Finite blocklength converse bounds for quantum channels

William Matthews

Statistical Laboratory, Centre for Mathematical Sciences, Wilberforce Road, Cambridge, CB3 0WB England

Stephanie Wehner

Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore, 117543

We derive upper bounds on the rate of transmission of classical information over quantum channels by block codes with a given blocklength and error probability, for both entanglement-assisted and unassisted codes, in terms of a unifying framework of quantum hypothesis testing with restricted measurements. Our bounds do not depend on any special property of the channel (such as memorylessness) and generalise both a classical converse of Polyanskiy, Poor, and Verdú as well as a quantum converse of Renner and Wang, and have a number of desirable properties. In particular our bound on entanglement-assisted codes is a semidefinite program and for memoryless channels its large n limit is the well known formula for entanglement-assisted capacity due to Bennett, Shor, Smolin and Thapliyal.

This work is concerned with the transmission of classical information over quantum channels by means of block codes. This is a central subject of study in quantum information theory, and the asymptotic rates of transmission for various types of code and channel in the large blocklength limit are the subject of celebrated theorems and intriguing open problems.

A more fundamental problem, of both theoretical and practical interest, is to obtain upper (or *converse*) and lower (or *achievability*) bounds on the optimal transmission rate for a given error probability ϵ and *finite* blocklength n. This is the subject of a number of recent results in quantum information [1–3] and remains an active topic of research in classical information [4, 5]. As Figure 1 illustrates, finite blocklength effects are substantial.

Here we present converse results for both entanglement-assisted and unassisted codes, in terms of a quantum hypothesis testing problem with restricted measurements. This provides a unifying framework which generalises an important classical result of Polyanskiy, Poor and Verdú [4] and includes an existing quantum converse of Wang and Renner [2].

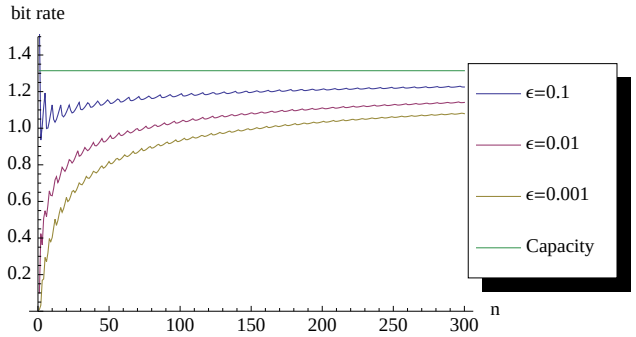

FIG. 1: Our upper bound (1) on the rate $R = (\log M_\epsilon^{\mathrm{E}}(\mathcal{E}^{\otimes n}))/n$ of entanglement-assisted codes of blocklength n and error probability $\epsilon = 0.01$, for the qubit depolarising channel $\mathcal{E}_{\mathrm{B|A}}[\rho_{\mathrm{A}}] = (1-p)\rho_{\mathrm{A}} + p(\mathbb{1}_{\mathrm{A}})/2$ with $p = 0.15$. The red line marks the capacity of the channel (roughly 1.31 bits/channel use) as given by the formula of Bennett, Shor, Smolin and Thapliyal [6].

Given a channel use (or uses) represented by a completely positive trace preserving (CPTP) map $\mathcal{E}_{\mathrm{B|A}}$ from states of a finite dimensional input system A to a finite dimensional output system B, we denote by $M_\epsilon^{\mathbf{C}}(\mathcal{E}_{\mathrm{B|A}}, \rho_{\mathrm{A}})$ the largest size of code in class $\mathbf{C}$ which, when the M messages are eqiprobable, has average input state ρ_{A} and error probability ϵ (see Figure 2). The largest size of any code in $\mathbf{C}$ with error probability ϵ is $M_\epsilon^{\mathbf{C}}(\mathcal{E}_{\mathrm{B|A}}) = \max_{\rho_{\mathrm{A}}} M_\epsilon^{\mathbf{C}}(\mathcal{E}_{\mathrm{B|A}}, \rho_{\mathrm{A}})$. If $\mathbf{C} = \mathrm{E}$ then the codes can be entanglement-assisted; if it is omitted, we only allow unassisted codes.

