nature COMMUNICATIONS

ARTICLE

Received 5 Aug 2015 | Accepted 16 Mar 2016 | Published 9 May 2016

DOI: 10.1038/ncomms11419 OPEN

Quantum coding with finite resources

Marco Tomamichel[1], Mario Berta[2] & Joseph M. Renes[3]

The quantum capacity of a memoryless channel determines the maximal rate at which we can communicate reliably over asymptotically many uses of the channel. Here we illustrate that this asymptotic characterization is insufficient in practical scenarios where decoherence severely limits our ability to manipulate large quantum systems in the encoder and decoder. In practical settings, we should instead focus on the optimal trade-off between three parameters: the rate of the code, the size of the quantum devices at the encoder and decoder, and the fidelity of the transmission. We find approximate and exact characterizations of this trade-off for various channels of interest, including dephasing, depolarizing and erasure channels. In each case, the trade-off is parameterized by the capacity and a second channel parameter, the quantum channel dispersion. In the process, we develop several bounds that are valid for general quantum channels and can be computed for small instances.

[1] School of Physics, University of Sydney, Sydney, New South Wales 2006, Australia. [2] Institute for Quantum Information and Matter, Division of Physics, Mathematics and Astronomy, California Institute of Technology, Pasadena, California 91125, USA. [3] Department of Physics, Institute for Theoretical Physics, ETH Zurich, 8093 Zürich, Switzerland. Correspondence and requests for materials should be addressed to M.T. (email: marco.tomamichel@sydney.edu.au).

One of the quintessential topics in quantum information theory is the study of reliable quantum information transmission over noisy quantum channels. Here 'channel' simply refers to a description of a physical evolution. In the standard formulation, one considers communication between two points connected by a memoryless channel that can be used many times in sequence. In this case, the sender first encodes a quantum state into a sequence of registers and then sends them one by one through the channel to the receiver. The receiver collects these registers and then attempts to decode the quantum state. Equivalently, one considers a collection of physical qubits that are exposed to independent noise. The goal is then to encode quantum information (logical qubits) into this system (physical qubits) so that the quantum information can be retrieved with high fidelity after a given time. One of the primary goals of information theory is to find fundamental limits imposed on any coding scheme that attempts to accomplish this task.

Following a tradition going back to Shannon's groundbreaking work[1], this problem is usually studied asymptotically: the quantum capacity of a channel[2–7] is defined as the optimal rate (in qubits per use of the channel) at which one can transmit quantum information with vanishing error as the number of sequential channel uses increases to infinity. In the context of information storage, the rate simply corresponds to the ratio of logical to physical qubits, and the number of physical qubits is taken to be asymptotically large. Such an asymptotic analysis has proven to be pertinent in the analysis of classical communication (cc) systems—but is it also satisfactory in the quantum setting?

Achieving (or approximately achieving) the quantum capacity generally requires both the receiver and sender to coherently manipulate an array of qubits that grows proportionally with the number of channel uses. More precisely, the sender is required to prepare arbitrary states that are entangled between all channel inputs and the receiver needs to perform a joint measurement on all channel outputs. While classical computers can readily operate on very large amounts of data, at least for the near future it appears unrealistic to expect that encoding and decoding circuits can store or coherently manipulate large numbers of qubits. Thus, it is natural to ask how well quantum coding schemes perform when we restrict the size of the quantum devices used for encoding the channel inputs and decoding its outputs. This is equivalent to considering communication with only a fixed number of channel uses.

In this work, following the footsteps of recent progress in classical information theory[8–11], we investigate how well one can transmit quantum information in a realistic scenario where the number of channel uses is limited. The quantum capacity is at most a proxy for the answer to this question, and we show with concrete examples that it is often not a very good one. For example, we find that in the order of a 1,000 qubits are required to get within 90% of the quantum capacity of a typical qubit dephasing channel. To overcome this issue, we develop a more precise approximate characterization of the performance of optimal coding schemes that takes into account finite size effects. We find that these effects are succinctly described by a second channel parameter (besides its capacity), which we name quantum channel dispersion. As such, our work generalizes recent progress in the study of cc over quantum channels[12,13].

Results

Model for quantum communication. In this work, we focus on codes enabling a state entangled with a reference system to be reliably transmitted through the channel. This is a strong requirement: reliable entanglement transmission implies reliable transmission, on average, of all pure input states. The coding scheme is depicted in Fig. 1. We are given a quantum channel $\mathcal{N} \equiv \mathcal{N}_{A\to B}$ and denote by $\mathcal{N}^{\otimes n}$ the n-fold parallel repetition of this channel. An entanglement-transmission code for $\mathcal{N}^{\otimes n}$ is given by a triplet $\{|M|, \mathcal{E}, \mathcal{D}\}$, where $|M|$ is the local dimension of a maximally entangled state $|\phi\rangle_{MM'}$ that is to be transmitted over $\mathcal{N}^{\otimes n}$. The quantum channels $\mathcal{E} \equiv \mathcal{E}_{M'\to A^n}$ and $\mathcal{D} \equiv \mathcal{D}_{B^n\to M''}$ are encoding and decoding operations, respectively. With this in hand, we now say that a triplet $\{R, n, \varepsilon\}$ is achievable on the channel $\mathcal{N}$ if there exists an entanglement-transmission code satisfying

$$\tfrac{1}{n}\log|M| \geq R \quad \text{and} \quad F\big(\phi_{MM''}, (\mathcal{D}\circ\mathcal{N}^{\otimes n}\circ\mathcal{E})(\phi_{MM'})\big) \geq 1-\varepsilon. \qquad (1)$$

Here R is the rate of the code, n is the number of channel uses and ε is the tolerated error or infidelity, measured in terms of Uhlmann's fidelity[14], $F(\rho,\sigma) := \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$.

The non-asymptotic achievable region of a quantum channel $\mathcal{N}$ is then given by the union of all achievable triplets $\{R, n, \varepsilon\}$. The goal of (non-asymptotic) information theory is to find tight bounds on this achievable region, in particular to determine if certain triplets are outside the achievable region and thus forbidden. For this purpose, we define its boundary

$$\hat{R}_{\mathcal{N}}(n;\varepsilon) := \max\{R : (R,n,\varepsilon)\text{is achievable on}\,\mathcal{N}\}, \qquad (2)$$

and investigate it as a function of n for a fixed value of ε. We will often drop the subscript $\mathcal{N}$ if it is clear which channel is considered. An alternative approach would be to investigate the boundary $\hat{\varepsilon}_{\mathcal{N}}(n;R) := \min\{\varepsilon : (R,n,\varepsilon)\,\text{is achievable}\}$, as in ref. 15. This leads to the study of error exponents (and the reliability function), as well as strong converse exponents. We will not discuss this here since such an analysis usually does not yield good approximations for small values of n.

