npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-026-01184-4

Optimising the relative entropy under semidefinite constraints

Gereon Koßmann[1] ✉ & René Schwonnek[2]

Finding the minimal relative entropy of two quantum states under semidefinite constraints is a pivotal problem located at the mathematical core of various applications in quantum information theory. An efficient method for providing provable upper and lower bounds is the central result of this work. Our primordial motivation stems from the essential task of estimating secret key rates for QKD from the measurement statistics of a real device. Further applications include the computation of channel capacities, the estimation of entanglement measures and many more. We build on a recently introduced integral representation of quantum relative entropy by [Frenkel, *Quantum* 7, 1102 (2023)] and provide reliable bounds as a sequence of semidefinite programs (SDPs). Our approach ensures provable sublinear convergence in the discretization, while also maintaining resource efficiency in terms of SDP matrix dimensions. Additionally, we can provide gap estimates to the optimum at each iteration stage.

Within the last four decades, the field of quantum cryptography has undertaken a massive evolution. Originating from theoretical considerations by Bennet and Brassard in 1984[1] we are now in a world where technologies like QKD systems and Quantum random number generators are on the edge of being a marked ready reality. Moreover, there is an ongoing flow (see e.g.[2,3] and references therein) of demonstrator setups and proof-of-principle experiments within the academic realm that bears a cornucopia of cryptographic quantum technologies that may reach a next stage in a not too far future.

Despite these gigantic leaps on the technological side, we have to constitute that the theoretical security analysis of quantum cryptographic systems is still in a process of catching up with these developments. To the best of our knowledge, there are yet no commercial devices with a fully comprehensive, openly accessible, and by the community verified security proof. Nevertheless, theory research has taken the essential steps in providing the building blocks for a framework that allows to do this[4]. Most notably, the development of the entropy accumulation theorem[5,6] and comparable techniques[7], allow us to deduce reliable guarantees on an ε-secure extractable finite key in the context of general quantum attacks requiring only bounds on an asymptotic quantity such as the conditional von Neumann entropy as input.

The pivotal problem, and the input to this framework, is to find a good lower bound on the securely extractable randomness that a cryptographic device offers in the presence of a fully quantum attacker[8]. Mathematically, this quantity is expressed by the conditional von Neumann entropy $H(X|E)$. Using Claude Shannon's intuitive description, it can be understood as the *uncertainty* an attacker E has about the outcome of a measurement X, which is performed by the user of a device. There are several existing numerical techniques for estimating this quantity given a set of measurement data provided by a device[9–14]. We will add to this collection, by providing a practical and resource efficient method for this problem, which interpolates between an executable tool and theoretical bounds on the relative entropy by convex interpolation.

At the core of our work stands a recently described[15,16], and pleasingly elegant, integral representation of the quantum (Umegaki) relative entropy[17] (see also[18]) that we employ in order to formulate the problem of reliably bounding $H(X|E)$ as an instance of semidefinite programs (SDP) by discretizing integrals. Our method comes with a provable sublinear convergence guarantee in the discretization, whilst staying resource efficient with the matrix dimension of the underlying SDPs. We furthermore can provide an estimate for the gap to the optimum for any discretization stage.

To this end, let $\mathcal{H} \cong \mathbb{C}^d$ be a finite-dimensional Hilbert space. Write $\mathcal{B}(\mathcal{H})$ for the (bounded) linear operators on $\mathcal{H}$ and $\mathcal{S}(\mathcal{H}) := \{\omega \in \mathcal{B}(\mathcal{H}) : \omega \geq 0,\ \mathrm{tr}[\omega] = 1\}$ for the set of quantum states (density operators). Let $h_i : \mathcal{B}(\mathcal{H}) \times \mathcal{B}(\mathcal{H}) \to \mathbb{R}$ be affine maps, for $i = 1, \ldots, n$. The central mathematical problem considered here—more general than estimating a conditional entropy $H(X|E)$ and not limited to QKD—is:

$$\begin{aligned} &\inf\ D(\rho \,\|\, \sigma) \\ &s.t.\ h_i(\rho, \sigma) \geq 0,\ i = 1, \ldots, n, \\ &\mu\, \sigma \leq \rho \leq \lambda\, \sigma, \\ &\rho, \sigma \in \mathcal{S}(\mathcal{H}), \end{aligned} \tag{1}$$

where the (Umegaki) quantum relative entropy is $D(\rho \,\|\, \sigma) := \mathrm{tr}\left[\rho\left(\log \rho - \log \sigma\right)\right]$. The constraint $\rho \leq \lambda\, \sigma$ (with finite λ) enforces $\mathrm{supp}(\rho)$

[1]Institute for Quantum Information, RWTH Aachen University, Aachen, Germany. [2]Institute for theoretical Physics, Leibniz University Hannover, Hannover, Germany. ✉e-mail: kossmann@physik.rwth-aachen.de

$\subseteq \mathrm{supp}(\sigma)$, ensuring the relative entropy to be finite; if, in addition, $\mu > 0$, then $\mathrm{supp}(\rho) = \mathrm{supp}(\sigma)$.

Despite being convex, this optimisation problem is highly non-linear and contains the analytically benign, but numerically problematic matrix logarithm. Thus, for general instances, (1) can not be solved directly by existing standard methods. The construction of a converging sequence of reliable lower bounds on the value c in (1) is the central technical contribution of this work.

Our focus task of estimating key-rates can be cast as an instance of this (see the last section of IV and Supplementary Note 7). Here, lower bounds on (1) directly translate into lower bounds on the key-rate, which is exactly the direction of an estimate needed for a reliable security proof. There is however a long list of further problems that can be formulated as an instance of (1). It includes for example the optimisation over all types of entropies which are expressible as relative entropies. For example we provide the calculation of the entanglement-assisted classical capacity of a quantum channel in the Supplementary Note 8 where one has to optimise in fact the mutual information of a bipartite system. The optimization problem (1) naturally generalizes from relative entropies to general f-divergences. With minimal adjustments, our method can also tackle this class. Despite not being the focus of this work, as a detailed numerical analysis is left for future work, we already formulated the relevant technical parts of the Methods section IV from this more general perspective.

Results

In the following, we denote by $\mathcal{B}(\mathcal{H})$ the set of (bounded) linear operators on a finite-dimensional Hilbert space $\mathcal{H}$ and $\mathcal{S}(\mathcal{H})$ the set of quantum states on $\mathcal{H}$, i.e. all positive operators with unit trace. The trace on $\mathcal{B}(\mathcal{H})$ is denoted as $\mathrm{tr}[\cdot]$. Moreover, any self adjoint operator $A \in \mathcal{B}(\mathcal{H})$, can be uniquely decomposed as a difference $A = A^+ - A^-$ of Hilbert-Schmidt orthogonal positive operators A^+ and A^-. Let $\mathrm{tr}^+[A] := \mathrm{tr}[A^+]$ denote the trace of the positive part of A (similarly $\mathrm{tr}^-[A] := \mathrm{tr}[A^-] = \mathrm{tr}^+[-A]$). Note that this is an SDP given by

$$\begin{aligned} \mathrm{tr}^+[A] = \sup\ & \mathrm{tr}[PA] \\ s.t.\ & 0 \le P \le \mathbb{I}. \end{aligned} \tag{2}$$

In the following we make use of the representation

$$D(\rho \parallel \sigma) = \int_\mu^\lambda \frac{ds}{s} \mathrm{tr}^+[\sigma s - \rho] + \log\lambda + 1 - \lambda \tag{3}$$

which was firstly described by Jenčová in ref. 15 and holds for pairs of quantum states that fulfill $\mu\sigma \le \rho \le \lambda\sigma$ with constants $\lambda > \mu \ge 0$. We remark that we always use $\mathrm{tr}^+[\cdot]$ in comparison to $\mathrm{tr}^-[\cdot]$ in[15]. The reason for that is the SDP characterization in (2), which can be written without a sign. As outlined in the following, and with more detail in the methods section, the representation (3) can be used to reformulate the non-linear function $D(\rho\|\sigma)$ as solution to a semidefinite minimisation. The leading idea of our method is then to incorporate this into (1) in order to obtain an SDP formulation of the whole problem. Along this path we make use of a discretisation of the integral in (3). This discretisation introduces a set of free variational parameters into our method, and a suboptimal choice of these will produce a gap. This gap can however be quantified and the discretisation parameters can be adjusted iteratively leading to an increasing sequence of estimates on (1).

