00 - 130

PHYSICAL REVIEW A, VOLUME 64, 010101(R)

Local filtering operations on two qubits

Frank Verstraete,* Jeroen Dehaene,† and Bart DeMoor‡
Research Group SISTA, Department of Electrical Engineering, Katholieke Universiteit Leuven, Kardinaal Mercierlaan 94, B-3001 Leuven, Belgium
(Received 28 November 2000; published 5 June 2001)

We consider one single copy of a mixed state of two qubits and investigate how its entanglement changes under local quantum operations and classical communications (LQCC) of the type $\rho' \sim (A\otimes B)\rho(A\otimes B)^\dagger$. We consider a real matrix parametrization of the set of density matrices and show that these LQCC operations correspond to left and right multiplication by a Lorentz matrix, followed by normalization. A constructive way of bringing this matrix into a normal form is derived. This allows us to calculate explicitly the optimal local filtering operations for concentrating entanglement. Furthermore, we give a complete characterization of the mixed states that can be purified arbitrarily close to a Bell state. Finally, we obtain a new way of calculating the entanglement of formation.

DOI: 10.1103/PhysRevA.64.010101 PACS number(s): 03.65.Ud, 03.67.−a, 89.70.+c

Entanglement of two separated quantum systems implies that there are nonlocal correlations between them. This feature of nonlocality has found practical applications in quantum information theory (see, for example, Ref. [1]). Most applications require that both parties share maximally entangled states. A realistic preparation and transmission of entangled states, however, yields mixed states. Therefore, Bennett *et al.* [2], proposed a protocol that allows one to obtain asymptotically a nonzero number of maximally entangled pure states by carrying out collective measurements on a large number of copies of entangled mixed states. Their scheme, however, required that the fidelity of the mixed states exceed 1/2. The Horodeckis subsequently showed how mixed states of arbitrary fidelity could be purified by first applying a filtering operation to each copy separately [3]. Linden *et al.* [4] then asked whether it is possible to obtain singlets out of mixed states by allowing only local operations on each copy separately. While this is possible for pure states, they proved that this is impossible in general for mixed states [4,5], as the best state one can obtain is a Bell-diagonal state [6]. The Horodeckis, however, gave an example of a mixed state that could be purified arbitrarily close to a singlet state through a process called quasidistillation [7].

We shed light on those results by observing that filtering operations on two qubits correspond to Lorentz transformations on a real parametrization of their density matrix. Using Lorentz transformations, this real parametrization can be brought into one of two types of normal forms, thus giving a characterization of all states that can be transformed into each other by local operations. Our scheme also yields a way of calculating the entanglement of formation [8], with as a by-product a simple proof of the necessity and sufficiency of the partial transpose criterion of Peres [9,10]. The main result of this Rapid Communication, however, is the fact that we provide a constructive way of finding the optimal positive operator valued measure (POVM) for concentrating the entanglement. We show that there exist two classes of states corresponding to the two normal forms: those that can be brought into Bell diagonal form leaving the rank of the density matrix constant, and those that can asymptotically be brought into Bell diagonal form with lower rank. This last class contains a subclass of mixed states that can be purified arbitrarily close to the singlet state.

In this paper we will consider the filtering operations

$$\rho' = \frac{(A\otimes B)\rho(A\otimes B)^\dagger}{\mathrm{Tr}[(A\otimes B)\rho(A\otimes B)^\dagger]}, \tag{1}$$

where $A^\dagger A \leq I_2, B^\dagger B \leq I_2$. Since a local projective measurement destroys all entanglement, we will only consider the cases $\det(A)\neq 0$ and $\det(B)\neq 0$. Let us now calculate how the entanglement of formation (EoF) changes under these local operations. The EoF of a two qubit system can be calculated as a convex monotonically increasing function of the concurrence [8]. As shown in Ref. [11], the concurrence of ρ is given by $\max(0,\tau_1-\tau_2-\tau_3-\tau_4)$ with $\{\tau_i\}$ the singular values of $X^T(\sigma_y\otimes\sigma_y)X$ with $\rho = XX^\dagger$. Under the filtering operations we have $X' = (A\otimes B)X/\sqrt{\mathrm{Tr}(A^\dagger A\otimes B^\dagger B\rho)}$. Since $(A\otimes B)^T(\sigma_y\otimes\sigma_y)(A\otimes B) = \det(A)\det(B)(\sigma_y\otimes\sigma_y)$, this proves the following theorem.

