Quantum extension of conditional probability

N. J. Cerf[1,2] and C. Adami[1]

[1]*W. K. Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, California 91125*
[2]*Information Systems Technology Section, Jet Propulsion Laboratory, Pasadena, California 91109*
(Received 31 October 1997; revised manuscript received 14 December 1998)

We analyze properties of the quantum conditional *amplitude* operator [Phys. Rev. Lett. **79**, 5194 (1997)], which plays a role similar to that of the conditional probability in classical information theory. The spectrum of the conditional operator that characterizes a quantum bipartite system is shown to be invariant under local unitary transformations and reflects its inseparability. More specifically, it is proven that the conditional amplitude operator of a separable state cannot have an eigenvalue exceeding 1, which results in a necessary condition for separability. A related separability criterion based on the non-negativity of the von Neumann conditional entropy is also exhibited. [S1050-2947(99)00608-3]

PACS number(s): 03.67.−a, 03.65.Bz, 89.70.+c

I. INTRODUCTION

Quantum inseparability, one of the most intriguing predictions of quantum mechanics, has remained the subject of intense activity since its discovery by Einstein, Podolsky, and Rosen (EPR) [1]. One of its most heralded consequences is the violation of the Bell inequalities [2], which experimentally demonstrates quantum nonlocality. Recently, with the advent of the fields of quantum computation and communication, quantum entanglement and the inseparability it implies has been exploited as a resource for information transmission and processing [3,4]. For example, it has been shown that the entanglement between two systems can be used in order to achieve quantum superdense coding or teleportation [5,6], two quantum communication schemes that have no classical counterpart. In this context, it was realized that Shannon's classical theory of information does not suffice to characterize these quantum informational processes. Consequently, an *extended* theory that explicitly takes the quantum phases into account must be constructed in order to properly incorporate quantum entanglement in an information-theoretic formalism.

In previous work [7–9], we have attempted to define such a quantum information-theoretic formalism relying on the notions of von Neumann conditional and mutual entropies, two quantities that we define in analogy with their classical equivalent. In this paper, we focus on the connection between quantum nonseparability and the conditional amplitude operator, an operator that plays the same role as the conditional probability when defining a quantum conditional entropy. We start by detailing the mathematical properties of the conditional amplitude operator (support, spectrum, connection with von Neumann entropies, etc.). We then derive a *necessary* condition for separability, based on the conditional von Neumann entropy and the underlying conditional amplitude operator. Namely, the eigenvalues of the latter operator cannot exceed 1 if the bipartite state is separable, as was conjectured in Refs. [7–9]. This condition is also *sufficient* for a 2×2 system in a mixture of (generalized) Bell states. It is *not* sufficient in general, however, as reflected by the possibility of a *dilution* of entanglement (i.e., the inseparability of an extended system which contains an inseparable com-

ponent is not guaranteed to be detected by this criterion). Since the von Neumann conditional entropy can be negative only if the conditional amplitude operator admits an eigenvalue larger than 1, a related—but weaker—separability condition is that the conditional entropy is non-negative (see also Refs. [7–9] and [10]).

II. CONDITIONAL AMPLITUDE OPERATOR AND von NEUMANN ENTROPY

In order to establish the notation, let us first sketch the information-theoretic treatment of a bipartite classical system characterized by two random variables A and B. If A and B are characterized by the joint probability distribution $p(a,b)$, one can define the joint Shannon entropy [11]

$$H(AB) = -\sum_{a,b} p(a,b)\log_2 p(a,b) \tag{1}$$

which reflects the randomness of the combined system AB. Using the probability of a conditional on b

$$p(a|b) = \frac{p(a,b)}{p(b)} \tag{2}$$

one then defines the entropy of A conditional on B

$$H(A|B) = \sum_b p(b)H(A|B=b)$$

$$= -\sum_b p(b)\sum_a p(a|b)\log_2 p(a|b)$$

$$= -\sum_{a,b} p(a,b)\log_2 p(a|b) \tag{3}$$

which characterizes the (average) remaining uncertainty of A when B is known [11]. Using Eq. (2), it is easy to prove that the conditional entropy is the entropy of the combined system reduced by the entropy of the known subsystem, that is, $H(A|B) = H(AB) - H(B)$.

