Conjectured Strong Complementary Information Tradeoff

Joseph M. Renes[1] and Jean-Christian Boileau[2]

[1]*Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstrasse 4a, 64289 Darmstadt, Germany*
[2]*Center for Quantum Information and Quantum Control, University of Toronto, Toronto, Ontario, M5S 1A7 Canada*

(Received 1 July 2008; published 9 July 2009)

We conjecture a new entropic uncertainty principle governing the entropy of complementary observations made on a system given side information in the form of quantum states, generalizing the entropic uncertainty relation of Maassen and Uffink [Phys. Rev. Lett. **60**, 1103 (1988)]. We prove a special case for certain conjugate observables by adapting a similar result found by Christandl and Winter pertaining to quantum channels [IEEE Trans. Inf. Theory **51**, 3159 (2005)], and discuss possible applications of this result to the decoupling of quantum systems and for security analysis in quantum cryptography.

DOI: 10.1103/PhysRevLett.103.020402 PACS numbers: 03.65.Ta, 03.67.Dd

One of the central mysteries of quantum mechanics is complementarity, the strange phenomenon that a given physical attribute can only be exhibited at the expense of another, complementary, attribute. The canonical example, wave-particle duality, is illustrated in the double slit experiment. Coherent light (or matter) traveling through both slits produces an interference pattern, a wavelike property which is, however, destroyed if one determines which path has been taken, a particlelike property. Such behavior vividly differentiates quantum from classical mechanics and led Feynman to famously observe that the double slit experiment ''has in it the heart of quantum mechanics'' [1].

The new field of quantum information theory takes a pragmatic approach to the mysteries of quantum mechanics, seeking to better understand them by asking which information processing tasks can or cannot be accomplished in this new arena. The results have been stunning. Quantum information cannot be copied but can be ''teleported'' from place to place. It can be used to improve the precision of everything from clock synchronization to gravitational-wave detectors to lithography. It can dramatically speed up certain computational tasks, such as searching an unordered list and factoring large integers. Quantum information cannot, however, be shared between many parties. For instance, maximal entanglement can be shared by only two parties, and entangling more parties means making the entanglement between any two of them weaker. This effect also enables cryptographic tasks which are impossible classically, such as unconditionally secure key exchange. This property of exclusiveness or privacy informs many aspects of how we reason about quantum information and quantum information processing [2].

The connection between complementarity and privacy stems from the entropic uncertainty relation due to Maassen and Uffink [3], then successively extended by Hall [4] and Cerf *et al.* [5]. The original version constrains the entropies of two noncommuting observables O^A and $\tilde{O}^A$ of a system A, and the latter versions extend this to explicitly include classical side information about the observables, stored either jointly in one external system R (Hall) or separately in two, B and E (Cerf *et al.*). These external systems might, for example, be ancillary systems used in von Neumann measurement processes, possibly of O^A or $\tilde{O}^A$ or both. Giving the B and E systems to parties Bob and Eve, respectively (the names are chosen in anticipation of the cryptographic implications to follow), the complementarity statement of Cerf *et al.* says that the information one party (Bob) could obtain about one observable (O^A) by measuring his system B, plus the information Eve could obtain about the other observable ($\tilde{O}^A$) by measuring E, cannot exceed a prescribed bound. Equivalently, one can say that there is a certain unavoidable amount of uncertainty or entropy about the two observables conditioned on respective measurements of the two systems B and E.

In this Letter we generalize the tradeoff to restrict the amount of conditional entropy the parties can have about noncommuting observables on A when they possess *quantum* side information. Quantum and classical side information behave differently and, in particular, the information represented by the quantum state may be significantly larger than the amount of classical information that can be extracted from it by measurement, a statement known as the Holevo bound [2,6]. Relatedly, classical side information is subject to *locking*, meaning that a modest amount of additional classical side information can greatly increase the total [7]. Quantum side information, in contrast, cannot be locked in this manner. We find numerical evidence for the generalized tradeoff for arbitrary observables and provide a proof for conjugate observables [8] related by a Fourier transform based on the proof of a related entropic inequality for quantum channels given by Christandl and Winter [9].

