

A Tight Uniform Continuity Bound for Equivocation

Mohammad A. Alhejji

JILA, University of Colorado/NIST
440 UCB,
Boulder, CO 80309, USA
Email: mohammad.alhejji@colorado.edu

Graeme Smith

JILA, University of Colorado/NIST
440 UCB,
Boulder, CO 80309, USA
Email: graeme.smith@colorado.edu

Abstract—

We prove a tight uniform continuity bound for the conditional Shannon entropy of discrete finitely supported random variables in terms of total variation distance.

I. INTRODUCTION

There has been significant work towards understanding the interplay between the Shannon entropy and various distance measures on the probability simplex [1], [2], [3]. In conjunction, remarkable progress has been made in the study of the continuity of the von Neumann entropy, or matrix entropy, versus trace distance [4], [5], [6]. In both cases, several proofs of a tight uniform continuity bound have been presented [1], [2], [7], [5], [8], [9]. On the other hand, uniform bounds, which are not tight but are independent of the size of the conditioning system, were proven for the conditional Shannon and von Neumann entropies in [10], [8]. In this note, We present a proof of a tight uniform continuity bound for the conditional Shannon entropy of discrete finitely supported random variables in terms of total variation distance.

Let $\mathcal{X} := \{1, 2, \dots, |\mathcal{X}|\}$ and $\mathcal{Y} := \{1, 2, \dots, |\mathcal{Y}|\}$. Let $\mathcal{P}_{\mathcal{X} \times \mathcal{Y}}$ denote the probability simplex with $|\mathcal{X}||\mathcal{Y}|$ atoms. The Shannon entropy of a random variable $X \sim p_X$ is defined as [11]

$$H(X) := - \sum_{i \in \mathcal{X}} p_X(i) \log p_X(i). \quad (1)$$

Here, all logarithms are meant in base 2. Similarly, for two jointly distributed random variables $(X, Y) \sim p_{XY}$, the joint Shannon entropy is given by

$$H(XY) := - \sum_{i \in \mathcal{X}} \sum_{j \in \mathcal{Y}} p_{XY}(i, j) \log p_{XY}(i, j), \quad (2)$$

and the conditional Shannon entropy $H(X|Y)$, also known as the equivocation in X given Y , is defined as

$$H(X|Y) := H(XY) - H(Y) \quad (3)$$

$$= \sum_{j \in \mathcal{Y}} p_Y(j) H(X|Y = j) \quad (4)$$

$$= - \sum_{i \in \mathcal{X}} \sum_{j \in \mathcal{Y}} p_{XY}(i, j) \log \frac{p_{XY}(i, j)}{p_Y(j)}. \quad (5)$$

Given two probability distributions $p_{XY}, q_{X'Y'} \in \mathcal{P}_{\mathcal{X} \times \mathcal{Y}}$, the total variation distance between them is given by

$$\text{TV}(p_{XY}, q_{X'Y'}) = \frac{1}{2} \sum_{i \in \mathcal{X}} \sum_{j \in \mathcal{Y}} |p_{XY}(i, j) - q_{X'Y'}(i, j)|. \quad (6)$$

A bona fide metric on the probability simplex, it captures the distinguishability of any two probability distributions [12].

There are at least two reasons to want the sharpest bounds on the variation of entropic quantities in terms of relevant distance measures. The first reason is that in practice we only have access to estimates of distributions, never the true distribution, of any given random variable. Second, in settings where communication rates can be evaluated only for a special class of distributions, it pays to have tight bounds on the error incurred by

approximating the rates of arbitrary distributions by the ones of the closest members of said special class [13], [14], [15].

