A Conceptually Simple Proof of the Quantum Reverse Shannon Theorem

Mario Berta[1,2], Matthias Christandl[1,2], and Renato Renner[1]

[1] Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
{berta,christandl,renner}@phys.ethz.ch
[2] Faculty of Physics, Ludwig-Maximilians-Universität München, 80333 Munich, Germany

Abstract. The Quantum Reverse Shannon Theorem states that any quantum channel can be simulated by an unlimited amount of shared entanglement and an amount of classical communication equal to the channel's entanglement assisted classical capacity. In this extended abstract, we summarize a new and conceptually simple proof of this theorem [journal reference: arXiv.org:quant-ph/0912.3805], which has previously been proved in [Bennett et al., arXiv.org:quant-ph/0912.5537]. Our proof is based on optimal one-shot Quantum State Merging and the Post-Selection Technique for quantum channels.

1 Introduction

The birth of classical information theory can be dated to 1948, when Shannon derived his famous 'Noisy Channel Coding Theorem' [23]. It shows that the capacity C of a classical channel $\mathcal{J}$ is given by the maximum, over the input distributions X, of the input/output mutual information

$$C = \max_X (H(X) + H(\mathcal{J}(X)) - H(X, \mathcal{J}(X))) \ .$$

Shannon also showed that the capacity does not increase if one allows to use shared randomness between the sender and the receiver. In 2001 Bennett et al. [3] proved the so called 'Classical Reverse Shannon Theorem' which states that, given free shared randomness between the sender and the receiver, every channel can be simulated using an amount of classical communication equal to the capacity of the channel. This is particularly interesting because it implies that in the presence of free shared randomness, the capacity of a channel $\mathcal{J}$ to simulate another channel $\mathcal{I}$ is given by the ratio of their plain capacities $C_R(\mathcal{J},\mathcal{I}) = \frac{C(\mathcal{J})}{C(\mathcal{I})}$ and hence only a single parameter remains to characterize classical channels.

In contrast to the classical case, a quantum channel has various distinct capacities [3, 9, 12, 17, 22, 24]. In [3] Bennett et al. argue that the entanglement assisted classical capacity C_E of a quantum channel $\mathcal{E}$ is the natural quantum generalization of the classical capacity of a classical channel. They show that

W. van Dam et al. (Eds.): TQC 2010, LNCS 6519, pp. 131–140, 2011.

the entanglement assisted classical capacity is given by the quantum mutual information

$$C_E = \max_{\rho}(H(\rho) + H(\mathcal{E}(\rho)) - H((\mathcal{E} \otimes \mathrm{id})\Phi_\rho)) \ ,$$

where the maximum goes over all input distributions ρ and Φ_ρ is a purification of ρ. Motivated by this, they conjectured the 'Quantum Reverse Shannon Theorem (QRST)' in [3]. Subsequently Bennett, Devetak, Harrow, Shor and Winter proved the theorem in [2]. The theorem states that any quantum channel can be simulated by an unlimited amount of shared entanglement and an amount of classical communication equal to the channel's entanglement assisted classical capacity. So if entanglement is for free, we can conclude in complete analogy with the classical case, that the capacity of a quantum channel $\mathcal{E}$ to simulate another quantum channel $\mathcal{F}$ is given by $C_E(\mathcal{E}, \mathcal{F}) = \frac{C_E(\mathcal{E})}{C_E(\mathcal{F})}$ and hence only a single parameter remains to characterize quantum channels.

Free entanglement in quantum information theory is usually given in the form of maximally entangled states. But for the Quantum Reverse Shannon Theorem it surprisingly turned out that maximally entangled states are not the appropriate resource for general input sources. More precisely, if one has only maximally entangled states as an entanglement resource, even if these are arbitrarily many, the Quantum Reverse Shannon Theorem cannot be proven [2]. This is because of an issue known as entanglement spread, which basically comes from the fact that entanglement cannot be conditionally discarded without either using communication or causing decoherence [11]. If we change the entanglement resource from maximally entangled states to embezzling states [29] however, the problem of entanglement spread can be overcome.

