New quantum Rényi divergences and their application to device-independent cryptography and quantum Shannon theory[a]

Peter Brown,[1] Hamza Fawzi,[2] and Omar Fawzi[1]

[1] *Univ Lyon, ENS Lyon, UCBL, CNRS, LIP, F-69342, Lyon Cedex 07, France*
[2] *DAMTP, University of Cambridge, United Kingdom*

In the analysis of quantum information processing tasks, the choice of distance measure between states or channels often plays a crucial role. This submission introduces new quantum Rényi divergences for states and channels that are based on a convex optimization program involving the matrix geometric mean. These divergences have mathematical and computational properties that make them applicable to a wide variety of problems. We use these Rényi divergences to obtain semidefinite programming lower bounds on the key rates for device-independent cryptography, and in particular we find a new bound on the minimal detection efficiency required to perform device-independent quantum key distribution without additional noisy preprocessing. Furthermore, we give several applications to quantum Shannon theory, in particular proving that adaptive strategies do not help in the strong converse exponent regime for quantum channel discrimination and obtaining improved bounds for quantum capacities.

Introduction

Rényi divergences are useful information theoretic measures of distinguishability, finding operational significance in characterizing the rates of various tasks such as hypothesis testing [3–5]. Moreover, they can be used to define entropic quantities like conditional entropies or measures of mutual information which in turn find their own operational meanings. In previous works, several different families of quantum Rényi divergences have been defined and studied including the sandwiched divergences [6, 7], the Petz divergences [8] and the geometric divergences [9]. Even though all these families match for classical states, they have different properties in the quantum setting that make them suited for different applications. For example, the sandwiched divergences had a crucial impact on the security proofs in the device-independent (DI) setting [10, 11]. Also, the geometric divergences were recently shown to have useful properties for channels [12] which led to many improved bounds on quantum capacities. In this work, we introduce two new families of Rényi divergences which are defined in terms of convex optimization problems and provide applications to device-independent cryptography and quantum Shannon theory.

Techniques

The first family, which we refer to as the *iterated mean divergences*, is designed so that it can be combined with the NPA hierarchy [23] to compute lower bounds on the rates of various device-independent protocols. It is defined for Rényi parameters $\alpha = 1 + \frac{1}{2^k - 1}$, where k is a positive integer, in terms of a semidefinite program with a number of variables that is linear in k. We refer to the full manuscript [1] for a definition of iterated mean divergences, but the key property for the applications is that, when written as a maximization, the divergence between the states ρ and σ can be expressed in terms of

$$\max_{V_1, V_2, \ldots, V_m} \operatorname{Tr}[V_1 \rho] + \operatorname{Tr}[V_2 \sigma] \ , \tag{1}$$

where the variables $V_1, \ldots, V_m$ are subject to noncommutative Hermitian polynomial constraints that are *independent of the dimension* of the states ρ and σ. This property can be shown to hold for the geometric divergences, but it is not known if such a property holds for the Petz or sandwiched divergences. As the geometric divergence can sometimes behave like the "worst-case" quantity $D_{\max}$ (in particular when ρ is

[a] This submission is based on the articles [1] and [2]

pure) we introduce the iterated mean divergence which cannot be larger than the geometric divergence and in general gives better bounds.

The second family of divergences is defined for all $\alpha > 1$ as

$$D_\alpha^{\#}(\rho\|\sigma) = \frac{1}{\alpha - 1} \log \min_{A \geq 0} \mathrm{Tr}\left[A\right] \quad \text{s.t.} \quad \rho \leq \sigma \#_{\frac{1}{\alpha}} A \ , \tag{2}$$

for any positive operators ρ and σ, where $\#_{\frac{1}{\alpha}}$ denotes the weighted matrix geometric mean. This divergence has several desirable computational and operational properties such as an efficient semidefinite programming representation for states and channels (when α is rational), and a chain rule property [2]. An important property of this new divergence is that by evaluating it on tensor powers, it gives a converging hierarchy of upper bounds on the sandwiched Rényi divergence. This also holds for quantum channels provided we take the regularized sandwiched Rényi divergence and this allows us to show that approximating the regularized sandwiched Rényi divergence is computable. This gives an interesting example of a nonadditive quantum entropic quantity whose regularization can still be computed. We hope that our methods can shed light on the computability of the many regularized quantities that appear in Shannon theory such as the quantum capacity.

