Monogamy of quantum entanglement and other correlations

Masato Koashi[1,2,*] and Andreas Winter[1,3,†]
[1]*Department of Computer Science, University of Bristol, Bristol BS8 1UB, United Kingdom*
[2]*CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences, The Graduate University for Advanced Studies (SOKENDAI), Hayama, Kanagawa 240-0193, Japan*
[3]*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
(Received 7 October 2003; published 18 February 2004)

It has been observed by numerous authors that a quantum system being entangled with another one limits its possible entanglement with a third system: this has been dubbed the "monogamous nature of entanglement." In this paper we present a simple identity which captures the trade off between entanglement and classical correlation, which can be used to derive rigorous monogamy relations. We also prove various other trade offs of a monogamy nature for other entanglement measures and secret and total correlation measures.

DOI: 10.1103/PhysRevA.69.022309 PACS number(s): 03.67.Mn

I. INTRODUCTION

One of the fundamental differences between classical correlations and quantum correlations is in their sharability among many parties. Classical correlations can be shared among many parties, while quantum ones cannot be freely shared. For example, if a pair of two-level quantum systems A and B have a perfect quantum correlation, namely, if they are in a maximally entangled state $|\Psi^-\rangle \equiv (|01\rangle - |10\rangle)/\sqrt{2}$, then the system A cannot be entangled to a third system C. This indicates that there is a limitation in the distribution of entanglement, and many researches have been devoted to capture this unique property, dubbed the "monogamy of quantum entanglement," in a quantitative way [1–4]. On the other hand, the above example also suggests a slightly different limitation on the two types of correlations. Note that system A cannot even be classically correlated to system C if AB is maximally entangled. Here a perfect quantum correlation excludes the possibility of classical correlations to other systems. One can also see that a perfect classical correlation between A and B will forbid system A from being entangled to other systems.

In this paper, we first show (Sec. II) that this mutually exclusive property can be cast into a simple equality. The derivation is straightforward once we choose suitable measures for the quantum correlation (entanglement cost) and for the classical correlation (one-way distillable common randomness). The equality also indicates a close connection between the two (apparently different) measures. We may say that the two measures are complementary to each other. In particular, the question of additivity of one measure can be reduced to that of the other. We also derive an inequality describing a limitation on the distribution of entanglement. Then, in Sec. III, we explore mutual limitations between more general measures of correlation: entanglement cost, general distillable entanglement, "squashed entanglement" [5], and distillable secret key.

*Electronic address: koashi@soken.ac.jp
†Electronic address: a.j.winter@bris.ac.uk

II. ENTANGLEMENT VERSUS CLASSICAL CORRELATION

Entanglement cost [6] is an operationally defined measure of bipartite entanglement. It connects an arbitrary bipartite state ρ_{AB} over system A and B to a standard bipartite state $(|01\rangle - |10\rangle)/\sqrt{2}$ which we call a singlet. Suppose that we want to prepare n pairs of systems in state $\rho_{AB}^{\otimes n}$ by local operations and classical communication (LOCC), using a resource of m singlets. The entanglement cost E_C of ρ_{AB} is defined as the infimum of the ratio m/n in the asymptotic limit $n \to \infty$, under the condition that the errors in the preparation should vanish in the same limit. It was shown [6] that E_C is equal to the regularized entanglement of formation E_f [7], namely,

$$E_C(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n}).$$

The entanglement of formation E_f is defined by

$$E_f(\rho_{AB}) = \lim_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\mathrm{Tr}_B[|\psi_i\rangle\langle\psi_i|]), \tag{1}$$

where $S(\rho)$ is the von Neumann entropy of density operator ρ and the minimum is taken over all ensembles $\{p_i, |\psi_i\rangle\}$ satisfying $\Sigma_i p_i |\psi_i\rangle\langle\psi_i| = \rho_{AB}$. The entanglement cost does not depend on whether the classical communication is allowed in both directions or restricted to one direction.

A convincing operational measure of the classical correlation inherent in a bipartite quantum state has been proposed only recently by Devetak and Winter [8] (but see also the recent work of Oppenheim and Horodecki [9] based on a thermodynamical idea, as well as Refs. [10] and [11] which adopt an approach via secret key rates). They consider the optimum amount of the perfect classical correlation that can be extracted from a bipartite state ρ_{AB}, measured in the number of maximally correlated classical bits ($r$bits). One problem in this approach is that if no communication is allowed, there is no way to produce a perfect correlation even if we weaken the restriction to an "almost perfect" correlation in the asymptotic sense. They thus considered the case where C $r$bits are extracted from ρ_{AB} via R bits of noiseless classical communication between A and B. Noting that R bits of noiseless classical communication can produce R $r$bits of classical correlation by itself, the net contribution of the state ρ_{AB} is $(C-R)$ $r$bits. This quantity should be optimized over R and over various protocols. Considering the n states $\rho_{AB}^{\otimes n}$, an asymptotic measure of distillable common randomness C_D is thus defined as the supremum of $(C-R)/n$ in the limit $n\to\infty$. Devetak and Winter have derived the formula for C_D when the classical communication is restricted in one direction. When the direction is from B to A, the distillable common randomness $C_D^{\leftarrow}$ is given by

$$C_D^{\leftarrow}(\rho_{AB})=\lim_{n\to\infty}\frac{1}{n}I^{\leftarrow}(\rho_{AB}^{\otimes n}).$$