Definition 1.1 (Hayden, van Dam [29]). *A bipartite state of the form*

$$|\mu(k)\rangle_{AB} = \frac{1}{\sqrt{G(k)}} \sum_{j=1}^{k} \frac{1}{\sqrt{j}} |jj\rangle_{AB} \ , \tag{1}$$

where $G(k) = \sum_{j=1}^{k} \frac{1}{j}$*, is called* embezzling state *of index* k *(which is the Schmidt-rank of* $|\mu(k)\rangle$*).*

These states have the following special feature.

Proposition 1.2 (Hayden, van Dam [29]). *Let* $\epsilon > 0$ *and let* $|\varphi\rangle_{AB}$ *be a bipartite pure (and normalized) state of Schmidt-rank* m*. Then the transformation*

$$|\mu(k)\rangle_{AB} \mapsto |\mu(k)\rangle_{AB} \otimes |\varphi\rangle_{AB} \tag{2}$$

can be accomplished with fidelity[1] *better than* $(1 - \epsilon)$ *for* $k > m^{1/\epsilon}$ *without any communication.*

[1] The fidelity between two normalized states ρ and σ is defined as $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$, where $\|\Gamma\|_1 = \mathrm{tr}\sqrt{\Gamma\Gamma^\dagger}$ is the trace norm.

In this extended abstract we summarize a conceptually simple proof of the Quantum Reverse Shannon Theorem. It is based on a new one-shot version for 'Quantum State Merging' and the 'Post-Selection Technique' for quantum channels. As in [2] we make use of embezzling states.

Quantum State Merging is a well known quantum information processing primitive [1, 13, 14, 18] and corresponds to the quantum generalization of classical Slepian and Wolf coding [25]. There are basically two (equivalent) versions of State Merging, one of them also called the 'Mother Protocol' [1]. Let ρ_{AB} be a bipartite quantum state, where A is with a party *Alice* and B is with another party *Bob*. State Merging answers the question of how much of a given resource (classical/quantum communication, entanglement) is needed in order to optimally transfer the A-part of ρ_{AB} to Bob (relative to a purifying system R).[2] The dual of this, called *Quantum State Splitting*, addresses the problem of how much of a given resource (classical/quantum communication, entanglement) is needed in order to transfer the B' part of a state $\rho_{B'B}$ held by Bob, (back) to Alice (relative to a purifying system R).[3]

The *Post-Selection Technique* was introduced in [7] and is a tool to show that two completely positive and trace preserving (CPTP) maps, that act symmetrically on an n-partite system, are almost equal, in the sense that they are close in the metric induced by the diamond norm [15]. The diamond norm involves a maximization over all possible input states. The Post-Selection Technique allows to drop this maximization. In fact, it suffices to consider a single de Finetti type input state (i.e. a state which consist of n identical and independent copies of an (unknown) state on a single subsystem).

Our proof of the Quantum Reverse Shannon Theorem is based on the following idea. Let $\mathcal{E}_{A\to B}$ be a quantum channel that takes inputs ρ_A on Alice's side and outputs $\mathcal{E}_{A\to B}(\rho_A)$ on Bob's side. To find a way to simulate this quantum channel, it is useful to think of $\mathcal{E}_{A\to B}$ as

$$\mathcal{E}_{A\to B}(\rho_A) = \mathrm{tr}_{A'}(U_{A\to BA'}\rho_A U_{A\to BA'}^{\dagger}) \ ,$$

where A' is an additional register and $U_{A\to BA'}$ is some isometry from A to BA'. This is the Stinespring dilation [26]. The idea is to first simulate the quantum channel locally at Alice's side, giving her $\sigma_{BA'} = U_{A\to BA'}\rho_A U_{A\to BA'}^{\dagger}$, and in a second step use State Splitting to do an optimal state transfer of the B-part to Bob's side, such that he holds $\sigma_B = \mathcal{E}_{A\to B}(\rho_A)$ in the end. This simulates the channel $\mathcal{E}_{A\to B}$. To prove the Quantum Reverse Shannon Theorem, it is then sufficient to show that the classical communication rate of the State Splitting protocol is $C_E(\mathcal{E})$.