These two families of divergences are very related. In fact, when $\alpha = 2$, they are equal. In addition, the second family can be shown to have the key property described in (1), but the iterated mean divergences, which when written in the dual minimization form closely resemble (2),[1] lead to better bounds in general for device-independent cryptography.

Application to DI cryptography

Device-independent cryptography enables the secure execution of cryptographic tasks on untrusted devices. Many of these schemes are possible due to the strong restrictions that Bell-inequality violations impose on the generating systems. For example, it is possible to construct randomness generation (RNG) [13–15] and key distribution (QKD) protocols [16] with device-independent security. Moreover, recent works have managed to develop the first rigorous security proofs against general quantum adversaries [11, 17, 18]. With the advent of theoretical tools such as the entropy accumulation theorem (EAT) [19, 20] and quantum probability estimation [21], proving security now has a fairly regimented structure [17].

The central problem that remains for the analysis and security proofs of new DI protocols is the question of how to calculate the *rate*. I.e., in DI-RNG how much randomness is generated or in DI-QKD how much secret key is generated per use of the device. For many DI protocols, including DI-RNG and DI-QKD, this problem reduces to minimizing the conditional von Neumann entropy over a set of quantum states that are characterized by restrictions on the correlations they can produce. Unfortunately, directly computing such an optimization is a highly non-trivial task due to both the fact that the problem is non-convex and that, as we are working device-independently, we cannot assume any a priori bound on the dimensions of the systems used within the protocol.

In this work we show that the iterated mean divergences can be used to compute lower bounds on the rates of device-independent protocols. More specifically, using the property described in (1), we show the corresponding conditional entropies defined via the iterated mean divergences may be written as noncommutative polynomial optimization problem, the structure of which is independent of the dimension of the systems. With such a form we are able to relax the device-independent optimization of our conditional entropies to a semidefinite program using the NPA hierarchy [23]. Finally, as the iterated mean conditional entropies are always no larger than the conditional von Neumann entropy, the results of our optimizations can be used to lower bound the rates of protocols.

We apply these conditional entropies to compute the rates device independent randomness expansion and quantum key distribution protocols. We compare the rates found with our method to an analytical bound [22] for protocols based on the CHSH game, rates computed using the min-entropy [24–26] and rates

[1] In the iterated mean divergence, the weighted matrix geometric mean in (2) is replaced by an iterated application of the matrix geometric mean, which explains the name.

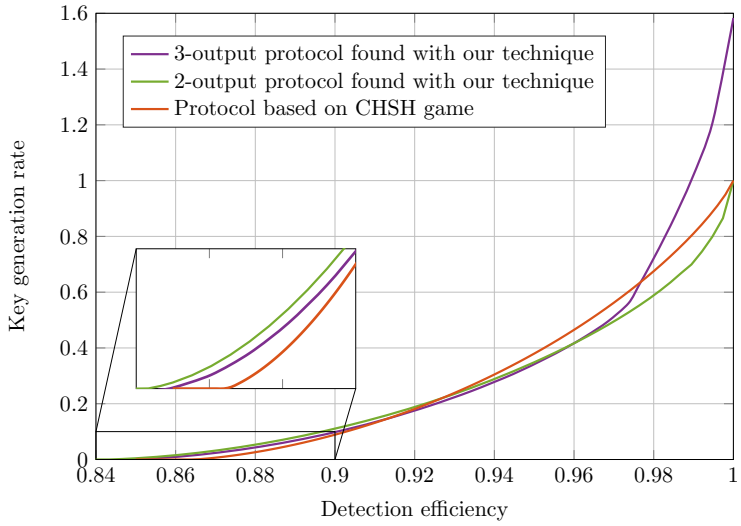

Figure 1. **Comparing key-rates of DIQKD protocols without noisy preprocessing.** We compare the asymptotic key-rates of a DI-QKD protocol based on the CHSH game [17, 22], a DI-QKD protocol for 2-input 2-output devices and a DI-QKD protocol for 2-input 3-output devices when the respective devices used in the protocol are subject to inefficient detectors. Note that the key-rates for the 3-output protocol can be smaller than the 2-output protocol in the regime of high noise as they were evaluated using different entropies from the iterated mean family.

