Operational meaning of quantum measures of recovery

Tom Cooney, Christoph Hirche, Ciara Morgan, Jonathan P. Olson, Kaushik P. Seshadreesan, John Watrous, and Mark M. Wilde

Phys. Rev. A **94**, 022310 — Published 10 August 2016

DOI: 10.1103/PhysRevA.94.022310

Operational meaning of quantum measures of recovery

Tom Cooney,[1] Christoph Hirche,[2] Ciara Morgan,[3] Jonathan P. Olson,[4]
Kaushik P. Seshadreesan,[5] John Watrous,[6, 7] and Mark M. Wilde[4, 8]

[1] *Department of Mathematics, State University of New York at Geneseo, Geneseo, New York 14454, USA*
[2] *Física Teòrica: Informació i Fenòmens Quàntics, Departament de Física, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain*
[3] *School of Mathematics and Statistics, University College Dublin, Belfield, Dublin 4, Ireland*
[4] *Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Louisiana State University, Baton Rouge, Louisiana 70803, USA*
[5] *Max Planck Institute for the Science of Light, Guenther-Scharowsky-Str. 1/ building 24, 91058 Erlangen, Germany*
[6] *Institute for Quantum Computing and School of Computer Science, University of Waterloo, Canada*
[7] *Canadian Institute for Advanced Research, Toronto, Canada*
[8] *Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

Several information measures have recently been defined which capture the notion of "recoverability." In particular, the fidelity of recovery quantifies how well one can recover a system A of a tripartite quantum state, defined on systems ABC, by acting on system C alone. The relative entropy of recovery is an associated measure in which the fidelity is replaced by relative entropy. In this paper, we provide concrete operational interpretations of the aforementioned recovery measures in terms of a computational decision problem and a hypothesis testing scenario. Specifically, we show that the fidelity of recovery is equal to the maximum probability with which a computationally unbounded quantum prover can convince a computationally bounded quantum verifier that a given quantum state is recoverable. The quantum interactive proof system giving this operational meaning requires four messages exchanged between the prover and verifier, but by forcing the prover to perform his actions in superposition, we construct a different proof system that requires only two messages. The result is that the associated decision problem is in QIP(2) and another argument establishes it as hard for QSZK (both classes contain problems believed to be difficult to solve for a quantum computer). We finally prove that the regularized relative entropy of recovery is equal to the optimal Type II error exponent when trying to distinguish many copies of a tripartite state from a recovered version of this state, such that the Type I error is constrained to be no larger than a constant.

I. INTRODUCTION

There are many facets of quantum science in which the notion of quantum state recovery is deeply embedded. This is particularly true for quantum error correction [1, 2] and quantum key distribution [3], where the primary goal is fundamentally that of recovery. In the former, the task is to reconstruct a quantum state where some part of the state has undergone noise or loss; in the latter, the task is to keep a message secure against an eavesdropper attempting a similar reconstruction. In either case, the success or failure of a protocol often hinges on whether a particular state in question is recoverable at all, or if the state is beyond repair.

A particularly important class of states are those that constitute a Markov chain. A classical Markov chain can be understood as a memoryless random process, i.e., a process in which the state transition probability depends only on the current state, and not on past states. If random variables X, Y, and Z form a classical Markov chain as $X \to Y \to Z$, then the classical conditional mutual information $I(X;Z|Y) = 0$, where

$$I(X;Z|Y) \equiv H(XY) + H(ZY) - H(Y) - H(XYZ) \quad (1)$$

and $H(X)$ is equal to the Shannon entropy of X. Classical Markov chains model an impressive number of natural processes in physics and many other sciences [4].

An attempt at understanding a quantum generalization of these ideas was put forward in [5], but it was later realized that these notions made sense only in the exact case [6]. That is, in analogy with the classical case mentioned above, the authors of [5] defined a quantum Markov chain to be a tripartite state ρ_{ABC} for which the conditional quantum mutual information (CQMI) $I(A;B|C)_\rho$ is equal to zero, where

$$I(A;B|C)_\rho \equiv H(AC)_\rho + H(BC)_\rho - H(C)_\rho - H(ABC)_\rho \quad (2)$$

and $H(AC)_\rho$ is equal to the von Neumann entropy of the reduced state ρ_{AC} (and likewise for $H(BC)_\rho$, $H(C)_\rho$, and $H(ABC)_\rho$). However, the later work in [6] (see also [7]) demonstrated that large perturbations of a quantum Markov state as defined in [5] can sometimes lead only to small increases of the CQMI, calling into question the definition of quantum Markov chains from [5].

Meanwhile, it has been known for some time that an equivalent description for the exact case $I(A;B|C)_\rho = 0$ exists in terms of recoverability. The work of Petz [8, 9] implies that there exists a recovery channel $\mathcal{R}_{C\to AC}$ such that $\rho_{ABC} = \mathcal{R}_{C\to AC}(\rho_{BC})$ if and only if $I(A;B|C)_\rho = 0$. This is in perfect analogy with the exact classical case mentioned above: for a state satisfying $I(A;B|C)_\rho = 0$, one could lose the A system and recover it back from

C alone. In this sense, all correlations between systems A and B are mediated through system C for quantum Markov chain states. Recoverability in this sense is thus intimately connected to Markovianity and represents a method for handling the approximate case, different from that given in [5].

To measure non-Markovianity in the approximate case, the general approach outlined in [10] was to quantify the "distance" from ρ_{ABC} to its closest recovered version. The main measure on which [10] focused was the *fidelity of recovery*, defined as

$$F(A;B|C)_\rho \equiv \sup_{\mathcal{R}_{C\to AC}} F(\rho_{ABC}, \mathcal{R}_{C\to AC}(\rho_{BC})), \quad (3)$$

where the quantum fidelity is defined as

$$F(\omega,\tau) \equiv \|\sqrt{\omega}\sqrt{\tau}\|_1^2 \quad (4)$$

for density operators ω and τ [11]. The optimization in (3) is with respect to quantum channels $\mathcal{R}_{C\to AC}$ acting on the C system and producing an output on the A and C systems. A related measure, defined in [10, Remark 6], is the *relative entropy of recovery*:

$$D(A;B|C)_\rho \equiv \inf_{\mathcal{R}_{C\to AC}} D(\rho_{ABC}\|\mathcal{R}_{C\to AC}(\rho_{BC})). \quad (5)$$

The quantum relative entropy is defined as

$$D(\omega\|\tau) \equiv \mathrm{Tr}\{\omega[\log\omega - \log\tau]\} \quad (6)$$

if $\mathrm{supp}(\omega) \subseteq \mathrm{supp}(\tau)$ and it is equal to $+\infty$ otherwise [12]. These are clearly well motivated measures of recovery / non-Markovianity, but hitherto they have been lacking concrete operational interpretations. This is the main question that we address in this paper.

