Entropy accumulation with improved second-order term

Frederic Dupuis, Omar Fawzi

Entropy accumulation with improved second-order term

Frédéric Dupuis and Omar Fawzi

Abstract

The entropy accumulation theorem [1] states that the smooth min-entropy of an n-partite system $A = (A_1, \ldots, A_n)$ is lower-bounded by the sum of the von Neumann entropies of suitably chosen conditional states up to corrections that are sublinear in n. This theorem is particularly suited to proving the security of quantum cryptographic protocols, and in particular so-called device-independent protocols for randomness expansion and key distribution, where the devices can be built and preprogrammed by a malicious supplier [2]. However, while the bounds provided by this theorem are optimal in the first order, the second-order term is bounded more crudely, in such a way that the bounds deteriorate significantly when the theorem is applied directly to protocols where parameter estimation is done by sampling a small fraction of the positions, as is done in most QKD protocols. The objective of this paper is to improve this second-order sublinear term and remedy this problem. On the way, we prove various bounds on the divergence variance, which might be of independent interest.

Index Terms

Quantum information theory, Cryptography

I. Introduction

There are many protocols in quantum cryptography, such as quantum key distribution, that work by generating randomness. Such protocols usually proceed as follows: we perform a basic subprotocol n times (for example, sending a photon in a random polarization from Alice to Bob), we then gather statistics about the protocol run (for example, we compute the error rate from a randomly chosen sample of the rounds), and we then conclude that the final state contains a certain amount of randomness, which can then be processed further. Mathematical tools that can quantify the amount of randomness produced by quantum processes therefore constitute the centerpiece of many security proofs in quantum cryptography. The entropy accumulation theorem [1] provides such a powerful tool that applies to a very general class of protocols, including device-independent protocols.

Informally, the main result of [1] is the following. Suppose we have an n-step quantum process like the one depicted in Figure 1, in which we start with a bipartite state $\rho_{R_0 E}$ and the R_0 share of the state undergoes an n step process specified by the quantum channels $\mathcal{M}_1$ to $\mathcal{M}_n$. At step i of the process, two quantum systems A_i and B_i are produced, from which one can extract a *classical* random variable X_i. The goal is then to bound the amount of randomness present in A_1^n given B_1^n, conditioned on the string X_1^n being in a certain set Ω. The X_i's are meant to represent the data we do statistics on, for example X_i might tell us that there is an error at position i, and we want to condition on the observed error rate being below some threshold. Stated informally, the statement proven in [1] is then

$$H_{\min}^{\varepsilon}(A_1^n | B_1^n E, X_1^n \in \Omega)_\rho \geqslant n \left(\inf_{q \in \Omega} f(q) \right) - \sqrt{n} c. \tag{1}$$

Here, the smooth min-entropy $H_{\min}^{\varepsilon}$ represents the amount of extractable randomness (see Definition II.8), the *tradeoff function* $f(q)$ quantifies the worst-case amount of entropy produced by one step of the process for an input state that is consistent with observing the statistics q, and c is a number that depends on ε, the event Ω and the tradeoff function f but not on n. One would then apply this theorem by replacing the $\mathcal{M}_i$'s by one step of the cryptographic protocol to obtain the desired bound. This is done, for example, in [2], [3] for device-independent randomness expansion and quantum key distribution.

While this method yields optimal bounds in the first order, the second-order term which scales as $\sqrt{n}$ is bounded more crudely, and for some applications, this term can become dominant very quickly. This is particularly the case in applications which estimate the amount of entropy produced by testing a small fraction of the positions, which includes a large number of protocols of interest. The reason for this is that the value of c in Equation (1) is proportional to the gradient of f. Now, suppose that we have a protocol where we are testing positions with probability $O(1/n)$; in general this will make the gradient of f proportional to n[1] and therefore the second-order term will become $\Omega(n^{3/2})$ and overwhelm the first-order term. This is

F. Dupuis is with the Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France.
O. Fawzi is with the Université de Lyon, ENS de Lyon, CNRS, UCBL, LIP, F-69342, Lyon Cedex 07, France.
Manuscript received XXXXX.

[1]Without getting into details, the tradeoff function f often takes the form $f(p) = g(\frac{p(1)}{\gamma})$, where p is a distribution on $\{0, 1\}$ and γ is the testing probability and g is a fixed affine function. As such if $\gamma = O(\frac{1}{n})$, the gradient of f is $\Omega(n)$. We refer the reader to [2], [3] or Section VI of this paper for more details on this.

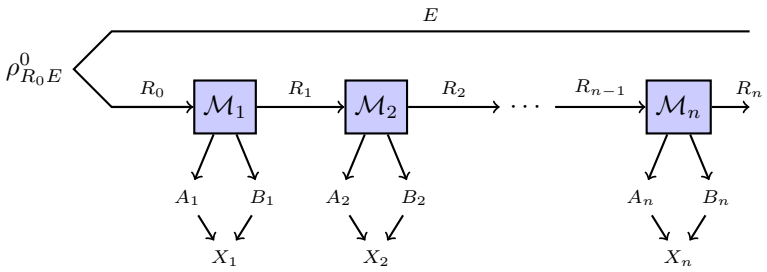

Fig. 1. Illustration of the type of process that the entropy accumulation theorem applies to.

worse than we would expect: when we perform the analysis using conventional tools such as Chernoff-Hoeffding bounds in cases that are amenable to it, we obtain a much better scaling behavior, and in particular we still expect a non-trivial bound when the testing rate is $O(1/n)$. As a further indication that the second-order term can be improved, we also note that in [2, Appendix B], they resort to applying the entropy accumulation theorem to blocks rather than single rounds in order to obtain a good dependence on the testing rate.

The goal of this paper is therefore to improve the second-order term in (1). Analyzing second-order correction terms is already commonplace in information theory ever since the 60s, with the work of Volker Strassen [4] who gave second-order bounds for hypothesis testing and channel coding. This topic has also seen a revival more recently [5]–[7]. Quantum versions of such bounds have been proven as well since then; for example, Li [8] and Tomamichel and Hayashi [9] have shown a second-order expansion for quantum hypothesis testing, and [9] additionally gives second-order expansions for several other entropic quantities of interest. Other more recent developments can also be found in [10]–[16].

Most of these results go one step further than we will in this paper, in that they pin down the $O(\sqrt{n})$ term *exactly*, usually by employing some form of the Berry-Esseen theorem to a carefully designed classical random variable. Unfortunately, this approach seems to fail here, and we must resort to slightly weaker bounds that nevertheless give the right scaling behavior for protocols with infrequent sampling, and that are largely good enough in practice.

a) Paper organization: : In Section II, we give the notation used and some preliminary facts needed for the rest of the paper, including the Rényi entropy chain rule that powers the original entropy accumulation result in Section II-C. Section III then introduces the *divergence variance* which governs the form of the second-order term, and discusses some of its properties. In Section IV, we present a new bound for the Rényi entropy in terms of the von Neumann entropy, and then apply it to the entropy accumulation theorem in Section V, with specific bounds for the case of protocols with infrequent sampling in Section V-A. We then compute finite-block-size bounds for the particular application of device-independent randomness expansion in Section VI and conclude with some open problems in Section VII.

II. Preliminaries

A. Notation

In the table below, we summarize some of the notation used throughout the paper:

Symbol	*Definition*
$A, B, C, \ldots$	Quantum systems, and their associated Hilbert spaces
$\mathcal{L}(A, B)$	Set of linear operators from A to B
$\mathcal{L}(A)$	$\mathcal{L}(A, A)$
X_{AB}	Operator in $\mathcal{L}(A \otimes B)$
$\mathcal{I}_A$	Identity map from $\mathcal{L}(A)$ to itself
$\mathcal{M}_{A\to B}$	The subscript $A \to B$ is to indicate that $\mathcal{M}$ is a linear map from $\mathcal{L}(A)$ to $\mathcal{L}(B)$
$\mathrm{D}(A)$	Set of normalized density operators on A
$X_A \geqslant Y_A$	$X_A - Y_A$ is positive semidefinite
A_i^j (with $j \geqslant i$)	Given n systems $A_1, \ldots, A_n$, this is a shorthand for $A_i, \ldots, A_j$
A^n	Often used as shorthand for $A_1, \ldots, A_n$
$\log(x)$	Logarithm of x in base 2
$\mathrm{Var}(X)$	Variance of the random variable X
$\mathrm{Cov}(X, Y)$	Covariance of the random variables X and Y
$D_\alpha(\rho\|\sigma)$	Sandwiched Rényi divergence (Definition II.3)
$D'_\alpha(\rho\|\sigma)$	Petz Rényi divergence (Definition II.4)
$H_\alpha(A\|B)_\rho$	$-D_\alpha(\rho_{AB}\|\mathrm{id}_A \otimes \rho_B)$
$H_\alpha^\uparrow(A\|B)_\rho$	$-\inf_{\sigma_B} D_\alpha(\rho_{AB}\|\mathrm{id}_A \otimes \sigma_B)$
$H'_\alpha(A\|B)_\rho$	$-D'_\alpha(\rho_{AB}\|\mathrm{id}_A \otimes \rho_B)$
$D_{\min}(\rho\|\sigma)$	$D_{\frac{1}{2}}(\rho\|\sigma)$
$D_{\max}(\rho\|\sigma)$	$D_\infty(\rho\|\sigma)$
$V(\cdot)$	Various divergence variance measures; see Section III

B. Entropic quantities

The central mathematical tools used in this paper are entropic quantities, i.e. various ways of quantifying the amount of uncertainty present in classical or quantum systems. In this section, we give definitions for the quantities that will play a role in our results.

Definition II.1 (Relative entropy)**.** For any positive semidefinite operators ρ and σ, the *relative entropy* is defined as

$$D(\rho\|\sigma) = \begin{cases} \frac{1}{\mathrm{tr}[\rho]}\mathrm{tr}[\rho(\log\rho - \log\sigma)] & \text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ \infty & \text{otherwise} \end{cases}.$$

Definition II.2 (von Neumann entropy)**.** Let $\rho_{AB} \in \mathrm{D}(AB)$ be a bipartite density operator. Then, the *conditional von Neumann entropy* is defined as

$$H(A|B)_\rho = -D(\rho_{AB}\|\mathrm{id}_A \otimes \rho_B).$$

Our proofs heavily rely on two versions of the Rényi relative entropy: the one first introduced by Petz [17], and the "sandwiched" version introduced in [18], [19]. We define both of these here:

Definition II.3 (Sandwiched Rényi divergence)**.** Let ρ be a quantum state, let σ be positive semidefinite, and let $\alpha \in [\frac{1}{2}, \infty]$. Then, the sandwiched Rényi divergence is defined as

$$D_\alpha(\rho\|\sigma) = \begin{cases} \frac{1}{\alpha-1}\log\mathrm{tr}\left[\left(\sigma^{-\frac{\alpha'}{2}}\rho\sigma^{-\frac{\alpha'}{2}}\right)^\alpha\right] & \text{if } \alpha < 1 \text{ or } \alpha > 1 \text{ and } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ \log\inf\{\lambda : \rho \leqslant \lambda\sigma\} & \text{if } \alpha = \infty \\ D(\rho\|\sigma) & \text{if } \alpha = 1 \\ \infty & \text{otherwise,} \end{cases} \tag{2}$$

where $\alpha' := \frac{\alpha-1}{\alpha}$. Note D_∞ is also referred to as $D_{\max}$ and $D_{\frac{1}{2}}$ as $D_{\min}$.

Definition II.4 (Petz Rényi divergence)**.** Let ρ be a quantum state, let σ be positive semidefinite, and let $\alpha \in [0, 2]$. Then, the Petz Rényi divergence is defined as

$$D'_\alpha(\rho\|\sigma) = \begin{cases} \frac{1}{\alpha-1}\log\mathrm{tr}\left[\rho^\alpha\sigma^{1-\alpha}\right] & \text{if } 0 < \alpha < 1 \text{ or } 1 < \alpha \leqslant 2 \text{ and } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ -\log\mathrm{tr}[\Pi_{\mathrm{supp}(\rho)}\sigma] & \text{if } \alpha = 0 \\ D(\rho\|\sigma) & \text{if } \alpha = 1 \\ \infty & \text{otherwise,} \end{cases} \tag{3}$$

where $\Pi_{\mathrm{supp}(\rho)}$ is the projector on the support of ρ.

These relative entropies can be used to define a conditional entropy:

Definition II.5 (Sandwiched Rényi conditional entropy)**.** For any density operator ρ_{AB} and for $\alpha \in [\frac{1}{2}, \infty]$ the *sandwiched α-Rényi entropy of A conditioned on B* is defined as

$$H_\alpha(A|B)_\rho = -D_\alpha(\rho_{AB}\|\mathrm{id}_A \otimes \rho_B).$$

Note that we also refer to $H_\infty(A|B)_\rho$ as $H_{\min}(A|B)_{\rho|\rho}$.

It turns out that there are multiple ways of defining conditional entropies from relative entropies. Another variant that will be needed in this work is the following:

Definition II.6. For any density operator ρ_{AB} and for $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty]$, we define

$$H_\alpha^\uparrow(A|B)_\rho = -\inf_{\sigma_B} D_\alpha(\rho_{AB}\|\mathrm{id}_A \otimes \sigma_B)$$

where the infimum is over all subnormalized density operators on B. Note that we also refer to $H_\infty^\uparrow(A|B)_\rho$ as $H_{\min}(A|B)_\rho$, called the *min-entropy*, and to $H_{\frac{1}{2}}^\uparrow(A|B)_\rho$ as $H_{\max}(A|B)_\rho$, called the *max-entropy*.

Finally, in the case of the min- and max-entropy, we will also need "smooth" versions. These are versions of the min- and max-entropy where we compute the entropy for the best state within ε of the actual state, where the distance is given by the purified distance. We begin by defining the purified distance [20]–[25]:

Definition II.7 (Purified distance)**.** Let ρ and σ be two subnormalized density operators. Then, the purified distance between ρ and σ is given by

$$P(\rho, \sigma) := \sqrt{1 - \left(\|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \mathrm{tr}[\rho])(1 - \mathrm{tr}[\sigma])}\right)^2}.$$

Note that this reduces to $P(\rho, \sigma) = \sqrt{1 - \|\sqrt{\rho}\sqrt{\sigma}\|_1^2}$ whenever either ρ or σ is normalized. We are now ready to define the smooth min- and max-entropy:

Definition II.8. For any density operator ρ_{AB} and for $\varepsilon \in [0, 1]$ the *ε-smooth min- and max-entropies of A conditioned on B* are given by:

$$H_{\min}^\varepsilon(A|B)_\rho = \sup_{\tilde{\rho}: P(\rho,\tilde{\rho}) \leqslant \varepsilon} H_{\min}(A|B)_{\tilde{\rho}}$$
$$H_{\max}^\varepsilon(A|B)_\rho = \inf_{\tilde{\rho}: P(\rho,\tilde{\rho}) \leqslant \varepsilon} H_{\max}(A|B)_{\tilde{\rho}}.$$

respectively, where $\tilde{\rho}$ is any subnormalized density operator that is ε-close to ρ in terms of the purified distance [24], [25].

C. Chain rule for Rényi entropies

In [1], the central piece of the proof was a chain rule for Rényi entropies. As our proof largely follows the same steps, we reproduce the most relevant statement here for the reader's convenience. For the proofs, we refer the reader to [1]. An important property of a tripartite state ρ_{ABC} that we will be using throughout the paper is the Markov chain condition written $A \leftrightarrow B \leftrightarrow C$ and defined by $I(A : C|B)_\rho = 0$.