To begin, let us rephrase the seminal capacity results in this language. The quantum capacity is defined as the asymptotic limit of $\hat{R}_{\mathcal{N}}(n;\varepsilon)$ when n (first) goes to infinity and ε vanishes. The capacity can be expressed in terms of a regularized coherent information[2,3,5–7,16]:

$$Q(\mathcal{N}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty}\hat{R}_{\mathcal{N}}(n;\varepsilon) = \sup_{\ell\in\mathbb{N}}\frac{I_c\left(\mathcal{N}^{\otimes\ell}\right)}{\ell} \geq I_c(\mathcal{N}), \qquad (3)$$

where the coherent information I_c is an entropic functional defined in Methods. This result is highly unsatisfactory, not least because the regularization makes its computation intractable. (The supremum in equation (3) is necessary in the following sense: there does not exist a universal constant ℓ_0 such that

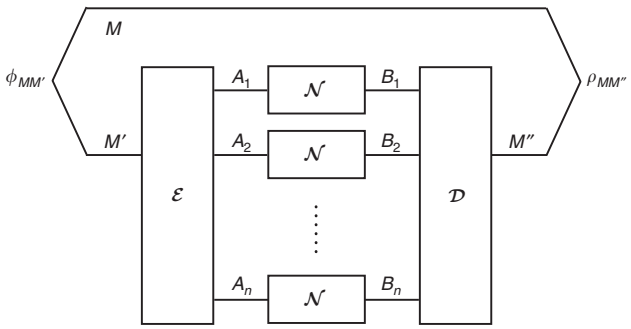

Figure 1 | Coding scheme for entanglement transmission. Coding scheme for entanglement transmission over n uses of a channel $\mathcal{N} \equiv \mathcal{N}_{A\to B}$. The systems M, M' and M'' are isomorphic. The encoder $\mathcal{E} \equiv \mathcal{E}_{M'\to A^n}$ encodes the part M' of the maximally entangled state $\phi_{MM'}$ into the channel input systems. Later, the decoder $\mathcal{D} \equiv \mathcal{D}_{B^n\to M''}$ recovers the state from the channel output systems. The performance of the code is measured using the fidelity $F(\phi_{MM''}, \rho_{MM''})$.

$Q(\mathcal{N}) \leq \frac{1}{\ell_0} I_c(\mathcal{N}^{\otimes \ell_0})$ for all channels $\mathcal{N}$[17].) Worse, the statement is not as strong as we would like it to be because it does not give any indication of the fundamental limits for finite ε or finite n.

For example, even sticking to the asymptotic limit for now, we might be willing to admit a small but nonzero error in our recovery. Formally, instead of requiring that the error vanishes asymptotically, we only require that it does not exceed a certain threshold, ε. Can we then achieve a higher asymptotic rate in the above sense? For cc this is ruled out by Wolfowitz's strong converse theorem[18]. However, surprisingly, the answer to this question is not known for general quantum channels. Recent work[19] at least settles the question in the negative for a class of generalized dephasing channels and in particular for the qubit dephasing channel

$$\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\rho + \gamma Z\rho Z, \tag{4}$$

where $\gamma \in [0, 1]$ is a parameter and Z is the Pauli Z operator. Dephasing channels are particularly interesting examples because dephasing noise is dominant in many physical implementations of qubits. The results of ref. 19 thus allow us to fully characterize the achievable region in the limit $n \to \infty$ for such channels, and in particular ensure that

$$\lim_{n\to\infty} \hat{R}_{\mathcal{Z}_\gamma}(n;\varepsilon) = I_c(\mathcal{Z}_\gamma), \tag{5}$$

independent of the value of $\varepsilon \in (0, 1)$. Note also that the regularization is not required here since dephasing channels are degradable[20].

Here we go beyond studying the problem in the asymptotic limit and develop characterizations of the achievable region for finite values of n. We find inner (achievability) and outer (converse) bounds on the boundary of the achievable region. We first discuss these bounds for three important example channels, the qubit dephasing, erasure and depolarizing channel, and then present bounds for general channels.

Qubit dephasing channel. We show that the non-asymptotic achievable region of the qubit dephasing channel is equivalent to the corresponding region of a (classical) binary symmetric channel. This allows us to employ results from classical information theory[10,21,22] to establish the following characterization of the achievable region for the qubit dephasing channel.

Theorem 1. For the qubit dephasing channel $\mathcal{Z}_\gamma$ with $\gamma \in [0, 1]$, the boundary $\hat{R}(n;\varepsilon)$ satisfies

$$\hat{R}(n;\varepsilon) = 1 - h(\gamma) + \sqrt{\frac{v(\gamma)}{n}}\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right), \tag{6}$$

where Φ is the cumulative normal distribution function, Φ^{-1} its inverse, $h(\cdot)$ denotes the binary entropy, and $v(\cdot)$ the corresponding variance, $v(\gamma) := \gamma(\log\gamma + h(\gamma))^2 + (1-\gamma)(\log(1-\gamma) + h(\gamma))^2$.

The expression without the remainder term $O(\frac{1}{n})$ is called the third order approximation of the (boundary of the) non-asymptotic achievable region. The quantity $v(\gamma)$ is the quantum channel dispersion and characterizes the finite size effects for quantum communication over the qubit dephasing channel. The approximation is visualized in Fig. 2 for an example channel with $\gamma = 0.1$. In Fig. 2a, we plot the smallest achievable error ε as a function of the rate R. Here we use the second order expansion without the term $\frac{1}{2n}\log n$ since it can conveniently be solved for ε. In the limit $n \to \infty$, we see an instantaneous transition of ε from 0 to 1, the signature of a strong converse: coding below the capacity $Q(\mathcal{Z}_\gamma) = 1 - h(\gamma)$ is possible with perfect fidelity, whereas coding above the capacity will necessarily result in a vanishing fidelity.

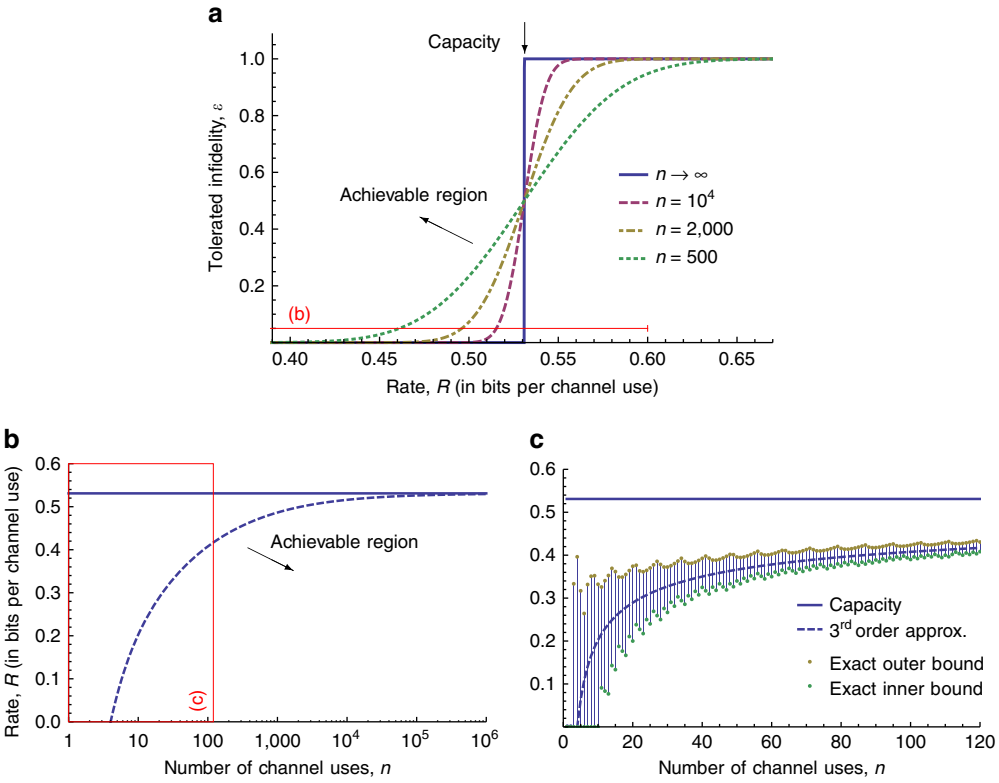

Figure 2 | Example 1—qubit dephasing channel. Approximation of the non-asymptotic achievable rate region of a qubit dephasing channel with $\gamma = 0.1$ (see Theorem 1). All numerical results are evaluated using the binary logarithm, that is, $\log \equiv \log_2$. (**a**) Boundary of the achievable region for fixed n with different values (second order approximation). (**b**) Boundary of the achievable region for fixed infidelity $\varepsilon = 5\%$ (third order approximation) in equation (6). (**c**) Comparison of strict bounds with third order approximation for fixed $\varepsilon = 5\%$.