Theorem 1. Under the filtering operations (1), the concurrence changes as

$$C' = C\frac{|\det(A)||\det(B)|}{\mathrm{Tr}(A^\dagger A\otimes B^\dagger B\rho)}. \tag{2}$$

It will turn out to be very useful to introduce the real and linear parametrization of the density matrix [12]

$$\rho = \frac{1}{4}\sum_{i,j} R_{ij}\sigma_i\otimes\sigma_j, \tag{3}$$

where the summation extends from 0 to 3 and with σ_0 the 2×2 identity matrix and $\sigma_1,\sigma_2,\sigma_3$ the Pauli spin matrices.

*Email address: frank.verstraete@esat.kuleuven.ac.be
†Email address: jeroen.dehaene@esat.kuleuven.ac.be
‡Email address: bart.demoor@esat.kuleuven.ac.be

Below we will often leave out the normalization of ρ and R. Note that normalization of R is very simple since $R_{0,0}=\mathrm{Tr}(\rho)$.

We will now prove how R transforms under the LQCC operations (1).

Theorem 2. The 4×4 *matrix* R *with elements* $R_{ij}=\mathrm{Tr}(\rho(\sigma_i\otimes\sigma_j))$ *transforms, up to normalization, under LQCC operations (1)* as

$$R'=L_A R L_B^T, \tag{4}$$

where L_A *and* L_B *are proper orthochronous Lorentz transformations given by*

$$L_A=T(A\otimes A^*)T^\dagger/|\det(A)|, \tag{5}$$

$$L_B=T(B\otimes B^*)T^\dagger/|\det(B)|, \tag{6}$$

$$T=\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&1\\0&1&1&0\\0&i&-i&0\\1&0&0&-1\end{pmatrix}. \tag{7}$$

This theorem can be proven by introducing the matrix $\tilde{\rho}_{kl,k'l'}=\rho_{kk',ll'}$ and noting that $R=4T\tilde{\rho}T^T$. It is easy to check that under the LQCC operations (1) $\tilde{\rho}$ transforms as $\tilde{\rho}'=(A\otimes A^*)\tilde{\rho}(B\otimes B^*)^T$, where the notation A^* is used to denote the elementwise complex conjugate. Therefore, R transforms as $R'=L_A R L_B^T|\det(A)||\det(B)|$ with $L_A=T(A\otimes A^*)T^\dagger/|\det(A)|$, $L_B=T(B\otimes B^*)T^\dagger/|\det(B)|$. Using the identities $A\sigma_y A^T=\det(A)\sigma_y$ and $T^\dagger M T^*=-\sigma_y\otimes\sigma_y$ with M the matrix associated with the Lorentz metric $M=\mathrm{diag}[1,-1,-1,-1]$, it is easily checked that $L_A M L_A^T=M=L_B M L_B^T$. Furthermore, the determinant of L_A and L_B is equal to $+1$, and the (0,0) element of L is positive, which completes the proof.

As the complex 2×2 matrices with determinant one indeed form the spinor representation of the Lorentz group, there is a 1-to-2 correspondence between each L_A and $A/\sqrt{\det(A)}$. It is interesting to note that when both A and B are unitary, the theorem reduces to the well known fact [12] that the rows and columns of R transform under $SO(3)$, which is indeed a subgroup of the Lorentz group.

With the above theorem in mind, a natural aim is to find a decomposition of R as $R=L_1\Sigma L_2^T$ with Σ diagonal and L_1,L_2 proper orthochronous Lorentz transformations. This would be the analog of a singular value decomposition, but now in the Lorentz instead of the Euclidean metric.