Here the function $I^{\leftarrow}$, which was proposed by Henderson and Vedral [12], is defined by

$$I^{\leftarrow}(\rho_{AB})=\max_{\{M_x\}}\left[S(\rho_A)-\sum_x p_x S(\rho_x)\right]=:\max I(X;A),$$

where the maximum is taken over all the measurements $\{M_x\}$ applied on system B, $p_x\equiv\mathrm{Tr}[(\mathbb{1}_A\otimes M_x)\rho_{AB}]$ is the probability of the outcome x, $\rho_x\equiv\mathrm{Tr}_B[(\mathbb{1}_A\otimes M_x)\rho_{AB}]/p_x$ is the state of system A when the outcome was x, and $\rho_A\equiv\mathrm{Tr}_B(\rho_{AB})$. The right-hand side in the first line is the Holevo quantity, for which the second line introduces a notation. This measure is asymmetric, and $C_D^{\leftarrow}(\rho_{AB})\neq C_D^{\rightarrow}(\rho_{AB})$ in general; in the classical case however, they coincide and are equal to the mutual information [13].

In order to connect the above two measures, let us introduce a duality relation among bipartite states. We say that the state $\rho_{AB'}$ is the B complement to ρ_{AB} when there exists a tripartite pure state $\rho_{ABB'}$ such that $\mathrm{Tr}_B(\rho_{ABB'})=\rho_{AB'}$ and $\mathrm{Tr}_{B'}(\rho_{ABB'})=\rho_{AB}$. As is obvious from the definition, $\rho_{AB'}$ is the B complement to ρ_{AB} if and only if ρ_{AB} is the B' complement to $\rho_{AB'}$. The state B complement to ρ_{AB} is unique up to local unitary operations on system B', namely, any two states $\rho_{AB'}$ and $\rho'_{AB'}$ that are B complement to the same state ρ_{AB} are connected by a unitary operation $U_{B'}$ on system B' as $\rho_{AB'}=(\mathbb{1}_A\otimes U_{B'})\rho'_{AB'}(\mathbb{1}_A\otimes U_{B'}^{\dagger})$. Now we can prove the following.

Theorem 1. When $\rho_{AB'}$ is the B complement to ρ_{AB},

$$E_f(\rho_A)+I^{\leftarrow}(\rho_{AB'})=S(\rho_A) \tag{2}$$

and

$$E_C(\rho_{AB})+C_D^{\leftarrow}(\rho_{AB'})=S(\rho_A), \tag{3}$$

where $\rho_A\equiv\mathrm{Tr}_B(\rho_{AB})=\mathrm{Tr}_{B'}(\rho_{AB'})$.

Proof. Let $\rho_{ABB'}$ be the pure state satisfying $\mathrm{Tr}_B(\rho_{ABB'})=\rho_{AB'}$ and $\mathrm{Tr}_{B'}(\rho_{ABB'})=\rho_{AB}$. Take an ensemble $\{p_i,|\psi_i\rangle\}$ achieving the minimum in Eq. (1). Since $\Sigma_i p_i|\psi_i\rangle\langle\psi_i|=\rho_{AB}$, there exists a measurement $\{\tilde{M}_i\}$ on system B' such that, if applied on state $\rho_{ABB'}$, the outcome i occurs with probability p_i, leaving the state of A and B in $|\psi_i\rangle$. If we neglect system B, this implies that if we apply $\{\tilde{M}_i\}$ on state $\rho_{AB'}$, the outcome i occurs with probability p_i, leaving the state of A in $\mathrm{Tr}_A[|\psi_i\rangle\langle\psi_i|]$. From the definition of $I^{\leftarrow}$, we have

$$\begin{aligned}I^{\leftarrow}(\rho_{AB'})&\geq S(\rho_A)-\sum_i p_i S(\mathrm{Tr}_A[|\psi_i\rangle\langle\psi_i|])\\&=S(\rho_A)-E_f(\rho_{AB}).\end{aligned} \tag{4}$$

