Measuring Quantum Entanglement without Prior State Reconstruction

Paweł Horodecki

Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-952 Gdańsk, Poland
(Received 19 March 2002; revised manuscript received 3 October 2002; published 22 April 2003)

It is shown that, despite strong nonlinearity, entanglement of formation of a two-qubit state can be measured without prior state reconstruction. Collective measurements on a small number of copies are provided that allow one to determine quantum concurrence via estimation of only *four* parameters. It is also pointed out that another entanglement measure based on so-called "negativity" can also be measured in a similar way. The result is related to the general problem: What kind of information can be extracted efficiently from an unknown quantum state?

Two-qubit state entanglement is well characterized. It is the only case where an analytical formula for the entanglement of formation E_f [1] has been provided with the help of so-called concurrence (see [2] for review). Simple necessary and sufficient conditions for the presence of entanglement in a two-qubit state are known [3,4], which involve the so-called positive partial transpose (PPT) map. However, the question is how to detect the presence of entanglement in an *unknown* state efficiently, i.e., with a minimal number of estimated parameters. The problem was that the PPT test is represented by a nonphysical operation. On the other hand, concurrence and entanglement of formation are complicated nonlinear functions. One might expect that they require full prior state reconstruction in general. The same might be expected to hold for any other entanglement measures [5,6] (see also [7]). Indeed direct detection of entanglement of formation [8,9] has succeeded only for pure two-qubit states and relied on a very special property of the function in that case. Even then, however, the procedure requires the estimation of more than one observable [8].

Quite recently, using a formula of the best structural physical approximation of Hermitian nonphysical maps [10], it has been shown [11] how to detect violation of the PPT separability test (or any positive map separability test) experimentally without *any* prior knowledge about the quantum state (for the analysis of the interferometric scheme, see [12]; cf. [13]).

In this work we provide a protocol detecting the concurrence of a given unknown state by the estimation of four parameters in collective measurements of a small (not more than eight) number of copies. We also point out how to estimate the computable entanglement measure [6] based on negativity [6,14] in a similar way. This gives quadratic gain in a number of parameters if compared to quantum tomography. The corresponding protocol can be generalized to any $d \otimes d'$ system. We discuss both presented protocols as far as the number of involved copies are concerned. In particular, to estimate two-qubit entanglement of formation one needs a slightly greater number of copies than in the state reconstruction scheme. It is, however, different for computable measure where both the number of estimated parameters and the number of involved copies are less than what state reconstruction requires. Subsequently we describe the protocols and conclude with some discussion.

Measuring two-qubit entanglement of formation.— Let us start with a general formula for the entanglement of formation E_f of a given bipartite state ϱ [1]: $E_f(\varrho) = \min_{\{p_i,\psi_i\}} \sum_i p_i S(\mathrm{Tr}_A(|\psi_i\rangle\langle\psi_i|))$ where $S(\sigma) = -\mathrm{Tr}(\sigma \log_2 \sigma)$ is the von Neumann entropy of state σ (counted in bits) and the minimum is taken over all ensembles $\{p_i, \psi_i\}$ such that $\sum_i p_i |\psi_i\rangle\langle\psi_i| = \varrho$. It has been shown that for two qubits entanglement of formation amounts to [2]

$$E_f(\varrho) = h\left(\frac{1 + \sqrt{1 - C(\varrho)^2}}{2}\right), \qquad (1)$$

where $h(x) \equiv -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon binary information. An important state function called concurrence [2],

$$C(\varrho) = \max[\sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}, 0], \qquad (2)$$

involves four real monotonically decreasing numbers $\{\lambda_i\}$ which are eigenvalues of the (non-Hermitian) matrix $\varrho\tilde\varrho$ with

$$\tilde\varrho = \Sigma \varrho^* \Sigma, \qquad \Sigma = \sigma_y \otimes \sigma_y, \qquad (3)$$

where Pauli matrices act on Alice and Bob qubits, respectively (recall that ϱ is a two-qubit state) and the asterisk stands for a complex conjugate. Obviously neither C nor E_f is measurable in the usual quantum mechanical sense; i.e., neither of them is an observable. This follows from the very fundamental laws of quantum mechanics: both functions are nonlinear in state parameters while only *linear* operations can be performed on a single copy. Still one can try to *estimate* them in another way—involving access to several copies. Such an approach succeeded for pure two-qubit states [9] based, however, on a very special property of a pure state, i.e., the dependence of its entanglement on eigenvalues of a reduced density matrix.