Discretisation and SDP formulation

For an interval (a, b) with $\mu < a < b < \lambda$ we have (see the discussion around Lemma 1) the basic estimate

$$\int_a^b \frac{ds}{s} \mathrm{tr}^+[\sigma s - \rho] \ge \mathrm{tr}^+[\sigma(b-a) + \rho \log(a/b)]. \tag{4}$$

Based on (4), we discretize the integral (3) on a grid of points $\mathbf{t} = (t_1, \ldots, t_r)$, i.e. intervals (t_k, t_{k+1}), and obtain an estimate on the relative entropy from below. We furthermore use that the evaluation of the functional $\mathrm{tr}^+[\cdot]$ can be formulated as an SDP, which in combination leads us to the following proposition:

Proposition 1. For any grid $\mathbf{t}$, with $\mu \le t_1 \le \cdots \le \cdots t_r = \lambda$, the relative entropy is bounded from below by the semidefinite optimisation

$$\begin{aligned} D(\rho \parallel \sigma) \ge \inf\ & \sum_{k=1}^{r-1} \mathrm{tr}[\mu_k] + \log\lambda + 1 - \lambda \\ s.t.\ & \mu_k \ge \alpha_k \rho + \beta_k \sigma, \\ & k = 1, \ldots, r-1 \\ & \mu_k \ge 0, \end{aligned} \tag{5}$$

with coefficients

$$\alpha_k = \log\left(\frac{t_k}{t_{k+1}}\right) \text{ and } \beta_k = t_{k+1} - t_k. \tag{6}$$

Proof. Supplementary Note 1. □

Approximation of 1

We are now in a position to state the main mechanism of our method. For this purpose we fix $\mu, \lambda \in \mathbb{R}_{\ge 0}$ what guarantees that if the optimization problem (1) is feasible, it has already finite value, because the value of λ is a bound on the $D_{\max}$-relative entropy of the set of feasible states. In many applications this is known beforehand, e.g. in the key rate estimation it is given by Hayashi's pinching inequality. Defining then a grid $\mathbf{t}$ on $[\mu, \lambda]$ and combining (5) with (1) yields the SDP

$$\begin{aligned} c_l(\mathbf{t}) := \inf\ & \sum_{k=1}^{r-1} \mathrm{tr}[\mu_k] + \log\lambda + 1 - \lambda \\ s.t.\ & h_i(\rho, \sigma) \ge 0,\ i = 1, \ldots, n \\ & \mu_k \ge \alpha_k \rho + \beta_k \sigma,\ k = 1, \ldots, r-1 \\ & \mu\sigma \le \rho \le \lambda\sigma \\ & \sigma, \rho \in \mathcal{S}(\mathcal{H}),\ \mu_k \ge 0, \end{aligned} \tag{7}$$

which is a lower bound on c from (1). Moreover, optimising over all grids $\mathbf{t}$ gives the tight bound

$$c = \sup_{\mathbf{t} \subset [\mu, \lambda]} c_l(\mathbf{t}). \tag{8}$$

This reduces the task of approximating c to the quest for a good grid $\mathbf{t}$. As every grid gives a valid lower bound by Proposition 1, we are now freed to employ heuristic methods and still obtain rigorous statements, for example in a security proof.

Upper bounds and a gap estimate

In order to construct an algorithm that terminates in finite time, it is helpful to give an estimate on the accuracy of an approximation. Similar to Proposition 1, we can also construct semidefinite upper bounds for c (see Supplementary Note 3), now involving coefficients $\gamma_k, \delta_k \in \mathbb{R}$ as described

in Supplementary Note 3. Similarly to (7) we have

$$\begin{aligned} c_u(\mathbf{t}) := \inf \sum_{k=1}^{r} \mathrm{tr}[v_k] + \log\lambda + 1 - \lambda \\ s.t.\, h_i(\rho,\sigma) \geq 0\, i = 1,\ldots,n \\ v_k \geq \gamma_k\rho + \delta_k\sigma,\ k = 1,\ldots,r. \\ \mu\sigma \leq \rho \leq \lambda\sigma \\ \sigma,\rho \in \mathcal{S}(\mathcal{H}),\ v_k \geq 0. \end{aligned} \tag{9}$$

Concluding (1), (9) and (7), we get the chain of inequalities $c_l(\mathbf{t}) \leq c \leq c_u(\mathbf{t})$ and a gap estimator

$$\Delta(\mathbf{t}) = c_u(\mathbf{t}) - c_l(\mathbf{t}). \tag{10}$$

Simple methods with convergence guarantee

As our methods for establishing the lower bound (7) and the upper bound (9) rely on estimates of an integral, convergence can be guaranteed if we are able to provide uniform bounds on the integrand for all pairs of feasible states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. Again, we observe that the bound λ on $D_{\max}(\rho \parallel \sigma)$ is essential; without it, states with orthogonal supports would immediately preclude such uniformity and this is precisely why the integral representation from[15] is particularly useful: it yields a compact integration interval $[\mu, \lambda]$, provided we can bound the $D_{\max}$-relative entropy for an optimal pair of states $\rho^\star$ and $\sigma^\star$ solving (1).

The final missing ingredients, beyond compactness, to guarantee uniform convergence in our setting are provided in Lemma 1, where we show that $g(s) := \mathrm{tr}^+[\sigma s - \rho]$ is convex, monotonically increasing, and Lipschitz continuous. With these tools in place, we prove in Proposition 3 that the upper bounds converge uniformly, since they are nothing more than a convex interpolation of the function $g(s)$.

The outcome of this discussion of tools is summarized in the following corollary.

Corollary 1. Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ with $\mu\sigma \leq \rho \leq \lambda\sigma$ and $\mu > 0$. Choose the grid recursively by

$$t_k = \begin{cases} \mu, & k = 1, \\ t_{k-1} + \sqrt{4\varepsilon\, t_{k-1}}, & k \geq 2. \end{cases} \tag{11}$$

Then the total approximation error obeys

$$c_u(\mathbf{t}) - c \leq \varepsilon, \tag{12}$$

and the number of grid points satisfies the explicit bound

$$r = \mathcal{O}\left(\sqrt{\frac{\lambda}{\varepsilon}}\right). \tag{13}$$

Proof. Using Proposition 3 with $f''(s) = 1/s$ yields convergence of the interpolation: use $\int_\mu^\lambda \sqrt{f''(s)}\, ds = \int_\mu^\lambda s^{-1/2} ds = 2(\sqrt{\lambda} - \sqrt{\mu})$, and since $1/s$ is decreasing on $[\mu, \lambda]$, $L_{k-1} = 1/t_{k-1}$, yielding (11). Moreover, Corollary 3 yields that uniform convergence of the bounds is enough in order to prove that the values of (9) converge to c in (1). □

Actually choosing $\mu = 0$ in Corollary 1 yields nothing special, because then we can apply our method on the interval $[\varepsilon, \lambda]$ and get an error ε in the approximation on the interval $[0, \varepsilon]$. For details see Corollary 2. Additionally, we provide in the section "Applications to QKD" an explicit explanation how the grid construction works in practice.

Moreover, as discussed rigorously in Section IV, the lower bounds can be interpreted as a specific type of optimal supporting lines (see Section IV for a precise definition), i.e., tangents lying below $g(s)$ with respect to an integral norm determined by the weight function $s \mapsto \frac{1}{s}$. Geometrically, this can be visualized via a mirroring argument in Fig. 3. Consequently, the estimate

$$c - c_l(\mathbf{t}) \leq \varepsilon \tag{14}$$

follows immediately from Corollary 1.

We can conclude this section with the result that in a numerical algorithm the gap in (10) is in the magnitude of ε. We conclude this section with the result that the gap in (10) is on the order of ε if we choose $\mathcal{O}\left(\sqrt{\frac{\lambda}{\varepsilon}}\right)$ many grid points in the discretization.

Heuristic methods

Motivated by the observation that our approximation reduces to a linear program when ρ and σ commute—and, in particular, $\mathrm{tr}^+[\sigma s - \rho]$ is then piecewise linear, i.e., a sum of affine segments combined via a pointwise maximum—we conclude that in this case a finite set of grid points already suffices for an exact result, due to the affine nature of our approximations. Consequently, a heuristic should also allow for routines that drop points from $\mathbf{t}$ in order to remain resource-efficient.