[2] More precisely, State Merging corresponds to the task of obtaining the state $\rho_{B'BR} = (\mathrm{id}_{A\to B'} \otimes \mathrm{id}_{BR})\rho_{ABR}$, where ρ_{ABR} is a purification of ρ_{AB}, R is a reference, and BB' is held by Bob.

[3] More precisely, State Splitting corresponds to the task of obtaining the state $\rho_{ABR} = (\mathrm{id}_{B'\to A} \otimes \mathrm{id}_{BR})\rho_{B'BR}$, where $\rho_{B'BR}$ is a purification of $\rho_{B'B}$, R is a reference, A is held by Alice and B is held by Bob.

We realize this idea in two steps. Firstly, we propose a new version of State Merging/Splitting (since the known protocols are not good enough to achieve a classical communication rate of C_E). For the analysis we require a 'Decoupling Theorem', which is optimal in the most general case, the so called one-shot case [4, 6, 10]. To quantify the resources needed for one-shot State Merging/Splitting, we make use of the 'Smooth Rényi Entropy Calculus' [8, 16, 19, 27, 28]. Secondly, we use the Post-Selection Technique to show that our protocol for one-shot State Splitting for a particular de Finetti type input state is sufficient to asymptotically simulate the channel $\mathcal{E}$ for a classical communication rate of C_E for any input. This then completes the proof of the Quantum Reverse Shannon Theorem.

This extended abstract is structured as follows. In Section 2 we introduce our notation and give some definitions. In particular, we review the smooth entropy measures that we need in the following. Our results about one-shot State Splitting are then discussed in Section 3. Finally, we sketch our proof of the Quantum Reverse Shannon Theorem in Section 4 (journal reference [5]).

2 (Smooth) Entropy Measures – Notation and Definitions

We assume that all Hilbert spaces, in the following denoted $\mathcal{H}$, are finite-dimensional. We write $|A|$ for the dimension of $\mathcal{H}_A$. The the set of linear, non-negative operators on $\mathcal{H}$ is denoted by $\mathcal{P}(\mathcal{H})$. $\mathbb{1}$ denotes the identity in $\mathcal{P}(\mathcal{H})$. We define the sets of normalized states $\mathcal{S}_=(\mathcal{H}) = \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho = 1\}$ and subnormalized states $\mathcal{S}_\leq(\mathcal{H}) = \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho \leq 1\}$).

In quantum information theory one usually makes the assumption that the resources are independent and identically distributed (i.i.d.) and is interested in asymptotic rates. In this case many operational quantities can be expressed in terms of a few information measures (which are usually based on the von Neumann entropy). In order to overcome the asymptotic and i.i.d. assumption, the Smooth Rényi Entropy Calculus was introduced by Renner et al. [19, 20, 21].

Recall the following standard definitions. The *von Neumann entropy* of $\rho \in \mathcal{S}_=(\mathcal{H})$ is defined as $H(\rho) = -\mathrm{tr}(\rho \log \rho)$. The *quantum relative entropy* of $\rho \in \mathcal{S}_\leq(\mathcal{H})$ with respect to $\sigma \in \mathcal{P}(\mathcal{H})$ is given by $D(\rho\|\sigma) = \mathrm{tr}(\rho \log \rho) - \mathrm{tr}(\rho \log \sigma)$. The *conditional von Neumann entropy* of A given B for $\rho_{AB} \in \mathcal{S}_=(\mathcal{H})$ is defined as $H(A|B)_\rho = -D(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B)$. The *mutual information* between A and B for $\rho_{AB} \in \mathcal{S}_=(\mathcal{H})$ is given by $I(A:B)_\rho = D(\rho_{AB}\|\rho_A \otimes \rho_B)$. Note that we can also write