Now, our goal will be to extend this construction for quantum variables characterized by density operators [density operators ρ are non-negative trace-class (unit-trace) Hermitian operators] in order to account for quantum entanglement as well as classical correlation. Let us consider a bipartite quantum system AB, characterized by a density operator ρ_{AB} in the product Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Each subsystem A or B is characterized by the reduced density operator $\rho_A = \mathrm{Tr}_B[\rho_{AB}]$ or $\rho_B = \mathrm{Tr}_A[\rho_{AB}]$, respectively, where Tr_A and Tr_B denote partial traces.

Definition 1. Define the conditional amplitude operator of A conditional on B as [7–9]

$$\rho_{A|B} \equiv \exp_2[\log_2 \rho_{AB} - \log_2(\mathbb{1}_A \otimes \rho_B)]$$
$$= \lim_{n \to \infty} [\rho_{AB}^{1/n}(\mathbb{1}_A \otimes \rho_B)^{-1/n}]^n \qquad (4)$$

which is a positive semidefinite Hermitian operator defined on the support of ρ_{AB} in the joint Hilbert space $\mathcal{H}_{AB}$ (see lemma 1). We call ''Hermitian'' the operators satisfying the property $\rho = \rho^\dagger$, while, strictly speaking, this property is called ''self-adjointness'' in the mathematical literature. However, they are equivalent for the bounded operators we consider here. In general, the support of a linear operator ρ is the closure of the set of all $|\psi\rangle$ of the domain of ρ for which $\rho|\psi\rangle \neq 0$. For bounded Hermitian operators, the support of ρ is simply the complement of the kernel of ρ, that is, the subspace of the domain of ρ that is spanned by the eigenvectors corresponding to nonzero eigenvalues.

The second expression in Eq. (4) relies on the Trotter product formula (see, e.g., Ref. [12]), $\exp(X+Y) = \lim_{n\to\infty}[\exp(X/n)\exp(Y/n)]^n$. (The Trotter formula is sometimes called the Lie product formula for finite-dimensional matrices, but it also holds for unbounded self-adjoint operators [12].) It explicitly emphasizes that the conditional amplitude operator is the natural quantum analog of the conditional probability, Eq. (2). As ρ_{AB} and $(\mathbb{1}_A \otimes \rho_B)^{-1}$ do not necessarily commute, the Trotter symmetrization guarantees that $\rho_{A|B}$ is a normal operator (it commutes with its Hermitian conjugate), so that its logarithm is well defined. Indeed, the exponential characterization of $\rho_{A|B}$ immediately implies its Hermiticity and non-negativity.

Lemma 1. $\mathrm{Ker}(\mathbb{1}_A \otimes \rho_B) \subseteq \mathrm{Ker}(\rho_{AB})$, where $\mathrm{Ker}(\rho)$ is the kernel of ρ (the set of all $|\psi\rangle$ of the domain of ρ for which $\rho|\psi\rangle = 0$). Consequently, the conditional amplitude operator $\rho_{A|B}$ is well defined on the support of ρ_{AB}.

