Simultaneous min-entropy smoothing on multiparty systems

Lukas Drescher

Supervision: Dr. Omar Fawzi, Prof. Dr. Renato Renner

Institute for Theoretical Physics, ETH Zurich

July 7, 2013

Abstract

We consider the multiparty typicality conjecture raised by Dutil from a one-shot perspective. Asking for a multipartite state close to the state of the system that is typical on different subsystems simultaneously, this conjecture serves as a placeholder for the general difficulty to transfer the concept of classical joint typicality to the quantum setting. In this work, we reformulate the multiparty typicality conjecture as an optimization problem for min-entropies of different marginals. We find that the resulting one-shot conjecture is satisfied whenever the marginals under consideration commute. In this case we provide an optimal bound on the distance of the optimal state that demonstrates that atypical correlations for different subsystems can form mutually exclusive events on the global system. We furthermore show that our conjecture also holds in the two party quantum case. The techniques are then generalized to a restricted case for more parties given that the marginals to optimize do not overlap. Finally, this leads to a proof of our conjecture for tripartite systems in a pure state.

Contents

1 Introduction

In this thesis we consider an aspect of joint typicality on multiparty systems from a one-shot perspective. Our work is based on a recent conjecture raised in the context of multiparty state merging. It is closely related to another conjecture concerning communication over a quantum multiple access channel. The conjectures shall be motivated in the following.

First, let us consider the task of multiparty state merging. The initial setting is given by a number of senders $A_1, \ldots, A_m$ that share an unknown quantum state with a single receiver B. The goal is now to merge the senders' systems to the receiver using only classical communication and a minimal amount of entanglement. This task was first investigated by Horodecki et al. [1]. They provided a protocol for one-party state merging with optimal entanglement rate. This one-party state merging strategy admits a generalization to the multiparty scenario applying it successively on every sender's system. In this manner, the corner points of the entanglement rate region of multiparty state merging have been shown to be achievable [1]. Intermediate points on the boundary of this region can be approximated by partitioning a large number of rounds of the protocol into sections, on each following a different successive one-party state merging strategy with an appropriately permuted ordering among the senders. This technique is referred to as time sharing.

Although the successive one-party state merging presented in [1] was shown to achieve the full rate region it has a fundamental disadvantage. That is, it does not yield a code to directly achieve intermediate points in the entanglement rate region without time sharing. This is especially a drawback in the one-shot setting, where time sharing is impossible. It was thus attempted by Dutil [2] to avoid its use suggesting a protocol where all senders initially perform a simultaneous measurement on their systems. The initial joint state of the systems $A_1 \cdots A_m B$ is then reconstructed at the receiver's system by local actions. In order to show that such a protocol succeeds with high probability the proof requires for the given initial state on $A_1 \cdots A_m$ the existence of a close state with typical purities on every subsystem. Such a state was proven to exist for two senders in [2], leaving the case for more senders as a conjecture. A proof of this so called "multiparty typicality conjecture", restated as conjecture 3.2 in chapter 3 in this thesis, would complete the error analysis of the multiparty state merging protocol suggested in [2].

Subsequent to Dutil's conjecture, Nötzel [3] considered the problem of multiparty typicality from a representation theoretic point of view. Contributing an alternative proof for the case of two parties, the argument could, however, not be generalized further.

In this thesis, we approach multiparty typicality from a one-shot perspective reformulating Dutil's conjecture in terms of smooth min-entropies introduced by Renner [4]. Smooth entropies can be used to optimize the rate of various information processing tasks allowing for small error to eliminate atypical behaviour of the system. In the case of the smooth min-entropy, this corresponds

to reducing atypically large probabilities in the state of the system, for which we use the term "smoothing". The multiparty typicality conjecture 3.2 in a slightly stronger form then asks whether one can smooth atypically large probabilities on all subsystems of a multiparty system without to change the state too much. That is, given a state we search for a close state whose min-entropy exceeds the largest min-entropy in a specified neighbourhood of the system's actual state on every subsystem. The existence of such a state would then directly imply the multiparty typicality conjecture by virtue of the asymptotic equipartition property as we show in section 3.

The second conjecture of close interest was raised by Fawzi et al. in [5], who considered classical communication over a quantum multiple access channel (MAC). This work is put into a larger context in the thesis by Savov [6]. The setting is given by m senders that are connected to a receiver by a single classical-quantum (cq) channel. Proving the ability of a particular protocol to almost certainly transmit information through the cq-MAC essentially consists of finding a decoding POVM that allows the receiver to reconstruct the senders' messages with high probability. One possible strategy introduced by Winter in [7] is known as successive decoding. In the case of two senders, this means that the receiver first decodes the message of the first sender followed by the message of the second sender using the side-information from the first sender's message he has already decoded. The side-information in the second step allows for an increase in the capacity from sender two to the receiver compared to the point-to-point communication scenario. The rate tuple corresponding with the described strategy together with the one for the same strategy with a permuted ordering among the senders in the decoding protocol marks the corner points in the capacity region of the cq-MAC. Using time sharing, one can again approximate any intermediate rate point by a convex combination of different corner point strategies. The described strategy can be generalized to m parties in a straight forward manner as shown in [7].

Naturally, as it is the case with successive one-party state merging such an approach is infeasible to reach non-extremal points on the boundary of the capacity region of the cq-MAC in the one-shot setting. Similarly, we can replace the successive decoding strategy by a simultaneous decoding protocol to relax the restriction to time shared codes. In order to obtain a natural generalization of the error analysis of such a protocol from the classical case, one would need to include the properties of different conditionally typical projectors in the decoding POVM. Since conditionally typical projectors contrary to the classical setting in general do not commute it is not clear how to construct such a measurement. Nevertheless, the existence of a simultaneous decoder for the cq-MAC has been proved for the case of two senders ([5], Theorem 2). For three parties with the exception of certain special cases ([5], Theorem 5) it remained a conjecture ([5], Conjecture 4). Similar to the multiparty typicality conjecture there exists a one-shot counterpart of this conjecture in terms of smooth conditional min-entropies, which is however out of the scope of this thesis.

A proof of this simultaneous decoding conjecture for the case of three senders would be of special importance to the study of quantum interference channels with two senders and two receivers which is the main topic of [5]. For short, an interference channel is a shared communication medium among multiple senders and multiple receivers, where the goal of each sender is to communicate with a matched receiver in the presence of interference. For general classical interference channels the set of strategies discovered by Han and Kobayashi [8] yields the best known to be achievable rates to date. The Han-Kobayashi strategy involves splitting of the codebooks of each of the two senders into a personal and a common part. The point of this distinction is that every receiver is required to decode both messages of his corresponding sender as well as the common message of the other sender. Translating this strategy to the quantum setting, we are confronted with two instances of a simultaneous decoding problem for three sender cq-MACs ([5], proof of Theorem 12). The basic problem in this context is that an arbitrary point in the rate region of both cq-MACs may not necessarily be achievable. That is, we can always construct codes which yield an optimal rate on one of the cq-MACs by time sharing. However, if the corner-point strategies of this cq-MAC do not lie in the rate region of the other cq-MAC the code might not even be decodable for the second receiver. Actually, the ultimate goal would be to prove the decodability of any code that corresponds to a point lying in the intersection of the rate regions of both cq-MACs. This is exactly implied by the simultaneous decoding conjecture. We note that the achievability of the quantum Han-Kobayashi rate region follows without the simultaneous decoding conjecture for three senders from the results of Sen [9] who used a sequential decoding technique and subsequently Savov ([6], Theorem 5.5), who reduced the need for the three sender simultaneous decoding conjecture to hold to the case of two senders, both proving the achievability of the larger quantum Chong-Motani-Garg rate region [10].

We proceed with an outline of the content of this thesis. After a short introduction, we show in chapter 3 how the multiparty typicality conjecture 3.2 is related to the one-shot conjecture 3.1 concerning smooth min-entropies. In chapter 4, we prove conjecture 3.1 under the assumption that the marginals commute. This is especially satisfied in the classical setting. We then provide an explicit example to demonstrate that the distance estimate on the typical state we found in the proof is optimal in general. Specifically, we show that for sufficiently large systems there exists states consisting of correlations that form mutually exclusive events yet each of them being strongly atypical on a different subsystem. As a consequence, eliminating all atypicalities comes at the cost of inducing an error that runs exponentially in the number of parties. That is, unless the smoothing parameter is chosen exponentially small (almost) the entire state has to be smoothed off to achieve all different optimization objectives! Subsequently, we address the general quantum case in chapter 5, first proving conjecture 3.1 in the case of two parties and then generalizing the employed techniques to prove a restricted form of the conjecture for more parties. To show the limits of our current techniques we dedicate section 5.1.3 to the study of the three party system. Motivated by the

failure of the considered techniques in this case, a different approach based on a classical intuition is pursued in section 5.2. We first rederive the result from chapter 4 in the classical setting and then outline the obstacles in a quantum generalization of this argument.

2 Preliminary work

2.1 Foundations of quantum information theory

We assume the reader to be familiar with classical information theory and give a short introduction to the formalism of quantum information theory. For a more comprehensive overview the reader is referred to the book by Nielsen and Chuang [12].

