## **Optimal Compression for Identically Prepared Qubit States**

Yuxiang Yang, <sup>1</sup> Giulio Chiribella, <sup>1,2,\*</sup> and Masahito Hayashi<sup>3,4</sup>

<sup>1</sup>Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong

<sup>2</sup>Canadian Institute for Advanced Research, CIFAR Program in Quantum Information Science, Toronto, Ontario M5G 1Z8, Canada

<sup>3</sup>Graduate School of Mathematics, Nagoya University, Nagoya, Japan

<sup>4</sup>Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore

(Received 9 June 2016; published 25 August 2016)

We establish the ultimate limits to the compression of sequences of identically prepared qubits. The limits are determined by Holevo's information quantity and are attained through use of the optimal universal cloning machine, which finds here a novel application to quantum Shannon theory.

DOI: 10.1103/PhysRevLett.117.090502

Introduction.—A fundamental feature distinguishing quantum states from classical probability distributions is the freedom in the choice of basis, which can be used to encode information even when the spectrum of the state is fixed. States with fixed spectrum can be used, for instance, as indicators of spatial directions [1,2], probes for frequency estimation [3,4], or even pieces of cryptocurrency [5]. Because of Holevo's bound [6], the basis information cannot be extracted from a single quantum particle, but becomes accessible when multiple copies of the same quantum state are available. Suppose that a sender wants to transmit to a receiver the information contained in a sequence of n identically prepared particles. In this scenario, an important question is how to minimize the amount of quantum bits (qubits) used in the transmission, subject to the requirement that the initial n-particle state can be approximately rebuilt at the receiver's end.

The compression of identically prepared states has been theoretically studied [7] and experimentally implemented [8] in the pure state case. For mixed states, two of us proposed a protocol [9] that compresses states with fixed spectrum and variable basis. The protocol encodes nidentically prepared qubits into a memory of  $3/2 \log n$ qubits, which is proven to be the smallest memory size when the decoder is bound by the conservation of the total angular momentum. Whether lifting the angular momentum constraint allows for further compression has remained an open problem so far. Moreover, little is known in the case where no prior information is available on the spectrum. Finding the optimal compression protocol for general quantum states is important for applications (where the spectrum may be unknown) and for the foundations of quantum theory, because it provides a characterization of the different information content of quantum states and classical probability distributions.

In this Letter we identify the optimal compression protocols for sequences of identically prepared qubits. We first consider states with known spectrum, devising a compression protocol that stores a sequence of *n* qubits into a memory of log n qubits, the ultimate limit set by Holevo's  $\chi$  quantity [6]. The memory reduction from  $3/2 \log n$  to  $\log n$  qubits is accomplished through a novel application of the optimal universal cloning machine [10–12], here used to modulate the values of the total angular momentum. On average, the modulation is of size  $\sqrt{n}$  and its logarithm is exactly the amount of memory saved by our protocol, compared to the optimal protocol with angular momentum preserving decoder [9]. We then address a new compression scenario where no prior information about the state is given. For this scenario, called full-model compression, we devise a protocol that uses a hybrid memory of  $\log n$  qubits and  $1/2 \log n$ classical bits. The protocol is optimal; in fact, no further compression can be achieved even if the hybrid memory is replaced by a fully quantum memory. The main result of the Letter is summarized by the following theorem:

**Theorem 1.** A sequence of n identically prepared qubit states can be optimally compressed into  $\log n$  qubits if the spectrum is known and into  $\log n$  qubits plus  $1/2 \log n$  classical bits if the spectrum is unknown.

Comparing the two protocols, we identify  $\log n$  qubits as the amount of information contained in the choice of basis and  $1/2 \log n$  bits as the information contained in the spectrum. This interpretation is consistent with the fact that  $1/2 \log n$  is the number of bits needed to faithfully compress n independent samples of a classical probability distribution over the binary set  $\{0,1\}$  [13].

