August 29, 2016 (Monday)

Superconducting qubit systems: recent experimental progress towards fault-tolerant quantum computing at IBM

Antonio D. Córcoles

IBM

Abstract. Quantum information processing has experienced dramatic experimental breakthroughs over the last couple of years in many physical platforms. With current attained metrics, the horizon appears promising for building increasingly powerful quantum processors. In this talk I will review recent progress on quantum error detection and correction on superconducting qubit systems at IBM. Our experiments, which are implemented within the stabilizer formalism present in the surface code architecture, aim at demonstrating quantum error correcting protocols for fault-tolerant quantum computing. As a conclusion, I will describe and reflect on the main experimental hurdles our field will have to tackle in the incoming years.

Observation of frequency-domain Hong-Ou-Mandel interference

Toshiki Kobayashi[1] * Rikizo Ikuta[1] Shuto Yasui[1] Shigehito Miki[2] Taro Yamashita[2] Hirotaka Terai[2] Takashi Yamamoto[1] Masato Koashi[3] Nobuyuki Imoto[1]

[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT), Kobe 651-2492, Japan*
[3] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan*

Abstract. Hong-Ou-Mandel (HOM) interference plays a key role in quantum optics and quantum information processing. Although many types of HOM interference have been demonstrated by using photons, plasmons, atoms and phonons, all of them essentially used the spatial or polarization degree of freedom. In this work, we report the first observation of the HOM interference between two photons with different frequencies. The frequency-domain HOM interferometer is implemented by a partial frequency conversion in a nonlinear optical medium with a strong pump light. Our results have important consequences for manipulating the photonic quantum states encoded in the frequency domain.

Keywords: Quantum interference, Nonlinear optics

1 Introduction

In the past three decades since the HOM interference has been proposed and demonstrated with two photons from spontaneous parametric down-conversion (SPDC) process [1], huge varieties of experiments based on the HOM interference revealed fundamental properties in quantum physics, especially in quantum optics, and its applications are widely spreading over quantum information processing. The HOM interference has been observed with not only photons but also other bosonic particles, e.g., surface plasmons[2], Helium 4 atoms[3] and phonons[4]. In spite of such demonstrations using various kinds of physical systems, to the best of our knowledge, all of them essentially used the spatial degree of freedom for the HOM interference, including the use of polarization modes of photons that are easily converted to and from spatial modes. The demonstrations use a beamsplitter (BS) which mixes the two particles in different spatial/polarization modes.

In this work[5], we report the first observation of the HOM interference between two photons with different frequencies in optical region. In contrast to the spatial interferometer, the frequency-domain HOM interferometer is implemented in a single spatial mode with a nonlinear optical frequency conversion[6, 7, 8]. In the experiment, we input a 780 nm photon and a 1522 nm photon to the frequency converter that partially converts the wavelengths of the photons between 780 nm and 1522 nm[8]. We measured coincidence counts between the output photons at 780 nm and those at 1522 nm from the frequency converter. The observed visibility of the HOM interference was 0.71 ± 0.04, which clearly exceeds the maximum value of 0.5 in the classical wave theory.

*kobayashi-t@qi.mp.es.osaka-u.ac.jp

2 Experimental setup

The experimental setup for the frequency-domain HOM interference by using the partial frequency converter[8] is shown in Fig. 1(a). We prepare a heralded single photon at 780 nm in mode A and a weak coherent light at 1522 nm in mode B with an average photon number of ~ 0.1. The two light pulses are combined by a dichroic mirror (DM_2) and then focused on a type-0 quasi-phase-matched periodically-poled $LiNbO_3$ (PPLN) waveguide for the frequency conversion.

The time difference between the two light pulses is adjusted by mirrors (M) on a motorized stage. The vertically polarized cw pump laser at 1600 nm is combined with the two input light pulses by DM_3 and focused on the PPLN waveguide. The effective pump power was set to 140 mW which corresponds to the conversion efficiency of ~ 0.4. After the frequency converter, the light pulses at 780 nm and 1522 nm are separated by DM_4 and Bragg gratings (BG_{U2} and BG_{L2}). They are then measured by an avalanche photodiode with the quantum efficiency of about 60% for 780-nm photons (D_{U2}) and by a superconducting single-photon detector (SSPD)[9] with the quantum efficiency of about 60% for the 1522-nm photons (D_L). In order to observe the HOM interference, we collect the threefold coincidence events among the three detectors D_{U1}, D_{U2} and D_L.

3 Experimental result

The experimental result of the dependency of the threefold coincidence counts on the optical delay is shown in Fig. 1(b). The observed visibility of 0.71 ± 0.04 at the zero delay point was obtained by the best fit to the experimental data with a Gaussian. The high visibility clearly shows the nonclassical HOM interference between the two light pulses in a single spatial mode with different frequencies. We also measured the visibilities at the

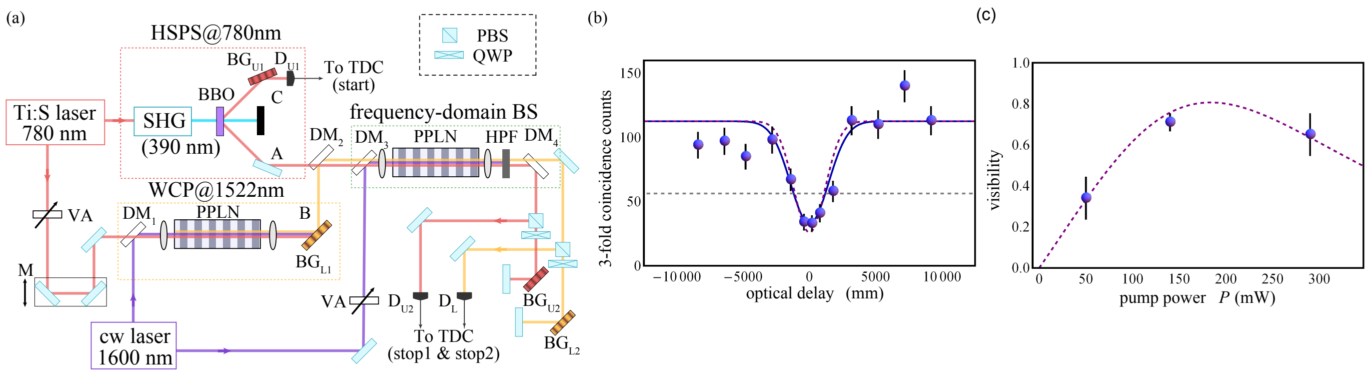


Figure 1: (a) The experimental setup of the frequency-domain HOM interference. In the experiment, the heralded single photon source (HSPS) at 780 nm and the weak coherent pulse (WCP) at 1522 nm are prepared to serve as two input photons to the frequency-domain BS. (b) The observed HOM dip at 140-mW pump power. The circles represent the experimental threefold coincidence counts. The solid curve is the Gaussian fit to the experimental counts. The dashed curve is obtained from our theoretical model with the experimental parameters. The dashed horizontal line describes the half values of the maximum of the fitting result. (c) The pump power dependence of the visibility. The circles are obtained from the experimental result. The dashed curve is obtained from our theoretical model with the experimental parameters.

pump power 50 mW and 290 mW, which corresponds to the conversion efficiencies ~ 0.2 and ~ 0.7, respectively. The experimental result is shown in Fig. 1(c). The observed visibilities are 0.34 ± 0.10 at 50 mW and 0.65 ± 0.10 at 290 mW. From our theoretical model, main reasons for the degradation of the visibility comes from the input light pulses; the effect of the multiphoton components in the coherent light pulse at 1522 nm and the broad bandwidth of the heralded single photon at 780 nm. If we use two single photons with the same bandwidth as that of the coherent light pulse, the visibility will be 0.98 at 190-mW pump power.

4 Conclusion

In conclusion, we have demonstrated the frequency-domain HOM interference between a heralded single photon at 780 nm and a weak laser light at 1522 nm in a single spatial mode by using the partial frequency converter based on the nonlinear optical effect. We observed the visibility of 0.71 ± 0.04, which clearly shows the nonclassical interference. We believe that our results give a novel tool for exploiting frequency-domain quantum phenomena and a way of scaling up the quantum information processing.

Acknowledgements

This work was supported by the JSPS Grant-in-Aid for JSPS Fellows Grant No. JP14J04677 and MEXT/JSPS KAKENHI Grant Nos JP25247068, JP15H03704, JP15KK0164 and JP25286077.

References

[1] C. K. Hong, Z. Y. Ou, & L. Mandel, Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* 59, 2044-2046 (1987).

[2] G. Di Martino *et al.* Observation of Quantum Interference in the Plasmonic Hong-Ou-Mandel Effect. *Phys. Rev. Applied* 1, 034004 (2014); J. S. Fakonas *et al.* Two-plasmon quantum interference. *Nat. Photon.* 8, 317 (2014).

[3] R. Lopes *et al.* Atomic Hong-Ou-Mandel experiment. *Nature* 520, 66 (2015).

[4] K. Toyoda, R. Hiji, A. Noguchi & S. Urabe, Hong-Ou-Mandel interference of two phonons in trapped ions. *Nature* 527, 74 (2015).

[5] T. Kobayashi *et al.* Frequency-domain Hong-Ou-Mandel interference *Nat. Photon.* 10, 441 (2016).

[6] S. Tanzilli *et al.* A photonic quantum information interface. *Nature* 437, 116 (2005).

[7] R. Ikuta, *et al.* Wide-band quantum interface for visible-to-telecommunication wavelength conversion. *Nat. Commun.* 2, 537 (2011).

[8] R. Ikuta *et al.* Observation of two output light pulses from a partial wavelength converter preserving phase of an input light at a single-photon level. *Opt. Express* 21, 27865 (2013).

[9] S. Miki, T. Yamashita, H. Terai & Z. Wang, High performance fiber-coupled NbTiN superconducting nanowire single photon detectors with Gifford-McMahon cryocooler. *Opt. Express* 21, 10208 (2013).

Realization of the contextuality-nonlocality tradeoff with a qubit-qutrit photon pair

Peng Xue[1] * Xiang Zhan[1] Xin Zhang[1] Jian Li[1] Yongsheng Zhang[2] Barry C. Sanders[3]

[1] *Department of Physics, Southeast University, Nanjing 211189, China*
[2] *Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*
[3] *Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*

Abstract. We report our experimental results on the no-disturbance principle, which imposes a fundamental monogamy relation on contextuality vs non-locality. We employ a photonic qutrit-qubit hybrid to explore no-disturbance monogamy at the quantum boundary spanned by non-contextuality and locality inequalities. In particular we realize the single point where the quantum boundary meets the no-disturbance boundary. Our results agree with quantum theory and satisfy the stringent monogamy relation thereby providing direct experimental evidence of a tradeoff between locally contextual correlations and spatially separated correlations. Thus, our experiment provides evidence that entanglement is a particular manifestation of a more fundamental quantum resource.

Keywords: nonlocality, contextuality, monogamy relation, entanglement

Quantum systems exhibit a wide range of non-classical and counter-intuitive phenomena. Corresponding experimental tests have been performed and support the necessity of quantum mechanics. The relation between contextual correlations and non-local correlations has been studied recently. It has been proven that the no-disturbance (ND) principle imposes monogamy relation between contextuality and non-locality and the quantum version of this monogamy relation is even more stringent.

We demonstrate no-disturbance monogamy spanned by non-contextuality and locality inequalities [1], which was theoretically proposed by Kurzyński et al. in [2]. Consider a scenario with two spatial separated observers Alice and Bob. Alice randomly chooses two compatible measurements from five measurements $\{A_i\}$ $(i = 1, ..., 5)$ and performs them on her system. Each two of A_i and $A_{(i+1)\bmod 5}$ are compatible. Whereas Bob chooses one of two incompatible measurements B_1, B_2 and performs them on his system. Each measurement has two outcomes ± 1.

One can test contextuality on Alice's system via KCBS inequality

$$\kappa_A = \langle A_1A_2\rangle + \langle A_2A_3\rangle + \langle A_3A_4\rangle + \langle A_4A_5\rangle + \langle A_5A_1\rangle \overset{\text{NCHV}}{\geqslant} -3. \quad (1)$$

Whereas CHSH locality inequality

$$\beta_{AB} = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_4B_1\rangle - \langle A_4B_2\rangle \overset{\text{LHV}}{\geqslant} -2 \quad (2)$$

can be tested on the systems of Alice and Bob.

The ND principle imposes a nontrivial tradeoff between the violations of CHSH and KCBS inequalities, i.e.,

$$\beta_{AB} + \kappa_A \overset{\text{ND}}{\geqslant} -5. \quad (3)$$

*gnep.eux@gmail.com

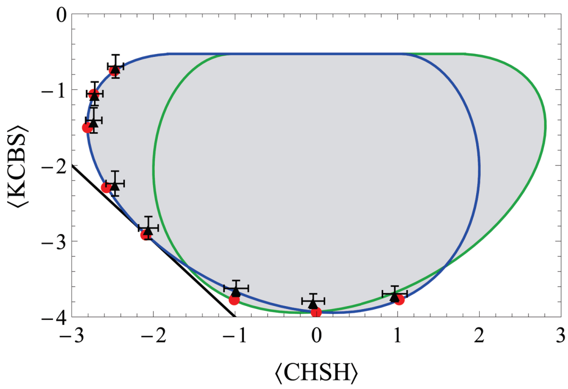


Figure 1: The region spanned by the allowed average values of CHSH and KCBS operators $\langle CHSH\rangle$ and $\langle KCBS\rangle$ can be divided into two overlapping parts and bounded by the solid curves. Every quantum state produces a point inside the region. However only the specific states can produce the points on the boundaries. The solid black straight line denotes the ND boundary. Experimental results of $\langle CHSH\rangle$ and $\langle KCBS\rangle$ are represented by the black triangles and compared to their theoretical predictions (red dots), producing the points on the boundary of the quantum region.

According to the ND principle, only one of these inequalities can be violated at a time. Quantum theory shows an additional monogamy relation between NCHV and LHV by restricting the possible values of (β_{AB}, κ_A) within a region in the parametric space spanned by the value of these two inequalities. The more stringent monogamy relation makes the quantum region to be smaller than that imposed by the ND principle. Therefore the boundary of the quantum region is more interesting. The quantum boundary touches the ND boundary in a single point.

To experimentally investigate quantum monogamy re-

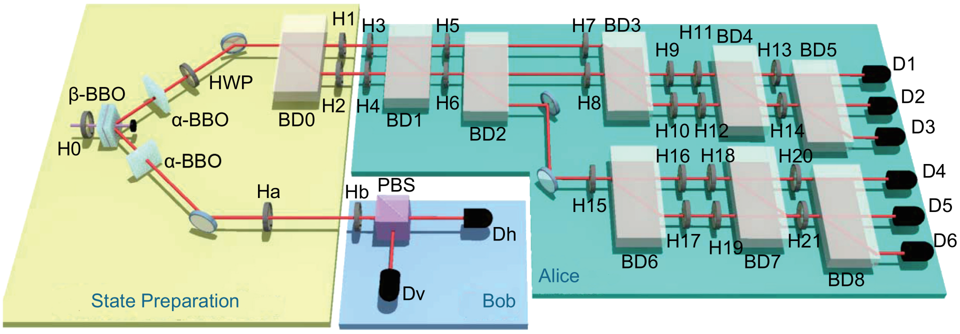


Figure 2: Experimental setup. Alice and Bob share entangled photon pairs which are generated via type-I SPDC. For Alice, cascade setup for sequentially measuring A_i and A_{i+1} is used to test KCBS inequality. Whereas, to test CHSH inequality B_j is measured via standard polarization measurements using HWP (Hb) and PBS.

lation between KCBS and CHSH inequalities, we produce the boundary of the quantum region in the parametric space spanned by the value of the two inequalities and especially the single point where the quantum boundary touches the ND boundary.

As illustrated in Fig. 2, our experimental setup consists of three modules: state preparation, Alice's measurement, and Bob's measurement. In the state preparation module, entangled photons of 801.6nm wavelength are generated in a type-I spontaneous parametric down-conversion (SPDC) process where two joint 0.5mm-thick β-barium-borate (β-BBO) crystals are pumped by a CW diode laser with 90mW of power. The visibility of entangled photonic state is larger than 95%. One of the photons as a qubit system is sent to Bob for his measurement. The other is then split by a birefringent calcite beam displacer (BD) into two parallel spatial modes. By employing the polarizations and spatial modes of a single photon, we can prepare arbitrary state of a qutrit.

To measure Alice's observables A_i and their correlations, we use cascaded Mach-Zehnder interferometers in three steps. The first step is to realize the measurement of A_i. Measuring A_iA_{i+1} requires two sequential measurements on the same photon. Since the single-observable measuring devices map its eigenstates to a fixed spatial path and polarization, with HWPs and BDs we can re-create the corresponding eigenstates of A_i for further measurement A_{i+1} in the second step. Two outcomes of A_i are each directed into identical but separated devices. In the third step we use the same interferometers in the first step to measurement A_{i+1}. Two identical A_{i+1} measuring devices are built, each of which is connected to the corresponding output port of the measuring device of A_i. The outcomes of the measurement A_iA_{i+1} are given by the responses of the detectors.

For Bob, the measurement of observable B_j is standard polarization measurement using HWP (Hb) and PBS. The photons are detected by Dh and Dv right after the PBS. For the photon detection, we only register the coincidence rates between the detectors of Alice and Bob.

We produce eight points on the quantum boundary corresponding to eight different input states. The experimental results on the average values of CHSH and KCBS operators are shown in Fig. 1. It is clear that the inequality (3) is always satisfied in experiment, and the violation of either KCBS or CHSH inequality forbids the violation of the other, in agreement with the quantum theory predictions. Especially, our results show the inequality (3) is tight, i.e., there is a state for which the inequality becomes an equality. We present the measured values $\langle CHSH\rangle_{\rm ex} = -2.061 \pm 0.120$, $\langle KCBS\rangle_{\rm ex} = -2.826 \pm 0.151$ in the single point where the quantum boundary touches the ND boundary and the inequality becomes an equality, i.e., $\beta_{AB} + \kappa_A = -5$ is satisfied within error bars.

The fact that the origin of Bell inequalities and contextual inequalities is the existence of joint probability distributions naturally raises the question as to whether similar monogamy relations exist between contextual correlations and nonlocal correlations. Our experiment provides an answer to this question. We observe the fundamental monogamy relation between contextuality and non-locality in a photonic qutrit-qubit system and show the first experimental evidence of a tradeoff between locally contextual correlations and spatially separated correlations imposed by quantum theory. The existence of the monogamy relation suggests the existence of a quantum resource of which entanglement is a particular form. The resource required to violate KCBS inequality can be transformed into entanglement which consumes to violate CHSH inequality. Our experiment sheds new light for further explorations of this quantum resource. Furthermore our results suggest monogamy relations between different types of correlations might be ubiquitous in nature and pave the way for further research on these monogamy relations.

References

[1] X. Zhan, X. Zhang, J. Li, Y. S. Zhang, B. C. Sanders, and P. Xue, Phys. Rev. Lett. 116, 090401 (2016).

[2] P. Kurzyński, A. Cabello and D. Kaszlikowski, Phys. Rev. Lett. **112**, 100401 (2014).

One-way and reference-frame independent EPR-steering

Sabine Wollmann,[1 *] Raj B. Patel,[1] Nathan Walk,[1 2] Michael J. W. Hall,[1] Howard M. Wiseman,[1] Geoff J. Pryde[1 †]

[1] *Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia*
[2] *Department of Computer Science, University of Oxford, Oxford OX1 3QD, United Kingdom*

Abstract. Einstein-Podolsky-Rosen steering is a type of quantum correlation intermediate to entanglement and Bell nonlocality. It is widely investigated for its foundational aspects and applications in quantum information and communication tasks. Here, we prove and experimentally observe that steering can be *one-way*, i.e. the ability to complete the protocol is asymmetric under change of the parties. We also prove and experimentally observe that steering can be demonstrated with 100% probability that this is invariant to rotations of the measurement settings.