Conversely, take a measurement $\{M_i\}$ on system B' achieving the maximum in the definition of $I^{\leftarrow}$, namely, $I^{\leftarrow}(\rho_{AB'})=S(\rho_A)-\Sigma_i p_i S(\rho_i)$. The rank of the operator M_i may be larger than one in general, so take a decomposition $M_i=\Sigma_j M_{ij}$ into rank-1 nonnegative operators M_{ij}. This gives a new measurement $\{M_{ij}\}$ on system B'. Let $p_{ij}\equiv\mathrm{Tr}[(\mathbb{1}_A\otimes M_{ij})\rho_{AB}]$ and $\rho_{ij}\equiv\mathrm{Tr}_B[(\mathbb{1}_A\otimes M_{ij})\rho_{AB}]/p_{ij}$. These are related to p_i and ρ_i as $p_i=\Sigma_j p_{ij}$ and $p_i\rho_i=\Sigma_j p_{ij}\rho_{ij}$. From the concavity of the von Neumann entropy, we have $S(\rho_A)-\Sigma_{ij}p_{ij}S(\rho_{ij})\geq S(\rho_A)-\Sigma_i p_i S(\rho_i)=I^{\leftarrow}(\rho_{AB'})$. The definition of $I^{\leftarrow}$ leads to the opposite inequality, and we thus have $S(\rho_A)-\Sigma_{ij}p_{ij}S(\rho_{ij})=I^{\leftarrow}(\rho_{AB'})$. Suppose that the measurement $\{M_{ij}\}$ is applied to the pure state $\rho_{ABB'}$. The probability of the outcome ij is given by p_{ij} defined above. When the outcome is ij, the state of AB becomes a pure state $|\phi_{ij}\rangle$, since M_{ij} is rank-1. We thus obtain an ensemble $\{p_{ij},|\phi_{ij}\rangle\}$ satisfying $\Sigma_{ij}p_{ij}|\phi_{ij}\rangle\langle\phi_{ij}|=\rho_{AB}$. If we neglect system B, the situation is identical to the case where $\{M_{ij}\}$ is applied to $\rho_{AB'}$. This implies that $\mathrm{Tr}_B[|\phi_{ij}\rangle\langle\phi_{ij}|]=\rho_{ij}$. Therefore,

$$\begin{aligned}E_f(\rho_{AB})&\geq\sum_{ij} p_{ij}S(\mathrm{Tr}_B[|\phi_{ij}\rangle\langle\phi_{ij}|])\\&=\sum_{ij} p_{ij}S(\rho_{ij})\\&=S(\rho_A)-I^{\leftarrow}(\rho_{AB'}).\end{aligned} \tag{5}$$

Equation (2) is proved by combining Eqs. (4) and (5). In order to derive Eq. (3), note that $\rho_{AB'}^{\otimes n}$ is the B complement to $\rho_{AB}^{\otimes n}$ because $\rho_{ABB'}^{\otimes n}$ is a purification of either of the states. Therefore, by the additivity of von Neumann entropy, $E_f(\rho_{AB}^{\otimes n})+I^{\leftarrow}(\rho_{AB'}^{\otimes n})=S(\rho_A^{\otimes n})=nS(\rho_A)$. Dividing by n and taking the limit $n\to\infty$, we obtain Eq. (3). ■

In order to represent the mutually exclusive property of classical and quantum correlations, let us consider a general tripartite mixed state ρ_{ABC}. We can always find a pure state ρ_{ABCD} on the four systems, such that $\mathrm{Tr}_D(\rho_{ABCD})=\rho_{ABC}$. Regarding systems C and D as a single system B', we can apply theorem 1 to obtain $E_f(\rho_{AB})+I^{\leftarrow}(\rho_{A(CD)})=S(\rho_A)$. It is straightforward to show $I^{\leftarrow}(\rho_{A(CD)})\geq I^{\leftarrow}(\rho_{AC})$ from the definition of $I^{\leftarrow}$. We thus obtain the following corollary.

Corollary 2. For any tripartite state ρ_{ABC},

$$E_f(\rho_{AB})+I^{\leftarrow}(\rho_{AC})\leq S(\rho_A) \tag{6}$$

and

$$E_C(\rho_{AB})+C_D^{\leftarrow}(\rho_{AC})\leqslant S(\rho_A). \tag{7}$$

The equality in each of the relations holds if ρ_{ABC} is pure.■

This corollary will be interpreted as follows. The local entropy $S(\rho_A)$ represents the effective size of the system A measured in qubits. This view is justified by the existence of a compression scheme [14] that transfers the contents of system A into $S(\rho_A)$ qubits per copy while retaining any correlation to other systems asymptotically faithfully. This size will be understood as the capacity of system A to make correlations to other systems. Here we are asking how one can correlate system A to system B and to system C at the same time, under the condition that the size of system A is limited to $S(\rho_A)$ qubits. The corollary states that the quantum correlation to one system and the classical correlation to the other system must use up this limited capacity of system A in a mutually exclusive way, namely, the two correlations cannot share the same fraction of the capacity. In other words, the existence of a certain amount of quantum (classical) correlation to one system is sufficient to restrict the classical (quantum) correlation to other systems by the same amount. One curious property stated in the corollary is that it is also necessary to restrict the correlations to other systems. This results from the fact that the inequalities are saturated whenever ρ_{ABC} is pure. Forming a quantum (classical) correlation to system A is the only way to assure that the classical (quantum) correlation between A and other systems is smaller than is available by the size of system A.