The state of a quantum system is given by a normalized positive semidefinite operator ρ on a Hilbert space A,

$$\rho \in \mathcal{S}_=(A) := \{\tau \in \mathcal{P}(A) | \operatorname{tr} \tau = 1\}.$$

Here, we denote the positive semi-definite cone, that is the set of hermitian operators with positive eigenvalues, by $\mathcal{P}(A) = \{\rho \in \operatorname{End}(A) | \rho \geq 0\}$. The state ρ is not immediately observable itself, but through measurements with probabilistic outcomes. A measurement is characterized by a positive operator-valued measure on the set of possible outcomes $\mathcal{X}$, that is a set $\{M_x\}_{x\in\mathcal{X}} \subset \mathcal{P}(A)$, with the property $\sum_{x\in\mathcal{X}} M_x = \mathbb{1}_A$. The probability of measuring a particular $x \in \mathcal{X}$ is given by $\operatorname{tr}(M_x\rho)$. The process of measuring a quantum system always imposes an evolution on its state. More generally, a quantum evolution is given by a trace preserving completely positive map, which can be represented as an operator sum by

$$\mathcal{E} : \rho \in \mathcal{S}_=(A) \mapsto \sum_k E_k \rho E_k^\dagger \in \mathcal{S}_\leq(A')$$

where the set $\{E_k\}_k \in \operatorname{Hom}(A, A')$ is called Kraus operators satisfying the condition $\sum_k E_k^\dagger E_k = \mathbb{1}_A$. The measurement considered above can then be seen as a quantum evolution from the system A to the classical-quantum system $X \otimes A$ by

$$\mathcal{E}_{A\to X\otimes A} : \rho \mapsto \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \sqrt{M_x}\rho\sqrt{M_x}.$$

Here, the post-measurement state of the system A is conditioned on the measurement outcome $x \in \mathcal{X}$ in the first factor of $X \otimes A$. If the measurement is unknown, the post-measurement state on A is just the reduced state $(\mathcal{E}_{A\to X\otimes A}(\rho))_A$.

The Hilbert space of a composite quantum system consisting of two parties A_1 and A_2 is given by the tensor product $A_1A_2 := A_1 \otimes A_2$. An m-party system with parties $A_1, \ldots, A_m$ is consequently described by $A_1 \cdots A_m =: A$. In the following, we use the letter A_i to equivalently denote the Hilbert space as well as a label for the system itself. Whenever we write $S \subset A_1 \cdots A_m$, $S \neq \emptyset$, we mean by S the subsystem with state space $\bigotimes_{A_i\in S, 1\leq i\leq m} A_i$. Its complementary system in $A_1 \cdots A_m$ is denoted by S^c, so that $S \otimes S^c = A$. We reserve the notation $|S|$ for the number of parties in subsystem S, except for section 4.1 where the notation $|\cdot|$ is used as a counting measure on classical registers. Furthermore, by $\mathcal{K} \subset 2^{A_1,\ldots,A_m} \setminus \{\emptyset\}$ we mean a collection of non-empty subsystems of A.

2.2 Distance measures

We use two distance measures based on extensions of the trace distance and the fidelity to subnormalized states,

$$\mathcal{S}_{\leq}(A) := \{\rho \in \mathcal{P}(A) | \operatorname{tr} \rho \leq 1\}.$$

Subnormalized states themselves do not have an immediate physical interpretation. However, they can be seen as density operators of a larger system restricted to a subsystem. Moreover, every non-zero subnormalized density operator corresponds to an element of $\mathcal{S}(A)$ through normalization. For subnormalized states, we define quantum evolutions as trace non-increasing completely positive maps. That is, in terms of Kraus operators we require only the inequality $\sum_k E_k^\dagger E_k \leq \mathbb{1}_A$ instead of equality. A more comprehensive introduction is given [13, Chapter 3].

For the following, let $\rho, \sigma \in \mathcal{S}_{\leq}(A)$ be subnormalized density operators. The trace distance is defined as

$$D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 + \frac{1}{2}|\operatorname{tr}(\rho - \sigma)|,$$

where $\|M\|_1 = \operatorname{tr}\left[\sqrt{M^\dagger M}\right]$ is the trace-norm. Another distance function that is more commonly used in this context is the purified distance [13].

$$P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2},$$

where the fidelity is given by

$$F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \operatorname{tr}\rho)(1 - \operatorname{tr}\sigma)}.$$

The two distance measures are related by

$$D(\rho, \sigma) \leq P(\rho, \sigma) \leq \sqrt{2D(\rho, \sigma)}. \tag{1}$$

For the trace distance, the closed ε-ball around ρ is denoted by $B_\varepsilon^D(\rho)$ and for the purified distance by $B_\varepsilon^P(\rho)$. Quantum evolutions are non-expansive maps in both the trace distance and the purified distance. That is, for any trace non-increasing completely positive map $\mathcal{E}$, we find

$$\begin{aligned} D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &\leq D(\rho, \sigma), \\ P(\mathcal{E}(\rho), \mathcal{E}(\sigma)) &\leq P(\rho, \sigma). \end{aligned} \tag{2}$$

2.3 Min-entropy

Let $\rho \in \mathcal{S}_{\leq}(A)$. The min-entropy of the state ρ is defined as $\mathbf{H}_{\min}(A)_\rho := -\log \lambda_{\max}(\rho)$ where $\lambda_{\max}(\rho) := \|\rho\|_\infty$ denotes the largest eigenvalue of ρ. For $\varepsilon > 0$ the smooth min-entropy of ρ is

$$\begin{aligned} \mathbf{H}_{\min}^{\varepsilon, X}(A)_\rho &:= \max_{\sigma \in B_\varepsilon^X(\rho)} \mathbf{H}_{\min}(A)_\sigma \\ &= -\log\Big(\min_{\sigma \in B_\varepsilon^X(\rho)} \lambda_{\max}(\sigma)\Big) \end{aligned} \tag{3}$$

where X can be chosen to be either D for trace-distance or P for purified distance. As the purified distance is more commonly used in this setting, we drop the superscript P when using it. Since $B_\varepsilon^X(\rho) \subset \mathcal{S}_\leq(A)$ is compact the maximum in (3) is well-defined and achieved by a state $\sigma \in B_\varepsilon^X(\rho)$,

$$\mathbf{H}_{\min}(A)_\sigma = \mathbf{H}_{\min}^{\varepsilon,X}(A)_\rho. \tag{4}$$

Note that this state σ necessarily lies on the boundary $\partial B_\varepsilon^X(\rho)$ since for every $\tau \in \operatorname{int}(B_\varepsilon^X(\rho))$ we can find a scalar $\lambda \in (0,1)$ so that $\mathbf{H}_{\min}(A)_{\lambda\tau} > \mathbf{H}_{\min}(A)_\tau$ while $\lambda\tau \in B_\varepsilon^X(\rho)$. The state σ can always be assumed to share a particular eigenbasis with ρ since a measurement $\mathcal{E}$ with respect to an eigenbasis of ρ increases neither the largest eigenvalue of σ nor the distance $X(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq X(\rho, \sigma)$.

As we demonstrate in the subsequent Lemma, the state $\sigma \in B_\varepsilon^X(\rho)$ that satisfies (4) has the following structure:

Lemma 2.1 (Min-entropy smoothing)**.** *Let $\rho \in \mathcal{S}_\leq(A)$, $\varepsilon > 0$. For $X = D$ the state $\sigma \in B_\varepsilon^X(\rho)$ that achieves* (4) *is not unique. Define the function*

$$f_\varepsilon^D(x) = \begin{cases} 2^{-\mathbf{H}_{\min}^{\varepsilon,D}(A)_\rho}, & x > 2^{-\mathbf{H}_{\min}^{\varepsilon,D}(A)_\rho} \\ x, & x \leq 2^{-\mathbf{H}_{\min}^{\varepsilon,D}(A)_\rho}. \end{cases}$$

Then $\sigma := f_\varepsilon^D(\rho) \in B_\varepsilon^D(\rho)$ satisfies (4) *for $X = D$. In contrast, for $X = P$ the state $\sigma \in B_\varepsilon^P(\rho)$ such that* (4) *holds is unique. For $\varepsilon > 0$ so that*

$$\phi := \arcsin(\varepsilon) \leq \begin{cases} \arctan\left(\sqrt{\frac{\frac{1}{m_\lambda} - \lambda}{\lambda'}}\right) - \beta & , \lambda' > 0, \\ \frac{\pi}{2} & , \lambda' = 0, \end{cases}$$

where $\lambda := \lambda_{\max}(\rho)$ with $m_\lambda := d_{\mathrm{Eig}(\rho,\lambda)}$, $\beta := \arccos(\sqrt{\lambda m_\lambda})$, $\lambda' := \max_{\mu \in \operatorname{Spec}\rho \setminus \{\lambda\}} \mu$, it is given by $\sigma := f_\varepsilon^P(\rho)$ with

$$f_\varepsilon^P(x) = \begin{cases} \frac{\cos^2(\beta+\phi)}{\cos^2(\beta)} x, & x > 2^{-\mathbf{H}_{\min}^{\varepsilon,P}(A)_\rho} \\ \frac{\sin^2(\beta+\phi)}{\sin^2(\beta)} x, & x \leq 2^{-\mathbf{H}_{\min}^{\varepsilon,P}(A)_\rho} \end{cases}$$

Proof As remarked previously, the determination of the min-entropy smoothing state reduces to the classical problem. That is we can restrict the optimization in (3) to density operators that commute with ρ. Since the ambiguity of the eigenbasis of σ as we shall see in the remainder of the proof will not affect our statements, we assume it to share a particular eigenbasis with ρ. We note that the trace distance and fidelity for subnormalized states $\rho, \sigma \in \mathcal{S}_\leq(A)$ are equal to the corresponding expressions for the normalized states $\hat{\rho} := \rho \oplus (1 - \operatorname{tr}\rho)$, $\hat{\sigma} := \sigma \oplus (1 - \operatorname{tr}\sigma)$ on the extended Hilbert space $A \oplus \mathbb{C}$.

Choosing a particular eigenbasis of ρ, we identify the states $\hat{\rho},\ \hat{\sigma}$ with points $p,\ q \in \mathbb{R}_+^{d_A+1}$ containing the eigenvalues in their components. The min-entropy optimization problem then translates to

$$\begin{aligned} \text{minimize} \quad & \max_{1\leq i\leq d_A} q_i \\ \text{subject to:} \quad & \frac{1}{2}\|p-q\|_1 = \varepsilon,\ \|q\|_1 = 1 \end{aligned}$$

in case of the trace distance. We can decompose $q-p = \{q-p\}_+ - \{q-p\}_-$ into its positive and negative part with 1-norm ε each due to $\|p\|_1 = 1 = \|q\|_1$. Only the negative part $-\{q-p\}_-$ can be used to minimize the object function, which is achieved by reducing the largest components of p by ε in total. The positive weight can be distributed arbitrarily over the other components as long as the object function is not changed. A feasible choice is $\{q-p\}_+ = (0,\ldots,0,\varepsilon)$ giving rise to the function f_ε^D defined in the Lemma.