Keywords: Quantum optics, Quantum information, EPR, nonlocality, steering, reference frame

Quantum entanglement is a key resource for quantum information and communication tasks, such as teleportation, entanglement swapping and quantum key distribution. Einstein-Podolsky-Rosen (EPR) steering is a quantum correlation that is distinct from other nonclassical correlations such as Bell nonlocality (1) and quantum nonseparability. Because of the nonlocal correlations, measuring one system affects the measurement results on the other system, hence the name 'steering'.

1 Asymmetric steering

Moving through the classes of quantum nonlocality, from Bell nonlocality towards nonseparability gives access to protocols which are more robust to noise (2) for projective measurements at the expense of increasing the number of parties and apparatus that need to be trusted. For entanglement witness tests and Bell inequality violations, both observers are untrusted or trusted respectively. However, EPR-steering, which was only recently formalized by Wiseman et al. (3), features a fundamental asymmetry in the sense that in a steering test the observers play different roles: one party is trusted while the other is untrusted. While the previous classes are symmetric —the effects persist under exchange of the parties - this does not necessarily hold for EPR-steering. The question which arises is whether sharing an asymmetric state can result in one-way EPR steering, where e.g. Alice can steer Bob's measurement outcomes, but not the other way around.

This question was first experimentally addressed by Händchen et al., who demonstrated Gaussian one-way EPR steering (4). However their investigation was restricted to Gaussian measurements on Gaussian states. However, there exists explicit examples of supposedly one-way steerable Gaussian states actually being two-way steerable using a broader class of measurements (5). Do states exist which are one-way steerable for arbitrary measurements? The answer is yes. Two independent groups, Nicolas Brunner's in Geneva and Howard Wiseman's in Brisbane, theoretically proved the existence of such states. Brunner's approach holds for arbitrary measurements with infinite settings, the so-called infinite-setting positive-operator-valued measures (POVMs), with the cost of using an exotic family of states to demonstrate the effect over an extremely small parameter range, which is unsuitable for experimental observation (6). Independently, Evans et al. showed one-way steerability exists for projective measurements of Werner states and loss (7), which are easier to realise experimentally.

In our work (5) we ask if we can extend the result in Ref. (6) to find a simple state which is steerable in one direction but cannot be steered in the other direction, even for the case of arbitrary measurements and infinite settings. We consider a shared Werner state for optical polarisation qubits, $\rho_W(\mu) = \mu |\psi_s\rangle\langle\psi_s| + (1-\mu)/4\, \mathbf{I}_x$, where $\mu \in [0,1]$, $\mathbf{I}_x$ is the identity and $|\psi_s\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ (7). Using a theorem of Ref.(6) allowed us to construct a state $\rho_{AB} = \frac{1-p}{3}\rho_W + \frac{p+2}{3}\frac{\mathbf{I}_A}{2} \otimes |v\rangle\langle v|$, where $|v\rangle$ is the vacuum state of Bob's mode and the probability p represents adding asymmetric loss in his arm. This state is one-way steerable for POVMs, if we can fulfil the condition $p > \frac{2\mu+1}{3}$.

In our experiment we investigated three different regimes: two-way steering, one-way steering for projective measurements and one-way steering for POVMs. The state for each steering regime was reconstructed via quantum state tomography and its fidelity with the closest Werner state, and its parameter μ, was determined (5). To demonstrate two-way steering, we measured Alice's steering parameter to be 8.4 standard deviations (SDs) above the classical bound and Bob's steering parameter violating the steering inequality by 5.1 SDs. Next we realized a one-way steerable state for projective measurements by inserting a loss in Bob's line (Fig.1). Alice remained able to steer Bob's state, violating the inequality by 7.3 SDs. The loss of information in Bob's arm made him unable to steer the other party. Finally, we investigated the regime where only one-way steering

*sabine.wollmann@griffithuni.edu.au
†g.pryde@griffith.edu.au

is possible, even for arbitrary POVMs. We were able to violate the inequality by 6.6 SDs in one direction. In the other direction, tomographic reconstruction verified the creation of a state that was provably unsteerable for POVMs. Thus, we observe genuine one-way EPR steering for the first time. We note that an independent demonstration was realised in Ref.(8). While their result is restricted to two measurement settings, our result holds for POVMs.

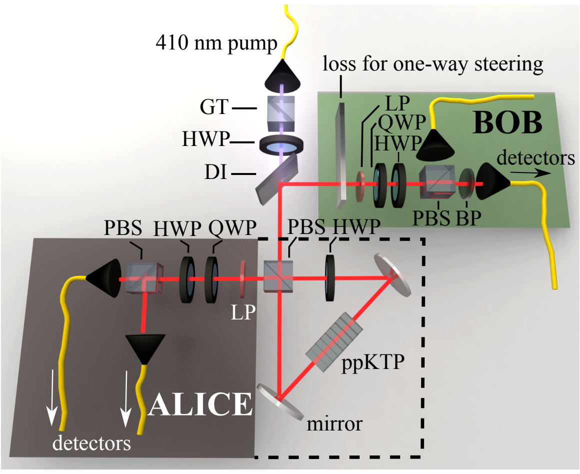


Figure 1: Experimental scheme. Both, Alice and Bob, are in control of their line and their detectors. The party which is steering is also in control of the source. Entangled photons at 820 nm were produced via SPDC (9). Different measurement settings are realized by rotating half- and quarter-wave plates relative to the polarizing beam splitters. The loss, inserted for one-way EPR-steering, was realized by a gradient neutral density filter mounted in front of Bob's line to control the fraction of photons received. Long pass (LP) filters remove pump photons co-propagating with the qubits before the latter are coupled into fibres and detected by photon counting modules and counting electronics.

2 Rotationally symmetric steering tests

In another experiment we also characterised the rotational invariance of EPR-steering. Establishing such a common reference frame —necessary for many quantum information tasks - is a nontrivial issue and can be highly resource intensive and technically demanding. The question is whether quantum nonlocality can be demonstrated without a shared reference frame. This question was experimentally (10; 11) answered for the CHSH inequality. Here, we formulate rotationally invariant steering inequalities for m measurement directions for Alice and n directions for Bob. In our experiment, they can estimate the average correlations $M_{jk} := \langle A_j B_k \rangle$ from their measurement outcomes. Alice has to violate the EPR-steering inequality $\|M\|_{tr} := tr\sqrt{M^T M} \leq \sqrt{m}$ for the trace-norm of the correlation matrix to demonstrate steering of Bob's state. For m=n=2, this trace-norm inequality is the best possible steering inequality that is invariant under local rotations that preserve the

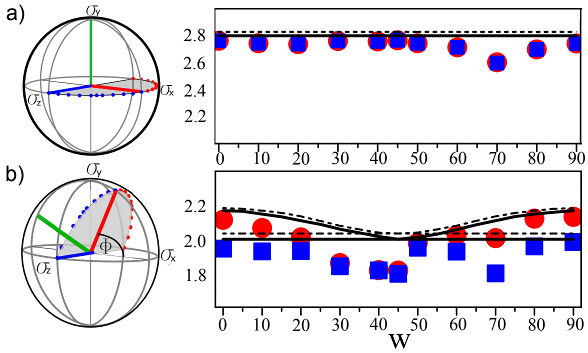


Figure 2: The Poincaré spheres show measurement directions (blue and red). Alice's measurement directions are rotated by 90° in 10° steps (dots) along the plane (grey) which was spanned by a_1(blue) and a_2 (red) forming an angle of $\Phi = 0°$ (a), and $\Phi = 64°$ (b) with the σ_x axis. We compare experimental data for the trace-norm inequality (blue square) and CFFW inequality (red circles) with modeled curves using a maximally entangled state (dashed line) and a Werner state $\rho_W(\mu)$ (solid line).

plane of Alice and Bob's measurement directions. If Alice's and Bob's measurement directions are sharing the same plane, EPR-steering is always possible, regardless of any rotations in the plane for a Werner state with $\mu > \frac{1}{\sqrt{2}}$. We compare our inequality with the CFFW inequality (12). In our experiment (Fig.1), we consider $m = n = 2$ orthogonal measurement directions for Alice and Bob in the $\sigma_x - \sigma_z$ plane (Fig.2). While Bob's measurement directions remained fixed along σ_x and σ_z, Alice's were rotated by $w = 10°$steps. We compared our trace-norm inequality (blue squares) with the CFFW inequality (red circles) and observed for both a violation of the bound (Fig.2a). Rotating by angle Φ out of the shared plane demonstrated the dependency of both inequalities on a shared measurement plane. At our chosen angle, using the trace-norm inequality did not allow us to demonstrate steering, while we could still violate the CFFW inequality despite its dependence on the rotation w along the plane (Fig.2b).

References

[1] J.S Bell, *Physics*, 1:195, 1964.
[2] A. J. Bennet et al., *Phys. Rev. X*, 2:031003, 2012.
[3] H. Wiseman et al., *Phys. Rev. Lett.*, 98:140402, 2007.
[4] V. Handchen et al., *Nat Photon*, 6:596, 2012.
[5] S. Wollmann et al., *Phys. Rev. Lett.*, 116:160403, 2016.
[6] M. T. Quintino et al., *Phys. Rev. A*, 92:032107, 2015.
[7] D.A. Evans et al., *Phys. Rev. A*, 90, 2014.
[8] K. Sun et al., *Phys. Rev. Lett.*, 116:160404, 2016.
[9] A. Fedrizzi et al., *Opt. Exp.*, 15:15377, 2007.
[10] P. Shadbolt et al., *Sci. Rep.*, 2:470, 2012.
[11] M. S. Palsson et al., *Phys. Rev. A*, 86:032322, 2012.
[12] E. G. Cavalcanti et al., *J. Opt. Soc. Am. B*, 32:A74, 2015.

Are Incoherent Operations Physically Consistent? – A Physical Appraisal of Incoherent Operations and an Overview of Coherence Measures

Eric Chitambar[1] * Gilad Gour[2 3] †

[1] *Department of Physics and Astronomy, Southern Illinois University, Carbondale, Illinois 62901, USA*
[2] *Department of Mathematics and Statistics, University of Calgary, AB, Canada T2N 1N4*
[3] *Institute for Quantum Science and Technology, University of Calgary, AB, Canada T2N 1N4*

Abstract. In this paper we establish a criterion of physical consistency for any resource theory. We show that all currently proposed basis-dependent theories of coherence fail to satisfy this criterion. We further characterize the physically consistent resource theory of coherence and find its operational power to be quite limited. After relaxing the condition of physical consistency, a number of new coherence measures are introduced based on relative Rényi entropies, and we study incoherent state transformations under different operational classes, including the newly proposed dephasing-covariant operations. Necessary and sufficient conditions are derived for the convertibility of qubit states.

Keywords: Quantum coherence, Quantum resource theories

1 Introduction

In quantum systems, the notion of coherence is ubiquitous. For instance, the state $|+\rangle = \sqrt{1/2}(|0\rangle + |1\rangle)$ can be seen as a coherent superposition of the states $|0\rangle$ and $|1\rangle$, while the state $|0\rangle$ can itself be seen as a coherent superposition of $|+\rangle$ and $|-\rangle = \sqrt{1/2}(|0\rangle - |1\rangle)$. Thus, without further qualification, it is completely ambiguous to say that one state has coherence while another does not. One way to make such a statement meaningful involves first identifying a fixed reference basis, and then defining coherence with respect to this basis. More precisely, a basis for the system's state space is specified (called the incoherent basis), and then a given state is deemed incoherent if it is diagonal in this basis.

Recently, researchers have used this distinction between coherent and incoherent states to construct resource theories of quantum coherence [1, 2, 3, 4]. A general resource theory for a quantum system is characterized by a pair $(\mathcal{F}, \mathcal{O})$, where $\mathcal{F}$ is a set of "free" states and $\mathcal{O}$ is a set of "free" quantum operations. Any state that does not belong to $\mathcal{F}$ is then deemed a resource state. Entanglement theory provides a prototypical example of a resource theory in which the free states are the separable or unentangled states, and the free operations are local operations and classical communication (LOCC). For quantum coherence, the free states are the incoherent states $\mathcal{I}$. As for the free or "incoherent" operations, many different approaches have been proposed, and a primary objective of this paper is to consider the physical meaning behind these approaches.

Specifically, we propose one notion of what it means for a quantum resource theory to be "physical," and then we see what type of incoherent operations fits this prescription. In principle, any pair $(\mathcal{F}, \mathcal{O})$ defines a resource theory, provided the operations of $\mathcal{O}$ act invariantly on $\mathcal{F}$; i.e. $\mathcal{E}(\rho) \in \mathcal{F}$ for all $\rho \in \mathcal{F}$ and all $\mathcal{E} \in \mathcal{O}$. However, this is just a mathematical restriction placed on the maps belonging to $\mathcal{O}$. It does not imply that $\mathcal{E} \in \mathcal{O}$ can actually be physically implemented without generating or consuming additional resource. The issue is a bit subtle here since in quantum mechanics, physical operations on one system ultimately arise from unitary dynamics and projective measurements on a larger system, a process mathematically described by a Stinespring dilation. A resource theory $(\mathcal{F}, \mathcal{O})$ defined on system A is said to be *physically consistent* if every free operation $\mathcal{E} \in \mathcal{O}$ can be obtained by an auxiliary state $\hat{\rho}_B$, a joint unitary U_{AB}, and a projective measurement $\{P_k\}_k$ that are all free in an extended resource theory $(\mathcal{F}', \mathcal{O}')$ defined a larger system AB, for which $\mathcal{F} = \mathrm{Tr}_B\mathcal{F}' := \{\mathrm{Tr}_B(\rho_{AB}) : \rho_{AB} \in \mathcal{F}'\}$. For example, LOCC renders a physically consistent resource theory of entanglement since any LOCC operation can be implemented using only local unitaries and projections.

The most well-known resources theories of quantum coherence are based on either Maximal Incoherent Operations (MIO) [1], Incoherent Operations (IO) [2], or Strictly Incoherent Operations (SIO) [3, 4]. We observe that none of these offer a physically consistent resource theory as just defined, and the true analog to LOCC in coherence theory has been lacking. We identify this hitherto missing piece as the class of *physically incoherent operations* (PIO). The previously studied operations MIO/IO/SIO are much closer akin to separable or non-entangling operations in entanglement theory, and we clarify what sort of physical interpretations can be given to these operations. The relationship between the different operational classes is depicted described by PIO $\subset$ SIO $\subset$ IO $\subset$ MIO.

2 Results

The following summarizes our main results. First, we fully characterize the class of physically incoherent operations (PIO).

*echitamb@siu.edu
†gour@ucalgary.ca

Proposition 1 *A CPTP map $\mathcal{E}$ is a physically incoherent operation if and only if it can be expressed as a convex combination of maps each having Kraus operators $\{K_j\}_{j=1}^r$ of the form*

$$K_j = U_j P_j = \sum_x e^{i\theta_x} |\pi_j(x)\rangle\langle x| P_j, \tag{1}$$

where the P_j form an orthogonal and complete set of incoherent projectors on system A and π_j are permutations.

Necessary and sufficient conditions for state transformations are derived.

Proposition 2 *For any two state $|\psi\rangle$ and $|\phi\rangle$, the transformation $|\psi\rangle \to |\phi\rangle$ is possible by PIO if and only if*

$$|\psi\rangle = \sum_{i=1}^k \sqrt{p_i} U_i |\phi\rangle, \tag{2}$$

where the U_i are incoherent isometries such that $P_i U_i|\phi\rangle = U_i|\phi\rangle$ for an orthogonal and complete set of incoherent projectors $\{P_i\}_i$.

While we find that PIO allows for optimal distillation of maximal coherence from partially coherent pure states in the asymptotic limit of many copies, the process is strongly irreversible. That is, maximally coherent states cannot be diluted into weakly coherent states at a nonzero rate, and they are thus curiously found to be the *least* powerful among all coherent states in terms of asymptotic convertibility.

Given this limitation of PIO and its similar weakness on the finite-copy level, it is therefore desirable from a theoretical perspective to consider more general operations. Consequently, we shift our focus to the development of coherence resource theories under different relaxations of PIO. To this end, we introduce the class of dephasing-covariant incoherent operations (DIO), which to our knowledge has never discussed before in literature. We provide physical motivation for DIO and show that these operations are just as powerful as Maximal Incoherent Operations (MIO) when acting on qubits. It turns out that all classes of incoherent operations behave equivalently for this task, and in fact, state convertibability depends on just two incoherent monotones. The first is the *Robustness of Coherence*, and is defined as

$$C_R(\rho) = \min_{t\geq 0} \left\{ t \;\middle|\; \frac{\rho + t\sigma}{1+t} \in \mathcal{I},\ \sigma \geq 0 \right\}.$$

Here we introduce a new type of robustness measure that we call the Δ-Robustness of Coherence:

$$C_{\Delta,R}(\rho) = \min_{t\geq 0} \left\{ t \;\middle|\; \frac{\rho + t\sigma}{1+t} \in \mathcal{I},\ \sigma \geq 0,\ \Delta(\sigma - \rho) = 0 \right\}.$$

While C_R is a monotone under MIO in general, for qubits $C_{\Delta,R}$ is also a MIO monotone. These two measures completely characterize qubit state transformations, as we prove in this paper.

Theorem 3 *For qubit state ρ and σ, the transformation $\rho \to \sigma$ is possible by either SIO, DIO, IO, or MIO if and only if both $C_R(\rho) \geq C_R(\sigma)$ and $C_{\Delta,R}(\rho) \geq C_{\Delta,R}(\sigma)$.*

Additional results include:

- We show that the so-called majorization condition decides transformation feasibility for the classes SIO and a special subclass of IO that we denote by sIO. However, whether or not the majorization condition also holds for IO remains an open problem and we point out mistakes in recent proofs claiming it does. By constructing an explicit family of transformations, we show that the majorization condition can be violated by MIO - even stronger the Schmidt rank can be increased by MIO. In addition, we demonstrate an operational equivalence between incoherent pure state transformations using PIO/SIO/sIO and the transformation of bipartite maximally correlated states using zero-communication LOCC/one-way LOCC/ two-way LOCC, respectively.

- We introduce a number of new incoherent monotones/measures for the various operational classes based. All of these measures are unified within a very general framework for constructing incoherent measures. Two class of measures included in this framework are the relative Rényi α-entropies of incoherence and the quantum relative Rényi α-entropies of incoherence.

- We discuss in greater detail the relationship between coherence resource theories based on asymmetry and those using a basis-dependent definition of coherence. We develop the resource theories of G-asymmetry and N-asymmetry, where G is the group of all incoherent unitaries and N is the group of all diagonal incoherent unitaries.

References

[1] J. Äberg. Quantifying Superposition. quant-ph/0612146, 2006.

[2] T. Baumgratz, M. Cramer, and M.B. Plenio. Quantifying Coherence. *Phys. Rev. Lett.*, 113(14):140401, 2014.

[3] A. Winter and D. Yang. Operational Resource Theory of Coherence. *Phys. Rev. Lett.*, 116(12):120404, 2015.

[4] B. Yadin, J. Ma, D. Girolami, M. Gu, V. Vedral. Quantum Processes which do not use Coherence. arXiv:1512.02085, 2015.