Corollary II.9 (Corollary 3.4 in [1])**.** *Let $\rho^0_{RA_1B_1}$ be a density operator on $R \otimes A_1 \otimes B_1$ and $\mathcal{M}$ be a trace-preserving completely-positive map from $\mathcal{L}(R)$ to $\mathcal{L}(A_2 \otimes B_2)$. Assuming that $\rho_{A_1B_1A_2B_2} = (\mathcal{M} \otimes \mathcal{I}_{A_1B_1})(\rho^0_{RA_1B_1})$ satisfies the Markov condition $A_1 \leftrightarrow B_1 \leftrightarrow B_2$, we have for $\alpha \in [\frac{1}{2}, \infty)$*

$$\inf_\omega H_\alpha(A_2|B_2A_1B_1)_{\mathcal{M}(\omega)} \leqslant H_\alpha(A_1A_2|B_1B_2)_{\mathcal{M}(\rho^0)} - H_\alpha(A_1|B_1)_{\rho^0} \leqslant \sup_\omega H_\alpha(A_2|B_2A_1B_1)_{\mathcal{M}(\omega)}$$

where the supremum and infimum range over density operators $\omega_{RA_1B_1}$ on $R \otimes A_1 \otimes B_1$. Moreover, if $\rho^0_{RA_1B_1}$ is pure then we can optimise over pure states $\omega_{RA_1B_1}$.

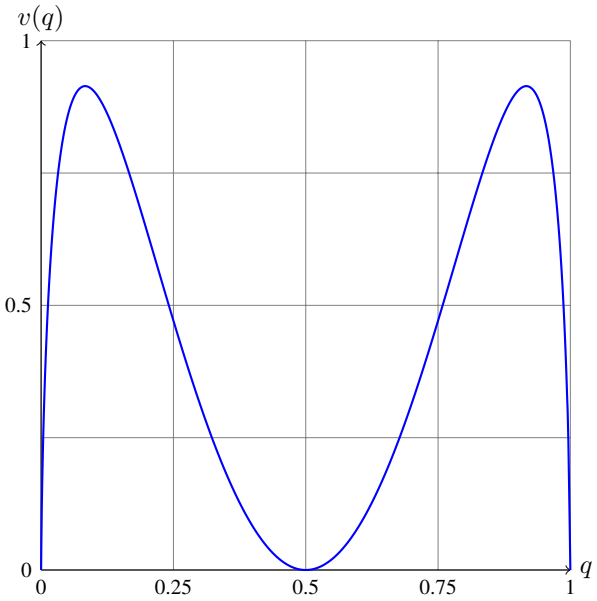

Fig. 2. Plot of $v(q) = V(X)$, where X is a Bernoulli RV with $\Pr[X = 0] = q$. It peaks at around $v(0.083) \approx 0.9142$.

III. The quantum divergence variance and its properties

The second-order term in our main result will be governed by a quantity called the quantum divergence variance, defined as follows:

Definition III.1 (Quantum divergence variance)**.** Let ρ, σ be positive semidefinite operators such that $D(\rho\|\sigma)$ is finite (i.e. $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma)$). Then, the quantum divergence variance $V(\rho\|\sigma)$ is defined as:

$$\begin{aligned} V(\rho\|\sigma) &:= \frac{1}{\operatorname{tr}[\rho]} \operatorname{tr}\left[\rho(\log\rho - \log\sigma - \mathrm{id} D(\rho\|\sigma))^2\right] \\ &= \frac{1}{\operatorname{tr}[\rho]} \operatorname{tr}\left[\rho(\log\rho - \log\sigma)^2\right] - D(\rho\|\sigma)^2. \end{aligned}$$

This was already defined in [9] and [8] under the names "quantum information variance" and "quantum relative variance" respectively; we instead choose a different name to clearly mark its relation to the divergence and to avoid confusion with the other variances that we are about to define.

Definition III.2 (Quantum conditional entropy variance)**.** Let ρ_{AB} be a bipartite quantum state. Then, the quantum conditional entropy variance $V(A|B)_\rho$ is given by:

$$V(A|B)_\rho := V(\rho_{AB}\|\mathrm{id}_A \otimes \rho_B).$$

Likewise, this was already defined in [9] under the name "quantum conditional information variance". Of course, the system in the conditioning can be omitted in the unconditional case. Finally, we define the quantum mutual information variance, first defined in [26]:

Definition III.3 (Quantum mutual information variance)**.** Let ρ_{AB} be a bipartite quantum state. Then, the quantum mutual information variance $V(A;B)_\rho$ is given by:

$$V(A;B)_\rho := V(\rho_{AB}\|\rho_A \otimes \rho_B).$$

These various quantities have a number of elementary properties that we prove here. First, to get a sense of what the divergence variance looks like in a simple case, we plot the divergence variance of a single bit X with $\Pr[X = 0]$ in Figure 2. We also note that the divergence variance does not satisfy the data processing inequality, even in the classical case; in other words, it is not true in general that $V(\rho\|\sigma) \geqslant V(\mathcal{E}(\rho)\|\mathcal{E}(\sigma))$ for a quantum channel $\mathcal{E}$. To see this, consider the following counterexample: let $\rho = |0\rangle\langle 0|$, $\sigma = \mathrm{id}$, and let $\mathcal{E}$ be a binary symmetric channel in the computational basis with error rate 0.083. Then, we can see from the plot in Figure 2 that $V(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) > V(\rho\|\sigma)$. It is also easy to see that the opposite inequality is also false in general.

Now, we show that the divergence variance obeys the following basic bounds:

Lemma III.4 (General bounds)**.** *For any positive semidefinite operators ρ, σ, with $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$, and any $\nu \in (0,1)$,*

$$V(\rho\|\sigma) \leq \frac{1}{\nu^2} \log^2 \left(2^{-\nu D(\rho\|\sigma)+\nu D'_{1+\nu}(\rho\|\sigma)} + 2^{\nu D(\rho\|\sigma)-\nu D'_{1-\nu}(\rho\|\sigma)} + 1\right). \tag{4}$$

Proof. First, without loss of generality, we restrict the space to the support of σ. We then proceed in a way similar to [27, Lemma 8]. We introduce $X = 2^{-D(\rho\|\sigma)}\rho \otimes (\sigma^{-1})^T$, $|\varphi\rangle = (\sqrt{\rho} \otimes \mathrm{id})|\gamma\rangle$ with $|\gamma\rangle = \sum_i |i\rangle \otimes |i\rangle$. We then have $V(\rho\|\sigma) = \frac{1}{\ln^2 2}\langle\varphi| \ln^2 X|\varphi\rangle$. Observe that we have for $\nu \in (0,1)$ and any $t > 0$

$$\begin{aligned}
\ln^2 t &= \frac{1}{\nu^2} \ln^2 t^\nu \\
&\leq \frac{1}{\nu^2} \left(\ln\left(t^\nu + \frac{1}{t^\nu}\right)\right)^2 \\
&\leq \frac{1}{\nu^2} \left(\ln\left(t^\nu + \frac{1}{t^\nu} + 1\right)\right)^2 ,
\end{aligned}$$

where in the first inequality, we used the fact that $\ln(x)^2 \leq \ln(x + \frac{1}{x})^2$ for any $x > 0$ and in the second inequality the fact that $x + \frac{1}{x} \geqslant 1$. As a result, we have that

$$(\Pi_{\mathrm{supp}(\rho)} \otimes \mathrm{id}) \ln^2 X (\Pi_{\mathrm{supp}(\rho)} \otimes \mathrm{id}) \leqslant \frac{1}{\nu^2} (\Pi_{\mathrm{supp}(\rho)} \otimes \mathrm{id}) \left(\ln\left(X^\nu + \frac{\mathrm{id}}{X^\nu} + \mathrm{id}\right)\right)^2 (\Pi_{\mathrm{supp}(\rho)} \otimes \mathrm{id})$$

and therefore

$$\langle\varphi| \ln^2 X|\varphi\rangle \leq \frac{1}{\nu^2} \langle\varphi| \left(\ln\left(X^\nu + \frac{\mathrm{id}}{X^\nu} + \mathrm{id}\right)\right)^2 |\varphi\rangle,$$

We now use the fact that the function $s \mapsto \ln^2(s)$ is concave on the interval $[e, +\infty)$ and that $|\varphi\rangle$ is in the span of the eigenvectors of $X^\nu + \frac{\mathrm{id}}{X^\nu} + \mathrm{id}$ with eigenvalues in $[3, \infty)$) to get

$$\langle\varphi| \ln^2 X|\varphi\rangle \leq \frac{1}{\nu^2} \ln^2 \left(\langle\varphi|X^\nu|\varphi\rangle + \langle\varphi|\frac{\mathrm{id}}{X^\nu}|\varphi\rangle + 1\right).$$

But observe that

$$\langle\varphi|X^\nu|\varphi\rangle = 2^{-\nu D(\rho\|\sigma)} \mathrm{tr}(\rho^{1+\nu}\sigma^{-\nu}) = 2^{-\nu D(\rho\|\sigma)+\nu D'_{1+\nu}(\rho\|\sigma)}$$

and

$$\langle\varphi|\frac{\mathrm{id}}{X^\nu}|\varphi\rangle = 2^{+\nu D(\rho\|\sigma)} \mathrm{tr}(\rho^{1-\nu}\sigma^{\nu}) = 2^{+\nu D(\rho\|\sigma)-\nu D'_{1-\nu}(\rho\|\sigma)} .$$

□

This leads to the following bounds for the conditional entropy variance and the mutual information variance:

Corollary III.5. *For any density operator ρ_{AB}, we have*

$$\begin{aligned}
V(A|B)_\rho &\leq \log^2(2d_A^2 + 1) \\
V(A;B)_\rho &\leq 4\log^2(2d_A + 1) .
\end{aligned}$$

Moreover, if the system A is classical, then the upper bounds can be improved to

$$\begin{aligned}
V(A|B)_\rho &\leq \log^2(2d_A + 1) \\
V(A;B)_\rho &\leq 4\log^2(2\sqrt{d_A} + 1) .
\end{aligned}$$

Proof. For the upper bound on $V(A|B)_\rho = V(\rho_{AB}\|\mathrm{id}_A \otimes \rho_B)$, using (4) for $\nu \in (0,1)$, we get:

$$\begin{aligned}
V(A|B)_\rho &\leq \frac{1}{\nu^2} \log^2 \left(2^{-\nu D(\rho_{AB}\|\mathrm{id}_A\otimes\rho_B)+\nu D'_{1+\nu}(\rho_{AB}\|\mathrm{id}_A\otimes\rho_B)} + 2^{\nu D(\rho_{AB}\|\mathrm{id}_A\otimes\rho_B)-\nu D'_{1-\nu}(\rho_{AB}\|\mathrm{id}_A\otimes\rho_B)} + 1\right) \\
&= \frac{1}{\nu^2} \log^2 \left(2^{\nu(H(A|B)_\rho - H'_{1+\nu}(A|B)_\rho)} + 2^{\nu(-H(A|B)_\rho + H'_{1-\nu}(A|B)_\rho)} + 1\right) \\
&\leq \frac{1}{\nu^2} \log^2 \left(2d_A^{2\nu} + 1\right),
\end{aligned}$$

where the first inequality uses Lemma III.4 and the last inequality uses the fact that all the entropy terms are bounded by $-\log d_A \leqslant H_\star(A|\star) \leqslant \log d_A$ (see e.g., [28, Lemma 5.2]). Taking the limit $\nu \to 1$, we get the desired result. In the case where ρ_{AB} is separable, we have instead $0 \leqslant H_\star(A|\star) \leqslant \log d_A$ which leads to the improved bound.

For the bound on $V(A;B) = V(\rho_{AB}\|\rho_A \otimes \rho_B)$, we use (4) with $\nu = \frac{1}{2}$ to have an upper bound of the form

$$\begin{aligned} V(A;B)_\rho &\leq 4\log^2\left(2^{-\frac{1}{2}D(\rho_{AB}\|\rho_A\otimes\rho_B)+\frac{1}{2}D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A\otimes\rho_B)} + 2^{\frac{1}{2}D(\rho_{AB}\|\rho_A\otimes\rho_B)-\frac{1}{2}D'_{\frac{1}{2}}(\rho_{AB}\|\rho_A\otimes\rho_B)} + 1\right) \\ &\leq 4\log^2\left(2^{\frac{1}{2}D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A\otimes\rho_B)} + d_A + 1\right), \end{aligned}$$

where we used the fact that $D(\rho_{AB}\|\rho_A \otimes \rho_B)$ and $D'_{\frac{1}{2}}(\rho_{AB}\|\rho_A \otimes \rho_B)$ are nonnegative and $D(\rho_{AB}\|\rho_A \otimes \rho_B) \leq 2\log d_A$. To conclude, it suffices to show that $D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A \otimes \rho_B) \leq 2\log d_A$. To do this, let ρ_{ABC} be a purification of ρ. We then have that:

$$\begin{aligned} D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A \otimes \rho_B) &\leqslant D'_{\frac{3}{2}}(\rho_{ABC}\|\rho_A \otimes \rho_{BC}) \\ &= 2\log \operatorname{tr}\left[\rho_{ABC}^{\frac{3}{2}}(\rho_A \otimes \rho_{BC})^{-\frac{1}{2}}\right] \\ &\leqslant 2\log\sqrt{\operatorname{tr}\left[\rho_{ABC}^{\frac{3}{2}}\rho_A^{-1}\right]\operatorname{tr}\left[\rho_{ABC}^{\frac{3}{2}}\rho_{BC}^{-1}\right]} \\ &= \log\left[\operatorname{tr}\left[\rho_{ABC}\rho_A^{-1}\right]\operatorname{tr}\left[\rho_{ABC}\rho_{BC}^{-1}\right]\right] \\ &\leqslant \log d_A + \log\dim\operatorname{supp}(\rho_{BC}) \\ &\leqslant 2\log d_A. \end{aligned}$$

We remark that the choice of looking at $D'_{\frac{3}{2}}$ is not arbitrary. In fact, $D'_{1+\nu}(\rho_{AB}\|\rho_A \otimes \rho_B)$ for $\nu > \frac{1}{2}$ may be arbitrarily large as can be seen with the following example. Let $|\Phi(\lambda)\rangle_{AB} = \sqrt{\lambda}|00\rangle_{AB} + \sqrt{1-\lambda}|11\rangle_{AB}$ for $\lambda \in [0,1]$. We set $\rho_{AB} = |\Phi(\lambda)\rangle\langle\Phi(\lambda)|_{AB}$. Then, we can compute

$$D'_{1+\nu}(\rho_{AB}\|\rho_A \otimes \rho_B) = \frac{1}{\nu}\log\operatorname{tr}\left[\lambda^{1-2\nu}|00\rangle\langle 00| + (1-\lambda)^{1-2\nu}|11\rangle\langle 11|\right],$$

which diverges as $\lambda \to 0$ for $\nu > \frac{1}{2}$.

