An Additive and Operational Entanglement Measure:
Conditional Entanglement of Mutual Information

Dong Yang,[1,2] Michał Horodecki,[3,4] and Z. D. Wang[1]

[1]*Department of Physics and Center of Theoretical and Computational Physics, The University of Hong Kong,
Pokfulam Road, Hong Kong, China*
[2]*Laboratory for Quantum Information and College of Mechatronics Engineering, China Jiliang University,
Hangzhou, Zhejiang 310018, China*
[3]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[4]*National Quantum Information Centre of Gdańsk, University of Gdańsk, 80-952 Sopot, Poland*

Based on the monogamy of entanglement, we develop the technique of quantum conditioning to build an *additive* entanglement measure: the conditional entanglement of mutual information. Its *operational* meaning is elaborated to be the minimal net "flow of qubits" in the process of partial state merging. The result and conclusion can also be generalized to multipartite entanglement cases.

Entanglement, as a key resource and ingredient in quantum information and computation as well as communication, plays a crucial role in quantum information theory. It is necessary to quantify entanglement from different standpoints. A number of entanglement measures have been proposed, and their properties have been explored extensively (see, e.g., Refs. [1,2], and references therein). Nevertheless several questions still remain unanswered, especially the following. (i) How to systematically introduce new entanglement measures. It is commonly accepted that an appropriate entanglement measure is necessarily nonincreasing under local operations and classical communication (LOCC). But few approaches to construct entanglement measures are known. For example, the entanglement of formation E_f [3] is established via the technique of "convex roof," and the relative entropy of entanglement E_r [4] is based on a concept of "distance." (ii) The operational meaning. Entanglement measures are largely studied by the monotonicity under LOCC operations, but little is known for the operational meaning except the distillable entanglement E_d [3] and entanglement of cost E_c [5]. Just recently, a new paradigm to explain entanglement measures was proposed based on quantum communication [6], where squashed entanglement E_{sq} [7] obtains its meaning. (iii) Additivity. It is a very desirable property that can largely reduce computation of entanglement. Since quantum mechanics is statistical, often operational meaning of entanglement measures is acquired only in an asymptotic regime of many copies of a given state. For additive measures, it is reduced to a single copy. Additivity holds for squashed entanglement E_{sq} [7] and logarithmic negativity E_N [8,9] and is conjectured to hold for E_f, but E_r is nonadditive [10]. (iv) Multipartite entanglement. It is more difficult to design multipartite entanglement measures; hence, it would be good if a bipartite one can be easily extended to multipartite regime.

In this Letter, based on the monogamy of entanglement, we develop the technique of quantum conditioning of a correlation function to construct entanglement measures. Taking the quantum mutual information as the correlation function, we formulate a new entanglement measure—the conditional entanglement of mutual information. Remarkably, it is *additive* with an *operational* meaning and can straightforwardly be generalized to multipartite cases.

Let us begin with the question of how to build an entanglement measure. The monogamy of entanglement [11] is a good starting point. It tells us that entanglement is a type of quantum correlation that cannot be shared. This feature is distinct from the classical correlation that can be shared. A simple example is the Bell state $|\Phi\rangle_{AB} = 1/\sqrt{2}(|00\rangle + |11\rangle)$ between Alice and Bob. Monogamy of the pure entangled state $|\Phi\rangle_{AB}$ excludes the possibility that any other party could correlate with it. It is different for the classical correlated state $\rho_{AB} = 1/2(|00\rangle\langle00| + |11\rangle\langle11|)$. Obviously, another party Charlie can share the correlation with the form $\rho_{ABC} = 1/2(|000\rangle\langle000| + |111\rangle\langle111|)$. The example is the extremal case in which the quantum correlation and the classical one are well separated. However, it is not the case for a generic mixed state. A correlation function $f(A{:}B)$ [12,13], for instance, quantum mutual information, usually contains a quantum correlation and a classical one and is "dirty" in the sense that the quantum correlation and the classical one are interwound in a complex way that cannot be separated neatly. How can we "distill" a "neat" quantum correlation? The technique is quantum extension and quantum conditioning. Quantum extension means that, given a state ρ_{AB}, we embed it into a larger state $\rho_{AA'BB'}$ such that ρ_{AB} is the reduced state of $\rho_{AA'BB'}$, i.e., $\text{tr}_{A'B'}\rho_{AA'BB'} = \rho_{AB}$. Apparently, $f(AA'{:}BB')$ is larger than $f(A{:}B)$. To return a correlation measure for ρ_{AB}, we consider the difference $f(AA'{:}BB') - f(A'{:}B')$. Now let us imagine for a while that quantum (q) and