This is especially relevant for the inner approximation, i.e., the upper bounds. In fact, one can delete all grid points except the one corresponding to the current optimizer from the previous iteration, since the upper bound is a continuous function of s. This yields a highly efficient heuristic for obtaining good upper bounds, made possible by the fact that we approximate the curves defined by $\mathrm{tr}^+[\sigma s - \rho]$ from above using a convex, continuous function. In comparison to the upper bounds, the lower bound (7) is not continuous. For this reason it is impossible to delete grid points. Therefore it becomes even more important to control the grid points wisely. An additional, but not rigorous way of getting the sequence of values monotone is that we can include a convex constraint such that the solver is enforced to stay monotone. Of course this destroys the fact that we want provable upper or lower bounds. But interestingly one can enforce monotony for a couple of rounds, then using the resulting pair of optimal states as a warm start without this constraint. This method is efficient and leads to good results.

The left plot shows the sublinear convergence rate in the discretization for a fixed state pair ρ and σ with the method from Corollary 1 in dimension 4. To be concrete, we calculated the relative entropy by its definition and the error between our approximation and this value for increasing number of grid points resulting from the iterative formula in Corollary 1. In the middle plot, we show a generic instance of (1) as discussed in (26). All numerical examples are available in the GitHub repository. The right plot shows the extractable randomness from (19) as a function of the parameter α for a state defined in (20) and a pair of mutually unbiased bases for Alice and Bob in various local dimensions up to 8, corresponding to a total dimension of 64. The plot exhibits the expected behavior with respect to depolarizing noise, parameterized by $\alpha \in [0, 1]$.

Application to quantum key distribution

We compare the key rate protocol for entanglement based QKD for local dimensions 2, 4 and 8 with the techniques from[12], our techniques and[14]. The first plot shows runtime estimates between all of the three methods and the second plots shows the precision in logarithmic scale. The system is equipped with a 13th Gen Intel® Core™ i3-1315U processor and 8 GB of RAM. The method by ref. 12 was not executable for local dimension 4 and 8, such that we replaced the values for 4 with values for local dimension 3.

The instances that initially motivate us to investigate (1) arise from the task of estimating the extractable randomness for applications in quantum cryptography. Consider a system consisting of three Hilbert spaces $\mathcal{H}_{ABE} := \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. In a basic entanglement-based QKD-setting two parties, say, Alice and Bob, perform measurements $X_0^A, \ldots, X_n^A$ and $X_0^B, \ldots, X_n^B$ on their shares of a tripartite quantum state $\psi_{ABE} \in \mathcal{H}_{ABE}$ provided by a third malicious party Eve. Following common conventions, the outcomes of measurements $X_0^A X_0^B$ will be used to generate a key, whereas

the data from all other measurements is used to test properties of the state ψ_{ABE}, and by this, bound the influence of Eve. For error correction, it is assumed that Alice's data, i.e., the outcomes of X_0^A, correspond to the correct key, which means that Bob has to correct the data arising from the measurement X_0^B. Furthermore, we will employ that each measurement X_i^S can be modeled by a channel $\Phi_i^S : \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{R}_{X_i^S})$ that maps states from a quantum system $\mathcal{H}_S$ to a probability distribution $p_{S,i}$ on a classical register $\mathcal{R}_{X_i^S}$. See also refs. 13,19 for more details on this model.

Within the notation above, the securely extractable randomness of Alice's key measurement is given by the conditional entropy $H(X_0^A|E)_{(\Phi_0^A\otimes id_E)[\rho_{AE}]}$ and depends on the reduced quantum state ρ_{AE} of the Alice-Eve system. Lower bounds on this quantity, which is up to now only defined in an asymptotic scenario, are essential for reliably bounding key rates in a full QKD setting involving multiple rounds. This accounts for the asymptotic regime, in which the Devetak-Winter formula[20] can be used, as well as for finitely many rounds under collective attacks, where the AEP can be used[21], and general attacks where either EAT[5,6] or de Finetti based methods can be employed[7,22,23].

Using a technical result for calculating the entropy of a state ρ_{AE}[13,19,24] (see Supplementary Note 2), we can express the conditional von Neumann entropy in terms of a relative entropy

$$H(X_0^A|E)_{\Phi_0^A[\rho_{AE}]} = D(\rho_{AB} \parallel \Phi_0^A[\rho_{AB}]). \tag{15}$$

Test data obtained from additional measurements X_i^S naturally give affine constraints on an unknown state ρ_{AB}. The central problem of lower bounding the extractable randomness can therefore be formulated as

$$\begin{aligned} &\inf\ D(\rho_{AB} \parallel \Phi_0^A[\rho_{AB}]) \\ &s.t.\ \Phi_i^A \otimes \Phi_j^B[\rho_{AB}] = p_{AB,ij} i,j = 1,\dots,n \\ &\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B) \\ &0 \le \rho_{AB} \le \lambda \Phi_0^A[\rho_{AB}] \end{aligned} \tag{16}$$

which is an instance of (1) to which we can apply our methodology. In order to solve (16), we need to fix constants μ and λ such that an optimal minimizer $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ satisfies

$$\mu \Phi_0^A(\rho_{AB}) \le \rho_{AB} \le \lambda \Phi_0^A(\rho_{AB}). \tag{17}$$

By Hayashi's pinching inequality, the value of λ can be chosen as the square root of the overall dimension and is therefore known in advance. Without loss of generality, the value of μ in (17) can be set to zero. In the numerical examples in the repository, the function `grid_function(c, epsilon, mu, lamb)` generates a sequence of grid points starting from the lower bound μ and ending at the upper bound λ as defined in Corollary 1. At each step, the next grid point is computed as

$$t_k = t_{k-1} + \sqrt{\frac{t_{k-1}\,\epsilon}{c}}, \tag{18}$$

where t_k denotes the current grid point. This process continues until the next point would exceed λ, at which stage the final grid value is set exactly to λ. The resulting sequence is returned as the vector `grid`.

With this in hand, we can formulate the following explicit optimization program (with $\alpha_k, \beta_k \in \mathbb{R}$ computed as in (6)) for provable lower bounds on (16):

$$\begin{aligned} &\inf \sum_{k=1}^{r-1} \mathrm{tr}[\mu_k] + \log\lambda + 1 - \lambda \\ &s.t.\ \Phi_i^A \otimes \Phi_j^B[\rho_{AB}] = p_{AB,ij}\ i,j = 1,\dots,n, \\ &\mu_k \ge \alpha_k \rho_{AB} + \beta_k \Phi_A^0(\rho_{AB})\ k = 1,\dots,r-1, \\ &\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B),\ \mu_k \ge 0. \end{aligned} \tag{19}$$

To construct a probability distribution $p_{AB,ij}$ as test data in the following examples, we start from a maximally entangled state $\Omega_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and mix it with white noise, obtaining

$$\Omega_{AB}(\alpha) := (1-\alpha)\,\Omega_{AB} + \alpha\,\frac{\mathbb{I}}{d}. \tag{20}$$

As measurement channels, we employ projective measurements in two mutually unbiased bases (see e.g.[25]). Solutions of (19) are shown in Fig. 1 the right plot for local dimensions, i.e. dimensions of Alice respectively Bob's system between 2, 4, 8, which corresponds to 1, 2, and 3 qubits per party and different values for $\alpha \in [0, 1]$. All results are achieved in seconds on a personal computer. Moreover, we can state a similar corollary as Corollary 1 for the special case of QKD:

Corollary 2. Let $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and Φ_0^A a projective measurement channel with $d_A = \dim \mathcal{H}_A$ many outcomes and choose $\varepsilon > 0$ fixed. Furthermore, choose the grid recursively by

$$t_k = \begin{cases} \varepsilon, & k = 1, \\ t_{k-1} + \sqrt{4\varepsilon\, t_{k-1}}, & k \ge 2. \end{cases} \tag{21}$$

Then the total approximation error for (19) obeys

$$c - c_l(\mathbf{t}) \le 2\varepsilon, \tag{22}$$

and the number of grid points satisfies the explicit bound

$$r = \mathcal{O}\left(\sqrt{\frac{d_A}{\varepsilon}}\right). \tag{23}$$

Proof. From Hayashi's pinching inequality (17), it follows immediately that we may choose $\lambda = d_A$. Moreover, on the interval $[\varepsilon, \lambda]$, we apply Corollary 1