Relating the Resource Theories of Entanglement and Quantum Coherence

Eric Chitambar[1] * Min-Hsiu Hsieh[2] †

[1] *Southern Illinois University*
[2] *University of Technology Sydney*

Keywords: Resource Theory; Coherence; Entanglement; LOCC

There has currently been much interest in constructing a resource theory of quantum coherence [1, 15, 2, 4, 13, 31, 29, 25, 20, 26, 30], in part because of recent experimental and numerical findings that suggest quantum coherence alone can enhance or impact physical dynamics in biology [17, 16, 12, 14], and thermodynamics [18, 21]. In a standard resource-theoretic treatment of quantum coherence, the free (or "incoherent") states are those that are diagonal in some fixed reference (or "incoherent") basis. Different classes of allowed (or "incoherent") operations have been proposed in the literature [1, 2, 20, 26, 30, 5, 19], however an essential requirement is that the incoherent operations act invariantly on the set of diagonal density matrices. Incoherent operations can then be seen as one of the most basic generalizations of classical operations since their action on diagonal states can always be simulated by classical processing.

In addition to coherence, entanglement is another precious resource in quantum information science. To properly unify coherence and entanglement under a common resource-theoretic framework, one must modify the scenario by adopting the "distant lab" perspective in which two or more parties share a quantum system but they are spatially separated from one another [24, 11]. In this setting, entanglement cannot be generated between the parties and it becomes another resource in play. When the constraint of locality is added to the incoherent framework, the allowable operations for Alice and Bob are then *local incoherent operations and classical communication* (LIOCC). The hybrid coherence-entanglement theory described here is similar in spirit to previous work on the locality-restricted resource theories of purity and asymmetry. The goal of this paper is to investigate the LIOCC convertibility between entanglement and coherence as resources in quantum information processing. For instance, how much local coherence and shared entanglement do Alice (A) and Bob (B) need to prepare a particular bipartite state ρ^{AB} using LIOCC? Conversely, how much coherence and entanglement can be distilled from a given state ρ^{AB} using LIOCC? We refer the detailed introduction of the bipartite coherence theory to the full paper [6]. The canonical resource states in the bipartite LIOCC framework are the maximally coherent bits (CoBits), $|\Phi_A\rangle := \sqrt{1/2}(|0\rangle^A + |1\rangle^A)$ and $|\Phi_B\rangle := \sqrt{1/2}(|0\rangle^B + |1\rangle^B)$ for Alice and Bob's systems respectively [2], as well as the entangled state $|\Phi_{AB}\rangle := \sqrt{1/2}(|00\rangle + |11\rangle)$, which we will call the maximally coherent entangled bit (eCoBit).

Asymptotic Manipulations of Entanglement and Coherence: We now describe the primary tasks studied in this paper, which can be seen as the resource-theoretic tasks recently analyzed by Winter and Yang in Ref. [29] but now with additional locality constraints. All of the detailed proofs can be found in Ref. [6], and here we just present the results. Let us begin with the problem of asymptotic state formation. A triple (R_A, R_B, E^{co}) is an achievable *coherence-entanglement formation triple* for the state ρ^{AB} if for every $\epsilon > 0$ there exists an LIOCC operation $\mathcal{L}$ and integer n such that $\mathcal{L}\left(\Phi_A^{\otimes\lceil n(R_A+\epsilon)\rceil} \otimes \Phi_B^{\otimes\lceil n(R_B+\epsilon)\rceil} \otimes \Phi_{A'B'}^{\otimes\lceil n(E^{co}+\epsilon)\rceil}\right) \overset{\epsilon}{\approx} \rho^{\otimes n}$. Dual to the task of formation is resource distillation. A triple (R_A, R_B, E^{co}) is an achievable *coherence-entanglement distillation triple* for ρ^{AB} if for every $\epsilon > 0$ there exists an LIOCC operation $\mathcal{L}$ and integer n such that $\mathcal{L}(\rho^{\otimes n}) \overset{\epsilon}{\approx} \Phi_A^{\otimes\lfloor n(R_A-\epsilon)\rfloor} \otimes \Phi_B^{\otimes\lfloor n(R_B-\epsilon)\rfloor} \otimes \Phi_{AB}^{\otimes\lfloor n(E^{co}-\epsilon)\rfloor}$. As we are dealing with asymptotic transformations, we should expect the optimal rate triples to be given by entropic quantities. We will also be interested in these entropic quantities after sending our state ω^{AB} through the completely dephasing channel, $\Delta(\omega) := \sum_{xy} |xy\rangle\langle xy|\omega|xy\rangle\langle xy|$. It will be convenient to think of $\Delta(\omega)$ as encoding random variables XY having joint distribution $p(x, y) = \langle xy|\Delta(\omega)|xy\rangle$. For this reason, we follow standard convention and replace the labels $(A, B) \to (X, Y)$ when discussing a dephased state. Our first main result completely characterizes the achievable rate region for the LIOCC formation of bipartite pure states.

Theorem 1 *For a pure state $|\Psi\rangle^{AB}$ the following triples are achievable coherence-entanglement formation rates*

$$(R_A, R_B, E^{co}) = \left(0,\ S(Y|X)_{\Delta(\Psi)},\ S(X)_{\Delta(\Psi)}\right) \tag{1}$$
$$(R_A, R_B, E^{co}) = \left(S(X)_{\Delta(\Psi)},\ S(Y|X)_{\Delta(\Psi)},\ \mathrm{E}(\Psi)\right) \tag{2}$$
$$(R_A, R_B, E^{co}) = \left(0,\ 0,\ S(XY)_{\Delta(\Psi)}\right) \tag{3}$$

as well as the points obtained by interchanging $A \leftrightarrow B$ in Eqns. (1) – (3). *Moreover, these points are optimal in the sense that any achievable rate triple must satisfy*

*echitamb@siu.edu
†Min-Hsiu.Hsieh@uts.edu.au

(i) $E^{co} \geq \mathrm{E}(\Psi)$*, (ii)* $R_A + R_B \geq S(XY)_{\Delta(\Psi)}$*, (iii)* $R_B + E^{co} \geq S(XY)_{\Delta(\Psi)}$.

For a mixed state ρ^{AB}, a formation protocol can be constructed that achieves the average rates for any ensemble $\{p_k, |\varphi_k\rangle^{AB}\}$ such that $\rho = \sum_k p_k |\varphi_k\rangle\langle\varphi_k|$ [3]. For instance, one can consider an ensemble whose average bipartite coherence attains the coherence of formation C_F for ρ; i.e. it is an ensemble $\{p_k, |\varphi_k\rangle^{AB}\}$ for ρ that minimizes $\sum_k p_k S(XY)_{\Delta(\varphi_k)}$ [31, 29]. Then for a mixed state ρ, the coherence rate sum $R_A + R_B$ of Eq. (2) can attain the coherence of formation $C_F(\rho)$. In the global setting where Alice and Bob are allowed to perform joint operations across system AB, it has been shown that $C_F(\rho)$ quantifies the optimal coherence consumption rate for generating ρ using global incoherent operations [29]. Our result then intuitively says that in the restricted LIOCC setting, the same coherence rate is sufficient to generate ρ, however they now need additional entanglement at a rate $\sum_k p_k \mathrm{E}(\varphi_k)$, where the ensemble $\{p_k, |\varphi_k\rangle^{AB}\}$ minimizes the average coherence of ρ.

Next, we introduce a new LIOCC monotone and provide its operational interpretation. To do so, we recall the recently studied task of *assisted* coherence distillation, which involves one party helping another distill as much coherence as possible through general quantum operations performed on the helper side and incoherent operations performed on the distillation side [7]. For a given state ρ^{AB}, the optimal asymptotic rate of coherence distillation on Bob's side when Alice helps is denoted by $C_a^{A|B}(\rho^{AB})$. When the roles are switched, the optimal asymptotic rate is denoted by $C_a^{B|A}(\rho^{AB})$. It was shown in Ref. [7] that $C_a^{A|B}(\rho^{AB}) = S(Y)_{\Delta(\Psi)}$ and $C_a^{B|A}(\rho^{AB}) = S(X)_{\Delta(\Psi)}$. With these quantities in hand, we define for a bipartite pure state $|\Psi\rangle^{AB}$ the function

$$\begin{aligned} C_{\mathcal{L}}(\Psi) = & \quad C_a^{A|B}(\Psi) + C_a^{B|A}(\Psi) - \mathrm{E}(\Psi) \\ = & \quad S(X)_{\Delta(\Psi)} + S(Y)_{\Delta(\Psi)} - \mathrm{E}(\Psi). \end{aligned} \tag{4}$$

Its extension to mixed states can be defined by a convex roof optimization [27]: $C_{\mathcal{L}}(\rho^{AB}) = \inf_{\{p_k, |\varphi_k\rangle^{AB}\}} \sum_k p_k C_{\mathcal{L}}(\varphi_k^{AB})$ for which $\rho^{AB} = \sum_k p_k |\varphi_k\rangle\langle\varphi_k|$.

Theorem 2 *The function $C_{\mathcal{L}}$ is an LIOCC monotone.*

We note that this is the first monotone of its kind since it behaves monotonically under LIOCC, but not general LOCC or even under LQICC, the latter being an operational class in which only one of the parties is required to perform incoherent operations (as opposed to LIOCC where *both* parties must perform incoherent operations) [7]. Using the monotonicity of $C_{\mathcal{L}}$, we are able to derive tight upper bounds on coherence distillation rates.

Theorem 3 *For a pure state $|\Psi\rangle^{AB}$ the following triples are achievable coherence-entanglement distillation rates*

$$(R_A, R_B, E^{co}) = \big(S(X)_{\Delta(\Psi)} - \mathrm{E}(\Psi),\ S(Y)_{\Delta(\Psi)},\ 0\big) \tag{5}$$

$$(R_A, R_B, E^{co}) = \big(0,\ S(Y|X)_{\Delta(\Psi)},\ I(X:Y)_{\Delta(\Psi)}\big), \tag{6}$$

as well as the points obtained by interchanging $A \leftrightarrow B$ in Eqn. (5) and (6). Moreover, these points are optimal in the sense that any achievable rate triple must satisfy (i) $R_A + R_B \leq C_{\mathcal{L}}(\Psi)$ and (ii) $R_B + E^{co} \leq S(Y)_{\Delta(\Psi)}$.

This theorem endows $C_{\mathcal{L}}$ with the operational meaning of quantifying how much local coherence can be simultaneously distilled from a pure state. For a state $|\Psi\rangle$ the maximum that Alice can help Bob distill coherence is $C_a^{A|B}$ while the maximum that Bob can help Alice is $C_a^{B|A}$. Evidently, they cannot both simultaneously help each other at these optimal rates. Instead, they are bounded away from simultaneous optimality at a rate equaling their shared entanglement. It is still unknown the precise range of achievable distillation triples (R_A, R_B, E^{co}_{max}), where E^{co}_{max} is the maximum eCoBit distillation rate. While we are able to prove that E^{co}_{max} is the regularized version of $I(X:Y)_{\Delta(\Psi)}$ optimized over all LIOCC protocols, we have no single-letter expression for this rate nor do we know the achievable local coherence rates for optimal protocols.

A natural question is whether $E^{co}_{max}(\Psi) = \mathrm{E}(\Psi)$. While this question remains open, we can show that $\mathrm{E}(\Psi)$ is achievable if the Schmidt basis of the final state need not be incoherent. More precisely, we say a number R is an achievable LIOCC entanglement distillation rate if for every $\epsilon > 0$, there exists an LIOCC protocol $\mathcal{L}$ acting on n copies of Ψ such that $\mathcal{L}(\Psi^{\otimes n}) \overset{\epsilon}{\approx} \Lambda_d$, where Λ_d is a $d \otimes d$ maximally entangled pure state (i.e. $\Lambda^A = \Lambda^B = \mathbb{I}/d$) with $\frac{1}{n}\log d > R - \epsilon$. The largest achievable distillation rate will be denoted by $E_D^{LIOCC}(\Psi)$.

Theorem 4 $E_D^{LIOCC}(\Psi) = \mathrm{E}(\Psi)$.

It is interesting to compare the coherence distillation rates using incoherent operations under different types of locality constraints. In Refs. [23, 8, 22, 10], similar comparisons were made in terms of purity (or work-information) extraction. Let C_D^{Global}, C_D^{LIOCC}, and C_D^{LIO} denote the optimal rate sum $R_A + R_B$ of local coherence distillation using global incoherent operations, LIOCC, and local incoherent operations (with no classical communication), respectively. In complete analogy to [23, 8, 22, 10], we define the *nonlocal coherence deficit* of a bipartite state ρ^{AB} as $\delta(\rho^{AB}) = C_D^{Global}(\rho^{AB}) - C_D^{LIOCC}(\rho^{AB})$ and the *LIOCC coherence deficit* as $\delta_c(\rho^{AB}) = C_D^{LIOCC}(\rho^{AB}) - C_D^{LIO}(\rho^{AB})$. Intuitively, the quantity $\delta(\rho^{AB})$ quantifies the coherence in a state that can only be accessed using nonlocal incoherent operations. Likewise, $\delta_c(\rho^{AB})$ gives the coherence in ρ^{AB} that requires classical communication to be obtained. The results of Winter and Yang imply that $C_D^{Global}(\Psi) = S(XY)_{\Delta(\Psi)}$ and $C_D^{LIO}(\Psi) = S(X)_{\Delta(\Psi)} + S(Y)_{\Delta(\Psi)} - 2\mathrm{E}(\Psi)$ for a bipartite pure state $|\Psi\rangle^{AB}$ [28]. Combined with Theorem 3, we can compute the two coherence deficits for pure states:

$$\delta(\Psi) = \mathrm{E}(\Psi) - I(X:Y)_{\Delta(\Psi)} \tag{7}$$

$$\delta_c(\Psi) = \mathrm{E}(\Psi). \tag{8}$$

It is curious that the entanglement $\mathrm{E}(\Psi)$ quantifies the coherence gain unlocked by *classical* communication.

Note that a similar phenomenon exists in the resource theory of purity; namely, the quantum deficit $\overline{\Delta}(\Psi)$ and classical deficit $\overline{\Delta}_c(\Psi)$ measure the analogous differences in local purity distillation by so-called "closed operations" (CO), and they are given by $\overline{\Delta}(\Psi) = \overline{\Delta}_c(\Psi) = \mathrm{E}(\Psi)$ [23, 8]. For the task of distilling CoBits, every protocol using incoherent operations can be seen as one using closed operations by accounting for all ancilla systems at the start of protocol [5]. However, closed operations allow for arbitrary unitary rotations, which are forbidden in coherence theory. The term $I(X:Y)_{\Delta(\Psi)}$ in $\delta(\Psi)$ identifies precisely the basis dependence in coherence theory and shows how this decreases the deficit $\delta(\Psi)$ relative $\overline{\Delta}(\Psi)$. On the other hand, there is evidently no basis dependency in the classical deficit $\delta_c(\Psi)$ and it is equivalent to $\Delta_c(\Psi)$.

Although our distillation results so far have only applied to pure states, we can deduce a very general result concerning the distillability of mixed states.

Theorem 5 *A mixed state ρ^{AB} has (LOCC) distillable entanglement iff entanglement can be distilled using LIOCC.*

Strengthening entanglement distillability criterion: As shown in Ref. [9], a state ρ has distillable entanglement iff for some k there exists rank two operators A and B such that the (unnormalized) state $A \otimes B\rho^{\otimes k} A \otimes B$ is entangled. By Theorem 3 and following the same argumentation of Ref. [9], we can further require that the A and B are incoherent operators; that is, they have the form $A = |0\rangle\langle\alpha_0| + |1\rangle\langle\alpha_1|$ and $B = |0\rangle\langle\beta_0| + |1\rangle\langle\beta_1|$ where $\Delta(\alpha_0) := \Delta(|\alpha_0\rangle\langle\alpha_0|)$ is orthogonal to $\Delta(\alpha_1) := \Delta(|\alpha_1\rangle\langle\alpha_1|)$, and likewise for $\Delta(\beta_0) := \Delta(|\beta_0\rangle\langle\beta_0|)$ for $\Delta(\beta_1) := \Delta(|\beta_1\rangle\langle\beta_1|)$. We are thus able to add an additional condition to the distillability criterion of Ref. [9]. We hope that the strengthened distillability criterion can be useful in the long-standing search for NPT bound entanglement.

Discussion: We would like to comment on the particular type of incoherent operations studied in this letter. As noted in the introduction, there have been various proposals for the "free" class of operations in a resource theory of coherence. This letter has adopted the incoherent operations (IO) of Baumgratz *et al.* [2], where each Kraus operator in a measurement just needs to be incoherence-preserving. While the class IO has drawbacks in terms of formulating a full physically consistent resource theory of coherence [30, 5], it nevertheless seems unlikely that the results of this letter would remain true if other operational classes were considered. For example, the strictly incoherent operations (SIO) proposed by Yadin *et al.* are unable to convert one eCoBit into a CoBit [30]. Thus, we believe that the interesting connections between IO coherence theory and entanglement demonstrated in this letter make a positive case for why IO is important in quantum information theory, independent of any other motivation. In fact, one could even put coherence aside and view LIOCC as just being a simplified subset of LOCC. As we have shown here, nontrivial conclusions about entanglement can indeed be drawn by studying LOCC from "the inside." This approach is somewhat dual to the standard practice of studying LOCC using more general separable operations (SEP), the chain of inclusions being LIOCC $\subset$ LOCC $\subset$ SEP. Interesting future work would be to consider more general connections between coherence non-generating and entanglement non-generating operations.

References

[1] J. Äberg, 2006. quant-ph/0612146.

[2] T. Baumgratz, M. Cramer, and M. B. Plenio. Quantifying coherence. *Phys. Rev. Lett.*, 113:140401, Sep 2014.

[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, Nov 1996.

[4] T. R. Bromley, M. Cianciaruso, and G. Adesso. Frozen quantum coherence. *Phys. Rev. Lett.*, 114:210401, May 2015.

[5] E. Chitambar and G. Gour, 2016. arXiv:1602.06969.

[6] E. Chitambar and M.-H. Hsieh, 2016. arXiv:1509.07458.

[7] E. Chitambar, A. Streltsov, S. Rana, M. N. Bera, G. Adesso, and M. Lewenstein. Assisted distillation of quantum coherence. *Phys. Rev. Lett.*, 116:070402, Feb 2016.

[8] M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen. Local information as a resource in distributed quantum systems. *Phys. Rev. Lett.*, 90:100402, Mar 2003.

[9] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80(24):5239–5242, Jun 1998.

[10] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen, and B. Synak-Radtke. Local versus nonlocal information in quantum-information theory: Formalism and phenomena. *Phys. Rev. A*, 71(6):062307, 2005.

[11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865, 2009.

[12] S. F. Huelga and M. B. Plenio. Vibrations, quanta and biology. *Contemp. Phys.*, 54(4):181–207, 2013.

[13] K. Korzekwa, M. Lostaglio, J. Oppenheim, and D. Jennings. 2015.

[14] N. Lambert, Y.-N. Chen, Y.-C. Cheng, C.-M. Li, G.-Y. Chen, and F. Nori. Quantum biology. *Nature Physics*, 9:10, 2013.

[15] F. Levi and F. Mintert. A quantitative theory of coherent delocalization. *New J. Phys.*, 16(3):033007, 2014.

[16] C.-M. Li, N. Lambert, Y.-N. Chen, G.-Y. Chen, and F. Nori. Witnessing quantum coherence: from solid-state to biological systems. *Sci. Rep.*, 2(885), 2012.

[17] S. Lloyd. Quantum coherence in biological systems. *J. Phys.: Conf. Series*, 302(1):012037, 2011.

[18] M. Lostaglio, D. Jennings, and T. Rudolph. Description of quantum coherence in thermodynamic processes requires constraints beyond free energy. *Nature Communications*, 6:6383, 2015.

[19] I. Marvian and R. W. Spekkens, 2016. arXiv:1602.08049.

[20] I. Marvian, R. W. Spekkens, and P. Zanardil, 2015. arXiv:1510.06474.

[21] V. Narasimhachar and G. Gour. Low-temperature thermodynamics with quantum coherence. *Nature Communications*, 6:7689, 2015.

[22] J. Oppenheim, K. Horodecki, M. Horodecki, P. Horodecki, and R. Horodecki. Mutually exclusive aspects of information carried by physical systems: Complementarity between local and nonlocal information. *Phys. Rev. A*, 68:022307, Aug 2003.