Main Result: Let $\epsilon \in (0, 1 - \frac{1}{|\mathcal{X}|}]$ and $p_{XY}, q_{X'Y'} \in \mathcal{P}_{\mathcal{X} \times \mathcal{Y}}$ be such that $\text{TV}(p_{XY}, q_{X'Y'}) \leq \epsilon$. The following inequality holds

$$|H(X|Y) - H(X'|Y')| \leq \epsilon \log(|\mathcal{X}| - 1) + h(\epsilon), \quad (7)$$

where $h(\cdot)$ is the binary entropy function. Moreover, the inequality is tight. This means that for all $\epsilon \in (0, 1 - \frac{1}{|\mathcal{X}|}]$, there exists a pair of probability distributions on $\mathcal{X} \times \mathcal{Y}$ such that the total variation distance between them is ϵ and (7) is saturated.

The mechanics of the proof are based on G-majorization, which refers to a group-induced preorder on a vector space [16], [17]. It is a generalization of Schur majorization, where the group in question is the symmetric group. That is, we say that the vector $q_{X'Y'}$ majorizes the vector p_{XY} whenever p_{XY} is in the convex hull of the orbit of $q_{X'Y'}$ under the action of the symmetric group, where the action is thought of in terms of the natural permutation representation. Since the Shannon entropy is strictly concave and invariant under the action of the symmetric group, this implies $H(XY) \geq H(X'Y')$, i.e., the Shannon entropy is strictly Schur-concave.

Equivocation is not Schur-concave. While it is concave, it is not invariant under the action of the symmetric group. It is, however, invariant under the action of a proper subgroup of the symmetric group. We use this invariance to prove the present result.

II. PROOF

Consider the set $\{p_{XY}(i, j) \mid i \in \mathcal{X}; j \in \mathcal{Y}\}$, where p_{XY} is a bivariate probability distribution. The conditional entropy $H(X|Y)$ associated with p_{XY} is invariant under permutations of j indices, as can be seen from (4). Furthermore, it is invariant under exchanges of the form $(i_1, j) \leftrightarrow (i_2, j) \forall i_1, i_2 \in \mathcal{X}$ and $j \in \mathcal{Y}$. These are the symmetries of the equivocation in X given Y . Denote this subgroup of the symmetric group by $S_{\mathcal{X}|\mathcal{Y}}$.

We note that the bound is monotonic in ϵ for $\epsilon \in (0, 1 - \frac{1}{|\mathcal{X}|}]$, and so we are free to take $\text{TV}(p_{XY}, q_{X'Y'}) = \epsilon$. Moreover, we assume without loss of generality that $H(X|Y) \geq H(X'|Y')$. We proceed in three steps.

A. Reordering

First, we order the components of the bivariate probability distributions in a suggestive way. We arrange the components to be in blocks of $|\mathcal{X}|$ components that share the same Y label. For definiteness, we order the $|\mathcal{Y}|$ blocks such that $q_{Y'}(j) - p_Y(j)$ is in a non-increasing order. For the block labeled by j , we define the two sets:

$$I_j = \{i \mid q_{X'Y'}(i, j) \geq p_{XY}(i, j)\}, \quad (8)$$

$$I_j^c = \{i \mid q_{X'Y'}(i, j) < p_{XY}(i, j)\}. \quad (9)$$

Remark that either of the two sets could be empty, but not both. Within the j th block, if both I_j and I_j^c are nonempty, put the elements of I_j ahead of those in I_j^c . That is, we relabel the components so that $i < i'$ for all $i \in I_j$ and $i' \in I_j^c$. Next, we order the elements of I_j such that $q_{X'Y'}(i, j)$ is non-increasing in i . We do the same for the elements of I_j^c .

B. Walking

The second step involves an optimized form of a proof technique due to Pinelis (see the third answer here [7]). We walk the two probability distributions across the probability simplex until $H(X'|Y') = 0$. In the process, we take care that the difference of equivocations does not decrease and that the total variation distance does not increase.