The last property gives us an operational definition of the amount of entanglement in reference to classical resources, rather than to quantum ones such as singlets. Considering that what we can directly ''perceive'' is only the classical quantity, it is natural to seek a tighter connection between entanglement and classical correlations. Bell's inequalities may serve as a tool for that purpose, but we do not know yet how to measure the amount of violation of Bell's inequalities in a satisfactory way, nor how to use Bell's inequalities to distinguish the states with bound entanglement from the separable ones. Here we can define the amount of entanglement in a bipartite state ρ_{AB} as follows. Consider any purification ρ_{ABC} of ρ_{AB}. The entanglement is defined as the difference between two values of one-way distillable common randomness as $E(\rho_{AB})\equiv C_D^{\leftarrow}(\rho_{A(BC)})-C_D^{\leftarrow}(\rho_{AC})$, where $C_D^{\leftarrow}(\rho_{A(BC)})$ represents the one-way distillable common randomness between A and the combined system of B and C, and $C_D^{\leftarrow}(\rho_{AC})$ represents the one between A and C. The amount $C_D^{\leftarrow}(\rho_{A(BC)})-C_D^{\leftarrow}(\rho_{AC})$ corresponds to the reduction in the amount of distillable classical correlations caused by the omission of system B. Since $C_D^{\leftarrow}(\rho_{A(BC)})=S(\rho_A)$, it follows from Eq. (3) that $E(\rho_{AB})=E_C(\rho_{AB})$. Thus the two measures coincide, but note that $E(\rho_{AB})$ is in the unit of $r$bits, while $E_C(\rho_{AB})$ is in the unit of $e$bits.

Since the von Neumann entropy satisfies the additivity $S(\rho\otimes\rho')=S(\rho)+S(\rho')$, theorem 1 implies that the sum of $E_f(\rho_{AB})$ and $I^{\leftarrow}(\rho_{AB'})$ is additive. Thus the additivity of one implies that of the other, namely, $E_f(\rho_{A_1B_1}\otimes\rho_{A_2B_2})=E_f(\rho_{A_1B_1})+E_f(\rho_{A_2B_2})$ holds if and only if $I^{\leftarrow}(\rho_{A_1B_1'}\otimes\rho_{A_2B_2'})=I^{\leftarrow}(\rho_{A_1B_1'})+I^{\leftarrow}(\rho_{A_2B_2'})$, where $\rho_{A_jB_j'}$ is the B_j complement to $\rho_{A_jB_j}$. Indeed, a similar relation holds for E_C and $C_D^{\leftarrow}$. The problem of the (super)additivity of the one-way distillable common randomness is thus dual to the problem of the (sub)additivity of entanglement cost or entanglement of formation. In particular, we can export the known results [15] about the additivity of entanglement of formation and cost to that of distillable common randomness through the duality of B-complement states.

One may wonder why a symmetric measure E_C and an asymmetric measure $C_D^{\leftarrow}$ are connected as in Eq. (3). Let us introduce the one-way entanglement cost $E_C^{\rightarrow}(\rho_{AB})$, which is defined as the entanglement cost when we restrict the classical communication to be one way from A to B. Then, we can regard Eq. (3) as resulting from the two equations $E_C^{\rightarrow}(\rho_{AB})+C_D^{\leftarrow}(\rho_{AB'})=S(\rho_A)$ and $E_C^{\rightarrow}(\rho_{AB})=E_C^{\leftarrow}(\rho_{AB})=E_C(\rho_{AB})$. The former connects two asymmetric measures as one would expect, and the latter refers to a symmetry lying in the quantum theory. Due to the presence of this symmetry, Eq. (3) happens to take an anomalous form. We can also state this symmetry in terms of one-way distillable common randomness, in the following corollary that is easily derived from theorem 1.