We then exhibit a family of states which saturate the bound before discussing some applications of our result. Building on [9,10], we derive a rigorous statement of the idea that if the AB system has nearly maximal quantum correlations, as measured by appropriately small quantum conditional entropies, then the AE system is nearly decoupled, i.e., in a product state. This is akin to the monog-

amy of entanglement, the fact that maximal entanglement cannot be shared by more than two parties, at the level of quantum correlations. In the context of quantum cryptography, this means composable security—that the key generated in quantum key distribution is secure in any further cryptographic application [11,12]—can be established by bounding the information that the (quantum) system B has on a basis conjugate to the basis of A used to encode the key.

Basic entropic uncertainty principles.—We begin by reviewing the existing entropic uncertainty principles. For a physical system A, consider any two observables O^A and $\tilde{O}^A$ represented by operators on a finite-dimensional Hilbert space. Let $c = \max_{jk} |\langle j|\tilde{k}\rangle|$, where $|j\rangle$ and $|\tilde{k}\rangle$ are the eigenvectors of O^A and $\tilde{O}^A$, respectively. Define $H(O^A)_\rho$ and $H(\tilde{O}^A)_\rho$ to be the respective Shannon entropies of the outcome probabilities of the measurements of O^A and $\tilde{O}^A$ on a given state ρ^A. Maassen and Uffink [3] showed that regardless of ρ^A,

$$H(O^A)_\rho + H(\tilde{O}^A)_\rho \geq -2\log_2 c, \tag{1}$$

meaning the entropies of observables sharing no common eigenstates cannot both be arbitrarily small. The constant c can be as large as $\log_2 d^A$, for d^A the dimension of the Hilbert space describing system A, and is exactly $\log_2 d^A$ if and only if the observables are *conjugate*. For conjugate observables, certainty regarding one observable implies complete uncertainty regarding the other.

Suppose now that we have some side information or background information relevant to A, for instance the result of measurement on some external system R which is correlated with A. Intuitively, the entropic uncertainty relation should still hold, since this information would simply factor into the description ρ^A of A. Indeed, the entropic uncertainty principle can be adapted to this case, and is equivalent to a result by Hall which he terms the information-exclusion principle [4]. Its derivation proceeds as follows.

Consider an arbitrary bipartite quantum state ρ^{AR} where A and R are two finite-dimensional Hilbert spaces. Let Γ^R be a positive operator-valued measure representing an arbitrary measurement on the system R (i.e., $\sum_j \Gamma_j^R = \mathbb{1}^R$ and $\Gamma_j^R \geq 0$ for all j). Measurement of Γ^R gives the outcome j with probability $q_j = \mathrm{Tr}[\rho^{AR}\Gamma_j^R]$, and leaves the marginal state of A given by $\rho_j^A := \frac{1}{q_j}\mathrm{Tr}_R[\rho^{AR}\Gamma_j^R]$ [13]. Applying the inequality Eq. (1) to each of the states ρ_j gives $H(O^A)_{\rho_j} + H(\tilde{O}^A)_{\rho_j} \geq -2\log_2 c$, where the entropies are computed using the conditional state ρ_j. Since this state is determined by the classical outcome of measurement on R, we can write $H(O^A)_{\rho_j}$ as $H(O^A|\Gamma_j^R)_\rho$ and likewise for observable $\tilde{O}^A$, where $H(O^A|\Gamma_j^R)_\rho$ is the conditional entropy of the O^A observable given the result of the Γ^R measurement. Averaging over all outcomes yields the information-exclusion principle:

$$H(O^A|\Gamma^R)_\rho + H(\tilde{O}^A|\Gamma^R)_\rho \geq -2\log_2 c. \tag{2}$$

This equation is particularly useful if we consider R to be a composite system, consisting of subsystems B and E, and Γ^R to be a composite measurement $\Gamma_{jk}^R = \Lambda_j^B \otimes \tilde{\Lambda}_k^E$, as put forth in [5]. Since conditioning reduces entropy, one obtains a tradeoff in the amount of information about O^A and $\tilde{O}^A$ which can be simultaneously stored in *separate* auxiliary systems B and E. We call this the (weak) complementary information tradeoff (CIT):

$$H(O^A|\Lambda^B)_\rho + H(\tilde{O}^A|\tilde{\Lambda}^E)_\rho \geq -2\log_2 c. \tag{3}$$

Now the information held by one party, in possession of system B, say, limits the information which another party could in principle obtain about a noncommuting observable. This tradeoff is immediately applicable in quantum cryptography, and in [14] we used it to motivate a new approach to the distillation of entanglement and secret keys. Our present goal is to find a stricter tradeoff.

