Entanglement witness derived from NMR superdense coding

2006 J. Phys. A: Math. Gen. 39 2151

(http://iopscience.iop.org/0305-4470/39/9/011)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 2151–2159 doi:10.1088/0305-4470/39/9/011

Entanglement witness derived from NMR superdense coding

Robabeh Rahimi[1], **Kazuyuki Takeda**[1], **Masanao Ozawa**[2] **and Masahiro Kitagawa**[1]

[1] Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan
[2] Graduate School of Information Sciences, Tohoku University, Aoba-ku, Sendai 980-8579, Japan

E-mail: rahimi@qc.ee.es.osaka-u.ac.jp

Received 10 August 2005, in final form 19 January 2006
Published 15 February 2006
Online at stacks.iop.org/JPhysA/39/2151

Abstract

It is shown that superdense coding (SDC) experiments by means of nuclear magnetic resonance (NMR) can show non-classical efficiency gain over classical communication only for nuclear spin polarization beyond a certain threshold, and this threshold coincides with that for non-separability of the density matrix. It is also claimed that transfer of two-bit information mediated by a single qubit in the previous NMR SDC experiments with low nuclear spin polarization is not ascribed to the non-classical effect induced by entanglement, but merely to a statistical effect in an ensemble system having a large number of molecules. Towards experimental detection of entanglement, a new class of entanglement witnesses is proposed, which is based on the measurement of nuclear spin magnetizations in the Bell basis and is suitable for actual NMR experiments.

PACS numbers: 03.65.Ud, 03.67.Hk, 87.64.Hd

1. Introduction

Nuclear magnetic resonance (NMR), which is widely used to investigate the structure and dynamics of chemical/biochemical materials [1], has been incorporated into quantum information science for a decade. Among several candidates for physical realization of quantum information processing, NMR is an outstanding approach, with which one can implement relatively complicated quantum algorithms [2]. However, there is confusion in NMR quantum information processing with regard to the role of entanglement in its implementation of non-local algorithms such as superdense coding (SDC) [3] and quantum teleportation [4].

Entanglement is believed to play an essential role in quantum information processing and particularly in the non-local quantum algorithms [5, 6], where remarkable non-classical effects arise such as transfer of two classical bits of information via a single qubit for SDC [3, 7] and transfer of a quantum state from one place to another for quantum teleportation [4]. This may imply that experimental demonstrations of these non-local algorithms by means of NMR [3, 4] had accompanied entanglement in the system of nuclear spins. On the other hand, however, there has also been a mathematical proof *against* the existence of entanglement in those NMR experiments and most NMR experiments performed with low nuclear spin polarization [8, 9]. It has been shown that a density matrix representing the nuclear spin state is separable into a direct product of submatrices (i.e., *not* entangled), unless the initial nuclear spin polarization exceeds a certain threshold. Since this threshold is far beyond the nuclear polarization in those NMR experiments, the nuclear spin systems in question cannot, according to the mathematical argument, possess entanglement.

In this work, we deal with this apparent controversy between the NMR experiments and the mathematical argument, taking SDC as an example of the non-local algorithms. We show that there is not any non-classical efficiency gain in the previous report on NMR SDC experiments, so that the seemingly successful implementation of NMR SDC is not due to the existence of entanglement, but is merely ascribed to a statistical effect specific to ensemble quantum computing. We also show that the efficiency gain due to the non-local quantum effect only arises for the initial nuclear spin polarization exceeding a certain threshold, and this threshold satisfactorily coincides with that for non-separability of the density matrix.

Once the apparent paradox has been resolved, we propose a scheme to experimentally detect entanglement, extending the concept of entanglement witness [10, 11]. We introduce a new class of entanglement witnesses based on the measurement of nuclear spin magnetizations in the Bell basis. This approach provides a simple and convenient way of evaluating the existence of entanglement in a single run experiment, and is applicable to all possible states encountered in SDC. Although the entanglement witness derived from the conventional approach is also shown to be measurable in a single run experiment, it requires pre-application of somewhat complicated unitary transformation which moreover depends on the quantum state of interest.