When the system A is classical, then we have $D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A\otimes\rho_B) \leq \log d_A$. In fact, we write $\rho_{AB} = \sum_a p(a)|a\rangle\langle a|_A \otimes \rho_B(a)$, where $\{p(a)\}_a$ is a probability distribution and $\rho_B(a)$ are density operators. Then, we compute

$$\begin{aligned} D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A \otimes \rho_B) &= 2\log\sum_a \operatorname{tr}\left[\left(p(a)^{\frac{3}{2}}|a\rangle\langle a| \otimes \rho_B(a)^{\frac{3}{2}}\right)\left(p(a)^{-\frac{1}{2}}|a\rangle\langle a| \otimes \rho_B^{-\frac{1}{2}}\right)\right] \\ &= 2\log\sum_a \operatorname{tr}\left[p(a)\rho_B(a)^{\frac{3}{2}}\rho_B^{-\frac{1}{2}}\right]. \end{aligned}$$

Now note that for any a, $\rho_B \geq p(a)\rho_B(a)$, and thus by operator monotonicity of $x \mapsto -x^{-\frac{1}{2}}$, we have $\rho_B^{-\frac{1}{2}} \leq p(a)^{-\frac{1}{2}}\rho_B(a)^{-\frac{1}{2}}$, we get

$$\begin{aligned} D'_{\frac{3}{2}}(\rho_{AB}\|\rho_A \otimes \rho_B) &\leqslant 2\log\sum_a p(a)^{\frac{1}{2}} \\ &\leqslant \log d_A. \end{aligned}$$

□

Next, we show that the divergence variance is additive, in the following sense:

Lemma III.6 (Additivity of the divergence variance)**.** *Let ρ, τ be density operators and σ, ω be positive semidefinite operators. Then,*

$$V(\rho \otimes \tau\|\sigma \otimes \omega) = V(\rho\|\sigma) + V(\tau\|\omega).$$

Proof. We have that

$$\begin{aligned}
&V(\rho\otimes\tau\|\sigma\otimes\omega)\\
&\quad= \operatorname{tr}\left[(\rho\otimes\tau)\left(\log(\rho\otimes\tau)-\log(\sigma\otimes\omega)-\mathrm{id}D(\rho\|\sigma)-\mathrm{id}D(\tau\|\omega)\right)^2\right]\\
&\quad= \operatorname{tr}\left[(\rho\otimes\tau)\left(\log\rho\otimes\mathrm{id}+\mathrm{id}\otimes\log\tau-\log\sigma\otimes\mathrm{id}-\mathrm{id}\otimes\log\omega-\mathrm{id}D(\rho\|\sigma)-\mathrm{id}D(\tau\|\omega)\right)^2\right]\\
&\quad= \operatorname{tr}\left[(\rho\otimes\tau)\left(\log\rho\otimes\mathrm{id}-\log\sigma\otimes\mathrm{id}-\mathrm{id}D(\rho\|\sigma)\right)^2\right]\\
&\qquad\quad+\operatorname{tr}\left[(\rho\otimes\tau)\left(\mathrm{id}\otimes\log\tau-\mathrm{id}\otimes\log\omega-\mathrm{id}D(\tau\|\omega)\right)^2\right]\\
&\qquad\quad+\operatorname{tr}\left[(\rho\otimes\tau)\left(\log\rho\otimes\mathrm{id}-\log\sigma\otimes\mathrm{id}-\mathrm{id}D(\rho\|\sigma)\right)\left(\mathrm{id}\otimes\log\tau-\mathrm{id}\otimes\log\omega-\mathrm{id}D(\tau\|\omega)\right)\right]\\
&\qquad\quad+\operatorname{tr}\left[(\rho\otimes\tau)\left(\mathrm{id}\otimes\log\tau-\mathrm{id}\otimes\log\omega-\mathrm{id}D(\tau\|\omega)\right)\left(\log\rho\otimes\mathrm{id}-\log\sigma\otimes\mathrm{id}-\mathrm{id}D(\rho\|\sigma)\right)\right]\\
&\quad= V(\rho\|\sigma)+V(\tau\|\omega)\\
&\qquad\quad+2\operatorname{tr}\left[\rho(\log\rho-\log\sigma-\mathrm{id}D(\rho\|\sigma))\right]\operatorname{tr}\left[\tau(\log\tau-\log\omega-\mathrm{id}D(\tau\|\omega))\right]\\
&\quad= V(\rho\|\sigma)+V(\tau\|\omega).
\end{aligned}$$

□

We also show that a conditional entropy variance with a classical variable X in the conditioning admits a decomposition in terms of the possible values of X:

Lemma III.7. *Let ρ_{ABX} be a tripartite state with X classical. Then,*

$$V(A|BX)_\rho=\sum_x p_x V(A|B,X=x)+\operatorname{Var}(W)$$

where W is a random variable that takes value $H(A|B,X=x)$ with probability p_x. In particular,

$$V(A|BX)_\rho\geqslant\sum_x p_x V(A|B,X=x).$$

Proof. We have that

$$\begin{aligned}
V(A|BX)_\rho &= \operatorname{tr}\left[\rho_{ABX}\left(\log\rho_{ABX}-\mathrm{id}_A\otimes\log\rho_{BX}\right)^2\right]-H(A|BX)^2\\
&= \sum_x p_x\operatorname{tr}\left[\rho_{AB|X=x}\left(\log\rho_{AB|X=x}+\mathrm{id}\log p_x-\mathrm{id}_A\otimes\log\rho_{B|X=x}-\mathrm{id}\log p_x\right)^2\right]\\
&\qquad -H(A|BX)^2\\
&= \sum_x p_x\operatorname{tr}\left[\rho_{AB|X=x}\left(\log\rho_{AB|X=x}-\mathrm{id}_A\otimes\log\rho_{B|X=x}\right)^2\right]\\
&\qquad -\left(\sum_x p_x H(A|B,X=x)\right)^2\\
&= \sum_x p_x\left(V(A|B,X=x)+H(A|B,X=x)^2\right)-\left(\sum_x p_x H(A|B,X=x)\right)^2\\
&= \sum_x p_x V(A|B,X=x)-\left(\sum_x p_x H(A|B,X=x)\right)^2+\sum_x p_x H(A|B,X=x)^2\\
&= \sum_x p_x V(A|B,X=x)-(\mathbb{E}W)^2+\mathbb{E}[W^2]\\
&= \sum_x p_x V(A|B,X=x)+\operatorname{Var}(W).
\end{aligned}$$

□

We will also need the following decomposition of the conditional entropy variance for Markov chains:

Lemma III.8. *Let ρ_{ABCDX} be a quantum state with X classical satisfying the Markov chain $AC\leftrightarrow X\leftrightarrow BD$; i.e. $I(AC:BD|X)=0$. Then,*

$$V(AB|CDX)=V(A|CX)+V(B|DX)+2\operatorname{Cov}(W_1,W_2),$$

where W_1 and W_2 are random variables that take value $H(A|C, X = x)$ and $H(B|D, X = x)$ according to the value of X, respectively. In particular, this shows that for a trivial B system, $V(A|CDX) = V(A|CX)$.

Proof. We perform the computation as follows:

$$\begin{aligned} V(AB|CDX) &= \sum_x p_x V(AB|CD, X = x) + \operatorname{Var}(W_1 + W_2) \\ &= \sum_x p_x (V(A|C, X = x) + V(B|D, X = x)) + \operatorname{Var}(W_1) + \operatorname{Var}(W_2) + 2\operatorname{Cov}(W_1, W_2) \\ &= V(A|CX) + V(B|DX) + 2\operatorname{Cov}(W_1, W_2), \end{aligned}$$

where the first equality follows from Lemma III.7, and the second equality from Lemma III.6. □

Finally, the following more specialized lemmas will be needed in the proof of our main result:

Lemma III.9. *Let $\rho_{ACD\bar{D}X}$ be a quantum state with X classical that can be written as*

$$\sum_x p_x |x\rangle\langle x|_X \otimes \rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)}$$

with $\tau_{\bar{D}}^{(x)} = \frac{\mathrm{id}_{\bar{D}}}{d_{\bar{D}}}$ for all x. Then,

$$V(ADX|C\bar{D}) \leqslant V(AX|C) + V(D|X\bar{D}) + 2\sqrt{V(AX|C)V(D|X\bar{D})}.$$

Proof. First, note that the chain rule together with the form of the state in the lemma gives $H(ADX|C\bar{D}) = H(AX|C) + H(D|X\bar{D})$. We can then proceed as follows:

$$\begin{aligned} V(ADX|C\bar{D}) = \sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \Big(&\log p_x \rho_{AC}^{(x)} \otimes \mathrm{id}_{D\bar{D}} \\ &+ \mathrm{id}_{AC} \otimes \log \tau_{D\bar{D}}^{(x)} - \mathrm{id}_{AD\bar{D}} \otimes \log \rho_C + \mathrm{id}_{ACD\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(ADX|C\bar{D}) \Big)^2 \Big] \\ = \sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \Big(&\log p_x \rho_{AC}^{(x)} \otimes \mathrm{id}_{D\bar{D}} - \mathrm{id}_{AD\bar{D}} \otimes \log \rho_C + \mathrm{id} H(AX|C) \Big)^2 \Big] \\ + \sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \Big(&\mathrm{id}_{AC} \otimes \log \tau_{D\bar{D}}^{(x)} + \mathrm{id}_{ACD\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(D|X\bar{D}) \Big)^2 \Big] \\ + 2 \sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \Big(&\log p_x \rho_{AC}^{(x)} \otimes \mathrm{id}_{D\bar{D}} - \mathrm{id}_{AD\bar{D}} \otimes \log \rho_C + \mathrm{id} H(AX|C) \Big) \\ &\Big(\mathrm{id}_{AC} \otimes \log \tau_{D\bar{D}}^{(x)} + \mathrm{id}_{ABD\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(D|X\bar{D}) \Big) \Big] \\ = V(AX|C) + V(D|X\bar{D}) + 2 \cdot \text{crossterm}, \end{aligned}$$

where we used in the second equality the fact that $\Big(\log p_x \rho_{AC}^{(x)} \otimes \mathrm{id}_{D\bar{D}} - \mathrm{id}_{AD\bar{D}} \otimes \log \rho_C + \mathrm{id} H(AX|C) \Big)$ and $\Big(\log \tau_{D\bar{D}}^{(x)} \otimes \mathrm{id}_{AC} + \mathrm{id}_{ABD\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(D|X\bar{D}) \Big)$ commute. To get the last equality, we observe that

$$\begin{aligned} &\sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \Big(\log p_x \rho_{AC}^{(x)} \otimes \mathrm{id}_{D\bar{D}} - \mathrm{id}_{AD\bar{D}} \otimes \log \rho_C + \mathrm{id} H(AX|C) \Big)^2 \Big] \\ &= \sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \Big(\log p_x \rho_{AC}^{(x)} - \mathrm{id}_A \otimes \log \rho_C + \mathrm{id} H(AX|C) \Big)^2 \Big] \\ &= V(AX|C), \end{aligned}$$

and

$$\begin{aligned} &\sum_x p_x \operatorname{tr}\Big[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \Big(\log \tau_{D\bar{D}}^{(x)} \otimes \mathrm{id}_{AC} + \mathrm{id}_{ACD\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(D|X\bar{D}) \Big)^2 \Big] \\ &= \operatorname{tr}\Bigg[\sum_x p_x |x\rangle\langle x| \otimes \tau_{D\bar{D}}^{(x)} \Bigg(\log \Bigg(\sum_x p_x |x\rangle\langle x| \otimes \tau_{D\bar{D}}^{(x)} \Bigg) - \mathrm{id}_D \otimes \log \Bigg(\sum_x p_x |x\rangle\langle x| \otimes \tau_{\bar{D}}^{(x)} \Bigg) \\ &\qquad + \mathrm{id}_{XD\bar{D}} H(D|X\bar{D}) \Bigg)^2 \Bigg] \\ &= V(D|\bar{D}X), \end{aligned}$$

We are now going to bound the cross term by applying the Cauchy-Schwarz inequality. Using the cyclicity of the trace for $(\rho_{AC}^{(x)})^{1/2}$, we have

$$\begin{aligned}\text{crossterm} = \operatorname{tr}\Bigg[&\left(\sum_x \sqrt{p_x}|x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2}\Big(\log p_x \rho_{AC}^{(x)} - \mathrm{id}_A \otimes \log \rho_C + \mathrm{id} H(AX|C)\Big) \otimes (\tau_{D\bar{D}}^{(x)})^{1/2}\right) \\ &\cdot \left(\sum_x \sqrt{p_x}|x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2} \otimes (\tau_{D\bar{D}}^{(x)})^{1/2}\Big(\log \tau_{D\bar{D}}^{(x)} + \mathrm{id}_{D\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(D|X\bar{D})\Big)\right)\Bigg] \\ \leqslant &\sqrt{\operatorname{tr}(YY^\dagger)\operatorname{tr}(ZZ^\dagger)},\end{aligned}$$

where $Y = \sum_x \sqrt{p_x}|x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2}\Big(\log p_x \rho_{AC}^{(x)} - \mathrm{id}_A \otimes \log \rho_C + \mathrm{id} H(AX|C)\Big) \otimes (\tau_{D\bar{D}}^{(x)})^{1/2}$ and $Z = \sum_x \sqrt{p_x}|x\rangle\langle x| \otimes (\rho_{A\bar{C}}^{(x)})^{1/2} \otimes (\tau_{D\bar{D}}^{(x)})^{1/2}\Big(\log \tau_{D\bar{D}}^{(x)} + \mathrm{id}_{D\bar{D}} \log d_{\bar{D}} + \mathrm{id} H(D|X\bar{D})\Big)$. We conclude by observing that $\operatorname{tr}(YY^\dagger) = V(AX|C)$ and $\operatorname{tr}(ZZ^\dagger) = V(D|X\bar{D})$. □

Lemma III.10. *For any state ρ_{ABC}, we have*

$$\begin{aligned}V(AC|B)_\rho = &V(A|B)_\rho + V(C|BA)_\rho \\ &+ \operatorname{tr}\left(\rho_{ABC}(\log \rho_{AB} - \log \rho_B + H(A|B))(\log \rho_{ABC} - \log \rho_{AB} + H(C|BA))\right) \\ &+ \operatorname{tr}\left(\rho_{ABC}(\log \rho_{ABC} - \log \rho_{AB} + H(C|BA))(\log \rho_{AB} - \log \rho_B + H(A|B))\right). \end{aligned} \tag{5}$$

Proof. Direct calculation. □

Lemma III.11. *Let ρ_{XAB} be of the form $\rho_{XAB} = \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes \rho_{AB,x}$ with $\operatorname{tr}(\rho_{AB,x}\rho_{AB,x'}) = 0$ when $x \neq x'$. Then we have*

$$V(AX|B)_\rho = V(A|B)_\rho \ . \tag{6}$$

In other words, if the states $\rho_{AB,x}$ are orthogonal for different values of x, then this effectively makes the subsystem X redundant for the purpose of computing the conditional entropy variance.