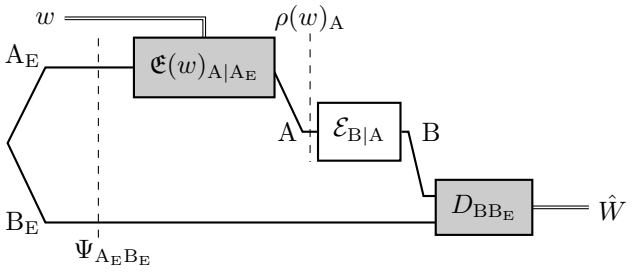

FIG. 2: In an **entanglement-assisted code** of block length of size M, the sender and receiver have systems $\mathrm{A_E}$ and $\mathrm{B_E}$ in an entangled state $\Psi_{\mathrm{A_E B_E}}$, and for each message $w \in [M]$ there is an encoding operation represented by the CPTP map $\mathfrak{E}(w)_{\mathrm{A|A_E}}$ from $\mathrm{A_E}$ to A. Following the use(s) of the channel, the decoder performs a POVM $D_{\mathrm{BB_E}}$ on $\mathrm{BB_E}$ to obtain the decoded message. An **unassisted code** can be viewed as a degenerate case where the decoding measurement operates only on the channel output B. Since $\mathrm{B_E}$ is completely ignored, there is no loss of generality if we take $\mathrm{B_E}$ and $\mathrm{A_E}$ to be trivial, one-dimensional systems. Then $\mathfrak{E}(w)$ is completely specified by its constant output $\rho(w)_{\mathrm{A}}$ on A. The average channel input induced by the encoding for equiprobable messages is $\rho_{\mathrm{A}} = \frac{1}{M}\sum_{w=1}^{M} \rho(w)_{\mathrm{A}}$.

In [4] Polyanskiy, Poor and Verdú showed that many existing *classical* converse results can be easily derived from a finite blocklength converse (heretofore, the 'PPV converse') which is obtained by a simple and conceptually appealing argument relating coding to hypothesis testing on the joint distribution of the channel input and channel output.

In [1] Wang and Renner independently gave a finite blocklength converse for coding over classical-quantum (c-q) channels using a very similar idea. In fact, for (discrete) classical channels their bound reduces to a particular restriction of the [4] converse. Their bound can be applied to general quantum channels by optimising over the encoding of messages to input states. In [2] Datta and Hsieh derive a finite blocklength converse for *entanglement-assisted coding* over quantum channels in terms of smoothed min- and max-entropies. They complement their converse with an one-shot achievability bound of a similar form, but it is not obvious how to compute either bound.

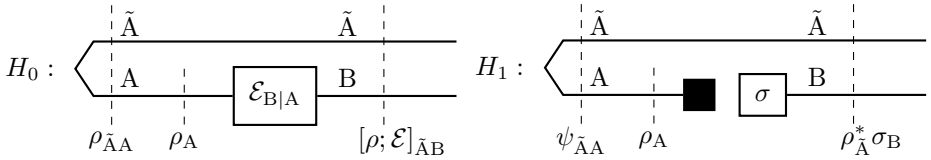

FIG. 3: The quantum hypothesis testing problem which appears in our bounds.

Our key result is a generalisation of the PPV bound to quantum channels. As shown in Fig. 3 the hypotheses specify quantum states of a bipartite system $\tilde{\mathrm{A}}\mathrm{B}$, where B is the output system of the channel and $\tilde{\mathrm{A}}$ is isomorphic to its input system. Defining a canonical purification of the average input state ρ_{A} by $\psi_{\tilde{\mathrm{A}}\mathrm{A}} := \rho_{\mathrm{A}}^{\frac{1}{2}} \Phi_{\tilde{\mathrm{A}}\mathrm{A}} \rho_{\mathrm{A}}^{\frac{1}{2}}$, where $\Phi_{\tilde{\mathrm{A}}\mathrm{A}} := \sum_{i,j=1}^{d_{\mathrm{A}}} |i\rangle_{\tilde{\mathrm{A}}} |i\rangle_{\mathrm{A}} \langle j|_{\tilde{\mathrm{A}}} \langle j|_{\mathrm{A}}$, hypothesis H_0

is that $\tilde{\mathrm{A}}\mathrm{B}$ is in the state $[\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}} := \mathcal{E}_{\mathrm{B}|\mathrm{A}}[\psi_{\tilde{\mathrm{A}}\mathrm{A}}]$ obtained by acting on this purification with the channel $\mathcal{E}_{\mathrm{B}|\mathrm{A}}$, whereas hypothesis H_1 is that the state of system B has been replaced by σ_{B}.

We obtain converses for both entanglement-assisted and unassisted codes as a function of the minimum type II error $\beta := \Pr(\text{guess } H_0|H_1, T)$, for tests T which have type I error $\alpha := \Pr(\text{guess } H_1|H_0, T)$ no greater than ϵ, and which can be implemented by operations in a class $\mathbf{\Omega}$ which depends on the class of codes:

$$D_\epsilon^{\mathbf{\Omega}}([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}\|\rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}}) = -\log\beta_\epsilon^{\mathbf{\Omega}}([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}, \rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}}) = \min_{T_{\tilde{\mathrm{A}}\mathrm{B}}\in\mathrm{T}\mathbf{\Omega}}\{\mathrm{Tr}T_{\tilde{\mathrm{A}}\mathrm{B}}\rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}} : \mathrm{Tr}T_{\tilde{\mathrm{A}}\mathrm{B}}[\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}} \geq 1-\epsilon.\}$$

The class **ALL** only demands that $T_{\tilde{\mathrm{A}}\mathrm{B}}$ be a valid POVM element ($0 \leq T_{\tilde{\mathrm{A}}\mathrm{B}} \leq \mathbb{1}$). By generalising the construction in [4] which takes codes for classical channels to classical hypothesis tests to a construction which takes entanglement-assisted codes to quantum tests (i.e. POVM elements), we show that $\log M_\epsilon^{\mathrm{E}}(\mathcal{E}_{\mathrm{B}|\mathrm{A}}, \rho_{\mathrm{A}}) \leq \min_{\sigma_{\mathrm{B}}} D_\epsilon([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}\|\rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}})$, and hence

$$\log M_\epsilon^{\mathrm{E}}(\mathcal{E}_{\mathrm{B}|\mathrm{A}}) \leq \max_{\rho_{\mathrm{A}}}\min_{\sigma_{\mathrm{B}}} D_\epsilon([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}\|\rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}}) \tag{1}$$

(where the omission of the test class superscript means that it is **ALL**). When the channel is classical this bound reduces to the PPV converse.