[23] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki. Thermodynamical Approach to Quantifying Quantum Correlations. *Phys. Rev. Lett.*, 89:180402, 2002.

[24] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *Quant. Inf. Comput.*, 7(1&2):1–51, Jan 2007.

[25] U. Singh, M. N. Bera, A. Misra, and A. K. Pati. 2015.

[26] A. Streltsov, 2015. arXiv:1511.08346.

[27] G. Vidal. Entanglement monotones. *J. Mod. Opt.*, 47:355, 2000.

[28] A. Winter. Secret, public and quantum correlation cost of triples of random variables. In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pages 2270–2274, Sept 2005.

[29] A. Winter and D. Yang. Operational resource theory of coherence. *Phys. Rev. Lett.*, 116:120404, Mar 2016.

[30] B. Yadin, J. Ma, D. Girolami, M. Gu, and V. Vedral, 2015.

[31] X. Yuan, H. Zhou, Z. Cao, and X. Ma. Intrinsic randomness as a measure of quantum coherence. *Phys. Rev. A*, 92:022124, Aug 2015.

An infinite dimensional Birkhoff's Theorem and LOCC-convertibility

Daiki Asakura[1] *

[1] *Graduate School of Information Systems, The University of Electro-Communications*

Abstract. Nielsen developed that the condition for the LOCC-convertibility of two pure states of a bipartite system in finite dimensional systems is given by a majorization relation of Schmidt cofficients of them. The key of the proof of this is Birkhoff's theorem in matrix theory. In this study, we establish an infinite dimensional version of Birkhoff's theorem and apply them to prove that the condition for LOCC convertibility holds in infinite dimensional systems as in the similar form in finite dimensional.

Keywords: LOCC-convertibility, Birkhoff's theorem, majorization

1 Introduction

Extensive efforts have been devoted to understand local operations and classical communications (LOCC), since LOCC protocols have many applications in quantum information theory. Among them, the convertibility under LOCC is one of the important topics in quantum information theory. Nielsen [1] developed the condition for the LOCC-convertibility of two pure states of a bipartite system in finite dimensional systems.

For pure states $|\psi\rangle\langle\psi|$ and $|\phi\rangle\langle\phi|$ of a bipartite system, we say that $|\psi\rangle\langle\psi|$ is majorized by $|\phi\rangle\langle\phi|$, if the Schmidt coefficients of $|\psi\rangle$ is majorized by those of $|\phi\rangle$. For state vectors $|\psi\rangle$ and $|\phi\rangle$, we say that $|\psi\rangle$ is majorized by $|\phi\rangle$, if the Schmidt coefficents of $|\psi\rangle$ is majorized by those of $|\phi\rangle$. Nielsen [1, 2] proved that

one can convert $|\psi\rangle$ to $|\phi\rangle$ by LOCC

$\iff$ $|\psi\rangle$ is majorized by $|\phi\rangle$.

Subsequently, Owari *et al.* [3] proved that the necessary condition for LOCC convertibility holds in infinite dimensional systems as in the same form in finite dimensional. Moreover, Owari *et al.* [3] introduced a notion of ϵ-convertibility by LOCC in infinite dimensional systems and proved that ϵ-convertibility for LOCC gives a characterization of the sufficient condition.

However, it has been open whether the sufficient condition also holds in infinite dimensional systems as in the same form.

In [2, Section12.5], the key tool and the essence of the Nielsen's proof of the sufficient condition for LOCC convertibility in finite dimensional systems is Birkhoff's theorem in matrix theory.

According to Birkhoff's theorem [4] [5, Section II.2],

(i) the extreme points of the convex set of doubly stochastic matrices are permutation matrices.

(ii) any doubly stochastic matrix can be represented as a convex combination of permutation matrices,

(iii) the set of doubly stochastic matrices coincides with the closed convex hull of the set of permutation matrices.

Moreover, (i), (ii), (iii) imply each other by Caratheodory Theorem.

Nielsen used Birkhoff's theorem (ii) in [2, Section12.5].

An infinite dimensional analogue of Birkhoff's theorem is known as Birkhoff's problem111, which was considered in [6, 7, 8, 9, 10, 11, 12] etc. Nevertheless, there is no study treated (ii). Unlike the finite dimensional case, (i), (ii) and (iii) are not always equivalent to each other in infinite dimensional case. Moreover in infinite dimensional cases (i) remained true, whereas the validity of (ii) and (iii) depend on the choice of topology. While in finite dimensional case (ii) is equivalent to (iii) by virtue of Caratheodory Theorem, in infinite dimensional case the assertion of (ii) can be stronger than the one of (iii).

In this study, we establish an infinite dimensional version of Birkhoff's theorem (i)(ii)(iii) with the weakly operator topology (WOT). In particular, we show that an infinite dimensional analogue of (ii) holds in WOT, and we apply this to prove a new characterization for LOCC-convertibility in infinite dimensional. Our characterization, of course, is a certain generalization of Nielsen's result. Moreover, our characterization implies the results of Owari *et al.* [3] as a corollary.

2 Main results

Let $\mathcal{H}$ be separable (at most countable infinite dimensional) Hilbert space. For a fixed CONS $(|i\rangle)_{i=1}^{\infty}$, let $\mathcal{P}(\mathcal{H})$, $\mathcal{D}(\mathcal{H})$ be the sets of bounded operators $\sum_{i,j=1}^{\infty} a_{ij}|i\rangle\langle j|$ satisfying the following (P), (D):

$$(P)\ a_{ij} = 0 \,\text{or}\, 1,\ \sum_{j=1}^{\infty} a_{ij} = 1,\ \sum_{i=1}^{\infty} a_{ij} = 1 \text{ (for any } i,j)$$

$$(D)\ a_{ij} \in [0,1],\ \sum_{j=1}^{\infty} a_{ij} = 1,\ \sum_{i=1}^{\infty} a_{ij} = 1 \text{ (for any } i,j).$$

Then, we can rewrite Birkhoff's theorem(ii) as following:

Theorem1(Birkhoff [4]) When $\mathcal{H} = \mathbb{C}^d$ and $(|i\rangle)$ is the standard basis in $\mathbb{C}^d$, denoting $\mathcal{P}(\mathcal{H}) =: \{P_n\}_{n=1}^{d!}$, for any $D \in \mathcal{D}(\mathcal{H})$, there exists a probability mass $\{p_n\}_{n=1}^{d!}$ such that

$$D = \sum_{n=1}^{d!} p_n P_n.$$

In this study, we get the following result:

*asakura0d@gmail.com

Theorem2(Asakura) For any $D \in \mathcal{D}(\mathcal{H})$, there exists a probability measure μ_D on $\mathcal{P}(\mathcal{H})$ such that

$$D = \int_{\mathcal{P}(\mathcal{H})} X d\mu_D(X),$$

where the integral converges in WOT.

3 Main result(2) : LOCC-convertibility

Nielsen's theorem [1] [2, Section12.5] can be written mathematically as following:

Theorem3(Nielsen[1, 2]) Let $\mathcal{H}$ and $\mathcal{K}$ be finite dimensional Hilbert spaces, and let ψ, $\phi \in \mathcal{H} \otimes \mathcal{K}$ be unit vectors. Then, the followings are equivalent.

- There exist a POVM $\{M_i\}_i$ on $\mathcal{H}$ and a set of unitary operators $\{U_i\}_i$ $\mathcal{K}$ such that

  $$|\phi\rangle\langle\phi| = \sum_i (M_i \otimes U_i)|\psi\rangle\langle\psi|(M_i^* \otimes U_i^*), \qquad (1)$$

  where the sum is finite sum.
- $\mathrm{Tr}_{\mathcal{K}} |\psi\rangle\langle\psi| \prec \mathrm{Tr}_{\mathcal{K}} |\phi\rangle\langle\phi|$ holds.

In this study, applying Theorem 2, we prove the following infinite dimensional analogue of Theorem 3. The following theorem is main results.

Theorem4(Asakura) Let $\mathcal{H}$ and $\mathcal{K}$ be infinite dimensional Hilbert spaces, and let ψ, $\phi \in \mathcal{H} \otimes \mathcal{K}$ be full rank unit vectors. Then, the followings are equivalent.

- There exist a Borel set I of a certain of metric space, a probability mesure μ on I, a set of densely defined (not necessarily bounded) operators $\{M_i\}_{i\in I}$ on $\mathcal{H}$, a dense subspace $\mathcal{H}_0 \subset \mathcal{H}$ and a set of unitary operators $\{U_i\}_{i\in I}$ on $\mathcal{K}$ such that

  $$|\psi\rangle \in \mathrm{D}(M_i \otimes U_i),\ i \in I, \qquad (2)$$

  $$(\mathrm{Tr}_{\mathcal{K}}|\psi\rangle\langle\psi|)\mathcal{H}_0 \subset \mathcal{H}_0, \qquad (3)$$

  $$\mathrm{D}(M_i) \supset \mathcal{H}_0,\ i \in I \qquad (4)$$

  $$\int_I \langle\eta|{M_i}^* M_i|\xi\rangle d\mu(i) = \langle\eta|\xi\rangle,\ \text{for } \eta, \xi \in \mathcal{H}_0, \qquad (5)$$

  $$I \ni i \mapsto (M_i \otimes U_i)|\psi\rangle\langle\psi|(M_i^* \otimes U_i^*) \in \mathfrak{C}_1(\mathcal{H}) \text{ is integrable}, \qquad (6)$$

  $$|\phi\rangle\langle\phi| = \int_I (M_i \otimes U_i)|\psi\rangle\langle\psi|(M_i^* \otimes U_i^*)d\mu(i),$$

  where the integral convergesges in $\mathfrak{C}_1(H)$. (7)
- $\mathrm{Tr}_{\mathcal{K}} |\psi\rangle\langle\psi| \prec \mathrm{Tr}_{\mathcal{K}} |\phi\rangle\langle\phi|$ holds.

In general case, Theorem 4 becomes the following theorem, which immediately follows from Theorem 4.

Theorem6(Asakura) Let $\mathcal{H}$ and $\mathcal{K}$ be infinite dimensional Hilbert spaces, and let ψ, $\phi \in \mathcal{H} \otimes \mathcal{K}$ be unit vectors.

- There exist $(I,\ \mu,\ \{M_i\}_{i\in I},\ \mathcal{H}_0,\ \{U_i\}_{i\in I})$ in Theorem 4 and infinite rank partial isometries $V_{\mathcal{H}}$, $V_{\mathcal{K}}$ such that

  $$|\phi\rangle\langle\phi| = (V_{\mathcal{H}} \otimes V_{\mathcal{K}})\Big(\int_I (M_i \otimes U_i)|\psi\rangle\langle\psi| (M_i^* \otimes U_i^*)d\mu(i)\Big)({V_{\mathcal{H}}}^* \otimes {V_{\mathcal{K}}}^*) \qquad (8)$$
- $\mathrm{Tr}_{\mathcal{K}} |\psi\rangle\langle\psi| \prec \mathrm{Tr}_{\mathcal{K}} |\phi\rangle\langle\phi|$ holds.

Moreover, by Theorem 6, we can construct a sequence of LOCC-quantum channel $\{\Lambda_n\}_n$ such that $\Lambda_n(|\psi\rangle\langle\psi|)$ converges (8) in the trace norm. Namely, we reprove the following result as a corollary of Theorem 6:

Theorem7(Owari*et al.* [3])

Let $\mathcal{H}$ and $\mathcal{K}$ be infinite dimensional Hilbert spaces, and let ψ, $\phi \in \mathcal{H} \otimes \mathcal{K}$ be unit vectors. If $\mathrm{Tr}_{\mathcal{K}} |\psi\rangle\langle\psi| \prec \mathrm{Tr}_{\mathcal{K}} |\phi\rangle\langle\phi|$ holds, then, for any $\epsilon > 0$, there exists a LOCC quantum channel Λ_ϵ such that

$$\|\Lambda_\epsilon(|\psi\rangle\langle\psi|) - |\phi\rangle\langle\phi|\|_1 < \epsilon.$$

References

[1] M.A.Nielsen, "Condition for a class of entanglement transformations", Physical Review Letters, Vol.83, Issue2 :436-439(1999)

[2] M.A.Nielesen, I.L.Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[3] M. Owari, S. L. Braunstein, K. Nemoto, M. Murao, " ε -convertibility of entangled states and extension of Schmidt rank in infinite dimensional systems", Quantum Information and Computation, Vol.8 :30-52(2008)

[4] G. Birkhoff. "Three observations on linear algebra".(Spanish) Univ. Nac. Tucuman. Revista A. 5 :147-151(1946)

[5] R. Bhatia, *Matrix Analysis*, Springer, New York, 1997.

[6] G. Birkhoff. *Lattice Theory*, revised ed., Amer. Math. Soc. Colloquium Pub., vol 25, 1948

[7] G. Birkhoff. *Lattice Theory*, third ed., Amer. Math. Soc. Colloquium Pub., vol 25, 1967

[8] Y. Safarov, "Birkoff's theorem and multidimensional spectra", Journal of Functional Analysis 222 :61-97(2005)

[9] J.R,Isbell, "Infinite Doubly Stochastic Matrices", Canada. Math .Bull. Vol.5, no.1 :1-4(1961)

[10] D.G.Kendall, "On Infinite Doubly Stochastic Matrices and Birkoff's problem". J. London Math. Soc.35 :81-84(1960)

[11] B. A. Rattray, J. E. L. Peck, "Infinite stochastic matrices", Trans. Roy. Soc. Canada. Sect. III. (3) 49 :55-57(1955)

[12] R. Grząślewicz. "On extreme infinite doubly stochastic matrices". Illinois Journal of Mathematics 31, no. 4 :529-543(1987)

How local is the information in MPS/PEPS tensor networks? (extended abstract)

Anurag Anshu[1] *   Itai Arad[1] †   Aditya Jain[2] ‡

[1] *Centre for Quantum Technologies, National University of Singapore, Singapore*
[2] *Center for Computational Natural Sciences and Bioinformatics, International Institute of Information Technology-Hyderabad, India*

Abstract. We introduce a new approach for approximating the expectation value of a local observable in ground states of local Hamiltonians that are represented as PEPS tensor-networks. Instead of contracting the full tensor-network, we estimate the expectation value using only a local patch of the tensor-network around the observable. Surprisingly, we demonstrate that this is often easier to do when the system is frustrated. We test our approach in 1D systems, where we show how the expectation value can be calculated up to at least 3 or 4 digits of precision, even when the patch radius is smaller than the correlation length.

Keywords: Local Hamiltonians, Ground states, Tensor networks, MPS, PEPS, SDP

1 Introduction

Variational tensor-network methods [1] provide a promising way for understanding the low-temperature physics of many-body condensed matter systems. In particular, they seem suitable for studying the ground states of highly frustrated systems, where the sign problem hinders many of the quantum Monte Carlo approaches. The best-known and by far the most successful tensor-network method is the Density Matrix Renormalization Group (DMRG) algorithm [2, 3]. It can be viewed as a variational algorithm for minimizing the energy of the system over the manifold of *Matrix Product States* (MPS) [4, 5], which are special types of tensor-network states a with linear 1D structure. In 2D and beyond the most natural generalization of MPS are the so-called *Projected Entangled Pairs States* (PEPS) tensor-network states [6, 7, 8, 9, 10]. PEPS have proven useful for understanding the physics of 2D lattice systems and in particular their entanglement structure. However, as a numerical method for studying 2D quantum systems, they still face substantial challenges which limit their applicability. In most cases, the best results are still obtained either by DMRG, in which a 1D MPS wraps around the 2D surface, or by quantum Monte Carlo methods.

There are several reasons for this qualitative difference between 1D and 2D systems. The most important one is the computational cost of *contracting* the 2D tensor network. While in 1D this cost scales linearly in the system size, it is exponential for 2D and above. Formally, contracting a PEPS is #P-hard [11], which is at least NP-hard. To overcome this exponential barrier, many approximation schemes have been devised [9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20]. However, while being physically motivated, none of them is rigorous, and to some extent they all produce uncontrolled approximations, even when dealing with the ground state itself. Moreover, while their computational cost is linear in PEPS size, it scales badly in the so-called 'bond-dimension' of the tensor-network, which limits their practical use to small systems/resolutions.

In this work we introduce a new approach for approximating the expectation value of a local observable in a 2D PEPS tensor-network. Our starting point is a simple observation that while the contraction of a general 2D PEPS is #P-hard, this is not necessarily the case if the PEPS describes a ground state of a gapped local Hamiltonian. Gapped ground states exhibit strong properties of locality, such as exponential decay of correlations [21] and are therefore subject to many constraints to which arbitrary PEPS are not. This enables us to use only a *local patch* of the PEPS tensor-network around the local observable to approximate its expectation value, which therefore leads to an efficient algorithm.

We identify two novel methods that provide *rigorous* upper- and lower- bounds on the expectation value. While we usually cannot give rigorous bound on the distance between these bounds, we demonstrate numerically that this distance – and hence the error in our approximation – can be surprisingly small.

The first method, which we call the 'basic method', is expected to give good results in the case of frustration-free gapped systems. The second one, which we call the 'commutator gauge optimization' (CGO) method, works only for frustrated systems by utilizing the many inter-constraints that the solutions of these systems have to satisfy. We show that it can be essentially reduced to a SDP program, which can be efficiently solved. In addition, it does not rely directly on the existence of a gap, and may work even when considering patches of the PEPS that are much smaller than the correlation length.

To test the validity of the two methods, we performed some numerical tests on 1D systems whose ground states are described by MPS. The main purpose of these tests was *not* to suggest a *practical* numerical method for estimating $\langle B\rangle$, but to demonstrate that a surprisingly large amount of information is found locally in a tensor network that represents a ground state, in particular if the system is frustrated – which is counter-intuitive.

*henrikabel.27@gmail.com
†arad.itai@fastmail.com
‡aditya.jain@research.iiit.ac.in

Our numerical experiments demonstrate that in the frustrated case, one can easily obtain 3-4 digits of $\langle B \rangle$ by accessing only a ball of radius $\ell \sim 3, 4$ around B — smaller than the correlation lengths of these models! Moreover, as we indicated above, this is better than the frustration-free case, where we could only recover 1-2 digits of $\langle B \rangle$. The full details of these numerical experiments can be found in the arXiv version of this paper at http://arxiv.org/abs/1603.06049.

While a *direct* implementation of the above methods for 2D systems is *not* numerically practical for 2D, we are confident that the observations underlying these algorithms can be turned into practical heuristics for the 2D problem.

References

[1] R. Orús, "A practical introduction to tensor networks: Matrix product states and projected entangled pair states," *Annals of Physics*, vol. 349, pp. 117 – 158, 2014.

[2] S. R. White, "Density matrix formulation for quantum renormalization groups," *Phys. Rev. Lett.*, vol. 69, pp. 2863–2866, Nov 1992.

[3] S. R. White, "Density-matrix algorithms for quantum renormalization groups," *Phys. Rev. B*, vol. 48, pp. 10345–10356, Oct 1993.

[4] S. Östlund and S. Rommer, "Thermodynamic limit of density matrix renormalization," *Physical review letters*, vol. 75, no. 19, p. 3537, 1995.

[5] S. Rommer and S. Östlund, "Class of ansatz wave functions for one-dimensional spin systems and their relation to the density matrix renormalization group," *Physical Review B*, vol. 55, no. 4, p. 2164, 1997.

[6] G. Sierra and M. A. Martin-Delgado, "The Density Matrix Renormalization Group, Quantum Groups and Conformal Field Theory," *arXiv preprint cond-mat/9811170*, 1998.

[7] Y. Hieida, K. Okunishi, and Y. Akutsu, "Numerical renormalization approach to two-dimensional quantum antiferromagnets with valence-bond-solid type ground state," *New Journal of Physics*, vol. 1, no. 1, p. 7, 1999.