Compression protocol for known spectrum.—Consider the compression of n qubits, independently prepared in the state  $\rho_g = g\rho g^\dagger$ , where  $\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$  is a fixed density matrix and  $g \in SU(2)$  is a variable unitary matrix implementing a change of basis. Without loss of generality, we assume  $p \ge 1/2$  (the case p < 1/2 is automatically accounted for by the change of basis). Using the Schur-Weyl duality [14], the state of the n qubits can be written in the block diagonal form

$$\rho_g^{\otimes n} = \bigoplus_{J=0}^{n/2} q_J \left( \rho_{g,J} \otimes \frac{I_{m_J}}{m_J} \right), \tag{1}$$

where the equality holds up to a global unitary transformation, known as the Schur transform and efficiently implementable on a quantum computer [15]. In Eq. (1), J is the quantum number of the total angular momentum [16],  $q_J$  is a probability distribution,  $\rho_{g,J}$  is a density matrix with support in an irreducible space  $\mathcal{R}_J$ , and  $I_{m_J}$  is the identity matrix on an  $m_J$ -dimensional multiplicity space  $\mathcal{M}_J$  [14]. The state  $\rho_{g,J}$  can be expressed in the Gibbs form [17]

$$\rho_{g,J} = \frac{e^{-\beta H_{g,J}}}{\text{Tr}[e^{-\beta H_{g,J}}]}, \qquad \beta = 2 \tanh^{-1}(2p - 1),$$

$$H_{g,J} = U_{g,J} \left( \sum_{m=-J}^{J} -m|J,m\rangle\langle J,m| \right) U_{g,J}^{\dagger}, \tag{2}$$

where  $\{|J,m\rangle\}_{m=-J}^{J}$  are the eigenstates of the z component of the angular momentum operator and  $U_{g,J}$  is the unitary matrix representing the change of basis g in the irreducible space  $\mathcal{R}_{J}$ .

We now show how to optimally compress the states  $\rho_g^{\otimes n}$ . In general, a compression protocol consists of two components: the encoder, which stores the input state into a memory, and the decoder, which attempts to reconstruct the input state from the state of the memory. The encoder and the decoder are both represented by completely positive trace preserving linear maps (also known as quantum channels) [18]. Therefore, a quantum compression protocol is specified by a couple  $(\mathcal{E}, \mathcal{D})$ , consisting of the encoding and the decoding channel, respectively. The performance of the protocol is determined by the tradeoff between two quantities: the memory size, quantified by the dimension  $d_{\text{enc}}$  of the memory's Hilbert space, and the compression error, measured by the worst-case trace distance between the initial state and the state recovered from the memory

$$\epsilon = \max_{g \in SU(2)} \frac{1}{2} \| \mathcal{D} \circ \mathcal{E}(\rho_g^{\otimes n}) - \rho_g^{\otimes n} \|_1, \tag{3}$$

with  $||A||_1 := \text{Tr}\sqrt{A^{\dagger}A}$ . The key issue is to minimize the memory size, while guaranteeing that the compression error vanishes in the large n limit.

The optimal protocol is based on two ingredients: The first is the concentration of the probability distribution  $q_J$  in Eq. (1). Explicitly, the probability is given by [9]

$$q_{J} = \frac{2J+1}{2J_{0}} \left[ B\left(\frac{n}{2} + J + 1\right) - B\left(\frac{n}{2} - J\right) \right]$$
 (4)

where B(k) is the binomial distribution with n+1 trials and probability p and  $J_0 \coloneqq (p-1/2)(n+1)$  is close to the average value  $\langle J \rangle = \sum_J J q_J$ . From the above expression it is clear that the values of J with  $|J-J_0| \gg \sqrt{n}$  have exponentially small probability in the large n limit. As a result, the performance of a compression protocol depends only on its action on the subspaces  $\mathcal{R}_J \otimes \mathcal{M}_J$  that satisfy the condition  $|J-J_0| = O(\sqrt{n})$ .