From the main result of [13], which established that

$$I(A;B|C)_\rho \geq -\log F(A;B|C)_\rho, \quad (7)$$

it is now understood that the CQMI itself is a measure of non-Markovianity as well. Before [13], an operational interpretation for the CQMI had already been given in [14, 15] as twice the optimal rate of quantum communication needed for a sender to transfer one share of a tripartite state to a receiver (generally shared entanglement is required for this task). Here, the decoder at the receiving end in this protocol plays the role of a recovery channel, an interpretation later used in [16]. A wave of recent work [17–31] on this topic has added to and complements [13], solidifying what appears to be the right notion of quantum Markovianity.

It follows from the concerns in recovery applications that one may have to systematically decide whether or not a given tripartite quantum state is recoverable. In this paper, we discuss two concrete scenarios in which this is the case. The first scenario is an experiment involving a single copy of the state ρ_{ABC} and the second involves many copies of such a state—for both settings, the goal is to decide whether a given tripartite state is recoverable.

In more detail, the first scenario asks: given a description of a quantum circuit that prepares a state ρ_{ABC}, what is the maximum probability with which someone could be convinced that the state is recoverable? Also, how difficult is the task of deciding if the state meets some criteria of recoverability when A is lost? We address these questions by defining the associated decision problem, called FoR for "fidelity of recovery." Using ideas from quantum complexity theory [32, 33], we show that the fidelity of recovery is equal to the maximum probability with which a verifier can be convinced that ρ_{ABC} is recoverable from ρ_{BC} by acting on system C alone. The quantum interactive proof system establishing this operational meaning for the fidelity of recovery is depicted in Figure 1 and follows intuitively from the duality property of fidelity of recovery, originally established in [10]. It also proves that FoR is contained in the complexity class QIP [32, 33].

However, the proof system in Figure 1 requires the exchange of four messages between the verifier and the prover, and from a computational complexity theoretic perspective, it is desirable to reduce the number of messages exchanged. In fact, this is certainly possible because a general procedure is known which reduces any quantum interactive proof system to an equivalent one which has only three messages exchanged [34]. In Section III, we contribute a different proof system for FoR which requires the exchange of only two messages between the verifier and the prover. The main idea is that the verifier can force the prover to perform his actions in superposition, and the result is that the FoR decision problem is in QIP(2). We also argue that FoR is hard for QSZK [35, 36], by building on earlier work in [37]. Note that both QSZK and QIP(2) contain problems believed to be difficult to solve by a quantum computer.

The second scenario in which we give an operational meaning for a recovery measure is an experiment involving many copies of the state ρ_{ABC}. Let n be a large positive integer. Suppose that either the state $\rho_{ABC}^{\otimes n}$ is prepared or the state $\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})$ is, where $\mathcal{R}_{C^n\to A^nC^n}$ is some arbitrary collective recovery channel acting on all n of the C systems. The goal is then to determine which is the case by performing a collective measurement on all of the systems $A^nB^nC^n$. There are two ways that one could make a mistake in this hypothesis testing setup. The first is known as the Type I error, and it is equal to the probability of concluding that $\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})$ was prepared if in fact $\rho_{ABC}^{\otimes n}$ was prepared. The other kind of error is the Type II error. Defining the regularized relative entropy of recovery as follows [16]:

$$D^\infty(A;B|C)_\rho \equiv \lim_{n\to\infty} \frac{1}{n} D(A^n;B^n|C^n)_{\rho^{\otimes n}}, \quad (8)$$

we prove that $D^\infty(A;B|C)_\rho$ is equal to the optimal exponent for the Type II error if the Type I error is constrained to be no larger than a constant $\varepsilon \in (0,1)$. That is, there exists a measurement such that the Type II error goes as $\approx 2^{-nD^\infty(A;B|C)_\rho}$ with the Type I error no larger than ε. However, if one tries to make the Type II error decay faster than $\approx 2^{-nD^{\infty}(A;B|C)_\rho}$, then it is impossible to meet the Type I constraint for any $\varepsilon \in (0,1)$. Thus, our result establishes a concrete operational interpretation of the regularized relative entropy of recovery in this hypothesis testing experiment. It was previously shown in [16] that

$$I(A;B|C)_\rho \geq D^{\infty}(A;B|C)_\rho \geq -\log F(A;B|C)_\rho, \quad (9)$$

but no operational interpretation of $D^{\infty}(A;B|C)_\rho$ was given there. In the rest of the paper, we provide more details of these operational interpretations in order to justify them.

II. OPERATIONAL MEANING OF FIDELITY OF RECOVERY

We now provide an operational interpretation for the fidelity of recovery, by considering the following computational task:

Problem 1 (FoR) *Given is a description of a quantum circuit that prepares a tripartite state ρ_{ABC}, along with real numbers $\alpha, \beta \in (0,1)$ satisfying $\alpha - \beta \geq [\text{poly}(n)]^{-1}$, for n denoting the circuit size. Promised that either*

$$\begin{aligned} YES: & \ F(A;B|C)_\rho \geq \alpha \qquad \text{or,} \\ NO: & \ F(A;B|C)_\rho \leq \beta, \end{aligned}$$

decide which of the above is the case.

Remark 2 *The additional assumption that $\alpha - \beta \geq [\text{poly}(n)]^{-1}$ is a common assumption which allows for amplifying the probability of deciding correctly, by employing error reduction procedures [34, 38]. This kind of assumption is required for most applications in quantum complexity theory [33, 39].*

The computational problem FoR is defined with the following in mind: a party constructs a state ρ_{ABC} by acting with the gates specified in a given circuit, and wants to know whether it is possible, if system A is lost, to recover the state when given access to system C only. A YES-instance of this problem then corresponds to a recoverable state, since by the definition of fidelity of recovery in (3), there exists a recovery channel $\mathcal{R}_{C\to AC}$ which acts on ρ_{BC} and satisfies the recovery criteria. A NO-instance implies that no such recovery channel exists. We note that this problem is distinct from deciding whether ρ_{ABC} is recoverable starting from the specification of the density matrix, a problem which has been shown to be decidable in classical polynomial time via a semi-definite program [26].