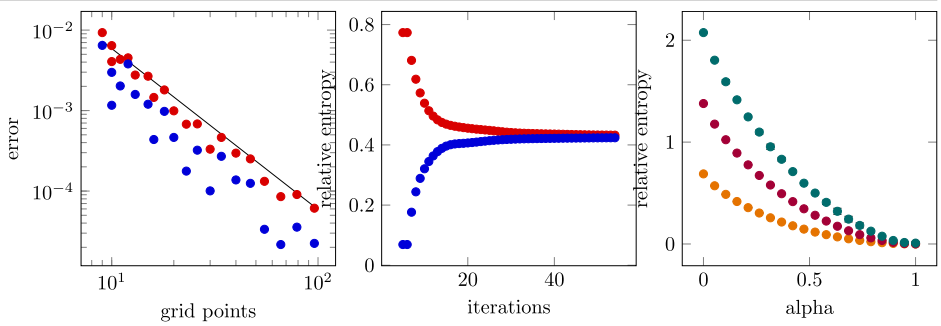

Fig. 1 | Blue are the lower bounds, green the upper bounds and the straight is a regression certifying the complexity statement In the right figure we compare local dimensions 2 (light green), 4 (green), and 8 (light blue).

to obtain an approximation error ε. Additionally, using the estimate

$$\begin{aligned}\mathrm{tr}^{+}\left[\Phi_0^A(\rho_{AB})\,s-\rho_{AB}\right] &= \sup_{0\le P\le \mathbb{I}} \mathrm{tr}\left[\mathrm{P}\left(\Phi_0^{\mathrm{A}}(\rho_{\mathrm{AB}})\,\mathrm{s}-\rho_{\mathrm{AB}}\right)\right]\\ &= \sup_{0\le P\le \mathbb{I}} \big(\mathrm{tr}[\mathrm{P}\,\Phi_0^{\mathrm{A}}(\rho_{\mathrm{AB}})]\,\mathrm{s}\\ &\qquad -\mathrm{tr}[\mathrm{P}\,\rho_{\mathrm{AB}}]\big)\\ &\le \sup_{0\le P\le \mathbb{I}} \mathrm{tr}[\mathrm{P}\,\Phi_0^{\mathrm{A}}(\rho_{\mathrm{AB}})]\,\mathrm{s}\\ &\le s,\end{aligned} \tag{24}$$

we can bound the contribution on the interval $[0, \varepsilon]$ as

$$\int_0^{\varepsilon}\frac{ds}{s}\,\mathrm{tr}^{+}\left[\Phi_0^A(\rho_{AB})\,s-\rho_{AB}\right]\le\int_0^{\varepsilon}ds=\varepsilon. \tag{25}$$

This shows that the additional error incurred by assuming $\mu = 0$ is at most ε. Combining these bounds yields (22). □

Further optimisation tasks that can be handled

As instances for the left and middle plots in Figure 1, we use a randomly generated matrix M (available in the repository) as a witness and solve problems of the form

$$\begin{aligned} c := \inf\ & D(\rho\parallel\sigma)\\ s.\,t.\ & \mathrm{tr}[\rho M]\ge\kappa_1,\\ & \mathrm{tr}[\sigma M]\le\kappa_2,\\ & \mu\sigma\le\rho\le\lambda\sigma,\\ & \sigma,\rho\in\mathcal{S}(\mathcal{H}),\end{aligned} \tag{26}$$

for various values of $\kappa_1, \kappa_2, \mu, \lambda \in \mathbb{R}$.

The left plot shows the sublinear convergence in the discretization predicted by Corollary 1 in dimension 4. We plot the error corresponding to the grid from (11) as a function of the number of grid points for a generic instance. Furthermore, in the left plot of Fig. 1, we perform a regression with the model function $n\mapsto\frac{c}{n^2}$ for a regression parameter c. The analysis shows that c is close to the chosen λ, as predicted by Corollary 1. This supports the conclusion that we have obtained the correct asymptotic convergence behavior.

Further instances of (1) are reported in Supplementary Note 7. Notable examples include bounds on the relative entropy of entanglement,

$$\min_{\sigma_{AB}\in\mathrm{SEP}(A:B)} D(\rho_{AB}\parallel\sigma_{AB}), \tag{27}$$

where SEP(A: B) denotes the set of separable states and ρ_{AB} is a possibly entangled state, as well as the classical capacity of a quantum channel (see also[9]).

The left picture shows that we can approximate a monotone and convex function from below with linear functions. It furthermore shows the corridor in which the divergence will be located. Furthermore, there is a degree of freedom in choosing a tangential straight from below. A mirrored straight g'', which is a feasible lower bound yields the same convergence rate for the lower bound. The worse case that could happen for approximation is that the function has a kink as shown on the right picture. The right picture shows an interval $[t_k, t_{k+1}]$. Then we see the error for the upper bound scales with the volume of a blunt triangle.

Discussion

The general optimisation problem in (1) is a central task in (quantum) information theory, as it encompasses all types of numerical estimates for which the relative entropy is the underlying quantity. A well-known example is given by (16), where the optimisation yields bounds on the extractable randomness in a QKD experiment (or, similarly, in a random number generation experiment). Recently, instances of (1) such as the relative entropy of entanglement in (27) and various channel-related quantities, including the classical capacity of a quantum channel, have also attracted attention. But, as already noted, the problem (1) is a nonlinear yet convex optimisation problem. Its difficulty stems from the fact that the relative entropy is only lower semicontinuous and, for certain pairs of states $(\rho, \sigma) \in \mathcal{S}(\mathcal{H}) \times \mathcal{S}(\mathcal{H})$ with $D_{\max}(\rho \parallel \sigma) = \infty$, takes the value $+\infty$. This property complicates the use of generic convex optimisation solvers for tackling (1).

Given the importance of (1), a variety of solutions have been developed with different purposes and techniques. Broadly speaking, these approaches can be classified into four categories according to their scope and the tools they employ.

The first class of methods includes the approach of[9], which estimates the relative entropy via the formula $D(\rho \parallel \sigma) = \mathrm{tr}[\rho(\log\rho - \log\sigma)]$ by numerically computing the matrix logarithm. This method is highly flexible but, for $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ with $\dim \mathcal{H} = d$, it requires working with matrices of size $d^2 \times d^2$. The second class, aimed particularly at estimating (16), includes the works[10,19,26]. The most recent of these[10] achieves very high precision (see Sec. 5, numerical testing, in ref. 10) for systems consisting of one qubit per party (i.e., Alice's and Bob's systems), but is restricted to equality constraints in (16). Inequality constraints are mentioned as an outlook for future work. The third class is represented by the recent work[14], which introduces a solver based on self-concordant barriers for specialized cones associated with the quantum (relative) entropy. This framework enables the direct application of interior-point methods to (1). Finally, in the fourth class,[12] and our present work use integral representations of the relative entropy. Specifically,[12] employs Kosaki's formula[27], while we use Frenkel's formula[16], approximating the relative entropy via numerical quadrature for the resulting integral representation.

With our technique, we propose, on the one hand, a concrete numerical tool for solving (1), which we benchmark against state-of-the-art instances in the QKD setting in Fig. 2, comparing with[14] and[12]. On the other hand, we introduce a technical method to estimate the relative entropy variationally in both directions, providing both upper and lower bounds. In comparison to other approaches, our methods contrasts by its simplicity. An implementation needs only some few line of code for implementing the SDP (1) in a favored solver and some iteration for refining the grid. This naturally provides a user with many directions for adapting refining and customizing our method beyond the implementation provided in the supplement. Furthermore, our SDP approximation can also be a starting point for an analytical handling of the relative entropy optimization problem. In terms of runtimes and resource demands our method, in its currently not highly optimized implementation, lies in between the method[12] and the recently launched and highly specialized software package[14]. However, we emphasize that[14] only addresses the case of the Umegaki relative entropy, whereas our techniques yield variational approximations for all f-divergences. In particular, since most f-divergences likely do not admit a closed-form expression analogous to the relative entropy with the matrix logarithm, our technique is, in this regime, the only applicable one.

