



Computational Hardness of Estimating Quantum Entropies via Binary Entropy Bounds

Yupan Liu   

School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne, Switzerland

Graduate School of Mathematics, Nagoya University, Japan

Abstract

We investigate the computational hardness of estimating the quantum α -Rényi entropy $S_\alpha^R(\rho) = \frac{\ln \text{Tr}(\rho^\alpha)}{1-\alpha}$ and the quantum q -Tsallis entropy $S_q^T(\rho) = \frac{1-\text{Tr}(\rho^q)}{q-1}$, both converging to the von Neumann entropy as the order approaches 1. The promise problems QUANTUM α -RÉNYI ENTROPY APPROXIMATION (RÉNYIQEA $_\alpha$) and QUANTUM q -TSALLIS ENTROPY APPROXIMATION (TSALLISQEA $_q$) ask whether $S_\alpha^R(\rho)$ or $S_q^T(\rho)$, respectively, is at least τ_Y or at most τ_N , where $\tau_Y - \tau_N$ is typically a positive constant. Previous hardness results cover only the von Neumann entropy (order 1) and some cases of the quantum q -Tsallis entropy, while existing approaches do not readily extend to other orders.

We establish that for all positive real orders, the rank-2 variants RANK2RÉNYIQEA $_\alpha$ and RANK2TSALLISQEA $_q$ are BQP-hard. Combined with prior (rank-dependent) quantum query algorithms in Wang, Guan, Liu, Zhang, and Ying (TIT 2024), Wang, Zhang, and Li (TIT 2024), and Liu and Wang (SODA 2025), our results imply:

- For all real order $\alpha > 0$ and $0 < q \leq 1$, LOWRANKRÉNYIQEA $_\alpha$ and LOWRANKTSALLISQEA $_q$ are BQP-complete, where both are restricted versions of RÉNYIQEA $_\alpha$ and TSALLISQEA $_q$ with ρ of polynomial rank.
- For all real order $q > 1$, TSALLISQEA $_q$ is BQP-complete.

Our hardness results stem from reductions based on new inequalities relating the α -Rényi or q -Tsallis binary entropies of different orders, where the reductions differ substantially from previous approaches, and the inequalities are also of independent interest.

2012 ACM Subject Classification Theory of computation \rightarrow Quantum information theory; Mathematics of computing \rightarrow Information theory; Theory of computation \rightarrow Quantum complexity theory

Keywords and phrases computational hardness, quantum state testing, quantum Rényi entropy, quantum Tsallis entropy, von Neumann entropy

Digital Object Identifier 10.4230/LIPIcs.STACS.2026.66

Related Version *Full Version:* <https://arxiv.org/abs/2601.03734v1> [41]

Funding This work was supported in part by funding from the Swiss State Secretariat for Education, Research and Innovation (SERI), in part by MEXT Q-LEAP grant No. JPMXS0120319794, and in part by JSPS KAKENHI grant No. JP24H00071.

Acknowledgements The author is grateful to François Le Gall and Qisheng Wang for helpful discussions, and especially to Qisheng Wang for mentioning references [38, 11]. The author also appreciates ChatGPT for suggesting the use of generalized binomial coefficients in proving Lemma 27. Additionally, the author thanks the anonymous reviewers for their constructive comments.

1 Introduction

Quantum state testing is a principal area in quantum property testing [45]. The general goal is to design efficient quantum testers that verify properties of quantum objects, extending classical (tolerant) distribution testing (see [13] and [27, Chapter 11]) to the non-commutative setting. An illustrative example concerns estimating the entropy of a quantum state ρ , particularly the von Neumann entropy $S(\rho) := -\text{Tr}(\rho \ln \rho)$, a central concept in quantum information theory. The task is to develop quantum algorithms that decide whether $S(\rho)$ is at least τ_Y or at most τ_N , where the promise gap $\tau_Y - \tau_N$ is typically a positive constant.

When an explicit circuit description (serving as “source code”) that prepares the state of interest is available, this example can be formalized as the promise problem QUANTUM ENTROPY APPROXIMATION (QEA), introduced in [5, 14]. This problem provides a complete characterization of the complexity classes NIQSZK [34], which consists of promise problems admitting non-interactive proof systems with quantum statistical zero-knowledge. Likewise, considering the entropy difference $S(\rho_0) - S(\rho_1)$ between two quantum states ρ_0 and ρ_1 leads to the promise problem QUANTUM ENTROPY DIFFERENCE (QED), which is complete for the complexity class QSZK [5], the interactive counterpart of NIQSZK.

Beyond the complexity-theoretic perspective, quantum state testing problems related to estimating quantum entropies – covering not only the von Neumann entropy but also its most popular generalization, the quantum α -Rényi entropy $S_\alpha^R(\rho) = \frac{\ln \text{Tr}(\rho^\alpha)}{1-\alpha}$ – often focus on minimizing query complexity [26, 55, 30, 65, 68] and sample complexity [2, 1, 69, 67]. Here, query complexity refers to the number of oracle calls (“queries”) to the state-preparation circuits (considered as black boxes), while sample complexity refers to the number of identical copies of the state. Moreover, the quantum Rényi entropy of different orders admits a broad range of applications, including characterizing entanglement in physical systems [32, 22], formulating entropic uncertainty relations [18], and advancing quantum cryptography, particularly through security proofs for quantum key distribution [52, 56, 74].

Another widely studied extension of the von Neumann entropy is the quantum q -Tsallis entropy, defined as $S_q^T(\rho) = \frac{1 - \text{Tr}(\rho^q)}{q-1}$, which plays an important role in physics, particularly in describing systems with non-extensive properties in statistical mechanics (see [58]). This quantity has recently attracted growing attention in works such as [43, 15]. See also scenarios closely related to the *integer*-order setting [49, 53, 76, 77], including some that establish lower bounds [16, 64]. Notably, both quantum Rényi and Tsallis entropies converge to the von Neumann entropy as the order α or q approaches 1.

Importantly, estimating (quantum) Rényi entropy appears inherently more challenging than estimating (quantum) Tsallis entropy for orders greater than 1. On one hand, as observed in [2, Appendix A], any estimator for α -Rényi entropy directly yields an estimator for q -Tsallis entropy with the same bound when $q = \alpha > 1$. On the other hand, while sample complexity lower bounds for estimating α -Rényi entropy with real-valued $\alpha > 1$ scale polynomially with the rank of the state (referred to as “rank-dependent” in this work) [48, 66], sample complexity upper and lower bounds for estimating q -Tsallis entropy with real-valued $q > 1$ are *independent* of the rank [43, 15].

This complexity-theoretic perspective connects closely to the query complexity setting. In particular, explicit rank-dependent estimators for quantum α -Rényi entropy with any positive order α [68, 65] implies that the corresponding promise problem restricted to states ρ of polynomial rank (the “low-rank” case), LOWRANKRÉNYIQEA $_\alpha$, is in BQP – in other words, this task is efficiently solvable by a universal quantum computer. For quantum q -Tsallis entropy, a rank-dependent estimator for orders $0 < q \leq 1$ [65] similarly implies that the

low-rank version, $\text{LOWRANKTSALLISQEA}_q$, is in BQP, while a rank-independent estimator for real-valued orders $q > 1$ [43] shows that the corresponding problem TSALLISQEA_q , *without rank constraints*, is also in BQP.

While the containments in BQP are well understood, hardness results are limited. Specifically, BQP-hardness has been established only for RANK2TSALLISQEA_q with $1 \leq q \leq 2$ [43], where the state of interest has exactly rank *two*, and no analogous BQP-hardness result is known for $\text{RANK2RÉNYIQEA}_\alpha$ beyond the special case $\alpha = 1$, which coincides with the von Neumann entropy. This gap leads to the following intriguing and natural question:

► **Problem 1.** How hard is the task of estimating α -Rényi or q -Tsallis entropy of quantum states for *all* positive order α or q ? Could the low-rank versions, $\text{LOWRANKRÉNYIQEA}_\alpha$ and $\text{LOWRANKTSALLISQEA}_q$,¹ capture the full power of quantum computation, that is, are these promise problems BQP-hard?

To establish lower bounds on query and sample complexities, one typically begins by identifying hard instances and then analyzing the resulting bounds for the corresponding scenarios, such as estimating quantum Rényi or Tsallis entropies of different orders. In contrast, establishing computational hardness in Problem 1 generally relies on reductions, since only a few natural hard problems are known for a given complexity class. Constructing such reductions from other promise problems to these entropy-approximation tasks is often technically more challenging than in other quantum state testing problems. This difficulty arises because differences of quantum entropies relate to closeness measures only in specific ways, and these relationships hold within a limited regime due to fundamental mathematical constraints, such as joint convexity, as discussed in Section 1.2.

1.1 Main results

In this work, we show that $\text{RANK2RÉNYIQEA}_\alpha$ and RANK2TSALLISQEA_q are BQP-hard for *all* positive orders α and q , even with constant additive-error precision (Theorem 2). Our results fully resolve Problem 1 in the low-rank setting and introduce a new, systematic approach to establishing the computational hardness of estimating quantum entropies.

► **Theorem 2** (Computational hardness of estimating quantum entropies, informal version of Theorems 29 and 34). *The following statements hold:*

- (1) For all real-valued $\alpha > 0$ and $\alpha = \infty$, $\text{RANK2RÉNYIQEA}_\alpha$ is BQP-hard;
- (2) For all real-valued $q > 0$, RANK2TSALLISQEA_q is BQP-hard.

We next summarize the known quantum query upper bounds for estimating quantum entropies [65, 68, 43], as presented in Table 1.² The input model underlying these upper bounds is the *purified quantum access input model*, originally introduced in [70]. In particular, these upper bounds imply containments of complexity classes when the descriptions of the state-preparation circuits (“source codes”) are explicitly provided.

By combining Theorem 2 with the quantum query algorithms of [65, 68, 43], whose upper bounds are summarized in Table 1, we obtain the following corollaries:

¹ The classical analog of the *low-rank* condition for quantum states in entropy estimation problems is the *poly-size support* condition for classical distributions. This problem has received much less attention, partly because classical distributions are inherently given in the computational basis, which is fixed and efficiently computable. By contrast, for quantum states the relevant basis is typically unknown and difficult to compute efficiently, even in low-rank cases, making the quantum version more compelling.

² The notation $\tilde{O}(f)$ is used to denote $O(f \text{ polylog}(f))$.

■ **Table 1** (Rank-dependent) quantum query complexity upper bounds.