In order to have a robust operational meaning, it is important for this decision problem to have an efficient verification strategy, so that another party is unable to convince the verifier that a state is recoverable, if in fact it is not. The complexity class QIP(k), introduced in [34, 40], captures this concept. A problem is said to be in QIP(k) if, given k distinct quantum messages exchanged between a verifier and a computationally unbounded prover, the verifier will accept YES-instances and reject NO-instances with very high probability. The prover will always try to make the verifier accept, regardless of whether the state in question is a YES- or NO-instance. To prove FoR $\subseteq$ QIP, we will show that $F(A;B|C)_\rho$ is equal to the maximum acceptance probability of the verifier in a particular quantum interactive proof system. If this is true, then we can immediately conclude that the probability of accepting a YES-instance is no smaller than α, and the probability of accepting a NO-instance is no larger than β, satisfying the properties of a QIP system. These probabilities can then be amplified to be exponentially close to the extremes of one and zero, respectively, by employing parallel repetition for QIP [34].

We now give an outline of a quantum interactive proof system with maximum acceptance probability equal to the fidelity of recovery, thus witnessing the containment FoR $\subseteq$ QIP. Recall that, for any pure four-party state ϕ_{ABCD}, the fidelity of recovery obeys the following duality relation [10]:

$$F(A;B|C)_\phi = F(A;B|D)_\phi. \quad (10)$$

The main idea behind this duality is that there is an optimal recovery channel for recovering A from C and an optimal dual "Uhlmann" recovery channel for recovering A from D, and their performance as measured by fidelity is equal, as guaranteed by Uhlmann's theorem [11]. The proof system we construct is related to the methods used in [10] to establish the relation in (10), but here we will have a computationally unbounded prover sequentially implement the recovery channel and the "Uhlmann" dual recovery channel [11]. In the setup of quantum interactive proofs, it is apparently necessary for such a prover to implement these channels given that the dimension of the Hilbert space is essentially exponentially large in n (size of the circuit needed to generate ρ_{ABC}). More explicitly, consider the following interaction between a verifier and a prover, depicted in Figure 1:

1. The verifier uses the description of the quantum circuit to prepare the mixed state ρ_{ABC} (with system D a purifying system). In Figure 1, this is denoted by a unitary U_ρ acting on many qubits prepared in the state $|0\rangle$, which we abbreviate simply as $|0\rangle$. The unitary U_ρ has output systems A, B, C, and D. So then $\rho_{ABC} = \text{Tr}_D\{|\phi\rangle\langle\phi|_{ABCD}\}$ where $|\phi\rangle_{ABCD} \equiv U_\rho|0\rangle$.

2. The verifier sends system C to the prover.

3. The prover acts with a general unitary $U_{CE\to A'C'F}$ on system C and an ancilla system E prepared in a fiducial state $|0\rangle_E$, and the output systems are F, A', and C'.

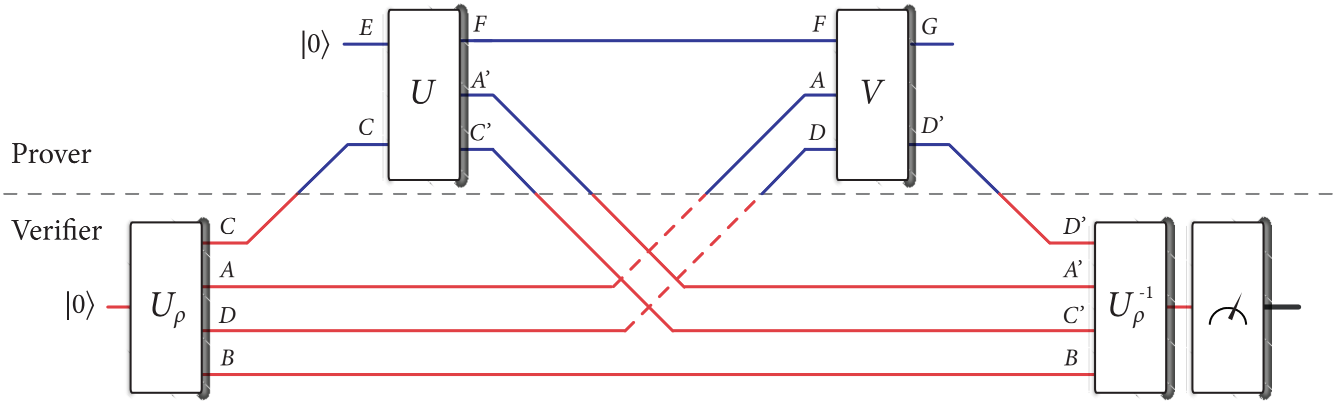

FIG. 1: This figure illustrates the quantum interactive proof system that establishes 1) an operational meaning of the fidelity of recovery and 2) the containment FoR $\subseteq$ QIP. There are four distinct quantum messages exchanged between the verifier and the prover.

4. The prover sends systems A' and C' to the verifier.

5. The verifier sends systems A and D to the prover.

6. The prover acts with a unitary $V_{ADF\to D'G}$ on systems F, A, and D that has output systems D' and G.

7. The prover sends D' back to the verifier.

8. The verifier accepts if and only if the projection of the final state onto the pure state $\phi_{A'BC'D'}$ is successful. This test can be conducted by applying the inverse of the preparation unitary U_ρ, measuring each of the output qubits in the computational basis, and accepting if and only if the measurement outcomes are all zeros.

From this interaction, we can show via a chain of equalities that the maximum acceptance probability of the proof system is equal to the fidelity of recovery of the state ρ_{ABC}. Consider that the maximum acceptance probability is equal to the following Euclidean norm:

$$\max_{U,V} \| \langle\phi|_{A'BC'D} V_{ADF\to D'G} U_{CE\to A'C'F} |\phi\rangle_{ABCD} |0\rangle_E \|_2^2$$

$$= \max_{U,V,|\varphi\rangle_G} |\langle\phi|_{A'BC'D} \langle\varphi|_G V U |\phi\rangle_{ABCD} |0\rangle_E|^2 \qquad (11)$$

$$= \max_{U,V} |\langle\phi|_{A'BC'D} \langle\varphi|_G V U |\phi\rangle_{ABCD} |0\rangle_E|^2 , \qquad (12)$$

where the first equality follows because there exists a unit vector $|\varphi\rangle_G$ which achieves the norm and the second because the optimization over $|\varphi\rangle_G$ can be absorbed into the optimization over the unitary $V_{ADF\to D'G}$. Consider that systems F, A, and D purify the following state

$$\mathrm{Tr}_{FAD}\{U\,(|\phi\rangle\langle\phi|_{ABCD} \otimes |0\rangle\langle 0|_E)\,U^\dagger\}$$
$$= \mathrm{Tr}_F\{U\,(\rho_{BC} \otimes |0\rangle\langle 0|_E)\,U^\dagger\}, \qquad (13)$$

and systems D and G purify the following state:

$$\mathrm{Tr}_{DG}\{|\phi\rangle\langle\phi|_{A'BC'D} \otimes |\varphi\rangle\langle\varphi|_G\} = \rho_{A'BC'}. \qquad (14)$$