[8] T. Nishino, Y. Hieida, K. Okunishi, N. Maeshima, Y. Akutsu, and A. Gendiar, "Two-Dimensional Tensor Product Variational Formulation," *Progress of Theoretical Physics*, vol. 105, no. 3, pp. 409–417, 2001.

[9] F. Verstraete and J. I. Cirac, "Renormalization algorithms for Quantum-Many Body Systems in two and higher dimensions," *eprint arXiv:cond-mat/0407066*, July 2004.

[10] F. Verstraete, V. Murg, and J. I. Cirac, "Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems," *Advances in Physics*, vol. 57, no. 2, pp. 143–224, 2008.

[11] N. Schuch, M. M. Wolf, F. Verstraete, and J. I. Cirac, "Computational complexity of projected entangled pair states," *Phys. Rev. Lett.*, vol. 98, p. 140506, Apr 2007.

[12] T. Nishino and K. Okunishi, "Corner transfer matrix renormalization group method," *Journal of the Physical Society of Japan*, vol. 65, no. 4, pp. 891–894, 1996.

[13] R. Orús and G. Vidal, "Simulation of two-dimensional quantum systems on an infinite lattice revisited: Corner transfer matrix for tensor contraction," *Phys. Rev. B*, vol. 80, p. 094403, Sep 2009.

[14] R. Orús, "Exploring corner transfer matrices and corner tensors for the classical simulation of quantum lattice systems," *Phys. Rev. B*, vol. 85, p. 205117, May 2012.

[15] L. Vanderstraeten, M. Mariën, F. Verstraete, and J. Haegeman, "Excitations and the tangent space of projected entangled-pair states," *Phys. Rev. B*, vol. 92, p. 201111, Nov 2015.

[16] M. Levin and C. P. Nave, "Tensor renormalization group approach to two-dimensional classical lattice models," *Phys. Rev. Lett.*, vol. 99, p. 120601, Sep 2007.

[17] Z. Y. Xie, H. C. Jiang, Q. N. Chen, Z. Y. Weng, and T. Xiang, "Second renormalization of tensor-network states," *Phys. Rev. Lett.*, vol. 103, p. 160601, Oct 2009.

[18] H. H. Zhao, Z. Y. Xie, Q. N. Chen, Z. C. Wei, J. W. Cai, and T. Xiang, "Renormalization of tensor-network states," *Phys. Rev. B*, vol. 81, p. 174411, May 2010.

[19] Z. Y. Xie, J. Chen, M. P. Qin, J. W. Zhu, L. P. Yang, and T. Xiang, "Coarse-graining renormalization by higher-order singular value decomposition," *Phys. Rev. B*, vol. 86, p. 045139, Jul 2012.

[20] I. Pižorn, L. Wang, and F. Verstraete, "Time evolution of projected entangled pair states in the single-layer picture," *Phys. Rev. A*, vol. 83, p. 052321, May 2011.

[21] M. B. Hastings, "Lieb-Schultz-Mattis in higher dimensions," *Phys. Rev. B*, vol. 69, p. 104431, Mar 2004.

Information-theoretical analysis of topological entanglement entropy and multipartite correlations

Kohtaro Kato[1] *   Fabian Furrer[1 2] †   Mio Murao[1 3] ‡

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, Tokyo, Japan*
[2] *NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Kanagawa, Japan*
[3] *Institute for Nano Quantum Information Electronics, The University of Tokyo, Tokyo, Japan*

Abstract. A special feature of the ground state in a topologically ordered phase is the existence of large-scale correlations depending only on the topology of the regions. These correlations can be detected by the topological entanglement entropy or by a measure called irreducible correlation. We show that these two measures coincide for states obeying an area law and having zero-correlation length. Moreover, we provide an operational meaning for these measures by proving its equivalence to the optimal rate of a particular class of secret sharing protocols. This establishes an information-theoretical approach to multipartite correlations in topologically ordered systems.

Keywords: topological order, multipartite correlations, conditional mutual information, maximum entropy method, secret sharing

1 Introduction

Topologically ordered phase is an exotic quantum phase that cannot be explained by conventional models based on *local* order parameters and symmetry-breaking. One way to classify the ground states with topological orders is by identifying characteristic large-scale global multipartite correlations (topological correlations). A possible measure to detect such topological correlations is the topological entanglement entropy (TEE) [1, 2], which also appears as the universal constant term in the area law [1]. The definition of the TEE is based on the idea that topological correlations reduce the entropy of ring-like regions compared to what is expected by considering the entropy of just local regions [2]. More precisely, the TEE quantifies the entropy reduction by subtracting the contributions of local correlations using a Venn-diagram calculation. Such a quantity of multipartite correlations is known in classical information theory [3]. However, the information-theoretical meaning of the function in both classical and quantum settings is not clear, since it lacks basic properties such as, e.g., positivity and it is always zero for any pure state in quantum settings.

The *irreducible correlation* [4] is an alternative measure of topological correlations which employs the maximum entropy method to quantify the genuinely tripartite correlations. The irreducible correlation is always non-negative, and it has a clear geometrical interpretation as the quantum analog of a correlation measure called the kth-order effect [5] in classical information-geometry. It has been conjectured that the 3rd-order irreducible correlation and the TEE coincide in the thermodynamic limit for gapped ground states [6].

Here, we partly resolve this conjecture and show that when the ground state obeys an area law and has zero-correlation length, the TEE and the 3rd-order irreducible correlation are equivalent. This sufficient condition holds for a wide class of exactly solvable spin models which describe non-chiral topological ordered phases. To show the equivalence, we calculate the 3rd-order irreducible correlation by explicitly constructing the maximum entropy state on region ABC that is consistent with all reduced density matrices (RDMs) of the ground state on AB, BC and AC. In general, calculating the maximum entropy state is a computationally hard problem. We overcome this challenge by employing the properties of *quantum Markov states* which saturate the strong subsdditivity [7].

We further show that under the same assumptions the irreducible correlation is equal to the optimal asymptotic rate of a secret sharing protocol as suggested in [4]. This leads to an operational interpretation of the TEE as the number of bits that can be hidden in global regions from any party that only has access to local regions.

2 Summary of results

Let us consider the RDMs of the ground state of a gapped spin lattice system on circle or ring-like regions ABC given in Fig. 1. We then define the TEE by

$$S_{\text{topo}} \equiv S_\rho(AB) + S_\rho(BC) + S_\rho(CA) - S_\rho(A) - S_\rho(B) - S_\rho(C) - S_\rho(ABC)\,, \quad (1)$$

which is in accordance with the one considered by Kitaev and Preskill [1]. Here, $S_\rho(A)$ represents the von Neumann entropy of the RDM ρ_A of region A. For regions as given in Fig. 1(c) , the above definition is consistent

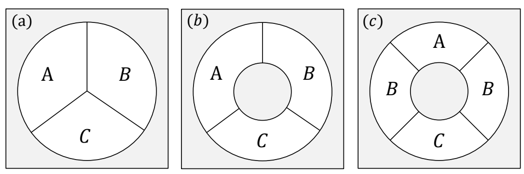


Figure 1: Examples of the region ABC for the calculation of TEE. The value of TEE of (a) is a half of others for a topologically ordered ground state due to the difference of the topology of the whole region ABC.

*kato@eve.phys.s.u-tokyo.ac.jp
†furrer@eve.phys.s.u-tokyo.ac.jp
‡murao@phys.s.u-tokyo.ac.jp

with the one by Levin and Wen [2] if it is possible to assume that there is no correlation between A and C, i.e., $\rho_{AC} = \rho_A \otimes \rho_C$. The TEE is interpreted as the difference between the entropy of ABC and the expected entropy of ABC by considering the entropy of just local regions [2].

Let us consider the closed convex set R^2_ρ of states which is consistent with all bipartite RDMs of ρ_{ABC}

$$R^2_\rho \equiv \{\sigma_{ABC} \mid \sigma_{AB} = \rho_{AB}, \sigma_{BC} = \rho_{BC}, \sigma_{AC} = \rho_{AC}\} \,. \tag{2}$$

We define the maximum entropy state by the state in R^2_ρ which maximizes the von Neumann entropy, i.e.,

$$\tilde{\rho}^{(2)}_{ABC} \equiv \underset{\sigma_{ABC} \in R^2_\rho}{\arg\max}\, S_\sigma(ABC) \,. \tag{3}$$

According to the maximum entropy principle, the maximum entropy state is the most "unbiased" inference of ρ_{ABC} if all of the bipartite marginals are known.

We define the 3rd-order irreducible correlation $C^{(3)}(\rho_{ABC})$ as [4]

$$C^{(3)}(\rho_{ABC}) \equiv S_{\tilde{\rho}^{(2)}}(ABC) - S_\rho(ABC) \,. \tag{4}$$

Note that the irreducible correlation has a clear information-geometric meaning as the distance from the closure of the set of all Gibbs states of 2-local Hamiltonians [8].

Our main result is that if the ground state satisfy the two properties in the following, the TEE is equivalent to the 3rd-order irreducible correlation.

(I) If two regions A and B are separated, $I_\rho(A:B) \equiv S_\rho(A) + S_\rho(B) - S_\rho(AB) = 0$.

(II) If region A and C are indirectly connected through B and ABC has no holes, ρ_{ABC} has zero conditional mutual infromation $I_\rho(A:C|B) \equiv I_\rho(A:BC) - I_\rho(A:B) = 0$.

Theorem 2.1 *If a ground state on a 2D spin lattice satisfies properties (I) and (II), the equality*

$$S_{\text{topo}} = C^{(3)}(\rho_{ABC}) \tag{5}$$

holds for all choices of regions depicted in Fig. 1.

It is widely accepted that a ground state in a gapped system obeys an area law of entanglement entropy for any connected region A with smooth boundaries, that is,

$$S_\rho(A) = \alpha|\partial A| - \gamma + \mathcal{O}(|\partial A|^{-1}) \,, \tag{6}$$

where α denotes a non-universal constant, $|\partial A|$ denotes the size of the boundary of region A. γ is another definition of the TEE and is equivalent to S_{topo} for the configuration in Fig. 1(a). In models with zero-correlation length, $\mathcal{O}(|\partial A|^{-1})$ can be negligible and the ground state satisfy both properties (I) and (II).

The key idea of the proof is to divide each region shown in Fig.1 so that each RDM is a quantum Markov state (QMS). A QMS conditioned on B is a tripartite state that satisfies property (II), i.e., $I_\rho(A:C|B) = 0$ [7]. We develop a technique of merging overlapping marginal QMS to construct the maximum entropy state $\tilde{\rho}^{(2)}_{ABC}$ by using the equivalence condition revealed in Ref. [7].

The equivalence of the TEE to the 3rd-order irreducible correlation also provides an operational interpretation of the TEE. Recall that if $C^{(3)}(\rho_{ABC})$ is nonzero, the global state in region ABC contains information that cannot be determined only from the marginals on AB, BC or AC. A similar situation is encountered in secret sharing protocols. It has been shown [4, 9] that for stabilizer states, the kth-order irreducible correlation of a n-partite state represents the difference between the asymptotic bit rate that can be hidden from k and from $k-1$ parties, where secrets are encoded by global unitaries which preserves all k (or $k-1$) RDMs. We show that this also holds true in our setting for $n = 3$ and $k = 2$.

Theorem 2.2 *For a tripartite state ρ_{ABC} satisfying properties (I) and (II), the equality*

$$r(\rho_{ABC}) = C^{(3)}(\rho_{ABC}) \tag{7}$$

holds for all choices of regions depicted in Fig. 1, where $r(\rho_{ABC})$ is the optimal secret sharing rate.

Thus, we provide new geometrical and operational meanings of the TEE. Our results motivate us to investigate the relationships between characteristic properties of topological orders by utilizing these information-theoretical meanings.

Acknowledgment

This work is supported by ALPS, the Project for Developing Innovation Systems of MEXT, Japan, and JSPS KAKENHI (Grant No. 26330006, No.24-02793 and No.15H01677). We also gratefully acknowledge the ELC project (Grant-in-Aid for Scientific Research on Innovative Areas MEXT KAKENHI (Grant No. 24106009)).

References

[1] A. Kitaev and J. Preskill. *Phys. Rev. Lett.*, 96:110404, 2006.

[2] M. A. Levin and X.-G. Wen. *Phys. Rev. Lett.*, 96:110405, 2006.

[3] W. J. McGill. *Psychometrika*, 19(2):97–116, 1954.

[4] D. L. Zhou. *Phys. Rev. Lett.*, 101:180505, Oct 2008.

[5] S.-I. Amari. *IEEE Trans. Inf. Theory*, 47(5):1701–1711, Jul 2001.

[6] J. Chen, et al. *New Journal of Physics*, 17(8):083019, 2015.

[7] P. Hayden, et al. *Comm. Math. Phys.*, 246(2):359–374, 2004.

[8] S. Weis. *AIP Conference Proceedings*, 1641, 2015.

[9] D. L. Zhou and L. You. *arXiv:quant-ph/0701029*, 2007.

Phase-like transitions in low-number quantum dots Bayesian magnetometry

Paweł Mazurek[1] * Michał Horodecki[1] Łukasz Czekaj[1] Paweł Horodecki[2 3]

[1] *Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*
[2] *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Narutowicza 11/12, 80-233 Gdańsk, Poland*
[3] *National Quantum Information Centre in Gdańsk, Andersa 27, 81-824 Sopot, Poland*

Abstract. We investigate metrological properties of systems of quantum dot electron spin qubits. Optimal strategies for probing the value of an external, static magnetic field are provided within Bayesian approach, with initial knowledge about the magnetic field described by its a priori Gaussian probability distribution. We report phase-like transitions between optimal protocols occurring during the system evolution. We show that optimal scenario requires initial entanglement and point out benefits of classical strategies for longer evolution times. We observe that non-Markovian effects, stemming from the interaction with environment, can provide limited metrological advantage for small magnetic fields. The full version of the paper is available at arXiv:1605.04279.

Keywords: quantum metrology, quantum dots, noise

1 Introduction

Quantum metrology relies on the fact that quantum correlations make state evolution more sensitive to dynamics which depends on some parameter that is supposed to be revealed. It is known that, in the so called frequentist approach, for estimating small variations of a deterministic parameter, for locally unbiased estimators dependent on its value and N systems undergoing independent evolution, quantum mechanics can offer a $1/N$ (so called Heisenberg scaling) improvement of the precision (defined by the deviation from the precise value) in the asymptotic limit. This should be compared to a scaling $1/\sqrt{N}$, available for classical resources, and referred to as quantum shot-noise limit. Generally it is known that in a situation when the parameter is a phase generated by some Hamiltonian evolution, then the local noise usually destroys the quantum effect (both in atomic spectroscopy and quantum optics), leading to at most constant improvement over classical scaling.

In the so-called Bayesian approach this scenario is altered so that the parameter to be estimated is a random variable with some a priori probability distribution. In many cases, this framework is more justified than the frequentist approach: it does not assume perfect knowledge about a system under consideration before an experiment and it outputs optimal estimators even for small N. We apply Bayesian metrology to a physical scenario where the form of the noise depends on the parameter. Specifically, we analyze a system of independent quantum dots interacting via hyperfine interaction with their local, maximally mixed spin environments [1], under a so called box model approximation. Spins of the electron dots are subject to external time independent magnetic field B with the random value characterized by the Gaussian probability distribution with a variance $\Delta^2 B_{prior}$ and mean B_0. The Bayesian approach allows to diminish the average mean square error of magnetic field estimator. It relies on measurements that may depend on time.

Our aim was to find the optimal initial state and measurement scheme which results in the smallest relative mean square error $\frac{\Delta^2 B_{est}}{\Delta^2 B_{prior}}$ of the estimator – a signature of the gain of information about the field. It is achieved by numerical optimization [2] yielding optimal strategies for given time of the evolution and initial probability distribution. The system evolution was solved analytically within the ,,box model" of hyperfine interaction, applicable in time regime that encompasses small times, where metrologicalally important effects occur.

2 Main results

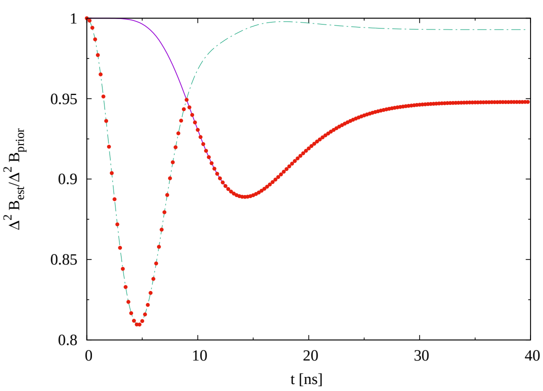


Figure 1: Comparison between 'perpendicular' (green dashed line) and 'parallel' (solid purple line) strategies for 1 quantum dot and prior Gaussian distribution with $B_0 = 7$ mT, $\Delta B_{prior} = 4$ mT. Red points represent the optimal strategy.

In order to sketch the action of noise on the evolution of the system, we start with a single qubit and com-

*pawel.mazurek@ug.edu.pl

pare two strategies, each optimal in different time regime (Fig. 1). The perpendicular strategy relies on preparing the state in Bloch sphere perpendicular to the field direction, and performing measurements of an observable represented by a Bloch sphere vector perpendicular to both field and state vectors. The parallel strategy relies on preparing the state in the direction of the magnetic field, and performing projective measurements along this direction. For large fields, the dynamics does not change populations of the system, hence the estimating of magnetic field can be done only through the phase, and perpendicular strategy is the optimal one, as in a case of a simple unitary evolution. The single minimum in the strategy comes from a trade-off between the damping of phase (resulting both from statistical averaging over prior field probability distribution and physical noise), and the rotation of the phase by magnetic field. For times long enough so that the coherences are nearly completely damped, the state ceases to depend on the magnetic field, hence there is no information gain. For intermediate magnetic fields, the populations of the system start to be effected by the magnetic field, and measurements of the occupation levels lead to information gain dominant in longer times. One should note that for small magnetic fields the ,,perpendicular" strategy proves to be effective even in the long time regime. This can be explained by the fact that, due to the memory effects stemming from the interaction with the environment, the coherences experience a revival to the value dependent on B and remain unaffected by the phase factors of the type $\exp[ig\mu_B Bt]$, which for non-zero $\Delta^2 B_{prior}$ would lead to their decay. Clearly, apart from the mentioned minor memory effects, the long time regime is entirely classical, as the estimation there is purely statistical, while in the short time regime, quantum coherences are crucial. For this reason, for more particles in non-negligible magnetic field, only for low times entanglement will lead to enhancement of estimation.

Indeed, by performing similar studies for systems of $N = 2, \ldots, 5$ dots, as well as Monte Carlo simulations, we showed that entanglement is the necessary resource for achieving the global optimum. In description of these systems below, we use the notation in which magnetic field is directed along z axis, and eigenstates of z-component of electron spin operator are given by $\hat{S}^z|0\rangle = \frac{\hbar}{2}|0\rangle$, $\hat{S}^z|1\rangle = -\frac{\hbar}{2}|1\rangle$, and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We denote GHZ(N)$= \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.

A feature characteristic for transition into larger systems is the growing structural complexity of the region that relies on product coherence states. We showed that the general sequence of optimal states for small number N of quantum dots is the following: (1) regime of initially entangled states, with (1a) regime of GHZ(N) and (1b) regime of GHZ(N) superposed with $|+\rangle^{\otimes N}$; (2) intermediate regime of optimal product coherent states $|+\rangle^{\otimes N-1}|0\rangle$, followed by $|+\rangle^{\otimes N-2}|0\rangle|0\rangle$, end so on; (3) regime of product states without coherences $|0\rangle^{\otimes N}$.