In Fig. 2b, we plot the third order approximation in equation (6) for the highest achievable rate, $\hat{R}(n;\varepsilon)$, as a function of n for a fixed fidelity of 95% (that is, we set $\varepsilon = 5\%$). For example, this allows us to calculate how many times we need to use the channel to approximately achieve the quantum capacity. The third order approximation shows that we need ~ 850 channel uses to achieve 90% of the quantum capacity. Note that a coding scheme achieving this would probably require us to coherently manipulate 850 qubits in the decoder, which appears to be a quite challenging task. This example shows that the capacity does not suffice to characterize the ability of a quantum channel to transmit information, and further motivates the study of the achievable region for finite n.

Finally, we remark that the third order approximation is quite strong even for small n. To prove this, we compare it to exact upper and lower bounds on $\hat{R}(n;\varepsilon)$ in Fig. 2c and see that the remainder term $O(\frac{1}{n})$ becomes negligible for fairly small $n \approx 100$ for the present values of γ and ε.

Qubit erasure channel. Another channel we can analyse in this manner is the qubit erasure channel, given by the map

$$\mathcal{E}_\beta : \rho \mapsto (1-\beta)\rho + \beta|e\rangle\langle e|, \tag{7}$$

where $\beta \in [0, 1]$ is the probability of erasure and $|e\rangle\langle e|$ is a pure state orthogonal to ρ that indicates erasure. Here we investigate coding schemes that allow free cc assistance between the sender and receiver in both directions, in parallel to the quantum transmission. This setting is quite natural because we can often assume that cc is considerably easier to implement than quantum communication (see Fig. 5 in Methods for a description of such codes). We denote the corresponding boundary of the achievable region by $\hat{R}^{cc}(n;\varepsilon)$. Since this includes all codes that do not take advantage of cc, we clearly have $\hat{R}(n;\varepsilon) \leq \hat{R}^{cc}(n;\varepsilon)$ for all channels. This inequality is strict for the erasure channel but for the dephasing channel we find that the asymptotic expansion in equation (6) holds for both $\hat{R}(n;\varepsilon)$ and $\hat{R}^{cc}(n;\varepsilon)$, that is, cc assistance does not help asymptotically (up to third order).

For the qubit erasure channel, we can determine the boundary $\hat{R}^{cc}(n;\varepsilon)$ exactly, again by generalizing[19] and relating the problem to that of the classical erasure channel.

Theorem 2. For the qubit erasure channel $\mathcal{E}_\beta$ with $\beta \in [0, 1]$, the boundary $\hat{R}^{cc}(n;\varepsilon)$ satisfies

$$\varepsilon = \sum_{l=n-k+1}^{n} \binom{n}{l} \beta^l (1-\beta)^{n-l} \left(1 - 2^{n\left(1-\hat{R}^{cc}(n;\varepsilon)\right)-l}\right). \tag{8}$$

Moreover, for large n, we have the expansion

$$\hat{R}^{cc}(n;\varepsilon) = 1 - \beta + \sqrt{\frac{\beta(1-\beta)}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{1}{n}\right). \tag{9}$$

The latter expression is a third order approximation of the achievable region, where $1-\beta$ is the quantum capacity and $\beta(1-\beta)$ is the quantum channel dispersion of the qubit erasure channel. In Fig. 3, we show this approximation for a qubit erasure channel with $\beta = 0.25$ and fidelity 99%. In Fig. 3a, we see that the non-asymptotic achievable region reaches 90% of the channel capacity for $n \approx 180$. Again, this confirms that the non-asymptotic treatment is crucial in the quantum setting. In Fig. 3b, we compare the third order approximation with the exact boundary of the achievable region in equation (8). We see that the approximation is already very precise (and the term $O(\frac{1}{n})$ thus negligible) for fairly small $n \approx 50$.

Qubit depolarizing channel. Another prominent channel is the qubit depolarizing channel. It is given by the map

$$\mathcal{D}_\alpha : \rho \mapsto (1-\alpha)\rho + \frac{\alpha}{3}(X\rho X + Y\rho Y + Z\rho Z), \tag{10}$$

where $\alpha \in [0, 1]$ is a parameter and X, Y, Z are the Pauli operators. For this channel, no closed formula for the quantum capacity $Q(\mathcal{D}_\alpha)$ is known, and the coherent information

$$I_c(\mathcal{D}_\alpha) = 1 - h(\alpha) - \alpha\log 3 \tag{11}$$

is only a strict lower bound on it[23]. However, various upper bounds on the quantum capacity of the qubit depolarizing channel have been established[24–28]. For example, in (ref. 24, Theorem 2) it is essentially shown that $Q(\mathcal{D}_\alpha) \leq Q(\mathcal{Z}_\alpha) = 1 - h(\alpha)$, the quantum capacity of the qubit dephasing channel with dephasing parameter α. Here we extend this result to the non-asymptotic setting and find the following outer (converse) bound for the achievable rate region that holds even with cc assistance.

Theorem 3. For the qubit depolarizing channel $\mathcal{D}_\alpha$ with $\alpha \in [0, 1]$, the boundary $\hat{R}^{cc}(n;\varepsilon)$ satisfies

$$\hat{R}^{cc}(n;\varepsilon) \leq 1 - h(\alpha) + \sqrt{\frac{v(\alpha)}{n}}\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right), \tag{12}$$

where the right-hand side is simply the asymptotic expansion of the boundary of the achievable rate region for the qubit dephasing channel $\mathcal{Z}_\alpha$ with dephasing parameter α as in Theorem 1.

In Fig. 4a, we plot the second order approximation of the outer bound for a depolarizing channel with $\alpha = 0.05$ and 99% fidelity.

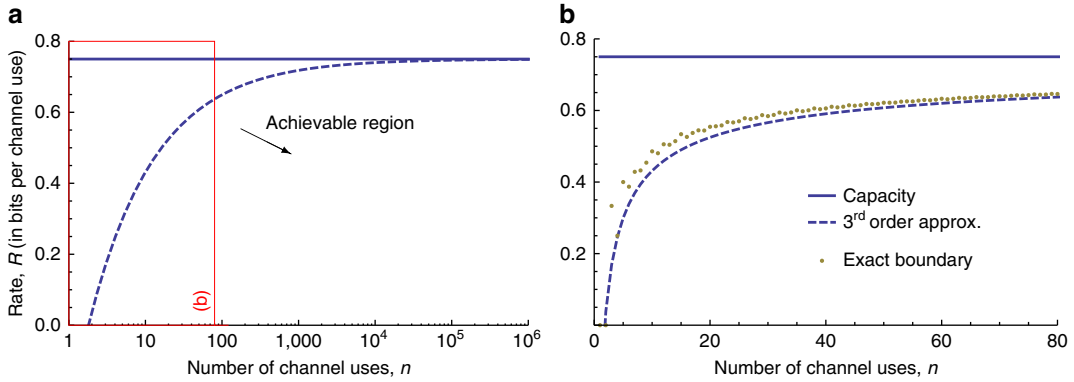

Figure 3 | Example 2—qubit erasure channel. Approximation of the non-asymptotic achievable rate region with classical communication assistance of a qubit erasure channel with $\beta = 0.25$ and fixed infidelity $\varepsilon = 1\%$ (see Theorem 2). (**a**) Boundary of the achievable region. (**b**) Comparison of exact bounds with third order approximation for small values of n.