Thus, by Uhlmann's theorem [11] with $V_{ADF\to D'G}$ as the Uhlmann unitary, it follows that (12) is equal to

$$\max_U F(\rho_{A'BC'}, \mathrm{Tr}_F\{U\,(\rho_{BC} \otimes |0\rangle\langle 0|_E)\,U^\dagger\})$$
$$= \max_{\mathcal{R}_{C\to A'C'}} F(\rho_{A'BC'}, \mathcal{R}_{C\to A'C'}(\rho_{BC}))$$
$$= F(A;B|C)_\rho, \qquad (15)$$

where the first equality follows by the well known theorem of Stinespring [41], which states that any quantum channel can be realized by adjoining an ancilla system, acting with a unitary, and tracing out a system. This establishes an operational interpretation of fidelity of recovery as the maximum acceptance probability of our quantum interactive proof system for FoR. By the reasoning given above, it follows that FoR $\subseteq$ QIP.

To establish that FoR is hard for QSZK, we need only consider that a special case of FoR occurs when the C system is trivial, in which case the recovery channel reduces to a preparation of a state on system A and we then need to decide whether $\max_{\sigma_A} F(\rho_{AB}, \sigma_A \otimes \rho_B)$ is above or below a given threshold. This problem however has already been shown in [37] to be QSZK-complete, from which we conclude that FoR is hard for QSZK.

III. A TWO-MESSAGE QUANTUM INTERACTIVE PROOF SYSTEM FOR FIDELITY OF RECOVERY

The quantum interactive proof system in Figure 1 gives a direct operational interpretation of the fidelity of recovery in terms of its maximum acceptance probability. However, from the perspective of computational complexity theory, the QIP system has more messages exchanged than are necessary. Indeed, a general result states that any QIP system can be parallelized to an equivalent one that has only three messages exchanged between the verifier and the prover [34].

In this section, we reduce the number of messages exchanged by showing that there exists a two-message quantum interactive proof system for the fidelity of recovery computational problem. By glancing at Figure 1, we see that the previous QIP system has the prover perform two actions: the recovery channel and the dual recovery channel, as discussed after (10). The idea of the two-message QIP system given in Figure 2 is to force the prover to perform both actions in superposition. In terms of the many worlds interpretation of quantum mechanics, we can think that the verifier employs quantum entanglement and the superposition principle to force the prover to perform the recovery channel on system C in one world, while in the other world redirecting the D system to the prover so that he can perform the dual recovery channel on it. The verifier can then check at the end whether the prover took the correct actions in each world by realigning systems in each world, performing a Bell measurement, and demanding that the original entangled state prepared be undisturbed by the prover's actions. The result is that if the fidelity of recovery is high (so that by (10) both $F(A;B|C)$ and $F(A;B|D)$ are near to one), then there is a high probability that the verifier will be convinced that this is the case. If the fidelity of recovery is low, then there is little chance for the prover to convince the verifier.

We now detail the two-message QIP system. Let $|\phi\rangle_{ABCD}$ denote the four-party pure state of interest. The proof system has the following steps:

1. The verifier prepares a Bell state
$$|\Phi^+\rangle_{TT'} \equiv \frac{1}{\sqrt{2}}(|00\rangle_{TT'} + |11\rangle_{TT'}), \tag{16}$$
the four-party pure state $|\phi\rangle_{ABCD}$, and the ancilla states $|0\rangle_{C'}$ and $|0\rangle_{D'}$.

2. The verifier performs a SWAP of D and D' controlled on the value in T being equal to zero and a SWAP of C and C' controlled on the value in T being equal to one.

3. The verifier sends systems T', C', and D' to the prover.

4. The prover performs a quantum channel with systems T', C', and D' as input and systems T'', A'', C'', and D'' as output, sending these back to the verifier. The output systems have the same size as the corresponding input systems and system A'' has the same size as system A. This quantum channel can be realized by adjoining an ancilla $|0\rangle_{E'}$ of sufficiently large size, performing a unitary $P_{T'C'D'E' \to T''C''D''A''F''}$ and a partial trace over system F''.

5. The verifier performs a SWAP of D and D'' controlled on the value in T being equal to zero and a SWAP of C and C'' controlled on the value in T being equal to one. He also performs a SWAP of A and A'' controlled on the value in T being equal to one.

6. The verifier performs an incomplete Bell measurement on systems T and T'', with measurement operators $\{\Phi^+_{TT''}, I_{TT''} - \Phi^+_{TT''}\}$, and accepts if and only if the outcome is $\Phi^+_{TT''}$.

Figure 2 depicts this two-message QIP system.

We now analyze the maximum acceptance probability of this QIP system and show that it can never exceed a quantity related to the fidelity of recovery. The acceptance probability given that the prover applies a particular unitary $P_{T'C'D'E' \to T''C''D''A''F''}$ is as follows:

$$\left\| \langle \Phi^+|_{TT''} F_{T=1,AA''} F_{T=0,DD''} F_{T=1,CC''} P \ F_{T=0,DD'} F_{T=1,CC'} |\Phi^+\rangle_{TT'} |\phi\rangle_{ABCD} |0\rangle_{C'} |0\rangle_{D'} |0\rangle_{E} \right\|_2^2 \tag{17}$$

where we have abbreviated $P \equiv P_{T'C'D'E' \to T''C''D''A''F''}$ and $F_{T=1,CC'}$ denotes a SWAP C and C' controlled on the value in T being equal to one (with a similar convention for the other controlled SWAP gates). We can then simplify the ket in the above expression as

$$\begin{aligned}
&F_{T=1,AA''} F_{T=0,DD''} F_{T=1,CC''} P \ F_{T=0,DD'} F_{T=1,CC'} |\Phi^+\rangle_{TT'} |\phi\rangle_{ABCD} |0\rangle_{C'} |0\rangle_{D'} |0\rangle_{E} \\
&\propto F_{DD''} P_{T'C'D'E' \to T''C''D''A''F''} |0\rangle_T |0\rangle_{T'} F_{DD'} |\phi\rangle_{ABCD} |0\rangle_{C'} |0\rangle_{D'} |0\rangle_{E'} \\
&\qquad + F_{AA''} F_{CC''} P_{T'C'D'E' \to T''C''D''A''F''} |1\rangle_T |1\rangle_{T'} F_{CC'} |\phi\rangle_{ABCD} |0\rangle_{C'} |0\rangle_{D'} |0\rangle_{E'} \qquad (18) \\
&= P_{T'C'D'E' \to T''C''DA''F''} |0\rangle_T |0\rangle_{T'} |\phi\rangle_{ABCD'} |0\rangle_{C'} |0\rangle_{D''} |0\rangle_{E'} \\
&\qquad + P_{T'C'D'E' \to T''CD''AF''} |1\rangle_T |1\rangle_{T'} |\phi\rangle_{A''BC'D} |0\rangle_{C''} |0\rangle_{D'} |0\rangle_{E'}, \qquad (19)
\end{aligned}$$