Theorem 3. The 4×4 *matrix* R *with elements* $R_{ij}=\mathrm{Tr}(\rho\,\sigma_i\otimes\sigma_j)$ *can be decomposed as*

$$R=L_1\Sigma L_2^T, \tag{8}$$

with L_1,L_2 *proper orthochronous Lorentz transformations, and* Σ *either of diagonal form* $\Sigma=\mathrm{diag}[s_0,s_1,s_2,s_3]$ with $s_0\geqslant s_1\geqslant s_2\geqslant|s_3|$, *or of the form*

$$\Sigma=\begin{pmatrix}a&0&0&b\\0&d&0&0\\0&0&-d&0\\c&0&0&a+c-b\end{pmatrix}, \tag{9}$$

with a,b,c,d real.

The proof of this theorem is quite technical. It heavily depends on results of matrix decompositions in spaces with indefinite metric [13]. We first introduce the matrix $C=MRMR^T$, which is M self-adjoint, i.e., $MC=C^TM$. Using theorem (5.3) in Ref. [13], it follows that there exist matrices X and J with $C=X^{-1}JX$, J consisting of a direct sum of real Jordan blocks and $XMX^T=N_J$ with N_J a direct sum of symmetric $n\times n$ matrices of the form $[S_{ij}]=\pm[\delta_{i+j,n+1}]$, with n the size of the corresponding Jordan block. Using Sylvester's law of inertia, there exists orthogonal O_J such that $N_J=O_J^TMO_J$. It is then easy to check that $O_JX=L_1^T$ is a Lorentz transformation. Therefore, the relations $C=MRMR^T=ML_1MO_JJO_J^TL_1^T$ hold. Left multiplying by M, Sylvester's law of inertia implies that there exists a matrix Σ with the same rank as J such that $MO_JJO_J^T=\Sigma M\Sigma^T$. Therefore, we have the relation $RMR^T=L_1\Sigma M\Sigma^TL_1^T$. If R has the same rank as RMR^T, this relation implies that there exists a Lorentz transformation L_2 such that $R=L_1\Sigma L_2^T$.

Let us now investigate the possible forms of Σ. Since $N_J=O_J^TMO_J$ has the signature $(+---)$, J can only be a direct sum of the following form: four 1×1 blocks; one orthogonal 2×2 block and two 1×1 blocks; one 2×2 Jordan block and two 1×1 blocks; one 3×3 Jordan block and one 1×1 block. Noting the eigenvalues of C as $\{\lambda_i\}$, it is easy to verify that a "square root" Σ in the four cases is respectively given by

(1) $\Sigma=\mathrm{diag}[\sqrt{|\lambda_0|},\sqrt{|\lambda_1|},\sqrt{|\lambda_2|},\sqrt{|\lambda_3|}]P$ with P a permutation matrix permutating the first column with one other column;

$$(2)\quad \Sigma=\mathrm{diag}\left[\sqrt{|\lambda_0|}\begin{pmatrix}\cos(\phi)&\sin(\phi)\\\sin(\phi)&-\cos(\phi)\end{pmatrix},\sqrt{|\lambda_2|},\sqrt{|\lambda_3|}\right];$$

$$(3)\quad \Sigma=\mathrm{diag}\left[\begin{pmatrix}a&b\\c&a+c-b\end{pmatrix},\sqrt{|\lambda_2|},\sqrt{|\lambda_3|}\right];$$

$$(4)\quad \Sigma=\mathrm{diag}\left[\begin{pmatrix}a&0&0\\b&\sqrt{a^2+b^2}&0\\0&\dfrac{-ab}{\sqrt{a^2+b^2}}&\dfrac{a^2}{\sqrt{a^2+b^2}}\end{pmatrix},\sqrt{|\lambda_3|}\right]$$

with $a=\sqrt{|\lambda_0|}$ and $b=-1/\sqrt{2|\lambda_0|}$.