The second ingredient of our compression protocol is a remarkable property of the optimal universal cloning machine (UCM) [11,12]. Mathematically, the UCM is described by a map transforming (operators supported in) the symmetric subspace of 2J qubits into (operators supported in) the symmetric subspace of 2K qubits. Here we allow J to be larger than K, in which case the "cloning" process just consists in getting rid of 2(J - K) qubits. With this convention, the cloning channel is

$$C_{J\to K}(\rho) = \begin{cases} \left(\frac{2J+1}{2K+1}\right) P_K(\rho \otimes P_{K-J}) P_K & J \leq K \\ \operatorname{Tr}_{2(J-K)}[\rho] & J > K \end{cases}$$
(5)

where  $P_x$  is the projector on the symmetric subspace of 2x qubits and  $Tr_x$  denotes the partial trace over the first x qubits. The key to our compression protocol is to regard the Gibbs states in Eq. (2) as states on the symmetric subspace of 2J qubits and to observe that UCM has the following property [19]:

**Lemma 1.** Universal cloning as a Gibbs state adapter. The universal cloning channel  $\mathcal{C}_{J\to K}$  transforms the Gibbs state  $\rho_{q,J}$  into the Gibbs state  $\rho_{q,K}$  with error

$$\|\mathcal{C}_{J\to K}(\rho_{a,J}) - \rho_{a,K}\|_{1} \le \delta^{1-s} + O(\delta),$$
 (6)

where s > 0 is an arbitrary constant and  $\delta := |J - K|/J$ .

This result establishes a bridge between the cloning of pure states and the compression of mixed states. Leveraging on Lemma 1 and on the concentration of the probability distribution  $\{q_J\}$ , we devise the following protocol: (i). *Encoder*. Perform the Schur transform. Then, measure the quantum number J with the nondemolition measurement that preserves the quantum information in each subspace  $\mathcal{R}_J \otimes \mathcal{M}_J$ . Discard the multiplicity register and apply the cloning channel  $\mathcal{C}_{J \to J_0}$  to the remaining state  $\rho_{g,J}$ . Store the output state  $\mathcal{C}_{J \to J_0}(\rho_{g,J})$  into a quantum memory of dimension  $d_{\text{enc}} = 2J_0 + 1$ . (ii). *Decoder*. Pick a value K at random with probability  $q_K$  and apply the cloning channel  $\mathcal{C}_{J_0 \to K}$  to the quantum memory. Append a multiplicity register in the maximally mixed state  $I_{m_K}/m_K$ . Finally, perform the inverse of the Schur transform.

The protocol, illustrated in Fig. 1, is mathematically described by the channels

$$\mathcal{E}(\rho) = \sum_{J=0}^{n/2} \mathcal{C}_{J \to J_0} [\text{Tr}_{\mathcal{M}_J} (\Pi_J \rho \Pi_J)],$$

$$\mathcal{D}(\rho) = \bigoplus_{K=0}^{n/2} q_K \left[ \mathcal{C}_{J_0 \to K} (\rho) \otimes \frac{I_{m_K}}{m_K} \right], \tag{7}$$

where  $\Pi_J$  is the projector on  $\mathcal{R}_J \otimes \mathcal{M}_J$  and  $\mathrm{Tr}_{\mathcal{M}_J}$  denotes the partial trace over  $\mathcal{M}_J$ .

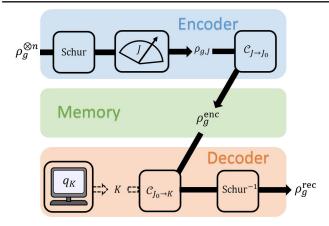


FIG. 1. Optimal compression for known spectrum and completely unknown basis. The encoder collects information from subspaces with different angular momenta and concentrates it into a system with angular momentum  $J_0$ . The decoder spreads the information back, modulating the angular momentum by  $\sqrt{n}$  units on average.