$$H(A|B)_\rho = -\inf_{\sigma_B} D(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B) \tag{3}$$

$$I(A:B)_\rho = \inf_{\sigma_B} D(\rho_{AB}\|\rho_A \otimes \sigma_B) \ , \tag{4}$$

where $\sigma_B \in \mathcal{S}_=(\mathcal{H}_B)$.

Following Datta [8] we define the *max-relative entropy* of $\rho \in \mathcal{S}_\leq(\mathcal{H})$ with respect to $\sigma \in \mathcal{P}(\mathcal{H})$ as

$$D_{\max}(\rho\|\sigma) = \inf\{\lambda \in \mathbb{R} : 2^\lambda \cdot \sigma \geq \rho\} \ . \tag{5}$$

The *conditional min-entropy* [19] of A given B for $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ is defined as

$$H_{\min}(A|B)_\rho = -\inf_{\sigma_B} D_{\max}(\rho_{AB} \| \mathbb{1}_A \otimes \sigma_B) = \sup_{\sigma_B} H_{\min}(A|B)_{\rho|\sigma} \ , \tag{6}$$

where $H_{\min}(A|B)_{\rho|\sigma} = -D_{\max}(\rho_{AB} \| \mathbb{1}_A \otimes \sigma_B)$ and $\sigma_B \in \mathcal{S}_{=}(\mathcal{H}_B)$. In the special case where B is trivial, we have $H_{\min}(A)_\rho = -\log \|\rho_A\|_\infty$.[4] The *max-information* that B has about A for $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ is defined as

$$I_{\max}(A:B)_\rho = \inf_{\sigma_B} D_{\max}(\rho_{AB} \| \rho_A \otimes \sigma_B) \ , \tag{7}$$

where $\sigma_B \in \mathcal{S}_{=}(\mathcal{H}_B)$. Note that unlike the mutual information, this definition is not symmetric. The smooth entropy measures are defined by extremizing the non-smooth measures over a set of nearby states, where our notion of nearby is expressed in terms of the *purified distance*. For $\rho, \sigma \in \mathcal{S}_{\leq}(\mathcal{H})$ it is defined as [28]

$$P(\rho, \sigma) = \sqrt{1 - \bar{F}(\rho, \sigma)^2} \ , \tag{8}$$

where $\bar{F}(\cdot\,, \cdot)$ denotes the *generalized fidelity* (which equals the standard fidelity if at least one of the states is normalized),

$$\bar{F}(\rho, \sigma) = \left\| \sqrt{\rho \oplus (1 - \mathrm{tr}\rho)} \sqrt{\sigma \oplus (1 - \mathrm{tr}\sigma)} \right\|_1 = \|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \mathrm{tr}\rho)(1 - \mathrm{tr}\sigma)} \ . \tag{9}$$

The purified distance is a distance measure. Henceforth we call ρ, $\sigma \in \mathcal{S}_{\leq}(\mathcal{H})$ ϵ-close if $P(\rho, \sigma) \leq \epsilon$ and denote this by $\rho \approx_\epsilon \sigma$. Miscellaneous properties of the purified distance are stated in Appendix A of [5]. We use the purified distance to specify a ball of subnormalized density operators around $\rho \in \mathcal{S}_{\leq}(\mathcal{H})$:

$$\mathcal{B}^\epsilon(\rho) = \{\overline{\rho} \in \mathcal{S}_{\leq}(\mathcal{H}) : P(\rho, \overline{\rho}) \leq \epsilon\} \ .$$

