Accessible versus Holevo Information for a Binary Random Variable

Rahul Jain
U.C. Berkeley *

Ashwin Nayak
U. Waterloo & Perimeter †

Abstract

The *accessible information* $I_{\mathrm{acc}}(\mathcal{E})$ of an ensemble $\mathcal{E}$ is the maximum mutual information between a random variable encoded into quantum states, and the probabilistic outcome of a quantum measurement of the encoding. Accessible information is extremely difficult to characterize analytically; even bounds on it are hard to place. The celebrated *Holevo bound* states that accessible information cannot exceed $\chi(\mathcal{E})$, the quantum mutual information between the random variable and its encoding. However, for general ensembles, the gap between the $I_{\mathrm{acc}}(\mathcal{E})$ and $\chi(\mathcal{E})$ may be arbitrarily large.

We consider the special case of a binary random variable, which often serves as a stepping stone towards other results in information theory and communication complexity. We show that for an ensemble $\mathcal{E} \triangleq \{(p,\rho_0),(1-p,\rho_1)\}$, $\quad I_{\mathrm{acc}}(\mathcal{E}) \;\geq\; H(p) - \sqrt{4p(1-p) - \chi(\mathcal{E})^2}$.

1 Introduction

Let X be a classical random variable taking values in a finite set $\{0,\ldots,n-1\}$ such that $\Pr(X=i) \triangleq p_i$. Let M be an encoding of X into (possibly mixed) quantum states in a finite dimensional, say d-dimensional, Hilbert space $\mathbb{C}^d$, such that $M = \rho_i$ when $X = i$. This gives rise to an ensemble of quantum states $\mathcal{E} \triangleq \{(p_i,\rho_i)\}$.

The mapping $i \mapsto \rho_i$ may be viewed as a quantum communication channel, and it is natural to ask how much information about X can be obtained from the transmitted signal M. The answer to this question depends heavily on the way we quantify the notion of "information". For example, one may seek to maximize the probability of guessing, via a measurement, the value i given an unknown state ρ_i from the ensemble $\mathcal{E}$. This quantity frequently arises in quantum communication, but has no simple description in terms of the ensemble. For a boolean random variable, the answer is related to the trace distance of the two density operators [Hel76, pp. 106–108]. While no analytical expression for this probability is known in the general case, we can still place meaningful bounds on it (see, e.g., Ref. [NS06]).

A different way of quantifying the information content of an ensemble arises in Quantum Information Theory. Consider a classical random variable $Y^{\mathcal{M}}$ that represents the result of a measurement of the

*Computer Science Division, University of California, Berkeley, CA 94720, USA. Email: rahulj@cs.berkeley.edu.

This work was supported by an Army Research Office (ARO), North California, grant number DAAD 19-03-1-00082.

†Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo, ON N2L 3G1, Canada. E-mail: anayak@math.uwaterloo.ca. A.N. is also Associate Member, Perimeter Institute for Theoretical Physics, Waterloo, Canada,

and his research is supported in part by NSERC, CIAR, MITACS, CFI, and OIT (Canada).

encoding $\mathcal{M}$. The *accessible information* $I_{\rm acc}(\mathcal{E})$ of the ensemble $\mathcal{E}$ is defined as the maximum mutual information $I(X:Y^{\mathcal{M}})$ obtainable via a quantum measurement $\mathcal{M}$:

$$I_{\rm acc}(\mathcal{E}) \quad \stackrel{\Delta}{=} \quad \max_{\mathcal{M}} I(X:Y^{\mathcal{M}}). \tag{1}$$

Accessible information is extremely difficult to characterize analytically, even for a binary random variable (see, e.g., Ref. [FvdG99, page 7], where it is referred to as *Shannon Distinguishability*). In a celebrated result, Holevo [Hol73] bounded the accessible information for an ensemble $\mathcal{E}$ by the quantum mutual information between the random variable X and its encoding M:

$$I_{\rm acc}(\mathcal{E}) \quad \leq \quad \chi(\mathcal{E}) \quad \stackrel{\Delta}{=} \quad S(\mathbb{E}_i[\rho_i]) - \mathbb{E}_i[S(\rho_i)] \quad = \quad I(X:M), \tag{2}$$

where $S(\rho)$ denotes von Neumann entropy of a density matrix ρ, and $I(A:B) = S(A) + S(B) - S(AB)$ denotes mutual information of a bipartite quantum system AB. The quantity $\chi(\mathcal{E})$ has come to be called the *Holevo information* of the ensemble.