where $F_{DD''}$ denotes a SWAP of D and D'' (with a similar convention for the other SWAP gates). Then the acceptance probability simplifies as follows:

$$\frac{1}{4} \left\| \begin{array}{r} \langle 0|_{T''} P_{T'C'D'E' \to T''C''DA''F''} |0\rangle_{T'} |\phi\rangle_{ABCD'} |0\rangle_{C'} |0\rangle_{D''} |0\rangle_{E'} \ + \\ \langle 1|_{T''} P_{T'C'D'E' \to T''CD''AF''} |1\rangle_{T'} |\phi\rangle_{A''BC'D} |0\rangle_{C''} |0\rangle_{D'} |0\rangle_{E'} \end{array} \right\|_2^2 . \tag{20}$$

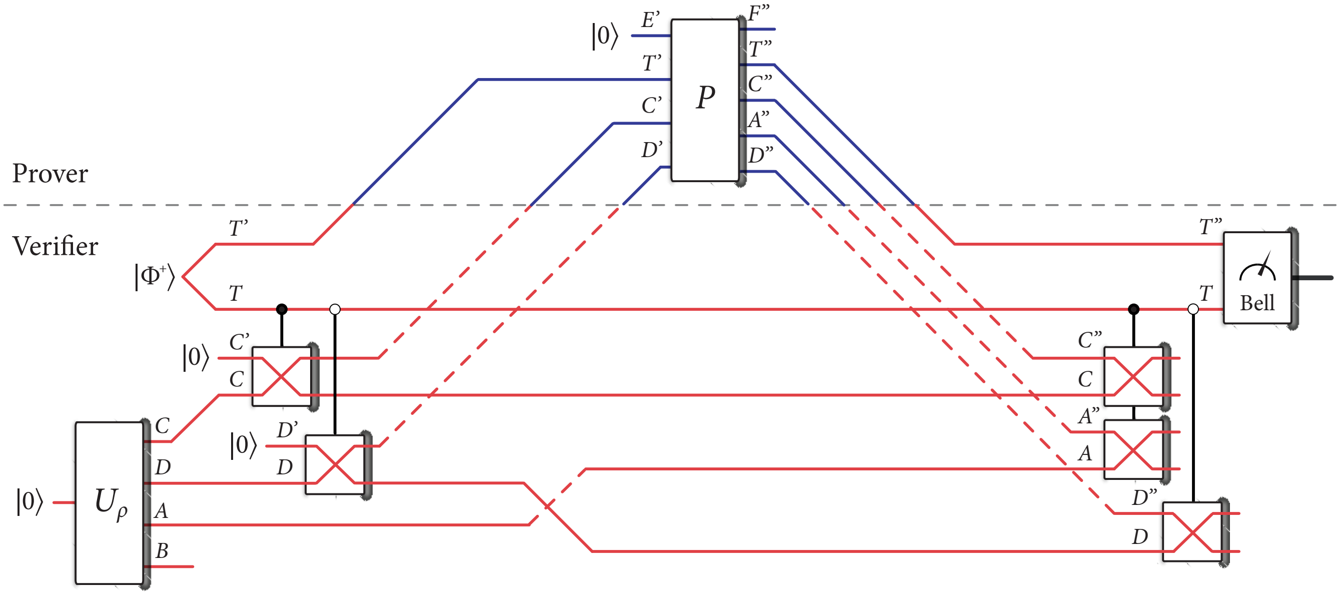

FIG. 2: A two-message quantum interactive proof system for deciding the fidelity of recovery computational problem. The quantum gates with crossed wires denote controlled SWAP gates, as described in the main text. A "filled-in" circle indicates that the SWAP occurs controlled on the value in T being equal to one, while a "hollowed-out" circle indicates that the SWAP occurs controlled on the value in T being equal to zero.

The following two operators are contractions because $P_{T'C'D'E'\to T''C''D''A''F''}$ is a unitary:

$$P^{00}_{C'D'E'\to C''DA''F''} \equiv \langle 0|_{T''} P_{T'C'D'E'\to T''C''DA''F''}|0\rangle_{T'}, \tag{21}$$

$$P^{11}_{C'D'E'\to CD''AF''} \equiv \langle 1|_{T''} P_{T'C'D'E'\to T''CD''AF''}|1\rangle_{T'}. \tag{22}$$

Then (20) is equal to

$$\frac{1}{4}\left\|P^{00}_{C'D'E'\to C''DA''F''}|\phi\rangle_{ABCD'}|0\rangle_{C'}|0\rangle_{D''}|0\rangle_{E'} + P^{11}_{C'D'E'\to CD''AF''}|\phi\rangle_{A''BC'D}|0\rangle_{C''}|0\rangle_{D'}|0\rangle_{E'}\right\|_2^2. \tag{23}$$

Now consider for any two vectors $|\varphi_1\rangle$ and $|\varphi_2\rangle$ that $\left\||\varphi_1\rangle + |\varphi_2\rangle\right\|_2^2 = \langle\varphi_1|\varphi_1\rangle + \langle\varphi_2|\varphi_2\rangle + 2\,\mathrm{Re}\{\langle\varphi_1|\varphi_2\rangle\}$, which implies that (23) is never larger than

$$\begin{aligned}
&\frac{1}{2}\left(1 + \mathrm{Re}\left\{\langle\phi|_{ABCD'}\langle 0|_{C'}\langle 0|_{D''}\langle 0|_{E'}\left(P^{00}_{C'D'E'\to C''DA''F''}\right)^\dagger P^{11}_{C'D'E'\to CD''AF''}|\phi\rangle_{A''BC'D}|0\rangle_{C''}|0\rangle_{D'}|0\rangle_{E'}\right\}\right)\\
&= \frac{1}{2} + \frac{1}{2}\mathrm{Re}\left\{\langle\phi|_{ABCD'}\left[\langle 0|_{C'}\langle 0|_{E'}\left(P^{00}_{C'D'E'\to C''DA''F''}\right)^\dagger|0\rangle_{C''}\right]\left[\langle 0|_{D''}P^{11}_{C'D'E'\to CD''AF''}|0\rangle_{D'}|0\rangle_{E'}\right]|\phi\rangle_{A''BC'D}\right\}\\
&= \frac{1}{2}\left(1 + \mathrm{Re}\left\{\langle\phi|_{ABCD'}\left(V_{D'\to A''DF''}\right)^\dagger U_{C'\to CAF''}|\phi\rangle_{A''BC'D}\right\}\right)\\
&\leq \frac{1}{2}\left(1 + \left|\langle\phi|_{ABCD'}\left(V_{D'\to A''DF''}\right)^\dagger U_{C'\to CAF''}|\phi\rangle_{A''BC'D}\right|\right),
\end{aligned} \tag{24}$$