For any $\epsilon \geq 0$, the *smooth conditional min-entropy* [19] of A given B for $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ is defined as

$$H^\epsilon_{\min}(A|B)_\rho = \sup_{\overline{\rho}_{AB}} H_{\min}(A|B)_{\overline{\rho}} \ , \tag{10}$$

where $\overline{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})$. The *smooth max-information* that B has about A for $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ is defined as

$$I^\epsilon_{\max}(A:B)_\rho = \inf_{\overline{\rho}_{AB}} I_{\max}(A:B)_{\overline{\rho}} \ , \tag{11}$$

where $\overline{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})$. These smooth entropy measures can be seen as generalizations of their corresponding von Neumann quantities in the sense of Lemmata B.17 and B.22 in [5], i.e. they asymptotically converge to the conditional von Neumann entropy and the mutual information resp. In Section 3 we give an operational meaning to the smooth max-information (see Theorem 3.2 and Theorem 3.3).[5]

[4] $\|\rho_A\|_\infty$ denotes the maximal eigenvalue of ρ_A.

[5] For an operational meaning of the smooth conditional min-entropy see e.g. [4, 19].

3 One-Shot Quantum State Splitting

State Merging, State Splitting and other related quantum information processing primitives are discussed in detail in [1, 13, 14, 18]. In contrast to the existing literature, we are not only interested in asymptotic rates, but in a (tight) one-shot protocol for State Splitting. For more details see [5].

Definition 3.1 (Quantum State Splitting with embezzling states). *Consider a system consisting of three parties; Alice, Bob and a reference. Let $\rho_{ACR} \in \mathcal{S}_{\leq}(\mathcal{H}_{ACR})$ be pure, where the reference is denoted by R and Alice has AC. Let B be an ancilla at Bob's side of the same size as C. Furthermore let Alice and Bob share an embezzling state of index k that lives on an additional register $\overline{AB}$. A process is called* embezzling State Splitting *of ρ_{ACR} with error ϵ if it consists of applying local operations at Alice's side, local operations at Bob's side, sending q qubits from Alice to Bob and outputs a state $\omega_{ABR} \approx_\epsilon \rho_{ABR}$ with $\rho_{ABR} = (\mathrm{id}_{C\to B} \otimes \mathrm{id}_{AR})\rho_{ACR}$. q is called quantum communication cost and $e_b = \lceil \log k \rceil$ is the embezzling cost.*

Theorem 3.2. *Let $\rho_{ACR} = |\psi\rangle\langle\psi|_{ACR} \in \mathcal{S}_{\leq}(\mathcal{H}_{ACR})$, $\epsilon > 0$, $\epsilon' \geq 0$ and $\epsilon'' > 0$. Then there exists an embezzling State Splitting protocol of ρ_{ACR} with a quantum communication cost of*

$$q \leq \frac{1}{2} I_{\max}^{\epsilon'}(C:R)_\rho + \log \frac{1}{\epsilon} + 4 + \log\log|C| \tag{12}$$

and an embezzling cost of

$$e_b \geq \lceil (\log|C| - \log\frac{1}{\epsilon})^{1/\epsilon''} \rceil \tag{13}$$

for an error of at most $\epsilon' + \sqrt{\epsilon} + |C|^{-1/2} + \sqrt{\epsilon''}$.

For a proof see Theorem III.2 in [5]. The following theorem shows that this is optimal up to small additive terms.

Theorem 3.3 (Converse). *There does not exist a State Splitting protocol with error ϵ and a quantum communication cost smaller than*

$$q = \frac{1}{2} I_{\max}^{\epsilon}(C:R)_\rho \ . \tag{14}$$

For a proof see Theorem III.9 in [5].