Transitions within the region (1) are characterized by a continuous change of the optimal initial state, while transitions inside (2) region, as well transitions (1)-(2) and (2)-(3), signalize a non-continuous change of the optimal initial state. One should note that the precision of field estimation grows with increasing N for all possible times of performing the measurements, with time of optimal information gain not strongly depending on N. We stress that for the regimes (2) and (3), in contrast with the entanglement regime (1), the effects associated with lack of initial knowledge described by a non-zero $\Delta^2 B_{prior}$ play a secondary role and the physical noise for longer times is solely beneficial for magnetometric purposes. Note that the whole regime is absent for a unitary evolution, which implies lack of discontinuous transitions in the optimal state space.

3 Discussion

The presented physical model enables the structure of the measurement strategy, involving measurement of occupation levels, to partially recover information that, due to noise, becomes inaccessible for phase-based measurements. Nevertheless, it does not enable to win over the noisless case, which for all investigated a priori Gaussian probability distributions achieve better information gains optimized over initial state, measurement strategy and time of performing the measurement.

The standard situation considered in the literature is when the parameter under consideration (here the magnetic field) is encoded into the system *directly* and the noise can only destroy that information. Here the dynamics makes the parameter imprinted both on the system and environment or - strictly speaking - into a global state of both. Despite the fact that the initial ancillas are maximally noisy and that the final noisy dynamics acts here completely locally, the corresponding noise is unavoidably ,,convoluted" with the original dynamics and the final result is such that we get the product noisy dynamics which has the parameter imprinted in a *nonstandard*, nonlinear way. On the other hand the imprinting the magnetic field by unitary dynamics is restricted to the Bloch sphere. Effectively we have then the two scenarios. In the latter the parameter is imprinted in the states on the sphere, while in the former, it is imprinted in the mixed states that in general belong to the interior of the sphere. It seems that this is *the geometry* of the two sets out of which only the one has the nonzero volume, that in general might make the difference in favor of the noisy scenario.

References

[1] Mazurek, P., Roszak, K., Chhajlany, R. W. & Horodecki, P. Sensitivity of entanglement decay of quantum-dot spin qubits to the external magnetic field. *Phys. Rev. A* **89**, 062318 (2014).

[2] Macieszczak, K., Fraas, M. & Demkowicz-Dobrzański, R. Bayesian quantum frequency estimation in presence of collective dephasing. *New Journal of Physics* **16**, 113002 (2014)

Separation between quantum Lovász number and entanglement-assisted zero-error classical capacity

Xin Wang[1] * Runyao Duan[1 2] †

[1] *Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology Sydney (UTS), NSW 2007, Australia*

[2] *UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*

Abstract. Before our work, it was unknown that whether the quantum Lovász number always coincides with the entanglement-assisted zero-error classical capacity of a quantum channel. In this paper, we resolve this open problem by explicitly constructing a class of qutrit-to-qutrit channels whose quantum Lovász number is strictly larger than its entanglement-assisted zero-error classical capacity. Interestingly, this class of channels is reversible in the presence of quantum no-signalling correlations.

Keywords: Zero-error classical capacity, Quantum Lovász number, Non-commutative graph

Introduction A fundamental problem of information theory is to determine the capability of a communication channel for delivering messages from the sender to the receiver. Shannon first investigated this problem in the zero-error setting and described the zero-error capacity of a channel as the maximum rate at which it can be used to transmit information with zero probability of confusion [1]. Recently the zero-error information theory has been studied in the quantum setting and many new phenomena were observed. One of the most remarkable results is that entanglement can be used to improve the zero-error capacity of a classical channel [2, 3]. Furthermore, there are more kinds of capacities when considering auxiliary resources, such as shared entanglement [2, 3, 4, 5] and no-signalling correlations [2, 6].

For the zero-error communication via quantum channels, the non-commutative graph associated with a quantum channel captures the zero-error communication properties of this channel [5], thus the non-commutative graph plays a similar role to confusability graph of a classical channel. It is well-known that the zero-error capacity is extremely difficult to compute for both classical and quantum channels. In Ref. [7], it was proved that computing the one-shot zero-error capacity of a quantum channel is QMA-complete and the calculation of the asymptotic zero-error capacity is even not known to be computable. Nevertheless, the zero-error capacities of classical channels and quantum channels are upper bounded by the the famous Lovász number of a confusability graph [8] and the quantum Lovász number [5] of a non-commutative graph, respectively. Furthermore, the entanglement-assisted zero-error capacity C_{0E} of a classical channel is also upper-bounded by the Lovász number [5, 9], and this notable result can be generalized to quantum channels by using the quantum Lovász number [5].

One of the most important and intriguing open problems in zero-error information theory is whether there is a gap between the entanglement-assisted zero-error capacity and the quantum Lovász number of a classical or quantum channel, which is frequently mentioned in Refs. [3, 5, 9, 10, 11, 12]. If they are equal, it would imply that C_{0E} is additive while the unassisted case is not [13].

In this paper, we show the answer to the open problem above is negative for quantum channels. We construct a class of qutrit-to-qutrit channels whose quantum Lovász number is strictly larger than its entanglement-assisted zero-error capacity. In particular, this class of channels is reversible under quantum no-signalling correlations (QNSC).

Main results The entanglement-assisted zero-error capacity C_{0E} of a channel is the optimal rate at which it is possible to transmit information perfectly while the sender and receiver share free entanglement. Since C_{0E} is not known to be computable, it is difficult to compare C_{0E} to the quantum Lovász

*xin.wang-8@student.uts.edu.au

†runyao.duan@uts.edu.au

number. The problem whether there exists a gap between them remained open for almost six years. Our approach to answer this problem is based on the class of channels $\mathcal{N}_\alpha(\rho) = C_\alpha \rho C_\alpha^\dagger + D_\alpha \rho D_\alpha^\dagger$ $(0 < \alpha \le \pi/4)$ with

$$C_\alpha = \sin\alpha|0\rangle\langle 1| + |1\rangle\langle 2|, D_\alpha = \cos\alpha|2\rangle\langle 1| + |1\rangle\langle 0|.$$

We first consider the QNSC assisted zero-error capacity [6], which is potentially larger than the entanglement-assisted case. We also use the QNSC assisted zero-error classical simulation cost $S_{0,NS}$ [6] during the proof, which is the minimum noiseless bits required to simulate a channel under QNSC. It holds that $C_{0E} \le C_{0,NS} \le S_{0,NS}$.

Proposition 1 *For* $\mathcal{N}_\alpha$ $(0 < \alpha \le \pi/4)$,

$$C_{0,NS}(\mathcal{N}_\alpha) = S_{0,NS}(\mathcal{N}_\alpha) = 2.$$

We then show the exact value of the quantum Lovász number of $\mathcal{N}_\alpha$.

Proposition 2 *For* $\mathcal{N}_\alpha$ $(0 < \alpha \le \pi/4)$,

$$\widetilde{\vartheta}(\mathcal{N}_\alpha) = 2 + \cos^2\alpha + \cos^{-2}\alpha > 4. \quad (1)$$

Combining Propositions 1 and 2, we can conclude that there is a separation between quantum Lovász number and entanglement-assisted zero-error classical capacity. This is based on the fact that C_{0E} is upper bounded by the QNSC assisted zero-error capacity $C_{0,NS}$. Our main result is presented as follows.

Theorem 3 *For the class of quantum channels* $\mathcal{N}_\alpha$ $(0 < \alpha \le \pi/4)$,

$$\log_2 \widetilde{\vartheta}(\mathcal{N}_\alpha) > C_{0,NS}(\mathcal{N}_\alpha) \ge C_{0E}(\mathcal{N}_\alpha). \quad (2)$$

Conclusions and discussions In summary, we construct a class of quantum channels whose quantum Lovász number is strictly larger than its entanglement-assisted zero-error capacity. This resolves a well-known open problem in zero-error quantum information. There are still several unsolved problems left. For instance, it is of great interest to study the case of classical channel. For the confusability graph G, a variant of Lovász number called Schrijver number [14, 15] was proved to be an tighter upper bound for the entanglement-assisted independence number than Lovász number [16] . However, it remains unknown whether Schrijver number will converge to Lovász number in the asymptotic setting. A gap between the regularized Schrijver number and Lovász number would imply a separation between $C_{0E}(G)$ and $\vartheta(G)$.

We would like to thank Andreas Winter for helpful suggestions. This work was partly supported by the Australian Research Council (Grant No. DP120103776 and No. FT120100449).

References

[1] C. E. Shannon, *IRE Trans. Inf. Theory* **2**, 8 (1956).

[2] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, *Phys. Rev. Lett.* **104**, 230503 (2010).

[3] D. Leung, L. Mancinska, W. Matthews, M. Ozols, and A. Roy, *Commun. Math. Phys.* **311**, 97 (2012).

[4] R. Duan and Y. Shi, *Phys. Rev. Lett.* **101**, 20501 (2008).

[5] R. Duan, S. Severini, and A. Winter, *IEEE Trans. Inf. Theory* **59**, 1164 (2013).

[6] R. Duan and A. Winter, *IEEE Trans. Inf. Theory* **62**, 891 (2016).

[7] S. Beigi and P. W. Shor, *arXiv:0709.2090.*

[8] L. Lovász, *IEEE Trans. Inf. Theory* **25**, 1 (1979).

[9] S. Beigi, *Phys. Rev. A*, vol. 82, no. 1, p. 10303, (2010).

[10] T. Cubitt, L. Mancinska, D. E. Roberson, S. Severini, D. Stahlke, and A. Winter, *IEEE Trans. Inf. Theory* **60**, 7330 (2014).

[11] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, *IEEE Trans. Inf. Theory* **57**, 5509 (2011).

[12] L. Mancinska, G. Scarpa, and S. Severini, *IEEE Trans. Inf. Theory* **59**, 4025 (2013).

[13] N. Alon, *Combinatorica* **18**, 301 (1998).

[14] A. Schrijver, *IEEE Trans. Inf. Theory*, **25**, 4, 1979.

[15] R. J. McEliece, E. R. Rodemich, and H. C. Rumsey Jr, *J. Comb. Inform. Syst. Sci*, **3**, 3, 1978.

[16] T. Cubitt, L. Mancinska, D. E. Roberson, S. Severini, D. Stahlke, and A. Winter, *IEEE Trans. Inf. Theory*, **60**, 11, 2014.

Maximum privacy without coherence, zero-error

Debbie Leung[1] *   Nengkun Yu[2 1 3] †

[1] *Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada*

[2] *Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*

[3] *Department of Mathematics & Statistics, University of Guelph, Guelph, Ontario, Canada*

Abstract. We study the possible difference between the quantum and the private capacities of a quantum channel in the zero-error setting. For a family of channels introduced by [LLSS14], we demonstrate an extreme difference: the zero-error quantum capacity is zero, whereas the zero-error private capacity is maximum given the quantum output dimension.

Keywords: Private Capacity, Zero-error, Quantum Capacity, Coherence

The quantum capacity $Q(\mathcal{N})$, measured in qubits per channel use, establishes the maximum rate for transmitting quantum information and how well we can perform quantum error correction. The private capacity $\mathcal{P}(\mathcal{N})$, in bits per channel use, gives the maximum rate of *private* classical communication. Errors that become negligible as the number of channel uses increases are allowed in the above definitions.

Understanding the relation between the quantum and the private capacities is an essential task in quantum Shannon theory. In [HHHO05], some channels $\mathcal{N}$ are found for which $Q(\mathcal{N}) = 0$ but $P(\mathcal{N}) > 0$, breaking a long-held intuition that coherence is necessary for privacy. In [LLSS14], a class of channels with $Q(\mathcal{N}) \le 1$ and $P(\mathcal{N}) = \log d$ is presented, where d^2 is the input dimension and log is taken base 2. As d increases, these channels saturate an upper bound for $P(\mathcal{N}) - Q(\mathcal{N})$ thus approximately realizing the largest possible separation between the two capacities.

Quite recently, the notion of zero-error capacity has been introduced for quantum channels [MA05]. We denote the zero-error quantum and private capacities for a quantum channel $\mathcal{N}$ as $Q_0(\mathcal{N})$ and $P_0(\mathcal{N})$ respectively. Zero-error private classical communication requires perfect data transmission such that no one but the receiver gains any information on the data. Clearly $Q_0(\mathcal{N}) \le Q(\mathcal{N}) \le \mathcal{P}(\mathcal{N})$ and $Q_0(\mathcal{N}) \le P_0(\mathcal{N}) \le \mathcal{P}(\mathcal{N})$.

In this paper, we study the zero-error quantum capacity of the channels introduced in [LLSS14], and demonstrate an exact extreme separation. For these channels, $P_0(\mathcal{N}) = \log d$ and $Q_0(\mathcal{N}) = 0$. In other words, each of these channels has no capacity to transmit quantum information perfectly, even it has full ability to distribute private information perfectly.

The notion of zero-error quantum capacity can be introduced as follows. Let $\alpha^q(\mathcal{N})$ be the maximum integer k such that there is a k-dimensional subspace $\mathcal{H}'_A$ of $\mathcal{H}_A$ that can be perfectly transmitted through $\mathcal{N}$. That is, there is a recovery quantum channel $\mathcal{R}$ from $\mathcal{D}(\mathcal{H}_B)$ to $\mathcal{D}(\mathcal{H}_{A'})$ so that $(\mathcal{R}\circ\mathcal{N})(\psi) = \psi$ for any $|\psi\rangle \in \mathcal{H}_{A'}$ (recall $\psi = |\psi\rangle\langle\psi|$). Then, $\log_2 \alpha^q(\mathcal{N})$ represents the maximum number of qubits one can send perfectly by one use of $\mathcal{N}$. The *zero-error quantum capacity* of $\mathcal{N}$, $Q_0(\mathcal{N})$, is defined as:

$$Q_0(\mathcal{N}) = \sup_{n\ge 1} \frac{\log_2 \alpha^q(\mathcal{N}^{\otimes n})}{n}. \tag{1}$$

we can invoke the following lemma from [CS12].

Lemma 1 *Let $\mathcal{N} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ be a quantum channel. One can transmit quantum information without error through a single use of $\mathcal{N}$ if and only if there are orthogonal states $|\alpha\rangle$ and $|\beta\rangle$ such that*

$$\operatorname{tr}\left[\mathcal{N}(|\alpha\rangle\langle\alpha|)\,\mathcal{N}(|\beta\rangle\langle\beta|)\right] = 0 \tag{2}$$

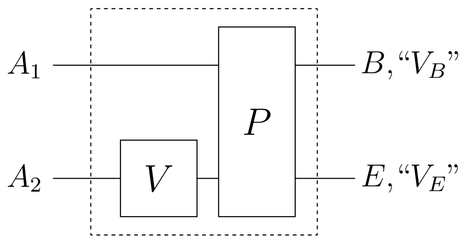
and

$$\operatorname{tr}\left[\mathcal{N}(|\alpha+\beta\rangle\langle\alpha+\beta|)\,\mathcal{N}(|\alpha-\beta\rangle\langle\alpha-\beta|)\right] = 0. \tag{3}$$

where $|\alpha \pm \beta\rangle = 1/\sqrt{2}(|\alpha\rangle \pm |\beta\rangle)$.

Private communication via a memoryless classical channel and quantum key distribution are well established subjects. Private classical communication of a quantum channel has more recently been formally introduced in [Dev05]. The private capacity of $\mathcal{N}$ measures the maximum rate of reliable classical data transmission via $\mathcal{N}$ while keeping the output of the complementary channel independent of the data.

The family of channels $\mathcal{N}_d$ introduced in [LLSS14] can be schematically summarized as follows:



(4)

For each integer $d \ge 2$, we define the channel $\mathcal{N}_d$ which has two input registers A_1 and A_2, each of dimension d. A unitary operation V is applied to A_2, followed by a controlled phase gate $P = \sum_{i,j} \omega^{ij} |i\rangle\langle i| \otimes |j\rangle\langle j|$ acting on A_1A_2, where ω is a primitive d^{th} root of unity. Bob

*wcleung@uwaterloo.ca

†nengkunyu@gmail.com

receives only A_1 (now relabeled as B) and "V_B", which denotes a classical register with a description of V. The A_2 register is discarded. The complementary channel has outputs A_2 (relabeled as E) and "V_E" which also contains a description of V. The isometric extension is given by

$$U_d \left|\psi\right\rangle_{A_1A_2} = \sum_V \sqrt{\mathrm{pr}(V)}\ \left(P\left(I \otimes V\right)\left|\psi\right\rangle_{A_1A_2}\right) \otimes \left|V\right\rangle_{V_B} \otimes \left|V\right\rangle_{V_E}.$$

Here, V is drawn from any exact unitary 2-design $\mathcal{G} = \{g_1, g_2, \cdots, g_m\}$.

It was shown in [LLSS14] that $P(\mathcal{N}_d) = \log d$. The method given by [LLSS14] to transmit private classical data has no error and has perfect secrecy so $P_0(\mathcal{N}_d) = \log d$. To be self-contained, we provide a quick argument here. Suppose the input into A_2 is half of a maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle_{A_2}|i\rangle_{A_3}$ where A_3 stays in Alice's possession. By the transpose trick, the unitary operations V and P can be replaced by unitary operations acting on A_1 and A_3 without changing the final state on B, E, A_3, V_B, V_E. So, the output of the complementary channel (E, V_E) is independent of the input. Moreover, $\mathcal{N}_d(|i\rangle\langle i| \otimes I/d) = |i\rangle\langle i|$. So $\log d$ bits can be transmitted perfectly and secretly.

Furthermore, [LLSS14] also shows that $Q(\mathcal{N}_d) \leq 1$. Intuitively, superposition of states in system A_1 will be heavily decohered by the P gate, because error correction is ineffective due to the random unitary V. However, [LLSS14] finds that $Q(\mathcal{N}_d) \geq 0.61$ for large d.

This motivates the current study, to demonstrate an extreme separation of P_0 and Q_0 using the channels $\mathcal{N}_d$. Our main result is that, no finite number of uses of $\mathcal{N}_d$ can be used to transmit one qubit with zero error. This implies in particular $Q_0(\mathcal{N}_d) = 0$, while $P_0(\mathcal{N}_d) = \log d$, attaining the extremes allowed by the quantum output dimension.

Our main technical result is a characterization of pairs of input states whose orthogonality is preserved by n uses of the channel.

Theorem 2 Let n be any positive integer, $|\psi_1\rangle = \sum_{i_1,\cdots,i_n} |i_1,\cdots,i_n\rangle\,|\alpha_{i_1,\cdots,i_n}\rangle$, and $|\psi_2\rangle = \sum_{i_1,\cdots,i_n} |i_1,\cdots,i_n\rangle\,|\beta_{i_1,\cdots,i_n}\rangle$ be two arbitrary pure state inputs for $\mathcal{N}_d^{\otimes n}$. Then, $\mathrm{tr}[\mathcal{N}_d^{\otimes n}(\psi_1)\mathcal{N}_d^{\otimes n}(\psi_2)] = 0$ if and only if at most one of $|\alpha_{i_1,\cdots,i_n}\rangle$ and $|\beta_{i_1,\cdots,i_n}\rangle$ is nonzero for each tuple $(i_1, \cdots, i_n)$.

In other words, states suitable for transmitting classical information through $\mathcal{N}_d^{\otimes n}$ without any error have no "overlap" in the computational basis of $A_1^{\otimes n}$.

As a consequence, we have

Theorem 3 For any positive integer n, $\mathcal{N}_d^{\otimes n}$ cannot transmit a qubit with zero error. In particular, this implies $Q_0(\mathcal{N}_d) = 0$.

To prove Theorem 2, the following two lemmas are needed,

Lemma 4 Let $|\psi_1\rangle = \sum_i |i\rangle\,|\alpha_i\rangle$ and $|\psi_2\rangle = \sum_i |i\rangle\,|\beta_i\rangle$ be two possible pure input states for $\mathcal{N}_d$. Then, $\mathrm{tr}[\mathcal{N}_d(\psi_1)\mathcal{N}_d(\psi_2)] = 0$ if and only if at most one of $|\alpha_i\rangle$ and $|\beta_i\rangle$ is nonzero for each i.