In the numerical benchmark, we observe that for small instances our technique achieves precision comparable to[12], but is strictly outperformed by the specialized solver[14] for relative entropy programming. In terms of runtime, our method shows a clear improvement over[12], while still yielding slower performance than[14]. Beyond the numerical benchmark for (1), it is also instructive to compare our technique with[12] from a technical perspective, since both approaches rely on integral representations and thus offer comparable flexibility. In particular, our method provides provable upper and lower bounds for (1), whereas[12] yields only upper bounds. This has the advantage that we can, for example, employ the dimension-efficient formula (15) in the QKD setting, and we can quantify a gap as in (10). As another concrete application, our the our discretization technique has enabled Moreover, the flexibility of our technique has enabled the first numerically applicable algorithm for obtaining provable bounds on the relative entropy of channels — an open problem since the development of

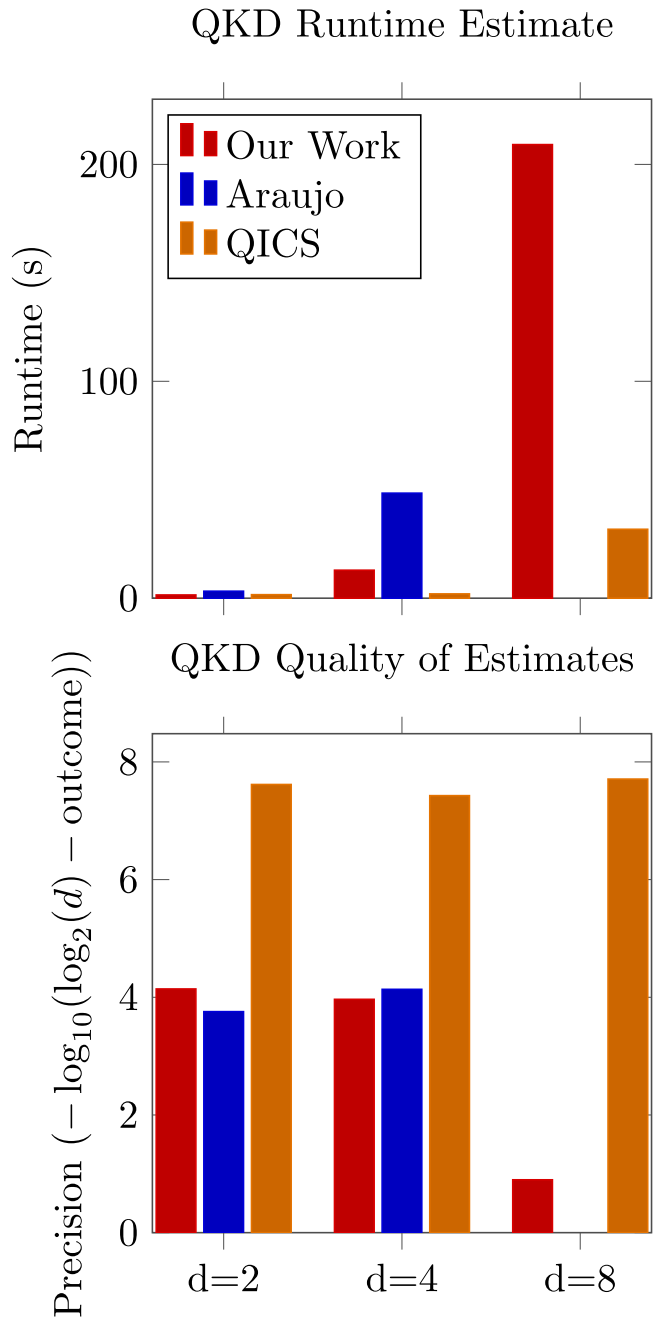

Fig. 2 | Our work is red, Araujo et al. blue and QICS orange.

resource theories for quantum channels[28]. Both applications in refs. 28 and 29 rely at their core on the discretization of Proposition 1. Although this is just one instance of the techniques presented here, and in both cases it is applied only to the Umegaki relative entropy in special scenarios, it shows that the general idea of a discretized integral representation with rigorous numerical analysis is very powerful.

Moreover, both techniques enable applications to device-independent quantum key distribution, as reported in refs. 11 and 29, which is not possible with[14]. In this regime[29] reports an efficiency advantage of our technique. From the perspective of divergences and despite the coincidental overlap in terms of the Umegaki relative entropy, our tools and those of [12] are complementary in a broad sense: Kosaki's integral formula can be extended to all operator monotone functions (see[27,Lem. 2.1]), while our approach can be generalized to all f-divergences as shown in Section IV.

Concretely regarding our technique, the fact that we need fixed integral bounds $0 < \mu \leq \lambda$ which on first view seems to be a disadvantage, turns out to be the important ingredient for a rigorous numerical analysis (i.e., theoretical error bounds). The existence of these values bounds the problem to finite range and one can think about the lower respective upper bounds as continuous functionals with values in a compact set. Therefore, a rigorous numerical analysis becomes applicable. It is a beautiful observation that compactness of the image of the functionals is equivalent to finite relative entropy. Since we are only interested in minimisation tasks here, we get rid of numerical analysis artifacts with infinities directly and naturally.

In contrast, controlling the number and places of supporting points is in general a difficult game with no a priori best solution. Of course one has to have in mind that practically the number of grid points must not be too big, because it increases the number of variables in the SDP solver directly. This calls for a clever heuristic, especially with regard to even larger dimensions. With the proofs of Proposition 3 we give a clear mathematical, and therefore rigorous, framework which one can use in constructing heuristics. In the error analysis of Proposition 3 we observe that it highly depends on f'' and its values on the grid intervals. For the function $s \mapsto s \log s$ the second derivative is given by $s \mapsto \frac{1}{s}$ and thus the error of our tools decrease as s becomes larger. In particular, if $s > 1$ the weight function $s \mapsto \frac{1}{s}$ in the integration is a damping factor. Thus, good heuristics for the Umegaki relative entropy should have a more refined grid for $s \in [\mu, 1]$ and a coarser grid in $[1, \lambda]$. Moreover, one could ask for an optimal quadrature rule regarding this specific type of integrands $s \mapsto f''(s)\mathrm{tr}^+[\sigma s - \rho]$ for f twice continuously-differentiable.

Another key could be to design a method that removes grid points as well. Many scenarios are possible here, which we leave open for future adjustment. In addition to heuristics, we would like to mention that our approach can also be carried out directly with the original integral representation of Frenkel[16]. Since the singularities at 0 and 1 play a decisive role there, it becomes much more difficult to extract provable scenarios. However, we did numerical experiments in this direction with success, but apparently without numerical analysis, i.e. theoretical error-dependencies.

We conclude with an outlook for future research. In terms of grid refinement, we believe that further improvements are possible, and that more advanced numerical quadrature techniques for the integration step in Proposition 3 and Corollary 1 may be applicable. From an information-theoretic perspective, a recent series of results has clarified how the family of α-f-divergences defined in ref. 16 relates to the well-known α-relative entropies—namely, the Petz and sandwiched relative entropies (see[30,31] for inequalities and[18,Thm. 3.2] for a regularization result). These findings suggest that our numerical techniques could be applied to estimate well-known α-entropies. Developing this connection and applying it to finite-resource tasks in information theory would be an interesting direction for future work.

Methods

As our tools easily generalize to f-divergences, we provide here the fully detailed analysis for general f-divergences. A f-divergence is defined as

$$D_f(\rho \parallel \sigma) := \int_1^\infty f''(s)\mathrm{tr}^+[\rho - s\sigma] + s^{-3}f''(s^{-1})\mathrm{tr}^+[\sigma - s\rho]\, ds, \tag{28}$$

where $f : (0, \infty) \to \mathbb{R}$ is assumed to be twice continuously differentiable with $f(1) = 0$ (see, e.g.,[18,Def. 2.4]). From[18,Prop. 2.6] it then follows that f-divergences are jointly convex in $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, satisfy the data-processing inequality (DPI) for positive trace-nonincreasing linear maps, and are faithful. As usual, we define for states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$

$$D_{\max}(\rho \parallel \sigma) := \inf\{\lambda > 0 \mid \rho \leq e^\lambda \sigma\} \tag{29}$$

where we use the convention $\inf\{\} = \infty$. We start with a first small result, generalizing[15,Cor. 1] from the Umegaki relative entropy to general f-divergences.