Order (α or q)	Quantum α -Rényi entropy	Quantum q -Tsallis entropy
(0, 1)	$\tilde{O}(r^{\frac{1}{\alpha}}/\epsilon^{1+\frac{1}{\alpha}})$ [68, Corollary 4]	$\tilde{O}(r^{\frac{3-q^2}{2q}}/\epsilon^{\frac{3+q}{2q}})$ [65, Theorem III.9]
1	$\tilde{O}(r/\epsilon^2)$ [65, Theorem III.1]	
(1, ∞)	$\tilde{O}(r/\epsilon^{1+\frac{1}{\alpha}})$ [68, Corollary 5]	$O(1/\epsilon^{1+\frac{1}{q-1}})$ [43, Theorem 3.2]

► **Corollary 3.** *For all real-valued $\alpha > 0$, $\text{LOWRANKRÉNYIQEA}_\alpha$ is BQP-complete.*

► **Corollary 4.** *The following holds:*

(1) *For all real-valued $q \in (0, 1]$, $\text{LOWRANKTSALLISQEA}_q$ is BQP-complete;*

(2) *For all real-valued $q > 1$, TSALLISQEA_q is BQP-complete.*

It is worth highlighting that the rank-2 case is the *smallest* non-trivial rank that captures BQP-hardness of estimating quantum entropies, since all pure states (i.e., the rank-1 case) have *zero* entropy. By contrast, for closeness testing of quantum states with respect to the trace distance, BQP-hardness already arises in the pure-state setting [51, 66]. The possibility that rank-2 instances capture BQP-hardness was implicitly suggested in [43]. Our proof of Theorem 2 further clarifies the underlying reason: the reduction essentially relies on inequalities relating quantum *binary* entropies of different orders (see Section 1.3 for details).

In addition to estimating quantum entropies of positive orders, we also investigate the order-zero case for quantum Rényi and Tsallis entropies, as stated in Theorem 5. For the Rényi entropy, this case corresponds to the quantum max (Hartley) entropy; while for the Tsallis entropy, it essentially coincides with the rank of the state.

► **Theorem 5** (Informal version of Theorem 39). *For order $\alpha = 0$ and $q = 0$,*

$\text{RANK2RÉNYIQEA}_\alpha$ *and* RANK2TSALLISQEA_q *are NQP-complete.*

Notably, the behavior of quantum query upper bounds for estimating these order-zero entropies aligns with Theorem 5: such bounds scale polynomially with the reciprocal of the smallest non-zero eigenvalue of the state [65, Section III.B], which can be arbitrarily small in general. In particular, the complexity class NQP can be viewed as a precise variant of BQP that always rejects *no* instances, where the promise gap may be arbitrarily small. This class is equal to the classical class $\text{coC=P} = \text{NQP}$ [3, 75], where C=P , introduced in [63], is closely related to the standard counting class PP, since $\text{C=P} \subseteq \text{PP} \subseteq \text{NP}^{\text{C=P}}$.³

1.2 Previous approaches to establishing computational hardness

Before presenting the proof techniques underlying Theorem 2, we briefly review known approaches to establishing the computational hardness of the QUANTUM ENTROPY APPROXIMATION PROBLEM (QEA) and its variants. One standard approach proceeds via

³ Since PP is closed under complement, it follows that $\text{coC=P} \subseteq \text{PP}$. For further details and properties of C=P , which lies within the counting hierarchy, we refer to [72].

the QUANTUM ENTROPY DIFFERENCE PROBLEM (QED), which concerns the quantity $S(\rho_0) - S(\rho_1)$ and can be solved using a search version of QEA.⁴ The key quantity in this approach is the distance version of the (quantum) entropy difference [59, 5], namely the quantum Jensen–Shannon divergence (QJS) introduced in [44],

$$\text{QJS}(\rho_0, \rho_1) := S\left(\frac{\rho_0 + \rho_1}{2}\right) - \frac{S(\rho_0) + S(\rho_1)}{2},$$

whose square root is a distance metric [62, 54]. A particularly direct proof was recently outlined in [43, Equation (4)], crucially relying on the following identity:

$$2 \cdot \text{QJS}(\rho_0, \rho_1) = S\left(\left(\frac{\rho_0 + \rho_1}{2}\right) \otimes \left(\frac{\rho_0 + \rho_1}{2}\right)\right) - S(\rho_0 \otimes \rho_1). \quad (1)$$

By combining Equation (1) with known inequalities relating QJS to the trace distance [23, 9], one can directly reduce the QUANTUM STATE DISTINGUISHABILITY PROBLEM (QSD), defined in terms of the trace distance, to QED. Since QSD is QSZK-hard [70, 71], it follows that QED is QSZK-hard under Karp reduction, and consequently, QEA is QSZK-hard under Turing reduction.

The tailor-made approach described above applies only to the order-1 case (von Neumann entropy). A more general method for proving the QSZK-hardness of QED, developed in [5] (see also a simplified version in [40]), relies on additional information-theoretic tools, including Fannes’ inequality. This method extends naturally to the promise problems TSALLISQEA_q and TSALLISQED_q for $1 < q \leq 2$, which are defined in [43] and correspond to the quantum q -Tsallis entropy of the relevant orders. The key quantity in this extension is the quantum q -Jensen–Tsallis divergence (QJT_q) introduced in [9], whose square root also serves as a distance metric [54]. The main technical challenge lies in the corresponding inequalities relating these divergences to the trace distance, which were established only very recently in [43, Section 4], using the joint convexity of QJT_q for the relevant orders [17, 61]. The proof is then completed in analogy with the order-1 case, employing Fannes’ inequality and the basic properties of the quantum q -Tsallis entropy as provided in [50, 24, 78], and the argument requires a complicated trade-off in choosing parameters.

Nevertheless, such joint convexity properties do not hold in general for the (quantum) q -Tsallis entropy of arbitrary order q , even in the classical case [12]. In addition, although the quantum α -Jensen–Rényi divergence (QJR_α) was studied a few years ago in [54] and shown to be the square of a metric for $0 < \alpha < 1$, its joint convexity has not been investigated and may not hold for positive order α in general.

Another common approach is to reduce the QUANTUM STATE CLOSENESS TO MAXIMALLY MIXED STATE (QSCMM) to QEA. This promise problem, defined via the trace distance with the state ρ_1 fixed to be the n -qubit maximally mixed state $(I/2)^{\otimes n}$, is complete for the class NQSZK [34, 5, 14]. These reductions rely on inequalities that relate different quantum entropies, such as the von Neumann entropy, to the trace distance $T(\rho, (I/2)^{\otimes n})$, which can be characterized through optimization problems. In particular, the optimization problem corresponding to the easy direction is typically convex, such as [35, Lemma 16], while the one for the hard direction may be *non-convex* in general,⁵ as in the case of the quantum q -Tsallis entropy $S_q^T(\rho)$ with $q = 1 + \frac{1}{n-1}$ [43, Section 4.4].

⁴ Specifically, one can decide whether a given QED instance corresponding to (ρ_0, ρ_1) is a *yes* or *no* instance by estimating $S(\rho_0)$ and $S(\rho_1)$ separately to the required precision.

⁵ For the order-1 case, the hard direction follows directly from the inequality in [60].

Since solving non-convex optimization problems, even approximately, is often technically challenging, this approach does not extend readily to quantum entropies of positive orders and requires further work in the low-rank setting. In particular, it is necessary to establish analogous inequalities that connect $S_q^T(\rho)$ with $T(\rho, \rho_{\mathcal{V}})$, where $\rho_{\mathcal{V}}$ denotes an n -qubit quantum state of polynomially bounded rank with uniformly distributed eigenvalues.

1.3 Proof techniques

We now outline the proof strategy underlying Theorem 2. Our starting point is an alternative and simplified argument establishing that RANK2QEA is BQP-hard, which serves as an illustrative example of our new approach. While this hardness result was already shown in [43, Theorem 1.2(1)], their proof establishes BQP-hardness only under Turing reduction, specifically through reductions to the counterpart quantum entropy difference problem.⁶

Our method is guided by two key observations. The first observation is the following identity: the quantum 2-Tsallis entropy of a rank-2 state $\frac{1}{2}(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|)$, which in some sense is “BQP-hard to prepare”, coincides with the 2-Tsallis *binary* entropy $H_2^T(x)$:

$$S_2^T\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right) = \frac{1 - |\langle\psi_0|\psi_1\rangle|^2}{2} = H_2^T\left(\frac{1 - |\langle\psi_0|\psi_1\rangle|}{2}\right). \quad (2)$$

In particular, these expressions are proportional to $1 - |\langle\psi_0|\psi_1\rangle|^2$, whose constant-precision estimation is known to be BQP-hard [51]. This equivalence immediately implies the BQP-hardness of RANK2TSALLISQEA₂. To extend the hardness result to RANK2TSALLISQEA_q for other orders q , including the order-1 case, i.e., the von Neumann entropy, it suffices to establish inequalities relating $H_2^T(x)$ to the q -Tsallis binary entropy.

The second observation is that the (Shannon) binary entropy admits the following power-type bounds, which have been known for more than two decades [57, 39], and can be expressed in terms of the 2-Tsallis binary entropy:⁷

$$2H\left(\frac{1}{2}\right) \cdot H_2^T(x) \leq H(x) \leq \sqrt{2}H\left(\frac{1}{2}\right) \cdot \sqrt{H_2^T(x)}. \quad (3)$$

Taken together, these two key observations yield a reduction from the quantity $1 - |\langle\psi_0|\psi_1\rangle|^2$, which is BQP-hard to estimate [51], to RANK2QEA, thereby establishing the BQP-hardness of RANK2QEA under Karp reduction.

Unlike the previous approach based on the quantum (Tsallis) entropy difference [5, 40, 43], which essentially relies on the quantum Jensen-type divergences and is therefore quite restrictive in the choice of orders, our new approach to establishing BQP-hardness extends beyond RANK2TSALLISQEA_q for arbitrary positive real orders and also applies to RANK2RÉNYIQEA_α. The first key observation admits a Rényi analogue, given by identity in Equation (4), which parallels Equation (2):

$$S_2^R\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right) = \ln(2) - \ln(1 + |\langle\psi_0|\psi_1\rangle|^2) = H_2^R\left(\frac{1 - |\langle\psi_0|\psi_1\rangle|}{2}\right). \quad (4)$$

⁶ Nevertheless, unlike other quantum complexity classes such as QSZK, BQP-hardness under Turing reduction is *no weaker* than BQP-hardness under Karp reduction, since the BQP subroutine theorem [6, Section 4] implies that $\text{BQP}^{\mathcal{A}} \subseteq \text{BQP}$ holds for any efficient quantum algorithm \mathcal{A} .

⁷ The lower bound is a special case of [31, Theorem II.6], with a direct proof given in [57]. The upper bound can be further strengthened to $H(x) \leq 2^{\frac{1}{2H(1/2)}} H(1/2) \cdot H_2^T(x)^{\frac{1}{2H(1/2)}}$ (see [57, Theorem 1.2]).