Proof. Using Lemma III.10, it suffices to show only the first term of (5) remains. In fact, we have $H(X|BA) = 0$ and

$$\begin{aligned}V(X|BA)_\rho &= \operatorname{tr}\left(\rho_{XAB}(\log \rho_{XAB} - \log \rho_{AB})^2\right) \\ &= \sum_x \operatorname{tr}\left(|x\rangle\langle x|_X \otimes \rho_{AB,x}\left(\sum_{x'} |x'\rangle\langle x'|_X \otimes \log \rho_{AB,x'} - \mathrm{id}_X \otimes \sum_{x'} \log \rho_{AB,x'}\right)^2\right) \\ &= \sum_x \operatorname{tr}\left(|x\rangle\langle x|_X \otimes \rho_{AB,x}\left(\sum_{x'} (|x'\rangle\langle x'|_X - \mathrm{id}_X)^2 \otimes \log^2 \rho_{AB,x'}\right)\right) \\ &= \sum_x \operatorname{tr}\left(|x\rangle\langle x|_X (|x\rangle\langle x|_X - \mathrm{id}_X)^2 \otimes \rho_{AB,x} \log^2 \rho_{AB,x}\right) \\ &= 0 \ .\end{aligned}$$

In addition, the other terms are also zero:

$$\begin{aligned}&\operatorname{tr}\left(\rho_{XAB}(\log \rho_{AB} - \log \rho_B + H(A|B))(\log \rho_{XAB} - \log \rho_{AB})\right) \\ &= \sum_x \operatorname{tr}\Bigg((|x\rangle\langle x| \otimes \rho_{AB,x})(\mathrm{id}_X \otimes (\log \rho_{AB} - \log \rho_B + \mathrm{id}_{AB} H(A|B)))(|x\rangle\langle x| \otimes \log \rho_{AB,x} \\ &\qquad - \mathrm{id}_X \otimes \sum_{x'} \log \rho_{AB,x'})\Bigg) \\ &= \sum_x \operatorname{tr}\left(\rho_{AB,x}(\log \rho_{AB} - \log \rho_B + \mathrm{id}_{AB} H(A|B))(\sum_{x'\neq x} \log \rho_{AB,x'})\right) \\ &= 0 \ ,\end{aligned}$$

using the orthogonality of $\rho_{AB,x}$ and $\rho_{AB,x'}$, and

$$\begin{aligned}
&\operatorname{tr}\left[\rho_{XAB}(\log\rho_{XAB}-\log\rho_{AB})(\log\rho_{AB}-\log\rho_B+H(A|B))\right]\\
&\qquad=\sum_x \operatorname{tr}\left[(|x\rangle\langle x|\otimes\rho_{AB,x})(|x\rangle\langle x|\otimes\rho_{AB,x}-\mathrm{id}_X\otimes\rho_{AB})(\log\rho_{AB}-\log\rho_B+\mathrm{id}_{XAB}H(A|B))\right]\\
&\qquad=\sum_x \operatorname{tr}\left[(|x\rangle\langle x|\otimes\rho_{AB,x})(|x\rangle\langle x|\otimes\rho_{AB,x}-\mathrm{id}_X\otimes\rho_{AB,x})(\log\rho_{AB}-\log\rho_B+\mathrm{id}_{XAB}H(A|B))\right]\\
&\qquad=0,
\end{aligned}$$

where we have used the fact that $\rho_{AB,x}\rho_{AB}=\rho_{AB,x}^2$ by the orthogonality conditions. □

IV. Continuity bounds for Rényi divergences

A critical step in the proof is an explicit continuity bound for D_α when α approaches 1. One such bound is given [28, Section 4.2.2]. However, this bound does not give explicit values for the remainder term. The following lemma computes an explicit remainder term for the case of classical probability distributions. As in [28, Section 4.4.2], we will then apply this lemma to Nussbaum-Szkoła distributions to get a similar result for the Petz divergence D'_α between quantum states.

Lemma IV.1. *Let ρ be a density operator and σ be a not necessarily normalized positive semidefinite operator. Let $\alpha>1$ and $\mu\in(0,1)$. Then, we have that*

$$D_\alpha(\rho\|\sigma)\leqslant D'_\alpha(\rho\|\sigma)\leqslant D(\rho\|\sigma)+\frac{(\alpha-1)\ln 2}{2}V(\rho\|\sigma)+(\alpha-1)^2K_{\rho,\sigma},$$

where

$$K_{\rho,\sigma}(\alpha,\mu)=\frac{1}{6\mu^3\ln 2}2^{(\alpha-1)(D'_\alpha(\rho\|\sigma)-D(\rho\|\sigma))}\ln^3\left(2^{(\alpha+\mu-1)(D'_{\alpha+\mu}(\rho\|\sigma)-D(\rho\|\sigma))}+e^2\right).$$

Proof. As mentioned above, we start by proving the statement for classical probability distributions. For this proof, it will be more convenient for us to do everything using natural logarithms; we will therefore use the "hatted" quantities $\hat{D}$ and $\hat{V}$ for all relative entropies and variances to denote their counterparts defined using the natural logarithm. Let P be a probability distribution and Q be a not necessarily normalized distribution. Define the random variable X with distribution P, and let $Z=e^{-\hat{D}(P\|Q)}\frac{P(X)}{Q(X)}$. Note that for any $\nu>0$, we have

$$\mathbb{E}[Z^\nu]=e^{-\nu\hat{D}(P\|Q)}\sum_x P(x)^{1+\nu}Q(x)^{-\nu} \tag{7}$$

$$=e^{-\nu(\hat{D}(P\|Q)-\hat{D}_{1+\nu}(P\|Q))}. \tag{8}$$

Now, letting $\nu=\alpha-1$, we have

$$\hat{D}_\alpha(P\|Q)=\frac{1}{\nu}\ln\left(\mathbb{E}[Z^\nu]\right)+\hat{D}(P\|Q). \tag{9}$$

Applying Taylor's inequality to the function $\nu\mapsto\mathbb{E}[Z^\nu]$ we have

$$\mathbb{E}[Z^\nu]\leq 1+\nu\mathbb{E}[\ln Z]+\frac{\nu^2}{2}\mathbb{E}[\ln^2 Z]+\frac{\nu^3}{6}\sup_{0<\gamma\leqslant\nu}\mathbb{E}[Z^\gamma\ln^3 Z]. \tag{10}$$

Using the fact that $\mathbb{E}[\ln Z]=0$ and

$$\mathbb{E}[\ln^2 Z]=\sum_x P(x)\left(\ln\frac{P(x)}{Q(x)}-\hat{D}(P\|Q)\right)^2 \tag{11}$$

$$=\hat{V}(P\|Q), \tag{12}$$

together with the inequality $\ln(1+x)\leqslant x$, we get

$$\hat{D}_\alpha(P\|Q)\leqslant\hat{D}(P\|Q)+\frac{\nu}{2}\hat{V}(P\|Q)+\frac{\nu^2}{6}\sup_{0<\gamma\leqslant\nu}\mathbb{E}[Z^\gamma\ln^3 Z]. \tag{13}$$

We now need to bound the remainder term. We want to use the concavity of $\ln^3$, but it is only concave on $[e^2,\infty)$. Hence, we start by using the fact that $\ln^3$ is nondecreasing and $Z^\gamma\geqslant 0$ to get

$$\mathbb{E}[Z^\gamma\ln^3 Z]=\frac{1}{\mu^3}\mathbb{E}[Z^\gamma\ln^3(Z^\mu)] \tag{14}$$

$$\leqslant\frac{1}{\mu^3}\mathbb{E}[Z^\gamma\ln^3(Z^\mu+e^2)] \tag{15}$$

$$=\frac{1}{\mu^3}\mathbb{E}[Z^\gamma]\frac{\mathbb{E}[Z^\gamma\ln^3(Z^\mu+e^2)]}{\mathbb{E}[Z^\gamma]}, \tag{16}$$

for any $\mu \in (0,1]$. Then we use the concavity of the function $t \mapsto \ln^3(t+e^2)$ on $[0,\infty)$ and get

$$\mathbb{E}[Z^\gamma \ln^3 Z] \leqslant \frac{1}{\mu^3}\mathbb{E}[Z^\gamma]\ln^3\left(\frac{\mathbb{E}[Z^\gamma(Z^\mu+e^2)]}{\mathbb{E}[Z^\gamma]}\right) \tag{17}$$

$$= \frac{1}{\mu^3}\mathbb{E}[Z^\gamma]\ln^3\left(\frac{\mathbb{E}[Z^{\mu+\gamma}]}{\mathbb{E}[Z^\gamma]}+e^2\right) \tag{18}$$

$$= \frac{1}{\mu^3}e^{\gamma(\hat{D}_{1+\gamma}(P\|Q)-\hat{D}(P\|Q))}\ln^3\left(\frac{e^{(\mu+\gamma)(\hat{D}_{1+\mu+\gamma}(P\|Q)-\hat{D}(P\|Q))}}{e^{\gamma(\hat{D}_{1+\gamma}(P\|Q)-\hat{D}(P\|Q))}}+e^2\right) \tag{19}$$

$$\leqslant \frac{1}{\mu^3}e^{\gamma(\hat{D}_{1+\gamma}(P\|Q)-\hat{D}(P\|Q))}\ln^3\left(e^{(\mu+\gamma)(\hat{D}_{1+\mu+\gamma}(P\|Q)-\hat{D}(P\|Q))}+e^2\right)\ , \tag{20}$$

where we used the fact that $\hat{D}_{1+\gamma}(P\|Q)-\hat{D}(P\|Q)\geqslant 0$. As this last expression is nondecreasing in γ, we get that

$$\sup_{0<\gamma\leqslant\nu}\mathbb{E}[Z^\gamma\ln^3 Z] \leqslant \frac{1}{\mu^3}e^{\nu(\hat{D}_{1+\nu}(P\|Q)-\hat{D}(P\|Q))}\ln^3\left(e^{(\mu+\nu)(\hat{D}_{1+\mu+\nu}(P\|Q)-\hat{D}(P\|Q))}+e^2\right). \tag{21}$$

This proves that

$$\hat{D}_\alpha(P\|Q) \leqslant \hat{D}(P\|Q)+\frac{(\alpha-1)}{2}\hat{V}(P\|Q)+\frac{(\alpha-1)^2}{6}(\text{RHS of (21)}) \tag{22}$$

and therefore, after converting back to base 2, that

$$D_\alpha(P\|Q) \leqslant D(P\|Q)+\frac{(\alpha-1)\ln 2}{2}V(P\|Q)+(\alpha-1)^2K_{P,Q}(\alpha,\mu) \tag{23}$$

with $K_{P,Q}(\alpha,\mu)=\frac{1}{6\mu^3\ln 2}2^{(\alpha-1)(D_\alpha(P\|Q)-D(P\|Q))}\ln^3\left(2^{(\alpha+\mu-1)(D_{\alpha+\mu}(P\|Q)-D(P\|Q))}+e^2\right)$.

Now in order to get the general statement, we use the fact that the Petz divergence between states ρ and σ is equal to the α-divergence of Nussbaum-Szkoła distributions [29], i.e., for all $\alpha\geqslant 0$

$$D'_\alpha(\rho\|\sigma) = D_\alpha(P^{[\rho,\sigma]}\|Q^{[\rho,\sigma]})\ ,$$

where $P^{[\rho,\sigma]}(x,y)=\lambda_x|\langle e_x|f_y\rangle|^2$ and $Q^{[\rho,\sigma]}(x,y)=\mu_y|\langle e_x|f_y\rangle|^2$ where $\{\lambda_x,|e_x\rangle\}_x$ are the eigenvalues and eigenvectors of ρ and $\{\mu_y,|f_y\rangle\}_y$ are the eigenvalues and eigenvectors of σ. Note that $P^{[\rho,\sigma]}$ and $Q^{[\rho,\sigma]}$ only depend on ρ and σ and not on α, and $P^{[\rho,\sigma]}$ and $Q^{[\rho,\sigma]}$ have the same normalization as ρ and σ, respectively. Note that by taking the limit $\alpha\to 1$, we also get $D(\rho\|\sigma)=D(P^{[\rho,\sigma]}\|Q^{[\rho,\sigma]})$. In addition, by taking the derivative at $\alpha=1$, we get that $V(\rho\|\sigma)=V(P\|Q)$ [28, Proposition 4.9]. Applying inequality (23) to $P^{[\rho,\sigma]}$ and $Q^{[\rho,\sigma]}$, we get the desired result. □

To obtain a quantitative continuity for $H_\alpha(A|B)_\rho$ at $\alpha=1$, it suffices to use Lemma IV.1 with $\rho=\rho_{AB}$, $\sigma=\mathrm{id}_A\otimes\rho_B$ together with the fact that $D_\alpha(\rho\|\sigma)\leqslant D'_\alpha(\rho\|\sigma)$. In addition, to simplify the statement, we set $\mu=2-\alpha$.

Corollary IV.2. *Let ρ_{AB} be a density operator. Then we have for any $\alpha\in(1,2)$,*

$$H_\alpha(A|B)_\rho \geqslant H(A|B)_\rho-\frac{(\alpha-1)\ln 2}{2}V(A|B)_\rho-(\alpha-1)^2K(\alpha)\ ,$$

where $K(\alpha)=\frac{1}{6(2-\alpha)^3\ln 2}\cdot 2^{(\alpha-1)(-H'_\alpha(A|B)_\rho+H(A|B)_\rho)}\ln^3\left(2^{-H'_2(A|B)_\rho+H(A|B)_\rho}+e^2\right)$.

V. Entropy accumulation with improved second order

We start by recalling the framework for the entropy accumulation theorem [1]. For $i\in\{1,\dots,n\}$, let $\mathcal{M}_i$ be a TPCP map from R_{i-1} to $X_iA_iB_iR_i$, where A_i is finite-dimensional and where X_i represents a classical value from an alphabet $\mathcal{X}$ that is determined by A_i and B_i together. More precisely, we require that, $\mathcal{M}_i=\mathcal{T}_i\circ\mathcal{M}'_i$ where $\mathcal{M}'_i$ is an arbitrary TPCP map from R_{i-1} to $A_iB_iR_i$ and $\mathcal{T}_i$ is a TPCP map from A_iB_i to $X_iA_iB_i$ of the form

$$\mathcal{T}_i(W_{A_iB_i})=\sum_{y\in\mathcal{Y},z\in\mathcal{Z}}(\Pi_{A_i,y}\otimes\Pi_{B_i,z})W_{A_iB_i}(\Pi_{A_i,y}\otimes\Pi_{B_i,z})\otimes|t(y,z)\rangle\langle t(y,z)|_{X_i}\ , \tag{24}$$

where $\{\Pi_{A_i,y}\}$ and $\{\Pi_{B_i,z}\}$ are families of mutually orthogonal projectors on A_i and B_i, and where $t:\mathcal{Y}\times\mathcal{Z}\to\mathcal{X}$ is a deterministic function.

The entropy accumulation theorem stated below will hold for states of the form

$$\rho_{A_1^nB_1^nX_1^nE}=\mathrm{tr}_{R_n}(\mathcal{M}_n\circ\cdots\circ\mathcal{M}_1\otimes\mathcal{I}_E)(\rho^0_{R_0E}) \tag{25}$$

where $\rho^0_{R_0E}\in\mathrm{D}(R_0\otimes E)$ is a density operator on R_0 and an arbitrary system E. In addition, we require that the Markov conditions

$$A_1^{i-1}\leftrightarrow B_1^{i-1}E\leftrightarrow B_i \tag{26}$$

be satisfied for all $i \in \{1, \dots, n\}$; i.e. $I(A_1^{i-1}; B_i | B_1^{i-1} E)_\rho = 0$.