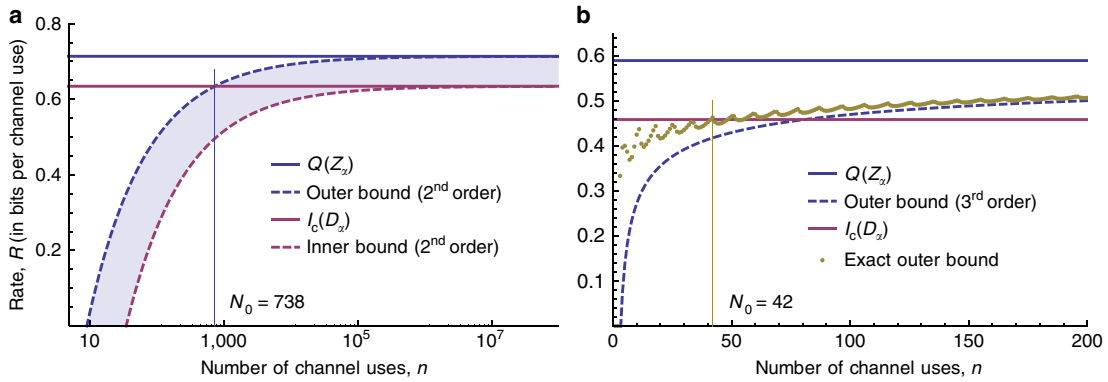

Figure 4 | Example 3—qubit depolarizing channel. Approximate inner and outer bounds on the non-asymptotic achievable rate region for the depolarizing channel (see Theorems 3 and 5) for fixed tolerated infidelity ε. The outer bounds apply to codes with classical communication assistance, whereas the inner bounds consider only unassisted codes. (**a**) Inner and outer bounds for $\alpha = 0.05$ and $\varepsilon = 1\%$. (**b**) Exact outer bound for $\alpha = 0.0825$ and $\varepsilon = 5.5\%$.

We see that to implement a code with a communication rate that exceeds the coherent information equation (3), we will need a quantum device that can process at least $N_0 = 738$ qubits coherently. Moreover, this statement remains true even if we allow for codes with cc assistance. This indicates that the question of whether the coherent information is a good or bad lower bound on the asymptotic quantum capacity is not of immediate practical relevance as long as we do not have a quantum computer that is able to perform a decoding operation on many hundreds of qubits.

In Fig. 4b, we examine a qubit depolarizing channel with parameters $\alpha = 0.0825$ and $\varepsilon = 5.5\%$. Instead of using an approximation for the outer bound, we use the exact outer bound to give the answer (it is 42) to the question of how many channel uses we need at minimum to exceed the coherent information. However, note that this does not give us any indication of what code (in particular if it is assisted or not), if any, can achieve this point.

General outer and inner bounds. We have so far focused our attention on three specific (albeit very important) examples of channels. However, many of the results derived in this article also hold more generally. For example, we find the following outer (converse) bound.

Theorem 4. For any quantum channel $\mathcal{N}$, the boundary $\hat{R}(n;\varepsilon)$ satisfies

$$\hat{R}(n;\varepsilon) \leq -\log f\left(\mathcal{N}^{\otimes n},\varepsilon\right), \tag{13}$$

where $f(\mathcal{N},\varepsilon)$ is the solution to a semidefinite optimization programme defined in equation 24 and Methods. Moreover, if $\mathcal{N}$ is covariant, we find the asymptotic expansion

$$\hat{R}^{\mathrm{cc}}(n;\varepsilon) \leq \hat{R}^{\mathrm{cc}}_{\mathrm{outer}}(n;\varepsilon), \quad \text{with}$$
$$\hat{R}^{\mathrm{cc}}_{\mathrm{outer}}(n;\varepsilon) = I_{\mathrm{R}}(\mathcal{N}) + \sqrt{\frac{V^{\varepsilon}_{\mathrm{R}}(\mathcal{N})}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right), \tag{14}$$

where the Rains information, $I_{\mathrm{R}}(\mathcal{N})$, and its variance, $V^{\varepsilon}_{\mathrm{R}}(\mathcal{N})$, are entropic functionals defined in equation (28) and equation (29) and Methods.

In fact, the bound in equation (13) holds also for codes that allow classical post-processing (cpp), as discussed in the Supplementary Notes. Covariant channels are discussed in Methods, and include the dephasing, erasure and depolarizing channels treated above. The semidefinite optimization programme $f(\mathcal{N},\varepsilon)$ is similar in spirit to the metaconverse for classical coding[10,29,30]. For quantum coding, alternative semidefinite optimization programme lower bounds on the error boundary $\hat{\varepsilon}_{\mathcal{N}}(n;R) := \max\{\varepsilon : (R,n,\varepsilon)\text{is achievable}\}$ for fixed rate R have been derived in ref. 15. Note that our bound equation (14) is tight up to the second order asymptotically for the qubit dephasing channel (Theorem 1) and the erasure channel with cc assistance (Theorem 2). However, in the generic covariant case the bound is not expected to be tight. Moreover, if the channel is not covariant we cannot asymptotically expand our outer bounds on the achievable rate region in a closed form as above.

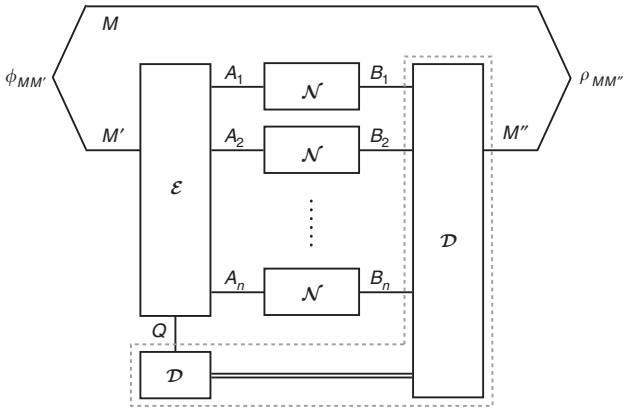

Figure 5 | Coding scheme for entanglement transmission with classical post-processing. Coding scheme for entanglement transmission over n uses of a channel $\mathcal{N}_{A\to B}$ with classical post-processing. The encoder $\mathcal{E} \equiv \mathcal{E}_{M'\to A^nQ}$ encodes M' into the channel input systems and a local memory Q. Later, the decoder $\mathcal{D} \equiv \mathcal{D}_{QB^n\to M''}$ recovers the maximally entangled state from the channel output systems and the memory Q using classical communication and local operations. The performance of the code is measured using the fidelity $F(\phi_{MM'},\rho_{MM''})$.

Finally, an inner (achievability) bound of the form shown in Theorem 1 also holds generally for all quantum channels.

Theorem 5. For any quantum channel $\mathcal{N}$, the boundary $\hat{R}(n;\varepsilon)$ satisfies

$$\hat{R}(n;\varepsilon) \geq R_{\mathrm{inner}}(n;\varepsilon), \quad \text{with}$$
$$\hat{R}_{\mathrm{inner}}(n;\varepsilon) = I_{\mathrm{c}}(\mathcal{N}) + \sqrt{\frac{V^{\varepsilon}_{\mathrm{c}}(\mathcal{N})}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right), \tag{15}$$

where the coherent information, $I_{\mathrm{c}}(\mathcal{N})$, and its variance, $V^{\varepsilon}_{\mathrm{c}}(\mathcal{N})$, are entropic functionals defined in equation 35 and equation 36 and Methods.

Note that the bound equation (15) is tight up to the second order asymptotically for the qubit dephasing channel (Theorem 1). For the erasure channel, this bound does not match the outer bound since it does not take into account cc assistance. For general channels, the bound does not tightly characterize the achievable region. In particular, for $n\to\infty$, it converges to the coherent information and not the regularized coherent information, which can be strictly larger[23]. However, we have reasons to conjecture that the bound is tight for degradable channels[20,31].