We must prove that any eigenvector $|\psi\rangle$ of $(\mathbb{1}_A \otimes \rho_B)$ with zero eigenvalue is such that $\rho_{AB}|\psi\rangle = 0$. First note that any such eigenvector $|\psi\rangle$ can be written as a linear combination of states $|\phi\rangle$, where

$$|\phi\rangle = |a\rangle \otimes |b\rangle \qquad (5)$$

and $|a\rangle$ is an arbitrary state vector in $\mathcal{H}_A$ while $|b\rangle$ is an eigenvector of ρ_B with zero eigenvalue, i.e., $\rho_B|b\rangle = 0$. Let us now consider the positive semidefinite operator $\tilde{\rho} \equiv (\mathbb{1}_A \otimes P_b)\rho_{AB}(\mathbb{1}_A \otimes P_b)$, with $P_b = |b\rangle\langle b|$. It is trivial to check that its partial trace over A vanishes, that is,

$$\mathrm{Tr}_A[\tilde{\rho}] = P_b \rho_B P_b = 0. \qquad (6)$$

This results from the general relation

$$\mathrm{Tr}_A[(\mathbb{1}_A \otimes \lambda_B)\mu_{AB}] = \lambda_B \mathrm{Tr}_A[\mu_{AB}], \qquad (7)$$

where λ_B and μ_{AB} are arbitrary operators in $\mathcal{H}_B$ and $\mathcal{H}_{AB}$, respectively. Since $\tilde{\rho}$ is positive semidefinite and traceless, we have $\tilde{\rho} = 0$. Thus, in particular, the expectation value of $\tilde{\rho}$ in the state $|\phi\rangle$ vanishes,

$$\langle\phi|\tilde{\rho}|\phi\rangle = \langle\phi|\rho_{AB}|\phi\rangle = 0, \qquad (8)$$

which in turn implies that $\rho_{AB}|\phi\rangle = 0$ since ρ_{AB} is positive semidefinite. As this is true for each term $|\phi\rangle$ in the superposition $|\psi\rangle$, we conclude that $\rho_{AB}|\psi\rangle = 0$.

Remark. Lemma 1 clearly implies that $\mathrm{Sup}(\rho_{AB}) \subseteq \mathrm{Sup}(\mathbb{1}_A \otimes \rho_B)$, that is, the support of ρ_{AB} is included in that of $\mathbb{1}_A \otimes \rho_B$. Equivalently, $\mathrm{Ker}(\mathbb{1}_A \otimes \rho_B) \cap \mathrm{Sup}(\rho_{AB}) = \varnothing$, so that the subspace spanned by the eigenvectors with zero eigenvalue of $\mathbb{1}_A \otimes \rho_B$ is disjoint from the support of ρ_{AB}, and therefore $\rho_{A|B}$ contains no singularities in the support of ρ_{AB}. Of course, there is a classical analog for probability distributions which ensures that $p(a|b) = p(a,b)/p(b)$ is well defined if a,b are such that $p(a,b) \neq 0$. Indeed, if b is such that $p(b) = 0$, then $p(a,b) = 0$, $\forall a$. This is obvious since $p(b) = \Sigma_a p(a,b)$ and $p(a,b) \geq 0$.

Definition 2. The conditional von Neumann entropy is defined using the joint density operator ρ_{AB} and the conditional amplitude operator $\rho_{A|B}$ as [7–9]

$$S(A|B) = -\mathrm{Tr}'[\rho_{AB} \log_2 \rho_{A|B}] \qquad (9)$$

in close analogy to the classical definition, Eq. (3). Thus, $S(A|B)$ corresponds to the *quantum* entropy of A conditional on B, and is mathematically well-defined as a consequence of lemma 1. The trace in Eq. (9) is restricted to the support of ρ_{AB}, i.e., the common eigenvectors $|\psi\rangle$ with zero eigenvalue of ρ_{AB} and $\mathbb{1}_A \otimes \rho_B$ are omitted in Tr'. This will be understood from now on, and we will omit the prime. (Strictly speaking, this argument is also used in classical information theory to define conditional entropies.)

Theorem 1. The definitions of $\rho_{A|B}$ and the conditional von Neumann entropy imply that $S(A|B) = S(AB) - S(B)$, as for Shannon entropies.