where in the above we have defined the contractions

$$V_{D'\to A''DF''} \equiv \langle 0|_{C''}P^{00}_{C'D'E'\to C''DA''F''}|0\rangle_{C'}|0\rangle_{E'}, \qquad U_{C'\to CAF''} \equiv \langle 0|_{D''}P^{11}_{C'D'E'\to CD''AF''}|0\rangle_{D'}|0\rangle_{E'}. \tag{25}$$

Consider that

$$\begin{aligned}
&\left|\langle\phi|_{ABCD'}\left(V_{D'\to A''DF''}\right)^\dagger U_{C'\to CAF''}|\phi\rangle_{A''BC'D}\right|\\
&\qquad\leq \max_{V,U}\left\{\left|\langle\phi|_{ABCD'}\left(V_{D'\to A''DF''}\right)^\dagger U_{C'\to CAF''}|\phi\rangle_{A''BC'D}\right| : \|V\|_\infty, \|U\|_\infty \leq 1\right\} = \sqrt{F}(A;B|C)_\phi.
\end{aligned} \tag{26}$$

where the last equality follows from the duality of fidelity of recovery and because any contraction can be written as a convex combination of isometries, so that there is an optimal pair of isometries achieving the maximum in the second line [42, Theorem 5.10]. Thus, the maximum acceptance probability for the QIP system is never higher than

$$\frac{1}{2}\left(1+\sqrt{F}(A;B|C)_\phi\right). \tag{27}$$

This upper bound on the acceptance probability can be achieved if the prover applies a unitary extension of the following isometry:

$$\begin{aligned} &P_{T'C'D'E'\to T''CD''AF''} = \\ &\quad |0\rangle_{T''}\langle 0|_{T'}\otimes V_{D'\to A''DF''}|0\rangle_{C''}\langle 0|_{C'}\langle 0|_{E'} \\ &\quad +|1\rangle_{T''}\langle 1|_{T'}\otimes U_{C'\to CAF''}|0\rangle_{D''}\langle 0|_{D'}\langle 0|_{E'}, \end{aligned} \tag{28}$$

where $V_{D'\to A''DF''}$ and $U_{C'\to CAF''}$ are isometries achieving the maximum in the fidelity of recovery $F(A;B|C)_\phi$.

Thus, in the case of a YES instance, there exists a strategy to convince the verifier to accept with the probability in (27), while in the case of a NO instance, no strategy can convince the verifier to accept with probability higher than that in (27). Given the promise from Problem 1 and known error reduction procedures for QIP(2) [38], these probabilities can then be amplified to be exponentially close to the extremes of one and zero, respectively.

IV. OPERATIONAL MEANING OF REGULARIZED RELATIVE ENTROPY OF RECOVERY

In this section, we provide an operational interpretation of the regularized relative entropy of recovery in the context of quantum hypothesis testing [43, 44]. The setting is as discussed in the introduction: Given are n copies of a state ρ_{ABC}, and the task is to determine whether $\rho_{ABC}^{\otimes n}$ is prepared or whether $\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})$ is prepared, where $\mathcal{R}_{C^n\to A^nC^n}$ is some recovery channel. This is an instance of a more general problem of discriminating between a state $\rho^{\otimes n}$ and a set $\mathcal{S}^{(n)}$ of states, where in our case:

$$\rho^{\otimes n} = \rho_{ABC}^{\otimes n}, \tag{29}$$

$$\mathcal{S}^{(n)} = \left\{\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n}) : \mathcal{R}\in \text{CPTP}\right\}, \tag{30}$$

with CPTP denoting the set of quantum channels from C^n to A^nC^n. This more general setting was studied in detail in [45], where it was found that the Type II rate of convergence simplifies if the following conditions hold:

1. (Convexity) $\mathcal{S}^{(n)}$ is convex and closed for all n.

2. (Full Rank) There exists a full rank state σ such that each $\mathcal{S}^{(n)}$ contains $\sigma^{\otimes n}$.

3. (Reduction) For each $\sigma\in\mathcal{S}^{(n)}$, $\text{Tr}_n\{\sigma\}\in\mathcal{S}^{(n-1)}$.

4. (Concatenation) If $\sigma_n\in\mathcal{S}^{(n)}$ and $\sigma_m\in\mathcal{S}^{(m)}$, then $\sigma_n\otimes\sigma_m\in\mathcal{S}^{(n+m)}$.

5. (Permutation invariance) $\mathcal{S}^{(n)}$ is closed under permutations.

We now verify that the set $\mathcal{S}^{(n)}$ as defined in (30) satisfies the above properties.

Convexity. Let $\mathcal{R}^1_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n}), \mathcal{R}^2_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\in\mathcal{S}^{(n)}$. Then for all $\lambda\in[0,1]$, we have that

$$\lambda\mathcal{R}^1_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n}) + (1-\lambda)\,\mathcal{R}^2_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\in\mathcal{S}^{(n)}$$

because $\lambda\mathcal{R}^1_{C^n\to A^nC^n}+(1-\lambda)\,\mathcal{R}^2_{C^n\to A^nC^n}$ is a quantum channel if $\mathcal{R}^1_{C^n\to A^nC^n}$ and $\mathcal{R}^2_{C^n\to A^nC^n}$ are. Furthermore, the set of all CPTP maps is closed.

Full Rank. Without loss of generality, we can assume that ρ_B is a full rank state. A particular recovery channel is one which traces out system C and replaces with the maximally mixed state on AC. Taking n copies of such a state gives a full-rank state in $\mathcal{S}^{(n)}$.

Reduction. Let $\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\in\mathcal{S}^{(n)}$. Consider that

$$\begin{aligned} &\text{Tr}_{A_nB_nC_n}\{\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\} = \\ &\qquad \text{Tr}_{A_nC_n}\{\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n-1}\otimes\rho_C)\}. \end{aligned} \tag{31}$$

This state is in $\mathcal{S}^{(n)}$ because the recovery channel for $\rho_{BC}^{\otimes n-1}$ could consist of tensoring in ρ_C, applying $\mathcal{R}_{C^n\to A^nC^n}$, and tracing out systems A_nC_n.