2. NMR SDC for a pure initial state

Let us consider a pair of nuclear spins $I = 1/2$ and $S = 1/2$ placed in a static magnetic field B_0, and suppose for a moment that the system is initially in a pure state $|\psi_0\rangle = |00\rangle$. The procedure of SDC, whose quantum circuit is described in figure 1, is as follows [7]. Firstly, the entangling operation $U_{\rm ent}$ is performed, i.e., a Hadamard gate on the I spin ($H_I \otimes I_S$) is followed by a controlled-NOT gate ($U_{\rm cn}$) whose control and target qubits are the I and S spins, respectively. The quantum state $|\psi_1\rangle$ after the entangling operation $U_{\rm ent} = U_{\rm cn}(H_I \otimes I_S)$ is represented as

$$|\psi_1\rangle = U_{\rm ent}|\psi_0\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv |\beta_{00}\rangle. \tag{2.1}$$

Here, $|\beta_{00}\rangle$ is known as one of the four Bell states [12]

$$|\beta_{zx}\rangle \equiv \frac{|0, x\rangle + (-1)^z|1, \bar{x}\rangle}{\sqrt{2}}, \tag{2.2}$$

where $z, x = 0, 1$ and $\bar{x} = 1 - x$. Secondly, the S spin is given to, say, Alice, and the I spin to, say, Bob. Bob then encodes a two-bit classical message zx on the I spin by applying a

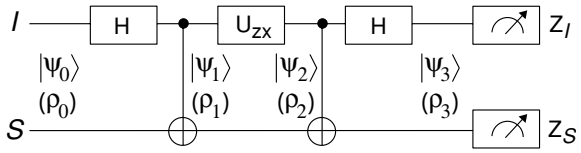

Figure 1. A quantum circuit for superdense coding for a system of nuclear spins I and S. The states $|\psi_i\rangle$ and ρ_i ($i = 0, 1, 2, 3$) correspond to that described in the text for the cases of a pure initial state and a mixed initial state, respectively. The final measurement is performed on the state $|\psi_3\rangle$ or ρ_3 using observables Z_I and Z_S corresponding to the nuclear spin magnetizations.

unitary operation $U_{zx} = Z^z X^x$, and then sends off the encoded qubit to Alice. The effect of the unitary transformation U_{zx} is to toggle $|\psi_1\rangle = |\beta_{00}\rangle$ into another Bell state. That is,

$$|\psi_2\rangle = U_{zx}|\beta_{00}\rangle = |\beta_{zx}\rangle. \tag{2.3}$$

Then, Alice applies the disentangling operation $U_{\text{disent}} = (H_I \otimes I_S)U_{\text{cn}}$, which is the inverse operation of U_{ent}. Now the state $|\psi_3\rangle$ becomes

$$|\psi_3\rangle = U_{\text{disent}}|\psi_2\rangle = |zx\rangle. \tag{2.4}$$

Finally, Alice performs measurement of the resultant magnetizations Z_I and Z_S and extracts the results as $(-1)^z$ and $(-1)^x$, from which Alice can tell the message zx encoded in the I spin by Bob.

In this ideal case of the pure initial state, the two classical bits of message zx would successfully be transferred via the I spin alone. Hence, communication by SDC is efficient by a factor of 2 as compared to the classical communication. Such non-classical efficiency gain is ascribed to the existence of entanglement in the Bell state.

3. NMR SDC for a mixed state

In actual NMR experiments carried out in a static magnetic field B_0 (typically $\sim$10 tesla), a system of nuclear spins is in a mixed state. In most cases, the Zeeman interaction

$$H = -\sum_{i=0}^{m-1} \frac{\hbar\gamma_i B_0}{2} Z_i \tag{3.1}$$

is overwhelmingly dominant over other nuclear spin interactions. Here, γ_i and Z_i are the gyromagnetic ratio and the z component of the Pauli operators of the ith spin, respectively. In thermal equilibrium at temperature T, nuclear spin polarization ϵ_i is given by

$$\epsilon_i = \tanh\left(\frac{-\gamma_i \hbar B_0}{2k_B T}\right), \tag{3.2}$$

from which probabilities p_i and q_i of finding the ith spin in the states $|0\rangle$ and $|1\rangle$, respectively, are obtained as

$$p_i = \frac{1+\epsilon_i}{2}, \qquad q_i = \frac{1-\epsilon_i}{2}. \tag{3.3}$$

In an ensemble of an m-qubit system, a density matrix representing a thermal equilibrium state is given by

$$\rho_{m\text{-}qubit} = \rho^1 \otimes \cdots \otimes \rho^m = \otimes_{i=1}^m \rho^i, \tag{3.4}$$

where ρ^i is the density matrix for the ith nuclear spin and is written as

$$\rho^i = p_i|0\rangle\langle 0| + q_i|1\rangle\langle 1|. \tag{3.5}$$

Except at very low temperatures, the energy splitting $\hbar\gamma_i B_0$ between the states $|0\rangle$ and $|1\rangle$ is much smaller than the thermal energy $k_B T$, and as a consequence, the nuclear spin polarization is very low and the system is in a highly mixed state. Accordingly, information processing should be evaluated statistically.