Let $\mathbb{P}$ be the set of probability distributions on the alphabet $\mathcal{X}$ of X_i, and let R be a system isomorphic to R_{i-1}. For any $q \in \mathbb{P}$ we define the set of states

$$\Sigma_i(q) = \left\{ \nu_{X_i A_i B_i R_i R} = (\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1} R}) : \quad \omega \in \mathrm{D}(R_{i-1} \otimes R) \text{ and } \nu_{X_i} = q \right\} , \tag{27}$$

where ν_{X_i} denotes the probability distribution over $\mathcal{X}$ with the probabilities given by $\langle x | \nu_{X_i} | x \rangle$. In other words, $\Sigma_i(q)$ is the set of states that can be produced at the output of the channel $\mathcal{M}_i$ and that have a reduced state on the X_i system equal to q.

Definition V.1. A real function f on $\mathbb{P}$ is called a *min-tradeoff function* (or simply tradeoff function for short) for $\mathcal{M}_i$ if it satisfies

$$f(q) \leqslant \min_{\nu \in \Sigma_i(q)} H(A_i | B_i R)_\nu \ .$$

Note that if $\Sigma_i(q) = \emptyset$, then $f(q)$ can be chosen arbitrarily. Our result will depend on some simple properties of the tradeoff function, namely the maximum and minimum of f, the minimum of f over valid distributions, and the maximum variance of f:

$$\begin{aligned}
\mathsf{Max}(f) &:= \max_{q \in \mathbb{P}} f(q) \\
\mathsf{Min}(f) &:= \min_{q \in \mathbb{P}} f(q) \\
\mathsf{Min}_\Sigma(f) &:= \min_{q : \Sigma_i(q) \neq \emptyset} f(q) \\
\mathsf{Var}(f) &:= \max_{q : \Sigma_i(q) \neq \emptyset} \sum_{x \in \mathcal{X}} q(x) f(\delta_x)^2 - \left(\sum_{x \in \mathcal{X}} q(x) f(\delta_x) \right)^2 ,
\end{aligned}$$

where δ_x stands for the distribution with all the weight on element x.

We write $\mathsf{freq}(X_1^n)$ for the distribution on $\mathcal{X}$ defined by $\mathsf{freq}(X_1^n)(x) = \frac{|\{i \in \{1,\dots,n\} : X_i = x\}|}{n}$. We also recall that in this context, an event Ω is defined by a subset of $\mathcal{X}^n$ and we write $\rho[\Omega] = \sum_{x_1^n \in \Omega} \mathrm{tr}(\rho_{A_1^n B_1^n E, x_1^n})$ for the probability of the event Ω and

$$\rho_{X_1^n A_1^n B_1^n E | \Omega} = \frac{1}{\rho[\Omega]} \sum_{x_1^n \in \Omega} |x_1^n\rangle\langle x_1^n| \otimes \rho_{A_1^n B_1^n E, x_1^n}$$

for the state conditioned on Ω.

Theorem V.2. *Let $\mathcal{M}_1, \dots, \mathcal{M}_n$ and $\rho_{A_1^n B_1^n X_1^n E}$ be such that (25) and the Markov conditions (26) hold, let $h \in \mathbb{R}$, let f be an affine min-tradeoff function for $\mathcal{M}_1, \dots, \mathcal{M}_n$, and let $\varepsilon \in (0,1)$. Then, for any event $\Omega \subseteq \mathcal{X}^n$ that implies $f(\mathsf{freq}(X_1^n)) \geqslant h$,*

$$H_{\min}^\varepsilon(A_1^n | B_1^n E)_{\rho_{|\Omega}} > nh - c\sqrt{n} - c' \tag{28}$$

holds for

$$\begin{aligned}
c &= \sqrt{2 \ln 2} \left(\log(2 d_A^2 + 1) + \sqrt{2 + \mathsf{Var}(f)} \right) \sqrt{1 - 2 \log(\varepsilon \rho[\Omega])} \\
c' &= \frac{35 (1 - 2 \log(\varepsilon \rho[\Omega]))}{\left(\log(2 d_A^2 + 1) + \sqrt{2 + \mathsf{Var}(f)} \right)^2} 2^{2 \log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} \ln^3 \left(2^{2 \log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2 \right)
\end{aligned}$$

where d_A is the maximum dimension of the systems A_i.

While the above give reasonable bounds in the general case, in order to obtain better finite n bounds in a particular case of interest, we advise the user to instead use the following bound for an $\alpha \in (1,2)$ that is either chosen carefully for the problem at hand or computed numerically:

$$H_{\min}^\varepsilon(A_1^n | B_1^n E)_{\rho_{|\Omega}} \geqslant nh - n \frac{(\alpha - 1) \ln 2}{2} V^2 - \frac{1}{\alpha - 1} \log \frac{2}{\varepsilon^2 \rho[\Omega]^2} - n (\alpha - 1)^2 K_\alpha \ , \tag{29}$$

with

$$V = \sqrt{\mathsf{Var}(f) + 2} + \log(2 d_A^2 + 1) \tag{30}$$

$$K_\alpha = \frac{1}{6 (2 - \alpha)^3 \ln 2} \cdot 2^{(\alpha - 1)(2 \log d_A + (\mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)))} \ln^3 \left(2^{2 \log d_A + (\mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))} + e^2 \right) \ . \tag{31}$$

Note that in general the optimal choice of α will depend on n; in Theorem V.2 we have chosen α so that $\alpha - 1$ scales as $\Theta(1/\sqrt{n})$, but other choices are possible. As described in the proof, in the case where the systems A_i are classical, we can

replace $2\log d_A$ by $\log d_A$ in (31), this comes from the fact that $H_\alpha(A_i|C) \geq 0$ whenever A_i is classical but can only be lower bounded by $-\log d_A$ in the general case. This bound holds under the exact same conditions as Theorem V.2 and for any $\alpha \in (1,2)$, and this is the bound we use to obtain the numerical results presented in the application presented in Section VI. The choice of α made to get Theorem V.2 is not the optimal one, but it was chosen to have a relatively simple expression showing the dependence on the main parameters without optimizing the constants.

The proof structure is the same as in [1]. The only difference is when using the continuity of D_α, we use the more precise estimate in Lemma IV.1, and we use the various properties of the entropy variance proven in Section III to bound the second-order term.

Proposition V.3. *Let $\mathcal{M}_1, \dots, \mathcal{M}_n$ and $\rho_{A_1^n B_1^n X_1^n E}$ be such that (25) and the Markov conditions (26) hold, let $h \in \mathbb{R}$, and let f be an affine min-tradeoff function f for $\mathcal{M}, \dots, \mathcal{M}_n$. Then, for any event Ω which implies $f(\mathsf{freq}(X_1^n)) \geqslant h$,*

$$H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} > nh - n\frac{(\alpha-1)\ln 2}{2}V^2 - \frac{\alpha}{\alpha-1}\log\frac{1}{\rho[\Omega]} - n(\alpha-1)^2 K_\alpha \tag{32}$$

holds for α satisfying $\alpha \in (1,2)$, and $V = \sqrt{\mathsf{Var}(f)+2}+\log(2d_A^2+1)$, where d_A is the maximum dimension of the systems A_i and K_α is defined in (31).

Proof. The first step of the proof is to construct a state that will allow us to lower-bound $H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}}$ using a chain rule similar to the one in Corollary II.9, while ensuring that the tradeoff function is taken into account. In order to achieve this, we proceed as in [1] and introduce an additional D system that can be thought of as an entropy price that encodes the tradeoff function. More precisely, for every i, let $\mathcal{D}_i : X_i \to X_i D_i$, be a TPCP map defined as

$$\mathcal{D}_i(W_{X_i}) = \sum_{x\in\mathcal{X}} \langle x|W_{X_i}|x\rangle \cdot |x\rangle\langle x|_{X_i} \otimes \tau(x)_{D_i} \ ,$$

where $\tau(x)$ is such that $H(D_i)_{\tau(x)} = \mathsf{Max}(f) - f(\delta_x)$ (here δ_x stands for the distribution with all the weight on element x). This is possible because $\mathsf{Max}(f) - f(\delta_x) \in [0, \mathsf{Max}(f) - \mathsf{Min}(f)]$ and we choose the dimension of the systems D_i to be equal to $d_D = \lceil 2^{\mathsf{Max}(f)-\mathsf{Min}(f)} \rceil$. More precisely, we fix $\tau(x)$ to be a mixture between a uniform distribution on $\{1, \dots, \lfloor 2^{\mathsf{Max}(f)-f(\delta_x)} \rfloor\}$ and a uniform distribution on $\{1, \dots, \lceil 2^{\mathsf{Max}(f)-f(\delta_x)} \rceil\}$. We note that compared to [1], our choice of state $\tau(x)$ is different. In fact, in [1], an additional system $\bar{D}$ was added to the conditioning and $\tau(x)$ was an appropriate mixture of a maximally entangled state on $D \otimes \bar{D}$ and a maximally mixed state on $D \otimes \bar{D}$. This choice is not adapted here because we will need the entropy variance of $\tau(x)$ to be small, for this reason we choose $\tau(x)$ to be basically uniform on a set of size $2^{\mathsf{Max}(f)-f(\delta_x)}$.

Now, let

$$\bar{\rho} := (\mathcal{D}_n \circ \cdots \circ \mathcal{D}_1)(\rho) \ .$$

Exactly as in the corresponding claim in [1], we can relate conditional entropy $H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}}$ to the conditional entropy of the constructed state $\bar{\rho}$:

$$H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} \geqslant H_\alpha^\uparrow(A_1^n D_1^n|B_1^n E)_{\bar{\rho}_{|\Omega}} - n\mathsf{Max}(f) + nh \ . \tag{33}$$

The next step is to relate the entropies on the conditional state $\rho_{|\Omega}$ to those on the unconditional state. To do this, we use Lemma A.1 applied to $\bar{\rho} = \rho[\Omega]\bar{\rho}_{|\Omega} + (\bar{\rho} - \rho[\Omega]\bar{\rho}_{|\Omega})$, together with the fact that $H_\alpha^\uparrow \geqslant H_\alpha$, and obtain

$$H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} \geqslant H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}} - \frac{\alpha}{\alpha-1}\log\frac{1}{\rho[\Omega]} - n\mathsf{Max}(f) + nh \ . \tag{34}$$

To show the desired inequality (32), it now suffices to prove that $H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}}$ is lower bounded by (roughly) $n\mathsf{Max}(f)$.

In order to lower bound $H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}}$, we are now going to use the chain rule for Rényi entropies in Corollary II.9 n times on the state $\bar{\rho}$, with the following substitutions at step i:

- $A_1 \to A_1^{i-1} D_1^{i-1}$
- $B_1 \to B_1^{i-1} E$
- $A_2 \to A_i D_i$
- $B_2 \to B_i$.

To check that the Markov chain condition holds, observe that $I(A_1^{i-1}D_1^{i-1} : B_i|B_1^{i-1}E) = I(A_1^{i-1} : B_i|B_1^{i-1}E) + I(D_1^{i-1} : B_i|B_1^{i-1}EA_1^{i-1})$. Using (26), we have that $I(A_1^{i-1} : B_i|B_1^{i-1}E) = 0$ and as D_1^{i-1} is determined by $A_1^{i-1}B_1^{i-1}$, we also have $I(D_1^{i-1} : B_i|B_1^{i-1}EA_1^{i-1}) = 0$. Thus, Corollary II.9 gives

$$\begin{aligned}
&H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}} \\
&\geqslant \sum_i \inf_{\omega_{R_{i-1}R}} H_\alpha(A_i D_i|B_i R)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} \\
&\geqslant \sum_i \inf_{\omega_{R_{i-1}R}} \left(H(A_i D_i|B_i R)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} - \frac{(\alpha-1)\ln 2}{2} V(A_i D_i|B_i R_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} - (\alpha-1)^2 K(\alpha) \right) \ ,
\end{aligned} \tag{35}$$

where we have invoked Corollary IV.2 in the second inequality. Here,

$$K(\alpha) = \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(-\eta_1+\eta_0)} \ln^3\left(2^{-\eta_2+\eta_0} + e^2\right) \ .$$

with $\eta_1 = H'_\alpha(A_iD_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)}$, $\eta_0 = H(A_iD_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)}$ and $\eta_2 = H'_2(A_iD_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)}$.

For any such state $\omega_{R_{i-1}R}$, we have

$$\begin{aligned} H(A_iD_i|B_iR)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} &= H(A_iX_iD_i|B_iR)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} \\ &= H(A_iX_i|B_iR)_{\mathcal{M}_i(\omega)} + H(D_i|X_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} \\ &= H(A_i|B_iR)_{\mathcal{M}_i(\omega)} + \sum_x q(x) H(D_i)_{\tau(x)} \\ &= H(A_i|B_iR)_{\mathcal{M}_i(\omega)} + \sum_x q(x)\big(\mathsf{Max}(f) - f(\delta_x)\big) \\ &= H(A_i|B_iR)_{\mathcal{M}_i(\omega)} + \mathsf{Max}(f) - f(q) \ , \end{aligned}$$

where $q = \mathcal{M}_i(\omega)_{X_i}$ denotes the distribution of X_i on $\mathcal{X}$ obtained from the state $\mathcal{M}_i(\omega)$. The third equality comes from the fact that X_i is determined by A_iB_i. The last equality holds because f is affine. Using the fact that f is a min-tradeoff function, we get that $H(A_i|B_iR)_{\mathcal{M}_i(\omega)} \geqslant f(q)$ and therefore:

$$\mathsf{Max}(f) \leqslant H(A_iD_i|B_iR)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} \leqslant \log d_{A_i} + \mathsf{Max}(f) - f(q) \ .$$

The lower bound allows us to lower bound the first term in Eq. (35). The upper bound will allow us to bound the last term in Eq. (35). In fact, as the systems D_i are classical, we have $\eta_1, \eta_2 \geqslant -\log d_{A_i}$ by Lemma A.2 (and in the case where A_i are classical, we have $\eta_1, \eta_2 \geqslant 0$) and thus

$$\begin{aligned} K(\alpha) &\leqslant \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(\log d_A + \log d_A + \mathsf{Max}(f) - f(q))} \ln^3\left(2^{\log d_A + \log d_A + \mathsf{Max}(f) - f(q)} + e^2\right) \\ &\leqslant \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))} \ln^3\left(2^{2\log d_A + \mathsf{Max}(f) - \mathsf{Min}_\Sigma(f)} + e^2\right) \ , \end{aligned}$$

as by definition $\Sigma_i(q)$ is not empty (it contains $\mathcal{M}_i(\omega)$).