classical (c) correlations sum up in a simple way. Then due to the unsharability of q we can write $f(AA': BB') = q(AB) + q(A'B') + c(AA': BB') \equiv q_1 + q_2 + c_{12}$, while $f(A':B') = q(A':B') + c(A':B') \equiv q_2 + c_2$. Subtracting, we get q_1 (i.e., what we want) plus the difference $c_{12} - c_2$ which, as we have seen, can be zero because classical correlations are sharable. In general, it will not vanish, so we take infimum over extensions, trying to squash out the classical correlations as much as we can. The infimum of the difference must be of purely quantum origin; hence, we treat it as a correction to our initial, oversimplified assumption.

For a given function $f(\cdot)$ quantifying a correlation, we have two candidates for its conditioned version:

$$C_f^s(\rho_{AB}) = \inf[f(\rho_{AA':BB'}) - f(\rho_{A':B'})], \quad (1a)$$

$$C_f^a(\rho_{AB}) = \inf[f(\rho_{A:BE}) - f(\rho_{A:E})], \quad (1b)$$

where infimum is taken over all extensions $\rho_{AA'BB'}$ (ρ_{ABE}) of ρ_{AB}. $C_f^s(\cdot)$ is the symmetric conditioned version of f while $C_f^a(\cdot)$ is the asymmetric one. Note that the above definition is similar to that of conditional entropy [14] $S(A|B) = S(AB) - S(B)$, with $S(\rho)$ as the von Neumann entropy $S(\rho) = -\text{Tr}\rho \log\rho$, and is thus referred to as *conditional entanglement*. As a matter of fact, squashed entanglement can be constructed by taking asymmetric conditioning of mutual information $E_{sq}(\rho_{AB}) = \frac{1}{2} \times \inf\{I(A:BE) - I(A:E)\} \equiv \frac{1}{2}\inf I(A:B|E)$, where $I(X:Y) = S(X) + S(Y) - S(XY)$ is quantum mutual information and $I(A:B|E) = S(AE) + S(BE) - S(ABE) - S(E)$ is conditional mutual information. It is notable that $I(A:BE) - I(A:E) = I(AE:B) - I(E:B)$ is symmetric with respect to systems AB though each term in the formula is asymmetric with respect to both parties. This gives the possibility to build symmetric entanglement measures by asymmetric conditioning. It is surprising that a neat quantum correlation can be obtained by subtracting two dirty functions. Does this approach really work? The answer is *yes* (see Ref. [15] to systematically introduce new entanglement measures based on quantum conditioning). We illustrate that a new entanglement measure can indeed be constructed by taking f to be quantum mutual information in the symmetric version. We add a factor $1/2$ and denote it by E_I. Most intriguingly, we show below that E_I is additive, has an operational meaning, and can be directly generalized to multipartite states where the factor $1/2$ has a good reason to exist.

Definition 1.—Let ρ_{AB} be a mixed state on a bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The conditional entanglement of mutual information for ρ_{AB} is defined as

$$E_I(\rho_{AB}) = \inf\tfrac{1}{2}\{I(AA':BB') - I(A':B')\}, \quad (2)$$

where the infimum is taken over all extensions of ρ_{AB}, i.e., over all states satisfying the equation $\text{Tr}_{A'B'}\rho_{AA'BB'} = \rho_{AB}$.

To justify that E_I is an appropriate entanglement measure, we now elaborate that it does satisfy two essential axioms that an entanglement measure should obey [1].