First, using Eqs. (4) and (9), we have

$$S(A|B) = -\mathrm{Tr}[\rho_{AB} \log_2 \rho_{AB}] + \mathrm{Tr}[\rho_{AB} \log_2(\mathbb{1}_A \otimes \rho_B)], \qquad (10)$$

where the first term on the right-hand side is clearly equal to $S(AB)$. In order to calculate the second term on the right-hand side of Eq. (10), we write

$$\mathrm{Tr}_A[\rho_{AB} \log_2(\mathbb{1}_A \otimes \rho_B)] = \mathrm{Tr}_A[\rho_{AB}(\mathbb{1}_A \otimes \log_2 \rho_B)]$$
$$= \mathrm{Tr}_A[\rho_{AB}]\log_2 \rho_B$$
$$= \rho_B \log_2 \rho_B, \qquad (11)$$

where we have made use of Eq. (7). This implies that the second term on the right-hand side of Eq. (10) is

$$\mathrm{Tr}_B[\rho_B \log_2 \rho_B] = -S(B) \qquad (12)$$

resulting in $S(A|B) = S(AB) - S(B)$.

Lemma 2. The spectrum of the conditional amplitude operator $\rho_{A|B}$ is invariant under unitary transformations of the product form $U_A \otimes U_B$ on ρ_{AB}.

Let us consider the isomorphism

$$\rho_{AB} \rightarrow \rho'_{AB} = (U_A \otimes U_B) \rho_{AB} (U_A^\dagger \otimes U_B^\dagger). \qquad (13)$$

We first calculate the partial trace of the joint density operator over A *after* this transformation, that is,

$$
\begin{aligned}
\rho'_B &= \mathrm{Tr}_A[\rho'_{AB}] = \mathrm{Tr}_A[(U_A \otimes U_B) \rho_{AB} (U_A^\dagger \otimes U_B^\dagger)] \\
&= \mathrm{Tr}_A[(\mathbb{1}_A \otimes U_B)(U_A \otimes \mathbb{1}_B) \rho_{AB} (U_A^\dagger \otimes \mathbb{1}_B)(\mathbb{1}_A \otimes U_B^\dagger)] \\
&= U_B \mathrm{Tr}_A[(U_A \otimes \mathbb{1}_B) \rho_{AB} (U_A^\dagger \otimes \mathbb{1}_B)] U_B^\dagger \\
&= U_B \rho_B U_B^\dagger,
\end{aligned}
\qquad (14)
$$

where we have used Eq. (7) and the basis invariance of the trace. This implies that the conditional amplitude operator transforms as

$$\rho_{A|B} \rightarrow \rho'_{A|B} = (U_A \otimes U_B) \rho_{A|B} (U_A^\dagger \otimes U_B^\dagger) \qquad (15)$$

so that its spectrum is conserved under $U_A \otimes U_B$ on ρ_{AB}. Note that the classical analog of a $U_A \otimes U_B$ isomorphism corresponds to permuting the rows and columns of the joint probability distribution $p(a,b)$, so that the classical counterpart of Eq. (15) is straightforward.

Remark. Lemma 2 suggests that the spectrum of $\rho_{A|B}$ is related to the separability of the state ρ_{AB}, since separability (or inseparability) must be conserved under a $U_A \otimes U_B$ isomorphism. This will be examined in the next section.

Corollary. The conditional von Neumann entropy $S(A|B)$ is invariant under a unitary transformation of the product form $U_A \otimes U_B$. This property results from the definition of $S(A|B)$, Eq. (9), together with Eq. (15), or can be checked trivially from theorem 1.

III. CONDITIONS FOR SEPARABILITY

Theorem 2. The operator $\sigma_{AB} \equiv -\log_2 \rho_{A|B} = \log_2(\mathbb{1}_A \otimes \rho_B) - \log_2 \rho_{AB}$ is positive semidefinite if the quantum bipartite system characterized by ρ_{AB} is separable.

