}} e^{i\alpha_j}, \qquad (17)$$

$$y_j = \Big(\sum_{k=0}^{m-1} |z_{kn+j}|^2\Big)^{\frac{1}{2}} e^{i\beta_j}, \qquad (18)$$

$$\alpha_j = (1 - \delta_{j,0})(\arg(z_{jn}) - \beta_0), \qquad (19)$$

$$\beta_j = \arg(z_j). \qquad (20)$$

We will omit the subscripts $\mathcal{H}_1$ and $\mathcal{H}_2$ since the Hilbert space will be clear from the context. Since

$$|z\rangle\langle z| = \sum_{i,k=0}^{m-1} \sum_{j,l=0}^{n-1} z_{in+j} \overline{z_{kn+l}} (|i\rangle\langle k|) \otimes (|j\rangle\langle l|) \qquad (21)$$

we find for the density operator

$$\rho_{\mathcal{H}_2} = \mathrm{tr}_{\mathcal{H}_1} |z\rangle\langle z| = \sum_{i=0}^{m-1} (\langle i| \otimes I_n)|z\rangle\langle z|(|i\rangle \otimes I_n) \qquad (22)$$

$$= \sum_{i=0}^{m-1} \sum_{j,l=0}^{n-1} z_{in+j} \overline{z_{in+l}} |j\rangle\langle l| \qquad (23)$$

and

$$\rho_{\mathcal{H}_1} = \mathrm{tr}_{\mathcal{H}_2} |z\rangle\langle z| = \sum_{i=0}^{n-1} (I_m \otimes \langle i|)|z\rangle\langle z|(I_m \otimes |i\rangle) \qquad (24)$$

$$= \sum_{j=0}^{n-1} \sum_{i,k=0}^{m-1} z_{in+j} \overline{z_{kn+j}} |i\rangle\langle k|. \qquad (25)$$

Since (when the equations (13) hold)

$$\overline{z_k} \sum_{i=0}^{m-1} z_{in+j} \overline{z_{in+l}} = \overline{z_l} \sum_{i=0}^{m-1} z_{in+j} \overline{z_{in+k}} \qquad (26)$$

and

$$\overline{z_{ln}} \sum_{j=0}^{n-1} z_{in+j} \overline{z_{kn+j}} = \overline{z_{in}} \sum_{j=0}^{n-1} z_{in+j} \overline{z_{ln+j}}, \qquad (27)$$

we find $\mathrm{rank}(\rho_{\mathcal{H}_1}) = \mathrm{rank}(\rho_{\mathcal{H}_2}) = 1$. Thus exactly one of the eigenvalues of $\rho_{\mathcal{H}_1}$ and exactly one of the eigenvalues of $\rho_{\mathcal{H}_2}$ are non-zero. Since $\rho_{\mathcal{H}_1}$ and $\rho_{\mathcal{H}_2}$ are positive operators with unit trace, they have eigenvalues $\{0, 1\}$ with appropriate multiplicities. Thus $S(\rho_{\mathcal{H}_1}) = S(\rho_{\mathcal{H}_2}) = 0$.

For the converse, suppose $S(\rho_{\mathcal{H}_1}) = S(\rho_{\mathcal{H}_2}) = 0$. We will consider $S(\rho_{\mathcal{H}_1}) = 0$. Since $\rho_{\mathcal{H}_1}$ is a positive operator with unit trace, the eigenvalues $\{\lambda_j, j = 1, \ldots, m\}$ must satisfy $0 \leq \lambda_j \leq 1$ and $\sum_{j=1}^{m} \lambda_j = 1$.

Since $-\lambda_j \log_m \lambda_j \geq 0$, we find that all the eigenvalues except one are zero. The eigenspace corresponding to the eigenvalue has the dimension $m-1$, i. e. there exist $m-1$ linearly independent vectors $|\boldsymbol{a}\rangle$ such that $\rho_{\mathcal{H}_1}|\boldsymbol{a}\rangle = 0$. Thus all vectors

$$\sum_{j=0}^{n-1}\sum_{k=0}^{m-1} z_{in+j}\overline{z_{kn+j}}|k\rangle \tag{28}$$

are orthogonal to all $m-1$ of the $|\boldsymbol{a}\rangle$, and as a consequence they are all scalar multiples of each other. Thus we find

$$\forall i,k,l \in \{0,1,\dots,m-1\}:$$

$$\sum_{j=0}^{n-1} z_{in+j}\overline{z_{kn+j}} = \alpha_{il}\sum_{j=0}^{n-1} z_{ln+j}\overline{z_{kn+j}}, \tag{29}$$

$$\sum_{j=0}^{n-1}(z_{in+j} - \alpha_{il}z_{ln+j})\overline{z_{kn+j}} = 0. \tag{30}$$

This is the inner product [1] between $\sum_{j=0}^{n-1}(z_{in+j} - \alpha_{il}z_{ln+j})|j\rangle$ and $\sum_{j=0}^{n-1} z_{kn+j}|j\rangle$.