The same inner bound has been shown independently and concurrently in ref. 32 using a different decoder.

Discussion

The main contributions of this work can be summarized as follows. We showed—both analytically and quantitatively—that the quantum channel capacity is insufficient to characterize achievable communication rates in the finite resource setting. We provided a remedy, showing that the capacity and quantum channel dispersion together provide a very good characterization, in particular for the practically relevant qubit dephasing, depolarization and erasure channels. This is crucial for practical considerations where one would like to rely on a simple and easy to evaluate formula to estimate the achievable rate region. For instance, one can use the estimated optimal rate region to benchmark explicit codes, for example, in designing a quantum repeater.

More precisely, for general channels, we gave inner (achievability) and outer (converse) bounds on the boundary of the achievable region for quantum communication with finite resources (*cf.,* Theorems 5 and 4). These bounds can be formulated as semidefinite programmes and thus evaluated for small instances. For larger instances, we show that the bounds admit a second order approximation featuring the dispersion (for the converse bound this requires the assumption of channel covariance) which can be evaluated efficiently. We then showed that the inner and outer bounds agree for the qubit dephasing channel (*cf.,* Fig. 2) and qubit erasure channel with cc assistance (*cf.,* Fig. 3) up to the third order asymptotically. For the qubit depolarizing channel (*cf.,* Fig. 4), we gave separate second order approximations for the inner and outer bounds. Closing the gap between these bounds (see shaded area in Fig. 4a), even asymptotically, remains one of the most tantalizing open questions in quantum information theory[26].

For general channels, many questions remain open. For example, we would like to understand if the inner bound in Theorem 5 characterizes the achievable region for all degradable channels[20] (*cf.,* the open questions in ref. 19). Also it would be interesting to explore higher order refinements for channels with zero quantum capacity (for example, for the erasure channel with $\beta\geq 1/2$ and no assistance). This might lead to a better understanding of superactivation of the quantum capacity[33]. Taking a broader view, convex relaxation, such as our semidefinite programme, provides a promising approach to better understand the rate region beyond studying entropic properties. For practical applications, the most important channel not addressed here is the qubit amplitude damping channel, and it is an important open question to analyse it in the finite resource regime.

Finally, we note that our analysis can be extended to the case of entanglement-assisted quantum communication. A short exhibition of this extension is provided in Supplementary Note 1.

Methods

General notation and codes. Here we sketch the main ideas of the proofs of Theorems 4 and 5, and a more detailed exposition is given in Supplementary Note 2. A detailed analysis of the example channels in Theorems 1–3 can be found in Supplementary Note 3.

We denote finite-dimensional Hilbert spaces corresponding to individual quantum systems by capital letters. In particular, we use A and B to model the channel input and output space, respevtively, whereas M and the isomorphic spaces M' and M'' are used to model the quantum systems containing the maximally entangled state to be transmitted. We also use A^n to denote the n-fold tensor product of A for any $n\in\mathbb{N}$. We use $\mathcal{P}(A)$ to denote the set of positive semidefinite operators on A, and $\mathcal{S}(A):=\{\rho_A\in\mathcal{P}(A)\colon \mathrm{tr}(\rho_A)=1\}$ to denote quantum states with unit trace on A. We denote the dimension of A by $|A|$. Pure states are of the form $\rho_A=|\phi\rangle\langle\phi|$, where $|\phi\rangle$ is a vector in A and $\langle\phi|$ its dual functional. The marginals of a bipartite quantum state $\rho_{AB}\in\mathcal{S}(AB)$ on A and B are denoted by ρ_A and ρ_B, respectively. A quantum channel $\mathcal{N}_{A\to B}$ is a completely positive trace-preserving map from states on A to states on B. For any state ρ_A, we define the canonical purification $|\psi^\rho\rangle_{AA'}:=|A|\sqrt{\rho_A}\otimes 1_{A'}|\phi\rangle_{AA'}$, where A' is isomorphic to A and $\phi_{AA'}$ is the maximally entangled state. To express our results, we use Umegaki's quantum relative entropy[34], $D(\rho\|\sigma):=\mathrm{tr}[\rho(\log\rho-\log\sigma)]$ and the quantum relative entropy variance[35,36], $V(\rho\|\sigma):=\mathrm{tr}\left[\rho(\log\rho-\log\sigma-D(\rho\|\sigma))^2\right]$. The coherent information and the coherent information variance[35] of a bipartite state ρ_{AB} are given as

$$I(A\rangle B)_\rho:=D(\rho_{AB}\|1_A\otimes\rho_B)\quad\text{and}\quad V(A\rangle B)_\rho:=V(\rho_{AB}\|1_A\otimes\rho_B). \tag{16}$$

We have defined unassisted entanglement-transmission codes in Results. Let us reintroduce them in the context of codes assisted by cpp. For this, we consider any quantum channel $\mathcal{N}\equiv\mathcal{N}_{A\to B}$ and its n-fold extension $\mathcal{N}^{\otimes n}$ that maps states on A^n to states on B^n. An entanglement-transmission code assisted by cpp for $\mathcal{N}^{\otimes n}$ is given by a triplet $\{|M|,\mathcal{E},\mathcal{D}\}$, as depicted in Fig. 5. Here $|M|$ is the local dimension of a maximally entangled state $|\phi\rangle_{MM'}$ that is to be transmitted over $\mathcal{N}^{\otimes n}$. The encoder $\mathcal{E}_{M'\to A^nQ}$ is a completely positive trace-preserving map that prepares the channel inputs $A_1, A_2, \ldots A_n$ and a local memory system, which we denote by Q. The decoder $\mathcal{D}_{QB^n\to M''}$ is a completely positive trace-preserving map that is restricted to local operations and cc with regard to the bipartition $Q{:}B^n$ and outputs M'' on the receiver's side.

The boundary of the achievable rate region for these codes is denoted by $\hat{R}^{\mathrm{cpp}}_{\mathcal{N}}(n,\varepsilon)$. Finally, we note that unassisted codes are recovered if we choose Q to be trivial. Hence, unassisted codes are contained in the set of assisted codes and we have $\hat{R}(n,\varepsilon)\leq\hat{R}^{\mathrm{cpp}}(n,\varepsilon)$. Moreover, for covariant channels we will see later that $\hat{R}^{\mathrm{cpp}}(n,\varepsilon){=}\hat{R}^{\mathrm{cc}}(n,\varepsilon)$ since all cc can be postponed to after the quantum communication. Hence, while we will in the following derive our converse bounds for $\hat{R}^{\mathrm{cpp}}(n,\varepsilon)$, they are also valid for $\hat{R}^{\mathrm{cc}}(n,\varepsilon)$ when the channel is covariant.