Let us consider a *separable* (or classically correlated) bipartite system AB which is characterized by the density operator ρ_{AB}, i.e., a convex combination of product states (see, e.g., Ref. [13]):

$$\rho_{AB} = \sum_i w_i (\rho_A^{(i)} \otimes \rho_B^{(i)}) \quad \text{with} \sum_i w_i = 1 \text{ and } 0 \le w_i \le 1,$$
$$(16)$$

where $\rho_A^{(i)}$ and $\rho_B^{(i)}$ are states in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The weights w_i can be viewed as the probability distribution of a random variable that is used by both parties in order to prepare their subsystems A and B. Namely, if the subsystem A (and B) is prepared in state $\rho_i^{(A)}$ (and $\rho_i^{(B)}$) when the random variable takes on value i, the state of the joint system is given by Eq. (16). Let us define the operator

$$\lambda_{AB} \equiv \mathbb{1}_A \otimes \rho_B - \rho_{AB}. \qquad (17)$$

It is easy to check that λ_{AB} is positive semi-definite if ρ_{AB} is separable. Indeed, in such a case we have

$$\lambda_{AB} = \sum_i w_i[(\mathbb{1}_A - \rho_A^{(i)}) \otimes \rho_B^{(i)}] \ge 0 \qquad (18)$$

since a sum of positive operators is a positive operator. (The two terms in square brackets are each ≥ 0.) Now, we can use the fact that, if X and Y are two Hermitian operators such that $X \ge Y > 0$ (the notation $X \ge Y$ means that $X - Y$ is a positive semidefinite operator), then $\ln X \ge \ln Y$, as implied by Löwner's theorem [14]. (Note that the converse is not true.) As a consequence, using $X = \mathbb{1}_A \otimes \rho_B$ and $Y = \rho_{AB}$, we conclude that $\lambda_{AB} \ge 0$ implies $\sigma_{AB} \ge 0$.

Corollary 1. Any separable bipartite state satisfies the condition $\rho_{A|B} \le 1$.

Since we have $\rho_{A|B} = \exp_2(-\sigma_{AB})$, theorem 2 shows indeed that no eigenvalue of the conditional amplitude operator exceeds 1 for a separable state, as was conjectured in Refs. [7–9]. This yields a simple *necessary* (but not sufficient) condition for separability. The classical analog of this property is that $-\log_2 p(a|b) \ge 0$, $\forall\ a,b$. The latter inequality simply results from the fact that $p(a|b) = p(a,b)/p(b) \le 1$, $\forall\ a,b$, as $p(b) = \Sigma_a p(a,b)$ and $p(a,b) \ge 0$.

Corollary 2. The conditional von Neumann entropy $S(A|B)$ is non-negative for a separable bipartite state.

Since we have $S(A|B) = \mathrm{Tr}[\rho_{AB} \sigma_{AB}]$, this simply follows from the fact that $\mathrm{Tr}[XY] \ge 0$ if $X, Y \ge 0$. Thus, the non-negativity of the conditional entropy is another (weaker) necessary condition for separability [7–9]. This has also been shown in general for Renyi entropies in Ref. [10]. Furthermore, the negativity of conditional entropies can be related to the violation of entropic Bell inequalities, as shown in Ref. [15].

Note that corollary 2 can also be obtained by using the concavity of $S(A|B)$ in a convex combination of ρ_{AB}'s, a property related to the strong subadditivity of quantum entropies [16]. If $\rho_{AB} = \Sigma_i w_i\ \rho_{AB}^{(i)}$, then

$$S(A|B) = S(\rho_{AB}) - S(\rho_B) \ge \sum_i w_i[S(\rho_{AB}^{(i)}) - S(\rho_B^{(i)})].$$
$$(19)$$

Using the fact that, for a separable state, the ith term gives $S(A|B) = S(\rho_A^{(i)})$ since A and B are independent, i.e., $\rho_{AB}^{(i)} = \rho_A^{(i)} \otimes \rho_B^{(i)}$, we obtain

$$S(A|B) \ge \sum_i w_i S(\rho_A^{(i)}) \ge 0. \qquad (20)$$

Note that a negative conditional von Neumann entropy $S(A|B)$ necessarily implies that an eigenvalue of $\rho_{A|B}$ exceeds 1, but the converse is not true. Thus, weak inseparability (in the sense that $S(A|B) \ge 0$ despite the inseparability of ρ_{AB}) may be revealed by the spectrum of $\rho_{A|B}$.