The above protocol requires a memory of  $\log(2J_0+1)=\log n+O(1)$  qubits. On the other hand, the error is arbitrarily small for large n: this is because the states  $\rho_{g,J}$  with  $|J-J_0|\gg \sqrt{n}$  have negligible probability according to Eq. (4), while the states  $\rho_{g,J}$  with  $|J-J_0|=O(\sqrt{n})$  can be faithfully encoded in the state  $\rho_{g,J_0}$ , thanks to Lemma 1 (see [19] for more details).

Optimality of the protocol with known spectrum.—Our protocol uses the minimum memory size compatible with the requirement of vanishing error. The argument goes as follows: For a generic ensemble  $\mathsf{E} = \{\rho_x, p_x\}$ , a measure of the information content is provided by Holevo's information [6]

$$\chi(\mathsf{E}) = H\left(\sum_{x} p_{x} \rho_{x}\right) - \sum_{x} p_{x} H(\rho_{x}) \tag{8}$$

where  $H(\rho)=-{\rm Tr}[\rho\log\rho]$  is the von Neumann entropy. When the ensemble E is faithfully stored in a quantum memory, the memory should be large enough to accommodate the Holevo information of E. Since a memory of dimension  $d_{\rm enc}$  can have at most a Holevo information of  $\log d_{\rm enc}$  [6], one has the bound  $\log d_{\rm enc} \geq \chi({\rm E})$ . For  $\epsilon > 0$ , an approximate version of the bound is [21]

$$\log d_{\text{enc}} \ge \chi(\mathsf{E}) - 2\epsilon \log d_{\mathsf{E}} + 2\mu(\epsilon),\tag{9}$$

where  $d_{\mathsf{E}}$  is the effective dimension, defined as the rank of the average state  $\rho_{\mathsf{E}} \coloneqq \sum_{x} p_{x} \rho_{x}$ , and  $\mu(\epsilon) \coloneqq -\epsilon \ln \epsilon$ .

Equation (9) sets a lower bound on the memory size, valid for arbitrary ensembles. However, the bound may not be tight. Notably, the bound is *not* tight for the ensembles considered in our Letter. The reason is the dimension-dependent term  $\log d_{\rm E}$ , which can be arbitrarily large: in our case, we have  $d_{\rm E}=2^n$  for  $p \neq 0$ , 1. To address this

problem, we use the notion of sufficient statistics [22]. An ensemble  $\mathsf{E}' = \{\rho_x', p_x\}$  is called a *sufficient statistics* for the ensemble  $\mathsf{E} = \{\rho_x, p_x\}$  if the states of  $\mathsf{E}$  can be encoded into states of  $\mathsf{E}'$  and decoded with zero error. Since the encoding is reversible, the ensembles  $\mathsf{E}$  and  $\mathsf{E}'$  have the same Holevo information, namely  $\chi(\mathsf{E}') = \chi(\mathsf{E})$ . Moreover, the number of qubits needed to encode the original ensemble  $\mathsf{E}$  up to error  $\epsilon$  is equal to the number of qubits needed to encode the ensemble  $\mathsf{E}'$ , up to the same error [19]. Using these facts, we can improve the bound (9), obtaining

$$\log d_{\rm enc} \ge \chi(\mathsf{E}) - 2\epsilon \log d_{\mathsf{E}}^{\rm min} + 2\mu(\epsilon),\tag{10}$$

where  $d_{\mathsf{E}}^{\min}$  is the minimum of  $d_{\mathsf{E}'}$  over all ensembles  $\mathsf{E}'$  that are sufficient statistics for  $\mathsf{E}$ . We call Eq. (10) the *Holevo bound for compression*.