Now we return to the relation $R=L_1\Sigma L_2^T$. L_1 and L_2 can be made proper and orthochronous by absorbing factors -1 into the rows and columns of Σ, yielding Σ'. Theorem 2 now implies that this Σ' corresponds to an unnormalized physical state, which means that ρ' corresponding to Σ' has no negative eigenvalues. It is easy to show that this requirement excludes cases 2 and 4 of the possible forms of Σ. The third case corresponds to Eq. (9). Furthermore, in the first case the permutation matrix has to be the identity and $|\lambda_0| \geqslant \max(|\lambda_1|,|\lambda_2|,|\lambda_3|)$. Multiplying by proper orthochronous Lorentz transformations, the elements $\{s_i\}$ of this diagonal Σ can always be ordered as $s_0 \geqslant s_1 \geqslant s_2 \geqslant |s_3|$.

The case where the rank of C is lower than the rank of R still has to be considered. This is only possible if the row-space of R has an isotropic subspace Q for which $QMQ^T = 0$. Some straightforward calculations reveal that the only physical states for which this holds have normal form (9) with $a=b=c$ and $d=0$ or $a=b$ and $c=d=0$. This completes the proof.

The two normal forms can be computed very efficiently by calculating the Jordan canonical decomposition of $C = MRMR^T$ and of $C' = MR^T MR$. It is easy indeed to show that, for example, in the case of diagonalizable R, the eigenvectors of C form a Lorentz matrix and $|s_i| = \sqrt{\lambda_i(C)}$. Note that we always order the diagonal elements such that $s_0 \geqslant s_1 \geqslant s_2 \geqslant |s_3|$.

States that are diagonal in R correspond to (unnormalized) Bell-diagonal states with ordered eigenvalues

$$\lambda_1 = (s_0 + s_1 + s_2 - s_3)/4, \tag{10}$$

$$\lambda_2 = (s_0 + s_1 - s_2 + s_3)/4, \tag{11}$$

$$\lambda_3 = (s_0 - s_1 + s_2 + s_3)/4, \tag{12}$$

$$\lambda_4 = (s_0 - s_1 - s_2 - s_3)/4, \tag{13}$$

whereas states of type (9) correspond to the rank deficient states

$$\rho = \frac{1}{2}\begin{pmatrix} a+c & 0 & 0 & d \\ 0 & 0 & 0 & 0 \\ 0 & 0 & b-c & 0 \\ d & 0 & 0 & a-b \end{pmatrix}. \tag{14}$$

For both cases it is easy to calculate the entanglement of formation analytically, respectively given by Ref. [14]

$$C = \max(0,(\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4)/(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4))$$
$$= \max(0,(-s_0 + s_1 + s_2 - s_3)/(2s_0))$$

and $C = \max(0,|d|/a)$.

Let us now consider an arbitrary state ρ with corresponding R. Combining theorems 1, 2, and 3, it follows that the concurrence of ρ is equal to the concurrence of the state corresponding to Σ multiplied by R_{00}. We have therefore proven the following theorem.

Theorem 4. Given a state ρ, and associated with this state $R = L_1 \Sigma L_2^T$, the concurrence of ρ is given by $C = max(0,(-s_0 + s_1 + s_2 - s_3)/2)$ or by $C = max(0,|d|)$ depending on the normal form Σ.