The second key observation involves inequalities relating Rényi or Tsallis binary entropies of different orders to the corresponding order-2 binary entropies. These inequalities, summarized in Tables 2 and 3, differ depending on the range of the orders under consideration.

■ **Table 2** Computational hardness of RANK2RÉNYIQEA_α with constant precision.

Range of α	Range of n	Hardness	Reduction from	New inequalities
$\alpha = 0$	$n \geq 2$	NQP-hard Theorem 39	N/A	None
$0 < \alpha < 1$	$n \geq \lceil 2/\alpha \rceil$	BQP-hard Theorem 31(1)	RANK2RÉNYIQEA ₂ Theorem 30	$H_2^R(x) \leq H_\alpha^R(x)$ $H_\alpha^R(x) \leq \ln(2)^{1-\frac{\alpha}{2}} \cdot H_2^R(x)^{\frac{\alpha}{2}}$
$1 \leq \alpha < 2$	$n \geq 2$	BQP-hard Theorem 31(2)	RANK2RÉNYIQEA ₂ Theorem 30	[4, Section 5.3] & Theorem 20
$\alpha = 2$	$n \geq 2$	BQP-hard Theorem 30	Estimating $1 - \langle \psi_0 \psi_1 \rangle ^2$ [51, Theorem 12]	None
$\alpha \in (2, \infty]$	$n \geq 2$	BQP-hard Theorem 32	RANK2RÉNYIQEA ₂ Theorem 30	$\frac{\alpha}{2(\alpha-1)} \cdot H_2^R(x) \leq H_\alpha^R(x) \leq H_2^R(x)$ Theorem 22 & [4, Section 5.3]

Interestingly, the inequalities for q -Tsallis binary entropy in Table 3 require consideration of an additional case. This phenomenon is intuitively linked to the monotonicity of the *normalized* q -Tsallis binary entropy, $\tilde{H}_q^T(x) := H_q^T(x)/H_q^T(1/2)$, implicitly studied in [19]. Numerical evidence suggests a transition point $q^*(x) \in [2, 3]$ at which $\tilde{H}_q^T(x)$ changes monotonicity: it is monotonically decreasing on $q \in [0, q^*(x))$ and monotonically increasing on $q > q^*(x)$. This informally explains the additional row for $q \in (2, 3]$ in Table 3.

■ **Table 3** Computational hardness of RANK2TSALLISQEA_q with constant precision.

Range of q	Range of n	Hardness	Reduction from	New inequalities
$q = 0$	$n \geq 2$	NQP-hard Theorem 39	N/A	None
$0 < q < 1$	$n \geq \lceil 1/q \rceil$	BQP-hard Theorem 36(1)	RANK2TSALLISQEA ₂ Theorem 35	$2H_q^T(\frac{1}{2}) \cdot H_2^T(x) \leq H_q^T(x)$ $H_q^T(x) \leq 2^{q/2} H_q^T(\frac{1}{2}) \cdot (H_2^T(x))^{q/2}$
$1 \leq q < 2$	$n \geq 2$	BQP-hard Theorem 36(2)	RANK2TSALLISQEA ₂ Theorem 35	[43, Lemma 4.8] & Theorem 24
$q = 2$	$n \geq 2$	BQP-hard Theorem 35	Estimating $1 - \langle \psi_0 \psi_1 \rangle ^2$ [51, Theorem 12]	None
$2 < q \leq 3$	$n \geq 2$	BQP-hard Theorem 37	RANK2TSALLISQEA ₂ Theorem 35	$\frac{q}{2(q-1)} \cdot H_2^T(x) \leq H_q^T(x) \leq 2H_q^T(\frac{1}{2}) \cdot H_2^T(x)$ Theorem 26(1)
$q \in (3, \infty)$	$n \geq \lceil \log_2 q \rceil$	BQP-hard Theorem 38	RANK2TSALLISQEA ₂ Theorem 35	$2H_q^T(\frac{1}{2}) \cdot H_2^T(x) \leq H_q^T(x)$ $H_q^T(x) \leq \frac{q}{2(q-1)} \cdot H_2^T(x)$ [43, Lemma 4.8] & Theorem 26(2)

1.4 Discussion and open problems

Perhaps the most intriguing open problem is the following – what are the limitations of our new approach for establishing the computational hardness of estimating quantum entropies? In particular, can one prove the hardness of the QUANTUM α -RÉNYI ENTROPY APPROXIMATION PROBLEM (RÉNYIQEA_α) for any positive order α ? The well-known inequalities

$$S_\infty^R(\rho) \leq S_2^R(\rho) \leq 2 \cdot S_\infty^R(\rho)$$

can be almost straightforwardly generalized to relate the (quantum) min-entropy to the (quantum) α -Rényi entropy for the order $\alpha > 1$.⁸

$$S_\infty^R(\rho) \leq S_\alpha^R(\rho) \leq \frac{\alpha}{\alpha - 1} \cdot S_\infty^R(\rho). \quad (5)$$

However, our new approach is effective only when the values of the quantum entropies and the promise gap are of comparable magnitude, e.g., when both are constant. Otherwise, reductions based on inequalities relating the quantum min entropy (in the order- ∞ case) to the quantum Rényi entropy of other orders break down for sufficiently large n .

Beyond this technical limitation, a more fundamental complexity-theoretic barrier arises. Specifically, estimating the min-entropy RÉNYIEA_∞ is coSBP -complete [73].⁹ Any reduction analogous to our approach for establishing Theorem 2 would imply that the $\text{ENTROPY APPROXIMATION PROBLEM EA}$ is coSBP -hard. Since EA is known to be NISZK -complete [28, 29], combining such a reduction with the coSBP -hardness of RÉNYIEA_∞ would yield

$$\text{coNP} \subseteq \text{coSBP} \subseteq \text{NISZK} \subseteq \text{SZK} \subseteq \text{AM} \cap \text{coAM}, \quad (6)$$

where the inclusion $\text{NP} \subseteq \text{MA} \subseteq \text{SBP}$ is proven in [7]. The inclusion $\text{coNP} \subseteq \text{AM}$ in Equation (6) would collapse the polynomial-time hierarchy to its second level [8].

In addition to this main open problem concerning the computational hardness of estimating the quantum Rényi entropy, there are two further open questions:

- (1) What is the computational hardness of estimating the quantum Rényi and Tsallis entropies of the order-0 in general?
- (2) Can the inequalities in Table 2 be tightened? For instance, is it possible to prove that $\left(\frac{H_\alpha^R(x)}{\ln(2)}\right)^{2/\alpha}$ is monotonically non-decreasing in α for all fixed $x \in [0, 1]$, as suggested by numerical evidence and as a generalization of Theorem 20?

1.5 Related works

We first review additional prior work on the computational complexity of decision problems related to entropies. A variant of $\text{ENTROPY APPROXIMATION (EA)}$, specifically the sampler associated with distributions described by a degree-3 polynomial, was shown to be SZKL -complete [21]. More recently, another variant of EA , where the promises involve different entropies – namely deciding whether the max entropy (order 0) is small or the smoothed 2-Rényi entropy is large – was proven to be NISZK -complete in [46], playing a key role in batch verification of non-interactive statistical zero-knowledge. Furthermore, variants of $\text{QUANTUM ENTROPY DIFFERENCE (QED)}$, which are connected to estimating the von Neumann entropy of quantum states, have attracted attention in recent years: the case where the state-preparation circuits are shallow depth was studied in [25] and shown to be as hard as the Learning with Errors (LWE) problem, while the case where the state-preparation circuits act on $O(\log n)$ qubits was shown to be BQL -complete in [37].

⁸ Let $\{\lambda_k\}_{k=1}^N$ denote the eigenvalues of an n -qubit quantum state ρ , where $N := 2^n$. The upper bound in Equation (5) follows from the fact that for all $\alpha > 1$, $\ln\left(\sum_{k=1}^N \lambda_k^\alpha\right) \geq \ln(\max_k \lambda_k^\alpha) = \alpha \ln \lambda_{\max}$, since $\ln(x)$ is monotonically increasing for $x > 0$. The argument is then completed by multiplying both sides by $1/(1 - \alpha)$.

⁹ We note that the promise problem $\text{CIRCUIT-MIN-ENT-GAP}$ defined in [73] is SBP -complete, but its promise conditions are the exact opposite of those in EA [29], which is why we consider the complement.

In addition to results on entropy-related decision problems, while there is no direct connection to our approach, it is worth noting that conceptually similar inequalities relating different orders of information-theoretic quantities, similar to the Rényi binary entropies in Table 3 and the Tsallis binary entropies in Table 3, were established in [42] for the quantum ℓ_α distance $T_\alpha(\rho_0, \rho_1)$ defined via the Schatten norm $\|A\|_\alpha := (\text{Tr}(|A|^\alpha))^{1/\alpha}$. Specifically, such inequalities connect the trace distance ($\alpha = 1$) to other orders where $\alpha > 1$.

2 Preliminaries

We assume a basic familiarity with quantum computation and the theory of quantum information. The reader may refer to [47] for an introduction. For notational convenience, we write $|\bar{0}\rangle$ to denote $|0\rangle^{\otimes a}$, where $a > 1$ is an integer.

2.1 Bounds for Tsallis and Rényi binary entropies

The q -logarithm function $\ln_q: \mathbb{R}^+ \rightarrow \mathbb{R}$ for any real $q \neq 1$ is defined as $\ln_q(x) := \frac{1-x^{1-q}}{q-1}$.

► **Definition 6** (Binary entropies). *The q -Tsallis binary entropy $H_q^T(x)$ and the α -Rényi binary entropy $H_\alpha^R(x)$ are defined by: for any $x \in [0, 1]$,*

$$H_q^T(x) := \frac{1 - x^q - (1-x)^q}{q-1} = -x^q \ln_q(x) - (1-x)^q \ln_q(1-x),$$

$$H_\alpha^R(x) := \frac{\ln(x^\alpha + (1-x)^\alpha)}{1-\alpha}.$$

The (Shannon) binary entropy arises as a limiting case of both the q -Tsallis binary entropy and the α -Rényi binary entropy as the order approaches 1:

$$H_1^T(x) = H_1^R(x) = H(x) := -x \ln x - (1-x) \ln(1-x),$$

where $H_1^T(x) := \lim_{q \rightarrow 1} H_q^T(x)$ and $H_1^R(x) := \lim_{\alpha \rightarrow 1} H_\alpha^R(x)$. The min binary entropy also arises as a limiting case of the α -Rényi binary entropy as α approaches ∞ :

$$H_\infty^R(x) = H_\infty(x) := -\ln(\max\{x, 1-x\}), \quad \text{where } H_\infty^R(x) := \lim_{\alpha \rightarrow \infty} H_\alpha^R(x).$$

We then list several useful bounds for the Tsallis and Rényi binary entropies:

► **Lemma 7** (Tsallis binary entropy lower bound, adapted from [43, Lemma 4.8]). *For any $q \in [0, 2] \cup [3, \infty)$, it holds that*

$$\forall x \in [0, 1], \quad 2H_q^T(1/2) \cdot H_2^T(x) = H_q^T(1/2) \cdot 4x(1-x) \leq H_q^T(x).$$

► **Lemma 8** (Monotonicity of Rényi binary entropy, adapted from [4, Section 5.3]). *For any $\alpha, \alpha' \in \mathbb{R}$ satisfying $0 \leq \alpha \leq \alpha' \leq \infty$, it holds that*

$$\forall x \in [0, 1], \quad H_\alpha^R(x) \geq H_{\alpha'}^R(x).$$

We also require the following folklore lower bound for the binary min-entropy, as presented, for example, in [20, Section 2]:

► **Proposition 9** (Binary min-entropy lower bound). $\forall x \in [0, 1], H_2^R(x) \leq 2 \cdot H_\infty(x)$.

