Quantum Inf Process (2012) 11:1503–1509
DOI 10.1007/s11128-012-0451-2

ERRATUM

Erratum to: The quantum dynamic capacity formula of a quantum channel; Public and private resource trade-offs for a quantum channel

Mark M. Wilde · Min-Hsiu Hsieh

Published online: 7 August 2012

Erratum to: Quantum Information Processing
DOI 10.1007/s11128-011-0310-6;
DOI 10.1007/s11128-011-0317-z

1 Introduction

In this erratum, we revise our Theorem 2 in Ref. [5] and Theorem 2 in Ref. [4]. We had previously claimed in these two theorems that the rate region for classical communication, quantum communication, and entanglement consumption, and the rate region for public communication, private communication, and secret key consumption, respectively, could be computed as a convex optimization program. These claims are not

The online version of the original article can be found under
doi:10.1007/s11128-011-0310-6; 10.1007/s11128-011-0317-z.

M. M. Wilde (✉)
School of Computer Science, McGill University, Montreal, QC H3A 2A7, Canada
e-mail: mark.wilde@mcgill.ca

M.-H. Hsieh
ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency, 5-28-3, Hongo, Bunkyo-ku, Tokyo, Japan
e-mail: minhsiuh@gmail.com

Present Address:
M.-H. Hsieh
Statistical Laboratory, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK

M.-H. Hsieh
Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering
and Information Technology (FEIT), University of Technology, Sydney (UTS),
Broadway, P.O. Box 127, Sydney, NSW 2007, Australia

correct, simply because the task of computing the Holevo information (a special case of both triple trade-off rate regions) cannot be done with a convex optimization program, as was known in prior work (see Ref. [3], for example). We also prove that the task of computing these rate regions for general channels is NP-complete, by exploiting a simple reduction from the task of computing a channel's Holevo information to the task of computing the full triple trade-off region and the fact that computing a channel's Holevo information is NP-complete [1].

We structure this erratum as follows. We first provide proofs that the Holevo information cannot be computed as a simple convex optimization program. We do this by showing that the Holevo information is concave in the input distribution for a fixed set of signaling states (Lemma 1), while it is convex in the signaling states if the input distribution is fixed (Lemma 2). Thus, the computation of the Holevo information cannot be done with a convex optimization program, and in general, for this function, a local maximum will not be a global one. Although these facts are already known, we did not find this explicitly worked out in the literature and thought it would be useful to do so here. We then provide revisions of Theorem 2 in Ref. [5] and Theorem 2 in Ref. [4] that demonstrate why the quantum dynamic capacity formula and the private dynamic capacity formula, respectively, are still relevant in simplifying the computation of the rate regions' boundaries. Specifically, we show that if these formulas single-letterize, then it is only necessary to compute the regions with respect to a single channel use, rather than with a regularization (an infinite number of them). Finally, we show that the tasks of computing the boundaries of both triple trade-off rate regions are NP-complete.

2 Holevo information is concave in the input distribution and convex in the signaling states

Lemma 1 *The Holevo information $I(X;B)$ is concave in the input distribution when the signal states are fixed, in the sense that*

$$\lambda I(X;B)_{\sigma_0} + (1-\lambda)\, I(X;B)_{\sigma_1} \leq I(X;B)_{\sigma}\,, \tag{1}$$

where σ_0^{XB} and σ_1^{XB} are of the form

$$\sigma_0^{XB} \equiv \sum_x p_X(x)\, |x\rangle\langle x|^X \otimes \mathcal{N}(\sigma_x)\,, \tag{2}$$

$$\sigma_1^{XB} \equiv \sum_x q_X(x)\, |x\rangle\langle x|^X \otimes \mathcal{N}(\sigma_x)\,, \tag{3}$$

and σ^{XB} is a mixture of the states σ_0^{XB} and σ_1^{XB} of the form:

$$\sigma^{XB} \equiv \sum_x \left[\lambda p_X(x) + (1-\lambda)\, q_X(x)\right] |x\rangle\langle x|^X \otimes \mathcal{N}(\sigma_x)\,, \tag{4}$$

where $0 \leq \lambda \leq 1$.