The Holevo bound is tight for ensembles of commuting states (equivalently, for classical mixtures). In fact, Petz [Pet03, Section 4.3] proves that these are the only ensembles for which $I(X:Y^{\mathcal{M}}) = I(X:M)$ is possible. There are ensembles for which $I_{\rm acc}(\mathcal{E})$ may be arbitrarily smaller than $\chi(\mathcal{E})$: a uniformly random ensemble of n states in a d-dimensional space (where d is suitably smaller than n) has this property with high probability.

Lower bounds on $I_{\rm acc}$ are hard to derive even for specific ensembles (cf. Refs. [FC94, JRW94]). In the simplest case of a binary random variable, Fuchs and van de Graaf [FvdG99] relate accessible information to the trace distance and fidelity of the density matrices. Fuchs and Caves [FC95] also consider the case of a binary random variable, stopping short of an explicit lower bound. We revisit this special case, and give a lower bound for accessible information in terms of Holevo information.

Relations between different measures of information in the binary case often form a stepping stone in results in information theory (see Ref. [FC94]) or in communication complexity (for example, see [KNTSZ06, JRS03]). We expect that our inequalities provide a more operationally useful view of accessible information, and find similar application.

Preliminaries

We quickly summarize the information theory concepts we use in this article. For a more comprehensive treatment, we refer the reader to a text such as [NC00].

Let $\mathcal{H}, \mathcal{K}$ be Hilbert spaces. For a quantum state $\rho \in \mathcal{H}$, we call a pure state $|\phi\rangle \in \mathcal{H} \otimes \mathcal{K}$ a *purification* of ρ if $\mathsf{Tr}_{\mathcal{K}} |\phi\rangle\langle\phi| = \rho$. The *fidelity* between (mixed) quantum states ρ, σ is defined as $B(\rho,\sigma) \stackrel{\Delta}{=} \max\ |\langle\phi|\psi\rangle|$, where the optimization is over states $|\phi\rangle$ which is a purification of ρ and $|\psi\rangle$ which is a purification of σ. For an operator A, we define its *trace norm* as $|A|_t \stackrel{\Delta}{=} \mathsf{Tr}\sqrt{A^\dagger A}$. For a state ρ, its *von-Neumann* entropy is defined as $S(\rho) \stackrel{\Delta}{=} -\mathsf{Tr}\rho\log\rho$. For $0 \leq p \leq 1$, let $H(p) \stackrel{\Delta}{=} -p\log p - (1-p)\log(1-p)$ denote the binary entropy function.

2 Uniform random variable

We first discuss the case of uniform random variable, i.e. when $\Pr(X=0) \stackrel{\Delta}{=} p = 1/2$. We start with a few lemmas which might be of independent interest.

Lemma 2.1 *For $i \in \{0,1\}$ let $\mathcal{E} \stackrel{\Delta}{=} \{(1/2, \rho_i)\}$ be an ensemble, where ρ_0, ρ_1 are pure states. Then,*

$$\chi(\mathcal{E}) \quad \leq \quad \sqrt{1 - B(\rho_0, \rho_1)^2} \quad = \quad \frac{|\rho_0 - \rho_1|_t}{2}.$$

Proof: Let θ be the angle between the pure states ρ_0 and ρ_1. Let $\rho = \frac{\rho_0 + \rho_1}{2}$ be the average density matrix. By a direct calculation we see that the eigenvalues of ρ are $\frac{1 \pm \cos\theta}{2}$. Therefore $|\rho_0 - \rho_1|_t = 2\sin\theta$ and $B(\rho_0, \rho_1) = \cos\theta$. Now we have the following fact (see, e.g. [FvdG99, p. 9, Fig. 1]):

Fact 2.2 *For $\delta \in [-\frac{1}{2}, \frac{1}{2}]$, $\quad H(\frac{1}{2} + \delta) \leq \sqrt{1 - (2\delta)^2}$.*

Since ρ_0, ρ_1 are pure states, $S(\rho_0) = S(\rho_1) = 0$. Using Fact 2.2,

$$\begin{aligned} \chi(\mathcal{E}) \quad &= \quad S(\rho) \quad = \quad H\left(\frac{1 + \cos\theta}{2}\right) \\ &\leq \quad \sqrt{1 - \cos^2\theta} \quad = \quad \sqrt{1 - B(\rho_0, \rho_1)^2} \quad = \quad \frac{|\rho_0 - \rho_1|_t}{2}, \end{aligned}$$

which is the claimed bound. ∎

Below we show a similar result when ρ_0, ρ_1 could be mixed states.