For the purified distance, we define $p,q \in S^{d_A} \subset \mathbb{R}^{d_A+1}$ component-wise as the square-root of the eigenvalues of $\hat{\rho},\ \hat{\sigma}$. The min-entropy optimization problem for the purified distance then is

$$\begin{aligned} \text{minimize} \quad & \max_{1\leq i\leq d_A} q_i \\ \text{subject to:} \quad & \langle p,q\rangle = \sqrt{1-\varepsilon^2},\ \|q\|_2 = 1 \end{aligned}$$

We note that $q = \sqrt{1-\varepsilon^2}p + q_\perp$ with $p \perp q_\perp$, $\|q_\perp\|_2 = \varepsilon$. Let $p_1 = \cdots = p_{m_\lambda} = \lambda$ be the maximal components of p. If ε is small enough so that there exists no feasible q with $q_j > \max_{1\leq i\leq m_\lambda} q_i$ the optimal $q_\perp$ is such that the overlap with $p_{\max} = (p_1,\ldots,p_{m_\lambda},0,\ldots,0)$ is minimized. Denoting by $\Pi : r \mapsto r - \langle p,r\rangle\, p$ the orthogonal projection onto $p^\perp := \{r \in \mathbb{R}^{d_A+1} |\, \langle p,r\rangle = 0\}$, we find by the Cauchy-Schwarz inequality

$$\begin{aligned} |\langle p_{\max}, q_\perp\rangle| &\overset{q_\perp\in p^\perp}{=} |\langle \Pi p_{\max}, q_\perp\rangle| \\ &\leq \|\Pi p_{\max}\|_2 \|q_\perp\|_2 \end{aligned}$$

with equality if $q_\perp \propto \Pi p_{\max}$ and hence we find the unique optimal $q_\perp = -\varepsilon\frac{\Pi p_{\max}}{\|\Pi p_{\max}\|_2} \in \mathrm{Span}\{p_{\max}, p\}$. Thus the unique optimal $q \in S^{d_A}$ is given by

$$\begin{aligned} q &= \cos(\phi)p - \sin(\phi)\frac{\Pi p_{\max}}{\|\Pi p_{\max}\|_2} \\ &= \cos(\beta+\phi)\frac{p_{\max}}{\|p_{\max}\|_2} + \sin(\beta+\phi)\frac{p-p_{\max}}{\sqrt{1-\|p_{\max}\|_2^2}} \end{aligned}$$

with $\varepsilon = \sin(\phi)$, $\|p_{\max}\|_2 = \cos(\beta)$. □

Using this Lemma, we define $\mathbf{H}_{\min}$-smoothing as a quantum operation. Concisely, we realize it as a multiplication operator on the eigenvalues $\{\lambda_i\}_i$ of the

state $\rho \in \mathcal{S}_{\leq}(A)$, mapping λ_i to $f_\varepsilon(\lambda_i)\lambda_i$. The smoothing function, $f_\varepsilon(x) := \frac{f_\varepsilon^D(x)}{x}$ for $x \in (0,1]$, $f_\varepsilon(0) := 1$, is chosen according to Lemma 2.1. Since $f_\varepsilon \leq 1$, we can represent this map as a quantum operation on $\mathcal{S}_{\leq}(A)$,

$$\mathcal{E} : \tau \mapsto \sqrt{f_\varepsilon}(\rho)\tau\sqrt{f_\varepsilon}(\rho). \tag{5}$$

Note that this map is also a feasible smoothing operation for P due to $\mathbf{H}_{\min}^{\varepsilon,P}(A)_\rho \leq \mathbf{H}_{\min}^{\varepsilon,D}(A)_\rho$ by (1). For the distance we then find $P(\rho, \mathcal{E}(\rho)) \leq \sqrt{2\varepsilon}$. An analogous construction for the purified distance is not possible since the Kraus operator would have eigenvalues that exceed 1 provided the spectrum of ρ contains more than a single non-zero eigenvalue. Cutting such a map down to a quantum operation by reducing the largest eigenvalue of the Kraus operator to 1, one generally induces a distance error of $P(\rho, \mathcal{E}(\rho)) \sim \sqrt{\varepsilon}$ in the limit $\varepsilon \to 0$.[1] Thus, we will use the trace distance to define the smoothing operation (5). Its Kraus operators, in the following denoted by $\Pi := \sqrt{f_\varepsilon^D(\rho)}$, then satisfy

$$\Pi \in \mathcal{P}(A),\ \Pi \leq \mathbb{1}_A,\ [\Pi, \rho] = 0.$$

Since the properties of the operation (5) that are essential for the proofs in this thesis are captured in these conditions, we will in the remainder of this thesis use them to define min-entropy smoothing as a quantum operation and refer to such a Π with additional property that $\sigma = \Pi\rho\Pi$ as a min-entropy smoothing operator.

The smooth min-entropy, moreover, exhibits the following important property:

Lemma 2.2 (Monotonicity of the smooth min-entropy)**.** *Let $\rho, \sigma \in \mathcal{S}_{\leq}(A)$, $\sigma \leq \rho$ and $\varepsilon > 0$. Then $\mathbf{H}_{\min}^{\varepsilon,X}(A)_\sigma \geq \mathbf{H}_{\min}^{\varepsilon,X}(A)_\rho$ for both $X = D$ and $X = P$.*

[1] Let A be a qubit with the state $\rho = \cos^2(\theta)|0\rangle\langle 0| + \sin^2(\theta)|1\rangle\langle 1|$, $\theta \in (0, \frac{\pi}{4})$. Ordering the Schmidt-coefficients of a purification non-increasingly, we obtain the Schmidt vector of ρ, $(\cos\theta, \sin\theta)$. The Schmidt vector of the min-entropy smoothing state for $\varepsilon \leq \sin(\frac{\pi}{4} - \theta)$ is then given by $\sqrt{s} = (\cos(\theta+\phi), \sin(\theta+\phi))$, $\phi = \arcsin(\varepsilon)$. This follows from the fact that the purified distance simplifies to the sine of the angle between Schmidt vectors for normalized states. The closest state σ to ρ with the property $\mathbf{H}_{\min}(A)_\sigma \geq \mathbf{H}_{\min}^{\varepsilon,P}(A)_\rho$ and $\sigma \leq \rho$ is then characterized by the Schmidt vector $\sqrt{s}^{\downarrow} = (\cos(\theta+\phi), \sin(\theta))$. This is the case since any state whose eigenspaces differ from those of ρ can be measured with respect to an eigenbasis of ρ. Such a measurement does neither affect the operator ordering between that state and ρ, nor decrease its min-entropy or increase its distance to ρ. After some trigonometric analysis we find for the fidelity

$$F(\rho,\sigma) = 1 - \cos(\theta)\underbrace{\cos\left(\frac{\pi-\phi}{2} - \theta\right)}_{=\cos\left(\frac{\pi}{2}-\theta\right)+\mathcal{O}(\varepsilon)}\underbrace{2\sin\left(\frac{\phi}{2}\right)}_{=\varepsilon+\mathcal{O}(\varepsilon^2)} = 1 - \frac{1}{2}\sin(2\theta)\varepsilon + \mathcal{O}(\varepsilon^2).$$

Since the purified distance involves the fidelity squared, we find $P(\rho,\sigma) = \sin(2\theta)\sqrt{\varepsilon} + \mathcal{O}(\varepsilon)$ in the limit $\varepsilon \to 0$. Thus for every non-pure normalized qubit state $\rho \in \mathcal{S}_{=}(A)$, $\rho \neq \frac{1}{2}\mathbb{1}_A$, we have

$$\lim_{\varepsilon\to 0} \frac{P(\rho,\sigma)}{\sqrt{\varepsilon}} = \sin(2\theta).$$

Proof Fix X to be either D or P. Let $\omega \in B_\varepsilon^X(\rho)$ be such that $\mathbf{H}_{\min}(\omega) = \mathbf{H}_{\min}^{\varepsilon,X}(\rho)$. Let $\sigma = \sum_i \mu_i |v_i\rangle \langle v_i|$ be a spectral decomposition of σ with strictly positive eigenvalues $\{\mu_i\}_i$. Let

$$E_i := \frac{\mu_i}{\langle v_i| \rho |v_i\rangle} |v_i\rangle \langle v_i| \leq \mathbb{1}_{\mathcal{H}}$$

be a set of positive operators and define the trace-non-increasing CPM $\mathcal{E}$

$$\mathcal{E} : \tau \to \sum_i \sqrt{E_i} \tau \sqrt{E_i}$$

By construction, one has $\mathcal{E}(\rho) = \sigma$. Using the monotonicity of X under trace non-increasing CPMs (2),

$$X(\mathcal{E}(\omega), \sigma) \leq X(\omega, \rho) \leq \varepsilon,$$

and the fact that

$$\begin{aligned} \|\mathcal{E}(\omega)\|_\infty &= \max_i \frac{\mu_i}{\langle v_i| \rho |v_i\rangle} \langle v_i| \omega |v_i\rangle \\ &\leq \max_i \langle v_i| \omega |v_i\rangle \\ &\leq \|\omega\|_\infty \end{aligned}$$

it follows that $\mathbf{H}_{\min}^{\varepsilon,X}(\sigma) \geq \mathbf{H}_{\min}(\mathcal{E}(\omega)) \geq \mathbf{H}_{\min}(\omega) = \mathbf{H}_{\min}^{\varepsilon,X}(\rho)$. □

3 Conjecture

We first present our one-shot conjecture on simultaneous min-entropy smoothing and then show how it is related to Dutil's multiparty typicality conjecture below.