We start by zooming into the j th block. If I_j is not empty, then we make the following replacements:

$$q_{X'Y'}(1, j) \mapsto q_{X'Y'}(1, j) + [q_{X'Y'}(i, j) - p_{XY}(i, j)], \quad (10)$$

$$q_{X'Y'}(i, j) \mapsto p_{XY}(i, j), \quad (11)$$

consecutively for each $i \in I_j \setminus \{1\}$. If I_j consists of a single element, then such replacements need not be done. By design, these replacements do not affect total variation distance. To see that $H(X'|Y')$ did not increase, we note that the old probability vector is in the convex hull of the orbit of the new vector under the action of $S_{\mathcal{X}|\mathcal{Y}}$. Put another way, the probability weights, conditional on j , are now more concentrated than before. After these replacements are made, the following inequalities will hold:

$$q_{X'Y'}(1, j) - p_{XY}(1, j) \geq 0, \quad (12)$$

$$p_{XY}(i, j) - q_{X'Y'}(i, j) \geq 0, \quad (13)$$

for each $i \in \mathcal{X} \setminus \{1\}$.

Next, we make $H(X'|Y' = j)$ zero by transferring probability weights in the block from the bottom to the top. Specifically, we make the following replacements:

$$q_{X'Y'}(1, j) \mapsto q_{X'Y'}(1, j) + q_{X'Y'}(i, j), \quad (14)$$

$$p_{XY}(1, j) \mapsto p_{XY}(1, j) + q_{X'Y'}(i, j), \quad (15)$$

$$q_{X'Y'}(i, j) \mapsto q_{X'Y'}(i, j) - q_{X'Y'}(1, j), \quad (16)$$

$$p_{XY}(i, j) \mapsto p_{XY}(i, j) - q_{X'Y'}(1, j), \quad (17)$$

consecutively for each $i \in \mathcal{X} \setminus \{1\}$. Note that the transfers were made in both probability distributions to ensure that the total variation distance remains the same. Observe what happens when a probability weight s , suitably small and non-negative, is taken from outcome (i, j) and given to outcome $(1, j)$ in both probability distributions. The difference of entropies changes by the following amount:

$$\begin{aligned} & \{[\eta(q_{X'Y'}(1, j) + s) - \eta(p_{XY}(1, j) + s)] \\ & - [\eta(q_{X'Y'}(1, j)) - \eta(p_{XY}(1, j))]\} \\ & + \{[\eta(p_{XY}(i, j)) - \eta(q_{X'Y'}(i, j))]\} \\ & - [\eta(p_{XY}(i, j) - s) - \eta(q_{X'Y'}(i, j) - s)]\}, \end{aligned}$$

where $\eta(x) = x \log x$. Since it is convex and inequalities (12) and (13) hold, the two differences in curly brackets are not negative. Hence, we can set $q_{X'Y'}(1, j) = q_{Y'}(j)$ and $q_{X'Y'}(i, j) = 0$ for $i \neq 1$. This implies that $H(X'|Y' = j)$ vanishes.

Now, say I_j is empty. Then it holds that $q_{X'Y'}(i, j) - p_{XY}(i, j) < 0$, for all $i \in \mathcal{X}$. It also holds that $q_{X'Y'}(1, j) \geq q_{X'Y'}(2, j) \geq \dots \geq q_{X'Y'}(|\mathcal{X}|, j)$. Our goal is still to take $H(X'|Y' = j)$ to zero. To do this, we increase $q_{X'Y'}(1, j)$ by transferring in probability weights from the rest of the outcomes in the block. As explained before, such transfers can only decrease $H(X'|Y')$. Furthermore, as long as $q_{X'Y'}(1, j) - p_{XY}(1, j) < 0$, these transfers can be done without affecting the total variation distance. If at any point $q_{X'Y'}(1, j) - p_{XY}(1, j) = 0$, we stop as (12) and (13) now hold for this block. In such a case, we start the process mentioned in the previous paragraph. Otherwise, we keep going until $q_{X'Y'}(1, j) = q_{Y'}(j)$.