computed using the recent numerical method developed in [27]. We find improvements in various scenarios over all previous methods. For example, the efficiency of our method allowed us to optimize over a family of two-input two-output QKD protocols. In doing so we found a new upper bound on the minimal detection efficiency required to perform DI-QKD with a two qubit system when we don't have an additional noisy preprocessing of the raw key [28, 29] (see Figure 1).[2] Finally, we demonstrate that our method can be used directly with the entropy accumulation theorem (EAT) [19, 20] by constructing explicit min-tradeoff functions from the solutions of our optimizations. Applying the security proof blueprints developed in [11, 17] our techniques can be readily used together with the EAT to construct complete security proofs of many DI protocols and compute finite round rates.

Application to quantum channel discrimination

For this abstract, we focus on an application to the task of quantum channel discrimination and we refer to the manuscript [2] for further applications. Imagine we would like to distinguish between two quantum channels $\mathcal{N}$ and $\mathcal{M}$ having black box access to n uses of one of them. The task of adaptive channel discrimination is to decide which channel we are dealing with. The word adaptive here refers to the fact that our use of one of the black boxes can depend on the outcomes of a previously used black box. By contrast, a strategy is called parallel (or nonadaptive) if the n black boxes are used in parallel on a fixed input state.

Channel discrimination is a fundamental task that has been studied in various contexts and there are multiple works that investigate the advantages that can be offered by adaptive strategies over parallel ones. In some regimes, we know that adaptive strategies can offer an advantage [30–32] whereas in some other settings, adaptive strategies do not help [33–35]. As an application of our new divergences, we establish a new regime where adaptive strategies do not offer an advantage for the task of channel discrimination: the asymptotic strong converse exponent regime for asymmetric hypothesis testing. In fact, we even characterize the strong converse exponent in this regime. The key properties that we used to achieve this result is a new chain rule for the sandwiched Rényi divergence which follows easily from the chain rule $D^{\#}_{\alpha}$, together with the explicit convergence bounds for the regularized sandwiched Rényi divergence that we obtain using $D^{\#}_{\alpha}$.

[2] Recently it was shown in [28, 29] that the minimal detection efficiency required to produce key in a CHSH based protocol could be lowered by the addition of noise to the raw key. We do not take such a protocol modification into account here.

[1] P. Brown, H. Fawzi, and O. Fawzi, "Computing conditional entropies for quantum correlations," *Preprint at arXiv:2007.12575*, 2020.

[2] H. Fawzi and O. Fawzi, "Defining quantum divergences via convex optimization," *Preprint at arXiv:2007.12576*, 2020.

[3] F. Hiai and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Communications in mathematical physics*, vol. 143, no. 1, pp. 99–114, 1991.

[4] T. Ogawa and H. Nagaoka, "Strong converse and stein's lemma in quantum hypothesis testing," in *Asymptotic Theory Of Quantum Statistical Inference: Selected Papers*, pp. 28–42, World Scientific, 2005.

[5] M. Mosonyi and T. Ogawa, "Quantum hypothesis testing and the operational interpretation of the quantum rényi relative entropies," *Communications in Mathematical Physics*, vol. 334, no. 3, pp. 1617–1648, 2015.

[6] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *Journal of Mathematical Physics*, vol. 54, p. 122203, 2013.

[7] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched rényi relative entropy," *Communications in Mathematical Physics*, vol. 331, no. 2, pp. 593–622, 2014.