Outer bounds on the achievable rate region. Our converse results are inspired by the strong converse results for generalized dephasing channels and the meta-converse for classical channel coding[10]. They are expressed in terms of the channel hypothesis testing Rains relative entropy, which is defined following the generalized divergence framework discussed in ref. 19. First, let us introduce the Rains set[25,37], which is a superset of the set of positive partial transpose (PPT) states. It is defined as $\mathrm{PPT}^*(A{:}B):=\left\{\tau_{AB}\in\mathcal{P}(AB)\middle|\|\mathcal{T}_B(\tau_{AB})\|_1\leq 1\right\}$, where $\mathcal{T}_B$ denotes the partial transpose map on B. We have the following crucial inequality (ref. 38, Lemma 2): for every $\sigma_{AB}\in\mathrm{PPT}^*(A{:}B)$, we have

$$\langle\phi|\sigma_{AB}|\phi\rangle_{AB}\leq\frac{1}{|M|} \tag{17}$$

for all maximally entangled states ϕ_{AB} of local dimension $|M|$. The set is closed under local quantum operations on A and B supported by cc between A and B. Finally, we employ the hypothesis testing relative entropy[39], (in the form of ref. 40)

$$D^\varepsilon_H(\rho\|\sigma):=-\log\min\{\mathrm{tr}[\Lambda\sigma]|0\leq\Lambda\leq 1\wedge\mathrm{tr}[\Lambda\rho]\geq 1-\varepsilon\}. \tag{18}$$

We first formulate a general metaconverse bounding possible rates R given a tolerated infidelity ε for a single use ($n=1$) of a fixed channel $\mathcal{N}\equiv\mathcal{N}_{A\to B}$. For this purpose, consider any state $\rho_{MM''}=\mathcal{D}\circ\mathcal{N}\circ\mathcal{E}(\phi_{MM'})$ at the output of a code achieving fidelity $1-\varepsilon$ and any state $\sigma_{MM''}\in\mathrm{PPT}^*(M{:}M'')$. These must satisfy, according to equation (17),

$$\mathrm{tr}[\sigma_{MM'}\phi_{MM'}]\leq\frac{1}{|M|}\quad\text{and}\quad\mathrm{tr}[\rho_{MM'}\phi_{MM'}]\geq 1-\varepsilon. \tag{19}$$

From this, we can conclude that $D^\varepsilon_H(\rho_{MM'}\|\sigma_{MM'})\geq\log|M|$ by using the projection $\Lambda=\phi_{MM'}$ as our hypothesis test in equation (18). At this stage, we can use the data-processing inequality of the hypothesis testing divergence[40] to remove the decoder from the picture. Minimizing over all auxiliary states $\sigma_{MQB}\in\mathrm{PPT}^*(MQ{:}B)$, this yields

$$\min_{\sigma_{MQB}}D^\varepsilon_H\left(\mathcal{N}_{A\to B}(\rho_{MQA})\|\sigma_{MQB}\right)\geq\log|M|,\quad\text{where}\quad\rho_{MQA}=\mathcal{E}(\phi_{MM'}). \tag{20}$$

Crucially, we rely on the fact that $\mathrm{PPT}^*(MQ{:}B)$ gets mapped into $\mathrm{PPT}^*(M{:}M'')$ by the action of the decoder. Now we observe that by choosing the register Q sufficiently large, we can assume that the encoder is an isometry without loss of generality. Hence, for a fixed marginal $\rho_A=\mathrm{tr}_{QM}(\rho_{MQA})$, we can rewrite the above inequality using the substitutions $A\to A'$ and $MQ\to A$ as

$$\min_{\sigma_{AB}\in\mathrm{PPT}^*(A:B)}D^\varepsilon_H\left(\mathcal{N}_{A'\to B}\left(\psi^\rho_{AA'}\right)\|\sigma_{AB}\right)\geq\log|M|. \tag{21}$$

Optimized over all codes (and thus marginals ρ_A), we find that

$$\hat{R}^{\mathrm{cpp}}(1;\varepsilon) \leq I_{\mathrm{R}}^{\varepsilon}(\mathcal{N}) \tag{22}$$

with the channel hypothesis testing Rains relative entropy defined as

$$I_{\mathrm{R}}^{\varepsilon}(\mathcal{N}) := \max_{\rho_A \in \mathcal{S}(A)} \min_{\sigma_{AB} \in \mathrm{PPT}'(A:B)} D_H^{\varepsilon}\left(\mathcal{N}_{A'\to B}\left(\psi_{AA'}^{\rho}\right) \| \sigma_{AB}\right). \tag{23}$$

Note that this outer bound also holds for coding schemes with (unphysical) PPT assistance including classical pre- and post-processing assistance (see ref. 15 for a more comprehensive discussion of PPT assisted codes). The bound can be further relaxed to $\hat{R}^{\mathrm{cpp}}(1;\varepsilon) \leq -\log f(\mathcal{N},\varepsilon)$, where $f(\mathcal{N},\varepsilon)$ is a semidefinite programme given below. This semidefinite optimization is discussed in more detail in Supplementary Note 4.

$$\begin{array}{rcll} f(\mathcal{N},\varepsilon) & = & \text{minimum} & \mathrm{tr}[\xi_A] \\ & & \text{subject to} & \xi_A, \Theta_{AB}, \Lambda_{AB}, \rho_A \geq 0 \\ & & & \xi_A \otimes 1_B \geq \Lambda_{AB} + \mathcal{T}_A(\Theta_{AB}) \\ & & & \Lambda_{AB} \leq \rho_A \otimes 1_B \\ & & & |A|\mathrm{tr}[\Lambda_{AB}\mathcal{N}_{A'\to B}(\phi_{AA'})] \geq 1-\varepsilon \\ & & & \mathrm{tr}[\rho_A] = 1 \end{array} \tag{24}$$

Moreover, the bound in equation (22) has the useful property that channel symmetries can be used to simplify its form, as we will see next. Suppose G is a group represented by unitary operators U_g on A and V_g on B. A quantum channel $\mathcal{N}_{A\to B}$ is covariant with respect to this group (and its representations) when

$$V_g \mathcal{N}(\cdot) V_g^{\dagger} = \mathcal{N}\left(U_g \cdot U_g^{\dagger}\right), \quad \forall g \in G. \tag{25}$$

Now the main workhorse to simplify our outer bounds for channels with symmetries is (ref. 19, Proposition 2), which states that we may restrict the optimization in equation (23) to input states that are invariant under the rotations $U_g \cdot U_g^{\dagger}$ for any $g \in G$. For channels of the form $\mathcal{N}^{\otimes n}$ which are invariant under permutation of the input and output systems, this allows us to restrict attention to input states that are permutation invariant.

Moreover, we call a channel covariant if it is covariant with respect to a group which has a representation U_g on A that is a one-design, that is, the map $\sum_{g\in G} \frac{1}{|G|} U_g(\cdot)U_g^{\dagger}$ always outputs the fully mixed state. In this case, the channel input state can be chosen to be fully mixed (respectively its purification is maximally entangled). Moreover, any such group allows for a corresponding teleportation protocol[41] (see the construction in ref. 42), and thus all interactive cc can be postponed until after the quantum communication is completed by the argument given in refs 43,44. From this, we can conclude that $\hat{R}^{\mathrm{cpp}}(n,\varepsilon) = \hat{R}^{\mathrm{cc}}(n,\varepsilon)$ for all covariant channels.

Now let $\mathcal{N}$ be a covariant quantum channel and $\phi_{AA'}$ a maximally entangled state. Then, our bound in equation (22) applied to the channel $\mathcal{N}^{\otimes n}$ yields

$$\hat{R}^{\mathrm{cc}}(n,\varepsilon) = \hat{R}^{\mathrm{cpp}}(n;\varepsilon) \leq \min_{\sigma_{AB} \in \mathrm{PPT}'(A:B)} \frac{1}{n} D_H^{\varepsilon}\left(\mathcal{N}_{A'\to B}(\phi_{AA'})^{\otimes n} \| \sigma_{AB}^{\otimes n}\right), \tag{26}$$

where we voluntarily restricted the minimization to product states of the form $\sigma_{AB}^{\otimes n}$ for some $\sigma_{AB} \in \mathrm{PPT}'(A:B)$. Moreover, since these states have tensor power structure, the outer bound can be expanded using[35,36]

$$\frac{1}{n} D_H^{\varepsilon}(\rho^{\otimes n} \| \sigma^{\otimes n}) = D(\rho\|\sigma) + \sqrt{\frac{V(\rho\|\sigma)}{n}} \Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right). \tag{27}$$

This leads to the formal statement of Theorem 4.