We thus have obtained a new method of calculating the entanglement of formation of a system of two qubits. Interestingly, it turns out that this characterization relates the concepts of entanglement of formation and of partial transposition (PT) [9]. Let us therefore define $R_{ij}^{PT} = \mathrm{Tr}(\rho^{PT}\sigma_i \otimes \sigma_j)$, which changes the sign of the third column of R. In the case of diagonal normal form of R, it is readily verified that the normal form of R^{PT} equals that of R except for the last element, where $s_3^{PT} = -s_3$. Retransforming Σ^{PT} to the ρ^{PT} picture, we see that the corresponding Bell-diagonal partial transposed state has minimal eigenvalue $(s_0 - s_1 - s_2 + s_3)/4$. We readily recognize the expression of the concurrence of Theorem 4 and therefore this eigenvalue is negative if and only if the concurrence exceeds 0. Moreover, we know that ρ^{PT} is related to this Bell-diagonal state by some similarity transformation $A \otimes B$, which cannot change the signature of a matrix due to the inertia law of Sylvester. In the case of normal form (9), analog reasoning shows that ρ^{PT} has a negative eigenvalue if and only if $|d| > 0$, which again is necessary and sufficient to have entanglement. This completes the proof of:

Theorem 5. Given a system of two qubits, this state is separable if and only if its partial transpose has a negative eigenvalue.

Although this result was already proven by Horodecki [10], we believe the previous derivation is of interest, since it connects the entanglement measures concurrence and negativity. Using this formalism, it indeed becomes possible to prove that the concurrence always exceeds the negativity, and it is furthermore possible to find a complete characterization of all states with maximal or minimal negativity for a given concurrence. This is important because in the two qubit case the negativity is a measure of the robustness of entanglement against noise.

Next we want to solve the problem of finding the POVM such as to have a nonzero chance to produce a new state with the highest possible entanglement. From Eq. (2), the maximum EoF is obtained with A,B minimizing the expression $\mathrm{Tr}(A^\dagger A \otimes B^\dagger B\rho)/(|\det(A)\det(B)|)$. Absorbing the factors $|\det(A)|$ and $|\det(B)|$ into A and B, it is sufficient to consider A and B with determinant 1. In the R picture, the optimization is then equal to minimizing the (0,0) element of $R = L_1 \Sigma L_2^T$ by appropriate L_A, L_B. Absorbing L_1 and L_2 into $L'_A = L_A L_1^T M$ and $L'_B = L_B L_2^T M$, this is equivalent to finding the optimal vectors l_A and l_B such that $l_a^T \Sigma l_B$ is minimized under the constrains $l_A^T M l_A = 1 = l_B^T M l_B$.

Let us first consider the case of diagonal Σ with elements $s_0 \geqslant s_1 \geqslant s_2 \geqslant |s_3|$. Parametrizing l_A as $(\sqrt{1+\|\vec{x}\|^2},\vec{x})$ and l_B as $(\sqrt{1+\|\vec{y}\|^2},\vec{y})$, the following inequalities hold: $l_A^T \Sigma l_B \geqslant s_0\sqrt{1+\|\vec{x}\|^2}\sqrt{1+\|\vec{y}\|^2} - s_1\|\vec{x}\|\|\vec{y}\| \geqslant s_0$. Therefore, the concurrence will be maximized for $\vec{x} = \vec{y} = 0$, leaving Σ in diagonal form. Collecting the previous results, it follows that if R is diagonalizable, the state with maximal concurrence that can be obtained from it by single copy LQCC operations is the one corresponding to Σ that is a Bell-diagonal state. This is in complete accord with the results of Kent *et al.* [6]. The optimal A and B are thus given by the 2×2 matrices corresponding to $L_1^T M$ and $L_2^T M$. The optimal POVM can then be obtained by dividing A and B by their largest singular value such that $A^\dagger A \leqslant 1$ and $B^\dagger B \leqslant 1$, followed by calculating the square roots $A_c=\sqrt{I_2-A^\dagger A}$ and $B_c=\sqrt{I_2-B^\dagger B}$, which are rank 1. The optimal POVM's to be performed on the two qubits are then given by $\{A,A_c\}$ and $\{B,B_c\}$, respectively. Note that the probability of measuring (A,B) is given by the inverse of the gain in concurrence divided by the product of the largest singular values of A and B, and that the rank of the Bell-diagonal state is equal to the rank of the original state. It has to be emphasized that this single copy distillation protocol is optimal. Moreover, the previous derivation gives us a complete continuous parametrization of the surfaces of constant concurrence in state space: these surfaces are generated by applying all trace-preserving Lorentz transformations to all the Bell-diagonal states with given entanglement, with as a special case the boundary between separable and entangled states.