Lemma 2.3 *For $i \in \{0,1\}$ let $\mathcal{E} \stackrel{\Delta}{=} \{(1/2, \rho_i)\}$ be an ensemble of possibly mixed states ρ_0, ρ_1. Then,*

$$\chi(\mathcal{E}) \quad \leq \quad \sqrt{1 - B(\rho_0, \rho_1)^2} \quad \leq \quad \sqrt{|\rho_0 - \rho_1|_t}.$$

Proof: Let $|\phi_0\rangle, |\phi_1\rangle$ be purifications of ρ_0, ρ_1 which achieve fidelity $B(\rho_0, \rho_1)$. Let us consider the encoding M' of X such that $M' = |\phi_0\rangle$ when $X = 0$, and $M' = |\phi_1\rangle$ when $X = 1$. From strong sub-additivity of von Neumann entropy (see, e.g., Ref. [NC00]), it follows that $I(X : M) \leq I(X : M')$. Now,

$$\begin{aligned} \chi(\mathcal{E}) \quad &= \quad I(X : M) \quad \leq \quad I(X : M') \\ &\leq \quad \sqrt{1 - B(|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|)^2} \quad = \quad \sqrt{1 - B(\rho_0, \rho_1)^2} \\ &\leq \quad \sqrt{2(1 - B(\rho_0, \rho_1))} \\ &\leq \quad \sqrt{|\rho_0 - \rho_1|_t}, \end{aligned}$$

where the last inequality follows from [FvdG99, Theorem 1]. ∎

We now have the following theorem.

Theorem 2.4 *For $i \in \{0,1\}$ let $\mathcal{E} \stackrel{\Delta}{=} \{(1/2, \rho_i)\}$ be a uniform ensemble of quantum states. Then,*

$$1 - \sqrt{1 - \chi(\mathcal{E})^2} \quad \leq \quad I_{\mathrm{acc}}(\mathcal{E}).$$

Proof: From [FvdG99, Theorem 1] we have that

$$1 - B(\rho_0, \rho_1) \quad \leq \quad I_{\mathrm{acc}}(\mathcal{E}).$$

Now from Lemma 2.3,

$$B(\rho_0, \rho_1) \quad \leq \quad \sqrt{1 - \chi(\mathcal{E})^2}.$$

Putting them together, we get the stated bound. ∎

3 Non-uniform random variable

In this section we discuss the case of a general binary random variable (p need not be $1/2$). Again, we first show a few lemmas which may be of independent interest.

Lemma 3.1 *Let* $\mathcal{E} \stackrel{\Delta}{=} \{(p, \rho_0), (1-p, \rho_1)\}$ *be an ensemble of quantum states. Then,*

$$H(p) - 2\sqrt{p(1-p)}\, B(\rho_0, \rho_1) \quad \leq \quad I_{\mathrm{acc}}(\mathcal{E}).$$

Proof: Let ρ'_0, ρ'_1 be the classical distributions resulting from a measurement that achieves the fidelity between ρ_0 and ρ_1 (cf. Ref. [FC95]). Let $\rho' = p\rho'_0 + (1-p)\rho'_1$. Let M' be the encoding of X such that $M' = \rho'_0$ when $X = 0$ and $M' = \rho'_1$ when $X = 1$. Let $p_0(m) \stackrel{\Delta}{=} \Pr(M' = m / X = 0), p(m) \stackrel{\Delta}{=} \Pr(M' = m)$ and $r_0(m) \stackrel{\Delta}{=} \Pr(X = 0/M' = m)$. We similarly define $p_1(m)$. Then, using the relations explained below, we have:

$$\begin{aligned}
I_{\mathrm{acc}} \;\geq\; I(X : M') &= H(p) - \sum_m p(m) H(r_0(m)) \\
&\geq H(p) - \sum_m p(m) \cdot 2\sqrt{r_0(m)(1 - r_0(m))} \\
&= H(p) - \sum_m 2\sqrt{p(1-p)p_0(m)p_1(m)} \\
&= H(p) - 2\sqrt{p(1-p)}\, B(\rho'_0, \rho'_1).
\end{aligned}$$

The second inequality follows from Fact 2.2. The next equation comes from the fact that $p\, p_0(m) = p(m)\, r_0(m)$ and $(1-p)\, p_1(m) = p(m)\,(1 - r_0(m))$. ■

Next we show the following.