Proof Let σ^{XUB} be the state

$$\sigma^{UXB} \equiv \sum_x \left[p_X(x) |x\rangle \langle x|^X \otimes \lambda |0\rangle \langle 0|^U + q_X(x) |x\rangle \langle x|^X \otimes (1-\lambda) |1\rangle \langle 1|^U \right] \\ \otimes \mathcal{N}(\sigma_x). \tag{5}$$

Observe that $\text{Tr}_U \left\{ \sigma^{XUB} \right\} = \sigma^{XB}$. Then, the statement of concavity is equivalent to

$$I(X; B|U)_\sigma \leq I(X; B)_\sigma. \tag{6}$$

We can rewrite this as

$$H(B|U)_\sigma - H(B|UX)_\sigma \leq H(B)_\sigma - H(B|X)_\sigma. \tag{7}$$

Observe that

$$H(B|UX)_\sigma = H(B|X)_\sigma, \tag{8}$$

that is, one can calculate that both of these are equal to

$$\sum_x [\lambda p_X(x) + (1-\lambda) q_X(x)] H(\mathcal{N}(\sigma_x)). \tag{9}$$

The statement of concavity then becomes

$$H(B|U)_\sigma \leq H(B)_\sigma, \tag{10}$$

which follows from concavity of quantum entropy. □

Lemma 2 *The Holevo information $I(X; B)$ is convex in the signal states when the input distribution is fixed, in the sense that*

$$\lambda I(X; B)_{\sigma_0} + (1-\lambda) I(X; B)_{\sigma_1} \geq I(X; B)_\sigma, \tag{11}$$

where σ_0^{XB} and σ_1^{XB} are of the form

$$\sigma_0^{XB} \equiv \sum_x p_X(x) |x\rangle \langle x|^X \otimes \mathcal{N}(\sigma_x), \tag{12}$$

$$\sigma_1^{XB} \equiv \sum_x p_X(x) |x\rangle \langle x|^X \otimes \mathcal{N}(\omega_x), \tag{13}$$

and σ^{XB} is a mixture of the states σ_0^{XB} and σ_1^{XB} of the form:

$$\sigma^{XB} \equiv \sum_x p_X(x) |x\rangle \langle x|^X \otimes \mathcal{N}(\lambda\sigma_x + (1-\lambda)\omega_x), \tag{14}$$

where $0 \leq \lambda \leq 1$.

Proof Let σ^{XUB} be the state

$$\sigma^{XUB} \equiv \sum_x p_X(x) |x\rangle \langle x|^X \otimes \left[\lambda |0\rangle \langle 0|^U \otimes \mathcal{N}(\sigma_x) + (1-\lambda) |1\rangle \langle 1|^U \otimes \mathcal{N}(\omega_x) \right]. \tag{15}$$

Observe that $\mathrm{Tr}_U \left\{ \sigma^{XUB} \right\} = \sigma^{XB}$. Then, convexity in the input states is equivalent to the statement

$$I(X; B|U)_\sigma \geq I(X; B)_\sigma . \tag{16}$$

Consider that

$$I(X; B|U)_\sigma = I(X; BU)_\sigma - I(X; U)_\sigma , \tag{17}$$

by the chain rule for the quantum mutual information. Since the input distribution $p_X(x)$ is fixed, there are no correlations between X and the convexity variable U, so that $I(X; U)_\sigma = 0$. Thus, the above inequality is equivalent to

$$I(X; BU)_\sigma \geq I(X; B)_\sigma , \tag{18}$$

which follows from the quantum data processing inequality. □

In the above two theorems, we have shown that the Holevo information is either concave or convex depending on whether the signal states or the input distribution is fixed, respectively. Thus, the computation of the Holevo information of a general quantum channel becomes difficult as the input dimension of the channel grows larger, since a local maximum of the Holevo information is not necessarily a global maximum.

3 Revision of Theorem 2 of Ref. [5] and Theorem 2 of Ref. [4]

Recall that the quantum dynamic capacity formula is defined as follows:

Definition 1 (Quantum Dynamic Capacity Formula) The quantum dynamic capacity formula of a quantum channel $\mathcal{N}$ is as follows:

$$D_{\lambda,\mu}(\mathcal{N}) \equiv \max_\sigma I(AX; B)_\sigma + \lambda I(A\rangle BX)_\sigma + \mu \left(I(X; B)_\sigma + I(A\rangle BX)_\sigma \right), \tag{19}$$

where σ is a state of the form

$$\sigma^{XAB} \equiv \sum_x p_X(x) |x\rangle \langle x|^X \otimes \mathcal{N}^{A' \to B}(\phi_x^{AA'}), \tag{20}$$

$\lambda, \mu \geq 0$, and these parameters λ and μ play the role of Lagrange multipliers.