For an ensemble system of isolated pairs of nuclear spins $I = 1/2$ and $S = 1/2$, the initial state is described by a density matrix ρ_0 represented as

$$\begin{aligned}\rho_0 &= (p_I|0\rangle\langle 0| + q_I|1\rangle\langle 1|) \otimes (p_S|0\rangle\langle 0| + q_S|1\rangle\langle 1|) \\ &= p_I p_S|00\rangle\langle 00| + p_I q_S|01\rangle\langle 01| + q_I p_S|10\rangle\langle 10| + q_I q_S|11\rangle\langle 11|. \end{aligned} \tag{3.6}$$

The state ρ_1 after performing the entangling operation U_{ent} is a general Bell diagonal state of the form

$$\begin{aligned}\rho_1 &= U_{\text{ent}}\rho_0 U_{\text{ent}}^\dagger \\ &= p_I p_S|\beta_{00}\rangle\langle\beta_{00}| + p_I q_S|\beta_{01}\rangle\langle\beta_{01}| \\ &\quad + q_I p_S|\beta_{10}\rangle\langle\beta_{10}| + q_I q_S|\beta_{11}\rangle\langle\beta_{11}|. \end{aligned} \tag{3.7}$$

Then, when Bob encodes the message zx by applying the unitary operation U_{zx}, the state ρ_1 is toggled into another Bell diagonal state ρ_2 given by

$$\begin{aligned}\rho_2 &= U_{zx}\rho_1 U_{zx}^\dagger \\ &= p_I p_S|\beta_{z,x}\rangle\langle\beta_{z,x}| + p_I q_S|\beta_{z,\bar{x}}\rangle\langle\beta_{z,\bar{x}}| \\ &\quad + q_I p_S|\beta_{\bar{z},x}\rangle\langle\beta_{\bar{z},x}| + q_I q_S|\beta_{\bar{z},\bar{x}}\rangle\langle\beta_{\bar{z},\bar{x}}|, \end{aligned} \tag{3.8}$$

and the state ρ_3 after the disentangling operation by Alice is obtained as

$$\begin{aligned}\rho_3 &= U_{\text{disent}}\rho_2 U_{\text{disent}}^\dagger \\ &= p_I p_S|z,x\rangle\langle z,x| + p_I q_S|z,\bar{x}\rangle\langle z,\bar{x}| \\ &\quad + q_I p_S|\bar{z},x\rangle\langle\bar{z},x| + q_I q_S|\bar{z},\bar{x}\rangle\langle\bar{z},\bar{x}| \\ &= (p_I|z\rangle\langle z| + q_I|\bar{z}\rangle\langle\bar{z}|) \otimes (p_S|x\rangle\langle x| + q_S|\bar{x}\rangle\langle\bar{x}|). \end{aligned} \tag{3.9}$$

The final measurement of the spin magnetizations is done on the ensemble system composed of n molecules. That is, the net magnetizations $\sum_{i=1}^n Z_I^{(i)}$ and $\sum_{i=1}^n Z_S^{(i)}$ are measured on the product state $\otimes_{i=0}^n \rho_3^{(i)}$, where $\rho_3^{(i)}$ stands for the density matrix ρ_3 of the ith molecule. The result of the measurement gives binomial probability distribution over $(-n, -n+1, \ldots, -1, 0, 1, \ldots, n-1, n)$ with the mean values μ_I and μ_S to be

$$\mu_I = (-1)^z np_I + (-1)^{\bar{z}} nq_I = (-1)^z n\epsilon_I, \qquad \mu_S = (-1)^x np_S + (-1)^{\bar{x}} nq_S = (-1)^x n\epsilon_S. \tag{3.10}$$