After all blocks have been processed, we can assume without any loss of generality that $q_{X'Y'}(i, j) = 0$ for all $i \neq 1$. With this in mind, we subject both probability

distributions to a stochastic process that averages over all the blocks. Specifically,

$$\mathcal{E} : \nu_{XY}(i, j) \mapsto \frac{1}{|\mathcal{Y}|} \sum_{j \in \mathcal{Y}} \nu_{XY}(i, j). \quad (18)$$

The stochastic map \mathcal{E} is a convex combination of elements in $S_{\mathcal{X}|\mathcal{Y}}$. This implies that $H(X|Y)$ will not decrease. Of course this processing does not change the fact that $H(X'|Y') = 0$ since only $q_{X'Y'}(1, j)$ are nonzero. Recall that the total variation distance between two distributions does not increase under stochastic maps. Note that the outputs of \mathcal{E} are always product distributions with a uniform marginal on \mathcal{Y} . As for \mathcal{X} , we have the following marginals

$$q_{X'}(1) = 1 \geq p_X(1) \geq 1 - \epsilon \quad (19)$$

$$q_{X'}(i) = 0 \leq p_X(i), \quad (20)$$

for $i \in \mathcal{X} \setminus \{1\}$.

C. Estimating

Since the two distributions can be assumed to be product distributions on $\mathcal{X} \times \mathcal{Y}$, then from here one can invoke the bound for the unconditional case [1] to finish the proof. For the sake of completeness, we include the following rather standard estimates.

Given distributions as in (19) and (20), we can upper-bound $H(X)$ in the following way:

$$\begin{aligned} H(X) &= -p_X(1) \log p_X(1) - \sum_{i \neq 1} p_X(i) \log p_X(i) \\ &\leq -p_X(1) \log p_X(1) \\ &\quad - \sum_{i \neq 1} \frac{(1 - p_X(1))}{|\mathcal{X}| - 1} \log \frac{(1 - p_X(1))}{|\mathcal{X}| - 1} \\ &= (1 - p_X(1)) \log (|\mathcal{X}| - 1) + h((1 - p_X(1))) \\ &\leq \epsilon \log (|\mathcal{X}| - 1) + h(\epsilon) \end{aligned}$$

where the first inequality follows because the vector $(\frac{1 - p_X(1)}{|\mathcal{X}| - 1})_{i=2}^{|\mathcal{X}|}$ is (Schur) majorized by $(p_X(i))_{i=2}^{|\mathcal{X}|}$. The second inequality comes from the monotonicity of the bound. This completes the proof.

To see that the bound is tight, let $\epsilon \in (0, 1 - \frac{1}{|\mathcal{X}'|}]$ be given and consider the following probability distributions.

$$q_{X'Y'}(1, 1) = 1 \quad (21)$$

$$p_{XY}(1, 1) = 1 - \epsilon \quad \text{and} \quad p_{XY}(i, 1) = \frac{\epsilon}{|\mathcal{X}'| - 1}, \quad (22)$$

for $i \in \mathcal{X} \setminus \{1\}$. Evidently, the two are separated by ϵ in total variation distance and the associated equivocations saturate the bound.

III. CONCLUDING REMARKS

We have presented a proof of a tight uniform continuity bound for the conditional Shannon entropy. The bound is independent of the alphabet size of the conditioning system. However, we have assumed in the proof that the conditioning system has finite support. It would be interesting to prove the bound without such an assumption, but we leave that as an open problem.

The proof depends crucially on the invariance of $H(X|Y)$ under the action of $S_{\mathcal{X}|\mathcal{Y}}$. Various forms of conditional Rényi entropies share this invariance [18], [19]. More generally, entropic quantities of interest are invariant under the action of some subgroup of the symmetric group. For example, the mutual information $I(X; Y) = H(X) + H(Y) - H(XY)$ is invariant under "local" permutations of indices, i.e., tensor products of permutations of X and Y labels. We believe such symmetries provide a path towards a better understanding of the behaviors of the corresponding quantities in terms of continuity and beyond.