Theorem 1 *Single-letterization of the quantum dynamic capacity formula implies that the computation of the Pareto optimal trade-off surface of the quantum dynamic capacity region requires an optimization over a single channel use.*

Proof We employ ideas from optimization theory for the proof (see Ref. [2]). We would like to characterize all the points in the capacity region that are Pareto optimal. Such a task is standard vector optimization in the theory of Pareto trade-off analysis (see Section 4.7 of Ref. [2]). We can phrase the optimization task as the following scalarization of the vector optimization task:

$$\max_{C,Q,E,p(x),\phi_x} w_C C + w_Q Q + w_E E \tag{21}$$

subject to

$$\begin{aligned} C + 2Q &\leq I(AX; B^n)_\sigma, & (22)\\ Q + E &\leq I(A\rangle B^n X)_\sigma, & (23)\\ C + Q + E &\leq I(X; B^n)_\sigma + I(A\rangle B^n X)_\sigma, & (24)\end{aligned}$$

where the maximization is over all C, Q, and E and over probability distributions $p_X(x)$ and bipartite states $\phi_x^{AA'^n}$. The geometric interpretation of the scalarization task is that we are trying to find a supporting plane of the dynamic capacity region where the weight vector $\left(w_C, w_Q, w_E\right)$ is the normal vector of the plane and the value of its inner product with (C, Q, E) characterizes the offset of the plane. The Lagrangian of the above optimization problem is

$$\begin{aligned}\mathcal{L}\left(C, Q, E, p_X(x), \phi_x^{AA'^n}, \lambda_1, \lambda_2, \lambda_3\right) \equiv\ & w_C C + w_Q Q + w_E E\\ & +\lambda_1 \left(I\left(AX; B^n\right)_\sigma - \left(C + 2Q\right)\right)\\ & +\lambda_2 \left(I\left(A\rangle B^n X\right)_\sigma - \left(Q + E\right)\right)\\ & +\lambda_3 \left(I\left(X; B^n\right)_\sigma + I\left(A\rangle B^n X\right)_\sigma\right.\\ & \left.-\left(C + Q + E\right)\right), \end{aligned}\tag{25}$$

and the Lagrange dual function g [2] is

$$g\left(\lambda_1, \lambda_2, \lambda_3\right) \equiv \sup_{C,Q,E,p(x),\phi_x^{AA'^n}} \mathcal{L}\left(C, Q, E, p_X(x), \phi_x^{AA'^n}, \lambda_1, \lambda_2, \lambda_3\right), \tag{26}$$

where $\lambda_1, \lambda_2, \lambda_3 \geq 0$. The optimization task simplifies if the Lagrange dual function does. Thus, we rewrite the Lagrange dual function as follows:

$$\begin{aligned} g\left(\lambda_1, \lambda_2, \lambda_3\right) = \sup_{C,Q,E,p(x),\phi_x^{AA'^n}} & w_C C + w_Q Q + w_E E + \lambda_1 \left(I\left(AX; B^n\right)_\sigma\right.\\ & \left.-\left(C + 2Q\right)\right) + \lambda_2 \left(I\left(A\rangle B^n X\right)_\sigma - \left(Q + E\right)\right)\\ & +\lambda_3 \left(I\left(X; B^n\right)_\sigma + I\left(A\rangle B^n X\right)_\sigma - \left(C + Q + E\right)\right) \end{aligned}\tag{27}$$

$$
\begin{aligned}
&= \sup_{C,Q,E,p(x),\phi_x^{AA'^n}} (w_C - \lambda_1 - \lambda_3)\, C + \left(w_Q - 2\lambda_1 - \lambda_2 - \lambda_3\right) Q \\
&\quad + (w_E - \lambda_2 - \lambda_3)\, E + \lambda_1 \Bigg(I\left(AX;B^n\right)_\sigma \\
&\quad + \frac{\lambda_2}{\lambda_1} I\left(A\rangle B^n X\right)_\sigma + \frac{\lambda_3}{\lambda_1}\left(I\left(X;B^n\right)_\sigma + I\left(A\rangle B^n X\right)_\sigma\right)\Bigg) \qquad (28) \\
&= \sup_{C,Q,E} (w_C - \lambda_1 - \lambda_3)\, C + \left(w_Q - 2\lambda_1 - \lambda_2 - \lambda_3\right) Q \\
&\quad + (w_E - \lambda_2 - \lambda_3)\, E + \lambda_1 \Bigg(\max_{p(x),\phi_x^{AA'^n}} I\left(AX;B^n\right)_\sigma + \frac{\lambda_2}{\lambda_1} I\left(A\rangle B^n X\right)_\sigma \\
&\quad + \frac{\lambda_3}{\lambda_1}\left(I\left(X;B^n\right)_\sigma + I\left(A\rangle B^n X\right)_\sigma\right)\Bigg). \qquad (29)
\end{aligned}
$$

The first equality follows by definition. The second equality follows from some algebra, and the last follows because the Lagrange dual function factors into two separate optimization tasks: one over C, Q, and E and another that is equivalent to the quantum dynamic capacity formula with $\lambda = \lambda_2/\lambda_1$ and $\mu = \lambda_3/\lambda_1$. Thus, the computation of the Pareto optimal trade-off surface requires just a single use of the channel if the quantum dynamic capacity formula in (19) single-letterizes. □