Example. The necessary separability condition $\rho_{A|B} \le 1$ can be illustrated for two quantum bits, when ρ_{AB} is an arbitrary mixture of the four Bell states $|\Phi^\pm\rangle = 2^{-1/2}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = 2^{-1/2}(|01\rangle \pm |10\rangle)$. The application of this criterion to Werner states (which are a special case of mixtures of Bell states) was shown in Refs. [7–9]. Note first

that, whatever the weights in such a mixture, $\rho_B = 1_B/2$, i.e., B is maximally disordered. Using Eqs. (4) and (17), we obtain $\rho_{A|B} = 2\rho_{AB}$ and $\lambda_{AB} = 1_{AB}/2 - \rho_{AB}$, which results in

$$\rho_{A|B} = 1_{AB} - 2\lambda_{AB}. \tag{21}$$

Thus, in this case, $\rho_{A|B}$ has all its eigenvalues ≤ 1 if and only if $\lambda_{AB} \geq 0$. (This is not true in general as the converse of Löwner's theorem does not hold.) This implies that $\rho_{A|B} \leq 1$ is also a *sufficient* separability condition for any mixture of Bell states (the proof relies on the fact that $\lambda_{AB} \geq 0$ is a necessary *and* sufficient separability condition for two quantum bits [17]). The same is true for mixtures of *generalized* Bell states (i.e., those states obtained by applying any local transformation $U_A \otimes U_B$ to the Bell states).

Theorem 3. There exist inseparable bipartite states ρ_{AB} such that the operator σ_{AB} is positive semidefinite; consequently, $\sigma_{AB} \geq 0$ (or $\rho_{A|B} \leq 1$) is *not* a sufficient condition for separability.

Let us consider a bipartite system AB characterized by ρ_{AB}, which we extend with another system $A'B'$ in the state $\rho_{A'B'}$. The joint system is then characterized by a density operator of the product form

$$\rho_{AA';BB'} = \rho_{AB} \otimes \rho_{A'B'}. \tag{22}$$

We first calculate the conditional amplitude operator of the joint system (AA' conditional on BB')

$$\rho_{AA'|BB'} = \exp_2[\log_2 \rho_{AA';BB'} - \log_2(1_{AA'} \otimes \rho_{BB'})], \tag{23}$$

where the reduced density operator describing BB' is

$$\rho_{BB'} = \mathrm{Tr}_{AA'}[\rho_{AA';BB'}] = \rho_B \otimes \rho_{B'}. \tag{24}$$

Using the identity $\ln(X \otimes Y) = \ln X \otimes 1 + 1 \otimes \ln Y$ for operators $X, Y > 0$ as well as its exponential, i.e., $\exp X \otimes \exp Y = \exp(X \otimes 1 + 1 \otimes Y)$, we obtain

$$\begin{aligned}\rho_{AA'|BB'} &= \exp_2[\log_2 \rho_{AB} \otimes 1_{A'B'} + 1_{AB} \otimes \log_2 \rho_{A'B'} \\ &\quad - 1_A \otimes \log_2 \rho_B \otimes 1_{A'B'} - 1_{AB} \otimes 1_{A'} \otimes \log_2 \rho_{B'}] \\ &= \exp_2[(\log_2 \rho_{AB} - 1_A \otimes \log_2 \rho_B) \otimes 1_{A'B'} \\ &\quad + 1_{AB} \otimes (\log_2 \rho_{A'B'} - 1_{A'} \otimes \log_2 \rho_{B'})] \\ &= \exp_2[\log_2 \rho_{AB} - 1_A \otimes \log_2 \rho_B] \\ &\quad \otimes \exp_2[\log_2 \rho_{A'B'} - 1_{A'} \otimes \log_2 \rho_{B'}]. \end{aligned} \tag{25}$$