Corollary 3. When $\rho_{AB'}$ is the B complement to ρ_{AB},

$$S(\rho_B)-C_D^{\rightarrow}(\rho_{AB})=S(\rho_{B'})-C_D^{\rightarrow}(\rho_{AB'}).$$

This is because both the left- and the right-hand sides are equal to $E_C(\rho_{BB'})$. ■

The mutual exclusiveness between classical and quantum correlations is by itself a property that is symmetric between the two types of correlations. The difference between the two correlations—the classical correlations can be freely shared, but the quantum ones cannot—arises from the following asymmetry. The two systems can have classical correlations without having any quantum correlations, but the converse is not true. It would be interesting to find an inequality representing the converse property, namely, to find an upper bound on the amount of quantum correlations for a given amount of classical correlations. Combined with Eq. (7), such an inequality will give us a general inequality expressing the monogamy of entanglement. As an example, here we prove the following inequality.

Proposition 4.

$$C_D^{\leftarrow}(\rho_{AB})\geqslant E_D^{\leftarrow}(\rho_{AB}), \tag{8}$$

where $E_D^{\leftarrow}(\rho_{AB})$ is the one-way distillable entanglement of state ρ_{AB}.

Namely, consider any purification $|\psi\rangle_{ABE}$ of ρ_{AB}, and any measurement on B which will result in a random variable X and post-measurement states on A and E. Then clearly,

$$I(X;A)\geqslant I(X;A)-I(X;E).$$

But according to Ref. [8] the maximum of the left-hand side over all measurements (regularized) equals $C_D^{\leftarrow}(\rho_{AB})$, while the same maximum (regularized) of the right-hand side is the secret key distillable by one-way discussion [11] $C_{\text{secret}}^{\leftarrow}(\psi_{ABE})$. (In secret key capacities, the indices, in this order, represent the first legitimate party, the second legitimate party, and the eavesdropper.) On the other hand, it is obvious that $C^{\leftarrow}_{\text{secret}}(\psi_{ABE}) \geq E^{\leftarrow}_{D}(\rho_{AB})$ since one can create one bit of secret key from one ebit of distilled entanglement. (It is also directly obtained by looking at the formulas derived in Ref. [11].) Putting together these estimates gives Eq. (8). ■

Combining Eq. (8) of proposition 4 with Eq. (7) of corollary 2, we obtain a new inequality describing the monogamy of entanglement.

Theorem 5.

$$E_C(\rho_{AB}) + E^{\leftarrow}_{D}(\rho_{AC}) \leq S(\rho_A), \tag{9}$$

for any state ρ_{ABC}. ■

III. OTHER CORRELATIONS

In the previous section, an inequality [Eq. (9)] describing the monogamy of entanglement has been derived from a close connection between two measures of bipartite correlations. In this section, we approach the monogamy of entanglement through completely different arguments. We are particularly interested in a family of inequalities in the form

$$E(\rho_{AB}) + E(\rho_{AC}) \leq E(\rho_{A(BC)}), \tag{10}$$

where $E(\rho_{AB})$ is a measure of correlation between systems A and B. In the following, we prove that the above form of inequality is true for the one-way distillable entanglement, the one-way distillable secret key, and the squashed entanglement.

Before doing so, it will be worthwhile noting that not all the entanglement measures satisfy the inequality (10). In particular, it does not hold for the entanglement cost, as seen by the following example. Consider the purification of the totally antisymmetric state on a two-qutrit system

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{6}}(|123\rangle - |132\rangle + |231\rangle - |213\rangle + |312\rangle - |321\rangle).$$

Note that all its two-party restrictions (in particular to AB and to AC) are isomorphic to the totally antisymmetric state, for which the entanglement of formation and entanglement cost are known to be 1 $e$bit [16]. Hence we have $E_C(\rho_{A(BC)}) = S(\rho_A) = \log_2 3 < 1+1 = E_C(\rho_{AB}) + E_C(\rho_{AC})$. This counterexample also implies that the monogamy inequality (9) derived in the previous section cannot be superseded by an inequality of the form (10).

An inequality in the form (10) has a natural interpretation when the measure E represents the optimal yield of distillation protocols. If an optimal protocol between A and B and an optimal protocol between A and C can be carried out simultaneously without interference, the combined protocol gives an yield $E(\rho_{AB}) + E(\rho_{AC})$, and hence the inequality (10) holds. This is indeed true for the one-way distillable entanglement. The argument is as follows: Let us introduce a purification of the state ρ_{ABC} on a system E, such that we can phrase everything in terms of a global pure state. B and C can both independently perform their halves of their respective protocols with A and send her (A) their classical messages. Clearly, then, A can complete the distillation of entanglement between her and B by a local unitary U, leaving the whole system in (a high-fidelity approximation of) the state $|\Phi_K\rangle_{AB} \otimes |\Psi\rangle_{A'CE}$. After this, she could reverse the action of U by applying U^{-1}, and apply another local unitary V, to complete the distillation of entanglement between her and C, leaving the whole system in (a high-fidelity approximation of) the state $|\Phi_L\rangle_{AC} \otimes |\Theta\rangle_{A'BE}$. Of course, after this naive protocol, we could not find the state $|\Phi_K\rangle_{AB}$ anywhere. Observe, however, that since after the first step AB is disentangled from the rest of the world, VU^{-1} could as well be applied with a "dummy state" $|\Phi_K\rangle_{\tilde{A}\tilde{\tilde{A}}}$ (totally in the possession of A) instead of $|\Phi_K\rangle_{AB}$, with the same resulting maximally entangled state $|\Phi_L\rangle_{AC}$ between A and C. Thus, A can extract both maximally entangled states with B and C at the same time. This operational argument proves the following inequality.