Concatenation. Let $\mathcal{R}^1_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\in\mathcal{S}^{(n)}$ and $\mathcal{R}^2_{C^m\to A^mC^m}(\rho_{BC}^{\otimes m})\in\mathcal{S}^{(m)}$. Then

$$\mathcal{R}^1_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\otimes\mathcal{R}^2_{C^m\to A^mC^m}(\rho_{BC}^{\otimes m})\in\mathcal{S}^{(n+m)}, \tag{32}$$

because

$$\begin{aligned} &\mathcal{R}^1_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\otimes\mathcal{R}^2_{C^m\to A^mC^m}(\rho_{BC}^{\otimes m}) = \\ &\qquad \left(\mathcal{R}^1_{C^n\to A^nC^n}\otimes\mathcal{R}^2_{C^m\to A^mC^m}\right)(\rho_{BC}^{\otimes n+m}), \end{aligned} \tag{33}$$

so that the recovery channel consists of the parallel concatenation of $\mathcal{R}^1_{C^n\to A^nC^n}$ and $\mathcal{R}^2_{C^m\to A^mC^m}$.

Permutation invariance. Here, we need to show that for $\sigma\in\mathcal{S}^{(n)}$, we have that $\pi\sigma\pi^\dagger\in\mathcal{S}^{(n)}$ for all permutations π of the n systems. Let $\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\in\mathcal{S}^{(n)}$. Then

$$\begin{aligned} &\pi_{A^nB^nC^n}\mathcal{R}_{C^n\to A^nC^n}(\rho_{BC}^{\otimes n})\,(\pi_{A^nB^nC^n})^\dagger \\ &= (\pi_{A^n}\otimes\pi_{B^n}\otimes\pi_{C^n})\,\mathcal{R}(\rho_{BC}^{\otimes n})\,(\pi_{A^n}\otimes\pi_{B^n}\otimes\pi_{C^n})^\dagger \\ &= (\pi_{A^n}\otimes\pi_{C^n})\,\mathcal{R}(\pi_{B^n}\rho_{BC}^{\otimes n}\pi_{B^n}^\dagger)\,(\pi_{A^n}\otimes\pi_{C^n})^\dagger \\ &= (\pi_{A^n}\otimes\pi_{C^n})\left[\mathcal{R}(\pi_{C^n}^\dagger\rho_{BC}^{\otimes n}\pi_{C^n})\right](\pi_{A^n}\otimes\pi_{C^n})^\dagger \\ &\in\mathcal{S}^{(n)}, \end{aligned} \tag{34}$$

where the second equality follows because the permutation of the B systems commutes with the recovery channel, the third because $\rho_{BC}^{\otimes n}$ is a permutation invariant state, and the last line because a potential recovery consists of applying the permutation $\pi^\dagger_{C^n}$, followed by $\mathcal{R}_{C^n\to A^nC^n}$, followed by the permutation $\pi_{A^n}\otimes\pi_{C^n}$.

From here, we can define a hypothesis testing relative entropy of recovery for a state ρ_{ABC} as follows:

$$D^\varepsilon_H(A;B|C)_\rho \equiv \inf_{\mathcal{R}_{C\to AC}} D^\varepsilon_H(\rho_{ABC}\|\mathcal{R}_{C\to AC}(\rho_{BC})),$$

where D^ε_H is the hypothesis testing relative entropy [46, 47], defined for two states ω and τ as

$$D^\varepsilon_H(\omega\|\tau)\equiv \\ -\log\min_Q\{\mathrm{Tr}\{Q\tau\} : 0\le Q\le I \wedge \mathrm{Tr}\{Q\omega\}\ge 1-\varepsilon\}.$$

By definition, the hypothesis testing relative entropy D^ε_H is equal to the optimal Type II error exponent when the Type I error cannot exceed $\varepsilon\in(0,1)$. By employing the main result of [45] and the above observations, we can conclude that

$$\lim_{n\to\infty}\frac{1}{n}D^\varepsilon_H(A^n;B^n|C^n)_{\rho^{\otimes n}} = D^\infty(A;B|C)_\rho, \qquad (35)$$

for all $\varepsilon\in(0,1)$. (Note that the limit as $\varepsilon\to 0$ is not needed.) This gives an operational interpretation of $D^\infty(A;B|C)_\rho$ as the optimal Type II error exponent as claimed.

V. CONCLUSION

We have given operational meaning to two different recovery measures: the fidelity of recovery and the relative entropy of recovery. The first occurs in a "one-shot" scenario, where we find that the fidelity of recovery is equal to the maximum probability with which a quantum prover can convince a quantum verifier that a given state is recoverable. As an additional contribution, we give a different quantum interactive proof system for the fidelity of recovery problem which has only two messages exchanged between the verifier and the prover. Thus we make progress on a computational problem related to recoverability by showing that the problem FoR is in QIP(2) and is hard for QSZK. The second operational interpretation occurs in a scenario involving many copies of a given tripartite state and represents a generalization of quantum Stein's lemma [43, 44]. We showed that the optimal Type II error exponent is equal to the regularized relative entropy of recovery if there is a constraint on the Type I error.

Going forward from here, it would be interesting to give better bounds on the computational problem FoR. For example, could we show that the general recoverability problem is hard for QIP(2)? For the hypothesis testing setup, can we give finer characterizations of the optimal Type II exponent when the Type I error is not a fixed constant but decays as well (cf., [48])? Perhaps the Rényi relative entropy of recovery studied in [49] would be relevant here? This question was recently addressed and solved in the specialized classical case [50], but additivity issues pose a significant challenge to extending results like these to the quantum case.

Acknowledgments

We are grateful to Mario Berta, Omar Fawzi, and Marco Tomamichel for discussions and for sharing an early draft of [49]. We also thank Patrick Hayden for discussions. CH is supported by the Spanish MINECO, project FIS2013-40627-P, as well as by the Generalitat de Catalunya, CIRIT project no. 2014 SGR 966. JW is supported in part by Canada's NSERC. MMW acknowledges support from the NSF under Award No. CCF-1350397.

[1] Frank Gaitan. *Quantum Error Correction and Fault Tolerant Quantum Computing.* CRC Press, 2008.

[2] Daniel A. Lidar and Todd A. Brun, editors. *Quantum Error Correction.* Cambridge University Press, 2013.

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, September 2009. arXiv:0802.4155.

[4] James R. Norris. *Markov Chains.* Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, 1997.