Proposition 2. For states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ define $\mu := e^{-D_{\max}(\sigma\|\rho)}$ and $\lambda := e^{D_{\max}(\rho\|\sigma)}$. Then we have

$$D_f(\rho \parallel \sigma) = \int_\mu^\lambda f''(s)\mathrm{tr}^+[s\sigma - \rho]\, ds + f(\lambda) + (1-\lambda)f'(\lambda). \tag{30}$$

Proof. Start from the definition (28)

$$D_f(\rho \parallel \sigma) = \int_1^\infty f''(\gamma)\mathrm{tr}^+[\rho - \gamma\sigma] + \gamma^{-3}f''(\gamma^{-1})\mathrm{tr}^+[\sigma - \gamma\rho]\, d\gamma, \tag{31}$$

With the change of variables $s = \gamma^{-1}$ in the second term,

$$D_f(\rho \parallel \sigma) = \int_1^\infty f''(s)\mathrm{tr}^+[\rho - s\sigma]\, ds + \int_0^1 f''(s)\mathrm{tr}^-[\rho - s\sigma]\, ds. \tag{32}$$

If $\mu\sigma \le \rho \le \lambda\sigma$, then $\mathrm{tr}^+[\rho - s\sigma] = 0$ for $s \ge \lambda$ and $\mathrm{tr}^-[\rho - s\sigma] = 0$ for $s \le \mu$, hence

$$D_f = \int_\mu^1 f''(s)\mathrm{tr}^-[\rho - s\sigma]\, ds + \int_1^\lambda f''(s)\mathrm{tr}^+[\rho - s\sigma]\, ds. \tag{33}$$

Using $\mathrm{tr}^+[\rho - s\sigma] = \mathrm{tr}^-[\rho - s\sigma] + (1-s)$ gives

$$D_f = \int_\mu^\lambda f''(s)\mathrm{tr}^-[\rho - s\sigma]\, ds + \int_1^\lambda (1-s)f''(s)\, ds. \tag{34}$$

Integration by parts yields

$$\begin{aligned} \int_1^\lambda (1-s)f''(s)ds &= \left[f(s) + (1-s)f'(s)\right]_1^\lambda \\ &= f(\lambda) + (1-\lambda)f'(\lambda), \end{aligned} \tag{35}$$

which proves (30). □

Proposition 2 shows that all tools needed for the relative entropy program (1) and the special case of $f(s) = s\log s$ can be discussed in the more general class of f-divergences and the optimization problem

$$\begin{aligned} c_f := \inf\ & D_f(\rho \parallel \sigma) \\ s.t.\ & h_i(\rho, \sigma) \ge 0\ i = 1, \ldots, n \\ & \mu\sigma \le \rho \le \lambda\sigma \\ & \sigma, \rho \in \mathcal{S}(\mathcal{H}). \end{aligned} \tag{36}$$

Particularly, the estimates in (7) and (9) are straightforward to generalize.

We divide the convergence analysis of (7) and (9) into two parts, namely the analysis of $\mathrm{tr}^+[\sigma s - \rho]$, which becomes a central ingredient and the convergence analysis itself then becomes the second part of this section.

Analysis of $\mathrm{tr}^+[\sigma s - \rho]$

Our method for the relaxations in (7) and (9) is based on the following observation in the f-divergence setting. Denote $w(s) := f''(s) \ge 0$ (recall that for a convex, differentiable function the derivative is an increasing function[32,Thm. 1.4.3] and thus the second derivative is positive) and use the terminology from Proposition 2 with $\mathrm{const}(\lambda) := f(\lambda) + (1-\lambda)f'(\lambda)$, then we have

$$\begin{aligned} D_f(\rho \parallel \sigma) - \mathrm{const}(\lambda) &= \int_\mu^\lambda w(s)\mathrm{tr}^+[\sigma s - \rho]\, ds \\ &= \int_\mu^\lambda w(s) \sup_{0 \le P \le \mathbb{I}} \mathrm{tr}\left[P(\sigma s - \rho)\right] ds. \end{aligned} \tag{37}$$

At this point, one may evaluate the supremum in P pointwise in $s \in [\mu, \lambda]$. But since $w(s) \ge 0$, it is valid for obtaining lower bounds to estimate the supremum once after integration. For this purpose choose $a, b \in [\mu, \lambda]$ such that $\mu \le a < b \le \lambda$ and estimate

$$\begin{aligned} &\int_a^b w(s) \sup_{0 \le P \le \mathbb{I}} \mathrm{tr}\left[P(\sigma s - \rho)\right] ds \\ &\ge \sup_{0 \le P \le \mathbb{I}} \int_a^b w(s)\mathrm{tr}\left[P(\sigma s - \rho)\right] ds. \end{aligned} \tag{38}$$

Of course, this is in general a loose estimate, but its interpretation is that we choose the best linear functional (via a single effect P) that lower bounds the trace term at the level of the weighted integral, rather than approximating the pointwise convex function $s \mapsto \mathrm{tr}^+[\sigma s - \rho]$ itself. Thus the supremum is reinterpreted from a pointwise optimization to an optimization over integrated values, while exploiting the structural properties of $s \mapsto \mathrm{tr}^+[\sigma s - \rho]$ collected in the following Lemma 1.

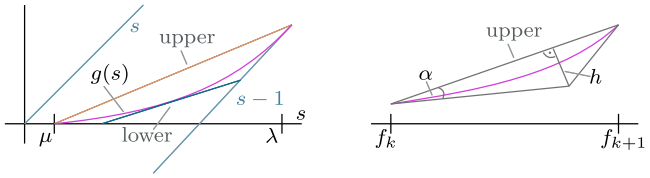

Fig. 3 | The convergence analysis. Upper and lower bound of a convex function g(s).

Lemma 1. (Properties of Divergence) Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ be two quantum states. Then $g(s) := \mathrm{tr}^+[\sigma s - \rho]$ has the following properties

(a) g is convex for $s \in \mathbb{R}$ and in particular continuous in (s, ρ, σ).
(b) g is monotonically increasing.
(c) $\mathrm{tr}^+[\sigma s - \rho]$ satisfies the data processing inequality, i.e. for every positive, trace-nonincreasing channel Φ we have

$$\mathrm{tr}^+[\sigma s - \rho] \ge \mathrm{tr}^+[\Phi(\sigma)s - \Phi(\rho)]\ \rho, \sigma \in \mathcal{S}(\mathcal{H}). \tag{39}$$

(d) for all $s \in \mathbb{R}$ we have $s - 1 \le \mathrm{tr}^+[\sigma s - \rho] \le s$.

Proof. Supplementary Note 4. □

The idea of our technique is to use a grid $\mathbf{t}$ and apply (38) interval-wise. Combining the facts that $\mathrm{tr}^+[\sigma s - \rho]$ is convex and monotonically increasing, and that interchanging the integration and supremum yields valuable lower bounds, suggests—at least heuristically—that even a small number of grid points is sufficient to obtain non-trivial lower bounds on (36).

Detailed convergence analysis

From Figure 3 it is geometrically evident that the optimised lower bound in Proposition 1 has an error no greater than that of the upper bound: by convexity, the mirrored straight line g'' is a feasible supporting line (see the discussion below for a precise definition of supporting line) for the lower bound in (7), and thus we obtain at least the same error dependence as the convex interpolation in the upper bound. Without loss of generality, and in order to focus the convergence analysis on the upper bound, in the following, we formalize this geometric observation using the properties of convex functions.

For $s \in \mathbb{R}$ let

$$g(s) := \mathrm{tr}^+[\sigma s - \rho],\ w(s) := f''(s) \ge 0, f(1) = 0, \tag{40}$$

and fix an interval $[a, b] \subseteq [\mu, \lambda]$. By Lemma 1(a), g is convex.

Recall the subdifferential of g at s_0:

$$\partial g(s_0) := \{\, m \in \mathbb{R} :\ g(s) \ge g(s_0) + m(s - s_0) \text{ for all } s \in \mathbb{R}\}. \tag{41}$$

For any $m \in \partial g(s_0)$ the affine map

$$T_{s_0,m}(s) := g(s_0) + m(s - s_0) \tag{42}$$

is a supporting line of g at s_0 (so $T_{s_0,m} \le g$ on $\mathbb{R}$ and $T_{s_0,m}(s_0) = g(s_0)$). The subdifferential mapping is monotone (see e.g.[32,Thm. 4.3.12]): if $s_1 < s_2$, $m_1 \in \partial g(s_1)$ and $m_2 \in \partial g(s_2)$, then

$$0 \le (m_2 - m_1)(s_2 - s_1) \;\Rightarrow\; m_1 \le m_2. \tag{43}$$

Recall the notion of left and right derivatives, denoted as $g'_+(\cdot), g'_-(\cdot)$, for convex functions from e.g.[32,Thm. 1.4.2] and define the secant of g over $[a, b]$ by

$$\begin{aligned} S_{a,b}(s) &:= g(a) + m_{a,b}(s - a), \\ m_{a,b} &:= \tfrac{g(b)-g(a)}{b-a} \in \left[g'_+(a),\, g'_-(b)\right]. \end{aligned} \tag{44}$$

By convexity and the generalized mean-value theorem for convex functions (see e.g.[32,Chap. 2,Ex. 2]), there exists $s^\star \in [a, b]$ with $m_{a,b} \in \partial g(s^\star)$. Hence the particular supporting line we use is simply

$$T_{s^\star,m_{a,b}}(s) = g(s^\star) + m_{a,b}(s - s^\star) \le g(s) \text{ for all } s, \tag{45}$$

and $T_{s^\star,m_{a,b}}(s^\star) = g(s^\star)$.