We now analyze the second term of Eq. (35). Using Lemma III.11 and then Lemma III.9 we have

$$\begin{aligned} V(A_iD_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} &= V(A_iX_iD_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} &(36)\\ &\leqslant \left(\sqrt{V(A_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)}} + \sqrt{V(D_i|X_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)}}\right)^2 \ . &(37)\end{aligned}$$

We bound the first term by the dimension of A using Corollary III.5.

$$V(A_i|B_iR_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} \leqslant \log^2(2d_A^2 + 1).$$

For the second term, using the notation $q = \mathcal{M}_i(\omega)_{X_i}$, we have using Lemma III.7

$$V(D_i|X_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} = \sum_{x\in\mathcal{X}} q(x) V(D_i)_{\tau(x)} + \mathrm{Var}(W) \ ,$$

where W takes the value $H(D_i)_{\tau(x)} = \mathsf{Max}(f) - f(\delta_x)$ with probability $q(x)$. We have

$$\begin{aligned} \mathrm{Var}(W) &= \sum_{x\in\mathcal{X}} q(x)(\mathsf{Max}(f) - f(\delta_x))^2 - \left(\sum_x q(x)(\mathsf{Max}(f) - f(\delta_x))\right)^2 \\ &\leqslant \sup_{\omega, q=\mathcal{M}_i(\omega)_{X_i}} \sum_{x\in\mathcal{X}} q(x) f(\delta_x)^2 - \left(\sum_x q(x) f(\delta_x)\right)^2 \\ &\leqslant \mathsf{Var}(f) \ . \end{aligned}$$

To bound $V(D_i)_{\tau(x)}$ recall that $\tau(x)$ is a mixture between the uniform distribution on $\{1, \ldots, \lfloor 2^{\mathsf{Max}(f)-f(\delta_x)} \rfloor\}$ and the uniform distribution on $\{1, \ldots, \lceil 2^{\mathsf{Max}(f)-f(\delta_x)} \rceil\}$. Note that if $2^{\mathsf{Max}(f)-f(\delta_x)}$ is an integer, $\tau(x)$ is uniformly distributed and thus $V(D_i)_{\tau(x)} = 0$. Assuming $2^{\mathsf{Max}(f)-f(\delta_x)}$ is not an integer, let $\lfloor 2^{\mathsf{Max}(f)-f(\delta_x)} \rfloor = k$. Then $\tau(x)$ is a distribution on $\{1, \ldots, k+1\}$ and we have for some p and $p' \leq p$, $\langle j|\tau(x)|j\rangle = p$ for all $j \in \{1, \ldots, k\}$ and $\langle k+1|\tau(x)|k+1\rangle = p'$. The normalization condition is $kp + p' = 1$ and thus, $p' = 1 - kp$. We can now observe that the entropy variance $V(D_i)_{\tau(x)}$ is

simply $\mathrm{Var}(-\log p + Z) = \mathrm{Var}(Z)$, where Z is a random variable that is equal to 0 with probability $1-p'$ and to $\log p - \log p'$ with probability p'. This variance can then be computed as

$$\begin{aligned}\mathrm{Var}(Z) &= \mathbb{E}[Z^2] - \mathbb{E}[Z]^2 \\ &= p'(\log p - \log p')^2 - p'^2(\log p - \log p')^2 \\ &= p'(1-p')\log^2\left(\frac{p}{p'}\right).\end{aligned}$$

Now, we use the fact that $\log^2 z \leqslant 2z$ and continue:

$$\mathrm{Var}(Z) \leqslant 2p'(1-p')\frac{p}{p'} \leqslant 2.$$

As a result,

$$V(D_i|X_i)_{(\mathcal{D}_i\circ\mathcal{M}_i)(\omega)} \leq 2 + \mathsf{Var}(f)\ .$$

Putting everything together, Eq. (34) becomes

$$\begin{aligned}H_\alpha^\uparrow(A_1^n|B_1^nE)_{\rho_{|\Omega}} \geqslant nh - n\frac{(\alpha-1)\ln 2}{2}\left(\log(2d_A^2+1) + \sqrt{2+\mathsf{Var}(f)}\right)^2 \\ - n(\alpha-1)^2K_\alpha - \frac{\alpha}{\alpha-1}\log\frac{1}{\rho[\Omega]}\ .\end{aligned}$$

□

Theorem V.2 is then obtained from Proposition V.3 by choosing α appropriately.

Proof of Theorem V.2. We start by lower-bounding the smooth min-entropy by a Rényi entropy: for $\alpha \in (1,2]$ (see e.g., [28, Proposition 6.5]), we have

$$H_{\min}^\varepsilon(A_1^n|B_1^nE)_{\rho_{|\Omega}} \geqslant H_\alpha^\uparrow(A_1^n|B_1^nE)_{\rho_{|\Omega}} - \frac{\log(2/\varepsilon^2)}{\alpha-1}\ . \tag{38}$$

Then Proposition V.3 yields for $\alpha \in (1, 1+\frac{1}{2\ln 2})$

$$\begin{aligned}H_{\min}^\varepsilon(A_1^n|B_1^nE)_{\rho_{|\Omega}} &> nh - n\frac{(\alpha-1)\ln 2}{2}V^2 - \frac{\alpha}{\alpha-1}\log\frac{1}{\rho[\Omega]} - n(\alpha-1)^2K_\alpha - \frac{\log(2/\varepsilon^2)}{\alpha-1} \\ &\geqslant nh - n\frac{(\alpha-1)\ln 2}{2}V^2 - \frac{1}{\alpha-1}\log\frac{2}{\varepsilon^2\rho[\Omega]^2} - n(\alpha-1)^2K\ ,\end{aligned} \tag{39}$$

where for the first inequality, K_α is as in (31) and in the second inequality, we used the fact that $\alpha \leqslant 1 + \frac{1}{2\ln 2}$ and defined

$$K = 12\cdot 2^{(2\log d_A + (\mathsf{Max}(f) - \mathsf{Min}_\Sigma(f))}\ln^3\left(2^{2\log d_A + (\mathsf{Max}(f)-\mathsf{Min}_\Sigma(f))} + e^2\right)\ .$$

To make the terms in $\alpha - 1$ and $\frac{1}{\alpha-1}$ match, we choose

$$\alpha := 1 + \frac{\sqrt{2\log\frac{2}{\rho[\Omega]^2\varepsilon^2}}}{\sqrt{n\ln 2}V}\ . \tag{40}$$

Assuming that $n \geqslant \frac{8\ln 2\log\frac{2}{\varepsilon^2\rho[\Omega]^2}}{V^2}$ to have $\alpha \leqslant 1 + \frac{1}{2\ln 2}$, we obtain

$$H_{\min}^\varepsilon(A_1^n|B_1^nE)_\rho > nh - \sqrt{n}V\sqrt{(2\ln 2)\log\frac{2}{\rho[\Omega]^2\varepsilon^2}} - \frac{2\log\frac{2}{\rho[\Omega]^2\varepsilon^2}}{V^2\ln 2}K. \tag{41}$$

Note that if $n < \frac{8\ln 2\log\frac{2}{\varepsilon^2\rho[\Omega]^2}}{V^2}$ then

$$\sqrt{n}V\sqrt{(2\ln 2)\log\frac{2}{\rho[\Omega]^2\varepsilon^2}} > \frac{1}{2}nV^2.$$

As we may assume $h \leq \log d_A$ (otherwise the event Ω will have zero probability) and using the definition of V, we have that

$$\begin{aligned}n\left(h - \frac{1}{2}V^2\right) &\leqslant n\log d_A - \frac{1}{2}(\sqrt{2} + \log(2d_A^2+1))^2 n \\ &\leqslant -n\log d_A\end{aligned}$$

which implies that (28) is true in a trivial way. □

A. EAT channels with infrequent sampling

This section can be seen as a user guide to apply the entropy accumulation result presented here in the very common setting where the "testing" is only done in a few rounds that are sampled at random. From the entropy accumulation point of view, the reason for testing is to restrict the optimization involved in the tradeoff function to states $\omega_{R_{i-1}R}$ satisfying the output statistics (27), e.g., winning the CHSH game with a certain probability. However, testing can be costly in terms of randomness or rate and for this reason, the probability of testing, denoted γ is often chosen to be small. We start by defining "channels with infrequent sampling", which formalizes the concept of a protocol in which we test only a few positions:

Definition V.4 (Channel with infrequent sampling)**.** A channel with testing probability $\gamma \in [0,1]$ is an EAT channel $\mathcal{M}_{i,R_{i-1}\to X_iA_iB_iR_i}$ such that $\mathcal{X} = \mathcal{X}' \cup \{\perp\}$ and that can be expressed as

$$\mathcal{M}_{i,R_{i-1}\to X_iA_iB_iR_i}(\cdot) = \gamma \mathcal{M}^{\text{test}}_{i,R_{i-1}\to X_iA_iB_iR_i}(\cdot) + (1-\gamma)\mathcal{M}^{\text{data}}_{i,R_{i-1}\to A_iB_iR_i}(\cdot)\otimes |\perp\rangle\langle\perp|_{X_i},$$

where $\mathcal{M}^{\text{test}}_i$ never outputs the symbol $\perp$ on X_i.

The following lemma gives a general way of constructing a tradeoff function f for the map $\mathcal{M}_i$ using a sort of "crossover" tradeoff function g for the map $\mathcal{M}_i$ but using the statistics from $\mathcal{M}^{\text{test}}_i$ only. More precisely, the function g is defined by restricting the input of the map $\mathcal{M}_i$ to be ones that are consistent with the output statistics given by the map $\mathcal{M}^{\text{test}}_i$. The lemma also gives general bounds on the relevant properties of f as a function of γ and simple properties of g.

Lemma V.5. *Let $\mathcal{M}_i = \mathcal{M}_{R_{i-1}\to X_iA_iB_iR_i}$ be a channel with testing probability γ as defined above. Assume that the affine function $g : \mathbb{P}(\mathcal{X}') \to \mathbb{R}$ satisfies for any $q \in \mathbb{P}(\mathcal{X}')$*

$$g(q') \leqslant \min_{\omega \in \mathrm{D}(R_{i-1}\otimes R)} \{H(A_i|B_iR)_{(\mathcal{M}_i\otimes\mathcal{I}_R)(\omega_{R_{i-1}R})} : \left((\mathcal{M}^{\text{test}}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1}R})\right)_{X_i} = q'\}. \tag{42}$$

Note that if the set $\{\omega \in \mathrm{D}(R_{i-1}\otimes R) : \left((\mathcal{M}^{\text{test}}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1}R})\right)_{X_i} = q'\}$ is empty, the minimum is set to $+\infty$ or in other words, there is no constraint on $g(q')$. Then, the affine function $f : \mathbb{P}(\mathcal{X}) \to \mathbb{R}$ defined by

$$\begin{aligned} f(\delta_x) &= \mathsf{Max}(g) + \frac{1}{\gamma}(g(\delta_x) - \mathsf{Max}(g)) \qquad \forall x \in \mathcal{X}' \\ f(\delta_\perp) &= \mathsf{Max}(g) \end{aligned}$$

is a min-tradeoff function for $\mathcal{M}_i$. Moreover,

$$\begin{aligned} \mathsf{Max}(f) &= \mathsf{Max}(g) \\ \mathsf{Min}(f) &= \left(1 - \frac{1}{\gamma}\right)\mathsf{Max}(g) + \frac{1}{\gamma}\mathsf{Min}(g) \\ \mathsf{Min}_\Sigma(f) &\geqslant \mathsf{Min}(g) \\ \mathsf{Var}(f) &\leq \frac{1}{\gamma}\left(\mathsf{Max}(g) - \mathsf{Min}(g)\right)^2. \end{aligned}$$

Proof. The value for $\mathsf{Min}(f)$ and $\mathsf{Max}(f)$ follow directly from the definition.

To prove that f is a tradeoff function for $\mathcal{M}_i$, we first determine $\Sigma_i(q)$ (see Definition V.1). If q is not of the form $q(x) = \gamma q'(x)$ when $x \in \mathcal{X}'$ and $q(\perp) = (1-\gamma)$ for some $q' \in \mathbb{P}(\mathcal{X}')$, then we know that $\Sigma_i(q) = \emptyset$. So it suffices to focus on distributions q that have this form. Then we have

$$\begin{aligned} f(q) &= \sum_{x\in\mathcal{X}'} q(x)\left(\mathsf{Max}(g) + \frac{1}{\gamma}\left(g(\delta_x) - \mathsf{Max}(g)\right)\right) + (1-\gamma)\mathsf{Max}(g) \\ &= \mathsf{Max}(g) + \sum_{x\in\mathcal{X}'} q'(x)(g(\delta_x) - \mathsf{Max}(g)) \\ &= g(q')\ . \end{aligned}$$

Using the condition (42), we get

$$\begin{aligned} f(q) = g(q') &\leq \min_{\omega\in\mathrm{D}(R_{i-1}\otimes R)} \{H(A_i|B_iR)_{(\mathcal{M}_i\otimes\mathcal{I}_R)(\omega_{R_{i-1}R})} : \left((\mathcal{M}^{\text{test}}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1}R})\right)_{X_i} = q'\} \\ &\leq \min_{\nu\in\Sigma_i(q)} H(A_i|B_iR)_\nu\ , \end{aligned}$$

where for the last inequality, we used the fact that for a $\nu \in \Sigma_i(q)$, there exists an $\omega_{R_{i-1}R}$ such that $(\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1}R}) = \nu$ and $\left((\mathcal{M}^{\text{test}}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1}R})\right)_{X_i} = q'$. Thus, f is a min-tradeoff function.

Now for $\mathsf{Min}_\Sigma(f)$, we have

$$\begin{aligned}\mathsf{Min}_\Sigma(f) &= \min_{q:\Sigma_i(q)\neq\emptyset} f(q) \\ &\geqslant \min_{q'\in\mathbb{P}(\mathcal{X}')} g(q') \\ &= \mathsf{Min}(g)\ .\end{aligned}$$

Finally, for the variance, we have for q such that $\Sigma_i(q) \neq \emptyset$,

$$\begin{aligned}&\sum_{x\in\mathcal{X}} q(x)\left(f(\delta_x) - \sum_{x\in\mathcal{X}} q(x) f(\delta_x)\right)^2 \\ &= \sum_{x\in\mathcal{X}'} \gamma q'(x)\left(\mathsf{Max}(g) + \frac{1}{\gamma}(g(\delta_x) - \mathsf{Max}(g)) - g(q')\right)^2 + (1-\gamma)(\mathsf{Max}(g) - g(q'))^2 \\ &= \frac{1}{\gamma}\sum_{x\in\mathcal{X}'} q'(x)\left((\mathsf{Max}(g) - g(\delta_x)) - \gamma(\mathsf{Max}(g) - g(q'))\right)^2 + (1-\gamma)(\mathsf{Max}(g) - g(q'))^2\ .\end{aligned}$$

We can expand the first term and get

$$\begin{aligned}&\frac{1}{\gamma}\sum_{x\in\mathcal{X}'} q'(x)\left((\mathsf{Max}(g) - g(\delta_x)) - \gamma(\mathsf{Max}(g) - g(q'))\right)^2 \\ &= \sum_{x\in\mathcal{X}'} \frac{q'(x)}{\gamma}\left((\mathsf{Max}(g) - g(\delta_x))^2 - 2\gamma(\mathsf{Max}(g) - g(\delta_x))(\mathsf{Max}(g) - g(q')) + \gamma^2(\mathsf{Max}(g) - g(q'))^2\right) \\ &= \sum_{x\in\mathcal{X}'} \frac{q'(x)}{\gamma}(\mathsf{Max}(g) - g(\delta_x))^2 - 2(\mathsf{Max}(g) - g(q'))^2 + \gamma(\mathsf{Max}(g) - g(q'))^2 \\ &\leqslant \frac{1}{\gamma}\left(\mathsf{Max}(g) - \mathsf{Min}(g)\right)^2 - (2-\gamma)(\mathsf{Max}(g) - g(q'))^2.\end{aligned}$$

As a result,

$$\mathsf{Var}(f) \leqslant \frac{1}{\gamma}\left(\mathsf{Max}(g) - \mathsf{Min}(g)\right)^2.$$

□

Applying Theorem V.2 for a map with infrequent sampling, we get a lower bound on the min-entropy of the following form:

$$H_{\min}^{\varepsilon} \geqslant nh - c_1\sqrt{\frac{n}{\gamma}} - c_2\ ,$$

where c_1 and c_2 are constants that only depend on $\varepsilon, \rho[\Omega], d_A$ and the properties of g but not on n or the testing probability γ (in the expression of c' in Theorem V.2 the variance $\mathsf{Var}(f)$ can always be lower bounded by 0). Note that such a bound will be non-trivial as soon as $\gamma \geqslant \frac{c}{n}$ for some constant c (which corresponds to testing a constant number of rounds). This is to be contrasted with the original entropy accumulation theorem [1] that instead gives a bound of the form $nh - c_1\frac{\sqrt{n}}{\gamma} - c_2$ and hence will give a trivial bound when $\gamma = o\left(\frac{1}{\sqrt{n}}\right)$.