[5] Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Communications in Mathematical Physics*, 246(2):359–374, April 2004. arXiv:quant-ph/0304007.

[6] Ben Ibinson, Noah Linden, and Andreas Winter. Robustness of quantum Markov chains. *Communications in Mathematical Physics*, 277(2):289–304, January 2008. arXiv:quant-ph/0611057.

[7] Paul Erker. How not to Rényi-generalize the quantum conditional mutual information. *Journal of Physics A: Mathematical and Theoretical*, 48(27):275303, July 2015. arXiv:1404.3628.

[8] Dénes Petz. Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. *Communications in Mathematical Physics*, 105(1):123–131, March 1986.

[9] Dénes Petz. Sufficiency of channels over von Neumann algebras. *Quarterly Journal of Mathematics*, 39(1):97–108, 1988.

[10] Kaushik P. Seshadreesan and Mark M. Wilde. Fidelity of recovery, squashed entanglement, and measurement recoverability. *Physical Review A*, 92(4):042321, October 2015. arXiv:1410.1441.

[11] Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical*

Physics, 9(2):273–279, 1976.

[12] Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

[13] Omar Fawzi and Renato Renner. Quantum conditional mutual information and approximate Markov chains. *Communications in Mathematical Physics*, 340(2):575–611, December 2015. arXiv:1410.0664.

[14] Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Physical Review Letters*, 100(23):230501, June 2008.

[15] Jon Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55(11):5339–5351, November 2009. arXiv:0706.2907.

[16] Fernando G. S. L. Brandão, Aram W. Harrow, Jonathan Oppenheim, and Sergii Strelchuk. Quantum conditional mutual information, reconstructed states, and state redistribution. *Physical Review Letters*, 115:050501, 2015. arXiv:1411.4921.

[17] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, September 2011. arXiv:1010.1750.

[18] Andreas Winter and Ke Li. A stronger subadditivity relation? http://www.maths.bris.ac.uk/ ∼csajw/ stronger_subadditivity.pdf, 2012.

[19] Isaac H. Kim. Application of conditional independence to gapped quantum many-body systems. http://www.physics.usyd.edu.au/quantum/Coogee2013, January 2013. Slide 43.

[20] Lin Zhang. A lower bound of quantum conditional mutual information. March 2014. arXiv:1403.1424.

[21] Mario Berta, Kaushik Seshadreesan, and Mark M. Wilde. Rényi generalizations of the conditional quantum mutual information. *Journal of Mathematical Physics*, 56(2):022205, February 2015. arXiv:1403.6102.

[22] Kaushik P. Seshadreesan, Mario Berta, and Mark M. Wilde. Rényi squashed entanglement, discord, and relative entropy differences. *Journal of Physics A: Mathematical and Theoretical*, 48(39):395303, September 2015. arXiv:1410.1443.

[23] Ke Li and Andreas Winter. Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps, 2014. arXiv:1410.4184.

[24] Mario Berta, Marius Lemm, and Mark M. Wilde. Monotonicity of quantum relative entropy and recoverability. *Quantum Information and Computation*, 15(15 & 16):1333–1354, November 2015. arXiv:1412.4067.

[25] Nilanjana Datta and Mark M. Wilde. Quantum Markov chains, sufficiency of quantum channels, and Rényi information measures. *Journal of Physics A: Mathematical and Theoretical*, 48(50):505301, December 2015. arXiv:1501.05636.

[26] Mario Berta and Marco Tomamichel. The fidelity of recovery is multiplicative. *IEEE Transactions on Information Theory*, 62(4):1758–1763, April 2016. arXiv:1502.07973.

[27] David Sutter, Omar Fawzi, and Renato Renner. Universal recovery map for approximate Markov chains. April 2015. arXiv:1504.07251.

[28] Mark M. Wilde. Recoverability in quantum information theory. *Proceedings of the Royal Society A*, 471(2182):20150338, October 2015. arXiv:1505.04661.

[29] Frédéric Dupuis and Mark M. Wilde. Swiveled Rényi entropies. June 2015. arXiv:1506.00981.

[30] David Sutter, Marco Tomamichel, and Aram W. Harrow. Strengthened monotonicity of relative entropy via pinched Petz recovery map. July 2015. arXiv:1507.00303.

[31] Marius Junge, Renato Renner, David Sutter, Mark M. Wilde, and Andreas Winter. Universal recovery from a decrease of quantum relative entropy. September 2015. arXiv:1509.07127.

[32] John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and System Science*, 2009. arXiv:0804.3401.

[33] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends in Theoretical Computer Science*, 11(1–2):1–215, 2016.

[34] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. *STOC '10: Proceedings of the 42nd ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[35] John Watrous. Limits on the power of quantum statistical zero-knowledge. *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468, November 2002. arXiv:quant-ph/0202111.

[36] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. arXiv:quant-ph/0511020.

[37] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. Quantum interactive proofs and the complexity of separability testing. *Theory of Computing*, 11(3):59–103, 2015. arXiv:1308.5788.

[38] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543, Atlanta, GA, USA, October 2009. arXiv:0905.1300.

[39] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. Prentice-Hall, Providence, Rhode Island, USA, 2002.

[40] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theor. Comput. Sci.*, 292(3):575–588, 2003.

[41] William F. Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6:211–216, 1955.

[42] Fuzhen Zhang. *Matrix Theory: Basic Results and Techniques*. Springer, 2011.

[43] Fumio Hiai and Dénes Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143(1):99–114, December 1991.

[44] Tomohiro Ogawa and Hiroshi Nagaoka. Strong converse and Stein's lemma in quantum hypothesis testing. *IEEE Transactions on Information Theory*, 46(7):2428–2433, November 2000. arXiv:quant-ph/9906090.

[45] Fernando G. S. L. Brandão and Martin B. Plenio. A generalization of quantum Stein's lemma. *Communications in Mathematical Physics*, 295(3):791–828, May 2010. arXiv:0904.0281.

[46] Francesco Buscemi and Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, March 2010. arXiv:0902.0158.

[47] Ligong Wang and Renato Renner. One-shot classical-

quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, May 2012. arXiv:1007.5456.

[48] Milán Mosonyi and Tomohiro Ogawa. Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. *Communications in Mathematical Physics*, 334(3):1617–1648, March 2015. arXiv:1309.3228.

[49] Mario Berta, Omar Fawzi, and Marco Tomamichel. On variational expressions for quantum relative entropies. December 2015. arXiv:1512.02615.

[50] Marco Tomamichel and Masahito Hayashi. Operational interpretation of Renyi information measures via composite hypothesis testing against product and Markov distributions. November 2015. arXiv:1511.04874.