Since we are now dealing with a statistical issue in an ensemble system, it is necessary to evaluate the distribution width and error probability. To be specific, we assume here that $z = x = 0$. The following discussion can straightforwardly be extended to other choices on zx. The corresponding variances are given by

$$\sigma_\xi^2 = 4np_\xi q_\xi = n\big(1 - \epsilon_\xi^2\big), \tag{3.11}$$

for $\xi = I, S$. Thereby, the relative distribution widths are characterized by

$$\frac{\sigma_\xi}{\mu_\xi} = \frac{\sqrt{n\big(1-\epsilon_\xi^2\big)}}{n\epsilon_\xi} \approx \frac{1}{\epsilon_\xi\sqrt{n}}. \tag{3.12}$$

Since the relative widths given in (3.12) decrease as $\sqrt{n}$, the greater the number of molecules, the closer the measurement is expected to give results to the mean values (3.10).

Now we evaluate the possibility of obtaining a negative value in the measurement of $Z_I^{(i)}$ even if the mean value $\mu_I = (-1)^{z=0} n\epsilon_I$ is positive. This error probability $P_{\rm e}$ is formulated as

$$P_{\rm e} = P\left(\sum_{i=1}^{n} Z_I^{(i)} < 0 \middle| z = 0\right). \tag{3.13}$$

In order to show that $P_{\rm e}$ is negligible for a range of n in most current NMR experiments, we use the DeMoivre and Laplace theorems [13]

$$P\left\{\alpha < \frac{\sum_i^n Z_I^{(i)} - \mu_I}{\sigma_I} < \beta\right\} \approx \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta {\rm e}^{-\frac{x^2}{2}}\, {\rm d}x, \tag{3.14}$$

from which we have for $n \gg 1$

$$\begin{aligned} P_{\rm e} &= P\left\{-\infty < \frac{\sum_i^n Z_I^{(i)} - \mu_I}{\sigma_I} < -\frac{\mu_I}{\sigma_I}\right\} \\ &\approx \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\mu_I/\sigma_I} {\rm e}^{-\frac{x^2}{2}}\, {\rm d}x \\ &\approx \frac{1}{\sqrt{2\pi}} {\rm e}^{-\frac{(n\epsilon_I^2)}{2}} \frac{1}{(\sqrt{n}\epsilon_I)}. \end{aligned} \tag{3.15}$$

In an ensemble system with a large number of molecules, the results of the measurement on the spin magnetizations Z_I and Z_S are very close to the mean values (3.10) with negligible error probabilities (3.15). In a typical NMR experiment, the number n of molecules is as large as $\sim 10^{18}$, and spin polarization ϵ is as small as $\epsilon \sim 10^{-5}$. Then we calculate $P_{\rm e}$ to be $\ll 10^{-100}$, which is virtually negligible. Therefore, we summarize the results of the measurement of the spin magnetizations Z_I and Z_S to be as follows:

$$\langle Z_I \rangle = (-1)^z \epsilon_I \qquad \langle Z_S \rangle = (-1)^x \epsilon_S. \tag{3.16}$$

In fact, actual NMR experiments do require a very large number of molecules due to the low sensitivity. The NMR signal intensity V_S is formally given by

$$V_S = \tfrac{1}{4}\sqrt{(Q/V)\mu_0 R\omega_I}\hbar\gamma_I n\epsilon_I, \tag{3.17}$$

where $\omega_I = \hbar\gamma_I$ is the resonance frequency, V is the volume of the detection coil and Q and R are the quality factor and the resistance of the resonant circuit, respectively. On the other hand, the noise amplitude V_N is determined by the Nyquist formula [14]

$$V_N = \sqrt{4k_B T R \Delta\nu}, \tag{3.18}$$

where $\Delta\nu$ is the amplifier bandwidth. Thus, in order to detect NMR signals with appreciable signal-to-noise ratio for moderate values $V \sim 1\ {\rm cm}^3$ and $Q \sim 10^2$, the number n of molecules is required to be larger than $\sim 10^{16}$. This lower bound for n happens to result in indiscernible statistical distribution and error probability. It follows that the two-bit message can be transferred, regardless of polarization and therefore separability of the density matrix. We emphasize that this does not necessarily mean that the NMR experiment described here is a real demonstration of SDC with the mixed states, because the successful transfer can merely be due to the statistical effect in an ensemble system having a very large number of molecules. The two-bit message carried by $\sim 10^{18}$ molecules (resources) cannot be counted as any gain in the first place.