Theorem 6.

$$E^{\leftarrow}_{D}(\rho_{AB}) + E^{\leftarrow}_{D}(\rho_{AC}) \leq E^{\leftarrow}_{D}(\rho_{A(BC)}), \tag{11}$$

for any state ρ_{ABC}.

This inequality can also be derived using a formula for $E^{\leftarrow}_{D}(\rho_{AB})$, which has recently been established by proving the "hashing inequality" [11]. Let us define the quantity

$$E^{\leftarrow(1)}_{D}(\rho_{AB}) \equiv \sup \sum_i p_i [S(\rho^{(i)}_{A}) - S(\rho^{(i)}_{AB})],$$

where the supremum is taken over all the local instruments carried out by B. The quantity p_i is the probability of having classical outcome i when the instrument is applied on state ρ_{AB}, and $\rho^{(i)}_{AB}$ is the state left by the instrument. Then, the formula is written as

$$E^{\leftarrow}_{D}(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E^{\leftarrow(1)}_{D}(\rho^{\otimes n}_{AB}).$$

From the strong subadditivity [17], we have

$$S(\rho_A) - S(\rho_{AB}) + S(\rho_A) - S(\rho_{AC}) \leq S(\rho_A) - S(\rho_{ABC}).$$

Then, the derivation of Eq. (11) is straightforward by noting that carrying out a local instrument on B and another on C can be regarded together as a local instrument on BC. ■

Following the analogy between entanglement and shared secret key (such as the monogamy, observed by numerous authors: a good sample is provided by Refs. [18,11,19]), it is possible to apply a similar argument to the case of the one-way distillable secret key. Before that, a few remarks will be helpful regarding the relation between the distillable secret key and the entanglement. The secret key $C_{\text{secret}}(\psi_{ABE})$ distillable from the pure state $|\psi\rangle_{ABE}$ by public (two-way) dissussion between A and B against an eavesdropper E can be regarded as a function of the marginal state $\rho_{AB} = \mathrm{Tr}_E(|\psi\rangle\langle\psi|_{ABE})$. This function is easily checked to be a proper entanglement monotone, hence can be regarded as a measure of entanglement. This measure lies between the distillable entanglement and the entanglement cost, namely,

$$E_D(\rho_{AB}) \leqslant C_{\text{secret}}(\psi_{ABE}) \leqslant E_C(\rho_{AB}).$$

The lower bound is obvious, and the upper bound comes from the fact that the entanglement of formation $(1/n)E_f(\rho_{AB}^{\otimes n})$ can be shown to be an upper bound by the following operational argument. An eavesdropper holding the E part of n copies of $|\psi\rangle_{ABE}$ can, by a suitable measurement, effect any pure state decomposition of the state shared between A and B and will only help them by announcing her measurement result; hence the distillable key length is upper bounded by the average of the distillable key lengths for these pure states, which is easily seen to be equal to their respective entropy of entanglement. Observe that this upper bound was recently improved in Ref. [19], where it was shown that C_{secret} is in fact upper bounded by the regularized relative entropy of entanglement (against separable states) [20]. The technique is very interesting in the present context: the key point is expressing secret key distillation as a distillation problem involving LOCC. With these remarks the following should not come as too big a surprise.

We prove that an inequality of the form (10) is true for $E(\rho_{A(BC)}) = C_{\text{secret}}^{\leftarrow}(\psi_{A(BC)E})$, namely,

Theorem 7.

$$C_{\text{secret}}^{\leftarrow}(\psi_{AB(CE)}) + C_{\text{secret}}^{\leftarrow}(\psi_{AC(BE)}) \leqslant C_{\text{secret}}^{\leftarrow}(\psi_{A(BC)E}).$$

In fact, even the stronger inequality

$$C_{\text{secret}}^{\leftarrow}(\rho_{ABE}) + C_{\text{secret}}^{\leftarrow}(\rho_{AC(BE)}) \leqslant C_{\text{secret}}^{\leftarrow}(\rho_{A(BC)E}) \quad (12)$$

holds for any four-partite state ρ_{ABCE}.