Lemma 5 [YDY14] For all positive integer n, there is no non-zero bipartite matrix M satisfying $M \geq 0$, $M^\Gamma \geq 0$, and $\mathrm{tr}(M(I-\Phi)^{\otimes n}) = 0$, where M^Γ denotes the partial transpose of bipartite matrix M.

In this paper, we show an extreme separation between zero-error quantum capacity and the private capacity by demonstrating for a class of channels that the private capacity is maximum given the output dimension, while there is no ability to transmit even one-qubit with any finite number of channel uses, when no error can be tolerated. We hope techniques from our work can be used to study the zero-error capacity of other channels.

References

[LLSS14] D. Leung, K. Li, G. Smith, and J. A. Smolin. Maximal Privacy without Coherence. *Physical Review Letters*, 113:030512, 2014.

[HHHO05] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94, 160502 (2005).

[MA05] R. A. C. Medeiros, F. M. de Assis. Zero-error capacity of a quantum channel. IJQI, 3(1):135-139, 2005.

[CS12] T. S. Cubitt and G. Smith. An Extreme Form of Superactivation for Quantum Zero-Error Capacities. *IEEE Transactions on Information Theory*, 58(3):1953–1961, 2012.

[Dev05] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. IEEE Trans. Inf. Theory 51, 44 (2005) (quant-ph/0304127v6).

[YDY14] N. Yu, R. Duan and M. Ying. Distinguishability of Quantum States by Positive Operator-Valued Measures with Positive Partial Transpose. *IEEE Transactions on Information Theory*, 60(4):2069-2079, 2014.

Unconstrained distillation capacities of a pure-loss bosonic broadcast channel

Masahiro Takeoka[1] Kaushik P. Seshadreesan[2] Mark M. Wilde[3]

[1] *National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan*
[2] *Max-Planck-Institut für die Physik des Lichts, 91058 Erlangen, Germany*
[3] *Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

Abstract. Bosonic channels are important in practice as they form a simple model for free-space or fiber-optic communication. We consider a single-sender multi-receiver pure-loss bosonic broadcast channel and establish the unconstrained capacity region for the distillation of bipartite entanglement and secret key between the sender and each receiver, where they are allowed arbitrary public classical communication.

Quantum key distribution (QKD) and entanglement distillation (ED) are two cornerstones of quantum communication technology. QKD enables two or more parties to share unconditionally secure random bit sequences whereas ED allows them to distill pure maximal entanglement from a quantum state shared via a noisy communication channel. In both protocols, the parties are allowed to perform (in principle) an unlimited amount of local operations and classical communication (LOCC).

One of the problem in optical quantum communication is the channel loss. For example, all known QKD protocols exhibit an exponential rate-loss tradeoff, in which the secret key rate drops exponentially with increasing fiber distance [1].

Some time after these limitations were observed, Refs. [2] provided a mathematical proof, using the notion of squashed entanglement [3], that the trade-off is indeed a fundamental limitation even with unconstrained input energy. One of the main results of [2] is an upper bound on the LOCC assisted quantum and secret key agreement capacity of a pure-loss bosonic channel, which is solely a function of the channel transmittance η (for finite energy, tighter bounds are also available [2]). Ref. [4] extended the squashed entanglement technique to obtain upper bounds for a variety of phase-insensitive Gaussian channels. Concurrently with [4], Ref. [5] improved the infinite-energy bound from [2] and conclusively established the unconstrained capacity of the pure-loss bosonic channel as $\mathcal{C}(\eta) = -\log_2(1-\eta)$.

Extension of the above point-to-point scenario to the network quantum communication scenarios such as broadcast and multiple access channels is an important direction. Even though various network quantum communication scenarios have been examined, there has been limited work on the LOCC-assisted quantum and private capacities. Only recently in [6] were nontrivial outer bounds on the achievable rates established for the LOCC-assisted capacities in a general m-receiver quantum broadcast channel (QBC) (for any $m \geq 1$) based on multipartite generalizations of the squashed entanglement [7] and the methods of [2].

In this paper, we consider a single-sender multiple-receiver pure-loss bosonic QBC and establish the unconstrained LOCC-assisted capacity region for the distillation of bipartite entanglement and secret key between the sender and each receiver. Consider a pure loss bosonic QBC $\mathcal{L}_{A'\to BC}$ where the channel splits the input state into three systems, one to each of Bob, Charlie, and the environment with transmittance η_B, η_C, and $1-\eta_B-\eta_C$, respectively, where $\eta_B, \eta_C \in [0,1], \eta_B+\eta_C \leq 1$. Physically it is modeled by a pair of beam splitters, in both the signal is mixed with a vacuum, where the first one induces pure loss and the second one splits the signal to Bob and Charlie. Alice wants to share the entanglement or secret keys with Bob and Charlie through n channel uses and unlimited amount of LOCC. Let us denote entanglement rates between Alice and Bob (Charlie) as E_{AB} (E_{AC}), and the secret key rate as K_{AB} (K_{AC}), respectively. Our main theorem is stated as follows:

Theorem 1 *The LOCC-assisted, unconstrained capacity region of the pure-loss bosonic QBC $\mathcal{L}_{A'\to BC}$ is given by*

$$E_{AB} + K_{AB} \leq \log_2([1-\eta_C]/[1-\eta_B-\eta_C]), \quad (1)$$

$$E_{AC} + K_{AC} \leq \log_2([1-\eta_B]/[1-\eta_B-\eta_C]), \quad (2)$$

$$E_{AB}+K_{AB}+E_{AC}+K_{AC} \leq -\log_2(1-\eta_B-\eta_C). \quad (3)$$

A complete proof is given in [8]. To prove the statement, we establish inner bounds on the achievable rate region by employing the quantum state merging protocol [9]. The converse part relies upon several tools. First, we utilize a teleportation simulation argument originally introduced in [10, Section V]. and recently extended in [5]. Next, it is known that the relative entropy of entanglement is an upper bound on the distillable key of a bipartite state [11]. Then the recent work in [5] stated how these two ideas are combined to upper bound the LOCC-assisted quantum and private capacities for certain class of point-to-point channels.

Also critical for the proof of the converse part is the fact that the physical implementation of $\mathcal{L}_{A'\to BC}$ is not unique. For example, we could have a first beam splitter split system B from C and E, and then a second one split C and E. It is also possible to split C at the first beam splitter. This observation implies a drastic simplification of the calculation of the relative entropy of entanglement. The obtained outer bounds match the inner bounds in the infinite-energy limit, thereby establishing the unconstrained capacity region. An example fothe rate region is shown in Fig. 1.

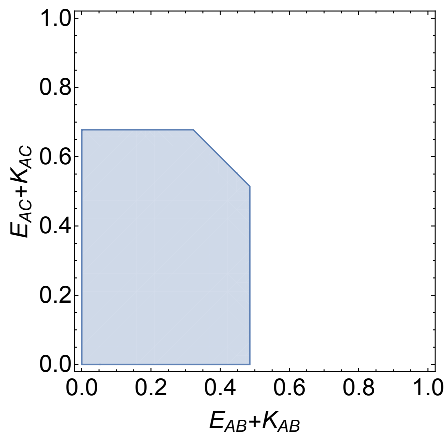


Figure 1: LOCC-assisted capacity region given by (1)–(3), where $(\eta_B, \eta_C) = (0.2, 0.3)$.

The above theorem can be generalized for single-sender multiple-receiver pure-loss broadcast channel $\mathcal{L}_{A'\to B_1\cdots B_m}$ with $m > 2$ which is characterized by a set of transmittances $\{\eta_{B_1}, \cdots, \eta_{B_m}\}$ with $\sum_{i=1}^m \eta_{B_i} \leq 1$ [12]. Let $\mathcal{B} = \{B_1, \cdots, B_m\}$, $\mathcal{T} \subseteq \mathcal{B}$, and $\overline{\mathcal{T}}$ be a complement of set $\mathcal{T}$. We have the following theorem:

Theorem 2 *The LOCC-assisted unconstrained capacity region of the pure-loss bosonic QBC* $\mathcal{L}_{A'\to B_1\cdots B_m}$ *is given by*

$$\sum_{B_i\in\mathcal{T}} E_{AB_i} + K_{AB_i} \leq \log_2\left(\frac{1-\eta_{\overline{\mathcal{T}}}}{1-\eta_{\mathcal{B}}}\right), \quad (4)$$

for all non-empty $\mathcal{T}$, *where* $\eta_{\mathcal{B}} = \sum_{i=1}^m \eta_{B_i}$ *and* $\eta_{\overline{\mathcal{T}}} = \sum_{B_i\in\overline{\mathcal{T}}} \eta_{B_i}$.

A complete proof is given in [8].

Our result could provide a useful benchmark for implementing a broadcasting of entanglement and secret key through linear optics networks which is usually used in real world quantum communications. Important open questions include the distillations of E_{BC} and K_{BC}, or even GHZ states through QBC, and determining the capacity region in both this setting and even the single-sender single-receiver case when there is an energy constraint on the transmitter which is practically more relevant.

References

[1] V. Scarani et al., *Rev. Mod. Phys.*, 81, 1301 (2009).

[2] M. Takeoka, S. Guha, and M. M. Wilde, *Nat. Commun.*, 5:5235 (2014), *ibid*, *IEEE Trans. Inf. Theory*, 60, 4987 (2014).

[3] M. Christandl and A. Winter, *J. Math. Phys.*, 45, 829 (2004).

[4] K. Goodenough, D. Elkouss, and S. Wehner, *New J. Phys.*, 18, 063005 (2016).

[5] S. Pirandola et al., arXiv:1510.08863.

[6] K. P. Seshadreesan et al., *IEEE Trans. Inf. Theory*, 62, 2849 (2016).

[7] D. Yang et al., *IEEE Trans. Inf. Theory*, 55, 3375 (2009).

[8] M. Takeoka, K. P. Seshadreesan, and M. M. Wilde, arXiv:1601.05563v2.

[9] M. Horodecki, J. Oppenheim, and A. Winter, *Nature*, 436, 673 (2005).

[10] C. H. Bennett et al., *Phys. Rev. A*, 54, 3824 (1996).

[11] K. Horodecki et al., *Phys. Rev. Lett.*, 94, 160502 (2005).

[12] S. Guha, Ph.D. dissertation, MIT, 2008.

Quantifying Asymmetric Einstein-Podolsky-Rosen Steering

Kai Sun[1 2 *] Xiang-Jun Ye[1 2 †] Jin-Shi Xu[1 2 ‡] Chuan-Feng Li[1 2 §]

[1] *Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei, Anhui 230026, P. R. China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, P. R. China*

Abstract. Einstein-Podolsky-Rosen (EPR) steering exhibits a unique asymmetric property, i.e., the steerability can differ between observers. This property is inherently different from the symmetric concepts of entanglement and Bell nonlocality, and it has attracted increasing interest. We propose a practical method to quantify the steerability. And we experimentally use it to quantify asymmetric EPR steering in the frame of projective measurements. Furthermore, we then clearly demonstrate one-way EPR steering. Our work provides a new insight into the fundamental asymmetry of quantum nonlocality and has potential applications in asymmetric quantum information processing.

Keywords: asymmetry, steering, quantification, one-way

Asymmetric EPR steering is an important open question proposed when EPR steering is reformulated in 2007 [1]. Supposing Alice and Bob share a pair of two-qubit state, it is easy to image that if Alice entangles with Bob, then Bob must also entangle with Alice. Such a symmetric feature holds for both entanglement and Bell nonlocality [2]. However, the situation is dramatically changed when one turns to a novel kind of quantum nonlocality, the EPR steering, which stands between entanglement and Bell nonlocality. It may happen that for some asymmetric bipartite quantum states, Alice can steer Bob but Bob cannot steer Alice. This distinguished feature would be useful for the one-way quantum tasks. The first experimental verification of one-way EPR steering was performed by using two entangled continuous variable systems in 2012 [3]. However, the experiments demonstrating one-way EPR steering [3, 4] are restricted to Gaussian measurements, and for more general measurements, like projective measurements, there is no experiment realizing the asymmetric feature of EPR steering even the theoretical analysis has been proposed [5].

Recently, we for the first time quantify the steerability and demonstrate one-way EPR steering in the simplest entangled system (two qubits) using two-setting projective measurements [6]. The asymmetric two-qubit states in the form of

$$\rho_{AB} = \eta|\Psi(\theta)\rangle\langle\Psi(\theta)| + (1-\eta)|\Phi(\theta)\rangle\langle\Phi(\theta)|, \quad (1)$$

where $0 \leq \eta \leq 1$, $|\Psi(\theta)\rangle = \cos\theta|0_A 0_B\rangle + \sin\theta|1_A 1_B\rangle$, $|\Phi(\theta)\rangle = \cos\theta|1_A 0_B\rangle + \sin\theta|0_A 1_B\rangle$, are prepared based on the setup shown in Figure 1. For all non-trivial ρ_{AB}, Alice can steer Bob's state. When $|\cos 2\theta| < |2\eta - 1|$, Bob can also steer Alice's state. If $|\cos 2\theta| \geq |2\eta - 1|$, there always exists a local hidden state model for Alice to reproduce her conditional states when Bob chooses any two directions to measure, which means Bob can *not* steer Alice's state.

Based on the steering robustness [7], we introduce an intuitive criterion R called as steering radius, which is defined as

$$R(\rho_{AB}) = \max_{\{\vec{n}_1,\vec{n}_2\}} \{r(\rho_{AB})_{\{\vec{n}_1,\vec{n}_2\}}\}, \quad (2)$$

to quantify the steerability. Here, $r(\rho_{AB})_{\{\vec{n}_1,\vec{n}_2\}}$ is explained below. In the case of two measurement settings $\{\vec{n}_1, \vec{n}_2\}$, there are at most four local hidden states, ρ_i ($i = a, b, c, d$), reproducing Bob's conditional states if Alice can *not* steer Bob's system. We can expand the hidden

*skaikai@mail.ustc.edu.cn
†xiangjun@ustc.edu.cn
‡jsxu@ustc.edu.cn
§cfli@ustc.edu.cn

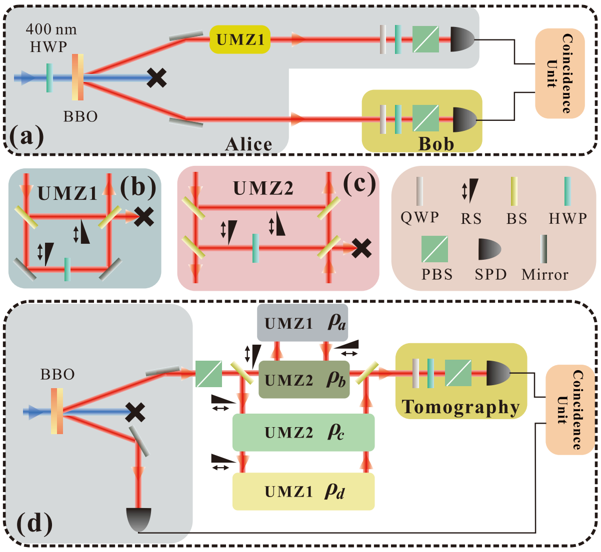


Figure 1: Experimental setup. **(a)**. The entangled photon pairs are prepared through the spontaneous parametric down conversion (SPDC) process by pumping the BBO crystal with ultraviolet pulses. The state's parameters η and θ can be detuned conveniently by employing the setup shown in **(a)** and the unbalanced Mach-Zehnder interferometer (UMZ) with beam splitters (BSs) and removable shutters (RSs) shown in **(b)**. A unit consisting of a quarter-wave plate (QWP) and a half-wave plate (HWP) on Alice's side is used to set the measurement direction. The same unit with an extra polarization beam splitter (PBS) on Bob's side is used to perform state tomography. Photons are collected into a single mode fiber equipped with a 3 nm interference filter and are then detected by a single-photon detector (SPD) on each side. **(d)**. The strategy is for local hidden states to reproduce the conditional states. One of the two photons is used as the trigger for the coincidence unit, and the other is used to prepare the four local hidden states, which can be conveniently prepared by employing the setup of **(b)** and **(c)**. The probabilities are controlled by adjusting the RSs.

states to the super quantum hidden state model (SQHSM), which means there are no physical restrictions on the states ρ_i and ρ_i, which can be located outside of the Bloch sphere. In such a case, there is generally more than one set of SQHSM. Thus, $r(\rho_{AB})_{\{\vec{n}_1,\vec{n}_2\}}$ can be defined as the radius of the SQHSM which is written as

$$\min_{SQHSM}\{\max\{L[\rho_a], L[\rho_b], L[\rho_c], L[\rho_d]\}\}, \quad (3)$$

where $L[\rho_i]$ $(i = a, b, c, d)$ denotes the length of Bloch vectors of the states ρ_i. If $r(\rho_{AB})_{\{\vec{n}_1,\vec{n}_2\}} > 1$, at least one of the hidden states is located beyond the Bloch sphere; thus, the model is not physical. The different values of R on two sides clearly illustrate the asymmetric feature of EPR steering. Furthermore, the one-way steering is demonstrated when $R > 1$ on one side and $R < 1$ on the other side (see Figure 2 (b)).

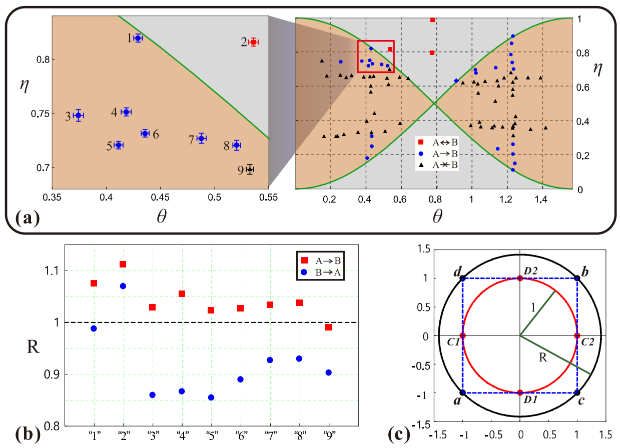


Figure 2: Experimental results for asymmetric EPR steering. **(a)** The distribution of the experimental states. The right column shows the entangled states we prepared, and the left column is a magnification of the corresponding region in the right column. The two green curves represent the cases of $|\cos 2\theta| = |2\eta - 1|$. The blue points and red squares represent the states realizing one-way and two-way EPR steering, respectively. The black triangles represent the states for which EPR steering task fails for both observers. **(b)** The values of R for the states labeled in the left column in **(a)**. The red squares represent the situation where Alice steers Bob's system, and the blue points represent the case where Bob steers Alice's system. **(c)** Geometric illustration of the strategy for local hidden states (black points) to construct the four normalized conditional states (red points) obtained from the maximally entangled state.

For the failing EPR steering process, the local hidden state model, which provides a direct and convinced contradiction between the nonlocal EPR steering and classical physics, is prepared experimentally to reconstruct the conditional states obtained in the steering process (see Figure 3).