Let us apply the bound to the ensemble  $\mathsf{E} = \{\rho_g^{\otimes n}, dg\}$ , where dg represents the uniform distribution over all changes of basis. For this ensemble, explicit calculation yields [19]

$$\chi(\mathsf{E}) = \log n + O(1). \tag{11}$$

A sufficient statistics for E is provided by the ensemble  $\mathsf{E}' = \{\rho'_g, dg\}$  with  $\rho'_g \coloneqq \bigoplus_{J=0}^{n/2} q_J \rho_{g,J}$ , obtained by getting rid of the multiplicity spaces in Eq. (1). The ensemble E' has effective dimension

$$d_{\mathsf{E}'} = \sum_{J=0}^{n/2} (2J+1) = \left(\frac{n}{2} + 1\right)^2,\tag{12}$$

which has been proven to be the minimum over all sufficient statistics [9,23]. Inserting Eqs. (11) and (12) into Eq. (10) we obtain the bound

$$\log d_{\text{enc}} \ge (1 - 4\epsilon) \log n - 4\epsilon - 2\mu(\epsilon) + O(1). \tag{13}$$

When  $\epsilon$  is asymptotically small, the leading term is  $\log n$ , the number of qubits used by our protocol. Hence, we conclude that the protocol is optimal and that the Holevo bound for compression is tight for the ensemble  $\mathsf{E}$ .

Compression protocol for arbitrary qubit states.—Let us now turn to the full-model compression. A simple protocol for compressing arbitrary states is to measure the magnitude of the total angular momentum, to store the outcome J in a classical memory and the state  $\rho_{g,J}$  in a quantum memory. Since J can take any value between 0 and n/2, this protocol requires  $\lceil \log(n/2+1) \rceil$  classical bits. Moreover, since  $\rho_{g,J}$  has support in a (2J+1)-dimensional space, the protocol requires  $\lceil \log(n+1) \rceil$  qubits in the worst case scenario. At first sight, it seems difficult to do any better: One cannot use less than  $\log n$  qubits, because

the input state could consist of n copies of a random pure state and no protocol can compress such a state in less than  $\log n$  qubits [9]. On the other hand, J can take n/2+1values and it is not possible to encode this information in less than  $\log n$  bits. Despite these facts, we now show that the amount of classical bits can be cut down by half with asymptotically negligible error. The key idea is that the decoder need not have full information about J: thanks to Lemma 1, two states  $\rho_{q,J}$  and  $\rho_{q,K}$  with  $|J - K| = O(\sqrt{n})$ are approximately interconvertible. Motivated by this fact, we partition the values of J into disjoint intervals  $L_1, ..., L_t$ of size  $O(\sqrt{n})$ . Instead of encoding the measurement outcome J, we compute the index i such that  $J \in L_i$  and store it in a classical memory. Since the index i can take  $O(\sqrt{n})$  values, the size of the memory is  $(1/2) \log n$ , instead of  $\log n$ . The details of the protocol are as follows: (i) Encoder. Perform the Schur transform. Then, measure the quantum number J with the nondemolition measurement that preserves the quantum information in each subspace  $\mathcal{R}_J \otimes \mathcal{M}_J$ . Find the index i(J) such that  $J \in L_{i(J)}$ . Discard the multiplicity register and send the remaining state  $\rho_{g,J}$  to the input of the quantum channel  $C_{J \to f(J)}$ , where f(J) is the median of the subset  $L_{i(J)}$ . Store the output state  $C_{J \to f(J)}(\rho_{q,J})$  in a quantum memory and the index i(J) in a classical memory. (ii) Decoder. Read the value of i(J) from the classical memory. For a given value of i(J), pick a random value K in the subset  $L_{i(J)}$  and apply the channel  $\mathcal{C}_{f(K) \to K}$  to the quantum memory. Then, append the multiplicity register in the maximally mixed state  $I_{m_K}/m_K$ . Finally, perform the inverse of the Schur transform.