Conjecture 3.1 (Simultaneous min-entropy smoothing)**.** *For any number of parties $m \in \mathbb{N}$ there exists a function g_m with $\lim_{\varepsilon \to 0} g_m(\varepsilon) = 0$ such that the following holds.*

For any state $\rho \in \mathcal{S}_{\leq}(A)$ on any m-party system $A = A_1 \cdots A_m$, there exists a state $\sigma \in B^P_{g_m(\varepsilon)}(\rho)$ that satisfies

$$\mathbf{H}_{\min}(S)_\sigma \geq \mathbf{H}^\varepsilon_{\min}(S)_\rho, \ \forall S \subset \{A_1, \ldots, A_m\}, \ S \neq \emptyset.$$

Note that the rate of convergence given by the function g_m is the same for all systems A with equal number of parties. For applications, it is important that g_m does not depend on the dimensions of the parties $A_1, \ldots, A_m$. We remark that equivalently to the purified distance one may also use the trace distance to formulate conjecture 3.1 by relation (1).

We now state the multiparty typicality conjecture (conjecture 3.2.7 in [2]).

Conjecture 3.2 (Multiparty typicality)**.** *Let $A = A_1 \cdots A_m$ be an m-party system in state $\rho \in \mathcal{S}_{\leq}(A)$. Fix $\varepsilon, \delta > 0$. For $n \in \mathbb{N}$ large enough there exists a state $\sigma \in B^{\|\cdot\|_1}_\varepsilon(\rho^{\otimes n})$ such that*

$$\mathrm{tr}((\sigma_{S^{\otimes n}})^2) \leq 2^{-n(\mathbf{H}(S)_\rho - \delta)}, \forall S \subset \{A_1, ..., A_m\}, \ S \neq \emptyset.$$

We note that the multiparty typicality conjecture 3.2 in the above form follows from the simultaneous min-entropy smoothing conjecture 3.1 applied to the system $A^{\otimes n}$ with parties $A_1^{\otimes n}, \ldots, A_m^{\otimes n}$ in the tensor power state $\rho^{\otimes n}$. To see this, we choose the smoothing parameter $\varepsilon' > 0$ such that $g_m(\varepsilon') \leq \varepsilon/2$. Then, by conjecture 3.1 there exists a state $\sigma \in B^P_{g_m(\varepsilon')}(\rho^{\otimes n})$ with $\|\sigma - \rho^{\otimes n}\|_1 \leq 2P(\sigma, \rho^{\otimes n}) \leq \varepsilon$ using (1) that satisfies

$$\begin{aligned}
\mathrm{tr}((\sigma_{S^{\otimes n}})^2) &\leq \lambda_{\max}(\sigma_{S^{\otimes n}}) \\
&\leq 2^{-\mathbf{H}^{\varepsilon'}_{\min}(S^{\otimes n})_{\rho^{\otimes n}}} \\
&\leq 2^{-n(\mathbf{H}(S)_\rho - \mathcal{O}(\frac{1}{\sqrt{n}}))}.
\end{aligned}$$

The last inequality follows by virtue of the asymptotic equipartition property [13].

4 Commutative min-entropy smoothing

In this chapter, we prove conjecture 3.1 under the assumptions that the min-entropy smoothing operations for different subsystems commute and only decrease the state of the system globally. These assumptions are always satisfied in the classical case. Furthermore, we provide an optimal distance bound g_m in this case.

In the following, we describe the state of a classical system $A = A_1 \cdots A_m$ by a density operator

$$\rho = \sum_{i_1=1}^{d_{A_1}} \sum_{i_2=1}^{d_{A_2}} \cdots \sum_{i_m=1}^{d_{A_m}} p_{i_1 \ldots i_m} |i_1\rangle\langle i_1|_{A_1} \otimes \cdots \otimes |i_m\rangle\langle i_m|_{A_m} \tag{6}$$

where $\{|i_k\rangle\}_{1 \leq i_k \leq d_{A_k}}$ denotes an orthonormal basis of A_k for all $k \in \{1, \ldots, m\}$ and $(p_{i_1 \ldots i_m})_{1 \leq i_k \leq d_{A_k}, 1 \leq k \leq m}$ is a probability distribution on the register $\prod_{k=1}^{m} \{1, \ldots, d_{A_k}\}$. Where the particular eigenbasis of ρ is not explicitly needed, we equivalently use the probability distribution $(p_{i_1 \ldots i_m})_{1 \leq i_k \leq d_{A_k}, 1 \leq k \leq m}$ to characterize ρ. The form (6) of the state ρ implies the commutation relations

$$[\rho_S \otimes \mathbb{1}_{S^c}, \rho_T \otimes \mathbb{1}_{T^c}] = 0 \tag{7}$$

for all non-empty $S, T \subset \{A_1, \ldots, A_m\}$. Subsequently, we show that conjecture 3.1 is satisfied under slightly weaker assumptions than (7) on the state ρ. In preparation for the result we prove the following.

Lemma 4.1. *Let $\rho \in \mathcal{S}_{\leq}(A)$, $\mathcal{K} \subset 2^{\{A_1, \ldots, A_m\}} \setminus \{\emptyset\}$. Let $\{\Pi^S\}_{S \in \mathcal{K}} \subset \mathcal{P}(A)$ with $\Pi^S \leq \mathbb{1}_S$ for all $S \in \mathcal{K}$, such that*

$$[\Pi^S, \Pi^T] = 0 \; \forall S, T \in \mathcal{K}, \tag{8}$$

$$[\Pi^S, \rho] = 0 \; \forall S \in \mathcal{K}. \tag{9}$$

Then the state

$$\sigma := \left(\prod_{S \in \mathcal{K}} \Pi^S \right) \rho \left(\prod_{S \in \mathcal{K}} \Pi^S \right) \tag{10}$$

satisfies

$$\sigma \leq \Pi^S \rho \Pi^S \; \forall S \in \mathcal{K} \tag{11}$$

$$D(\rho, \sigma) \leq \sum_{S \in \mathcal{K}} D(\rho_S, \Pi^S \rho_S \Pi^S). \tag{12}$$

Proof We first show equation (11). Fix a subsystem $S \in \mathcal{K}$. By the commutation relations (8) the operator Π^S may be moved to the outermost position,

$$\sigma = \Pi^S \Pi^{\$} \rho \Pi^{\$} \Pi^S,$$

where $\$:= \mathcal{K} \setminus \{S\}$ and $\Pi^{\$} = \prod_{T \in \$} \Pi^T$ accordingly. Since for any $T \in \$$, Π^T and ρ are simultaneously diagonalizable and $\Pi^T \leq \mathbb{1}_A$ we find $\Pi^T \rho \Pi^T \leq \rho$.

By induction it follows that $\Pi^{\$}\rho\Pi^{\$} \leq \rho$. Applying Π^S to this inequality gives $\sigma \leq \Pi^S\rho\Pi^S$ as required.

To compute a bound for $D(\rho,\sigma)$ consider an arbitrary ordering $(S^i)_{1\leq i\leq|\mathcal{K}|}$ of all considered subsystems $\mathcal{K}$. Define $\tilde{\Pi}^i := \prod_{j=1}^{i-1}\Pi^{S^j}$ for $1 \leq i \leq |\mathcal{K}|$ (the empty product is defined to be $\mathbb{1}_A$). By the commutation relations (8) $\tilde{\Pi}^i$ is hermitian. Since $\|\tilde{\Pi}^i\|_\infty \leq \prod_{j=1}^{i-1}\|\Pi^j\|_\infty \leq 1$, we have $\tilde{\Pi}^i \leq \mathbb{1}_A$. Then

$$\begin{aligned} D(\rho,\sigma) &\leq \sum_{i=1}^{|\mathcal{K}|} D(\tilde{\Pi}^i\rho\tilde{\Pi}^i, \tilde{\Pi}^i\Pi^{S^i}\rho\Pi^{S^i}\tilde{\Pi}^i) \\ &\leq \sum_{i=1}^{|\mathcal{K}|} D(\rho, \Pi^{S^i}\rho\Pi^{S^i}) \\ &= \sum_{i=1}^{|\mathcal{K}|} D(\rho_{S^i}, \Pi^{S^i}\rho_{S^i}\Pi^{S^i}) \end{aligned}$$

where we used the monotonicity of D under the trace non-increasing CPMs $\mathcal{E}_i : \tau \to \tilde{\Pi}^i\tau\tilde{\Pi}^i$ in the second line (2). In the third line we applied the property of the trace distance that for

$$\tau,\omega \in \mathcal{S}_{\leq}(\mathcal{H}), \tau \geq \omega : D(\tau,\omega) = \mathrm{tr}(\tau-\omega) \tag{13}$$

to the inequality $\rho \geq \Pi^{S^i}\rho\Pi^{S^i}$. □

This Lemma can be employed to prove conjecture 3.1 in the case where the min-entropy smoothing operations for different subsystems commute and only decrease the state of the system globally.

Corollary 4.2. *Let $\rho \in \mathcal{S}_{\leq}(A)$, $\mathcal{K} \subset 2^{\{A_1,\ldots A_m\}} \setminus \{\emptyset\}$ and $\varepsilon > 0$. For $S \in \mathcal{K}$ define $\Pi^S \in \mathcal{P}(S)$, $\Pi^S \leq \mathbb{1}_S$ such that*

$$\begin{aligned} &\mathbf{H}_{\min}(S)_{\Pi^S\rho\Pi^S} = \mathbf{H}^{\varepsilon,D}_{\min}(S)_\rho, \\ &D(\rho_S, \Pi^S\rho_S\Pi^S) \leq \varepsilon. \end{aligned} \tag{14}$$

If $\{\Pi^S\}_{S\in\mathcal{K}}$ and ρ fulfill conditions (8) and (9) then $\sigma \in \mathcal{S}_{\leq}(A)$ defined as in (10) satisfies

$$\mathbf{H}_{\min}(S)_\sigma \geq \mathbf{H}^{\varepsilon,D}_{\min}(S)_\rho \;\forall S \in \mathcal{K} \tag{15}$$

$$D(\rho,\sigma) \leq |\mathcal{K}|\varepsilon. \tag{16}$$

Proof Apply Lemma 4.1 and use Lemma (2.2) for $\sigma \leq \rho$ to obtain (15). □

Note that this proof can be generalized replacing the smoothing maps $\rho \mapsto \Pi^S \rho \Pi^S$ by arbitrary trace non-increasing CPMs $\mathcal{E}^S$ acting on the global system A with

$$\begin{aligned} \mathbf{H}_{\min}(S)_{\mathcal{E}^S(\rho)} &= \mathbf{H}_{\min}^{\varepsilon,D}(S)_\rho, \\ D(\rho, \mathcal{E}^S(\rho)) &\leq \varepsilon \end{aligned}$$

for all $S \in \mathcal{K}$. The condition of commutative, globally state decreasing min-entropy smoothing (8), (9) then become $\mathcal{E}^S \circ \mathcal{E}^T = \mathcal{E}^T \circ \mathcal{E}^S$ and $\mathcal{E}^S(\rho) \leq \rho$ for all $S, T \in \mathcal{K}$.