4. Detection of entanglement

From the density matrix ρ_2 in (3.8), we obtain a probability for successful SDC to be $p_I p_S$, with which a two-bit message can be transferred through a single qubit. On the other hand, in classical communication, a single-bit channel can carry at most one bit of information even if the message is a two-bit message. Then, the best the receiver can do is just to bet on the other bit, which will turn out to be correct with a probability of $1/2$. Therefore, the efficiency gain in SDC over the classical communication is attained provided that

$$p_I p_S > 1/2 \tag{4.1}$$

is satisfied. It is worth noting here that this condition exactly coincides with the condition for the non-separability of ρ_2 derived from, e.g., the negativity criterion [15, 16]. Hence, the NMR experiments and the mathematical argument are satisfactorily consistent to each other, and the apparent confusion between them has indeed been resolved.

To put it another way, when a quantity F defined by

$$F \equiv 1/2 - p_I p_S \tag{4.2}$$

has a negative value, the NMR SDC accompanies entanglement and exhibits non-classical nature. Detection of entanglement through finding a negative value for an observable is reminiscent of the entanglement witness [10, 11]. The entanglement witness is a Hermitian operator $W = W^\dagger$ which has positive mean values for all separable states ρ, $\mathrm{Tr}(W\rho) > 0$, but a negative mean value for at least one entangled state σ_{ent}, $\mathrm{Tr}(W\sigma_{\mathrm{ent}}) < 0$. We rewrite F as

$$\begin{aligned} F &= \tfrac{1}{2} - \tfrac{1}{4}(1+\epsilon_I)(1+\epsilon_S) \\ &= \tfrac{1}{2} - \tfrac{1}{4}(1+|\langle Z_I\rangle|)(1+|\langle Z_S\rangle|), \end{aligned} \tag{4.3}$$

where we have used (3.16). The absolute values are required for the evaluation of the function F for different choices of zx.

The measurement on the state ρ_3 with the observables Z_I and Z_S is equivalent to the measurement on the state ρ_2 (or ρ_1 in the special case of $z = x = 0$) in the Bell basis because

$$\begin{aligned} \langle Z_I\rangle &= \mathrm{Tr}\,\rho_3(Z_I \otimes I_S) \\ &= \mathrm{Tr}\,\rho_2(X_I \otimes X_S) = \langle W_1\rangle \end{aligned} \tag{4.4}$$

$$\begin{aligned} \langle Z_S\rangle &= \mathrm{Tr}\,\rho_3(I_I \otimes Z_S) \\ &= \mathrm{Tr}\,\rho_2(Z_I \otimes Z_S) = \langle W_2\rangle, \end{aligned} \tag{4.5}$$

where the two observables W_1 and W_2 are defined as

$$W_1 \equiv U_{\mathrm{disent}}^\dagger (Z_I \otimes I_S) U_{\mathrm{disent}} = X_I \otimes X_S, \tag{4.6}$$

$$W_2 \equiv U_{\mathrm{disent}}^\dagger (I_I \otimes Z_S) U_{\mathrm{disent}} = Z_I \otimes Z_S. \tag{4.7}$$

From (4.3), (4.4) and (4.5), F is further rewritten as

$$F \equiv f(\langle W_1\rangle, \langle W_2\rangle) \equiv \tfrac{1}{2} - \tfrac{1}{4}(1+|\langle W_1\rangle|)(1+|\langle W_2\rangle|). \tag{4.8}$$

Since magnetizations carry information as to spin polarization, separate and simultaneous measurement of the observables W_1 and W_2 tells us the existence of entanglement. That is, if $\langle W_1\rangle$ and $\langle W_2\rangle$ satisfy

$$F \equiv f(\langle W_1\rangle, \langle W_2\rangle) < 0, \tag{4.9}$$

then the state is entangled. In the sense that a set of W_1 and W_2 gives information on the existence of entanglement through negativity of F (4.8), W_1 and W_2 can be regarded as a new class of entanglement witnesses. Furthermore, the measurement of magnetizations is quite straightforward in actual NMR experiments [1].