[8] D. Petz, "Quasi-entropies for finite quantum systems," *Reports on Mathematical Physics*, vol. 23, pp. 57–65, 1986.

[9] K. Matsumoto, "A new quantum version of f-divergence," in *Nagoya Winter Workshop: Reality and Measurement in Algebraic Quantum Theory*, pp. 229–273, Springer, 2015.

[10] C. A. Miller and Y. Shi, "Universal security for randomness expansion from the spot-checking protocol," *SIAM Journal on Computing*, vol. 46, no. 4, pp. 1304–1335, 2017.

[11] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature communications*, vol. 9, no. 1, p. 459, 2018.

[12] K. Fang and H. Fawzi, "Geometric Rényi divergence and its applications in quantum channel capacities," *Preprint at arXiv:1909.05758*, 2019.

[13] R. Colbeck, *Quantum and Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2007. Also available as arXiv:0911.3814.

[14] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *Journal of Physics A*, vol. 44, no. 9, p. 095305, 2011.

[15] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, pp. 1021–1024, 2010.

[16] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[17] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs," *SIAM Journal on Computing*, vol. 48, no. 1, pp. 181–225, 2019.

[18] Y. Zhang, H. Fu, and E. Knill, "Efficient randomness certification by quantum probability estimation," *Phys. Rev. Research*, vol. 2, p. 013016, Jan 2020.

[19] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," *Communications in Mathematical Physics*, vol. 379, pp. 1–47, 2020.

[20] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order term," *IEEE Transactions on information theory*, vol. 65, no. 11, pp. 7596–7612, 2019.

[21] E. Knill, Y. Zhang, and H. Fu, "Quantum probability estimation for randomness with quantum side information." e-print arXiv:1806.04553, 2018.

[22] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, no. 4, p. 045021, 2009.

[23] S. Pironio, M. Navascués, and A. Acín, "Convergent relaxations of polynomial optimization problems with noncommuting variables," *SIAM Journal on Optimization*, vol. 20, no. 5, pp. 2157–2180, 2010.

[24] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4337–4347, 2009.

[25] J.-D. Bancal, L. Sheridan, and V. Scarani, "More randomness from the same data," *New Journal of Physics*, vol. 16, no. 3, p. 033011, 2014.

[26] O. Nieto-Silleras, S. Pironio, and J. Silman, "Using complete measurement statistics for optimal device-independent randomness evaluation," *New Journal of Physics*, vol. 16, no. 1, p. 013035, 2014.

[27] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, "Computing secure key rates

for quantum key distribution with untrusted devices," *Preprint at arXiv:1908.11372*, 2019.
[28] M. Ho, P. Sekatski, E.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, "Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution," *Physical Review Letters*, vol. 124, no. 23, p. 230502, 2020.
[29] E. Woodhead, A. Acín, and S. Pironio, "Device-independent quantum key distribution based on asymmetric CHSH inequalities," *Preprint at arXiv:2007.16146*, 2020.
[30] R. Duan, Y. Feng, and M. Ying, "Perfect distinguishability of quantum operations," *Phys. Rev. Lett.*, vol. 103, p. 210501, Nov 2009.
[31] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, "Adaptive versus nonadaptive strategies for quantum channel discrimination," *Phys. Rev. A*, vol. 81, p. 032339, Mar 2010.
[32] D. Puzzuoli and J. Watrous, "Ancilla dimension in quantum channel discrimination," *Annales Henri Poincaré*, vol. 18, pp. 1153–1184, Apr 2017.
[33] M. Hayashi, "Discrimination of two channels by adaptive methods and its application to quantum system," *IEEE Transactions on Information Theory*, vol. 55, no. 8, pp. 3807–3820, 2009.
[34] M. Berta, C. Hirche, E. Kaur, and M. M. Wilde, "Amortized channel divergence for asymptotic quantum channel discrimination," 2018. arXiv:1808.01498.
[35] K. Fang, O. Fawzi, R. Renner, and D. Sutter, "Chain rule for the quantum relative entropy," *Physical Review Letters*, vol. 124, no. 10, p. 100501, 2020.