Thus, we have

$$\rho_{AA'|BB'} = \rho_{A|B} \otimes \rho_{A'|B'} \tag{26}$$

which parallels the classical relation $p(aa'|bb') = p(a|b)p(a'|b')$ if AB and $A'B'$ are independent bipartite systems, that is, if $p(a,a';b,b') = p(a,b)p(a',b')$. Consequently, we have

$$\Sigma(\rho_{AA'|BB'}) = \Sigma(\rho_{A|B}) \otimes \Sigma(\rho_{A'|B'}) \tag{27}$$

where $\Sigma(\rho)$ stands for the spectrum of ρ.

Now, let us assume that AB is an inseparable system with $\sigma_{AB} \ngeq 0$ or $\rho_{A|B} \nleq 1$. In other words, the operator $\rho_{A|B}$ admits

an eigenvalue that exceeds 1. Assume also that $A'B'$ corresponds to two independent systems in a product state, that is, $\rho_{A'B'} = \rho_{A'} \otimes \rho_{B'}$. The resulting conditional amplitude operator for $A'B'$ is then $\rho_{A'|B'} = \rho_{A'} \otimes 1_{B'}$, just like its classical counterpart $p(a|b) = p(a)$ if $p(a,b) = p(a)p(b)$. Obviously, we then have $\rho_{A'|B'} \leq 1$, as expected since $A'B'$ is separable. According to Eq. (27), the eigenvalues of $\rho_{AA'|BB'}$ are the pairwise products of eigenvalues of $\rho_{A|B}$ with eigenvalues of $\rho_{A'|B'}$. Therefore, it is easy to find a system $A'B'$ with eigenvalues of $\rho_{A'|B'}$ small enough so that the product of any of them with an unclassical (>1) eigenvalue of $\rho_{A|B}$ results in eigenvalues of $\rho_{AA'|BB'}$ that are all ≤ 1. The extended system is then characterized by $\sigma_{AA';BB'} \geq 0$ or $\rho_{AA'|BB'} \leq 1$, while it obviously contains an inseparable component AB. Such a *dilution* of inseparability is always achievable with a system $A'B'$ that is large enough and maximally disordered (i.e., $\rho_{A'B'} \sim 1_{A'} \otimes 1_{B'}$). Consequently, the condition that $\sigma_{AB} \geq 0$ or $\rho_{A|B} \leq 1$ cannot be sufficient for separability.

Remark 1. Eq. (27) implies that, if AB and $A'B'$ are inseparable systems with $\rho_{A|B} \nleq 1$ and $\rho_{A'|B'} \nleq 1$, then the inseparability of the joint system is necessarily revealed by $\rho_{AA'|BB'} \nleq 1$.

Remark 2. While $\lambda_{AB} \geq 0$ is a sufficient separability condition for 2×2 and 2×3 systems [17], it cannot be concluded that $\sigma_{AB} \geq 0$ or $\rho_{A|B} \leq 1$ is also sufficient in these cases, as the converse of Löwner's theorem does not hold. Interestingly, we found numerical evidence that only very few inseparable states of two qubits exist with $\rho_{A|B} \leq 1$. These "slightly inseparable" states which have a classical conditional amplitude operator might have interesting properties that are worth investigating.