Formal Theorem 4. Let $\mathcal{N} \equiv \mathcal{N}_{A\to B}$ be a covariant quantum channel and let $\phi_{AA'}$ be maximally entangled. We define the Rains information of $\mathcal{N}$ as

$$I_{\mathrm{R}}(\mathcal{N}) := \min_{\sigma_{AB} \in \mathrm{PPT}'(A:B)} D(\mathcal{N}_{A'\to B}(\phi_{AA'}) \| \sigma_{AB}), \tag{28}$$

where we let $\Pi \subset \mathrm{PPT}'(A:B)$ be the set of states that achieve the minimum. The variance of the channel Rains information is

$$V_{\mathrm{R}}^{\varepsilon}(\mathcal{N}) := \begin{cases} \max\limits_{\sigma_{AB}\in\Pi} V(\mathcal{N}_{A'\to B}(\phi_{AA'}) \| \sigma_{AB}) & \text{for} \quad \varepsilon < \frac{1}{2} \\ \min\limits_{\sigma_{AB}\in\Pi} V(\mathcal{N}_{A'\to B}(\phi_{AA'}) \| \sigma_{AB}) & \text{for} \quad \varepsilon \geq \frac{1}{2} \end{cases}. \tag{29}$$

For any fixed $\varepsilon \in (0,1)$, the achievable region with classsical communication assistance satisfies

$$\begin{aligned} &\hat{R}^{\mathrm{cc}}(n;\varepsilon) \leq \hat{R}^{\mathrm{cc}}_{\mathrm{outer}}(n;\varepsilon), \quad \text{with} \\ &\hat{R}^{\mathrm{cc}}_{\mathrm{outer}}(n;\varepsilon) = I_{\mathrm{R}}(\mathcal{N}) + \sqrt{\frac{V_{\mathrm{R}}^{\varepsilon}(\mathcal{N})}{n}} \Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right). \end{aligned} \tag{30}$$

Inner bounds on the achievable rate region. We use the decoupling approach[45–47], and in particular a one-shot bound[31] which is a tighter version of previous bounds[48–50]. To reproduce their result, we need the following additional notation. Sub-normalized quantum states are collected in the set $\mathcal{S}_{\bullet}(A) := \{\rho_A \in \mathcal{P}(A) : \mathrm{tr}(\rho_A) \leq 1\}$. The purified distance[51] ε-ball around $\rho \in \mathcal{S}(A)$ is then defined as $\mathcal{B}^{\varepsilon}(\rho_A) := \left\{\bar{\rho}_A \in \mathcal{S}_{\bullet}(A) \middle| F(\bar{\rho}_A, \rho_A) \geq (1-\varepsilon)^2\right\}$. Finally, for $\rho_{AB} \in \mathcal{S}(AB)$ and $\varepsilon \geq 0$ the smooth conditional min-entropy[51–53] is defined as

$$H_{\min}^{\varepsilon}(A|B)_{\rho} := \sup_{\bar{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} \sup_{\sigma_B \in \mathcal{S}(B)} \sup\left\{\lambda \in \mathbb{R} \middle| \bar{\rho}_{AB} \leq 2^{-\lambda} \cdot 1_A \otimes \sigma_B\right\}. \tag{31}$$

Let us now restate (Proposition 20 in ref. 31) expressed in terms of the non-asymptotic achievable region as introduced in the Results. Let $\mathcal{N}_{A\to B}$ be a quantum channel with complementary channel $\mathcal{N}^{\mathrm{c}}_{A\to E}$. Then $\{R, 1, \varepsilon\}$ is achievable if, for some $\eta \in (0, \varepsilon]$ and some state $\rho_A \in \mathcal{S}(A)$, we have

$$R \leq H_{\min}^{\sqrt{\varepsilon}-\eta}(A|E)_{\omega} - 4\log\frac{1}{\eta}, \tag{32}$$

where $\omega_{AE} = (\mathcal{I}_A \otimes \mathcal{N}^{\mathrm{c}}_{A'\to E})\left(\psi^{\rho}_{AA'}\right)$. This leads immediately to the following inner bound on the achievable region. Using $\omega_{A^nE^n} = (\mathcal{I}_{A^n} \otimes (\mathcal{N}^{\mathrm{c}}_{A'\to E})^{\otimes n})(\psi_{A^nA'^n})$, we have

$$\hat{R}(n;\varepsilon) \geq \sup_{\eta\in(0,\varepsilon)} \sup_{\rho_{A^n} \in \mathcal{S}(A^n)} \frac{1}{n}\left(H_{\min}^{\sqrt{\varepsilon}-\eta}(A^n|\mathrm{E}^n)_{\omega} - 4\log\frac{1}{\eta} - 1\right). \tag{33}$$

The problem with this bound is that it is generally hard to evaluate, even for moderately large values of n. Hence we are interested to further simplify the expression on the right-hand side in this regime. To do so, we choose $\eta = 1/\sqrt{n}$ and use input states of the form $\rho_A^{\otimes n}$. This yields the following relaxation, which holds if $n > \frac{1}{\varepsilon}$:

$$\hat{R}(n;\varepsilon) \geq \sup_{\rho_A \in \mathcal{S}(A)} \frac{1}{n}\left(H_{\min}^{\varepsilon_n}(A^n|E^n)_{\omega^{\otimes n}} - 2\log n - 1\right). \tag{34}$$

Here we introduced $\varepsilon_n = \sqrt{\varepsilon} - 1/\sqrt{n}$ and ω_{AE} as in equation (32). Using a second order expansion[35] similar to the one in equation (27), we give an asymptotic expansion of the expression on the right-hand side of equation (34). This yields Theorem 5.

Formal Theorem 5. Let $\mathcal{N} \equiv \mathcal{N}_{A\to B}$ be a quantum channel. We define its coherent information as

$$I_{\mathrm{c}}(\mathcal{N}) := \max_{\rho_A \in \mathcal{S}(A)} I(A\rangle B)_{\omega}, \quad \text{with} \quad \omega_{AB} = (\mathcal{I}_A \otimes \mathcal{N}_{A'\to B})\left(\psi^{\rho}_{AA'}\right) \tag{35}$$

and let $\Pi \subset \mathcal{S}(A)$ be the set of states that achieve the maximum. Define

$$V_{\mathrm{c}}^{\varepsilon}(\mathcal{N}) := \begin{cases} \min\limits_{\rho_A\in\Pi} V(A\rangle B)_{\omega} & \text{for} \quad \varepsilon < \frac{1}{2} \\ \max\limits_{\rho_A\in\Pi} V(A\rangle B)_{\omega} & \text{for} \quad \varepsilon \geq \frac{1}{2} \end{cases}. \tag{36}$$

Then, for any fixed $\varepsilon \in (0,1)$, the achievable region satisfies

$$\begin{aligned} &\hat{R}(n;\varepsilon) \geq \hat{R}_{\mathrm{inner}}(n;\varepsilon), \quad \text{with} \\ &\hat{R}_{\mathrm{inner}}(n;\varepsilon) = I_{\mathrm{c}}(\mathcal{N}) + \sqrt{\frac{V_{\mathrm{c}}^{\varepsilon}(\mathcal{N})}{n}} \Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right). \end{aligned} \tag{37}$$