As introductorily indicated, choosing $\mathcal{K} = 2^{\{A_1,\ldots A_m\}} \setminus \{\emptyset\}$ Corollary 4.2 proves conjecture 3.1 for all classical states. In particular, with the choice $\Pi^S = \sqrt{f_\varepsilon^D(\rho_S)}$, f_ε^D as defined in chapter 2, the eigenspaces of the state ρ_S always refine the eigenspaces of Π^S for every $S \in \mathcal{K}$. We can employ this to conclude that (8), (9) follow from (7) $\forall S, T \in \mathcal{K} \cup \{A\}$. In fact, conjecture 3.1 has a well-defined classical limit. Even if quantum states are available to define a simultaneous min-entropy smoother σ it can be chosen to be classical whenever ρ is classical. This follows from the fact that a measurement of σ in the classical basis cannot increase neither its largest eigenvalue on any subsystem nor the distance to ρ on the total system. Therefore, the closest simultaneous min-entropy smoother of a given classical state can always be assumed to be classical.

Corollary 4.2 does, however, not only apply to classical states. In particular, the commutation relations (7) $\forall S, T \in \mathcal{K} \cup \{A\}$ do not imply that the state ρ is classical. As an example consider a bipartite system $A_1 A_2$ in the entangled pure state

$$|\psi\rangle = \sum_{j=1}^{d} \frac{1}{\sqrt{d}} |j, j\rangle_{A_1 A_2}, \tag{17}$$

where $\{|j\rangle_{A_i}\}_{1 \leq j \leq d_{A_i}}$ is an arbitrary orthonormal set on A_i for $i = 1, 2$ and $1 \leq d \leq \min\{d_{A_1}, d_{A_2}\}$. This state has one-party marginals that are fully mixed on their support which immediately implies (7). Hence, we find that Corollary 4.2 holds for the special class of bipartite entangled pure states whose Schmidt coefficients are fully degenerate.

In fact this is the most general bipartite pure state to which Corollary 4.2 applies if $\mathcal{K}$ contains a one party subsystem A_i. To see this, observe that (9) requires $\Pi^{A_i} |\psi\rangle \propto |\psi\rangle$. By analysing the effect of Π^{A_i} on the Schmidt-coefficients of $|\psi\rangle$, this can only be satisfied if Π^{A_i} is a multiple of the identity on $\mathrm{supp}|\psi\rangle\langle\psi|_{A_i}$. Then by definition of Π^{A_i}, $|\psi\rangle\langle\psi|_{A_i}$ can have only one non-zero eigenvalue and hence $|\psi\rangle$ is given by (17).

For the case of a general bipartite pure state one may ask whether there exist small perturbations of the smoothing operators so that the modified Π^{A_i}, $i = 1, 2$, achieve $[\Pi^{A_i}, |\psi\rangle\langle\psi|] = 0$ while satisfying the property

$$\mathbf{H}_{\min}(A_i)_{\Pi^{A_i} |\psi\rangle\langle\psi| \Pi^{A_i}} \geq \mathbf{H}_{\min}^{\varepsilon,D}(A_i)_{|\psi\rangle\langle\psi|}.$$

This, however, is not the case since it implied that $\sigma \leq |\psi\rangle\langle\psi|$ for σ defined as in (10) and hence $\sigma = \lambda|\psi\rangle\langle\psi|$, $\lambda \in (0,1)$. Now, let $|\psi\rangle$ have Schmidt-coefficients $\sqrt{c+\varepsilon}$ with multiplicity 1 and $\sqrt{c}$ with multiplicity $d-1$, where $d := \min\{d_{A_1}, d_{A_2}\}$, $c := \frac{1-\varepsilon}{d}$. We then find that $\lambda \leq \frac{c}{c+\varepsilon} = \frac{1-\varepsilon}{1+(d-1)\varepsilon}$. Hence if the parties A_1, A_2 are large enough the state σ will have vanishingly small trace, $\operatorname{tr}\sigma = \lambda$. Thus, for a pure multiparty state ψ, a close min-entropy smoother of a one-party subsystem in general cannot be smaller than $|\psi\rangle\langle\psi|$ on the total system with respect to the positive semidefinite operator ordering.

We conclude this section with the observation that for every bipartite pure state ψ we can always find a commuting family $\{\Pi^S\}_{S\in\mathcal{K}}$ with the properties in (14). This is due to the fact that one can choose $\Pi^{A_1A_2} \propto \mathbb{1}_{A_1A_2}$. In fact, the state defined in (10) then satisfies (15) as the interested reader may verify. The expression ε on the right hand side of expression (16) then has to be replaced by $\sqrt{2\varepsilon}$. Since the proof of these facts involves techniques introduced in section 5.1.1, we omit it here.

4.1 Optimal classical simultaneous min-entropy smoothing

We provide an example that shows that the distance bound (16) can be saturated in the classical setting. For the functions $\{g_m\}_{m\in\mathbb{N}}$ introduced in chapter 3 this implies that the choice

$$g_m(\varepsilon) = (2^m - 1)\varepsilon$$

is optimal in the classical limit of conjecture 3.1 formulated in terms of the trace distance.

Theorem 4.3 (Optimal classical simultaneous min-entropy smoothing)**.** *Let $\bar{\varepsilon} > 0$. There exists $N_{\bar{\varepsilon}} \in \mathbb{N}$ such that on every classical system $A = A_1 \cdots A_m$ with $\min_{1\leq i\leq m} d_{A_i} \geq N_{\bar{\varepsilon}}$ the following holds. For any $\mathcal{K} \subset 2^{\{A_1,\ldots,A_m\}} \setminus \{\emptyset\}$ there is a state p such that for every $\varepsilon \in (0, \bar{\varepsilon}]$ any classical state q with*

$$\mathbf{H}_{\min}(S)_q \geq \mathbf{H}^{\varepsilon,D}_{\min}(S)_p \quad \forall S \in \mathcal{K} \tag{18}$$

satisfies

$$D(p,q) \geq |\mathcal{K}|\varepsilon. \tag{19}$$

Asymptotically, as $\bar{\varepsilon} \to 1/|\mathcal{K}|$, we can choose $N_{\bar{\varepsilon}} = \mathcal{O}((1/|\mathcal{K}| - \bar{\varepsilon})^{-m})$.

The intuition behind the proof of this Theorem is to construct a state p whose min-entropy smoothing operations for any two different subsystems in $\mathcal{K}$ must act on different entries of the associated probability distribution. This is precisely the case when the entries of p that contribute to the peak probabilities of different marginals form disjoint sets on the register of the total system. The proof of Theorem 4.3, hence, consists of the construction of a state p with this disjoint smoothing property.

Before addressing the general case it is instructive to consider two parties first. Let the parties A_1, A_2 have equal dimension, $d_{A_1} = d_{A_2} = 2n^2 + 1$ for $n \in \mathbb{N}$. Define a state p on the register $\{-n^2, \ldots, n^2\}^2$ by the probability distribution

$$p = \begin{pmatrix} & & & \frac{f_{A_2}}{2n^2} & & & \iddots \\ & & & \vdots & & \frac{f_{A_1A_2}}{2n} & \\ & & & \frac{f_{A_2}}{2n^2} & \iddots & & \\ \frac{f_{A_1}}{2n^2} & \cdots & \frac{f_{A_1}}{2n^2} & 0 & \frac{f_1}{2n^2} & \cdots & \frac{f_1}{2n^2} \\ & & \iddots & \frac{f_{A_2}}{2n^2} & & & \\ & \frac{f_{A_1A_2}}{2n} & & \vdots & & & \\ \iddots & & & \frac{f_{A_2}}{2n^2} & & & \end{pmatrix}, \tag{20}$$

where only every n-th entry on the diagonal is occupied by $\frac{f_{A_1A_2}}{2n}$. All blank entries are set to 0. Let $\mathcal{K} \subset \{A_1, A_2, A_1A_2\}$. For $S \in \mathcal{K}$ define $f_S := \frac{1}{|\mathcal{K}|}$, else set $f_S := 0$. Then we make the following claim restating Theorem 4.3 for two parties.

Claim. For every $\bar{\varepsilon} < \frac{1}{|\mathcal{K}|}$ there exists $n_0 \in \mathbb{N}$ so that $\forall n \geq n_0$, $\forall \varepsilon \leq \bar{\varepsilon}$ any classical state q on A_1A_2 with

$$\mathbf{H}_{\min}(S)_q \geq \mathbf{H}^{\varepsilon,D}_{\min}(S)_p \; \forall S \in \mathcal{K} \tag{21}$$

satisfies $D(p, q) \geq |\mathcal{K}|\varepsilon$.

Proof To prove this claim we denote the horizontal non-zero line in (20) by h^{A_1}, the vertical non-zero line by h^{A_2} and the non-zero diagonal by $h^{A_1A_2}$. Computing the marginals to

$$(p_{A_j})_i \begin{cases} = f_{A_j} & \text{if } i = 0 \\ \leq \frac{f_{A_1A_2}}{2n} + \frac{f_{A_{\{1,2\}\setminus\{j\}}}}{2n^2} & \text{else.} \end{cases}$$

We observe that the entries of p_S, $S \in \mathcal{K}$, coming from h^S dominate all others by order n. Hence, for any $\varepsilon < \frac{1}{|\mathcal{K}|}$ there exists an n_0 so that $\forall n \geq n_0$ a probability weight of at least ε has to be removed from h^S in order to smooth p on S. Since the only common entry of the sets $\{h^S\}_{S\in\mathcal{K}}$ has probability 0 the claim follows. □

The construction of p in (20) can be naturally generalized to m parties. The probability distribution p is then defined on the discrete m-cube. The discrete lines h^S are replaced by discrete hyperplanes, each lying orthogonal to the main diagonal of the subspace associated to the subsystem S. The density of non-zero entries on these hyperplanes decreases exponentially in the number of parties in subsystem S. We will in the following define the required geometric entities and then proceed with the proof of Theorem 4.3.