2.2 Different notions of quantum entropies for states

Next, we introduce different notions of quantum entropies for states:

► **Definition 10** (Quantum entropies). *Let ρ be a quantum state. The quantum q -Tsallis entropy $S_q^T(\rho)$ and the quantum α -Rényi entropy $S_\alpha^R(\rho)$ of ρ are defined by*

$$S_q^T(\rho) := \frac{1 - \text{Tr}(\rho^q)}{q - 1} = -\text{Tr}(\rho^q \ln_q(\rho)) \quad \text{and} \quad S_\alpha^R(\rho) := \frac{\ln \text{Tr}(\rho^\alpha)}{1 - \alpha}.$$

Furthermore, as the order approaches 1, both the quantum q -Tsallis entropy and the quantum α -Rényi entropy converge to the von Neumann entropy $S(\rho)$:

$$S_1^T(\rho) := \lim_{q \rightarrow 1} S_q^T(\rho), \quad S_1^R(\rho) := \lim_{\alpha \rightarrow 1} S_\alpha^R(\rho), \quad \text{and} \quad S_1^T(\rho) = S_1^R(\rho) = S(\rho) := -\text{Tr}(\rho \ln(\rho)).$$

The quantum min entropy also arises as a limiting case of the quantum α -Rényi entropy as α approaches ∞ , where $\lambda_{\max}(\rho)$ denotes the largest eigenvalue of ρ :

$$S_\infty^R(\rho) = S_\infty(\rho) := -\ln(\lambda_{\max}(\rho)), \quad \text{where} \quad S_\infty^R(\rho) := \lim_{\alpha \rightarrow \infty} S_\alpha^R(\rho).$$

We also present the promise problem for estimating quantum Tsallis entropies:

► **Definition 11** (Quantum q -Tsallis Entropy Approximation, TSALLISQEA_q , adapted from [43, Definition 5.1]). *Let Q be a quantum circuit acting on m qubits and having n specified output qubits, where $m(n)$ is a polynomial in n . Let ρ be the quantum state obtained by running Q on $|0\rangle^{\otimes m}$ and tracing out the non-output qubits. Let $g(n)$ and $t(n)$ be positive, efficiently computable functions. The promise problem $\text{TSALLISQEA}_q[t(n), g(n)]$ asks whether the following holds:*

- Yes: A quantum circuit Q such that $S_q^T(\rho) \geq t(n) + g(n)$;
- No: A quantum circuit Q such that $S_q^T(\rho) \leq t(n) - g(n)$.

2.3 Computational hardness of estimating the pure-state infidelity

We start by defining a promise problem closely related to FIDELITY-PURE-PURE, introduced in [51, Problem 1]:

► **Definition 12** (Pure-State Infidelity Estimation, PUREINFIDELITY). *Let Q_0 and Q_1 be quantum circuits acting on m qubits with n specified output qubits, where $m(n)$ is a polynomial in n . Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be pure quantum states obtained by running Q_0 and Q_1 on $|0\rangle^{\otimes m}$, respectively. Let $a(n)$ and $b(n)$ be positive efficiently computable functions. The promise problem $\text{PUREINFIDELITY}[a(n), b(n)]$ asks whether the following holds:*

- Yes: A pair of quantum circuits (Q_0, Q_1) such that $1 - |\langle \psi_0 | \psi_1 \rangle|^2 \geq a(n)$;
- No: A pair of quantum circuits (Q_0, Q_1) such that $1 - |\langle \psi_0 | \psi_1 \rangle|^2 \leq b(n)$;

The promise problem PUREINFIDELITY , essentially the task of estimating the pure-state infidelity, $1 - |\langle \psi_0 | \psi_1 \rangle|^2$, to within constant precision, is BQP-hard:

► **Lemma 13** (PUREINFIDELITY is BQP-hard, adapted from [51, Theorem 12]). *For any integer $n \geq 2$, it holds that $\text{PUREINFIDELITY}[(1 - 2^{-n})^2, 2^{-2n}]$ is BQP-hard.*

The proof can be found in [41, Section 2.3] in the full version. It is worth mentioning that, subsequent to [51], constructions similar to Lemma 13 were used to establish hardness for closeness testing problems with respect to other closeness measures between pure states, such as the (squared) Hilbert–Schmidt distance [37, Lemma 4.23], the trace distance [66, Theorem 4.1] and [43, Lemma 2.17].

2.4 Useful identities from infinite series

Following [33, Section 25], we define the *generalized binomial coefficients*, which is denoted by $\binom{a}{k}$, for any real α and non-negative integer k :

$$\binom{a}{0} := 1 \quad \text{and} \quad \binom{a}{k} := \frac{a(a-1)\cdots(a-k+1)}{1\cdot 2\cdots k} \quad \text{for } k \in \mathbb{N}_+. \quad (7)$$

Moreover, we make use of the following properties of the generalized binomial series:

► **Proposition 14** (Identities for generalized binomial coefficients). *The following holds:*

- (1) $\forall \alpha \in \mathbb{R}, \quad (1+x)^a + (1-x)^a = 2 \sum_{k=0}^{\infty} \binom{a}{2k} x^{2k}$ when $|x| < 1$.
- (2) $\forall \alpha \in \mathbb{R}, \quad \sum_{k=1}^{\infty} \binom{a}{2k} k = 2^{a-3} a$.

Proof. Item (1) follows directly from the identity given in [33, Equation (119)]. To establish Item (2), we differentiate both sides of Item (1) with respect to x , yielding

$$a(1+x)^{a-1} - a(1-x)^{a-1} = 2 \sum_{k=1}^{\infty} \binom{a}{2k} k x^{2k-1}. \quad (8)$$

Taking the limit as $x \rightarrow 1$ on both sides of Equation (8), we obtain Item (2). ◀

► **Proposition 15** (Sign conditions for generalized binomial coefficients). *For any real number $a > 0$ and integer $k \geq 1$, the generalized binomial coefficient $\binom{a}{2k} \geq 0$ if and only if the integer $\max\{0, 2k - \lceil a \rceil\}$ is even.*

Proof. Noting that $\binom{a}{2k} \cdot (2k)! = \prod_{j=0}^{2k-1} (a-j)$, the sign of $\binom{a}{2k}$ is thus determined by the parity of the number of integers $j \in \{0, 1, 2, \dots, 2k-1\}$ satisfying $a-j < 0$. It is evident that this count is zero when $a \geq 2k$ and equals $2k - \lceil a \rceil$ when $a < 2k$, which completes the proof. ◀

We also require the following identity for power series, as stated in [33, Footnote 13]:

$$\forall r \in \mathbb{N}_+, \quad 1 - x^r = (1-x) \sum_{j=0}^{r-1} x^j. \quad (9)$$

3 New bounds for Rényi and Tsallis binary entropies

In this section, we present new bounds for the α -Rényi and q -Tsallis binary entropies:

► **Theorem 16** (New bounds for α -Rényi binary entropy). *For all $x \in [0, 1]$, the following bounds with respect to the 2-Rényi binary entropy hold:*

- (1) For every $\alpha \in (0, 2]$, $H_\alpha^R(x) \leq \ln(2)^{1-\frac{\alpha}{2}} \cdot H_2^R(x)^{\frac{\alpha}{2}}$.
- (2) For every $\alpha \in [2, \infty]$, $\frac{\alpha}{2(\alpha-1)} \cdot H_2^R(x) \leq H_\alpha^R(x)$.

► **Theorem 17** (New bounds for q -Tsallis binary entropy). *For all $x \in [0, 1]$, the following bounds with respect to the 2-Tsallis binary entropy hold:*

- (1) For every $q \in (0, 2]$, $H_q^T(x) \leq 2^{\frac{q}{2}} H_q^T(\frac{1}{2}) \cdot (H_2^T(x))^{\frac{q}{2}}$.
- (2) For every $q \in [2, 3]$, $\frac{q}{2(q-1)} \cdot H_2^T(x) \leq H_q^T(x) \leq 2H_q^T(\frac{1}{2}) \cdot H_2^T(x)$.
- (3) For every $q \in [3, \infty)$, $2 \cdot H_q^T(\frac{1}{2}) \cdot H_2^T(x) \leq H_q^T(x) \leq \frac{q}{2(q-1)} \cdot H_2^T(x)$.

Our proof relies on the correspondence among quantum Jensen-type divergence for pure states, the associated quantum entropies of rank-2 states, and the corresponding binary entropies, as detailed in Section 3.1. The proof of Theorem 16 is given in Section 3.2, while that of Theorem 17 is deferred to Section 3.3.

3.1 Mapping quantum entropies of rank-2 states to binary entropies

► **Theorem 18** (Characterizing QJT_q and QJR_α between pure states via binary entropies). *For any pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ on the same number of qubits, the following holds:*

$$(1) \text{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = S_q^T\left(\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right)^q\right) = H_q^T\left(\frac{1 - |\langle\psi_0|\psi_1\rangle|}{2}\right).$$

$$(2) \text{QJR}_\alpha(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = S_\alpha^R\left(\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right)^q\right) = H_\alpha^R\left(\frac{1 - |\langle\psi_0|\psi_1\rangle|}{2}\right).$$

To establish Theorem 18, we first note that the first equality in both Items (1) and (2) holds immediately, since $S_q^T(|\psi\rangle\langle\psi|) = 0$ and $S_\alpha^R(|\psi\rangle\langle\psi|) = 0$ for any pure state $|\psi\rangle$ and for all orders q and α . To demonstrate the second equality, we require the following lemma concerning the trace of powers of a rank-2 quantum state:

► **Lemma 19** (Trace of uniform rank-2 quantum state powers). *For any pure quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ on the same number of qubits, the following holds: For any $q \in \mathbb{R}_+$,*

$$\text{Tr}\left(\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right)^q\right) = \sum_{b \in \{0,1\}} \frac{(1 + (-1)^b |\langle\psi_0|\psi_1\rangle|)^q}{2^q} = 2^{-q+1} \sum_{k=0}^{\infty} \binom{q}{2k} |\langle\psi_0|\psi_1\rangle|^{2k}.$$

Here, the generalized binomial coefficients $\binom{q}{2k}$ are defined in Equation (7).