We would have C and E_f determined for arbitrary given ϱ if only we knew the following numbers: $\lambda_1, \lambda_2,$

λ_3, λ_4. They come from a rather complicated nonlinear function of ϱ. Surprisingly for any unknown ϱ they can be physically measured by estimating only *four* parameters (instead of 15 describing full density matrix) if joint

$$\varrho \otimes \varrho \xrightarrow{\Lambda_1} \varrho_1 \Longrightarrow \langle M_1 \rangle = \sum_i \lambda_i, \qquad \varrho \otimes \varrho \otimes \varrho \otimes \varrho \xrightarrow{\Lambda_2} \varrho_2 \Longrightarrow \langle M_2 \rangle = \sum_i (\lambda_i)^2,$$

$$\varrho \otimes \varrho \otimes \varrho \otimes \varrho \otimes \varrho \otimes \varrho \xrightarrow{\Lambda_3} \varrho_3 \Longrightarrow \langle M_3 \rangle = \sum_i (\lambda_i)^3, \qquad \varrho \otimes \varrho \otimes \varrho \otimes \varrho \otimes \varrho \otimes \varrho \otimes \varrho \otimes \varrho \xrightarrow{\Lambda_4} \varrho_4 \Longrightarrow \langle M_4 \rangle = \sum_i (\lambda_i)^4. \quad (4)$$

According to the above, each 20 copies from a given sample of systems in state ϱ is divided into four groups consisting of two, four, six, and eight copies, respectively. Then we subject each group to some specific quantum channel (i.e., completely positive trace preserving map) Λ_k, $k = 1, 2, 3, 4$. As a result we get quantum states ϱ_k. Finally, we estimate mean values $\langle M_k \rangle \equiv \mathrm{Tr}(\varrho_k M_k)$ of four observables M_k. They represent the moments needed to reconstruct the values $\{\lambda_i\}$. Moreover, as we see below, each $\langle M_k \rangle$ can be determined via estimation of a single parameter in binary positive operator valued measure (POVM).

To see how the above scheme works we need to recall the concept of physical approximation of the PPT operation [11]. Namely the trace preserving map

$$\Lambda_{XY}(\sigma_{XY}) = \frac{d}{d^3 + 1} I_X \otimes I_Y + \frac{1}{d^3 + 1} (\sigma_{XY})^{T_Y} \quad (5)$$

is physically implementable on any bipartite $d \otimes d$ state σ_{XY} defined on $\mathcal{H}_X \otimes \mathcal{H}_Y$. Thus Λ_{XY} corresponds to what in literature is called *quantum channel*. In formula (5) I_X, I_Y stand for identity matrices corresponding to subsystem X, Y, respectively, while the operation $(\cdot)^{T_Y}$ stands for the partial transposition map [3] which simply transposes indices corresponding to the second subsystem Y. The map (5) is called a *structural physical approximation* (see [10,11]) of the partial transposition map. The latter is unphysical in the sense that it cannot be physically implemented by itself. In particular, one can define in a similar way such an approximation for the transposition map. For two qubits the latter coincides with the previously introduced universal-NOT gate (see [15]).

A detailed description of the scheme (4) is presented in two steps.

Step I. Action of channels Λ_k: We define quantum channel Λ_k as being composed of two physical operations: (i) the map (5) with $d = d_k \equiv 4^k$ and spaces $\mathcal{H}_X$ ($\mathcal{H}_Y$) describing all the copies on the odd (even) position in the kth group and (ii) the subsequent action of unitary operation Σ on each "even" copy. For instance, in the second group $\varrho \otimes \varrho \otimes \varrho \otimes \varrho$ ($k = 2$) the first and the third copy correspond to subsystem X, while the remaining two represent subsystem Y. Only copies belonging to Y will be subjected to subsequent action (ii) of unitary operation Σ.