Let $m \in \mathbb{N}$ be an arbitrary number of parties. Let all parties $A_1, \ldots, A_m$ be isomorphic with dimension $d_{A_i} = N = 2n^m + 1$ for $n \in \mathbb{N}$. The state of the system can be represented by a probability distribution p on the cubical register

$$C := \{-n^m, ..., n^m\}^m = (N-1)I^m \cap \mathbb{Z}^m \subset \mathbb{R}^m,$$

where $I := [-\frac{1}{2}, \frac{1}{2}]$. We identify the j-th component of the global state $(i_1, \ldots, i_m)$ with the state of party A_j. For $T \subset \{A_1, \ldots, A_m\}$, $T \neq \emptyset$, define the continuous hyperplane

$$H^T := \left(\sum_{j, A_j \in T} e_j \right)^{\perp} \subset \mathbb{R}^m, \tag{22}$$

where $(e_i)_{1 \leq i \leq m}$ denote the standard basis vectors of $\mathbb{R}^m$ and $(\cdot)^{\perp}$ is the orthogonal complement with respect to the standard inner product. Restricting H^T to the register C, we obtain the discrete hyperplane

$$\begin{aligned} h^T &:= H^T \cap C \\ &= \left\{ (k_1, \ldots, k_m) \in C | \sum_{j, A_j \in T} k_j = 0 \right\}. \end{aligned} \tag{23}$$

We can reduce the density of states on this hyperplane by a factor of $n^{|T|-1}$ by defining

$$\hat{h}^T := \{(k_1, \ldots, k_m) \in h^T | (k_j)_{j, A_j \in T} \subset n\mathbb{Z}^{|T|}\}. \tag{24}$$

This construction can be repeated naturally when a subsystem $S \subset \{A_1, \ldots, A_m\}$, $S \neq \emptyset$, takes over the role of the total system. We denote the register on S by

$$C_S := \{(i_s)_{s, A_s \in S}\} = \{-n^m, \ldots, n^m\}^{|S|} \subset \mathbb{R}^{|S|}. \tag{25}$$

Note that the indexing used for the components of a state $i \in C_S$ is kept the same as in C, that is $i = (i_l)_{l, A_l \in S}$. For $T \subset S$, we can then define the continuous hyperplane

$$(H^T)_S := \left(\sum_{l, A_l \in T} e_l \right)^{\perp} \subset \mathbb{R}^{|S|}$$

in analogy to (22). Restricting it to the register C_S, we obtain the discrete hyperplane

$$(h^T)_S := (H^T)_S \cap C_S \tag{26}$$

as in (23) and finally

$$(\hat{h}^T)_S := \{(k_1, \ldots, k_m) \in (h^T)_S | (k_j)_{j, A_j \in T} \subset n\mathbb{Z}^{|T|}\}. \tag{27}$$

To prove Theorem 4.3 we need the following Lemma on the size of the discrete hyperplanes (23), (24), which by construction transfers to the ones defined in (26), (27).

Lemma 4.4. *Let $T \subset \{A_1, \ldots, A_m\}$, $T \neq \emptyset$. The discrete volume of the hyperplanes h^T (23) and $\hat{h}^T$ (24) is*

$$\begin{aligned} |h^T| &= \delta_{|T|} N^{m-1}(1 + \mathcal{O}(N^{-1})), \\ |\hat{h}^T| &= \hat{\delta}_{|T|} N^{m-1-\frac{|T|-1}{m}}(1 + \mathcal{O}(N^{-(1-\frac{1}{m})})), \end{aligned} \tag{28}$$

in the limit $N \to \infty$ with $\delta_{|T|} \in [\frac{1}{\sqrt{|T|}}, \sqrt{\frac{2}{|T|}}]$, $\hat{\delta}_{|T|} = 2^{-\frac{|T|-1}{m}} \delta_{|T|}$. Especially, both terms in (28) *are bounded from above by N^{m-1}. Moreover, h^T has the largest volume among all discrete hyperplanes in C lying parallel to it.*

Proof From the definition (23) of h^T, (24) of $\hat{h}^T$, it follows that the components $(k_l)_{l, A_l \in T^c}$ of the vector $(k_1, \ldots, k_m)$ can be chosen freely in the set $\{-n^m, \ldots, n^m\}^{|T^c|}$. The remaining ones, $(k_l)_{l, A_l \in T}$, must sum to 0 forming the hyperplane $(h^T)_T$, $(\hat{h}^T)_T$ respectively, on the register C_T. We note that $(\hat{h}^T)_T = (h^T)_T \cap n\mathbb{Z}^{|T|} = (H^T)_T \cap 2n^m I^{|T|} \cap n\mathbb{Z}^{|T|}$ and thus, performing a dilation by $\frac{1}{n}$,

$$|(\hat{h}^T)_T| = |(H^T)_T \cap 2n^{m-1} I^{|T|} \cap \mathbb{Z}^{|T|}|.$$

Hence, the size of $(h^T)_T$, $(\hat{h}^T)_T$, is the same as that of

$$q^T(t) := tQ^T \cap \mathbb{Z}^{|T|},$$

where $Q^T := (H^T)_T \cap 2I^{|T|}$, choosing $t = n^m$, $t = n^{m-1}$ respectively.

We may apply Ehrhart's theorem on integer dilations of integral polytopes[2] to quantify $|q^T(t)|$ for $t \in \mathbb{N}$. For this purpose, we set $m^* := |T|$ and use a linear indexing convention on C_T in this part of the proof. Define a linear map via

$$F : \begin{array}{ll} (H^T)_T & \to \mathbb{R}^{m^*-1} \\ e_k - e_1 & \mapsto e_{k-1} \end{array}$$

which maps $q^T(t)$ bijectively to a subset of the integer lattice $\mathbb{Z}^{m^*-1}$. The image of Q^T under F is an integral polytope in $\mathbb{R}^{m^*-1}$. This can be seen from the fact

[2]The object under consideration in Ehrhart's theorem is a convex d-dimensional integral polytope $Q \subset \mathbb{R}^d$. That is a polytope with vertices on the lattice $\mathbb{Z}^d$. The theorem states that the number of integer points contained in the dilated polytope tQ, where $t \in \mathbb{N}$, is a polynomial of degree d in t,

$$L_Q(t) := |tQ \cap \mathbb{Z}^d| = \sum_{i=0}^{d} c_i t^i.$$

Normalizing $L_Q(t) = |Q \cap \frac{1}{t}\mathbb{Z}^d|$ by t^d and considering the limit $t \to \infty$ we can identify the coefficient c_d to be the d-dimensional volume of Q. This follows from the fact that Q can be arbitrarily well approximated by a finite union of d-cubes of edge length $\frac{1}{t}$ centered at points on the lattice $\frac{1}{t}\mathbb{Z}^d$ that lie in Q. For a more comprehensive introduction to Ehrhart's theory the interested reader may consult [16]

that the vertices of Q^T lie on the edges of the cube $2I^{m^*}$ while their coordinates must sum to 0. By the fact that F is a linear isomorphism, we then find

$$\begin{aligned} |q^T(t)| &= |tQ^T \cap \mathbb{Z}^{m^*}| \\ &\overset{F \text{ bij.}}{=} \left|tF(Q^T) \cap \mathbb{Z}^{m^*-1}\right| \\ &\overset{t\in\mathbb{N}}{=} \operatorname{vol}_{\mathbb{R}^{m^*-1}}(F(Q^T))t^{m^*-1} + \mathcal{O}(t^{m^*-2}), \end{aligned} \tag{29}$$

where we have applied Ehrhart's theorem to the integral polytope $F(Q^T)$. To compute the volume of $F(Q^T)$, note that $\operatorname{vol}_{(H^T)_T}$ is the contraction of $\operatorname{vol}_{\mathbb{R}^{m^*}}$ with the unit outer normal $\nu = \frac{1}{\sqrt{m^*}}(1,\dots,1)$ in terms of linear forms.[3] Pulling this form back under F^{-1}, we obtain

$$(F^{-1})^* \operatorname{vol}_{(H^T)_T} = \det(\nu, F^{-1}(e_1), \dots, F^{-1}(e_{m^*-1}))\operatorname{vol}_{\mathbb{R}^{m^*-1}}$$

with

$$\begin{aligned} \det(\nu, F^{-1}(e_1), \dots, F^{-1}(e_{m^*-1})) &= \det \begin{pmatrix} \frac{1}{\sqrt{m^*}} & -1 & -1 & \cdots & -1 \\ \frac{1}{\sqrt{m^*}} & 1 & 0 & \cdots & 0 \\ \frac{1}{\sqrt{m^*}} & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \frac{1}{\sqrt{m^*}} & 0 & \cdots & 0 & 1 \end{pmatrix} \\ &= \sqrt{m^*}. \end{aligned}$$

Thus, we conclude that

$$\begin{aligned} \operatorname{vol}_{\mathbb{R}^{m^*-1}}(F(Q^T)) &= \frac{1}{\sqrt{m^*}}(F^{-1})^* \operatorname{vol}_{(H^T)_T}(F(Q^T)) \\ &= \frac{1}{\sqrt{m^*}} \operatorname{vol}_{(H^T)_T}(Q^T). \end{aligned}$$

Finally, we note that the volume of a central (m^*-1)-dimensional slice through the unit cube I^{m^*} has been shown to be bounded from below by 1 in [17] and subsequently from above by $\sqrt{2}$ in [18]. [4] Thus, inserting $t = n^m$, $t = n^{m-1}$, in (29) we recover the size of $(h^T)_T$, $(\hat{h}^T)_T$ respectively,

$$\begin{aligned} |(h^T)_T| &= \frac{1}{\sqrt{m^*}} \operatorname{vol}_{(H^T)_T}\left(\frac{1}{2}Q^T\right) N^{m^*-1}(1+\mathcal{O}(N^{-1})), \\ |(\hat{h}^T)_T| &= \frac{1}{2^{\frac{m^*-1}{m}}\sqrt{m^*}} \operatorname{vol}_{(H^T)_T}\left(\frac{1}{2}Q^T\right) N^{m^*-1-\frac{m^*-1}{m}}(1+\mathcal{O}(N^{-(1-\frac{1}{m})})). \end{aligned}$$

and hence (28) follows.