We note that entanglement can also be detected in principle by measuring the conventional entanglement witness [10, 11]. For ρ_2, the entanglement witness derived through the conventional approach [10, 11] is

$$W = \tfrac{1}{4}(I_I \otimes I_S + (-1)^{\bar{z}} X_I \otimes X_S + (-1)^{\bar{z}}(-1)^{\bar{x}} Y_I \otimes Y_S + (-1)^{\bar{x}} Z_I \otimes Z_S). \tag{4.10}$$

In the appendix, we show that this conventional entanglement witness can also be measured in a single run-through measurement of the spin magnetizations, if we assume the ability of implementing any form of unitary transformations. Nevertheless, the new scheme introduced in this work still has an advantage that there is no need to change the experimental operations for different choices of zx. On the other hand, the conventional entanglement witness requires a somewhat complicated pre-applied unitary transformation, which moreover depends on the choices of z and x.

5. Conclusion

NMR with very low nuclear spin polarizations prohibits the existence of entanglement. Although two-bit information is correctly detected in a NMR SDC experiment irrespective of polarization, it can be merely due to a statistical effect in an ensemble system having a large number of molecules. For a completely reliable demonstration of NMR SDC, spin polarization should inevitably be enhanced over a certain threshold, which has been shown to coincide with the condition for non-separability of the states. Taking advantage of these results, we have introduced a new class of entanglement witnesses suitable particularly for NMR experiments, which is straightforwardly measurable in a single run experiment and is generally applicable to every Bell diagonal state. Despite that detection of entanglement through the conventional entanglement witness is also possible in a single NMR experiment, it requires pre-application of a complicated unitary transformation that depends on the choice of the two-bit message.

Acknowledgments

RR and MK are grateful to Dr Fumiaki Morikoshi for helpful discussions. RR would like to thank Akira SaiToh for contributions to the appendix. This work has been supported by CREST of Japan Science and Technology Agency.

Appendix. Single run detection of the conventional entanglement witness

Here we show that the conventional entanglement witness is measurable in a single NMR experiment by applying an appropriate unitary transformation that depends on the choices of z and x prior to the measurement of the spin magnetizations. Suppose that we have an observable $\tilde{W} = U^\dagger \tilde{W}_o U = U^\dagger(aZ_I \otimes I_S + bI_I \otimes Z_S + cI_I \otimes I_S)U$ with coefficients $a, b, c \in \mathbf{R}$ and a unitary transformation $U \in U(4)$. The problem here is to find a set of a, b, c and U such that

$$\operatorname{Tr} \rho_2 \tilde{W} = \operatorname{Tr} \rho_2 W \tag{A.1}$$

for each of the four possible messages zx, where W is the conventional entanglement witness given in (4.10).

Here we deal with the case of $z = x = 0$, in which the entanglement witness W is

$$W = \tfrac{1}{4}(I_I \otimes I_S - X_I \otimes X_S + Y_I \otimes Y_S - Z_I \otimes Z_S). \tag{A.2}$$

We require (A.1) to hold for any p_I and p_S. By considering the case $p_I = p_S = 1/2$ (the maximally mixed state), we immediately obtain $c = 1/4$ from

$$\operatorname{Tr} \rho_2 W = \tfrac{1}{4}, \qquad \operatorname{Tr} \rho_2 \tilde{W} = \operatorname{Tr} U\rho_2 U^\dagger \tilde{W}_o = c. \tag{A.3}$$

Now we re-formulate problem (A.1) using $\rho_2 = \rho_1$ ($z = x = 0$) and $\rho_1 = U_{\text{ent}}\rho_0 U_{\text{ent}}^\dagger$ into

$$\operatorname{Tr} \rho_1 (W' - V^\dagger \tilde{W}_o V) = 0, \tag{A.4}$$

where $V = UU_{\text{ent}}$ and $W' = U_{\text{ent}}^\dagger W U_{\text{ent}}$. Since ρ_0 is a diagonal matrix, the diagonal elements of $W' - V^\dagger \tilde{W}_o V$ ought to be zero, and have the following form:

$$W' - V^\dagger \tilde{W}_o V = \begin{pmatrix} 0 & a_{01} & a_{02} & a_{03} \\ a_{01}^* & 0 & a_{12} & a_{13} \\ a_{02}^* & a_{12}^* & 0 & a_{23} \\ a_{03}^* & a_{13}^* & a_{23}^* & 0 \end{pmatrix}. \tag{A.5}$$