Strong complementary information tradeoff.—What if we regard the quantum state of the auxiliary system itself as the side information? Is there any limit to the uncertainty of complementary observables in this case? One might conjecture that the quantum version of Eq. (2) holds, replacing the conditional Shannon entropy $H(O^A|\Gamma^R)$ with the conditional von Neumann entropy $S(O^A|R)_\rho = S(\rho_{O^A}^{AR}) - S(\rho^R)$, where $\rho_{O^A}^{AR}$ is the quantum state obtained after measuring the observable O on the state ρ and averaging over all outcomes. However, this is false in general. To take an extreme example, the singlet state of two spin-$\frac{1}{2}$ particles is perfectly anticorrelated in every basis, meaning that $S(O^A|R) = S(\tilde{O}^A|R) = 0$ for *any* nondegenerate observables. This is merely the statement that quantum correlations, in the form of entanglement, are stronger than classical correlations.

Instead, the conjecture should be applied to the weak CIT, Eq. (3), and the result is the strong CIT:

$$S(O^A|B)_\rho + S(\tilde{O}^A|E)_\rho \geq -2\log_2 c. \tag{4}$$

The strong CIT immediately implies the weak CIT via the Holevo bound $S(O^A|\Gamma^B) \geq S(O^A|B)$ for any measurement Γ [2,6], and also the original entropic uncertainty principle by taking B and E to be one dimensional.

The claim is supported by numerical investigation of small dimensions d_A, d_B, $d_E \leq 12$, which has found no counterexample when testing at least 2000 random states in each of the 11^3 combinations of dimensions. By itself this is relatively weak evidence, but for conjugate observables O^A, $\tilde{O}^A$ related by a Fourier transform, e.g., $\tilde{O}^A = F^A O^A F^{A\dagger}$, Eq. (4) follows from strong subadditivity (SSA) of the von Neumann entropy. Assuming that the eigenvectors of O^A define a standard basis, we can redefine the eigenvalues of the observables so that $O \to Z = \sum_k \omega^k |k\rangle\langle k|$ and $\tilde{O} \to X = \sum_k |k+1\rangle\langle k|$, where $\omega = e^{2\pi i/d}$, the generalized Pauli operators [15]. Then the vari-

ous properties of X and Z can be used to construct a proof, in a manner entirely similar to [9], who establish a similar tradeoff for the ability of a quantum channel to transmit conjugate information. In the present context, the proof goes as follows.

Proof of special case.—Consider any ρ^{ABE} where $\dim(A) = d$. We can assume that ρ^{ABE} is a pure state without loss of generality, since E can always be redefined to include the purification. As a consequence of SSA, the value of $S(O^A|E)_\rho$ cannot be increased by enlarging E (cf. [2], Theorem 11.15). So if the inequality is true for any pure state then it must also be true for any mixed state. Using the properties of X and Z one can write $\bar{\rho}^{ABE}_{X^A} = \frac{1}{d}\sum_k X^A_k \rho^{ABE} X^{\dagger A}_k$ and $\bar{\rho}^{ABE}_{Z^A} = \frac{1}{d}\sum_k Z^A_k \rho^{ABE} Z^{\dagger A}_k$. Here we have used a nonstandard notation, defining $X^A_k := (X^A)^k$ and $Z^A_k := (Z^A)^k$. Now let $\rho^{ABE}_{jk} := X^A_j Z^A_k \rho^{ABE} Z^{\dagger A}_k X^{\dagger A}_j$ and define

$$\Omega^{A'B'AB} := \frac{1}{d^2}\sum_{jk} P^{A'}_j \otimes P^{B'}_k \otimes \rho^{AB}_{jk}, \tag{5}$$

for $P_j = |j\rangle\langle j|$. A' and B' are two new systems such that $\dim(A') = \dim(B') = d$. The sum of j and k is understood to be over all values from 1 to d. Direct calculation shows that