Moreover, since g is the pointwise supremum of the affine forms $s \mapsto \mathrm{tr}[P(\sigma s - \rho)]$ over effects P ($0 \le P \le I$), the supremum at $s^\star$ is attained by at least one effect $P^\star$ (see Danskin's theorem). For such a $P^\star$ we have

$$g(s^\star) = \mathrm{tr}\left[P^\star(\sigma s^\star - \rho)\right] \text{ and } m_{a,b} = \mathrm{tr}[P^\star \sigma], \tag{46}$$

so, equivalently, $T_{s^\star,m_{a,b}}(s) = \mathrm{tr}\left[P^\star(\sigma s - \rho)\right]$.

As a minor result, we require an adapted error analysis for the trapezoid method for the special case of a convex function. This result is essentially the classical error estimate for the trapezoid rule, as found in standard textbooks on numerical analysis (see, e.g.,[33,Eq. 5.1.7]), but stated without the assumption of differentiability.

Lemma 2. Let g be convex on $[\mu, \lambda]$ and let $\mu = t_1 < t_2 < \cdots < t_r = \lambda$ be a partition. Denote on each $[t_k, t_{k+1}]$ the secant from (44) as

$$S_k(t) \equiv S_{t_k,t_{k+1}}(t). \tag{47}$$

Then the trapezoidal–rule error satisfies

$$\sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} S_k(t)\, dt - \int_\mu^\lambda g(t)\, dt \le \tag{48}$$

$$\sum_{k=1}^{r-1} \frac{(t_{k+1} - t_k)^2}{8} \left(g'_-(t_{k+1}) - g'_+(t_k)\right). \tag{49}$$

Proof. This is [34, Cor. 3]. □

Lemma 2 enables us to prove the following technical lemma.

Lemma 3. For every convex function g and any $a < b$, the secant $S_{a,b}$ of g on $[a, b]$ and any supporting line $T_{a,b}$ of g at some $s^\star \in [a, b]$ and $w \ge 0$ and $L_{a,b} := \sup_{s\in[a,b]} w(s)$, we have

$$\int_a^b w(s)\, \left(S_{a,b}(s) - g(s)\right) ds \le \frac{L_{a,b}}{4}\, (b - a)^2\, \left(g'_-(b) - g'_+(a)\right), \tag{50}$$

$$\int_a^b w(s)\, \left(g(s) - T_{a,b}(s)\right) ds \le \frac{L_{a,b}}{4}\, (b - a)^2\, \left(g'_-(b) - g'_+(a)\right). \tag{51}$$

Proof. See Supplementary Note 6. □

Thus, on each grid interval $[t_k, t_{k+1}]$:

(i) the upper error from convex interpolation by secants, and
(ii) the lower error from the best affine minorant realized by a single effect P

are both bounded by the common quantity in (50)-(51). Thus, using the coarse weights $L_k := \sup_{s\in[t_k,t_{k+1}]} w(s)$, the optimized lower bound is at least as good as the upper bound.

Moreover, Eq. (48) has the interesting consequence that for convex g, g'_+ and g'_- exist everywhere and are nondecreasing, hence

$$\sum_{k=1}^{r-1} \left(g'_-(t_{k+1}) - g'_+(t_k)\right) \le g'_-(t_r) - g'_+(t_1), \tag{52}$$

by the observation that $-(g'_+(t_k) - g'_-(t_k)) \le 0$.

Proposition 3. (Convergence for f-divergences)

Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ with $\mu\sigma \le \rho \le \lambda\sigma$. Approximate a f-divergence via the convex interpolation upper bound on a grid $\mathbf{t} = (\mu = t_1 < t_2 < \cdots < t_r = \lambda)$:

$$\sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} w(s) g(s) ds \le \sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} w(s) S_k(s) ds, \tag{53}$$

with $g(s) = \mathrm{tr}^+[\sigma s - \rho]$ and S_k the secant of g on $[t_k, t_{k+1}]$. Fix a target accuracy $\varepsilon > 0$ and choose the grid recursively by

$$t_k = \begin{cases} \mu & k = 1 \\ t_{k-1} + \sqrt{\frac{4\varepsilon}{L_{k-1}}} & k \ge 2 \end{cases} \tag{54}$$

with $L_{k-1} := \sup_{s\in[t_{k-1},t_k]} w(s)$. Then the total interpolation error obeys

$$\sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} w(s) \left(S_k(s) - g(s)\right) ds \le \varepsilon, \tag{55}$$

and the number of grid points satisfies

$$r = \mathcal{O}\left(\frac{1}{\sqrt{\varepsilon}} \int_\mu^\lambda \sqrt{f''(s)} ds\right). \tag{56}$$

Proof. On each interval we have (see Lemma 2)

$$\begin{aligned} &\textstyle\int_{t_k}^{t_{k+1}} w(s) \left(S_k(s) - g(s)\right) ds \\ &\le \tfrac{L_k}{4} (t_{k+1} - t_k)^2 \left(g'_-(t_{k+1}) - g'_+(t_k)\right). \end{aligned} \tag{57}$$

Choose the grid by (54), so that $(t_{k+1} - t_k)^2 \le 4\varepsilon / L_k$; hence the k-th interval contributes at most $\varepsilon\left(g'_-(t_{k+1}) - g'_+(t_k)\right)$. Summing over k and using (52) with Lemma 1 (d), which yields that (52) can be estimated with 1 for $g(s) = \mathrm{tr}^+[\sigma s - \rho]$, because $\mathrm{tr}[\sigma] = 1$, implies

$$\begin{aligned} \textstyle\sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} w(s) \left(S_k - g\right) ds &\le \varepsilon \sum_{k=1}^{r-1} \left(g'_-(t_{k+1}) - g'_+(t_k)\right) \\ &\le \varepsilon. \end{aligned} \tag{58}$$

For the grid size, from (54) we have $t_k - t_{k-1} = \sqrt{4\varepsilon / L_{k-1}}$. By continuity of w, there exists $s_{k-1} \in [t_{k-1}, t_k]$ with $L_{k-1} = w(s_{k-1})$, hence

$$1 \le \frac{\sqrt{w(s_{k-1})}}{\sqrt{4\varepsilon}} (t_k - t_{k-1}). \tag{59}$$

Summing from $k = 2$ to r and passing to the Riemann sum limit gives

$$\begin{aligned} r - 1 &\le \tfrac{1}{\sqrt{4\varepsilon}} \sum_{k=1}^{r-1} \sqrt{w(s_k)}(t_{k+1} - t_k) \\ &\le z \tfrac{1}{\sqrt{4\varepsilon}} \int_{\mu}^{\lambda} \sqrt{w(s)} ds, \end{aligned} \tag{60}$$

which proves the stated bound on r. □

Recalling now the general optimization problem in the language of f-divergences (36) yields that we can approximate the value c_f by the upper bounds $c_u(\mathbf{t})$, because the bounds guarantee uniform convergence as stated in the next corollary.

Corollary 3. Let c_f be the value of (1). For a grid $\mathbf{t} = (\mu = t_1 < \cdots < t_r = \lambda)$ define

$$\begin{aligned} U_{\mathbf{t}}(\rho, \sigma) \; := \; & \sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} w(s)\, S_k(s)\, ds \\ & + f(\lambda) + (1 - \lambda) f'(\lambda), \end{aligned} \tag{61}$$

and the corresponding relaxation value

$$\begin{aligned} & c_u(\mathbf{t}) = \\ & \inf \left\{ U_{\mathbf{t}}(\rho, \sigma) : \; h_i(\rho, \sigma) \ge 0, \; \mu\sigma \le \rho \le \lambda\sigma, \; \rho, \sigma \in \mathcal{S}(\mathcal{H}) \right\}. \end{aligned} \tag{62}$$

Similarly, define with (42)

$$\begin{aligned} V_{\mathbf{t}}(\rho, \sigma) \; := \; & \sum_{k=1}^{r-1} \int_{t_k}^{t_{k+1}} w(s)\, T_{t_k, t_{k+1}}(s)\, ds \\ & + f(\lambda) + (1 - \lambda) f'(\lambda), \end{aligned} \tag{63}$$

and the corresponding relaxation value

$$\begin{aligned} & c_l(\mathbf{t}) = \\ & \inf \left\{ V_{\mathbf{t}}(\rho, \sigma) : \; h_i(\rho, \sigma) \ge 0, \; \mu\sigma \le \rho \le \lambda\sigma, \; \rho, \sigma \in \mathcal{S}(\mathcal{H}) \right\}. \end{aligned} \tag{64}$$

If $\mathbf{t}$ is chosen by (54) for a target accuracy $\varepsilon > 0$, then

$$c_f - \varepsilon \le c_l(\mathbf{t}) \le c_f \le c_u(\mathbf{t}) \le c_f + \varepsilon \tag{65}$$

and

$$r = \mathcal{O}\left(\frac{1}{\sqrt{\varepsilon}} \int_{\mu}^{\lambda} \sqrt{f''(s)}\, ds \right). \tag{66}$$

In particular, for any refining sequence of grids with $\varepsilon \downarrow 0$ we have $c_l(\mathbf{t}) \uparrow c_f$ and $c_u(\mathbf{t}) \downarrow c_f$ (monotone value convergence).