Since $\dim(\mathcal{H}_1) = m$, the vectors cannot all be orthogonal and non-zero. Suppose

$$|\boldsymbol{b}\rangle := \sum_{j=0}^{n-1}(z_{in+j} - \alpha_{il}z_{ln+j})|j\rangle \tag{31}$$

is non-zero. The vectors $\sum_{j=0}^{n-1} z_{in+j}|j\rangle$ and $\sum_{j=0}^{n-1} z_{ln+j}|j\rangle$ define at most a two-dimensional vector space. If $z_{in+j} = z_{ln+j} = 0$ for all j, then $z_{in+j} = \alpha_{il}z_{ln+j}$ trivially, where we choose $\alpha_{il} = 1$. If this is not the case, the vector $|\boldsymbol{b}\rangle$ is a linear combination of these two vectors and yet is orthogonal to both – a contradiction. Thus we conclude

$$\forall j \in \{0,1,\dots,n-1\}: z_{in+j} = \alpha_{ik}z_{kn+j}. \tag{32}$$

If $\alpha_{ik} = 0$, then $z_{in+j} = z_{kn+j} = 0$ and $z_{in+j}z_{kn+l} = 0 = z_{kn+j}z_{in+l}$. Thus we consider the case $\alpha_{ik} \neq 0$. In this case we have $\alpha_{ik} = \alpha_{ki}^{-1}$. Now we consider

$$z_{in+j}z_{kn+l} = \alpha_{ik}z_{kn+j}\alpha_{ki}z_{in+l} = z_{in+l}z_{kn+j}. \tag{33}$$

Thus the two conditions for separability are equivalent.

3. Implications for Computer Algebra

The condition $S(\rho_{\mathcal{H}_1}) = 0$ is a compact criterium for separability, so we should ask the question, when are the conditions (13) we have derived useful? The condition involves equations quadratic in mn, so at least there are only a polynomial number of tests in m and n. In a computer algebra application the density operators will in general be symbolic. The condition $S(\rho_{\mathcal{H}_1}) = 0$ involves determining the rank of $\rho_{\mathcal{H}_1}$. This could be determined by Gauss elimination, which involves a total of $(mn)^2 + O((\min\{m,n\})^3)$ multiplications, including the calculation of the density matrix from the pure state. Here the criterium is independent of basis, whereas our condition relies on the choice of a particular basis. However, in computer algebra applications we usually choose a basis before any computation, and changing the basis is a simple computational task. Our criterium is simpler to test and involves less than $\frac{1}{2}(mn)^2$ multiplications. Thus in applications such as finding quantum algorithms using genetic programming [8] where efficiency in determining fitness is important, it may be useful and more efficient to apply our criteria. Of course testing for entanglement is important since entanglement is a necessary criterium for universal quantum computation.

[1] W.-H. Steeb, Hilbert Spaces, Wavelets, Generalised Functions and Modern Quantum Mechanics, Kluwer Academic Publishers, Dordrecht 1998.

[2] J. Preskill, Quantum Information and Computation, http://www.theory.caltech.edu/ preskill/ph229.

[3] W.-H. Steeb and Y. Hardy, Int. J. Theor. Physics, **39**, 2765 (2000).

[4] W.-H. Steeb and Y. Hardy, Int. J. Mod. Physics C **11**, 69 (2000).

[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed State Entanglement and Quantum Error Correction, http://xxx.lanl.gov/quant-ph/9604024.

[6] Y. Hardy and W.-H. Steeb, Classical and Quantum Computing with C++ and Java Simulations, Birkhäuser Verlag, Basel 2001.

[7] W.-H. Steeb, Matrix Calculus and Kronecker Product with Applications and C++ Programs, World Scientific, Singapore 1997.

[8] L. Spector, H. Barnum, H. J. Bernstein, and N. Swamy, Finding a Better-than-Classical Quantum AND/OR Algorithm using Genetic Programming, Proceedings of the 1999 Congress on Evolutionary Computation, IEEE Press.