As in the case of the one-way distillable entanglement, we can prove the inequality by showing that two distillation protocols can be carried out at the same time. The protocols achieving the key rates $C_{\text{secret}}^{\leftarrow}(\rho_{ABE})$ (between B and A) and $C_{\text{secret}}^{\leftarrow}(\rho_{AC(BE)})$ (between C and A) can be integrated in one protocol in which B and C independently perform their local operations, and send public messages to A. She then completes first the protocol with B—by the protocol in Ref. [11], in which she in fact "decodes with high probability" the secret key already held by B, hence by the gentle measurement principle she will induce only little disturbance to her state. This means she then can also complete the protocol with C with high fidelity of success. By definition of the protocol she ends up with key shared with B (secret against E) and key shared with C (secret against BE). The fact that the latter one is secret against B ensures that the two keys are (almost) independent. Thus A and BC can obtain a secret key of length $C_{\text{secret}}^{\leftarrow}(\rho_{ABE}) + C_{\text{secret}}^{\leftarrow}(\rho_{AC(BE)})$ against E if B and C cooperate.

Again, as in the case of the one-way distillable entanglement, we can also prove Eq. (12) by the formula for $C_{\text{secret}}^{\leftarrow}(\rho_{ABE})$ derived in Ref. [11], namely,

$$C_{\text{secret}}^{\leftarrow}(\rho_{ABE}) = \lim_{n\to\infty} \frac{1}{n} C_{\text{secret}}^{\leftarrow(1)}(\rho_{ABE}^{\otimes n})$$

with

$$C_{\text{secret}}^{\leftarrow(1)}(\rho_{ABE}) \equiv \max[I(X;A) - I(X;E)],$$

where the maximum is taken over all measurements at B (result X). Then, the left-hand side of Eq. (12) is (the regularization of) the maximum of

$$[I(X;A) - I(X;E)] + [I(Y;A) - I(Y;BE)]$$

over all measurements at B (result X) and measurements at C (result Y). On the other hand, we have

$$\begin{aligned} I(X;A) - I(X;E) + I(Y;A) - I(Y;BE) & \\ &\leqslant I(X;A) - I(X;E) + I(Y;AX) - I(Y;EX) \\ &= I(X;A) + I(Y;A|X) - I(X;E) - I(Y;E|X) \\ &= I(XY;A) - I(XY;E), \end{aligned}$$

where the last line, again by the formula, is upper bounded by $C_{\text{secret}}^{\leftarrow}(\rho_{A(BC)E})$, the right-hand side of Eq. (12). ■

As a special case of Eq. (12), we can derive a monogamy relation involving common randomness and secret key. By setting system E as a trivial one (and by swapping notations B and C), we obtain

$$C_{\text{secret}}^{\leftarrow}(\rho_{ABC}) + C_D^{\leftarrow}(\rho_{AC}) \leqslant C_D^{\leftarrow}(\rho_{A(BC)}).$$

Finally, we show that the inequality of the form (10) is true for the so-called "squashed entanglement" [5]

$$E_{\text{sq}}(\rho_{AB}) = \inf\left\{\frac{1}{2} I(A;B|E) : \rho_{AB} = \mathrm{Tr}_E(\rho_{ABE})\right\},$$

where the infimum is over all extensions ρ_{ABE} of the state ρ_{AB} (i.e., states whose partial trace over E is ρ_{AB}), and

$$I(A;B|E) = S(\rho_{AE}) + S(\rho_{BE}) - S(\rho_{ABE}) - S(\rho_E)$$

is the conditional quantum mutual information. For it we can prove the following.

Theorem 8. For any tripartite state ρ_{ABC},

$$E_{\text{sq}}(\rho_{AB}) + E_{\text{sq}}(\rho_{AC}) \leqslant E_{\text{sq}}(\rho_{A(BC)}). \quad (13)$$

Using the chain rule for the (conditional) mutual information with any state extension ρ_{ABCE}:

$$\begin{aligned} \frac{1}{2} I(A;BC|E) &= \frac{1}{2} I(A;B|E) + \frac{1}{2} I(A;C|BE) \\ &\geqslant E_{\text{sq}}(\rho_{AB}) + E_{\text{sq}}(\rho_{AC}), \end{aligned}$$

since E extends AB and BE extends AC. As this is true for every state extension of ρ_{ABC} we obtain the claim. ■

While no operational interpretation has so far been found for the squashed entanglement, the above inequality has an interesting corollary for operationally defined measures of entanglement. This comes from the property that E_{sq} is lower bounded by E_D (distillation under bidirectional protocols) and upper bounded by E_C [5]. As a consequence, we obtain the following from Eq. (13).