VI. Sample application: Device-independent randomness expansion

We now apply our result to one of the main problems to which the original EAT was applied, namely randomness expansion [2], [30]–[34]. This was done using the original EAT in [2], and, to simplify matters, the protocol we will consider here will be essentially the same. The basic task is the following: we are given a pair of devices from a malicious manufacturer; these devices might have been preprogrammed arbitrarily by the manufacturer, but once we have them, they cannot communicate back to the manufacturer. Our goal is to use those devices to generate a uniformly random string, independent from any other data in the universe, and in particular independent from the quantum data the manufacturer might have kept about our devices. It turns out to be impossible to do this without having a little bit of randomness to begin with, but it is possible to expand a small random string into a much longer one.

We give a security proof for the DI-RE protocol based on the CHSH game described in the box below. Recall that the CHSH game works as follows: a referee chooses uniformly random bits X and Y as inputs for the two devices, and the two devices must respond with $A, B \in \{0,1\}$ respectively without communicating with each other after the questions have been received. The devices win the game if $A \texttt{ XOR } B = XY$ and lose otherwise. The best winning probability for devices using a classical strategy is $3/4$, while the optimal quantum strategy wins with probability $\cos^2(\pi/8) \approx 0.85$. In [2, Equation (12)]

(based on [35, Section 2.3]), they give a bound on the amount of randomness produced by the devices assuming that they are using a strategy that allows them to win with probability at least ω; this bound is given by:

$$H(AB|TE, X = x, Y = y) \geqslant g^*(\omega) := 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega(\omega - 1) + 3}\right) \tag{43}$$

for any inputs $x, y \in \{0, 1\}$ and $\omega \in [\frac{3}{4}, \cos^2(\pi/8)]$. This bound is zero at $\omega = 3/4$, one at $\omega = \cos^2(\pi/8)$, and becomes nontrivial as soon as $\omega > 3/4$. The devices are initialized in an arbitrary state by the manufacturer, and at every round of the protocol, we play the game with the devices. To ensure that only a small amount of randomness is consumed by the process of generating the inputs, we randomly choose a small number of test positions (by generating a bit T equal to 1 for test rounds and 0 otherwise), and generate X and Y uniformly at random only for those positions. For the other rounds (that we call the "data" rounds), we always fix the inputs to $X = 0$ and $Y = 0$. In the parameter estimation step of the protocol, the number of test rounds for which $A \texttt{ XOR } B = XY$ is computed. For mathematical convenience, we will choose the positions of the test rounds in an iid manner; i.e. each individual round will have a probability γ of being a test round.

CHSH-based DI-RE protocol

Protocol arguments

$n \in \mathbb{N}$	:	number of rounds
$\gamma \in (0, 1)$	:	probability that a given position is part of the test set
$e \in [0, 1]$	:	minimum fraction of games won that is tolerated
$r \in \mathbb{R}_+$	:	generation rate

1) *Distribution:* For $i \in \{1, \ldots, n\}$:
   a) Generate a random bit T_i such that $\Pr[T_i = 1] = \gamma$.
   b) If $T_i = 0$, set $X_i = 0, Y_i = 0$, otherwise, generate X_i and Y_i uniformly over $\{0, 1\}$.
   c) Obtain outputs A_i and B_i from the two devices.
2) *Parameter estimation:* Count the number of indices l in the test set for which $A_i \texttt{ XOR } B_i \neq X_iY_i$. If $l > (1 - e)\gamma n$, then the protocol is aborted.
3) *Randomness extraction:* Apply some fixed randomness extractor $F : \{0, 1\}^k \times \mathscr{A}^n \times \mathscr{B}^n \to \{0, 1\}^{rn}$ to a uniform k-bit seed and the string (A_1^n, B_1^n); output the result as the final string.

Fig. 3. Description of the CHSH-based DI-RE protocol.

We model the behavior of the devices as follows. We let σ_{ME} be the initial state of the device, M is the system that represents the internal memory of the devices, and E is some reference system that may be in the possession of the manufacturer. Now, let $\mathcal{M}_i : M \to MT_iX_iY_iA_iB_i$ be the TPCP map that is applied by the devices in round i. We assume that each of these is of the form depicted in Figure 4, with the position subscript i added to the appropriate systems. The state at the end of step 2 of the protocol is thus:

$$\rho_{MT_1^nX_1^nY_1^nA_1^nB_1^nE} = (\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1)(\sigma_{ME}) \ ,$$

and we have computed

$$l := |\{i : T_i = 1, A_i \texttt{ XOR } B_i \neq X_iY_i\}| \ .$$

Furthermore, we define Ω as the event that we do not abort after step 2; or, in other words, it is the event that $l \leqslant (1 - e)\gamma n$. To apply the entropy accumulation theorem to this setting, we need a min-tradeoff function for the $\mathcal{M}_i$'s. Since Theorem V.2 demands an affine tradeoff function, the natural choice is to pick the tangent to g^* in (43) at a suitably chosen point $\omega \in (\frac{3}{4}, \cos^2(\frac{\pi}{8}))$. Note that we must also check that the tradeoff function is defined appropriately for all possible distributions we might observe.[2]

We are now going to use entropy accumulation to prove Theorem VI.1 below, which gives a bound on the randomness generation rate r, i.e., the ratio of uniform bits that can be generated per round of CHSH. To get a feeling for the sort of entropy production rates that can be expected of this protocol, we have plotted the final rate obtained (i.e. the lower bound on $\frac{1}{n}H_{\min}^{\varepsilon}(A_1^nB_1^n|ET_1^nX_1^nY_1^n)$) as a function of the number of rounds n when we fix the threshold e to 0.8, and when we vary the sampling probability γ. The result is in Figure 5. We note that the bounds in the figure are not obtained using the bound stated in Theorem V.2 directly but rather we used (29) with an α optimized numerically for each point on the curve.

[2]For instance, we might observe a winning rate strictly above $\cos^2(\pi/8)$ on the testing rounds: if the true winning probability of the devices is very close to optimal, then statistical fluctuations might push us slightly over the edge.

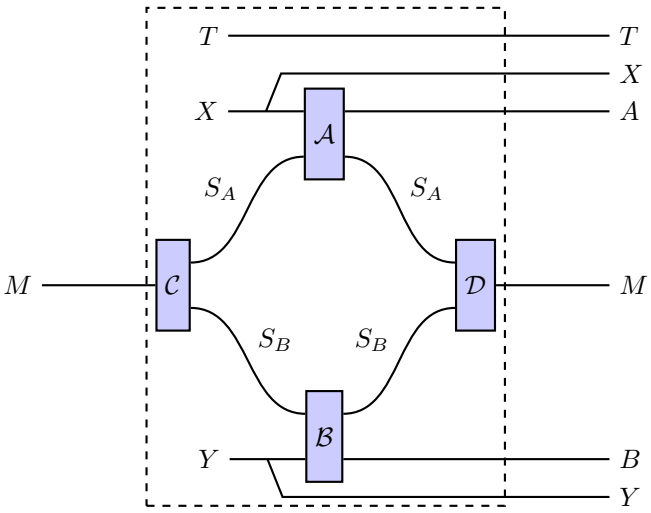

Fig. 4. Circuit diagram of $\mathcal{M} : M \to MTXYAB$. For every round of the protocol, a circuit of this form is applied, where $\mathcal{A}$ and $\mathcal{B}$ are arbitrary TPCP maps with classical output systems A and B, respectively, $\mathcal{C}$ and $\mathcal{D}$ are arbitrary TPCP maps, T is a bit equal to 1 with probability γ, and X and Y are generated uniformly at random whenever $T = 0$, and are fixed to $0, 0$ otherwise.

Theorem VI.1. *For any device fulfilling the above conditions and for any $\varepsilon \in (0,1)$, testing probability $\gamma \in (0,1)$ and $\frac{3}{4} < e < \cos^2(\frac{\pi}{8})$, after step 2 of the CHSH-based DI-RE protocol, it is the case that either:*

1) *The min-entropy of $\rho_{|\Omega}$ satisfies:*

$$H_{\min}^{\varepsilon}(A_1^n B_1^n | E T_1^n X_1^n Y_1^n)_{\rho_{|\Omega}} > n g^*(e) - \sqrt{\frac{n}{\gamma}} c - c',$$

where $c = \sqrt{2 \ln 2} \left(\log 33 + \sqrt{2 + \frac{1}{\gamma} \left(\frac{dg^*}{d\omega}(e) \right)^2} \right) \sqrt{1 - 4 \log(\varepsilon)}$ and c' is a constant only depending on ε and $\frac{dg^*}{d\omega}(e)$, or

2) *The protocol aborts with probability at least $1 - \varepsilon$.*

First note that applying a Chernoff bound, it is simple to see that provided $e < \cos^2(\pi/8)$, there exist devices that abort the protocol with probability $2^{-\Omega(\gamma n)}$. In addition, provided one is in the first case, one can obtain a secure random string of length roughly $n g^*(e)$ by choosing the extractor F to be some quantum-proof randomness extractor, such as those presented in [36]. The protocol uses approximately $(h(\gamma) + 2\gamma)n$ random bits, to decide about the testing rounds and to choose the inputs of the players on those rounds and $O(\log^3 n)$ random bits for the seed of the randomness extractor. By taking $\gamma = \Theta(\frac{\log n}{n})$ for instance we have used a polylogarithmic (in n) number of random bits and generated a linear number of bits n, thus achieving exponential randomness expansion. We refer the reader to [34], [37] for further discussions on the way to generate the random bits needed for the protocol.

Proof. We apply Theorem V.2 on ρ with the substitutions $A_i \to A_i B_i$, $B_i \to T_i X_i Y_i$, and $X_i \to C_i$, where

$$C_i = \begin{cases} \perp & \text{if } T_i = 0 \\ 1 & \text{if } T_i = 1 \text{ and } A_i \texttt{ XOR } B_i = X_i Y_i \\ 0 & \text{if } T_i = 1 \text{ and } A_i \texttt{ XOR } B_i \neq X_i Y_i. \end{cases}$$

Note that C_i is a deterministic function of the classical registers $A_i B_i X_i Y_i T_i$ and the Markov conditions are clearly satisfied.

Note that the maps $\mathcal{M}_i$ correspond to infrequent sampling maps with testing probability γ. As such, to compute a tradeoff function, we use the approach proposed in Lemma V.5. We start by determining a function $g : \mathbb{P}(\{0,1\}) \to \mathbb{R}$ satisfying the property (42). Note that a distribution $q \in \mathbb{P}(\{0,1\})$ can be uniquely specified by $q(1) \in [0,1]$. For this reason, we will interpret g as a function $g : [0,1] \to \mathbb{R}$. Note that the map $\mathcal{M}_i^{\text{test}}$ is of the form in Figure 4 except that T is fixed to 1 and thus X and Y are chosen uniformly at random, whereas $\mathcal{M}_i^{\text{data}}$ corresponds to T being fixed to 0. The inequality (43) mentioned above shows that g^* satisfies the property (42) when $q'(1) \in [\frac{3}{4}, \cos^2(\frac{\pi}{8})]$. However, g^* is not an affine function. Nonetheless, g^* is convex so any tangent provides a lower bound and also satisfies the property (42). We consider the function obtained by taking the tangent at the point $p_b \in (\frac{3}{4}, \cos^2(\frac{\pi}{8}))$: for $p \in [0,1]$

$$g_{p_b}(p) = g^*(p_b) + (p - p_b) \frac{dg^*}{d\omega}(p_b) \ . \tag{44}$$

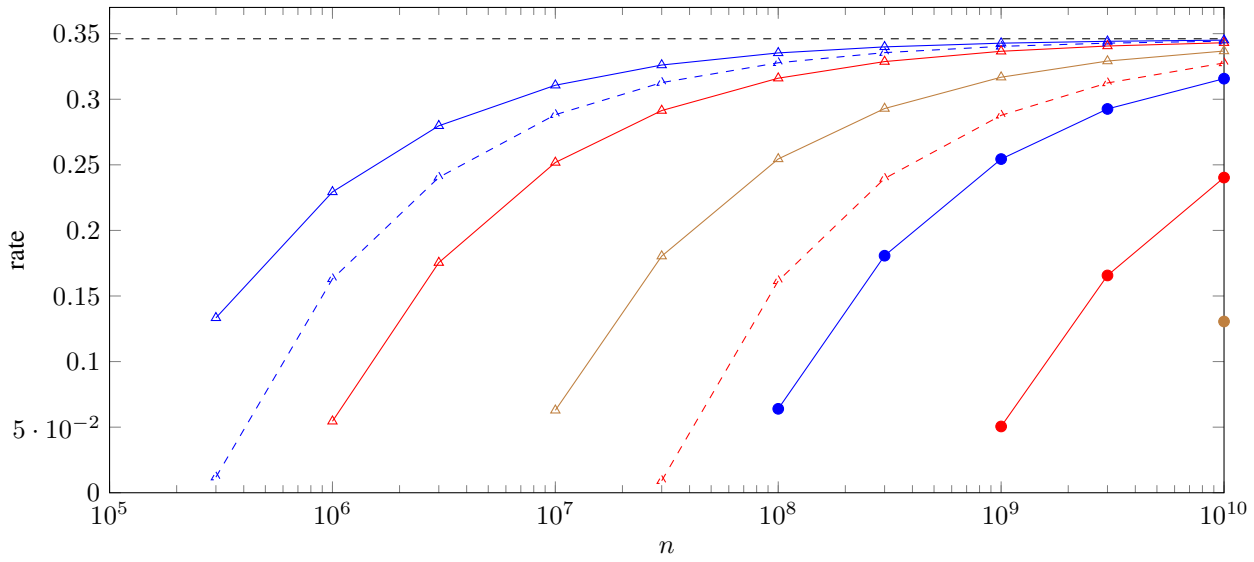

Fig. 5. Plot of the final entropy rate achieved as a function of the number of rounds n for several values of the sampling probability γ, when fixing the winning threshold e to 0.8, for both this paper (solid lines) and using the blocking technique of [2, Appendix B, rates given by equation (36)] (dashed lines). In decreasing order, we have $\gamma = 1$, $\gamma = 0.1$, $\gamma = 0.01$, $\gamma = 0.001$, $\gamma = 0.0001$, and the last point is $\gamma = 3 \times 10^{-5}$. We point out that the blocking technique of [2] only gives positive rates in this regime when $\gamma = 1$ and $\gamma = 0.1$. Here, we fixed $\varepsilon = 10^{-5}$ and assumed that $\rho[\Omega] \geqslant 10^{-5}$. The black dashed line at the top corresponds to the first-order rate of roughly 0.3461, i.e. when $n \to \infty$.