Let the channels Λ_k act on groups of states according to the scheme (4). As a result we get the following four states:

measurements are available. The idea of the present method is to find (in collective quantum measurements) four "moments" that allow us to reconstruct λ's and, consequently, concurrence completely. The scheme of the corresponding protocol is very simple:

$$\varrho_k = \frac{d_k}{d_k^3 + 1} I_X \otimes I_Y + \frac{1}{d_k^3 + 1} (\varrho \otimes \tilde{\varrho})^{\otimes k},$$
$$k = 1, \dots, 4. \quad (6)$$

Up to the maximal noise part, the above states can be considered as "proportional" to the matrices $(\varrho \otimes \tilde{\varrho})^{\otimes k}$. In fact, they differ from the matrices by a shrinking factor $\frac{1}{d_k^3 + 1}$ at the "Bloch vector." This property is similar to what happens in the theory of approximate cloning or in the case of universal-NOT gate [15].

Step II. Measurement of moments $\langle M_k \rangle$: There is a method [10,12] that allows one to measure spectrum state estimation with the help of observables constructed from shift operators V_n [16]. They have the property

$$\mathrm{Tr}(V_{(n)} A_1 \otimes \dots \otimes A_n) = \mathrm{Tr}(A_1 A_2 \dots A_n). \quad (7)$$

Combining the above property with the fact that all moments $\sum_i (\lambda_i)^k$ are real, one can see that the latter are mean values of the following observables:

$$M_k = \frac{d_k^3 + 1}{2} (V_{(2k)} + V_{(2k)}^\dagger) - d_k^3 I, \quad (8)$$

when each of them is calculated on state ϱ_k [see scheme (4)]. Finally, the numbers λ_k can be inferred uniquely from the moments. This can be shown in a similar way by using the techniques of Ref. [10].

Now an important point is that each mean $\langle M_k \rangle$ can be detected (up to rescaling) as *a single parameter* in special binary POVM [17]: following Ref. [12] each observable M_k can be encoded into some ancilla and then its mean value can be reproduced from the measurement of the elementary binary observable (Pauli matrix σ_z) (see [18] for modified binary POVM with minimal single-qubit ancilla). This concludes the description of the protocol.

The presented method is parametrically efficient: it requires fewer parameters to be measured than state reconstruction does (4 instead of 15). It is not so as long as the number of copies is concerned: one "round" of quantum tomography requires 15 copies while here [see (4)] we require $2 + 4 + 6 + 8 = 20$ copies in each round of the protocol. However, the factor $r = r_p r_c \equiv$ "number of parameters $\times$ number of copies" is here less ($r = 80$) than for the state reconstruction schemes ($r = 165$). Even more striking is the fact that while the number of copies consumed in one round of the experiment

is increased only by 33% (from 15 to 20), the number of parameters is decreased almost 4 times (from 15 to 4). It suggests that an optimal method of entanglement estimation should exist that consumes the same number of copies as state reconstruction but requires a lesser number of parameters (5 or 6). Note that the present method is useful when we are allowed to use a small number of apparatuses with *fixed* architecture. One can also anticipate the existence of a tradeoff between r_p and r_c involved in the estimation of any entanglement measure. Optimization of the tradeoff is an interesting open problem.

Note that above we have asked the question: "How much entanglement is in the system?" Our measurement protocol allows one to find an answer to this question. Of course, the protocol solves also a less detailed problem: "Is there any entanglement in the system at all"? One can, however, discern the two questions above and consider the scenario when the observer knows that two-qubit entanglement is present in the system but has no idea "how much." Below we provide a protocol for such a scenario based on the fact [19] that if the $2 \otimes 2$ state ϱ is entangled, then the smallest eigenvalue of the matrix $\gamma \equiv \Sigma \varrho^{T_A} \Sigma \varrho^{T_B}$ is proportional to $\frac{C(\varrho)^2}{4}$. The modified protocol must involve the map (5) (with transposed subsystems suitably permuted) to produce the new states γ'_k with Bloch vector proportional to $(\Sigma \varrho^{T_A} \otimes \varrho^{T_B})^{\otimes k}$ (here they play the same role as states ϱ_k in *Step I*). Then one should estimate eigenvalues of γ_k in the same way as in Step II and infer $C(\varrho)$ following the result of Ref. [19]. The above protocol answers the quantitative (how much) question provided that observers have qualitative information that there exists entanglement in the system. To get the information one can use a physical application of the PPT test [11]. Because of its binary character (possible "yes-no" answer) it requires *less* measurement effort than the quantitative stage described above. We can use this fact to minimize measurement effort: if the PPT test does not reveal any entanglement, we just abandon the second stage.