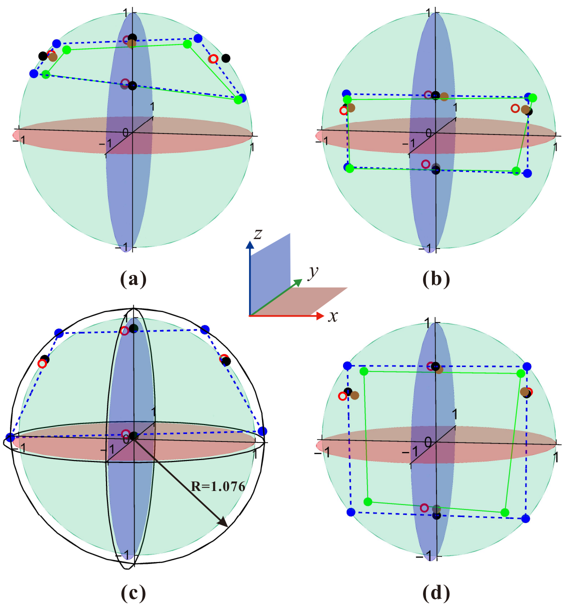


Figure 3: The experimental results of the normalized conditional states and local hidden states shown in the Bloch sphere. The theoretical and experimental results of the normalized conditional states are marked by the black and red points (hollow), respectively. The blue and green points represent the results of the four local hidden states in theory and experiment, respectively. The normalized conditional states constructed by the local hidden states are shown by the brown points. **(a)** and **(c)** Show the case in which Alice steers Bob's system, whereas **(b)** and **(d)** show the case in which Bob steers Alice's system. The parameters of the shared state in **(a)** and **(b)** are $\theta = 0.442$ and $\eta = 0.658$; the parameters of the shared state in **(c)** and **(d)** are $\theta = 0.429$ and $\eta = 0.819$. **(a)**, **(b)** and **(d)** Show that the local hidden state models exist, and the steering tasks fail. **(c)** Shows that no local hidden state model exists for the steering process with the constructed hidden states located beyond the Bloch sphere and $R = 1.076$.

The quantification of EPR steering provides an intuitional and fundamental way to understand the EPR steering. The demonstrated asymmetric EPR steering, especially one-way steering, helps us to investigate the asymmetric feature of quantum nonlocality. This is significant within quantum foundations and quantum information, and shows the potential applications in the tasks of one-way quantum key distribution [8] and the quantum subchannel discrimination [7], even within the frame of two-setting measurements.

References

[1] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.*, 98, 140402, 2007.

[2] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics (Long Island City, N. Y.)*, 1, 195, 1964.

[3] Vitus Händchen *et al.*. Observation of one-way Einstein-Podolsky-Rosen steering. *Nature Photonics*, 6, 596, 2012.

[4] Seiji Armstrong *et al.*. Multipartite Einstein-Podolsky-Rosen steering and genuine tripartite entanglement with optical networks. *Nature Physics*, 11, 167, 2015.

[5] Joseph Bowles, Tamás Vértesi, Marco Túlio Quintino, and Nicolas Brunner. One-way Einstein-Podolsky-Rosen steering. *Phys. Rev. Lett.*, 112, 200402, 2014.

[6] Kai Sun *et al.*. Experimental quantification of asymmetric Einstein-Podolsky-Rosen steering. *Phys. Rev. Lett.*, 116, 160404, 2016.

[7] Marco Piani and John Watrous. Necessary and sufficient quantum information characterization of Einstein-Podolsky-Rosen steering. *Phys. Rev. Lett.*, 114, 060404, 2015.

[8] Cyril Branciard *et al.*. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85, 010301, 2012.

A Quantum Paradox of Choice: More Freedom Makes Summoning a Quantum State Harder

Emily Adlam[1] *　　Adrian Kent[1 2] †

[1] *Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.*

[2] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*

Abstract. The properties of quantum information in space-time can be investigated by studying operational tasks. In one such task, summoning, an unknown quantum state is supplied at one point, and a call is made at another for it to be returned at a third. Hayden-May recently proved necessary and sufficient conditions for guaranteeing successful return of a summoned state for finite sets of call and return points when there is a guarantee of at most one summons. We prove necessary and sufficient conditions when there may be several possible summonses and complying with any one constitutes success. We show there is a "quantum paradox of choice" in summoning: the extra freedom in completing the task makes it strictly harder. This intriguing result has practical applications for distributed quantum computing and cryptography and also implications for our understanding of relativistic quantum information and its localization in space-time.

Keywords: Relativistic quantum cryptography, distributed quantum computing, summoning

It is well known that the exploitation of quantum effects gives rise to exciting new possibilities for computation, information processing and cryptography[3, 16, 13, 15, 5], but more recently, it has been realized that placing quantum information under relativistic constraints leads to the emergence of further unique effects[11, 9, 7] and since this area has not yet been well explored, it is likely that many useful relativistic quantum phenomena remain to be discovered.

In this project, we have been studying constraints on quantum information processing that arise in the relativistic context, and have uncovered a new and surprising effect: under appropriate circumstances, transmitting a quantum message may be possible if there is only one option for the place of delivery, but impossible if multiple options are offered, so having more freedom can sometimes make a relativistic quantum task more difficult. This apparent paradox has important consequences for our understanding of how quantum states may be propagated in distributed quantum computers, global financial networks and other contexts where relativistic signalling constraints are important.

The starting point for our project is a task known as summoning, in which an agent is given an unknown quantum state and required to produce it at a point in space-time in response to a call made at some earlier point[11]. The combination of the relativistic no-signalling principle[14] and the quantum no-cloning theorem[4, 17] together impose strict constraints on the possible geometric configurations of call and return points. Our work involves a generalization of this task in which calls may be made at any number of call points and the agent is required to return the state at any one of the return points corresponding to one of the calls: we have proved a theorem establishing necessary and sufficient conditions on the possible geometric configurations of call and return points in space-time for which there exists a protocol that guarantees a successful response to this task, and showed that these are strictly stronger conditions than those established by Hayden-May[7] for the original summoning task. Thus, strangely, giving an agent more possible ways to respond to this task actually makes it harder for him to respond successfully.

The resolution of the apparent paradox rests on a previously unappreciated feature of summoning tasks. Prima facie it seems that the guarantee of at most one call plays no special role in a summoning task other than to ensure that Alice is never required to produce two copies of an unknown state, in violation of the no-cloning theorem. It thus initially seems paradoxical that summoning becomes strictly harder if we allow the possibility of more than one call, even though only one valid response is required. However, if Alice knows that no more than one call will occur, learning that a call has been made at one point tells her that there are no calls at any other point, and this allows her to coordinate the behaviour of her agents via the global call distribution. A single call gives Alice less information if multiple calls can occur: she learns nothing about the distribution of calls at other points. She thus cannot use the call distribution to coordinate her agents actions in the same way. In other words, the guarantee of at most one call provides a resource that gives Alice the ability to complete tasks that would be impossible without it.

The effect we describe has important practical applications, because the no-summoning theorem has already been used for the development of new protocols in relativistic quantum cryptography[8, 10, 12, 1, 2], and our stronger results suggest further ways of exploiting summoning as a general way of controlling the flow of quantum information. For example, our result is a useful way of characterizing possible distributed parallel quantum computations in which the output of a sub-protocol is routed to one of several parallel computations which call

*ea385@cam.ac.uk

†apak@cam.ac.uk

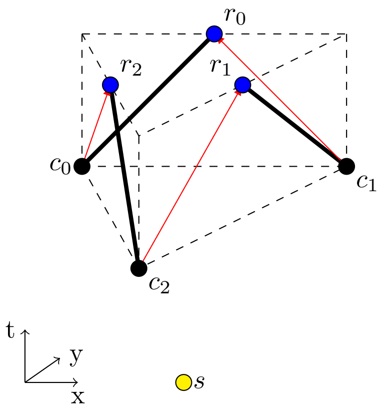


Figure 1: A 2 + 1 dimensional example of a spacetime configuration of call and repsonse points where summoning is possible if it is guaranteed that there will be only one call, but not if more than one call may arrive.

for the output when they reach a certain state[6]. We thus expect this result to find application in future cryptographic protocols as well as in quantum network algorithms.

Our result also has interesting theoretical implications: there is a long-standing tradition of using apparent paradoxes to refine our understanding of quantum theory[3, 16, 13, 15, 5], but this new effect is perhaps the first intrinsically relativistic quantum paradox, in the sense that the effect can be exhibited only in the framework of relativistic quantum theory. Our project thus offers a useful starting point for probing intuitions about the nature of quantum states as spatiotemporal entities - an area which has received comparatively little attention in recent debates over the reality of the quantum state.

References

[1] E. Adlam and A. Kent. Deterministic relativistic quantum bit commitment. *International Journal of Quantum Information*, 13:1550029, June 2015.

[2] E. Adlam and A. Kent. Device-independent relativistic quantum bit commitment. *Physical Review A*, 92(2):022315, August 2015.

[3] M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acín, N. Gisin, and S. Pironio. Guess Your Neighbor's Input: A Multipartite Nonlocal Game with No Quantum Advantage. *Physical Review Letters*, 104(23):230404, June 2010.

[4] D. Dieks. Communication by EPR Devices. *Phys. Lett.*, A92:271–272, 1982.

[5] P. Gawron, J. A. Miszczak, and J. Sladkowski. Noise Effects in Quantum Magic Squares Game. *ArXiv e-prints*, January 2008.

[6] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390–393, November 1999.

[7] P. Hayden and A. May. Summoning Information in Spacetime, or Where and When Can a Qubit Be? *Journal of Physics A*, March 2016.

[8] A. Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

[9] A Kent. Quantum Tasks in Minkowski Space. *Class. Quantum Grav.*, 29, 2012.

[10] A. Kent. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Physical Review Letters*, 109(13):130501, September 2012.

[11] A. Kent. A no-summoning theorem in relativistic quantum theory. *Quantum Information Processing*, 12(2):1023–1032, 2013.

[12] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental Bit Commitment Based on Quantum Communication and Special Relativity. *Phys. Rev. Lett.*, 111:180504, Nov 2013.

[13] L. Mančinska, D. E. Roberson, and A. Varvitsiotis. Deciding the existence of perfect entangled strategies for nonlocal games. *ArXiv e-prints*, June 2015.

[14] L. Sartori. *Understanding Relativity: A Simplified Approach to Einstein's Theories.* University of California Press, 1996.

[15] Marco Tomamichel, Serge Fehr, Jdrzej Kaniewski, and Stephanie Wehner. One-sided device-independent qkd and position-based cryptography from monogamy games. In Thomas Johansson and PhongQ. Nguyen, editors, *Advances in Cryptology EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 609–625. Springer Berlin Heidelberg, 2013.

[16] Thomas Vidick. The complexity of entangled games. *Phd thesis, University of California, Berkeley*, 2011.

[17] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, October 1982.

Dimension Witnesses Beyond Non-Classicality Tests

Edgar A. Aguilar[1] * Máté Farkas[1] † Marcin Pawłowski[1] ‡

[1] *Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland, National Quantum Information Centre in Gdańsk, 81-824 Sopot, Poland*

Abstract. Current experimental tests of non-classicality are binary in their conclusions, regardless of the dimension. Either a physical information carrier is considered to be classical in nature, or else it is said to be quantum. Nevertheless, this does not imply straight away that the experimental setup can produce any desired quantum state of the desired dimension. In this work, we provide a refined dimension witness based on Quantum Random Access Codes, which is able to distinguish between fully classical states, classical-quantum states, separable quantum states, and arbitrary high-dimensional quantum states. These results will be useful to the community, in order to correctly characterize the power of existing experimental setups, to know which quantum information and computation protocols are within our grasp.

Keywords: Dimension Witness, QRACs, Classical-Quantum States

The dimension, or degrees of freedom, of physical information carriers is crucial. In order for quantum computers to show a true practical advantage over their classical counterparts, they must operate on systems of large dimension. That is why we are increasingly striving to coherently control systems of large dimensions [1, 2, 3, 4]. Another promising area is that of quantum information processing, where the dimension of the system is also regarded as a resource. Not only do higher dimensional systems offer more computational and communication power, but they are also useful in e.g. Bell experiments [5, 6] Hence, the quantum information community has come up with the brilliant idea of a dimension witness, originally based on the violation of some particular Bell inequalities [7], and then extended to the prepare and measure scenario [8].

Dimension witnesses can be understood in slightly different ways, depending on the underlying assumptions, but in general refer to some linear function on measurement outcome probabilities. For example, in [7] the systems are assumed to be quantum in nature, and the dimension witness is a Bell inequality which cannot be violated without using quantum systems of at least a specific size. The other example to compare is [8], where they use ideas from state discrimination theory to make a dimension witness that can distinguish between a classical and a quantum system.

While dimension witnesses have been of great help for experimentalists, there is a subtle issue that has been missing in the analysis thus far, which we illustrate with an example. Imagine an experimentalist has complete control over photonic qubit systems but can only create these systems independently (e.g. one at a time), and she does this 20 times. Surely, if done correctly, it's possible to find a dimension witness that makes 20 qubits in a product state perform better than 20 classical bits and then make a claim like "*I work with Hilbert Spaces of Dimension 1 Million*". While, this is strictly not a lie, it is very misleading! Hence, we look for a dimension witness that can signal whether the experimentalist has full (coherent) control of the Hilbert space, in the previous example this would imply arbitrary entanglement between said photons.

This work provides a simple tool for experimental teams to determine up to which dimension they have full control of their Hilbert space (i.e. they can create all states of said dimension). This is very important for the community, as a benchmark tool to check our progress on building quantum computers, and also for experimentalists to know which protocols they can feasibly execute. We focus on the prepare and measure scenario, which is the most general case. Since the point is to show that there is complete coherent control of a particular dimension, it doesn't matter if the physical information carriers are divided as entangled particles, or just one system in an arbitrary state. In particular, we focus on Random Access Codes (RACs), where we call the preparation part of the experiment Alice, and the measurement part Bob.

A $n^d \to 1$ *Random Access Code* (RAC) is a strategy in which Alice tries to compress a n-dit string into 1 dit, such that Bob can recover any of the n dits with high probability [10]. Specifically, Alice receives an input string $X = x_0x_1 \cdots x_{n-1}$ where $x_i \in [d]$, and we write $[d] \equiv \{0, 1, 2, \ldots, d-1\}$. She is allowed to send one dit $a = E_c(X)$ to Bob. On the other side, Bob receives an input $y \in [n]$, and together with Alice's message a, outputs $b = D_c(a, y)$ as a guess for x_y. If Bob's guess is correct (i.e. $b = x_y$) then we say that they *win*, otherwise we say that they *lose*. Since both encoding and decoding functions are in general probabilistic, we in fact quantify the probability of success $p(b = x_y)$. As a figure of merit for the encoding-decoding strategy, we use the average success probability $P = \frac{1}{nd^n} \sum_X \sum_y p(b = x_y)$.

Similarly, we may define $n^d \to 1$ Quantum Random Access Codes (QRACs) with the only change being that Alice tries to compress her input string into a d-dimensional quantum system. The decoding function is nothing more than a quantum measurement, i.e. he outputs his guess b with probability $\mathrm{tr}[\rho_a M_b^y]$. It can be shown that the maximum average success probability can be achieved with pure states ($\rho_a = |a\rangle\langle a|$) [10].

*ed.alex.aguilar@gmail.com
†mate.frks@gmail.com
‡dokmpa@univ.gda.pl

Similarly, it is possible to argue that this maximum is achieved when the operators M_b^y are projective measurements, which is what we shall henceforth be assuming.

Assume the dimension factorizes as $d = ab$ (with $a \geq b$), then in general we are interested in the following 5 cases: $C_{ab}, C_aQ_b, C_bQ_a, Q_aQ_b, Q_{ab}$. In the same order, these are to be understood as: a classical system of dimension ab, a classical system of dimension a and a quantum system of dimension b, a classical system of dimension b and a quantum system of dimension a, a quantum system of dimension a in a separable state with a quantum system of dimension b, and a quantum system of dimension ab. This is trivially generalized. The **Main Result** of our work deals with constructing explicit dimension witnesses which are able to differentiate the above cases. The explicit construction is technical, but an example of how our tools can be used is provided, as well as the main ideas regarding the proof.

Example. For a classical $2^d \to 1$ RAC the average success probability is $P_{C_d} = \frac{1}{2} + \frac{1}{d}$, while for the quantum case the $2^d \to 1$ QRAC has an average success probability of $P_{Q_d} = \frac{1}{2} + \frac{1}{2\sqrt{d}}$. We look at dimension 4, with $P_{C_4} = 0.625$ and $P_{Q_4} = 0.75$, and with our main result we are able to calculate $P_{C_2Q_2} = 0.6546$ and $P_{Q_2Q_2} \approx 0.7286$. This means that, it is not enough for the experimentalist to obtain an average success probability greater than P_{C4}, to claim that she has complete control over 4-dimensional Hilbert space. Surely, this would imply immediately that her states are not entirely classical, but the big prize in this example would be to obtain an experimental result above the $P_{Q_2Q_2}$ value.

Now we briefly present the key ideas of our proof. First, we prove that an identity decoding function (where Bob's outcome measurements are directly used in the output without further post-processing) cannot be worse than the optimal decoding function. Second, adaptive measurements cannot outperform non-adaptive ones. By this we mean, Bob's measurement strategy only depends on his input y, and in the optimal case does not depend on the measurement results of the first systems. These two points, make it so that essentially Alice and Bob are playing two parallel QRACs at the same time. Finally, for a given $2^d \to 1$ QRAC, we derive "maximal quantum curves" which relate the probability of guessing dit 1, as a function of the probability of guessing dit 2 when using the optimal quantum mechanical strategy - which involves using Mutually Unbiased Bases [11].

Up to this point, we need to assume that the system is a specific dimension d, and then we are able to provide the tools necessary for distinguishing the nature of said system. This is problematic, because sometimes experimentalists don't even know what is the effective dimension of their system. Hence, we propose a very simple $1^{d_0} \to 1$ QRAC (which is just state discrimination in disguise), where d_0 is a guess of the dimension size. If the average success probability is less than 1, then we express it as $\frac{d}{d_0}$, and d is the effective system size the experimentalist should be working with. Specifically, the experimentalist would know that his system is at least dimension d, and if if it were this dimension, then she could say how classical or quantum it is.

Finally, we conclude by saying that our main result can be used to prove that for some cases $P_{Q_a} > P_{Q_bQ_c}$ even if $a < bc$. This just shows that indeed having access to the full Hilbert space is a great resource, and it is this what we should be checking when developing new quantum technologies.

References

[1] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, "Generation and confirmation of a (100 100)-dimensional entangled quantum system," vol. 111, no. 17, pp. 6243–6247, 2014.

[2] M. Malik, M. Mirhosseini, M. Lavery, J. Leach, M. Padgett, and R. Boyd, "Direct measurement of a 27-dimensional orbital-angular-momentum state vector," vol. 5, p. 3115, 2014.

[3] M. McLaren, F. S. Roux, and A. Forbes, "Realising high-dimensional quantum entanglement with orbital angular momentum," *ArXiv e-prints*, May 2013.

[4] V. D'Ambrosio, F. Bisesto, F. Sciarrino, J. F. Barra, G. Lima, and A. Cabello, "Device-independent certification of high-dimensional quantum systems," *Phys. Rev. Lett.*, vol. 112, p. 140503, Apr 2014.

[5] S. Massar, "Nonlocality, closing the detection loophole, and communication complexity," *Phys. Rev. A*, vol. 65, p. 032121, Mar 2002.

[6] T. Vértesi, S. Pironio, and N. Brunner, "Closing the detection loophole in bell experiments using qudits," *Phys. Rev. Lett.*, vol. 104, p. 060401, Feb 2010.

[7] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani, "Testing the dimension of hilbert spaces," *Phys. Rev. Lett.*, vol. 100, p. 210503, May 2008.

[8] N. Brunner, M. Navascués, and T. Vértesi, "Dimension witnesses and quantum state discrimination," *Phys. Rev. Lett.*, vol. 110, p. 150501, Apr 2013.

[9] S. Wehner, M. Christandl, and A. C. Doherty, "Lower bound on the dimension of a quantum system given measured data," *Phys. Rev. A*, vol. 78, p. 062112, Dec 2008.

[10] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum Random Access Codes with Shared Randomness," *ArXiv e-prints*, Oct. 2008.

[11] E. Aguilar, J. Borkała, P. Mironowicz, and M. Pawłowski, "Using Quantum Random Access Codes to Understand Mutually Unbiased Bases," *in preparation.*