References

1. Shannon, C. A mathematical theory of communication. *Bell Syst. Tech. J.* **27,** 379–423 (1948).
2. Barnum, H., Knill, E. & Nielsen, M. A. On quantum fidelities and channel capacities. *IEEE Trans. Inf. Theory* **46,** 1317–1329 (2000).
3. Barnum, H., Nielsen, M. A. & Schumacher, B. Information transmission through a noisy quantum channel. *Phys. Rev. A* **57,** 4153 (1998).
4. Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory* **51,** 44–55 (2005).
5. Lloyd, S. The capacity of the noisy quantum channel. *Phys. Rev. A* **55,** 1613–1622 (1996).
6. Schumacher, B. & Nielsen, M. A. Quantum data processing and error correction. *Phys. Rev. A* **54,** 2629 (1996).
7. Shor, P. W. *Lectures Notes, MSRI Workshop on Quantum Computation* (2002).
8. Strassen., V. in *Trans. Third Prague Conference on Information Theory* 689–723 (Prague, Czech Republic, 1962).
9. Hayashi, M. Information spectrum approach to second-order coding rate in channel coding. *IEEE Trans. Inf. Theory* **55,** 4947–4966 (2009).
10. Polyanskiy, Y., Poor, H. V. & Verdú, S. Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theory* **56,** 2307–2359 (2010).
11. Tan, V. Y. F. Asymptotic Estimates in Information Theory with Non-Vanishing Error Probabilities. *Found. Trends Commun. Inf. Theory* **11** (2014).
12. Tomamichel, M. & Tan, V. Y. F. Second-order asymptotics for the classical capacity of image-additive quantum channels. *Commun. Math. Phys.* **338,** 103–137 (2015).
13. Datta, N., Tomamichel, M. & Wilde., M. M. *On the second-order coding rates for entanglement-assisted communication*. Preprint at http://arxiv.org/abs/1405.1797 (2016).
14. Uhlmann., A. The transition probability for states of star-algebras. *Ann. Phys.* **497,** 524–532 (1985).
15. Leung, D. & Matthews, W. On the power of PPT-preserving and non-signalling codes. *IEEE Trans. Inf. Theory* **61,** 4486–4499 (2015).

16. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **461,** 207–235 (2005).
17. Cubitt, T. *et al.* Unbounded number of channel uses are required to see quantum capacity. *Nat. Commun.* **6,** 6739 (2015).
18. Wolfowitz, J. A note on the strong converse of the coding theorem for the general discrete finite-memory channel. *Inform. Control* **3,** 89–93 (1960).
19. Tomamichel, M., Wilde, M. M. & Winter, A. Strong converse rates for quantum communication. Preprint at http://arxiv.org/abs/1406.2946 (2014).
20. Devetak, I. & Shor, P. W. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun. Math. Phys.* **256,** 287–303 (2005).
21. Gallager, R. G. *Information Theory and Reliable Communication* (Wiley, 1968).
22. Poltyrev, G. Bounds on the decoding error probability of binary linear codes via their spectra. *IEEE Trans. Inf. Theory* **40,** 1284–1292 (1994).
23. DiVincenzo, D., Shor, P. & Smolin, J. Quantum-channel capacity of very noisy channels. *Phys. Rev. A* **57,** 830–839 (1998).
24. Rains, E. M. Entanglement purification via separable superoperators. Preprint at http://arxiv.org/abs/quant-ph/9707002 (1997).
25. Rains, E. M. A semidefinite program for distillable entanglement. *IEEE Trans. Inf. Theory* **47,** 2921–2933 (2001).
26. Smith, G. & Smolin, J. A. in *IEEE Information Theory Workshop Proceedings* 368–372 (2008).
27. Smith, G., Smolin, J. A. & Winter., A. The quantum capacity with symmetric side channels. *IEEE Trans. Inf. Theory* **54,** 4208–4217 (2008).
28. Sutter, D., Scholz, V. B. & Renner, R. Approximate degradable quantum channels. Preprint at http://arxiv.org/abs/1412.0980 (2014).
29. Matthews, W. A linear program for the finite block length converse of Polyanskiy-Poor-Verdú via nonsignaling codes. *IEEE Trans. Inf. Theory* **58,** 7036–7044 (2012).
30. Matthews, W. & Wehner, S. Finite blocklength converse bounds for quantum channels. *IEEE Trans. Inf. Theory* **60,** 7317–7329 (2014).
31. Morgan, C. & Winter, A. 'Pretty strong' converse for the quantum capacity of degradable channels. *IEEE Trans. Inf. Theory* **60,** 317–333 (2014).
32. Beigi, S., Datta, N. & Leditzky, F. Decoding quantum information via the petz recovery map. Preprint at http://arxiv.org/abs/1504.04449 (2015).
33. Smith, G. & Yard, J. T. Quantum communication with zero-capacity channels. *Science* **321,** 1812–1815 (2008).
34. Umegaki, H. Conditional expectation in an operator algebra. *Kodai Math. Sem. Rep.* **14,** 59–85 (1962).
35. Tomamichel, M. & Hayashi, M. A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Trans. Inf. Theory* **59,** 7693–7710 (2013).
36. Li, K. Second-order asymptotics for quantum hypothesis testing. *Ann. Stat.* **42,** 171–189 (2014).
37. Audenaert, K., De Moor, B., Vollbrecht, K. & Werner, R. F. Asymptotic relative entropy of entanglement for orthogonally invariant states. *Phys. Rev. A* **66,** 032310 (2002).
38. Rains, E. M. Bound on distillable entanglement. *Phys. Rev. A* **60,** 179–184 (1999).
39. Hiai, F. & Petz, D. The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.* **143,** 99–114 (1991).
40. Wang, L. & Renner, R. One-shot classical-quantum capacity and hypothesis testing. *Phys. Rev. Lett.* **108,** 200501 (2012).
41. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen Channels. *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
42. Werner, R. F. All teleportation and dense coding schemes. *J. Phys. A* **34,** 7081–7094 (2001).
43. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54,** 3824–3851 (1996).
44. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. The ultimate rate of quantum communications. Preprint at http://arxiv.org/abs/1510.08863 (2015).
45. Dupuis, F. *The Decoupling Approach to Quantum Information Theory.* PhD thesis, Univ. Montréal. Available at http://arxiv.org/abs/1004.1641 (2009).
46. Dupuis, F., Berta, M., Wullschleger, J. & Renner, R. One-shot decoupling. *Commun. Math. Phys.* **328,** 251–284 (2014).
47. Hayden, P., Horodecki, M., Yard, J. & Winter, A. A decoupling approach to the quantum capacity. *Open Syst. Inf. Dyn.* **15,** 7–19 (2008).
48. Berta., M. Single-Shot Quantum State Merging. Diploma thesis, ETH Zurich. Available at http://arxiv.org/abs/0912.4495 (2008).
49. Buscemi, F. & Datta, N. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Trans. Inf. Theory* **56,** 1447–1460 (2010).
50. Datta, N. & Hsieh, M.-H. The apex of the family tree of protocols: optimal rates and resource inequalities. *N. J. Phys.* **13,** 093042 (2011).
51. Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **56,** 4674–4681 (2010).
52. Renner., R. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich. Available at http://arxiv.org/abs/quant-ph/0512258 (2005).
53. Tomamichel, M. *Quantum Information Processing with Finite Resources—Mathematical Foundations,* Vol. 5 (Springer International Publishing, 2016).

Acknowledgements

We thank Chris Ferrie, Chris Granade, William Matthews, David Sutter and Mark Wilde for helpful discussions. M.T. is funded by an ARC Discovery Early Career Researcher Award Fellowship and acknowledges support from the ARC Centre of Excellence for Engineered Quantum Systems (EQUS). M.B. acknowledges funding provided by the Institute for Quantum Information and Matter. J.M.R. was supported by the Swiss National Science Foundation (through the National Centre of Competence in Research 'Quantum Science and Technology').

Author contributions

M.T., M.B. and J.R. developed the main ideas and technical results. M.T. wrote the manuscript with the help of M.B. and J.R.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Tomamichel, M. *et al.* Quantum coding with finite resources. *Nat. Commun.* 7:11419 doi: 10.1038/ncomms11419 (2016).

This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/