ACKNOWLEDGMENT

We thank Shawn Geller, Alexander Kwiatkowski, Felix Jimenez, Felix Leditzky and Emanuel Knill for useful discussions and insightful comments regarding the manuscript. GS was supported by NSF CAREER award CCF 1652560.

REFERENCES

- [1] Z. Zhang, "Estimating mutual information via kolmogorov distance," *IEEE Transactions on Information Theory*, vol. 53, no. 9, pp. 3280–3282, Sep. 2007.
- [2] S. Ho and R. W. Yeung, "The interplay between entropy and variational distance," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 5906–5929, Dec 2010.
- [3] I. Sason, "Entropy bounds for discrete random variables via maximal coupling," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7118–7131, Nov 2013.
- [4] M. Fannes, "A continuity property of the entropy density for spin lattice systems," *Comm. Math. Phys.*, vol. 31, no. 4, pp. 291–294, 1973. [Online]. Available: <https://projecteuclid.org:443/euclid.cmp/1103859037>
- [5] K. M. R. Audenaert, "A sharp continuity estimate for the von neumann entropy," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 28, pp. 8127–8136, jun 2007. [Online]. Available: <https://doi.org/10.1088%2F1751-8113%2F40%2F28%2Fs18>
- [6] E. P. Hanson and N. Datta, "Maximum and minimum entropy states yielding local continuity bounds," *Journal of Mathematical Physics*, vol. 59, no. 4, p. 042204, 2018. [Online]. Available: <https://doi.org/10.1063/1.5000120>
- [7] I. Pinelis, "Entropy and total variation distance (answer)," MathOverflow, visited on 2019-08-03. [Online]. Available: <https://mathoverflow.net/questions/310689/entropy-and-total-variation-distance>
- [8] A. Winter, "Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints," *Communications in Mathematical Physics*, vol. 347, no. 1, pp. 291–313, Oct 2016. [Online]. Available: <https://doi.org/10.1007/s00220-016-2609-8>
- [9] E. P. Hanson and N. Datta, "Tight uniform continuity bound for a family of entropies," 2017.
- [10] R. Alicki and M. Fannes, "Continuity of quantum conditional information," *Journal of Physics A: Mathematical and General*, vol. 37, no. 5, pp. L55–L57, jan 2004. [Online]. Available: <https://doi.org/10.1088%2F0305-4470%2F37%2F5%2F01>
- [11] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. New York, NY, USA: Wiley-Interscience, 2006.
- [12] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1216–1227, May 1999.
- [13] D. Leung and G. Smith, "Continuity of quantum channel capacities," *Communications in Mathematical Physics*, vol. 292, no. 1, pp. 201–215, Nov 2009. [Online]. Available: <https://doi.org/10.1007/s00220-009-0833-1>
- [14] M. E. Shirokov, "Tight uniform continuity bounds for the quantum conditional mutual information, for the holevo quantity, and for capacities of quantum channels," *Journal of Mathematical Physics*, vol. 58, no. 10, p. 102202, 2017. [Online]. Available: <https://doi.org/10.1063/1.4987135>
- [15] D. Sutter, V. B. Scholz, A. Winter, and R. Renner, "Approximate degradable quantum channels," *IEEE Transactions on Information Theory*, vol. 63, no. 12, pp. 7832–7844, Dec 2017.
- [16] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and its Applications*, 2nd ed. Springer, 2011, vol. 143.
- [17] A. Steerneman, "G-majorization, group-induced cone orderings, and reflection groups," *Linear Algebra and its Applications*, vol. 127, pp. 107 – 119, 1990. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/002437959090338D>
- [18] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, 1st ed. Springer Publishing Company, Incorporated, 2015.

[19] S. Arimoto, “Information measures and capacity of order α for discrete memoryless channels,” *Topics in Information Theory*, 1977. [Online]. Available: <https://ci.nii.ac.jp/naid/10022581674/en/>