1. Entanglement does not increase under LOCC, i.e., $E_I[\Lambda(\rho)] \leq E_I(\rho)$*, for any LOCC operation* Λ*.*—The monotonicity under LOCC implies that entanglement remains invariant under local unitary transformations. This comes from the fact that local unitary transformations are reversible LOCC. The convexity of entanglement used to be considered as a mandatory ingredient of the mathematical formulation of monotonicity [1,16]. At present, the convexity is thought to be merely a convenient mathematical property. Also, there is a common agreement that the strong monotonicity—monotonicity *on average* under LOCC—is unnecessary but useful [1,16]. Many known existing entanglement measures are convex and satisfy the strong monotonicity. We will show that E_I satisfies the strong monotonicity.

Since, as we will see further, E_I is convex, it is sufficient to prove that E_I is nonincreasing under a local measurement [17] (without loss of generality, we can check it only on Alice's side), namely, $E_I(\rho_{AB}) \geq \sum_k p_k E_I(\tilde{\rho}_{AB}^k)$, where $\tilde{\rho}_{AB}^k = A_k \rho_{AB} A_k^\dagger / p_k$, $p_k = \text{tr} A_k \rho_{AB} A_k^\dagger$, and $\sum_k A_k^\dagger A_k = I_A$. Another way to describe the measurement process is as follows. First, one attaches two ancillary systems A_0 and A_1 in states $|0\rangle_{A_0}$ and $|0\rangle_{A_1}$ to system AB. Second, a unitary operation $U_{AA_0A_1}$ on AA_0A_1 is performed. Third, the system A_1 is traced out to get the state as $\tilde{\rho}_{A_0AB} = \sum_k A_k \rho_{AB} A_k^\dagger \otimes (|k\rangle\langle k|)_{A_0}$. Now for any extension state $\rho_{AA'BB'}$, we get the state after the measurement on A: $\tilde{\rho}_{A_0AA'BB'} = \sum_k A_k \rho_{AA'BB'} A_k^\dagger \otimes (|k\rangle\langle k|)_{A_0} = \sum_k p_k \tilde{\rho}_{AA'BB'}^k \otimes (|k\rangle\langle k|)_{A_0}$. Most crucially, we have

$$I(\rho_{AA':BB'}) - I(\rho_{A':B'}) = I(0_{A_0A_1} \otimes \rho_{AA':BB'})$$
$$- I(\rho_{A':B'}) \quad (3a)$$
$$= I(U_{A_0A_1A}(0_{A_0A_1} \otimes \rho_{AA':BB'}))$$
$$- I(\rho_{A':B'}) \quad (3b)$$
$$\geq I(\tilde{\rho}_{A_0AA':BB'}) - I(\tilde{\rho}_{A':B'}) \quad (3c)$$
$$= \sum_k p_k[I(\tilde{\rho}_{AA':BB'}^k) - I(\tilde{\rho}_{A':B'}^k)]$$
$$+ \sum_k p_k I(\tilde{\rho}_{A':B'}^k) - I(\tilde{\rho}_{A':B'})$$
$$+ S(\tilde{\rho}_{BB'}) - \sum_k p_k S(\tilde{\rho}_{BB'}^k)$$
$$= \sum_k p_k[I(\tilde{\rho}_{AA':BB'}^k) - I(\tilde{\rho}_{A':B'}^k)]$$
$$+ \chi(BB') + \chi(A'B') - \chi(A')$$
$$- \chi(B') \geq \sum_k p_k[I(\tilde{\rho}_{AA':BB'}^k)$$
$$- I(\tilde{\rho}_{A':B'}^k)], \quad (3d)$$

where $\chi(\rho) = S(\rho) - \sum_k p_k S(\rho^k)$ is the Holevo quantity of the ensemble $\{p_k, \rho^k\}$. The equality of (3b) follows from invariance of quantum mutual information under local uni-

tary operations, while the inequalities of (3c) and (3d) stem from, respectively, the fact that quantum mutual information and the Holevo quantity are nonincreasing under tracing out a subsystem. Consequently, we have proved that E_I is nonincreasing on average under LOCC operations.