$$S(A'|AB)_\Omega = S(\bar{\rho}^{AB}_{Z^A}) - S(\rho^B) = S(Z^A|B)_\rho, \tag{6}$$

$$S(B'|AB)_\Omega = S(\bar{\rho}^{AB}_{X^A}) - S(\rho^B) = S(X^A|B)_\rho, \tag{7}$$

$$S(A'B'|AB)_\Omega = \log_2 d + S(A|B)_\rho. \tag{8}$$

Strong subadditivity is just the statement that $S(A'B'|AB) \le S(A'|AB) + S(B'|AB)$ (cf. [2], Theorem 11.16), so

$$S(Z^A|B)_\rho + S(X^A|B)_\rho \ge \log_2 d + S(A|B)_\rho. \tag{9}$$

Define the probability distribution p_k and quantum states $|\varphi_k\rangle^{BE}$ such that $|\rho\rangle^{ABE} = \sum_k \sqrt{p_k}\,|k\rangle^A|\varphi_k\rangle^{BE}$. Using $S(\bar{\rho}^{AB}_{Z^A}) = H(p_k) + \sum_k p_k S(\varphi^B_k) = H(p_k) + \sum_k p_k S(\varphi^E_k) = S(\bar{\rho}^{AE}_{Z^A})$, a simple calculation reveals that $S(Z^A|B)_\rho - S(Z^A|E)_\rho = S(A|B)_\rho$ and hence for an arbitrary pure ρ^{ABE},

$$S(X^A|B)_\rho + S(Z^A|E)_\rho \ge \log_2 d. \qquad \square$$

Saturating the bound.—Since the bound relies solely on SSA, saturating the bound means fulfilling the SSA equality conditions. A useful form of these is given in [16], which states in the present case that the AB state space must decompose as $\mathcal{H}^{AB} \simeq \bigoplus_s \mathcal{H}^{L_s} \otimes \mathcal{H}^{R_s}$, so that

$$\Omega^{A'B'AB} = \bigoplus_s r_s \sigma^{A'L_s} \otimes \omega^{B'R_s} \tag{10}$$

for some states $\sigma^{A'L_s}$, $\omega^{B'R_s}$ and probabilities r_s. Projecting $A'B'$ onto the jkth outcome gives $\rho_{jk} = d^2 \bigoplus_s r_s \sigma^{L_s}_j \otimes \omega^{R_s}_k$, where $\sigma^{L_s}_j = \mathrm{Tr}[P^{A'}_j \sigma^{A'L_s}]$ and similarly for $\omega^{R_s}_k$. Thus, the action of X^A_j and Z^A_k on ρ^{AB} must be on different subsystems within each s sector.

One way to arrange for this is to take ρ^{AB} to be one of the Bell states $|\Phi_{jk}\rangle^{AB} = \frac{1}{\sqrt{2}} X^B_j Z^B_k (|00\rangle + |11\rangle)^{AB}$. Then there is only one s sector, and the spaces $\mathcal{H}^L$, $\mathcal{H}^R$ are two dimensional, so that $|\Phi_{jk}\rangle \simeq |jk\rangle$. Bell states saturate the bound in the most trivial manner possible: both $S(X^A|B)$ and $S(Z^A|B) = 0$.

A more interesting example is afforded by the state $|\psi\rangle^{ABE} = \frac{1}{\sqrt{d}}\sum_k |k\rangle^A|\varphi_k\rangle^{BE}$, where we set $|\varphi_k\rangle^{BE} = \sum_{uv} \sqrt{q_{uv}}\,|u\rangle^B |\eta_{uv}\rangle^{E_1} Z^{E_2}_k |v\rangle^{E_2}$ with arbitrary states $|\eta_{u,v}\rangle$ and distribution q_{uv}. Here the entropies $S(X^A|B)$ and $S(Z^A|E)$ do not necessarily take on extremal values, but their counterparts $S(Z^A|B)$ and $S(X^A|E)$ do. For starters, $S(Z^A|B) = \log_2 d$ since φ^B_k is independent of k. Meanwhile, $S(X^A|E) = 0$ can be quickly derived by making the substitution $|k\rangle^A Z^{E_2}_k |v\rangle^{E_2} = Z^A_v |k\rangle^A |v\rangle^{E_2}$ in the definition of $|\psi\rangle$. Thus, the ρ^{AB}_{jk} derived from $|\psi\rangle$ meet the equality conditions, and therefore $S(X^A|B) + S(Z^A|E) = \log_2 d$.