[3] That is $\operatorname{vol}_{(H^T)_T}(v_1,\dots,v_{m^*-1}) := \operatorname{vol}_{\mathbb{R}^{m^*}}(n, v_1, \dots, v_{m^*-1})\ \forall v_1,\dots,v_{m^*-1} \in (H^T)_T$

[4] A summary of these results can be found in the first chapter of [19].

To see that $|(h^T)_T| \leq N^{m^*-1}$ is immediate since the choice of the first m^*-1 components of a state in $(h^T)_T$ completely determines the remaining one as they have to sum to 0.

It remains to prove that h^T maximizes the volume among all discrete hyperplanes in C parallel to it. Parametrizing parallel hyperplanes by

$$h_x^T = \left\{ (k_1, \ldots, k_m) \in C | \sum_{l, A_l \in T} k_l = x \right\},$$

for $x \in \mathbb{Z}$, we can prove that

$$\forall x, y \in \mathbb{Z},\ |x| \leq |y| :\ |h_x^T| \geq |h_y^T|$$

by induction over the number of parties in A. For this purpose, we define discrete hyperplanes on the register of the system $A_1 \cdots A_{m-1}$ by

$$(h_x^{T \setminus A_m})_{A_1 \cdots A_{m-1}} := \{(k_1, \ldots, k_{m-1}) \in C_{A_1 \cdots A_{m-1}} | \sum_{l, A_l \in T} k_l = x\},$$

for $x \in \mathbb{Z}$. The induction step uses that for all $x \in \mathbb{N}_0$,

$$\begin{aligned} |h_x^T| - |h_{x+1}^T| &= \sum_{k_m = -\frac{N-1}{2}}^{\frac{N-1}{2}} |(h_{x-k_m}^{T \setminus A_m})_{A_1 \cdots A_{m-1}}| - \sum_{k_m = -\frac{N-1}{2}}^{\frac{N-1}{2}} |(h_{x+1-k_m}^{T \setminus A_m})_{A_1 \cdots A_{m-1}}| \\ &= |(h_{x-\frac{N-1}{2}}^{T \setminus A_m})_{A_1 \cdots A_{m-1}}| - |(h_{x+1+\frac{N-1}{2}}^{T \setminus A_m})_{A_1 \cdots A_{m-1}}| \overset{\text{ind. hyp.}}{\geq} 0, \end{aligned}$$

and the inversion symmetry of the cube C, $|h_{-x}^T| = |h_x^T|$. □

We are now ready to prove the Theorem.

Proof (of Theorem 4.3) We construct an explicit state p that generalizes (20) with the property that any simultaneous min-entropy smoother q on subsystems $\mathcal{K}$ must satisfy (19). Set $\Omega^S := \hat{h}^S \setminus (\bigcup_{T \in \mathcal{K}, T \neq S} \hat{h}^T)$, define the state

$$p_{i_1 \ldots i_m} = \begin{cases} \frac{f_S}{|\Omega^S|} & \text{if } (i_1, \ldots, i_m) \in \Omega^S \\ 0 & \text{else,} \end{cases} \tag{30}$$

The parameter f_S is a probability weight associated with hyperplane $\hat{h}^S$. As we shall see in the remainder of the proof, to saturate the bound (19) it can be adjusted to any value that is larger than ε provided the dimension N is sufficiently large. In this case, it will always be necessary to remove a probability weight ε from $(\hat{h}^S)_S$ on p_S to achieve the smooth min-entropy of p on subsystem S.

Fix a subsystem $S \in \mathcal{K}$. Let $i = (i_j)_{j, A_j \in S}$ be an element of the register C_S. Denote by

$$G_i := \{(k_1, \ldots, k_m) \in C | k_j = i_j,\ \forall j, A_j \in S\} \subset C$$

the set of states on the total system A that are compatible with i on subsystem S. It is precisely this set that we sum over when computing the marginal $(p_S)_i$.

In the following, we compute the S-marginal of p. Since $G_i \subset \hat{h^S}$ for $i \in (\hat{h}^S)_S$, we have

$$(p_S)_i = \frac{f_S}{|\Omega^S|} \left| G_i \setminus \left(\bigcup_{T \in \mathcal{K}, T \not\subset S} \hat{h}^T \right) \right|, \quad i \in (\Omega^S)_S := (\hat{h}^S)_S \setminus \left(\bigcup_{T \in \mathcal{K}, T \subsetneq S} (\hat{h}^T)_S \right). \tag{31}$$

First, we observe that

$$|\Omega^S| \leq |\hat{h}^S| \tag{32}$$

and bound

$$\begin{aligned} |G_i \cap \hat{h}^T| &= \left| \left\{ (k_1, \ldots, k_m) \in G_i | \sum_{l, A_l \in T \setminus S} k_l = - \sum_{l, A_l \in T \cap S} i_l, \, (k_l)_{l, A_l \in T} \in n\mathbb{Z}^{|T|} \right\} \right| \\ &\leq |(h^{T \setminus S})_{S^c}| \leq N^{|S^c|-1}, \; T \not\subset S. \end{aligned} \tag{33}$$

To see this, note that the components $(k_l)_{l, A_l \in S}$ are fixed by G_i. The remaining ones, $(k_l)_{l, A_l \in S^c}$, together with the condition $\sum_{l, A_l \in T \setminus S} k_l = - \sum_{l, A_l \in T \cap S} i_l$ form a subset of a hyperplane on C_{S^c} parallel to $(h^{T \setminus S})_{S^c}$ and hence the second line follows from Lemma 4.4.

We conclude that

$$\begin{aligned} \left| G_i \setminus \left(\bigcup_{T \in \mathcal{K}, T \not\subset S} \hat{h}^T \right) \right| &\geq \underbrace{|G_i|}_{= N^{|S^c|}} - \sum_{T \in \mathcal{K}, T \not\subset S} \underbrace{|G_i \cap \hat{h}^T|}_{\leq N^{|S^c|-1}} \\ &\geq N^{|S^c|}(1 - \mathcal{O}(N^{-1})) \end{aligned} \tag{34}$$

using (33) to obtain the second line. We can now lower bound p_S on $(\Omega^S)_S$ by

$$(p_S)_i \geq \frac{f_S}{|(\hat{h}^S)_S|}(1 - \mathcal{O}(N^{-1})), \quad i \in (\Omega^S)_S \tag{35}$$

using the fact that $|\hat{h}^S| = N^{|S^c|}|(\hat{h}^S)_S|$.

For subsystems $T \subsetneq S$ we find

$$(p_S)_i \leq \frac{f_T}{|\Omega^T|}|G_i|, \quad i \in (\hat{h}^T)_S. \tag{36}$$

To obtain an upper bound on these probabilities, we note that

$$\begin{aligned} |\Omega^T| &\geq |\hat{h}^T| - \sum_{U \in \mathcal{K}, U \neq T} \underbrace{|\hat{h}^T \cap \hat{h}^U|}_{\leq |(\hat{h}^T)_T||(\hat{h}^{U \setminus T})_{T^c}|} \\ &\geq |\hat{h}^T|(1 - \mathcal{O}(N^{-1})), \end{aligned} \tag{37}$$

where Lemma 4.4 was used in the last step. We therefore find

$$\begin{aligned}(p_S)_i &\leq \frac{f_T}{|(\hat{h}^T)_S|}(1+\mathcal{O}(N^{-1})) \\ &= \frac{f_T}{|(\hat{h}^S)_S|}\frac{\hat{\delta}_{|S|}}{\hat{\delta}_{|T|}}\frac{1}{N^{\frac{|S|-|T|}{m}}}(1+\mathcal{O}(N^{-(1-\frac{1}{m})})) \\ &= \frac{1}{|(\hat{h}^S)_S|}\mathcal{O}(N^{-\frac{1}{m}}), \quad i \in (\hat{h}^T)_S\end{aligned} \tag{38}$$

for $T \subsetneq S$ expanding by $|(\hat{h}^S)_S|$ and using Lemma 4.4 to obtain the last line.

To bound p_S on all states on C_S lying outside of the hyperplanes $\{(\hat{h}^T)_S\}_{T\in\mathcal{K},T\subset S}$, we find

$$\begin{aligned}(p_S)_i &\leq \sum_{T\in\mathcal{K},T\not\subseteq S} \frac{f_T}{\underbrace{|\Omega^T|}_{\overset{(37)}{\leq}|\hat{h}^T|(1+\mathcal{O}(N^{-1}))}} \overbrace{|G_i \cap \hat{h}^T|}^{\overset{(33)}{\leq} N^{|S^c|-1}} \\ &\overset{(28)}{\leq} \sum_{T\in\mathcal{K},T\not\subseteq S} \frac{f_T}{\hat{\delta}_{|T|}} \frac{N^{|S^c|-1}}{N^{m-1-\frac{|T|-1}{m}}}(1+\mathcal{O}(N^{-(1-\frac{1}{m})})) \\ &\leq |\mathcal{K}| \max_{T\in\mathcal{K},T\not\subseteq S} \frac{f_T}{\hat{\delta}_{|T|}} \frac{\hat{\delta}_{|S|}}{|(\hat{h}^S)_S|} \frac{1}{N^{1-\frac{|T|-|S|}{m}}}(1+\mathcal{O}(N^{-(1-\frac{1}{m})})) \\ &= \frac{1}{|(\hat{h}^S)_S|}\mathcal{O}(N^{-\frac{1}{m}})\end{aligned} \tag{39}$$

again expanding by $|(\hat{h}^S)_S|$ and using Lemma 4.4 in the last step. Thus, if ε is such that

$$\varepsilon \overset{!}{<} \left(\min_{i\in(\Omega^S)_S}(p_S)_i - \max_{i\notin(\Omega^S)_S}(p_S)_i\right)|(\Omega^S)_S|, \tag{40}$$

a probability amount ε has to be removed from Ω^S in p in order to achieve the smooth min-entropy on S. Analogous to (37), one obtains

$$|(\Omega^S)_S| \geq |(\hat{h}^S)_S|(1-\mathcal{O}(N^{-(1-\frac{1}{m})})) \tag{41}$$

Hence, putting together the previous expressions (35), (38) and (39) with the last equation, the right hand side of (40) is lower bounded by $f_S - \mathcal{O}(N^{-\frac{1}{m}})$. Therefore, if $\varepsilon < \min_{S\in\mathcal{K}} f_S$ inequality (40) is satisfied if N is sufficiently large and hence for every $S \in \mathcal{K}$ a probability weight ε has to be removed from $\hat{h}^S$ in p to achieve the smooth min-entropy. Choosing $f_S := \frac{1}{|\mathcal{K}|}$, $S \in \mathcal{K}$, $f_S = 0$ else, proves optimality of the bound (19).