The class **L** of *local* tests corresponds operationally to those which can be implemented by classical hypothesis testing on the joint outcome of local operations on the two subsystems (possibly correlated by shared randomness). Since our construction is shown to take unassisted codes to local tests, we obtain the bounds $M_\epsilon(\mathcal{E}_{\mathrm{B}|\mathrm{A}}, \rho_{\mathrm{A}}) \leq \min_{\sigma_{\mathrm{B}}} \beta_\epsilon^{\mathbf{L}}([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}, \rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}})$ and

$$\log M_\epsilon(\mathcal{E}_{\mathrm{B}|\mathrm{A}}) \leq \max_{\rho_{\mathrm{A}}}\min_{\sigma_{\mathrm{B}}} D_\epsilon^{\mathbf{L}}([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}, \rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}}). \tag{2}$$

The Wang-Renner bound is shown to be equivalent to making the (sometimes suboptimal [5]) choice $\sigma_{\mathrm{B}} = \mathcal{E}_{\mathrm{B}|\mathrm{A}}[\rho_{\mathrm{A}}]$ and taking $\mathbf{\Omega}$ to be the class of tests **LC1** which can be implemented by local measurements and one-way classical communication from Alice and Bob.

The bound (1) for entanglement-assisted codes has a number of desirable properties: (i) It is asymptotically tight for memoryless channels. In common with the bound of Datta and Hsieh, analysing the large block length behaviour of the bound for memoryless channels recovers the converse part of the single-letter formula for entanglement-assisted capacity proven by Bennett, Shor, Smolin and Thapliyal [6].

(ii) Generalising results of Polyanskiy [5] we show that $\beta_\epsilon([\rho;\mathcal{E}]_{\tilde{\mathrm{A}}\mathrm{B}}\|\rho_{\tilde{\mathrm{A}}}^*\sigma_{\mathrm{B}})$ is convex in ρ_{A} and concave in σ_{B}. This enables one to use symmetries of the channel to restrict the optimisation over ρ_{A} and σ_{B} to states with corresponding symmetries. (iii) Unlike the bound of Datta and Hsieh, the bound (1) has an explicit formulation as *semidefinite program* (SDP) which is a natural generalisation of the linear program (LP) given in [7] for the PPV converse. Combined with property (ii), this allows it to be efficiently computed for highly symmetric channels, as we have done for Figure 1.

Since the Wang-Renner bound is asymptotically tight for the unassisted capacity (and for the product state capacity, thus recovering the HSW theorem) [3], the stronger bound (2) also has these properties, but is otherwise less attractive, as it lacks an SDP formulation and does not possess the convexity property mentioned above.

However, the formulation in terms of restricted hypothesis testing makes it clear that by moving to less restrictive conditions on the test, we might obtain weaker, but more tractable bounds.

When $\mathbf{\Omega}$ is **LC1**, or the larger class **PPT** of tests T whose partial transpose is a valid POVM element, the convexity property does hold, as does the symmetrisation argument, and for **PPT**

the bound is given by an SDP. It seems unlikely that the **PPT** bound is asymptotically tight, but it might prove useful for certain channels.

To demonstrate the use of our bound on entanglement-assisted codes, we show how to evaluate it exactly for depolarising channels. We also discuss the relationship of the work to existing results on strong converse bounds for quantum channels, and to security proofs in the noisy-storage model.

[1] L. Wang and R. Renner. One-shot classical-quantum capacity and hypothesis testing. *Phys. Rev. Lett.*, 108:200501, May 2012.

[2] N. Datta and M.-H. Hsieh. One-shot entanglement-assisted quantum and classical communication. *ArXiv e-prints*, May 2011.

[3] N. Datta, M. Mosonyi, M-H. Hsieh, and F. G. S. L. Brandao. Strong converse capacities of quantum channels for classical information. *To appear in IEEE Trans. Inf. Th*, 2011.

[4] Y. Polyanskiy, H. V. Poor, and S. Verdú. Channel coding rate in the finite blocklength regime. *IEEE Transactions on Information Theory*, pages 2307–2359, 2010.

[5] Y. Polyanskiy. Saddle point in the minimax converse for channel coding. *Submitted to IEEE Transactions on Information Theory*, 2012.

[6] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *Information Theory, IEEE Transactions on*, 48(10):2637–2655, October 2002.

[7] W. Matthews. A linear program for the finite block length converse of Polyanskiy-Poor-Verdú via non-signalling codes. *To appear in IEEE Trans. Inf. Th*, 2011.