4 The Quantum Reverse Shannon Theorem

We now present our main result; a proof of the Quantum Reverse Shannon Theorem. Let $\mathcal{E}_{A\to B}$ be a quantum channel with

$$\begin{aligned} \mathcal{E}_{A\to B} : \mathcal{S}(\mathcal{H}_A) &\to \mathcal{S}(\mathcal{H}_B) \\ \rho_A &\mapsto \mathcal{E}_{A\to B}(\rho_A) \ , \end{aligned}$$

where we want to think of A being at Alice's side and B being at Bob's side. The Quantum Reverse Shannon Theorem states that if we have an embezzling state (of arbitrary large index) between Alice and Bob, we can asymptotically simulate $\mathcal{E}_{A\to B}$ only using local operations at Alice's side, local operations at Bob's side, and a classical communication rate (from Alice to Bob) of

$$C_E(\mathcal{E}) = \max_{\rho} I(B:R)_{(\mathcal{E}\otimes \mathrm{id})(\Phi)} \ , \tag{15}$$

where Φ_{AR} is a purification of ρ_A.[6] Using Stinespring's dilation [26], we can think of $\mathcal{E}_{A\to B}$ as

$$\mathcal{E}_{A\to B}(\rho_A) = \mathrm{tr}_{B'}(U_{A\to BA'}\rho_A U^{\dagger}_{A\to BA'}) \ ,$$

where A' is an additional register with $|A'| \leq |A||B|$ and $U_{A\to BA'}$ is some isometry from A to BA'. The idea of our proof is to first simulate the quantum channel locally at Alice's side, giving us $\sigma_{BA'} = U_{A\to BA'}\rho_A U^{\dagger}_{A\to BA'}$, and then use embezzling State Splitting to do an optimal state transfer of the B-part to Bob's side, such that he holds $\sigma_B = \mathcal{E}_{A\to B}(\rho_A)$ in the end. Note that we can replace the quantum communication in the embezzling State Splitting protocol by twice as much classical communication since we have free entanglement and can therefore use teleportation. Although the free entanglement is given in the form of embezzling states, maximally entangled states can be created without any (additional) communication (Proposition 1.2). Because the quantum reverse Shannon theorem makes an asymptotic statement, we have to make our considerations for a general $n \in \mathbb{N}$. The idea is then to show the existence of a protocol $\mathcal{F}^n_{A\to B}$ that is arbitrarily close to $\mathcal{E}^{\otimes n}_{A\to B}$ for $n \to \infty$, has a classical communication rate of $C_E(\mathcal{E})$ and works for any input. We do this by using the post-selection technique (Proposition D.4 in [5]).

Since the post-selection technique only applies to permutation invariant maps, we need to ensure that the protocol that we want to use for the simulation of $\mathcal{E}^{\otimes n}_{A\to B}$, can be made to act symmetrically on the n-partite input system $\mathcal{H}^{\otimes n}_A$. This can be done by inserting a symmetrization step, that uses maximally entangled states (cf. Figure 1). For more details see Section IV of [5].

Let $\delta > 0$. The way to go is to show the existence of a permutation invariant $\mathcal{F}^n_{A\to B}$ with the desired properties as discussed above (i.e. it should be local and have a classical communication rate of $C_E(\mathcal{E})$) and

$$\|((\mathcal{E}^{\otimes n}_{A\to B} - \mathcal{F}^n_{A\to B}) \otimes \mathrm{id}_{RR'})(\zeta^n_{ARR'})\|_1 \leq \delta(n+1)^{-(|A|^2-1)} \ , \tag{16}$$

where $\zeta^n_{ARR'}$ is a purification of $\zeta^n_{AR} = \int \rho^{\otimes n}_{AR} d(\rho_{AR})$, ρ_{AR} is pure and $d(.)$ is the measure on the normalized pure states on $\mathcal{H}_{AR}$ induced by the Haar measure on the unitary group acting on $\mathcal{H}_{AR}$, normalized to $\int d(.) = 1$. Once we have achieved this it follows from the post-selection technique (Proposition D.4

[6] Since all purifications give the same amount of entropy, we do not need to specify which one we use.