The protocol is illustrated in Fig. 2. The explicit expression of the channels  $\mathcal{E}$  and  $\mathcal{D}$ , as well as the proof that the error vanishes in the large n limit can be found in [19]. Here we emphasize a few points: First, it is convenient to choose one interval—say,  $L_t$ —to contain only the value J = n/2. In this way, the protocol acts as the identity in the symmetric subspace and pure states are compressed without error. Second, random sampling in the decoder is essential for achieving vanishing error. This fact is illustrated in Fig. 3, which shows that sampling yields a wellbehaved interpolation of the spectral distribution in Eq. (4), while the lack of sampling leads to a poor approximation. Third, comparing the full model compression with the fixed-spectrum compression leads us to identify  $1/2 \log n$ bits as the amount of memory needed to store the information about the spectrum. This interpretation is consistent with the fact that  $1/2 \log n$  bits is the size of the smallest classical memory needed to faithfully store n samples of a generic probability distribution over the set  $\{0,1\}$  [13].

Optimality for the full-model compression.—The optimality of the full-model protocol can be proven with the same techniques used for fixed spectrum. In fact, an even stronger result holds: replacing the hybrid memory with a

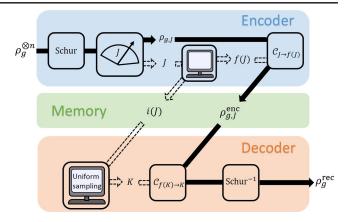


FIG. 2. Optimal full-model compression. The encoder disassembles an arbitrary sequence of n identically prepared qubits into a classical part  $(1/2 \log n)$  bits) and a quantum part  $(\log n)$  qubits). The decoder recombines these two pieces of information, approximately retrieving the initial state of the sequence.

fully quantum memory does not improve the compression, because  $3/2 \log n$  qubits is the minimum memory size allowed by the Holevo bound for compression [19].

Conclusion.—In this Letter we showed how to compress identically prepared qubits in the smallest possible memory. The key technique is the use of universal cloning to convert Gibbs states of different angular momentum. Converting Gibbs states is a novel application of quantum cloning [24–26] and may inspire further applications in the resource theory of quantum thermodynamics, both in the free [27] and in the size-restricted case [28]. Extending our results, it is also interesting to investigate the relation between cloning and compression for other families of states, such as phase [29,30] and mirror-phase [31] covariant states, and mixed states of arbitrary finite dimensional systems [9]. The recent implementations of various

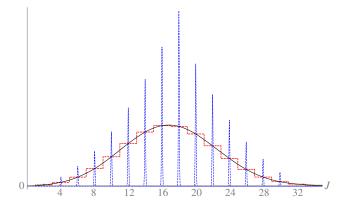


FIG. 3. Spectral distributions of the output states with and without sampling. A comparison of the spectral distributions of the following states: the original state  $\rho_g^{\otimes n}$  (black, solid line), the output state of the optimal protocol (red, dashed line), and the output state of a protocol with the same encoder of the optimal protocol and a decoder without sampling (blue, dashed line).

quantum cloning machines [32–35] suggest that prototypes of optimal compression may be experimentally demonstrated in the near future.

We acknowledge the referees of this Letter for useful suggestions that helped improve the presentation. G. C. is supported by the Canadian Institute for Advanced Research (CIFAR), by the Hong Kong Research Grant Council through Grant No. 17326616, by National Science Foundation of China through Grant No. 11675136, and by the HKU Seed Funding for Basic Research. Y. Y. is supported by a Hong Kong and China Gas Scholarship. M. H. is partially supported by a MEXT Grant-in-Aid for Scientific Research (A) No. 23246071 and the Okawa Research Grant. Centre for Quantum Technologies is a Research Centre of Excellence funded by the Ministry of Education and the National Research Foundation of Singapore. This work was completed during the "Hong Kong Workshop on Quantum Information and Foundations," organized with support from the Foundational Question Institute (FQXi-MGA-1502).