IV. CONCLUSION

Given a bipartite system characterized by a density operator ρ_{AB}, we define a conditional amplitude operator $\rho_{A|B}$ (a positive semidefinite Hermitian operator defined on the support of ρ_{AB}) which plays the same role as the conditional probability but in quantum information theory. Specifically, this operator can be used to define a conditional von Neumann entropy, $S(A|B) = -\mathrm{Tr}[\rho_{AB} \log_2 \rho_{A|B}]$, in perfect analogy with Shannon conditional entropy. Quantum counterparts of many classical properties also hold: (i) $\rho_{A|B}$ is defined on the support of ρ_{AB}, so that $S(A|B)$ is well defined, (ii) $S(A|B) = S(AB) - S(B)$, (iii) $\rho_{A|B} = \rho_A \otimes 1_B$ if A and B are independent, (iv) $\rho_{AA'|BB'} = \rho_{A|B} \otimes \rho_{A'|B'}$ if $\rho_{AA';BB'} = \rho_{AB} \otimes \rho_{A'B'}$, (v) $\rho_{A|B}$ transforms as $(U_A \otimes U_B)\rho_{A|B}(U_A^\dagger \otimes U_B^\dagger)$ when performing a local unitary transformation $U_A \otimes U_B$ on ρ_{AB}, so that its spectrum and therefore $S(A|B)$ are invariant under such transformations on ρ_{AB}.

The main nonclassical feature that appears when dealing with a quantum bipartite system rather than a classical one is that $\rho_{A|B}$ may have a "nonclassical" spectrum, that is, eigenvalues of $\rho_{A|B}$ may exceed 1, which in turn implies that $S(A|B)$ can be negative. More specifically, we have shown that $\rho_{AB} \leq 1$ for any separable state, which also straightforwardly implies $S(A|B) \geq 0$. Therefore, a *necessary* condition for separability is that the conditional amplitude operator has a "classical" spectrum, or that the conditional entropy is

non-negative (the latter is a weaker condition). These conditions are *not* sufficient in general, since extending an inseparable state with a separable one of large dimension may result in a *dilution* of inseparability, that is, it may give rise to a state with $\rho_{A|B} \leq 1$. In other words, some inseparable states exist with $\rho_{A|B} \leq 1$, and certainly some with $S(A|B) \geq 0$ (even if $\rho_{A|B} \nleq 1$). This dilution effect can be found even in the case of 2×2 systems. Still, the separability condition $\rho_{A|B} \leq 1$ happens to be sufficient for a 2×2 system in a mixture of generalized Bell states [or states with maximally disordered subsystems that are characterized by a T matrix (T states) [10]]. Very recently, a novel type of multipartite entanglement has been discovered which is not revealed in any

bipartite separation [18], and gives rise to so-called ''bound'' entanglement [19]. Analyzing the spectrum of conditional amplitude operators for such systems might shed new light on multipartite entanglement.

ACKNOWLEDGMENTS

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] J. S. Bell, Physics (N.Y.) **1**, 195 (1964); Rev. Mod. Phys. **38**, 447 (1966).

[3] D. P. DiVincenzo, Science **270**, 255 (1995).

[4] A. Barenco *et al.*, Phys. Rev. Lett. **74**, 4083 (1995).

[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[6] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[7] N. J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997).

[8] N. J. Cerf and C. Adami, in *New Developments on Fundamental Problems in Quantum Physics*, edited by M. Ferrero and A. van der Merwe (Kluwer Academic, Dordrecht, 1997), pp. 77–84.

[9] N. J. Cerf and C. Adami, Physica D **120**, 62 (1998); in *Proceedings of the Fourth Workshop on Physics and Computation*, edited by T. Toffoli *et al.* (New England Complex Systems Institute, Cambridge, MA, 1996), p. 65.

[10] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996).

[11] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948); **27**, 623 (1948).

[12] M. Reed and B. Simon, *Methods of Modern Mathematical Physics* (Academic Press, New York, 1979), Vol. I, pp. 295–297.

[13] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[14] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, 1985).

[15] N. J. Cerf and C. Adami, Phys. Rev. A **55**, 3371 (1997).

[16] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).

[17] N. J. Cerf, C. Adami, and R. M. Gingrich, Phys. Rev. A **60**, 898 (1999).

[18] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).

[19] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).