Using $W' = \operatorname{diag}\left(-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$ and $\tilde{W}_o = \operatorname{diag}(a+b, a-b, -a+b, -a-b) + \frac{1}{4}(I_I \otimes I_S)$, we obtain

$$\begin{pmatrix} -\frac{3}{4} & -a_{01} & -a_{02} & -a_{03} \\ -a_{01}^* & \frac{1}{4} & -a_{12} & -a_{13} \\ -a_{02}^* & -a_{12}^* & \frac{1}{4} & -a_{23} \\ -a_{03}^* & -a_{13}^* & -a_{23}^* & \frac{1}{4} \end{pmatrix} = V^\dagger \begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & -\beta & 0 \\ 0 & 0 & 0 & -\alpha \end{pmatrix} V, \tag{A.6}$$

where $\alpha = a + b$ and $\beta = a - b$. This leads to

$$\alpha|V_{0i}|^2 + \beta|V_{1i}|^2 - \beta|V_{2i}|^2 - \alpha|V_{3i}|^2 = h_i, \tag{A.7}$$

where $h_0 = -3/4$, and $h_1 = h_2 = h_3 = 1/4$. The unitarity of V also requires

$$|V_{0i}|^2 + |V_{1i}|^2 + |V_{2i}|^2 + |V_{3i}|^2 = 1. \tag{A.8}$$

An example of the set that satisfies (A.7) and (A.8) suffices for the proof. We put, e.g., $\alpha = 3/4$ and $\beta = 0$ and get

$$V = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & \mathrm{e}^{\mathrm{i}\pi 2/3} & \mathrm{e}^{-\mathrm{i}\pi 2/3} \\ 0 & 1 & \mathrm{e}^{-\mathrm{i}\pi 2/3} & \mathrm{e}^{\mathrm{i}\pi 2/3} \\ 0 & 1 & 1 & 1 \\ \sqrt{3} & 0 & 0 & 0 \end{pmatrix}. \tag{A.9}$$

It is also possible to prove in a quite similar manner that there exists a set of a, b, c and U that satisfies (A.1) for any other choice than $z = x = 0$. For general zx, only h_i in (A.7) is needed to be modified as $h_{x+2z} = 3/4$ and other $=1/4$. We note, however, that different sets of a, b, c and U are required for different choices of z and x, in contrast to the new entanglement witness proposed in the present work, which covers every possible message zx. For instance, from (A.7) we obtain for $z = x = 0$ and $i = 0$

$$\alpha|V_{00}|^2 + \beta|V_{10}|^2 - \beta|V_{20}|^2 - \alpha|V_{30}|^2 = -\tfrac{3}{4}, \tag{A.10}$$

which is satisfied by the set given in (A.9). However, this set of α and β cannot fulfil the requirement for, e.g., $x \neq z = 1$ and $i = 0$ that

$$\alpha|V_{00}|^2 + \beta|V_{10}|^2 - \beta|V_{20}|^2 - \alpha|V_{30}|^2 = \tfrac{1}{4}. \tag{A.11}$$

References

[1] Ernst R R, Bodenhausen G and Wokaun A 1994 *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Oxford: Oxford University Press)
[2] Vandersypen L M K, Steffen M, Breyta G, Yannoni C S, Sherwood M H and Chuang I L 2001 *Nature* **414** 883
[3] Fang X, Zhu X, Feng M, Mao X and Du F 2000 *Phys. Rev.* A **61** 022307
[4] Nielsen M A, Knill E and Laflamme R 1998 *Nature* **396** 52
[5] Ekert A and Jozsa R 1998 *Phil. Trans. R. Soc.* A **356** 1769
[6] Linden N and Popescu S 2001 *Phys. Rev. Lett.* **87** 047901
[7] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[8] Zyczkowski K, Horodecki P, Sanpera A and Lewenstein M 1998 *Phys. Rev.* A **58** 883
[9] Braunstein S L, Caves S M, Jozsa R, Linden N, Popescu S and Schack R 1999 *Phys. Rev. Lett.* **83** 1054
[10] Terhal B M and Horodecki P 2000 *Phys. Rev.* A **61** 040301
[11] Lewenstein M, Kraus S B, Cirac J I and Horodecki P 2000 *Phys. Rev.* A **62** 052310
[12] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[13] Feller W 1968 *An Introduction to Probability Theory and its Applications* (New York: Wiley)
[14] Nyquist H 1928 *Phys. Rev.* **32** 110
[15] Peres A 1996 *Phys. Rev. Lett.* **77** 1413
[16] Horodecki H, Horodecki P and Horodecki R 1996 *Phys. Lett.* A **223** 1