The proof of Lemma 19 proceeds by analyzing the eigenvalues of the matrix $|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|$, which yields $\text{Tr}((|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|)^q) = (1 - |\langle\psi_0|\psi_1\rangle|)^q + (1 + |\langle\psi_0|\psi_1\rangle|)^q$. Together with Proposition 14(1), this establishes Lemma 19. The complete proof can be found in the full version, specifically in [41, Section 3.1].

3.2 New bounds for α -Rényi binary entropy

In this subsection, we present the proof of Theorem 16.

3.2.1 The cases of $0 < \alpha < 2$

► **Theorem 20** (α -Rényi binary entropy upper bound when $0 < \alpha \leq 2$). *The following holds:*

$$\forall \alpha \in (0, 2], \quad \forall x \in [0, 1], \quad H_\alpha^R(x) \leq \ln(2)^{1 - \frac{\alpha}{2}} \cdot H_2^R(x)^{\frac{\alpha}{2}}.$$

The proof of Theorem 20 relies on the correspondence between QJR_α for pure states and the α -Rényi binary entropy (Theorem 18(2)). It thus remains to show the following lemma:

► **Lemma 21** (QJR_2 vs. QJR_α for $0 < \alpha \leq 2$). *For any pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, it holds that: $\forall \alpha \in (0, 2]$, $\text{QJR}_\alpha(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \leq \ln(2)^{1 - \frac{\alpha}{2}} \cdot \text{QJR}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)^{\frac{\alpha}{2}}$.*

We sketch the proof of Lemma 21, with details provided in the full version [41, Section 3.2.1]. The case $\alpha = 1$ follows from [57, Theorem 1.2], and $\alpha = 2$ holds trivially. For $1 < \alpha < 2$, we study the ratio

$$R(|\langle\psi_0|\psi_1\rangle|; \alpha) := (\alpha - 1) \cdot \frac{\text{QJR}_\alpha(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)}{\text{QJR}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)^{\alpha/2}},$$

and in particular the monotonicity of a function $F(x; \alpha)$ related to $\frac{\partial}{\partial x} R(x; \alpha)$. By analyzing functions derived from its first- and second-order derivatives with respect to α , we show that $F(x; \alpha)$ changes monotonicity exactly once at some $\alpha^*(x) \in (1, 2)$. Since $F(x; 1) = F(x; 2)$ for $x \in [0, 1]$, this implies $R(x; \alpha)$ is non-increasing in x , so the upper bound is attained at $R(0; \alpha)$. The case $0 < \alpha < 1$ is similar but simpler: defining $\widehat{R}(x; \alpha)$ and $\widehat{F}(x; \alpha)$, we analyze the derivative of $\widehat{F}(x; \alpha)$ with respect to α term by term.

3.2.2 The cases of $\alpha \geq 2$

► **Theorem 22** (α -Rényi binary entropy lower bound when $\alpha \geq 2$). *The following holds:*

$$\forall \alpha \geq 2, \quad \forall x \in [0, 1], \quad \frac{\alpha}{2(\alpha - 1)} \cdot \mathbb{H}_2^{\mathbb{R}}(x) \leq \mathbb{H}_\alpha^{\mathbb{R}}(x).$$

To prove Theorem 22, we use the correspondence between QJR_α for pure states and the α -Rényi binary entropy (Theorem 18(2)). It thus suffices to prove the following lemma:

► **Lemma 23** (QJR_2 vs. QJR_α for $\alpha \geq 2$). *For any pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, it holds that:*

$$\forall \alpha \geq 2, \quad \frac{\alpha}{2(\alpha - 1)} \cdot \text{QJR}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \leq \text{QJR}_\alpha(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|).$$

The proof of Lemma 23 proceeds by showing the non-negativity of

$$F(|\langle\psi_0|\psi_1\rangle|; \alpha) = (\alpha - 1)\text{QJR}_\alpha(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) - \frac{\alpha}{2} \cdot \text{QJR}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|).$$

We analyze a function related to the derivative of $F(x; \alpha)$ with respect to x , showing that $F(x; \alpha)$ is monotonically non-increasing on $x \in [0, 1]$. The bound then follows by evaluating the endpoint $F(x; \alpha) \geq F(1; \alpha) = 0$. The detailed proof can be found in the full version, specifically in [41, Section 3.2.2].

3.3 New bounds for q -Tsallis binary entropy

In this subsection, we demonstrate the proof of Theorem 17.

3.3.1 The cases of $0 < q \leq 2$

► **Theorem 24** (q -Tsallis binary entropy upper bound for $0 < q \leq 2$). *The following holds:*

$$\forall q \in (0, 2], \quad \forall x \in [0, 1], \quad \mathbb{H}_q^{\mathbb{T}}(x) \leq 2^{\frac{q}{2}} \mathbb{H}_q^{\mathbb{T}}\left(\frac{1}{2}\right) \cdot (\mathbb{H}_2^{\mathbb{T}}(x))^{\frac{q}{2}}.$$

It is worth noting that Theorem 24 improves the previous bound,

$$\forall q \in [1, 2], \quad \forall x \in [0, 1], \quad \mathbb{H}_q^{\mathbb{T}}(x) \leq \sqrt{2} \mathbb{H}_q^{\mathbb{T}}(1/2) \cdot \mathbb{H}_2^{\mathbb{T}}(1/2)^{1/2},$$

which was established in [43, Lemma 4.9]. To demonstrate Theorem 24, we utilize the correspondence between QJT_q for pure states and the Tsallis q -binary entropy (Theorem 18(1)). As a result, it remains to establish the following lemma:

► **Lemma 25** (QJT_2 vs. QJT_q for $0 < q \leq 2$). *For any pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, it holds that $\forall q \in (0, 2]$, $\text{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \leq 2^{\frac{q}{2}} \mathbb{H}_q^{\mathbb{T}}\left(\frac{1}{2}\right) \cdot (\text{QJT}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|))^{\frac{q}{2}}$.*

We sketch the proof of Lemma 25. The case $\alpha = 1$ was shown in [39, Theorem 8], and the case $\alpha = 2$ holds trivially. For the case $0 < q < 1$, we consider the ratio function

$$F(|\langle \psi_0 | \psi_1 \rangle|; q) := (1 - q) \cdot \frac{\text{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)}{\text{QJT}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)^{q/2}},$$

which decomposes a product of two functions $F_1(x; q)$ and $F_2(x; q)$. We analyze the monotonicity of the main term of $\frac{\partial}{\partial x} F(x; q)$, denoted by $T(x; q)$, noting the remainder is non-negative. By studying the first-order and second-order derivatives of $T(x; q)$ with respect to x , we can prove that $F(x; q)$ is monotonically non-increasing on $x \in [0, 1]$, so the upper bound is attained at the endpoint $F(0; q)/(1 - q)$. The case $1 < q < 2$ follows by a similar argument, and we omit the details. The complete proof of Lemma 25 is provided in the full version, as detailed in [41, Section 3.3.1].

3.3.2 The cases of $q \geq 2$

► **Theorem 26** (q -Tsallis binary entropy bounds for $q \geq 2$). *The following holds:*

- (1) $\forall q \in [2, 3], \forall x \in [0, 1], \quad \frac{q}{2(q-1)} \cdot \text{H}_2^T(x) \leq \text{H}_q^T(x) \leq 2\text{H}_q^T\left(\frac{1}{2}\right) \cdot \text{H}_2^T(x).$
- (2) $\forall q \geq 3, \forall x \in [0, 1], \quad 2\text{H}_q^T\left(\frac{1}{2}\right) \cdot \text{H}_2^T(x) \leq \text{H}_q^T(x) \leq \frac{q}{2(q-1)} \cdot \text{H}_2^T(x).$

It is noteworthy that the lower bound in Theorem 26(2) was already established in Lemma 7 (cf. [43, Lemma 4.9]). To prove Theorem 26, we use the correspondence between QJT_q for pure states and the Tsallis q -binary entropy (Theorem 18(1)), together with the observation that, for any pure states $|\psi_0\rangle$ and $|\psi_1\rangle$,

$$\text{QJT}_3(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = \frac{3}{4} \cdot \text{QJT}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|).$$

Consequently, it suffices to prove the following lemma, which considers the intervals $q \in [2, 3]$ and $q \in [3, \infty)$ separately:

► **Lemma 27** (QJT_2 vs. QJT_q for $q \geq 2$). *For any pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, it holds that:*

- (1) $\forall q \in [2, 3], \quad \frac{q}{2(q-1)} \leq \frac{\text{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)}{\text{QJT}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)} \leq 2\text{H}_q^T\left(\frac{1}{2}\right).$
- (2) $\forall q \geq 3, \quad 2\text{H}_q^T\left(\frac{1}{2}\right) \leq \frac{\text{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)}{\text{QJT}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)} \leq \frac{q}{2(q-1)}.$

The proof of Lemma 27 considers the ratio function

$$\frac{\text{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)}{\text{QJT}_2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)} \propto F(|\langle \psi_0 | \psi_1 \rangle|^2; q) := \sum_{k=1}^{\infty} \binom{q}{2k} \sum_{l=0}^{k-1} |\langle \psi_0 | \psi_1 \rangle|^{2l}.$$

Studying the first-order derivative $\frac{\partial}{\partial x} F(x; q)$ requires understanding the conditions on the sign of the generalized binomial coefficients (Proposition 15), leading to three cases: when $q \in (2, 3]$, when $\lceil q \rceil \geq 4$ is an even integer, and when $\lceil q \rceil \geq 5$ is an odd integer. Consequently, one can show that the monotonicity of $F(x; q)$ with respect to q changes at $q = 3$: it is non-increasing for $q \leq 3$ and non-decreasing for $q > 3$. The bounds then follow by evaluating the endpoints $x = 0$ and $x \rightarrow 1^-$. The complete proof can be found in the full version, particular in [41, Section 3.3.2].

4 Computational hardness of $\text{RANK2RÉNYIQEA}_\alpha$

We introduce a restricted version of the QUANTUM α -RÉNYI ENTROPY APPROXIMATION PROBLEM (RÉNYIQEA_α), where the quantum state has rank at most t wo:

► **Definition 28** (Rank-Two Quantum α -Rényi Entropy Approximation, $\text{RANK2RÉNYIQEA}_\alpha$). *Let Q be a quantum circuit acting on m qubits and having n specified output qubits, where $m(n)$ is a polynomial in n . Let ρ be a quantum state obtained by running Q on $|0\rangle^{\otimes m}$ and tracing out the non-output qubits, such that the rank of ρ is at most two. Let $g(n)$ and $t(n)$ be positive efficiently computable functions. The promise problem $\text{RANK2RÉNYIQEA}_\alpha[t(n), g(n)]$ asks whether the following holds:*

- Yes: A quantum circuit Q such that $S_\alpha^R(\rho) \geq t(n) + g(n)$;
- No: A quantum circuit Q such that $S_\alpha^R(\rho) \leq t(n) - g(n)$.