Corollary 9.

$$E_D(\rho_{AB})+E_D(\rho_{AC})\leqslant E_C(\rho_{A(BC)}), \tag{14}$$

for any state ρ_{ABC}.

Note that this is in no relation of dependence with Eq. (11): there both the left- and the right-hand sides can be smaller since we use one-way distillation.

IV. DISCUSSION

In this paper we have contributed to an understanding of the monogamy of quantum entanglement by casting it into a variety of quantitative trade offs between measures of entanglement and more general correlation measures. All these are of the form of an upper bound on the sum of a correlation measure for *A*-*B* and (maybe another measure) for *A*-*C* for a tripartite state on *ABC*. This trade off assumes the very pleasing form of a complementarity identity for entanglement cost and one-way distillable classical correlation, linking these two quantities and showing that their additivity problems are equivalent: this extends Shor's recent list of four equivalent additivity questions [21] to five entries. It would be interesting to find an operational proof for theorem 1, which here we have proved using only formal properties of the definitions of E_f and $I^{\leftarrow}$.

We then went on to exploit our relation to study other trade offs involving further entanglement and correlation measures: we gave an example that the entanglement cost does not obey a symmetric trade off, but showed that the squashed entanglement does—which leads to our only example of a mutual trade off for correlation measures based on distillation under bidirectional communication. For measures based on optimal yields under unidirectional communication, we derived monogamy relations through an operational argument, and also gave an alternative proof based on the basic properties of entropic functions.

There are a number of open questions regarding the possibility of other inequalities. Along the line discussed in Sec. II, an important question is whether one can replace $S(\rho_A)$ in the inequality (7) by a correlation measure between *A* and *BC* that is equal to $S(\rho_A)$ whenever ρ_{ABC} is pure [for example, the entanglement cost $E_C(\rho_{A(BC)})$]. For inequalities in the form (10) in Sec. III, interesting cases will be $E(\rho_{AB})=E_D^{\rightarrow}(\rho_{AB})$, $E(\rho_{AB})=E_D(\rho_{AB})$, and similar ones for the secret key. A crucial difference here is that, for a similar operational argument to be carried out, one must show that the party *A* can increase the expected coherent information between *A* and *B* by a measurement, without contaminating the correlation between *A* and *C*. It is not clear, and is an interesting question, whether this is always true or not.

ACKNOWLEDGMENT

A.W. was supported by the U.K. Engineering and Physical Sciences Research Council.

[1] D. Bruß, Phys. Rev. A **60**, 4344 (1999); W. Dür, G. Vidal, and J. I. Cirac, *ibid.* **62**, 062314 (2000); M. Koashi, V. Bužek, and N. Imoto, *ibid.* **62**, 050302 (2000); K. A. Dennison and W. K. Wootters, *ibid.* **65**, 010301R (2001); A. Higuchi and A. Sudbery, Phys. Lett. A **273**, 213 (2000).

[2] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[3] M. Fannes, J. T. Lewis, and A. Verbeure, Lett. Math. Phys. **15**, 255 (1988); G. A. Raggio and R. F. Werner, Helv. Phys. Acta **62**, 980 (1989).

[4] B. M. Terhal, quant-ph/0307120 (unpublished).

[5] M. Christandl and A. Winter, quant-ph/0308088 (unpublished).

[6] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2001).

[7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); **78**, 2031(E) (1997); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[8] I. Devetak and A. Winter, quant-ph/0304196 (unpublished).

[9] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **89**, 180402 (2002); M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, *ibid.* **90**, 100402 (2003); M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0302129 (unpublished).

[10] R. Wilmink, Ph.D. thesis, Bielefeld, Germany, 2003. Available at the following URL: http://www.mathematik.uni-bielefeld.de/~rwilmink/dissertation.pdf

[11] I. Devetak and A. Winter, quant-ph/0306078 (unpublished); M. Horodecki and P. Horodecki (unpublished).

[12] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).

[13] R. Ahlswede and I. Csiszár, IEEE Trans. Inf. Theory **39**, 1121 (1993).

[14] B. Schumacher, Phys. Rev. A **51**, 2738 (1995); R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994).

[15] C. King, J. Math. Phys. **43**, 1247 (2002); **43**, 4641 (2002); P. W. Shor, *ibid.* **43**, 4334 (2002); G. Vidal, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **89**, 027901 (2002); K. Matsumoto, T. Shimono, and A. Winter, quant-ph/0206148 (unpublished).

[16] F. Yura, J. Phys. A **36**, L237 (2003).

[17] E. H. Lieb and M. B. Ruskai, J. Math. Phys. **14**, 1938 (1973).

[18] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).

[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0309110 (unpublished).

[20] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[21] P. W. Shor, quant-ph/0305035 (unpublished).