Lemma 3.2 *Let* $\mathcal{E} \stackrel{\Delta}{=} \{(p, \rho_0), (1-p, \rho_1)\}$ *be an ensemble such that* ρ_0, ρ_1 *are pure states. Then,*

$$\chi(\mathcal{E}) \quad \leq \quad 2\sqrt{p(1-p)(1 - B(\rho_0, \rho_1)^2)}.$$

Proof: Let θ be the angle between the pure states ρ_0 and ρ_1 so that $B(\rho_0, \rho_1) = \cos\theta$. Let $\rho = p\rho_0 + (1 - p)\rho_1$. By a direct calculation we see that the eigenvalues of ρ are

$$\frac{1 \pm \sqrt{1 - 4p(1-p)\sin^2\theta}}{2}.$$

Therefore from Fact 2.2 we have,

$$\begin{aligned}
\chi(\mathcal{E}) = S(\rho) &= H\left(\frac{1 + \sqrt{1 - 4p(1-p)\sin^2\theta}}{2}\right) \\
&\leq 2\sin\theta\, \sqrt{p(1-p)} = 2\sqrt{p(1-p)(1 - B(\rho_0, \rho_1)^2)}.
\end{aligned}$$

■

As a corollary of the above lemma, we get:

Corollary 3.3 *Let* $\mathcal{E} \triangleq \{(p, \rho_0), (1-p, \rho_1)\}$ *be an ensemble where* ρ_0, ρ_1 *may be mixed states. Then,*

$$\chi(\mathcal{E}) \quad \leq \quad 2\sqrt{p(1-p)(1-B(\rho_0,\rho_1)^2)}.$$

Proof: As before, let $|\phi_0\rangle, |\phi_1\rangle$ be purifications of ρ_0, ρ_1 which achieve fidelity between the two states. Let us consider the encoding M' of X such that $M' = |\phi_0\rangle$ when $X = 0$ and $M' = |\phi_1\rangle$ when $X = 1$. Again from the strong sub-additivity property of von Neumann entropy it follows that $I(X : M) \leq I(X : M')$. Now,

$$\begin{aligned} \chi(\mathcal{E}) &= I(X:M) \quad \leq \quad I(X:M') \\ &\leq 2\sqrt{p(1-p)(1-B(|\phi_0\rangle\langle\phi_0|, |\phi_1\rangle\langle\phi_1|)^2)} \\ &= 2\sqrt{p(1-p)(1-B(\rho_0,\rho_1)^2)}, \end{aligned}$$

as required. ■

Finally we get our main inequality.

Theorem 3.4 *Let* $\mathcal{E} \triangleq \{(p, \rho_0), (1-p, \rho_1)\}$ *be an ensemble. Then,*

$$H(p) - \sqrt{4p(1-p) - \chi(\mathcal{E})^2} \quad \leq \quad I_{\mathrm{acc}}(\mathcal{E}).$$

Proof: Follows immediately from Lemma 3.1 and Corollary 3.3. ■

4 Concluding remarks

In Theorem 3.4 we bounded the accessible information of an arbitrary ensemble corresponding to a binary random variable from below, by relating it to the Holevo χ quantity. By a theorem of Petz [Pet03, Section 4.3], whenever the states in the ensemble are not orthogonal, no measurement achieves Holevo information. While this does not rule out the possibility of the two quantities being equal in the limit of more and more refined measurements, we believe that strict inequality holds. For this reason, the lower bound in terms of Holevo information becomes significant. The strength and usefulness of our bound would of course depend on the application at hand. We leave the possibility of a tighter bound open.

References

[FC94] Christopher A. Fuchs and Carlton M. Caves. Ensemble-dependent bounds for accessible information in quantum mechanics. *Physical Review Letters*, 73(23):3047–3050, December 1994.

[FC95] Christopher A. Fuchs and Carlton M. Caves. Mathematical techniques for quantum communication theory. *Open Systems and Information Dynamics*, 3(3):345–356, 1995. Also quant-ph/9604001.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[Hel76] Carl W. Helstrom. *Quantum Detection and Estimation Theory*, volume 123 of *Mathematics in Science and Engineering*. Academic Press, New York, 1976.

[Hol73] A.S. Holevo. Some estimates of the information transmitted by quantum communication channels. *Problems of Information Transmission*, 9(3):177–183, 1973. Russian version in *Problemy Peredachi Informatsii 9* (1973), 3–11.

[JRS03] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A lower bound for bounded round quantum communication complexity of set disjointness. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, Los Alamitos, CA, USA, 2003. IEEE Press. Also quant-ph/0303138.

[JRW94] Richard Jozsa, Daniel Robb, and William K. Wootters. Lower bound for accessible information in quantum mechanics. *Physical Review A*, 49(2):668–677, February 1994.

[KNTSZ06] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, and David Zuckerman. Interaction in quantum communication. Technical Report quant-ph/0603135, ArXiv.org Preprint Archive, `http://www.arxiv.org/abs/quant-ph/`, March 2006. Submitted to *IEEE Transactions on Information Theory*.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[NS06] Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *Journal of the ACM*, 53(1):1–23, January 2006.

[Pet03] Dénes Petz. Monotonicity of quantum relative entropy revisited. *Reviews in Mathematical Physics*, 15(1):79–91, 2003.