2. Entanglement is not negative and is zero for separable states.—The inequality $E_I \geq 0$ comes from the fact that the quantum mutual information is nonincreasing under tracing subsystems of both sides. For a separable state ρ_{AB}, it can always be decomposed into a separable form: $\rho_{AB} = \sum_{i,j} p_{ij} \phi_A^i \otimes \phi_B^j$. An extension state may be chosen to be $\rho_{AA'BB'} = \sum_{i,j} p_{ij} \phi_A^i \otimes (|i\rangle\langle i|)_{A'} \otimes \phi_B^j \otimes (|j\rangle\langle j|)_{B'}$. It is obvious that $I(AA':BB') = I(A':B')$, and thus $E_I = 0$ for separable states.

Continuity.—The conditional entanglement of mutual information is asymptotically continuous; i.e., if $|\rho_{AB} - \sigma_{AB}| \leq \epsilon$, then $|E_I(\rho) - E_I(\sigma)| \leq K\epsilon \log d + O(\epsilon)$, where $|\cdot|$ is the trace norm for matrix, K is a constant, $d = \dim\mathcal{H}_{AB}$, and $O(\epsilon)$ is a function that depends only on ϵ (in particular, it does not depend on dimension) and satisfies $\lim_{\epsilon\to 0} O(\epsilon) = 0$.

The proof of the asymptotic continuity is similar to that for squashed entanglement and is presented in the appendix of Ref. [15].

Convexity.—E_I is convex; i.e., $E_I[\lambda\rho + (1 - \lambda)\sigma] \leq \lambda E_I(\rho) + (1 - \lambda)E_I(\sigma)$ for $0 \leq \lambda \leq 1$.

Proof.—For any extension states $\rho_{AA'BB'}$ and $\sigma_{AA'BB'}$, we consider the extension state $\tau_{AA'A''BB'B''} = \lambda\rho_{AA'BB'} \otimes (|0\rangle\langle 0|)_{A''} \otimes (|0\rangle\langle 0|)_{B''} + (1 - \lambda)\sigma_{AA'BB'} \otimes (|1\rangle\langle 1|)_{A''} \otimes (|1\rangle\langle 1|)_{B''}$ and have $I(\tau_{AA'A'':BB'B''}) - I(\tau_{A'A'':B'B''}) = \lambda[I(\rho_{AA':BB'}) - I(\rho_{A':B'})] + (1 - \lambda)[I(\sigma_{AA':BB'}) - I(\sigma_{A':B'})]$. This implies E_I is convex.

An immediate corollary of convexity is that $E_I \leq E_f$ and furthermore $E_I \leq E_c$ due to the following additivity.

Proposition 1.—$E_I(\rho_{AB} \otimes \sigma_{CD}) = E_I(\rho_{AB}) + E_I(\sigma_{CD})$.

Proof.—On the one hand, for any extension states $\rho_{AA'BB'}$ and $\sigma_{CC'DD'}$, $\rho_{AA'BB'} \otimes \sigma_{CC'DD'}$ is an extension state of $\rho_{AB} \otimes \sigma_{CD}$.

$$I(AA'CC':BB'DD') - I(A'C':B'D')$$
$$= I(AA':BB') - I(A':B') + I(CC':DD') - I(C':D'). \tag{4}$$

So $E_I(\rho_{AB} \otimes \sigma_{CD}) \leq E_I(\rho_{AB}) + E_I(\sigma_{CD})$ holds.

On the other hand, for extension states $\tau_{ACE':BDF'}$ of $\rho_{AB} \otimes \sigma_{CD}$, $\tau_{ACE':BDF'}$ is an extension state of ρ_{AB} and $\tau_{CE':DF'}$ is an extension state of σ_{CD}. Therefore we have
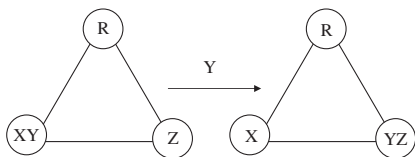
$$I(ACE':BDF') - I(E':F') = I(ACE':BDF') - I(CE':DF')$$
$$+ I(CE':DF') - I(E':F'). \tag{5}$$

This means that $E_I(\rho_{AB} \otimes \sigma_{CD}) \geq E_I(\rho_{AB}) + E_I(\sigma_{CD})$. So we have finally the additivity equality.