Note that g_{p_b} satisfies property (42) required by Lemma V.5: when $p \in [\frac{3}{4}, \cos^2(\frac{\pi}{8})]$ it follows from the fact that $g_{p_b}(p) \leq g^*(p)$, when $p \in [0, \frac{3}{4}]$ from the fact that $g_{p_b}(p) \leqslant 0$ and recall that for $p > \cos^2(\pi/8)$, the right hand side of (42) is $+\infty$. To get the bound stated in the theorem, we simply take $p_b = e$, but we note that choosing $p_b < e$ can lead to better bounds depending on the values of γ and n. Note that $\mathsf{Max}(g_{p_b}) = g_{p_b}(1)$ and $\mathsf{Min}(g_{p_b}) = g_{p_b}(0)$. Applying Lemma V.5, we get a min-tradeoff function f defined by $f(\delta_0) = g_{p_b}(1) + \frac{1}{\gamma}(g_{p_b}(0) - g_{p_b}(1)), f(\delta_1) = f(\delta_\perp) = g_{p_b}(1)$ and satisfies $\mathsf{Min}_\Sigma(f) \geqslant g_{p_b}(0)$ and $\mathsf{Var}(f) \leq \frac{1}{\gamma}(g_{p_b}(1) - g_{p_b}(0))^2$.

As previously mentioned Ω is defined to be the event of not aborting, i.e. using the notation of the EAT we have

$$\Omega = \{x_1^n \in \{0, 1, \perp\}^n : |\{i : x_i = 0\}| \leq (1 - e)\gamma n\}.$$

Observe that we have for $x_1^n \in \Omega$,

$$\begin{aligned} f(\mathsf{freq}(x_1^n)) &= \mathsf{freq}(x_1^n)(0) f(\delta_0) + \mathsf{freq}(x_1^n)(1) f(\delta_1) + \mathsf{freq}(x_1^n)(\perp) f(\delta_\perp) \\ &= \mathsf{freq}(x_1^n)(0) \left(g_{p_b}(1) - \frac{1}{\gamma}(g_{p_b}(1) - g_{p_b}(0)) \right) + (1 - \mathsf{freq}(x_1^n)(0)) g_{p_b}(1) \\ &\geqslant g_{p_b}(1) + (1 - e)(g_{p_b}(0) - g_{p_b}(1)) \\ &= g_{p_b}(e) \ . \end{aligned}$$

Note that if $\Pr[\Omega] < \varepsilon$, then we are in case 2 of the theorem, so we will assume that $\rho[\Omega] = \Pr[\Omega] \geqslant \varepsilon$. Applying Theorem V.2, we get

$$H_{\min}^{\varepsilon}(A_1^n B_1^n | E T_1^n X_1^n Y_1^n)_{\rho|\Omega} > n g_{p_b}(e) - \sqrt{\frac{n}{\gamma}} c - c',$$

where $c = \sqrt{2 \ln 2} \left(\log 33 + \sqrt{2 + \frac{1}{\gamma} \left(\frac{dg^*}{d\omega}(p_b) \right)^2} \right) \sqrt{1 - 4 \log(\varepsilon)}$ and c' is a constant only depending on ε and $\frac{dg^*}{d\omega}(p_b)$. □

VII. Conclusion and Open Problems

The new version of the entropy accumulation theorem presented here can now be applied directly to protocols with infrequent sampling (or to other situations where the entropy variance is significantly different from the local dimension) without paying too heavy a price. In particular, in the infrequent sampling case, the scaling in the sampling frequency γ roughly matches what we would expect in the classical i.i.d. case from Chernoff-type bounds.

As we noted earlier, another way to obtain this scaling in the infrequent sampling case is by the blocking technique used in [2, Appendix B]: instead of applying the (original) EAT to individual rounds, they apply it to blocks of size $O(\frac{1}{\gamma})$, which ensures that each block has roughly one test round. By doing this, one gets a tradeoff function (which now acts on blocks)

whose gradient scales correctly. There are multiple advantages of our method over this technique. First, it is more general, since it can gracefully handle cases beyond infrequent sampling, where $\mathsf{Var}(f)$ is substantially different from the local dimension for other reasons. It is also more natural and simpler to use, there is no need to handle the additional parameters related to the blocking. Furthermore, it appears to lead to significantly better bounds: the numerical results we obtain for the protocol given in Section VI are substantially better (see the dashed lines in Figure 5 for the bounds obtained using the blocking method), and there is no particular reason to think that this case is not representative.

While the results given here are largely good enough in practice, there are still open questions remaining. First: can we find a version of the theorem with an optimal second-order term? Ideally, we could hope for a second-order term that matches what we see in the i.i.d. case, which would look like $\sqrt{nV}\Phi^{-1}(\varepsilon^2)$ (e.g., in [9]), where Φ is the cumulative distribution function of a Gaussian distribution, and V would be an appropriate entropy variance term. Here we fall short of this in two ways: first, our V quantity is the result of applying some inequalities in the proof (see Equation (37)) that are not always tight; this may however be unavoidable if one wants to have a clean expression in terms of $\mathsf{Var}(f)$. The second issue is that the dependence in ε does not match the $\Phi^{-1}(\varepsilon)$ or $\Phi^{-1}(\varepsilon^2)$ that is usually seen in second-order expansions, but is instead similar to what is done in the fully quantum AEP of [27] and in the original EAT. This also seems very difficult to overcome in our situation, since these terms usually arise from an application of the Berry-Esseen theorem, which quantifies how much a sum of iid random variables diverges from a normal distribution, and therefore depends very strongly on the iid assumption which we do not have here.

We could also scale back our goals a bit and try to improve the last term, namely the c' in Equation (28). As it stands, this term arises from a sequence of ad-hoc inequalities that could very well be improved. It would be particularly interesting to understand which parameters this term should "really" depend on: for example, the expression we give here depends on $\rho[\Omega]$ and ε, but this may well be an artifact of our choice of α in the proof. We thus leave these questions as open problems.

APPENDIX

Lemma A.1 (Lemma B.5 in [1])**.** *Let ρ_{AB} be a quantum state of the form $\rho = \sum_x p_x \rho_{AB|x}$, where $\{p_x\}$ is a probability distribution over $\mathcal{X}$. Then, for any $x \in \mathcal{X}$ and any $\alpha \in (1, \infty)$,*

$$H_\alpha^\uparrow(A|B)_\rho - \frac{\alpha}{\alpha - 1} \log\left(\frac{1}{p_x}\right) \leqslant H_\alpha^\uparrow(A|B)_{\rho_{|x}} \ . \tag{45}$$

and for $\alpha \in (0, 1)$,

$$H_\alpha^\uparrow(A|B)_\rho - \frac{\alpha}{\alpha - 1} \log\left(\frac{1}{p_x}\right) \geqslant H_\alpha^\uparrow(A|B)_{\rho_{|x}} \ . \tag{46}$$

Lemma A.2. *Let $\rho_{ABX} = \sum_x p_x \rho_{AB}(x) \otimes |x\rangle\langle x|_X$ be a quantum state with X classical. Then, for any $\alpha \in (0, 1) \cup (1, 2]$, we have*

$$H'_\alpha(AX|B) \geqslant -\log d_A.$$

Proof. First, let us define the extension $\rho_{ABXX'} = \sum_x p_x \rho_{AB}(x) \otimes |xx\rangle\langle xx|_{XX'}$, and observe that by data processing, $H'_\alpha(AX|B) \geqslant H'_\alpha(AX|BX')$. Thus,

$$\rho_{ABXX'}^\alpha \rho_{BX'}^{1-\alpha} = \sum_x p_x \rho_{AB}(x)^\alpha \rho_B(x)^{1-\alpha} \otimes |xx\rangle\langle xx|_{XX'}$$

and therefore

$$\begin{aligned} H'_\alpha(AX|B) &\geqslant H'_\alpha(AX|BX') \\ &= \frac{1}{1-\alpha} \log \sum_x p_x 2^{(1-\alpha) H'_\alpha(A|B, X=x)_\rho} \\ &\geqslant \frac{1}{1-\alpha} \log \sum_x p_x 2^{(\alpha-1)\log d_A} \\ &\geqslant -\log d_A. \end{aligned}$$

□

ACKNOWLEDGMENTS

The authors would like to thank Rotem Arnon-Friedman for bringing to our attention the suboptimal dependence on the testing probability in the original entropy accumulation theorem and Renato Renner for his comments. We would also like the thank the IEEE Transactions on Information Theory reviewers for their detailed feedback on the manuscript. This work is supported by the French ANR project ANR-18-CE47-0011 (ACOM).

REFERENCES

[1] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation*, 2016. arXiv: 1607.01796.

[2] R. Arnon-Friedman, R. Renner, and T. Vidick, *Simple and tight device-independent security proofs*, 2016. arXiv: 1607.01797.

[3] 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.

[4] V. Strassen, "Asymptotische Abschätzungen in Shannons Informationstheorie," in *Trans. 3rd Prague Conf. Inf. Theory*, 1962, pp. 689–723.

[5] M. Hayashi, "Information spectrum approach to second-order coding rate in channel coding," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4947–4966, Nov. 2009. DOI: 10.1109/TIT.2009.2030478. arXiv: 0801.2242 [cs.IT].

[6] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *Information Theory, IEEE Transactions on*, vol. 56, no. 5, pp. 2307–2359, May 2010. DOI: 10.1109/TIT.2010.2043769.

[7] Y. Polyanskiy, "Channel coding: Non-asymptotic fundamental limits," PhD thesis, Princeton University, 2010.

[8] K. Li, "Second-order asymptotics for quantum hypothesis testing," *Annals of Statistics*, vol. 42, no. 1, pp. 171–189, Feb. 2014. DOI: 10.1214/13-AOS1185. arXiv: 1208.1400.

[9] M. Tomamichel and M. Hayashi, "A hierarchy of information quantities for finite block length analysis of quantum tasks," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7693–7710, Nov. 2013. DOI: 10.1109/TIT.2013.2276628. arXiv: 1208.1478.

[10] M. Tomamichel and V. Y. F. Tan, "Second-order coding rates for channels with state," *Information Theory, IEEE Transactions on*, vol. 60, no. 8, pp. 4427–4448, Aug. 2014. DOI: 10.1109/TIT.2014.2324555.

[11] ——, "Second-order asymptotics for the classical capacity of image-additive quantum channels," *Communications in Mathematical Physics*, vol. 338, no. 1, pp. 103–137, 2015. DOI: 10.1007/s00220-015-2382-0.

[12] F. Leditzky, "Relative entropies and their use in quantum information theory," PhD thesis, University of Cambridge, 2016. arXiv: 1611.08802.

[13] S. Beigi and A. Gohari, "Quantum achievability proof via collision relative entropy," *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7980–7986, Dec. 2014. DOI: 10.1109/TIT.2014.2361632. arXiv: 1312.3822.

[14] S. Beigi, N. Datta, and F. Leditzky, "Decoding quantum information via the petz recovery map," *Journal of Mathematical Physics*, vol. 57, no. 8, p. 082 203, 2016. DOI: 10.1063/1.4961515. arXiv: 1504.04449.

[15] N. Datta and F. Leditzky, "Second-order asymptotics for source coding, dense coding, and pure-state entanglement conversions," *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 582–608, Jan. 2015. DOI: 10.1109/TIT.2014.2366994. arXiv: 1403.2543.

[16] N. Datta, Y. Pautrat, and C. Rouzé, "Second-order asymptotics for quantum hypothesis testing in settings beyond i.i.d.—quantum lattice systems and more," *Journal of Mathematical Physics*, vol. 57, no. 6, p. 062 207, 2016. DOI: 10.1063/1.4953582. arXiv: 1510.04682.

[17] D. Petz, "Quasi-entropies for finite quantum systems," *Reports on Mathematical Physics*, vol. 23, no. 1, pp. 57–65, 1986. DOI: 10.1016/0034-4877(86)90067-4.

[18] 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. DOI: 10.1007/s00220-014-2122-x. arXiv: 1306.1586.

[19] 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, no. 12, 122203, 2013. DOI: 10.1063/1.4838856. arXiv: 1306.3142.

[20] A. E. Rastegin, "Relative error of state-dependent cloning," *Phys. Rev. A*, vol. 66, p. 042 304, 4 Oct. 2002. DOI: 10.1103/PhysRevA.66.042304.

[21] ——, "Lower bound on the relative error of mixed-state cloning and related operations," *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 5, no. 6, S647–S650, Oct. 2003. DOI: 10.1088/1464-4266/5/6/017. arXiv: quant-ph/0208159.

[22] A. Gilchrist, N. K. Langford, and M. A. Nielsen, "Distance measures to compare real and ideal quantum processes," *Phys. Rev. A*, vol. 71, p. 062 310, 6 Jun. 2005. DOI: 10.1103/PhysRevA.71.062310. arXiv: quant-ph/0408063.

[23] A. E. Rastegin, *Sine distance for quantum states*, 2006. arXiv: quant-ph/0602112.

[24] M. Tomamichel, R. Colbeck, and R. Renner, "Duality between smooth min- and max-entropies," *IEEE Trans. Inform. Theory*, vol. 56, p. 4674, 2010. arXiv: 0907.5238.

[25] M. Tomamichel, "A framework for non-asymptotic quantum information theory," PhD thesis, ETH Zurich, 2012. arXiv: 1203.2142.

[26] N. Datta, M. Tomamichel, and M. M. Wilde, "On the second-order asymptotics for entanglement-assisted communication," *Quantum Information Processing*, vol. 15, no. 6, pp. 2569–2591, Jun. 2016. DOI: 10.1007/s11128-016-1272-5. arXiv: 1405.1797.

[27] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," *IEEE Trans. Inform. Theory*, vol. 55, pp. 5840–5847, 2009. arXiv: 0811.1221.

[28] M. Tomamichel, *Quantum information processing with finite resources: Mathematical foundations*. Springer, 2015, vol. 5. arXiv: 1504.00233.

[29] M. Nussbaum and A. Szkoła, "The chernoff lower bound for symmetric quantum hypothesis testing," *Annals of Statistics*, vol. 37, no. 2, pp. 1040–1057, 2009. DOI: 10.1214/08-AOS593. arXiv: quant-ph/0607216.

[30] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," PhD thesis, University of Cambridge, 2006. arXiv: 0911.3814.

[31] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *J. Phys. A - Math. Gen.*, vol. 44, p. 095 305, 9 2011. arXiv: 1011.4474.

[32] S. Pironio, A. Acín, S. Massar, A. de La Giroday, D. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. Manning, *et al.*, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010. arXiv: 0911.3427.

[33] U. Vazirani and T. Vidick, "Certifiable quantum dice: Or, true random number generation secure against quantum adversaries," in *Proc. ACM STOC*, ACM, 2012, pp. 61–76. arXiv: 1111.6054.

[34] C. A. Miller and Y. Shi, *Universal security for randomness expansion*, 2014. arXiv: 1411.6608.

[35] 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. 045 021, 2009. DOI: 10.1088/1367-2630/11/4/045021. arXiv: 0903.4460.

[36] A. De, C. Portmann, T. Vidick, and R. Renner, "Trevisan's extractor in the presence of quantum side information," *SIAM J. Comput.*, vol. 41, no. 4, pp. 915–940, 2012. arXiv: 0912.5514.

[37] M. Coudron, T. Vidick, and H. Yuen, "Robust randomness amplifiers: Upper and lower bounds," in *Proc. APPROX-RANDOM*, Springer, 2013, pp. 468–483. arXiv: 1305.6626.