The main result of this section is that $\text{RANK2RÉNYIQEA}_\alpha$ is BQP-hard for every positive order α , even under a constant promise gap (i.e., precision):

► **Theorem 29** (Computational hardness of $\text{RANK2RÉNYIQEA}_\alpha$). *There exists a family of threshold functions $t(n; \alpha)$ and gap functions $g(n; \alpha)$, with the gap function bounded below by some universal constant, such that the following statements hold:*

- (1) *For every real-valued order $\alpha \in (0, 1)$, $\text{RANK2RÉNYIQEA}_\alpha[t(n; \alpha), g(n; \alpha)]$ is BQP-hard for all integers $n \geq \lfloor 2/\alpha \rfloor$.*
- (2) *For every order $\alpha \in [1, \infty]$, $\text{RANK2RÉNYIQEA}_\alpha[t(n; \alpha), g(n; \alpha)]$ is BQP-hard for all integers $n \geq 2$.*

The explicit forms of $t(n; \alpha)$ and $g(n; \alpha)$ depend on the interval of α – namely, $(0, 1)$, $[1, 2)$, $\{2\}$, and $(2, \infty]$ – and are provided in Theorems 30–32.

The proof of Theorem 29 will be developed in the remainder of this section by analyzing each interval of α specified in the theorem separately.

4.1 The case of $\alpha = 2$

► **Theorem 30** (RANK2RÉNYIQEA_2 is BQP-hard). *Let $t(n)$ and $g(n)$ be efficiently computable functions. For any integer $n \geq 2$,*

$\text{RANK2RÉNYIQEA}_2[t(n), g(n)]$ *is BQP-hard.*

Here, the threshold function is chosen as

$$t(n) = \frac{1}{2}(\ln(2) - \ln(1 - 2^{-2n-1})) - 2^{-n} + 2^{-2n-1},$$

and the gap function is given by

$$g(n) = \frac{1}{2} \ln(2 - 2^{-2n}) - 2^{-n} + 2^{-2n-1}.$$

The proof of Theorem 30 reduces from PUREINFIDELITY, which corresponds to the quantity $1 - |\langle \psi_0 | \psi_1 \rangle|^2$ and is BQP-hard (Lemma 13), to RANK2RÉNYIQEA_2 using the identity in Equation (4). The complete proof can be found in the full version, as detailed in [41, Section 4.1].

4.2 The cases of $0 < \alpha < 2$

► **Theorem 31** ($\text{RANK2RÉNYIQEA}_\alpha$ is BQP-hard when $0 < \alpha < 2$). Let $t(n; \alpha)$ and $g(n; \alpha)$ be efficiently computable functions, where $n \in \mathbb{N}$ and $\alpha \in \mathbb{R}$. The following statements hold:

(1) $\forall \alpha \in (0, 1), \forall n \geq \lceil 2/q \rceil$,

$\text{RANK2RÉNYIQEA}_\alpha[t(n; \alpha), g(n; \alpha)]$ is BQP-hard.

(2) $\forall \alpha \in [1, 2), \forall n \geq 2$,

$\text{RANK2RÉNYIQEA}_\alpha[t(n; \alpha), g(n; \alpha)]$ is BQP-hard.

Here, the threshold function is given by

$$t(n; \alpha) = \frac{\ln(2)}{2} - 2^{-n} + 2^{-2n-1} + \frac{\ln(2)}{2} \cdot (-\log_2(1 - 2^{-2n-1}))^{\alpha/2},$$

and the gap function is chosen as

$$g(n; \alpha) = \frac{\ln(2)}{2} - 2^{-n} + 2^{-2n-1} - \frac{\ln(2)}{2} \cdot (-\log_2(1 - 2^{-2n-1}))^{\alpha/2}.$$

The proof of Theorem 31 reduces RANK2RÉNYIQEA_2 to $\text{RANK2RÉNYIQEA}_\alpha$ for $\alpha \in (0, 2)$ using the monotonicity of the Rényi binary entropy (Lemma 8, cf. [4, Section 5.3]) and the upper bound of the α -Rényi entropy for $\alpha \in (0, 2)$ (Theorem 20). Since our choice of $g(n; \alpha)$ is monotonically increasing on $n \geq 2$, showing that $g(2; \alpha)$ for $\alpha \in [1, 2)$ is bounded below by some constant proves Item (2), while establishing $g(\lceil 2/\alpha \rceil; \alpha) \geq g(2/\alpha; \alpha)$ for $\alpha \in (0, 1)$ with a different constant lower bound proves Item (1). The detailed proof is provided in the full version, particularly in [41, Section 4.2].

4.3 The cases of $\alpha \in (2, \infty]$

► **Theorem 32** ($\text{RANK2RÉNYIQEA}_\alpha$ is BQP-hard when $\alpha \geq 2$). Let $t(n; \alpha)$ and $g(n; \alpha)$ be efficiently computable functions. For all $\alpha \in (2, \infty]$ and all integers $n \geq 2$,

$\text{RANK2RÉNYIQEA}_\alpha[t(n; \alpha), g(n; \alpha)]$ is BQP-hard.

Here, the threshold function is given by

$$t(n; \alpha) = \frac{\alpha}{4(\alpha - 1)} \cdot (\ln(2) - 2^{-n+1} + 2^{-2n}) - \frac{1}{2} \cdot \ln(1 - 2^{-2n-1}),$$

and the gap function is chosen as

$$g(n; \alpha) = \frac{\alpha}{4(\alpha - 1)} \cdot (\ln(2) - 2^{-n+1} + 2^{-2n}) + \frac{1}{2} \cdot \ln(1 - 2^{-2n-1}).$$

Moreover, when $\alpha = \infty$, the threshold and gap functions satisfy $t(n, \infty) = \lim_{\alpha \rightarrow \infty} t(n, \alpha)$ and $g(n, \infty) = \lim_{\alpha \rightarrow \infty} g(n, \alpha)$, respectively.

The proof of Theorem 32 reduces RANK2RÉNYIQEA_2 to $\text{RANK2RÉNYIQEA}_\alpha$ for $\alpha \in (2, \infty)$ using the monotonicity of the Rényi binary entropy (Lemma 8, cf. [4, Section 5.3]) and the lower bound on the α -Rényi entropy for $\alpha > 2$ (Theorem 22). The argument is completed by showing that our choice of $g(n; \alpha)$ is monotonically increasing on $n \geq 2$ at fixed $\alpha \geq 2$, while $g(2; \alpha)$ is monotonically decreasing on $\alpha \geq 2$. To prove the case $\alpha = \infty$, we consider the limiting case as α approaches ∞ , where our choices of $t(n; \alpha)$ and $g(n; \alpha)$ extend directly. The complete proof can be found in the full version, specifically in [41, Section 4.3].

5 Computational hardness of RANK2TSALLISQEA_q

We start by considering a restricted version of the QUANTUM q -TSALLIS ENTROPY APPROXIMATION PROBLEM (TSALLISQEA_q) introduced in [43], in which the quantum state is constrained to have rank at most *two*:

► **Definition 33** (Rank-Two Quantum q -Tsallis Entropy Approximation, RANK2TSALLISQEA_q). *Let Q be a quantum circuit acting on m qubits and having n specified output qubits, where $m(n)$ is a polynomial in n . Let ρ be a quantum state obtained by running Q on $|0\rangle^{\otimes m}$ and tracing out the non-output qubits, such that the rank of ρ is at most two. Let $g(n)$ and $t(n)$ be positive efficiently computable functions. The promise problem RANK2TSALLISQEA_q[$t(n), g(n)$] asks whether the following holds:*

- Yes: A quantum circuit Q such that $S_q^T(\rho) \geq t(n) + g(n)$;
- No: A quantum circuit Q such that $S_q^T(\rho) \leq t(n) - g(n)$.

This section's main result establishes that RANK2TSALLISQEA_q is BQP-hard for every real-valued positive order q , even when the promise gap (i.e., precision) is constant:

► **Theorem 34** (Computational hardness of RANK2TSALLISQEA_q). *There exists a family of threshold functions $t(n; \alpha)$ and gap functions $g(n; \alpha)$, with the gap function bounded below by some universal constant, such that the following statements hold:*

- (1) *For every real-valued order $q \in (0, 1)$, RANK2TSALLISQEA_q[$t(n; q), g(n; q)$] is BQP-hard for all integers $n \geq \lceil 1/q \rceil$.*
- (2) *For every order $q \in [1, 3]$, RANK2TSALLISQEA_q[$t(n; q), g(n; q)$] is BQP-hard for all integers $n \geq 2$.*
- (3) *For every real-valued order $q \in (3, \infty)$, RANK2TSALLISQEA_q[$t(n; q), g(n; q)$] is BQP-hard for all integers $n \geq \lfloor \log_2 q \rfloor$.*

The explicit forms of $t(n; q)$ and $g(n; q)$ depend on the interval of q – namely, $(0, 1)$, $[1, 2)$, $\{2\}$, $(2, 3]$, and $(3, \infty)$ – and are given in Theorems 35–38.

It is worth noting that the BQP-hardness of RANK2TSALLISQEA_q for $1 \leq q \leq 2$ under Turing reduction was shown in [43, Theorem 5.8]. In contrast, our constructions in Theorem 35 and Theorem 36(2) give a more direct approach and demonstrate the BQP-hardness under Karp reduction. The remainder of this section is devoted to the proof of Theorem 34, which proceeds by examining each interval of q identified in the theorem individually.

5.1 The case of $q = 2$

► **Theorem 35** (RANK2TSALLISQEA₂ is BQP-hard). *Let $t(n)$ and $g(n)$ be efficiently computable functions. For any integer $n \geq 2$,*

RANK2TSALLISQEA₂[$t(n), g(n)$] *is BQP-hard.*

Here, the threshold function is chosen as $t(n) = \frac{1}{4} - 2^{-n-1} + 2^{-2n-1}$, and the gap function is specified as $g(n) = \frac{1}{4} - 2^{-n-1}$.

The proof of Theorem 35 reduces from PUREINFIDELITY, which is BQP-hard (Lemma 13), to RANK2TSALLISQEA₂ via the identity in Equation (2). The detailed proof can be found in the full version, particularly in [41, Section 5.1].