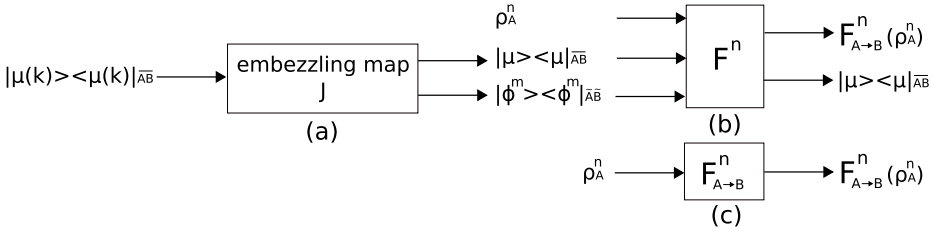

Fig. 1. (a) $\mathcal{J}$ is the map that embezzles m maximally entangled states $|\Phi^m\rangle\langle\Phi^m|_{\tilde{A}\tilde{B}}$ out of $|\mu\rangle\langle\mu|_{\overline{AB}}$. These maximally entangled states are then used for a symmetrization step. (b) The whole protocol $\mathcal{F}^n_{A\to B}$ (that should simulate $\mathcal{E}^{\otimes n}_{A\to B}$) a priori takes $\rho^n_A \otimes |\mu\rangle\langle\mu|_{\overline{AB}} \otimes |\Phi^m\rangle\langle\Phi^m|_{\tilde{A}\tilde{B}}$ as an input. But since this input is constant on all registers except for A, we can think of the map as in (c), namely as a CPTP map $\mathcal{F}^n_{A\to B}$ which only takes the input ρ^n_A.

in [5]) that $\|\mathcal{E}^{\otimes n}_{A\to B} - \mathcal{F}^n_{A\to B}\|_\diamond \leq \delta$, and this is what we want to show.[7] Since we only need to consider the particular de Finetti type input state $\zeta^n_{ARR'}$ to show (16), we can use the State Splitting protocol of Theorem 3.2 for $\zeta^n_{ARR'}$ to construct $\mathcal{F}^n_{A\to B}$. A lengthy calculation (see Section IV of [5]) shows, that a classical communication rate of $C_E(\mathcal{E})$ is sufficient to get (16). This concludes the proof of the Quantum Reverse Shannon Theorem.

Acknowledgments

We thank Jürg Wullschleger and Andreas Winter for inspiring discussions. MB and MC are supported by the Swiss National Science Foundation (grant PP00P2-128455) and the German Science Foundation (grants CH 843/1-1 and CH 843/2-1). RR acknowledges support from the Swiss National Science Foundation (grant 200021-119868).

References

[1] Abeyesinghe, A., Devetak, I., Hayden, P., Winter, A.: The mother of all protocols: Restructuring quantum information's family tree. Proc. R. Soc. A 465(2108), 2537 (2009), arXiv.org:quant-ph/0606225

[2] Bennett, C.H., Devetak, I., Harrow, A.W., Shor, P.W., Winter, A.: The quantum reverse Shannon theorem (2006), arXiv.org:quant-ph/0912.5537

[3] Bennett, C.H., Shor, P.W., Smolin, J.A., Thapliyal, A.V.: Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. IEEE Trans. Inf. Theory 48(10), 2637 (2002), arXiv.org:quant-ph/0106052

[4] Berta, M.: Single-shot quantum state merging, Diploma thesis ETH Zurich (2008), arXiv.org:quant-ph/0912.4495

[7] For a precise definition of the Diamond norm see [15].