Multilevel systems and computable entanglement measure.—For general bipartite $d \otimes d$ systems (they can be called multilevel systems) there is no analytical formula for entanglement of formation. However, at least one nontrivial entanglement measure can be calculated analytically. This is the so-called "computable entanglement measure" [6], cf. [20]

$$E_c(\varrho) = \log_2 \|\varrho^{T_B}\|, \qquad (9)$$

where $\| \cdot \|$ stands for trace norm which for the Hermitian operator amounts to the sum of moduli of its eigenvalues. In particular, the quantity $(\|\varrho^{T_B}\| - 1)$ is introduced to quantify entanglement [14] and after normalization $N = (\|\varrho^{T_B}\| - 1)/2$ called *negativity* has been shown [6] to be *entanglement monotone* [21]. The measure (9) is weaker than entanglement of formation; it "detects," however, all free, i.e., distillable, entanglement of bipartite systems.

167901-3

To estimate the measure we must experimentally determine the following quantity:

$$\|\varrho^{T_B}\| = \sum_i |\lambda'_i|, \qquad (10)$$

where $\{\lambda'_i\}$ are eigenvalues of the partially transposed state ϱ^{T_B}. The above formula is crucial for subsequent analysis.

We now apply the scheme of Ref. [11] making, however, full use of its output rather than focusing on its minimal eigenvalue. For any bipartite $d \otimes d$ state ϱ the scheme consists of application of the map (5) which leads to a new quantum state $\varrho_1 = \Lambda_{AB}(\varrho)$ with eigenvalues $\{\lambda_i\}$. They are related to eigenvalues λ'_i by the following affine function:

$$\lambda_i = \frac{d}{d^3 + 1} + \frac{1}{d^3 + 1} \lambda'_i. \qquad (11)$$

The key point is that $\{\lambda_i\}$ *can be determined* experimentally via measurement of $r_p = d^2 - 1$ observables (see [10–12]). It is *much less* than $d^4 - 1$ required for quantum tomography. Having λ_i's one can calculate all the parameters $\lambda'_i = (d^3 + 1)\lambda_i - d$ and substitute them to the formula (9) which provides the value of the corresponding measure.

It is interesting that in the present scenario one has also gained in the number of copies involved. Indeed we have $r_c = 2 + 3 + \ldots + d^2 = (d^4 + d^2 - 2)/2$ instead of $r_c = d^4 - 1$.

The whole scenario can be immediately generalized to any $d \otimes d'$ system with $d \neq d'$. Only the parameters in (5) will change slightly. They can be easily calculated with help of the structural approximation formula [10].

Discussion.—In conclusion we have provided the first nontrivial protocols of entanglement estimation that require no prior knowledge about the states. The first presented protocol allows one to detect two-qubit entanglement of formation with the help of joint measurements on a small number of systems. In one round the method requires 33% of copies more than state reconstruction (20 instead of 15). However, it needs *almost 4 times less* parameters (4 instead of 15) than quantum tomography does. We have also shown how to estimate the experimentally computable measure of entanglement E_c based on the partial transpose operation. We have pointed out how the protocol from Ref. [11] allows one to determine E_c with the help of the estimation of only $d^2 - 1$ parameters instead of $d^4 - 1$ ones required by all state reconstruction procedures. The scheme provides also a gain in the number of copies consumed: $r_c = (d^4 + d^2 - 2)/2$ instead of $r_c = d^4 - 1$ due to state reconstruction schemes.

It would be interesting to find a similar protocol determining some parameters of the best separable approximation of two-qubit quantum states (for instance, the entangled part of the Lewenstein-Sanpera decomposition [22]). It involves the question of how to find

167901-3

experimentally the eigenvector corresponding to the least negative eigenvalue of partially transposed density matrix ϱ^{T_Y}. To get the eigenvector with minimal measurement cost would be particularly interesting because it plays a crucial role in the only universal protocol of two-qubit entanglement distillation [23]. In the above context basic questions naturally arise: (i) Is it possible to estimate the eigenvector corresponding to the extreme eigenvalue of a given density matrix without prior reconstruction of the latter? (ii) If so, how efficiently can it be done? Any possible solution for these problems must take into account the fundamental restrictions on quantum "nonlinear operations" [10,24].