- \*Corresponding author. giulio@cs.hku.hk
- [1] E. Bagan, M. A. Ballester, R. D. Gill, A. Monras, and R. Muñoz-Tapia, Phys. Rev. A 73, 032301 (2006).
- [2] G. Chiribella, G. M. D'Ariano, C. Macchiavello, P. Perinotti, and F. Buscemi, Phys. Rev. A 75, 012315 (2007).
- [3] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. Cirac, Phys. Rev. Lett. 79, 3865 (1997).
- [4] A. Smirne, J. Kołodyński, S. F. Huelga, and R. Demkowicz-Dobrzański, Phys. Rev. Lett. 116, 120801 (2016).
- [5] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, Proc. Natl. Acad. Sci. U.S.A. 109, 16079 (2012).
- [6] A. S. Holevo, Prob. Peredachi Inf. 9, 3 (1973).
- [7] M. Plesch and V. Bužek, Phys. Rev. A 81, 032317 (2010).
- [8] L. A. Rozema, D. H. Mahler, A. Hayat, P. S. Turner, and A. M. Steinberg, Phys. Rev. Lett. 113, 160504 (2014).
- [9] Y. Yang, G. Chiribella, and D. Ebler, Phys. Rev. Lett. 116, 080501 (2016).
- [10] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996).
- [11] N. Gisin and S. Massar, Phys. Rev. Lett. 79, 2153 (1997).
- [12] R. F. Werner, Phys. Rev. A 58, 1827 (1998).
- [13] B. S. Clarke and A. R. Barron, IEEE Trans. Inf. Theory 36, 453 (1990).

- [14] W. Fulton and J. Harris, Representation Theory (Springer Science & Business Media, New York, 1991), Vol. 129.
- [15] D. Bacon, I. L. Chuang, and A. W. Harrow, Phys. Rev. Lett. 97, 170502 (2006).
- [16] For concreteness, here we assume n to be even and J to be integer, but all the arguments hold also for odd n and semi-integer J.
- [17] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. 82, 4344 (1999).
- [18] A. S. Holevo, Statistical Structure of Quantum Theory (Springer Science & Business Media, Berlin, 2001), Vol. 67.
- [19] See Supplemental Materials at http://link.aps.org/ supplemental/10.1103/PhysRevLett.117.090502 for, which contains [20], the proofs of Lemma 1, detailed precision analyses, and optimality proofs of both compression protocols.
- [20] M. Hayashi, Commun. Math. Phys. 293, 171 (2010).
- [21] M. Wilde, in *Quantum Information Theory* (Cambridge University Press, Cambridge, England, 2013), Chap. 18.
- [22] D. Petz, Commun. Math. Phys. 105, 123 (1986).
- [23] M. Koashi and N. Imoto, Phys. Rev. Lett. 87, 017902 (2001).
- [24] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. 77, 1225 (2005).
- [25] N. J. Cerf and J. Fiurasek, Prog. Opt. 49, 455 (2006).
- [26] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu, Phys. Rep. 544, 241 (2014).
- [27] F. G. S. L. Brandao, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Phys. Rev. Lett. 111, 250404 (2013).
- [28] H. Tajima and M. Hayashi, arXiv:1405.6457.
- [29] D. Bruß, M. Cinchetti, G. Mauro D'Ariano, and C. Macchiavello, Phys. Rev. A 62, 012302 (2000).
- [30] F. Buscemi, G.M. D'Ariano, C. Macchiavello, and P. Perinotti, Phys. Rev. A 74, 042309 (2006).
- [31] K. Bartkiewicz, A. Miranowicz, and Ş. K. Özdemir, Phys. Rev. A 80, 032306 (2009).
- [32] E. Nagali, D. Giovannini, L. Marrucci, S. Slussarenko, E. Santamato, and F. Sciarrino, Phys. Rev. Lett. **105**, 073602 (2010).
- [33] H. Chen, D. Lu, B. Chong, G. Qin, X. Zhou, X. Peng, and J. Du, Phys. Rev. Lett. 106, 180404 (2011).
- [34] K. Bartkiewicz, K. Lemr, A. Černoch, J. Soubusta, and A. Miranowicz, Phys. Rev. Lett. 110, 173601 (2013).
- [35] W.-B. Wang, C. Zu, L. He, W.-G. Zhang, and L.-M. Duan, Sci. Rep. 5, 12203 (2015).