It is quite remarkable that the property of additivity is rather easy to prove for conditional entanglement while it is extremely tough for other candidates. The reason lies in that the conditional entanglement is naturally superadditive while others are usually subadditive.

Before we elaborate on the operational meaning of the measure E_I, we briefly recall that of quantum conditional mutual information [18], in which the quantum mutual information one [19] corresponds to a special case. Quantum conditional mutual information is given the operational meaning in the process of quantum state redistribution [18]. The situation is depicted in Fig. 1: Initially, XY is with Alice and Z with Bob. R is the reference system such that Φ_{RXYZ} is pure. The task is that Alice sends Y to Bob while the final state is still in the pure state Φ_{RXYZ}. Alice and Bob share entanglement for free and have an ideal quantum channel to communicate. No classical communication is allowed. To accomplish the task, the minimal number of qubits that are required to transfer from Alice to Bob is $Q = 1/2 I(R:Y|Z)$.

In a recent paper [6], the squashed entanglement received the operational meaning with the aid of that of conditional mutual information. It gives a hint for finding the operational meaning for E_I since it can be regarded as a measure constructed in the same spirit. Does the conditional function $\frac{1}{2}\{I(AA':BB') - I(A':B')\}$ have an operational meaning? It turns out that it does. Even more, it is a conservative quantity, which describes a process, but depends only on the initial and final states. The scenario where it works is a process called partial state merging (PSM). Here we take the name partial state merging that is somewhat different from the original one in [14]. The situation of PSM is depicted in Fig. 2: Initially, AA' is with Alice and BB' with Bob, E is with the merging center, and the whole state $\Phi_{AA'BB'E}$ is pure. The task is to transfer A and B to the center while the final state remains the same. There is infinite entanglement and an ideal quantum channel between Alice (Bob) and the center. But no entanglement and no channel exist between Alice and Bob. No classical communication is allowed between Alice (Bob) and the center. To accomplish the task, the minimal net flow of qubits to the center is none other than $Q = \frac{1}{2} \times \{I(AA':BB') - I(A':B')\}$, where the flow into the center is regarded as positive flow while that out is negative. There
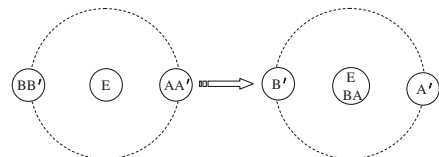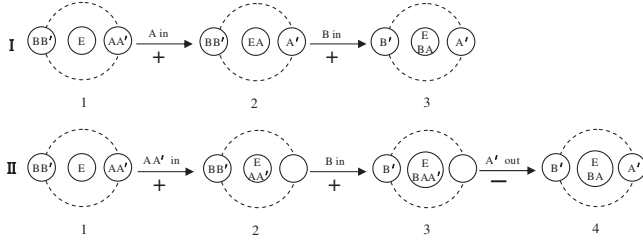

FIG. 1.   Quantum state redistribution.

FIG. 2.   Partial state merging.

FIG. 3.   Two typical routes.

FIG. 4.   Partial state merging and partial state distribution.

are many different routes to merge A and B. Dramatically, the net flow is a conservative quantity independent of the different routes of merging. Without loss of generality, we take the two typical routes in Fig. 3 to show this. In routes I and II, the net flow of qubits to E is calculated as

$$Q_{\rm I} = 1/2\{I(BB':A|E) + I(A':B|EA)\}$$
$$= 1/2\{I(AA':BB') - I(A':B')\},$$
$$Q_{\rm II} = 1/2\{I(BB':AA') + 0 - I(A':B')\},$$

where the relation $S(X) = S(Y)$ is used when XY is in a pure state. Of course, there are other routes; however, the net flow to the center is the same.