Proof. By Proposition Proposition 3 and Lemma 3, for every feasible pair (ρ, σ),

$$\begin{aligned} D_f(\rho \parallel \sigma) - \varepsilon \le V_{\mathbf{t}}(\rho, \sigma) \le D_f(\rho \parallel \sigma) \\ \le U_{\mathbf{t}}(\rho, \sigma) \le D_f(\rho \parallel \sigma) + \varepsilon. \end{aligned} \tag{67}$$

Taking the infimum over the common feasible set yields (similarly for the lower bound)

$$c_f = \inf D_f \le \inf U_{\mathbf{t}} = c_u(\mathbf{t}) \le \inf(D_f + \varepsilon) = c_f + \varepsilon. \tag{68}$$

The stated bound on r follows directly from Proposition Proposition 3. □

Data availability

Data is provided within the manuscript or supplementary information files. An implementation for all use cases is accessible upon request.

Received: 25 March 2025; Accepted: 12 January 2026;
Published online: 23 January 2026

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
2. Nadlinger, D. P. et al. Experimental quantum key distribution certified by bell's theorem. *Nature* **607**, 682–686 (2022).
3. Zhang, W. et al. A device-independent quantum key distribution system for distant users. *Nature* **607**, 687–691 (2022).
4. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **06**, 1–127 (2008).
5. Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation. *Commun. Math. Phys.* **379**, 867–913 (2020).
6. Metger, T., Fawzi, O., Sutter, D. & Renner, R. Generalised entropy accumulation. 844–850 (IEEE). https://doi.org/10.1109/FOCS54457.2022.00085 (2022).
7. Christandl, M., König, R. & Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **102**. https://doi.org/10.1103/PhysRevLett.102.020504 (2009).
8. Senno, G., Strohm, T. & Acín, A. Quantifying the intrinsic randomness of quantum measurements. *Phys. Rev. Lett.* **131**. https://doi.org/10.1103/PhysRevLett.131.130202 (2023).
9. Fawzi, H. & Fawzi, O. Efficient optimization of the quantum relative entropy. *J. Phys. A: Math. Theor.* **51**, 154003. https://doi.org/10.1088/1751-8121/aab285 (2018).
10. Hu, H., Im, J., Lin, J., Lütkenhaus, N. & Wolkowicz, H. Robust interior point method for quantum key distribution rate computation. *Quantum* **6**, 792 (2022).
11. Brown, P., Fawzi, H. & Fawzi, O. Device-independent lower bounds on the conditional von neumann entropy. *Quantum* **8**, 1445 (2024).
12. Araujo, M., Huber, M., Navascués, M., Pivoluska, M. & Tavakoli, A. Quantum key distribution rates from semidefinite programming. *Quantum* **7**, 1019 (2023).
13. Tan, E. Y.-Z., Schwonnek, R., Goh, K. T., Primaatmaja, I. W. & Lim, C. C.-W. Computing secure key rates for quantum cryptography with untrusted devices. *npj Quantum Inf* **7**, 158 (2021).
14. He, K., Saunderson, J. & Fawzi, H. Qics: Quantum information conic solver. https://arxiv.org/abs/2410.17803 (2024).
15. Jenčová, A. Recoverability of quantum channels via hypothesis testing. *Lett. Math. Phys.* **114**. https://doi.org/10.1007/s11005-024-01775-2 (2024).
16. Frenkel, P. E. Integral formula for quantum relative entropy implies data processing inequality. *Quantum* **7**, 1102 (2023).
17. Hiai, F. & Petz, D. The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.* **143**, 99–114 (1991).
18. Hirche, C. & Tomamichel, M. Quantum rényi and f-divergences from integral representations. *Commun. Math. Phys.* **405**. https://doi.org/10.1007/s00220-024-05087-3 (2024).
19. Winick, A., Lütkenhaus, N. & Coles, P. J. Reliable numerical key rates for quantum key distribution. *Quantum* **2**, 77 (2018).
20. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A: Math., Phys. Eng. Sci.* **461**, 207–235 (2005).
21. Tomamichel, M., Colbeck, R. & Renner, R. A fully quantum asymptotic equipartition property. *IEEE Trans. Inf. Theory* **55**, 5840–5847 (2009).
22. Renner, R. & Cirac, J. I. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**. https://doi.org/10.1103/PhysRevLett.102.110504 (2009).
23. Arnon-Friedman, R. & Renner, R. de finetti reductions for correlations. *J. Math. Phys.* **56**. https://doi.org/10.1063/1.4921341 (2015).

24. Tomamichel, M.*Quantum Information Processing with Finite Resources* (Springer International Publishing, 2016).
25. Klappenecker, A. & Rötteler, M.*Constructions of Mutually Unbiased Bases*, 137-144 (Springer Berlin Heidelberg). https://doi.org/10.1007/978-3-540-24633-6_10 (2004).
26. Coles, P. J., Metodiev, E. M. & Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nat. Commun.* **7**. https://doi.org/10.1038/ncomms11712 (2016).
27. KOSAKI, H. Relative entropy of states: A variational expression. *J. Oper. Theory* **16**, 335–348 (1986).
28. Koßmann, G. & Wilde, M. M. Semidefinite optimization of the quantum relative entropy of channels. https://arxiv.org/abs/2410.16362. (2024).
29. Koßmann, G. & Schwonnek, R. Bounding the conditional von-neumann entropy for device independent cryptography and randomness extraction. https://arxiv.org/abs/2411.04858 (2024).
30. Beigi, S., Hirche, C. & Tomamichel, M. Some properties and applications of the new quantum *f*-divergences. https://arxiv.org/abs/2501.03799 (2025).
31. Liu, P.-C., Hirche, C. & Cheng, H.-C. Layer cake representations for quantum divergences. https://arxiv.org/abs/2507.07065 (2025).
32. Niculescu, C. P. & Persson, L.-E.*Convex Functions and Their Applications: A Contemporary Approach* (Springer Nature Switzerland). https://doi.org/10.1007/978-3-031-71967-7 (2025).
33. Stewart, D. E.*Numerical Analysis: A Graduate Course* (Springer International Publishing). https://doi.org/10.1007/978-3-031-08121-7 (2022).
34. Dragomir, S. S. A Generalised Trapezoid Type Inequality for Convex Functions. arXiv. https://arxiv.org/abs/math/0305374 (2003).
35. Fawzi, H. & Fawzi, O. Efficient optimization of the quantum relative entropy. *J. Phys. A Math. Theor.* **51**, 154003 (2018).

Acknowledgements

We thank Mario Berta, Tobias J. Osborne, Hermann Kampermann, Martin Plavala and Zhen-Peng Xu for fruitful discussions. We thank Omar Fawzi for pointing us to the reference[35] from which we took the examples in the supplementary material. We thank Florian Oerke and Felix Golke for spotting several typos in the manuscript. GK acknowledges support from the Excellence Cluster—Matter and Light for Quantum Computing (ML4Q). GK acknowledges funding by the European Research Council (ERC Grant Agreement No. 948139). R.S.\ is supported by the DFG under Germany's Excellence Strategy—EXC-2123 QuantumFrontiers—390837967 and SFB 1227 (DQ-mat), the Quantum Valley Lower Saxony, and the BMBF projects ATIQ, SEQUIN, QuBRA, and CBQD.

Author contributions

G.K. and R.S. contributed equally to the work.

Funding

Open Access funding enabled and organized by Projekt DEAL.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-026-01184-4.

Correspondence and requests for materials should be addressed to Gereon Koßmann.