In more concrete terms, the ρ^{AB}_{jk} meet the equality conditions because $\psi^{AB} = \sum_v q_v \tilde{P}^A_v \otimes \xi^B_v$, with $\xi^B_v = \sum_{uu'} \sqrt{q_{u|v} q_{u'|v}} \langle \eta_{uv}|\eta_{u'v}\rangle |u\rangle\langle u'|^B$. Thus, the action of X^A_j has no effect on ψ^{AB}, as it is already diagonal in the X^A basis. Therefore we need only keep one s sector and can dispense entirely with $\mathcal{H}^{L_s}$ in the decomposition of ρ^{AB}_{jk}, setting $\mathcal{H}^{R_s} = \mathcal{H}^{AB}$. It remains an open question whether any state can saturate the bound $S(X^A|B) + S(Z^A|E) \ge \log_2 d$ and its counterpart $S(Z^A|B) + S(X^A|E) \ge \log_2 d$ without taking on extremal values in either case.

Privacy criterion.—An immediate application of the strong CIT is in bounding the correlations between two systems A and E, possessed by Alice and Eve, respectively, using the known correlations between A and B, possessed by Bob. The weak form can also be used for this purpose, but the types of correlations that can be bounded are weaker as we now explain.

Consider the state ρ^{ABE} and suppose that there exists a measurement $\tilde{\Lambda}^B$ such that $H(\tilde{O}^A|\tilde{\Lambda}^B)_\rho \le \epsilon$. This implies $H(O^A|\Lambda^E)_\rho \ge -2\log_2 c - \epsilon$, or equivalently, $I(O^A{:}\Lambda^E) \le \epsilon + H(O^A)_\rho + 2\log_2 c$. Supposing further that $H(O^A)_\rho \le -2\log_2 c$, as would necessarily be the case for conjugate observables, we obtain a bound on Eve's information about O^A: $I(O^A{:}\Lambda^E) \le \epsilon$. Applied to a quantum key distribution scenario where Alice's key is given by the measurement of the observable O^A, this ensures a certain level of privacy of the key [5]. However, due to locking, this security criterion is not *universally composable* [17], meaning that the key cannot be safely used in arbitrary further cryptographic protocols. For a precise definition of universal composability and an exhaustive explanation on why a suitable security criterion should be composable, see [11,12].

On the other hand, the strong CIT *can* be used to obtain a composable security criterion. The same conditions as above now imply that the eavesdropper's Holevo informa-

tion is small, $I(O^A{:}E) \leq \epsilon$, which is a composable security criterion [11]. We can use the strong CIT to give an even more direct statement, in the form of sufficient conditions for decoupling Alice from Eve.

Decoupling theorem.—Suppose ρ^{ABE} is a tripartite state subject to the conditions $S(\rho^A) \leq -2\log_2 c$, $S(O^A|B)_\rho \leq \epsilon_1$, and $S(\tilde{O}^A|B)_\rho \leq \epsilon_2$. Then

$$\mathrm{Tr}\,|\rho^{AE} - \rho^A \otimes \rho^E| \leq 2\sqrt{\epsilon_1 + \epsilon_2}. \tag{11}$$

Proof.—The proof assumes that the strong CIT holds for the observables O^A and $\tilde{O}^A$. Observe that the mixed state case follows from the pure state case since the trace distance cannot increase when removing the purifying system. Thus, we can assume that ρ^{ABE} is a pure state. Then a straightforward calculation reveals that $S(\tilde{O}^A|E)_\rho = S(A|E)_\rho + S(\tilde{O}^A|B)_\rho$, using the fact that given the value of $\tilde{O}^A$, the entropy of Eve's state is identical to the entropy of Bob's state. Using this to substitute for $S(\tilde{O}^A|E)_\rho$ in the strong complementary information tradeoff, the three given conditions yield $S(\rho^A) - S(A|E)_\rho \leq \epsilon_1 + \epsilon_2$. This can be written as $S(\rho^{AE}||\rho^A \otimes \rho^E) \leq \epsilon_1 + \epsilon_2$, and since the relative entropy and the trace distance are related by $(\mathrm{Tr}|\rho^{AE} - \rho^A \otimes \rho^E|)^2 \leq 4S(\rho^{AE}||\rho^A \otimes \rho^E)$ [18], this concludes the proof. □