Similarly, the private dynamic capacity formula is defined as follows:

Definition 2 (Private Dynamic Capacity Formula) The private dynamic capacity formula of a quantum channel $\mathcal{N}$ is as follows:

$$
\begin{aligned}
P_{\lambda,\mu}(\mathcal{N}) \equiv \max_\sigma I(YX;B)_\sigma + \lambda\left[I(Y;B|X)_\sigma - I(Y;E|X)_\sigma\right] + \mu\left[I(YX;B)_\sigma\right. \\
\left. - I(Y;E|X)_\sigma\right], \qquad (30)
\end{aligned}
$$

where $\lambda, \mu \geq 0$, σ^{XYBE} is a state of the following form:

$$
\sigma^{XYBE} \equiv \sum_{x,y} p_{X,Y}(x,y)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_{x,y}^{A'}), \qquad (31)
$$

$U_{\mathcal{N}}^{A'\to BE}$ is an isometric extension of the channel $\mathcal{N}$, and the states $\rho_{x,y}^{A'}$ are mixed.

We obtain the following revision of Theorem 2 of Ref. [4] in a similar way:

Theorem 2 *Single-letterization of the private dynamic capacity formula implies that the computation of the Pareto optimal trade-off surface of the private dynamic capacity region requires an optimization over a single channel use.*

Proof The proof exploits the same techniques as the proof of Theorem 1 above. □

4 Computing the trade-off region is NP-complete

We finally prove that the task of computing the boundary of the trade-off regions, even in the case where the region single-letterizes, is an NP-complete problem. We do so by appealing to the results of Beigi and Shor [1].

Theorem 3 *Suppose $\mathcal{N}$ is a quantum channel that acts on a d-dimensional Hilbert space and is specified by poly(d) number of bits. Let $\partial\mathcal{C}_{\text{CQE}}(\mathcal{N})$ denote the boundary of the single-letter quantum dynamic capacity region given by (9–11) in Theorem 1 of Ref. [5]. Then deciding whether poly(d) number of rate triples (C, Q, E) (some of which are on the C, Q, or E axes) all lie inside the boundary $\partial\mathcal{C}_{\text{CQE}}(\mathcal{N})$ is* NP-complete.

Proof We prove this theorem by showing that this decision problem is in NP and is “harder” than the problem of computing the Holevo formula for the quantum channel $\mathcal{N}$, which has already been shown to be NP-complete [1].

First, we can easily prove that the decision problem is in NP. If $\mathcal{N}$ is a quantum channel and all of the rate triples (C, Q, E) lie inside the boundary $\partial\mathcal{C}_{\text{CQE}}(\mathcal{N})$, then for each rate triple, there is an ensemble $\{p_X(x), \rho_x\}_{x\in\mathcal{X}}$ such that $|\mathcal{X}| \leq \text{poly}(d)$ (a simple application of Caratheodory’s theorem) and such that the rate triple lies inside the region given by (9–11) of Theorem 1 of Ref. [5]. Therefore given these ensembles corresponding to the rate triples, the verifier can check in polynomial time whether the rate triples lie inside the region.

To show that this decision problem is NP-hard, there is a simple reduction from the task of computing the Holevo formula to the task of computing the full region. In particular, given a method for deciding whether a polynomial number of rate triples are inside the region, one could use this to decide whether the Holevo formula is larger than some constant. Thus, the above decision problem is NP-complete. □

Remark 1 A similar decision problem for the single-letter private dynamic capacity region is NP-complete. This follows by the same proof because the Holevo formula is a special rate triple in the single-letter private dynamic capacity region.

Acknowledgements We are grateful to Graeme Smith for pointing out Ref. [1] to us and noting the conflict between our previous claims and the results in Ref. [1].

References

1. Beigi, S., Shor, P.: On the complexity of computing zero-error and Holevo capacity of quantum channels. September 2007. arXiv:0709.2090.
2. Boyd, S., Vandenberghe, L.: *Convex Optimization*. Cambridge University Press, Cambridge (2004)
3. Hayashi, M., Imai, H., Matsumoto, K., Ruskai, M.B., Shimono, T.: Qubit channels which require four inputs to achieve capacity: implications for additivity conjectures. Quant. Inform. Comput. **5**, 13–31 (2005). arXiv:quant-ph/0403176
4. Wilde, M.M., Hsieh, M.-H.: Public and private resource trade-offs for a quantum channel. Quant. Inform. Process. May 2010. arXiv:1005.3818 (accepted)
5. Wilde, M.M., Hsieh, M.-H.: The quantum dynamic capacity formula of a quantum channel. Quant. Inform. Process. April 2010. arXiv:1004.0458 (accepted)