5.2 The cases of $0 < q < 2$

► **Theorem 36** (RANK2TSALLISQEA_q is BQP-hard when $0 < q < 2$). Let $t(n; q)$ and $g(n; q)$ be efficiently computable functions, where $n \in \mathbb{N}$ and $q \in \mathbb{R}$. The following statements hold:

(1) $\forall q \in (0, 1), \forall n \geq \lceil 1/q \rceil$,

$\text{RANK2TSALLISQEA}_q[t(n; q), g(n; q)]$ is BQP-hard.

(2) $\forall q \in [1, 2), \forall n \geq 2$,

$\text{RANK2TSALLISQEA}_q[t(n; q), g(n; q)]$ is BQP-hard.

Here, the threshold function is defined as

$$t(n; q) = H_q^T\left(\frac{1}{2}\right) \cdot \frac{1}{2} \left((1 - 2^{-n})^2 + 2^{-nq} \right),$$

and the gap functions is given by

$$g(n; q) = H_q^T\left(\frac{1}{2}\right) \cdot \frac{1}{2} \left((1 - 2^{-n})^2 - 2^{-nq} \right).$$

The proof of Theorem 36 reduces RANK2TSALLISQEA_2 to RANK2TSALLISQEA_q for $0 < q < 1$ using the lower and upper bounds for the q -Tsallis binary entropy (Lemma 7 and Theorem 24). Since our choice of $g(n; q)$ is monotonically increasing for $q \in (0, 2)$, one can show that $g(2; q)$ is lower bounded by a universal constant for $q \in [1/2, 2)$ and $n \geq 2$, proving Item (2). Because $\lceil 1/q \rceil = 2$ for $1/2 \leq q \leq 1$, the remainder in the proof shows that $g(1/q; q)$ is lower bounded by another universal constant for $0 < q < 1/2$, proving Items (1) and (2). The complete proof is given in the full version, as detailed in [41, Section 5.2].

5.3 The cases of $2 < q \leq 3$ and $q > 3$

► **Theorem 37** (RANK2TSALLISQEA_q is BQP-hard when $2 \leq q < 3$). Let $t(n; q)$ and $g(n; q)$ be efficiently computable functions. For all $q \in (2, 3]$ and all integers $n \geq 2$,

$\text{RANK2TSALLISQEA}_q[t(n; q), g(n; q)]$ is BQP-hard.

Here, the threshold and gap functions are defined as

$$t(n; q) = \frac{q}{4(q-1)} \cdot \left(\frac{1}{2} - 2^{-n} \right) + 2^{-2n-1} \cdot \left(H_q^T\left(\frac{1}{2}\right) + \frac{q}{4(q-1)} \right),$$

$$g(n; q) = \frac{q}{4(q-1)} \cdot \left(\frac{1}{2} - 2^{-n} \right) - 2^{-2n-1} \cdot \left(H_q^T\left(\frac{1}{2}\right) - \frac{q}{4(q-1)} \right).$$

► **Theorem 38** (RANK2TSALLISQEA_q is BQP-hard when $q > 3$). Let $t(n; q)$ and $g(n; q)$ be efficiently computable functions. For all $q > 3$ and all integers $n \geq \lceil \log_2(q) \rceil$,

$\text{RANK2TSALLISQEA}_q[t(n; q), g(n; q)]$ is BQP-hard.

Here, the threshold and gap functions are chosen as

$$t(n; q) = \frac{1}{2} H_q^T\left(\frac{1}{2}\right) - 2^{-2n-1} \left(H_q^T\left(\frac{1}{2}\right) - \frac{q}{4(q-1)} \right),$$

$$g(n; q) = \frac{1}{2} H_q^T\left(\frac{1}{2}\right) - 2^{-2n-1} \left(H_q^T\left(\frac{1}{2}\right) + \frac{q}{4(q-1)} \right).$$

The proofs of Theorems 37 and 38 reduce RANK2TSALLISQEA₂ to RANK2TSALLISQEA_q for $q \in (2, 3]$ and $q > 3$, respectively, using the inequalities between QJT₂ and QJT_q for pure states (Lemma 27), particularly by rewriting them in terms of the q -Tsallis binary entropy $H_q^T((1 - |\langle \psi_0 | \psi_1 \rangle|)/2)$. The complete proofs are provided in the full version, specifically in [41, Sections 5.3 and 5.4].

6 Computational complexity of estimating order-0 quantum entropies of rank-2 states

We begin by simplifying the definitions of quantum Tsallis and Rényi entropies of order 0, yielding the following expressions:

$$S_0^T(\rho) = \text{rank}(\rho) - 1 \quad \text{and} \quad S_0^R(\rho) = \ln \text{rank}(\rho). \quad (10)$$

The main result of this section proves that the promise problems RANK2TSALLISQEA₀ and RANK2TSALLISQEA₀ are not only NQP-complete, but also their NQP-hardness persists even under the largest possible promise gap:

► **Theorem 39.** *For all $n \geq 2$, the following holds:*

RANK2RÉNYIQEA₀[$\ln(2), 0$] and RANK2TSALLISQEA₀[$1, 0$] are NQP-complete.

Notably, the NQP containment follows almost directly from the SWAP test, which was originally proposed for pure states in [10] and later extended to mixed states in [36], as stated in [41, Lemma 6.2]. The complete proof of Theorem 39 can be found in the full version, as detailed in [41, Section 6.1].

References

- 1 Jayadev Acharya, Ibrahim Issa, Nirmal V. Shende, and Aaron B. Wagner. Estimating quantum entropy. *IEEE Journal on Selected Areas in Information Theory*, 1(2):454–468, 2020. Preliminary version in *ISIT 2019*. doi:10.1109/JSAIT.2020.3015235.
- 2 Jayadev Acharya, Alon Orlitsky, Ananda Theertha Suresh, and Himanshu Tyagi. Estimating Renyi entropy of discrete distributions. *IEEE Transactions on Information Theory*, 63(1):38–56, 2017. doi:10.1109/TIT.2016.2620435.
- 3 Leonard M. Adleman, Jonathan Demarrais, and Ming-Deh A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997. doi:10.1137/S0097539795293639.
- 4 Christian Beck and Friedrich Schögl. *Thermodynamics of Chaotic Systems: An Introduction*. Cambridge Nonlinear Science Series. Cambridge University Press, 1993. doi:10.1017/cbo9780511524585.
- 5 Avraham Ben-Aroya, Oded Schwartz, and Amnon Ta-Shma. Quantum expanders: motivation and construction. *Theory of Computing*, 6(3):47–79, 2010. Preliminary version in *CCC 2008*. doi:10.4086/toc.2010.v006a003.
- 6 Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933.
- 7 Elmar Böhler, Christian Glaßer, and Daniel Meister. Error-bounded probabilistic computations between MA and AM. *Journal of Computer and System Sciences*, 72(6):1043–1076, 2006. Preliminary version in *MFCS 2003*. ECCC:TR03-069. doi:10.1016/J.JCSS.2006.05.001.
- 8 Ravi B. Boppana, Johan Håstad, and Stathis Zachos. Does coNP have short interactive proofs? *Information Processing Letters*, 25(2):127–132, 1987. doi:10.1016/0020-0190(87)90232-8.
- 9 Jop Briët and Peter Harremoës. Properties of classical and quantum Jensen–Shannon divergence. *Physical Review A*, 79(5):052311, 2009. doi:10.1103/PhysRevA.79.052311.

- 10 Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001. doi:10.1103/PhysRevLett.87.167902.
- 11 Mark Bun, Robin Kothari, and Justin Thaler. The polynomial method strikes back: tight quantum query bounds via dual polynomials. *Theory of Computing*, 16(10):1–71, 2020. Preliminary version in *STOC 2018*. doi:10.4086/toc.2020.v016a010.
- 12 Jacob Burbea and Calyampudi Radhakrishna Rao. On the convexity of some divergence measures based on entropy functions. *IEEE Transactions on Information Theory*, 28(3):489–495, 1982. doi:10.1109/tit.1982.1056497.
- 13 Clément L. Canonne. A survey on distribution testing: your data is big, but is it blue? In *Theory of Computing Library*, number 9 in Graduate Surveys, pages 1–100. University of Chicago, 2020. ECCC:TR15–063. doi:10.4086/toc.gs.2020.009.
- 14 André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis, and Salil Vadhan. Interactive and noninteractive zero knowledge are equivalent in the help model. In *Proceedings of the Fifth Theory of Cryptography Conference*, pages 501–534. Springer, 2008. IACR ePrint:2007/467. doi:10.1007/978-3-540-78524-8_28.
- 15 Kean Chen and Qisheng Wang. Improved sample upper and lower bounds for trace estimation of quantum state powers. In *The 38th Annual Conference on Learning Theory*, volume 291 of *Proceedings of Machine Learning Research*, pages 1008–1028. PMLR, 2025. arXiv:2505.09563.
- 16 Kean Chen, Qisheng Wang, Zhan Yu, and Zhicheng Zhang. Simultaneous estimation of nonlinear functionals of a quantum state. *arXiv preprint*, 2025. arXiv:2505.16715.
- 17 Richard Y. Chen and Joel A. Tropp. Subadditivity of matrix ϕ -entropy and concentration of random matrices. *Electronic Journal of Probability*, 19(27):1–30, 2014. doi:10.1214/ejp.v19-2964.
- 18 Patrick J Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, 89(1):015002, 2017. doi:10.1103/RevModPhys.89.015002.
- 19 Zoltán Daróczy. Generalized information functions. *Information and Control*, 16(1):36–51, 1970. doi:10.1016/s0019-9958(70)80040-7.
- 20 Yevgeniy Dodis, Thomas Ristenpart, and Salil P. Vadhan. Randomness condensers for efficiently samplable, seed-dependent sources. In *Proceedings of the 9th International Conference on Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 618–635. Springer, 2012. doi:10.1007/978-3-642-28914-9_35.
- 21 Zeev Dvir, Dan Gutfreund, Guy N. Rothblum, and Salil P. Vadhan. On approximating the entropy of polynomial mappings. In *Proceedings of the Second Symposium on Innovations in Computer Science*, pages 460–475. Tsinghua University Press, 2011. ECCC:TR10–160. URL: <http://conference.iis.tsinghua.edu.cn/ICS2011/content/papers/28.html>.
- 22 Jens Eisert, Marcus Cramer, and Martin B Plenio. Colloquium: Area laws for the entanglement entropy. *Reviews of Modern Physics*, 82(1):277–306, 2010. doi:10.1103/RevModPhys.82.277.
- 23 Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999. doi:10.1109/18.761271.
- 24 Shigeru Furuichi, Kenjiro Yanagi, and Ken Kuriyama. A generalized Fannes’ inequality. *Journal of Inequalities in Pure and Applied Mathematics*, 8(1):5, 2007. arXiv:1001.1390.
- 25 Alexandru Gheorghiu and Matty J Hoban. On estimating the entropy of shallow circuit outputs. *arXiv preprint*, 2020. arXiv:2002.12814.
- 26 András Gilyén and Tongyang Li. Distributional property testing in a quantum world. In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, volume 151 of *LIPICs*, pages 25:1–25:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPICs.ITCS.2020.25.
- 27 Oded Goldreich. *Introduction to Property Testing*. Cambridge University Press, 2017. doi:10.1017/9781108135252.