This theorem makes rigorous the intuition that full quantum correlations, in the sense of small quantum conditional entropy, between two systems A and B is equivalent to being decoupled from any other system E. The same intuition has different, though related, rigorous expressions. When thinking of quantum correlations as entanglement, this goes under the heading of monogamy of entanglement [19]. Or, instead of using quantum mutual information, one can imagine there exist measurements on B which could predict both the outcome of X^A and Z^A, and the same sort of decoupling result holds [14,20].

Conclusion.—We have proposed a tradeoff in the amount of information simultaneously available about complementary observables, formulated in terms of the quantum conditional entropy. It can be seen as the natural extension of the reformulation by Cerf *et al.* of the information-exclusion principle and the entropic uncertainty principle. It is also the "static" version, applicable to quantum states, of Christandl and Winter's "dynamic" conjugate information tradeoff, which is formulated for quantum channels. The proof of the latter leads immediately to a proof of the strong complementary information tradeoff, and numerical investigation reveals that the tradeoff appears to hold for arbitrary observables. We have also discussed conditions under which the tradeoff can be saturated, as well as described some applications to quantum cryptography and derived a decoupling criterion for quantum states.

It would be interesting to determine if a similar bound holds for the smoothed conditional max entropies and/or max entropies, which are generalizations of the classical Renyi entropes of order ∞ and $1/2$, respectively, and have direct operational interpretations [21]. They are often relevant in studying information processing protocols at the single-shot rather than asymptotic level, and are therefore more fundamental. Note that the original derivation of Maassen and Uffink already gives the unconditional result $H_{\min} + H_{\max} \geq -2\log_2 c$.

The authors acknowledge fruitful discussions with Gernot Alber, Matthias Christandl, Robert König, and Stephanie Wehner. J. C. B. received support from NSERC and Quantumworks.

[1] R. P. Feynman, *Feynman Lectures on Physics* (Addison Wesley, Longman, 1970).
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
[3] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[4] M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1995).
[5] N. J. Cerf *et al.*, Phys. Rev. Lett. **88**, 127902 (2002).
[6] A. S. Holevo, Prob. Peredachi Inf. **9**, 3 (1973).
[7] D. P. DiVincenzo *et al.*, Phys. Rev. Lett. **92**, 067902 (2004).
[8] Two observables are *conjugate* if each of the eigenvectors of one is an equal-weight superposition of all the eigenvectors of the other observable.
[9] M. Christandl and A. Winter, IEEE Trans. Inf. Theory **51**, 3159 (2005).
[10] P. Hayden, P. W. Shor, and A. Winter, Open Syst. Inf. Dyn. **15**, 71 (2008).
[11] M. Ben-Or *et al.*, in *Second Theory of Cryptography Conference* (Springer, Cambridge, MA, 2005), Vol. 3378, pp. 386–406.
[12] R. Renner and R. König, in Ref. [11], pp. 407–425.
[13] Note that Hall simply starts with the ensemble $\mathcal{E} = \{q_j, \rho_j^A\}$, whereas here it arises from measurement of R.
[14] J. M. Renes and J.-C. Boileau, Phys. Rev. A **78**, 032335 (2008).
[15] These operators are not Hermitian, but as only the eigenvectors concern us here, this is of no consequence.
[16] P. Hayden *et al.*, Commun. Math. Phys. **246**, 359 (2004).
[17] R. König *et al.*, Phys. Rev. Lett. **98**, 140502 (2007).
[18] M. Ohya and D. Petz, *Quantum Entropy and Its Use* (Springer-Verlag, Berlin, 1993).
[19] M. Koashi and A. Winter, Phys. Rev. A **69**, 022309 (2004).
[20] M. Koashi, arXiv:0704.3661v1.
[21] R. König, R. Renner, and C. Schaffner, arXiv:0807.1338v1.