The present results naturally lead also to another interesting question: Is it possible to estimate efficiently other entanglement measures (such as relative entropy of entanglement [25]) or, more generally, correlation measures (such as the one from Ref. [26]) based on von Neumann entropy? For pure states the answer is positive as all the measures are equivalent to the entropy of the reduced density matrices which at the same time is proportional to the index of correlation $I = S_A + S_B - S_{AB}$. For mixed states the latter serves rather as a measure of global (quantum + classical) correlations [26]. Following the present analysis I can be efficiently measured without state reconstruction in general. The present method cannot be generalized to relative entropy of entanglement or distillable entanglement until analytical (or partially analytical) formulas for those measures are known.

Furthermore, from the point of view of general quantum information theory, a very important problem follows: *What kind of information (whatever it means) can be extracted from an unknown quantum state at a small measurement cost?* Here we have considered extraction of information represented by a single parameter (entanglement measure). It is closely related to the following problem: *What kind of measurement information can be extracted from the state in the protocols destroying as little quantum information as possible?* Indeed measurement of a small number of parameters can always be interpreted as an incomplete von Neumann measurement which destroys quantum information less than a complete measurement does. An illustrative example is a detection of spectrum without state reconstruction via Young diagram projections proposed in Ref. [27] (for alternative spectrum detection, see [12]). The above issues are crucial for some quite fundamental processes such as universal quantum compression. For example, it has been shown [28] that the quantum source can be compressed efficiently only if one knows the *single* parameter represented by von Neumann entropy of the source. The entropy can be estimated *without prior knowledge* about a state: measurement effort (see [12]; cf. [27]) is the same as in the present protocol estimating measure E_c. Finally, we have considered one of the basic problems in general entanglement theory: "How can one detect the amount of entanglement experimentally?" This question concerns

not only entanglement itself: any answer relates to the properties of information contained in unknown quantum states.

[1] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[2] W. K. Wootters, Quant. Inf. Comp. **1**, 27 (2001).
[3] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[4] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[5] V. Vedral and M. Plenio, Phys. Rev. A **57**, 1619 (1998).
[6] R. F. Werner and G. Vidal, Phys. Rev. A **65**, 032314 (2002).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).
[8] J. M. G. Sancho and S. F. Huelga, Phys. Rev. A **61**, 042303 (2000).
[9] A. Acin, R. Tarrach, and G. Vidal, Phys. Rev. A **61**, 062307 (2000). The main result generalizes to any $d \otimes d'$ pure state via spectrum estimation of one local density matrix (taking a subsystem with smaller d is more efficient).
[10] P. Horodecki, quant-ph/0111036.
[11] P. Horodecki and A. Ekert, Phys. Rev. Lett. **89**, 127902 (2002).
[12] A. K. Ekert, C. M. Alves, D. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, Phys. Rev. Lett. **88**, 217901 (2002).
[13] R. Filip, Phys. Rev. A **65**, 062320 (2002).
[14] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 833 (1998).
[15] V. Buzek, M. Hillery, and R. F. Werner, Phys. Rev. A, **60**, 2626 (1999); V. Buzek, M. Hillery, and R. F. Werner, J. Mod. Opt. **47**, 211 (2000).
[16] Shift on $(C^m)^{\otimes n}$ is defined as follows: $V_{(n)} e_1 \otimes e_2 \otimes \ldots \otimes e_n = e_n \otimes e_1 \otimes \ldots \otimes e_{n-1}$ for any basis vectors $\{e_l\}$.
[17] Alternatively $\langle M_k \rangle$ can be expressed in terms of "mean" of V_k and, as such, determined interferometrically [12].
[18] P. Horodecki, quant-ph/0210163 [Phys. Rev. A (to be published)].
[19] T. Wellens and M. Kuś, Phys. Rev. A **64**, 052302 (2001).
[20] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).
[21] G. Vidal, J. Mod. Opt. **47**, 35 (2000).
[22] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
[23] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[24] J. Fiurasek, quant-ph/0111107.
[25] V. Vedral and M. Plenio, Phys. Rev. A **57**, 1619 (1998).
[26] B. M. Terhal, M. Horodecki, D. W. Leung, and D. P. DiVincenzo, quant-ph/0202044.
[27] M. Keyl and R. F. Werner, Phys. Rev. A **64**, 052311 (2001).
[28] R. Jozsa, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **81**, 1714 (1998).