[5] Berta, M., Christandl, M., Renner, R.: A Conceptually Simple Proof of the Quantum Reverse Shannon Theorem (2009), arXiv.org:quant-ph/0912.3805, submitted to Comm. Math. Phys. (2009)
[6] Berta, M., Dupuis, F., Renner, R., Wullschleger, J.: Optimal decoupling (2010) (in preparation)
[7] Christandl, M., König, R., Renner, R.: Post-selection technique for quantum channels with applications to quantum cryptography. Phys. Rev. Lett 102, 20504 (2009), arXiv.org:quant-ph/0809.3019
[8] Datta, N.: Min- and max- relative entropies and a new entanglement monotone. IEEE Trans. Inf. Theory 55(6), 2816 (2009), arXiv.org:quant-ph/0803.2770
[9] Devetak, I.: The private classical capacity and quantum capacity of a quantum channel. IEEE Trans. Inf. Theory 51, 44 (2005), arXiv:quant-ph/0304127
[10] Dupuis, F.: The Decoupling Approach to Quantum Information Theory. PhD thesis, Université de Montréal (2009), arXiv.org:quant-ph/1004.1641
[11] Harrow, A.W.: Entanglement spread and clean resource inequalities. Proc. XVI Int. Cong. Math. Phys. 536 (2009), arXiv.org:quant-ph/0909.1557
[12] Holevo, A.S.: The capacity of the quantum communication channel with general signal states. IEEE Trans. Inf. Theory 44, 269 (1998), arXiv.org:quant-ph/9611023
[13] Horodecki, M., Oppenheim, J., Winter, A.: Partial quantum information. Nature 436, 673–676 (2005), arXiv.org:quant-ph/0505062
[14] Horodecki, M., Oppenheim, J., Winter, A.: Quantum state merging and negative information. Comm. Math. Phys 269, 107 (2006), arXiv.org:quant-ph/0512247
[15] Kitaev, A.: Quantum computations: algorithms and error correction. Russian Math. Surveys 52, 1191 (1997)
[16] König, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theory 55(9), 4337 (2009), arXiv.org:quant-ph/0807.1338
[17] Lloyd, S.: Capacity of the noisy quantum channel. Phys. Rev. A 55, 1613 (1997), arXiv.org:quant-ph/9604015
[18] Oppenheim, J.: State redistribution as merging: introducing the coherent relay (2008), arXiv.org:quant-ph/0805.1065
[19] Renner, R.: Security of Quantum Key Distribution. PhD thesis, ETH Zurich (2005), arXiv.org:quant-ph/0512258
[20] Renner, R.S., König, R.: Universally Composable Privacy Amplification Against Quantum Adversaries. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 407–425. Springer, Heidelberg (2005)
[21] Renner, R., Wolf, S.: Smooth Rényi entropy and applications. In: Proc. IEEE Int. Symp. Inf. Theory, vol. 233 (2004)
[22] Schumacher, B., Westmoreland, M.D.: Sending classical information via noisy quantum channels. Phys. Rev. A 56, 131 (1997)
[23] Shannon, C.E.: A mathematical theory of communication. Bell. Syst. Tech. J. 423, 379–423, 623–656 (1948)
[24] Shor, P.W.: The quantum channel capacity and coherent information. In: Lecture notes, MSRI Workshop on Quantum Computation (2002)
[25] Slepian, D., Wolf, J.: Noiseless coding of correlated information sources. IEEE Trans. Inf. Theory 19, 461 (1971)
[26] Stinespring, W.: Positive function on C*-algebras. Proc. Amer. Math. Soc. 6, 211 (1955)

[27] Tomamichel, M., Colbeck, R., Renner, R.: A fully quantum asymptotic equipartition property. IEEE Trans. Inf. Theory 55(12), 5840 (2009), arXiv.org:quant-ph/0811.1221
[28] Tomamichel, M., Colbeck, R., Renner, R.: Duality between smooth min- and max-entropies. IEEE Trans. Inf. Theory 56(9), 4674 (2010), arXiv.org:quant-ph/0907.5238
[29] van Dam, W., Hayden, P.: Universal entanglement transformations without communication. Phys. Rev. A, Rapid Comm. 67, 060302(R) (2003), arXiv.org:quant-ph/0201041