- 28 Oded Goldreich, Amit Sahai, and Salil Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 399–408, 1998. doi:10.1145/276698.276852.
- 29 Oded Goldreich and Salil Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pages 54–73. IEEE, 1999. ECCC:TR98-063. doi:10.1109/ccc.1999.766262.
- 30 Tom Gur, Min-Hsiu Hsieh, and Sathyawageeswar Subramanian. Sublinear quantum algorithms for estimating von neumann entropy. *arXiv preprint*, 2021. arXiv:2111.11139.
- 31 Peter Harremoës and Flemming Topsøe. Inequalities between entropy and index of coincidence derived from information diagrams. *IEEE Transactions on Information Theory*, 47(7):2944–2960, 2001. doi:10.1109/18.959272.
- 32 Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, 2009. doi:10.1103/RevModPhys.81.865.
- 33 Konrad Knopp. *Theory and Application of Infinite Series*. Dover Books on Mathematics. Dover Publications, 1990.
- 34 Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Proceedings of the 14th International Symposium on Algorithms and Computation*, pages 178–188. Springer, 2003. doi:10.1007/978-3-540-24587-2_20.
- 35 Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Generalized quantum Arthur–Merlin games. *SIAM Journal on Computing*, 48(3):865–902, 2019. Preliminary version in *CCC 2015*. doi:10.1137/17m1160173.
- 36 Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin–Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, 2009:3, 2009. Preliminary version in *ISACC 2003*. doi:10.1007/978-3-540-24587-2_21.
- 37 François Le Gall, Yupan Liu, and Qisheng Wang. Space-bounded quantum state testing via space-efficient quantum singular value transformation. To appear in *computational complexity*, 2026. arXiv:2308.05079.
- 38 Tongyang Li and Xiaodi Wu. Quantum query complexity of entropy estimation. *IEEE Transactions on Information Theory*, 65(5):2899–2921, 2019. doi:10.1109/TIT.2018.2883306.
- 39 Jianhua Lin. Divergence measures based on the Shannon entropy. *IEEE Transactions on Information Theory*, 37(1):145–151, 1991. doi:10.1109/18.61115.
- 40 Yupan Liu. Quantum state testing beyond the polarizing regime and quantum triangular discrimination. *computational complexity*, 34(11):1–67, 2025. doi:10.1007/s00037-025-00273-8.
- 41 Yupan Liu. Computational hardness of estimating quantum entropies via binary entropy bounds. *arXiv preprint*, 2026. arXiv:2601.03734v1.
- 42 Yupan Liu and Qisheng Wang. On estimating the quantum ℓ_α distance. In *Proceedings of the 33rd Annual European Symposium on Algorithms*, volume 351 of *LIPICs*, pages 105:1–105:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025. doi:10.4230/LIPICs.ESA.2025.105.
- 43 Yupan Liu and Qisheng Wang. On estimating the trace of quantum state powers. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 947–993. SIAM, 2025. doi:10.1137/1.9781611978322.28.
- 44 Ana P. Majtey, Pedro W. Lambert, and Domingo P. Prato. Jensen–Shannon divergence as a measure of distinguishability between mixed quantum states. *Physical Review A*, 72(5):052310, 2005. doi:10.1103/PhysRevA.72.052310.
- 45 Ashley Montanaro and Ronald de Wolf. A survey of quantum property testing. In *Theory of Computing Library*, number 7 in Graduate Surveys, pages 1–81. University of Chicago, 2016. doi:10.4086/toc.gs.2016.007.

- 46 Changrui Mu, Shafik Nassar, Ron D. Rothblum, and Prashant Nalini Vasudevan. Strong batching for non-interactive statistical zero-knowledge. In *Proceedings of the 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, volume 14656 of *Lecture Notes in Computer Science*, pages 241–270. Springer, 2024. IACR ePrint:2024/229. doi:10.1007/978-3-031-58751-1_9.
- 47 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010. doi:10.1017/CB09780511976667.
- 48 Ryan O’Donnell and John Wright. Quantum spectrum testing. *Communications in Mathematical Physics*, 387(1):1–75, 2021. Preliminary version in *STOC 2015*. doi:10.1007/s00220-021-04180-1.
- 49 Yihui Quek, Eneet Kaur, and Mark M. Wilde. Multivariate trace estimation in constant quantum depth. *Quantum*, 8:1220, 2024. doi:10.22331/Q-2024-01-10-1220.
- 50 Guido A. Raggio. Properties of q -entropies. *Journal of Mathematical Physics*, 36(9):4785–4791, 1995. doi:10.1063/1.530920.
- 51 Soorya Rethinasamy, Rochisha Agarwal, Kunal Sharma, and Mark M. Wilde. Estimating distinguishability measures on quantum computers. *Physical Review A*, 108(1):012409, 2023. doi:10.1103/PhysRevA.108.012409.
- 52 Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009. doi:10.1103/RevModPhys.81.1301.
- 53 Myeongjin Shin, Junseo Lee, Seungwoo Lee, and Kabgyun Jeong. Resource-efficient algorithm for estimating the trace of quantum state powers. *Quantum*, 9:1832, 2025. doi:10.22331/q-2025-08-27-1832.
- 54 Suvrit Sra. Metrics induced by Jensen–Shannon and related divergences on positive definite matrices. *Linear Algebra and its Applications*, 616:125–138, 2021. doi:10.1016/j.laa.2020.12.023.
- 55 Sathyawageeswar Subramanian and Min-Hsiu Hsieh. Quantum algorithm for estimating α -Renyi entropies of quantum states. *Physical Review A*, 104(2):022428, 2021. doi:10.1103/PhysRevA.104.022428.
- 56 Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017. doi:10.22331/q-2017-07-14-14.
- 57 Flemming Topsøe. Bounds for entropy and divergence for distributions over a two-element set. *Journal of Inequalities in Pure and Applied Mathematics*, 2(2), 2001. URL: <https://eudml.org/doc/122035>.
- 58 Constantino Tsallis. *Nonextensive Statistical Mechanics and Its Applications*, chapter I. Nonextensive Statistical Mechanics and Thermodynamics: Historical Background and Present Status, pages 3–98. Springer, 2001. doi:10.1007/3-540-40919-x_1.
- 59 Salil P Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, Massachusetts Institute of Technology, 1999. URL: <https://dspace.mit.edu/handle/1721.1/85349>.
- 60 Igor Vajda. Note on discrimination information and variation. *IEEE Transactions on Information Theory*, 16(6):771–773, 1970. doi:10.1109/TIT.1970.1054557.
- 61 Dániel Virosztek. Jointly convex quantum Jensen divergences. *Linear Algebra and its Applications*, 576:67–78, 2019. doi:10.1016/j.laa.2018.03.002.
- 62 Dániel Virosztek. The metric property of the quantum Jensen–Shannon divergence. *Advances in Mathematics*, 380:107595, 2021. doi:10.1016/j.aim.2021.107595.
- 63 Klaus W. Wagner. The complexity of combinatorial problems with succinct input representation. *Acta Informatica*, 23(3):325–356, 1986. doi:10.1007/BF00289117.
- 64 Qisheng Wang. Information-theoretic lower bounds for approximating monomials via optimal quantum tsallis entropy estimation. *arXiv preprint*, 2025. doi:10.48550/arXiv.2509.03496.
- 65 Qisheng Wang, Ji Guan, Junyi Liu, Zhicheng Zhang, and Mingsheng Ying. New quantum algorithms for computing quantum entropies and distances. *IEEE Transactions on Information Theory*, 70(8):5653–5680, 2024. doi:10.1109/TIT.2024.3399014.

- 66 Qisheng Wang and Zhicheng Zhang. Fast quantum algorithms for trace distance estimation. *IEEE Transactions on Information Theory*, 70(4):2720–2733, 2024. doi:10.1109/TIT.2023.3321121.
- 67 Qisheng Wang and Zhicheng Zhang. Time-efficient quantum entropy estimator via sampler. In *Proceedings of the 32nd Annual European Symposium on Algorithms*, pages 101:1–101:15, 2024. doi:10.4230/LIPIcs.ESA.2024.101.
- 68 Xinzhao Wang, Shengyu Zhang, and Tongyang Li. A quantum algorithm framework for discrete probability distributions with applications to Rényi entropy estimation. *IEEE Transactions on Information Theory*, 70(5):3399–3426, 2024. doi:10.1109/TIT.2024.3382037.
- 69 Youle Wang, Benchu Zhao, and Xin Wang. Quantum algorithms for estimating quantum entropies. *Physical Review Applied*, 19(4):044041, 2023. doi:10.1103/PhysRevApplied.19.044041.
- 70 John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468. IEEE, 2002. doi:10.1109/SFCS.2002.1181970.
- 71 John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. Preliminary version in *STOC 2006*. doi:10.1137/060670997.
- 72 Thomas Watson. The complexity of deciding statistical properties of samplable distributions. *Theory of Computing*, 11:1–34, 2015. Preliminary version in *STACS 2014*. ECCC:TR13–124. doi:10.4086/TOC.2015.V011A001.
- 73 Thomas Watson. The complexity of estimating min-entropy. *computational complexity*, 25(1):153–175, 2016. ECCC:TR12–070. doi:10.1007/S00037-014-0091-2.
- 74 Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002, 2020. doi:10.1103/RevModPhys.92.025002.
- 75 Tomoyuki Yamakami and Andrew C. Yao. $\text{NQP}_{\mathbb{C}} = \text{coC}_{=}P$. *Information Processing Letters*, 71(2):63–69, 1999. doi:10.1016/S0020-0190(99)00084-8.
- 76 Rui-Qi Zhang, Xiao-Qi Liu, Jing Wang, Ming Li, Shu-Qian Shen, and Shao-Ming Fei. Explicit formulas for estimating trace of reduced density matrix powers via single-circuit measurement probabilities. *Advanced Quantum Technologies*, 8(9), 2025. doi:10.1002/qute.202500376.
- 77 Yukun Zhang, Yusen Wu, You Zhou, and Xiao Yuan. Measuring less to learn more: Quadratic speedup in learning nonlinear properties of quantum density matrices. *arXiv preprint*, 2025. arXiv:2509.01571.
- 78 Zhengmin Zhang. Uniform estimates on the Tsallis entropies. *Letters in Mathematical Physics*, 80:171–181, 2007. doi:10.1007/s11005-007-0155-1.