Given the operational meaning of the quantity $Q = \frac{1}{2} \times \{I(AA':BB') - I(A':B')\}$, we immediately obtain the operational meaning of E_I.

Proposition 2.—For a given mixed state ρ_{AB} to be merged to a center, the conditional entanglement of mutual information is the minimal net flow of qubits to the center with the optimal side information $\rho_{A'B'}$.

Notice that, for separable state ρ_{AB}, there always exist the side information $\rho_{A'B'}$ such that the net flow of qubits to the center is zero. The more entangled ρ_{AB} is, the greater is the flow of qubits to the merging center.

The result and conclusion can be straightforwardly generalized to the multipartite case where the multipartite version of E_I is defined as $E_I = \inf\frac{1}{2}\{I_n(A_1A_1':\cdots:A_nA_n') - I_n(A_1':\cdots:A_n')\}$, and $I_n = \sum_i S(A_i) - S(A_1 \ldots A_n)$ is the multipartite mutual information [20].

Proposition 3.—The conditional entanglement for multipartite mutual information is additive:

$$E_I(\rho_{A_1 \ldots A_n} \otimes \sigma_{B_1 \ldots B_n}) = E_I(\rho_{A_1 \ldots A_n}) + E_I(\sigma_{B_1 \ldots B_n}).$$

Proposition 4.—For a multipartite mixed state $\rho_{A_1 \ldots A_n}$ to be merged to a center, the conditional entanglement of mutual information is the minimal net flow of qubits to the center with the optimal side-information $\rho_{A_1' \ldots A_n'}$.

One can check that $Q = \frac{1}{2}\{I(AA':BB') - I(A':B')\}$ is also the quantity that describes the flow of qubits out of the center in the process of partial state distribution (PSD) that is the reversed process of PSM. In Fig. 4, we depict the two reversible processes for a tripartite state. It is easy to see that the factor $1/2$ remains throughout calculating the flow of qubits. This gives an operational ground that the factor is $1/2$ even f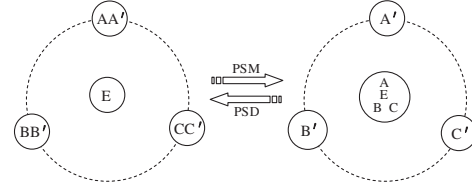or multipartite entanglement. Notice that if only the monotonicity under LOCC is required, the factor can be taken, for example, $1/n$ for the n-partite case that is also reduced to the same formula for bipartite case. However, it does not match the operational meaning.

In summary, we have constructed an additive entanglement measure—conditional entanglement of mutual information—and elaborated its operational meaning. The conclusions have been generalized to multipartite entanglement, with an additive and operational multipartite entanglement measure being provided for the first time.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, arXiv:quant-ph/0702225 [Rev. Mod. Phys. (to be published)].
[2] M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007).
[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[4] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[5] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2001).
[6] J. Oppenheim, arXiv:0801.0458v1.
[7] M. Christandl and A. Winter, J. Math. Phys. (N.Y.) **45**, 829 (2004).
[8] K. Życzkowski *et al.*, Phys. Rev. A **58**, 883 (1998).
[9] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).
[10] K. G. H. Vollbrecht and R. F. Werner, Phys. Rev. A **64**, 062307 (2001).
[11] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989).
[12] A measure of correlations is required at least to be non-increasing under local operations; see [13].
[13] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[14] M. Horodecki, J. Oppenheim, and A. Winter, Nature (London) **436**, 673 (2005).
[15] D. Yang, M. Horodecki, and Z. D. Wang, arXiv:quant-ph/0701149.
[16] M. B. Plenio, Phys. Rev. Lett. **95**, 090503 (2005).
[17] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[18] I. Devetak and J. Yard, arXiv:quant-ph/0612050v1.
[19] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, arXiv:quant-ph/0606225v1.
[20] R. Horodecki, Phys. Lett. A **187**, 145 (1994).