The optimal single copy distillation protocol for states with normal form (9) still have to be derived. An analogous reasoning as in the diagonal case leads to the conclusion that l_A and l_B are vectors associated with the Lorentz transformations bringing Eq. (9) into diagonal form. This is, however, only possible in the limit where l_A and l_B contain factors $\lim_{t\to\infty}[\sqrt{1+t^2},0,0,t]$ and $\lim_{t\to\infty}[\sqrt{1+t^2},0,0,-t]$, respectively. This indeed allows one to bring R asymptotically into diagonal form with diagonal elements given by $[\sqrt{(a-b)(a+c)},d,-d,\sqrt{(a-b)(a+c)}]$ and off-diagonal elements of order $1/t^2$, yielding a state infinitesimally close to a Bell-diagonal state. The probability of getting this state during a measurement of the optimal POVM, however, scales as $\lim_{t\to\infty}1/t^2$. This is equivalent to the quasidistillation protocol by Horodecki [7]. In this limit of $t\to\infty$, the rank of the new state is less than the original one, and its concurrence is given by $|d|/\sqrt{(a-b)(a+c)}$.

In the case where $a-b=a+c=|d|$, we are therefore able to create a state arbitrarily close to the singlet state. Therefore, the only mixed states that can be quasipurified to the singlet state by single copy LQCC operations are the rank 2 states having normal form (9) with $a-b=a+c=|d|$. These states are mixtures of a Bell state with a separable pure state orthogonal to it, and are therefore of measure zero in comparison with the class of rank 2 states.

In conclusion, we obtained insight into the problem of local filtering on one copy of two qubits by introducing the notion of Lorentz transformations on a real matrix parametrization of their density matrix. This matrix can be brought into one of two types of normal forms. These normal forms contain all the information about the entanglement of formation and reveal an elementary connection between concurrence and the partial transpose criterion of Peres. Moreover, this formalism enabled us to derive in a constructive way the optimal local filtering operations for concentrating entanglement on an arbitrary mixed state of two qubits. This could be of great utility in constructing optimal distillation protocols. We showed that states of the first type can be locally transformed into a Bell-diagonal state of the same rank with finite probability, whereas states of the second kind can asymptotically be transformed into Bell diagonal states with lower rank. This last class is of special interest as is contains the mixed states that can be transformed arbitrarily close to the singlet state.

This work was supported by the Flemish government through Research Council K. U. Leuven (Concerted Research Action Mefisto-666), FWO Project Nos. G.0240.99, G.0256.97 and Research Communities ICCoS and ANMMM; and IWT projects EUREKA 2063-IMPACT, STWW; the Belgian State: through IUAP P4-02 and IUAP P4-2 and the Sustainable Mobility Programme Project No. MD/01/24; the European Commission through TMR Networks ALAPEDES and System Identification, Brite/Euram Thematic Network (NICONET), and Industrial Contract Research: ISMC, Data4S, Electrabel, Laborelec, Verhaert, Europay.

[1] H.-K. Lo, S. Popescu, and T. Spiller, *Introduction to Quantum Computation and Information* (World Scientific, Singapore, 1998).
[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[4] N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **81**, 3279 (1998).
[5] A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).
[6] A. Kent, N. Linden, and S. Massar, Phys. Rev. Lett. **83**, 2656 (1999).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
[8] W. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[9] A. Peres, Phys. Rev. Lett. **76**, 1413 (1996).
[10] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[11] F. Verstraete, K. Audenaert, and B. de Moor, e-print quant-ph/0011110.
[12] J. Schlienz and G. Mahler, Phys. Rev. A **52**, 4396 (1995).
[13] I. Gohberg, P. Lancaster, and L. Rodman, *Matrices and Indefinite Scalar Products* (Birkhauser Verlag, Basel, 1983).
[14] S. Hill and W. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).