From the condition $\varepsilon \overset{!}{<} f_S - \mathcal{O}(N^{-\frac{1}{m}})$ we conclude that to satisfy (19) for p with $f_S = 1/|\mathcal{K}|$ in the limit $\varepsilon \to 1/|\mathcal{K}|$ the dimension of the parties $d_{A_i} = N$ can be taken as

$$N = \mathcal{O}((1/|\mathcal{K}| - \varepsilon)^{-m}).$$

Hence, the lower bound $N_{\bar{\varepsilon}}$ in the Theorem can be chosen to grow only polynomially in the inverse difference $1/|\mathcal{K}| - \bar{\varepsilon}$ as $\bar{\varepsilon}$ tends to $1/|\mathcal{K}|$.

□

The proof of Theorem 4.3 demonstrates that the if the smoothing parameters are not the same, e.g. we have a collection $\{\varepsilon_S\}_{S\in\mathcal{K}}$, $\sum_{S\in\mathcal{K}} \varepsilon_S = 1 - \delta < 1$, the distance bound (19) still holds in the altered form

$$D(p, q) \geq \sum_{S\in\mathcal{K}} \varepsilon_S.$$

Set $f_S = \varepsilon_S + \frac{\delta}{|\mathcal{K}|}$ in the definition of p for an example. Note that the probability weights $\{f_S\}_{S\in\mathcal{K}}$ do not have to be equal either in order to saturate the bound (19). In fact, the distribution p may even be varied further, e.g. by choosing it non-uniform on $\hat{h}^S$, without to lose the disjoint smoothing property. To obtain this property in this case with our proof techniques, the only condition on p is that all entries of p_S on $(\Omega^S)_S$ (up to such that can asymptotically form an impossible event) must fall off faster than $N^{\frac{1}{2m}}/|(\hat{h}^S)_S|$ but slower than $N^{-\frac{1}{2m}}/|(\hat{h}^S)_S|$ as $N \to \infty$.

The fidelity of any simultaneous $\mathbf{H}_{\min}$-smoother q to p (defined as in the proof of Theorem 4.3 with $f_S = 0$ for $S \notin \mathcal{K}$) such that $\mathbf{H}_{\min}(S)_q \geq \mathbf{H}^{\varepsilon,P}_{\min}(S)_p$ must satisfy

$$\begin{aligned} F(p, q) &\leq \sum_{S\in\mathcal{K}} \cos(\theta_S)\cos(\theta_S + \phi) \\ &= 1 - \sum_{S\in\mathcal{K}} \cos(\theta_S)\sin(\theta_S)\varepsilon + \mathcal{O}(\varepsilon^2) \end{aligned}$$

in the limit ($\varepsilon \to 0$), where $\theta_S = \arccos(\sqrt{f_S})$, $\phi = \arcsin(\varepsilon)$. Thus,

$$\begin{aligned} P(p, q) &\geq \sqrt{2\sum_{S\in\mathcal{K}} \cos(\theta_S)\sin(\theta_S)\varepsilon} + \mathcal{O}(\varepsilon) \\ &= \sqrt{\sum_{S\in\mathcal{K}} \sqrt{f_S}\sqrt{1 - f_S}2\varepsilon} + \mathcal{O}(\varepsilon) \end{aligned}$$

where the leading term is maximized by the uniform distribtion $f_S = \frac{1}{|\mathcal{K}|}$, $S \in \mathcal{K}$, yielding

$$P(p, q) = \sqrt[4]{|\mathcal{K}| - 1}\sqrt{2\varepsilon} + \mathcal{O}(\varepsilon).$$

5 General quantum case

We now consider conjecture 3.1 in the general quantum setting. We present a proof for the case of two parties using an iterative smoothing technique according to a particular ordering of the subsystems. A generalization of this argument to a restricted case for more parties is then made, where the subsystems to smooth do not mutually overlap. This is then used to prove conjecture 3.1 for three parties in a pure state. We subsequently proceed with an analysis of the simplest case where our techniques fail. That is a three party system in a mixed state. Given these limits, we subsequently pursue a non-iterative approach based on minimization in the positive semi-definite cone to prove conjecture 3.1. We rederive the result in the classical case and point out the shortcomings of this technique in the general quantum case.

Throughout this chapter we will use the following basic invariance property of the purified distance.

Lemma 5.1. *Let* $S \in 2^{\{A_1,\ldots,A_m\}} \setminus \{\emptyset\}$. *If* $\tau \in \mathcal{S}_{\leq}(A)$, $\Pi^S \in \mathcal{P}(S)$, $\Pi^S \leq \mathbb{1}_S$, *are such that* $[\Pi^S, \tau_S] = 0$, *then*

$$P(\tau, \Pi^S \tau \Pi^S) = P(\tau_S, \Pi^S \tau_S \Pi^S). \tag{42}$$

Proof The inequality "$\geq$" follows by the monotonicity property of the purified distance (2) under the TPCPM tr_{S^c}. To derive the other inequality we use Uhlmann's Theorem for the fidelity [14]. Let $|\psi\rangle \in AR$ be a purification of τ, then

$$\begin{aligned} \|\sqrt{\tau}\sqrt{\Pi^S \tau \Pi^S}\|_1 &\geq \langle\psi| \Pi^S |\psi\rangle \\ &= \mathrm{tr}(\Pi^S \tau_S) \\ &\overset{[\Pi^S,\tau_S]=0}{=} \|\sqrt{\tau_S}\sqrt{\Pi^S \tau_S \Pi^S}\|_1 \end{aligned}$$

where in the first line it was used that $\Pi^S |\psi\rangle$ is a purification of $\Pi^S \tau \Pi^S$. As $\mathrm{tr}(\Pi^S \tau \Pi^S) = \mathrm{tr}(\Pi^S \tau_S \Pi^S)$ and $\mathrm{tr}(\tau) = \mathrm{tr}(\tau_S)$ we conclude

$$F(\tau, \Pi^S \tau \Pi^S) = F(\tau_S, \Pi^S \tau_S \Pi^S).$$

□

This Lemma is a manifestation of a more general fact stated in Corollary 3.6 in [13]. That is, there always exists an isometric extension of a given state on a subsystem relative to a reference state defined on the total system if we work in the purified distance. Lemma 5.1 gives a concrete formula for this extension for special cases. Note that one can in general not replace the operator product $\Pi^S \cdot \Pi^S$ in (42) by an incomplete measurement of the form $\mathcal{E}_S(\cdot) := \sum_x P_x^S \cdot P_x^S$, $P_x^S \in \mathcal{P}(S)$, that has the same effect on τ_S and satisfies $\Pi^S = \sum_x P_x^S$. To see this, observe that

for a pure state $\psi \in A$,

$$\begin{aligned} F(\psi, \mathcal{E}_S(\psi)) &= \sqrt{\sum_x \langle\psi| P_x^S |\psi\rangle^2} \\ &\leq \sqrt{\langle\psi| \sum_x P_x^S |\psi\rangle^2} \\ &= \langle\psi| \Pi^S |\psi\rangle = F(\psi_S, \mathcal{E}_S(\psi_S)). \end{aligned}$$

The inequality in the second line becomes strict as soon as there exist more than one operator P_x^S that have non-zero overlap with ψ, $\langle\psi| P_x^S |\psi\rangle > 0$. In the case where only one operator P_x^S has non-zero overlap with ψ the considered measurement $\mathcal{E}_S(\cdot)$ is equivalent to the operator product $\Pi^S \cdot \Pi^S$. We conclude that the outcome of an incomplete measurement $\mathcal{E}_S$ of a state τ on a subsystem in general is not an isometric extension of the measurement outcome on that subsystem, $\mathcal{E}_S(\tau_S)$, relative to τ.

As a consequence, to obtain an explicit extension of the min-entropy smoother σ on a subsystem $S \subsetneq A$ for a given state $\rho \in S_{\leq}(A)$,

$$\mathbf{H}_{\min}(S)_\sigma = \mathbf{H}_{\min}^{\varepsilon,D}(S)_\rho$$

we are forced to write it in the form $\sigma = \Pi^S \rho \Pi^S$. Replacing $\Pi^S \cdot \Pi^S$ by an incomplete measurement with respect to an eigenbasis of ρ_S with the same effect on ρ_S will in general perturb the state ρ too much. The reader interested in an example may consider a maximally entangled state on a bipartite system A_1A_2, $\Pi^{A_1} = \mathbb{1}_{A_1}$ and $\mathcal{E}_{A_1}$ a measurement in the A_1-part of the Schmidt basis of ψ. The outcome $\mathcal{E}_{A_1}(\psi)$ under this measurement is a maximally correlated classical state with $P(\psi, \mathcal{E}_{A_1}(\psi)) = \sqrt{1 - \frac{1}{d_{A_1}}}$.

Finally, note that the trace-distance exhibits a property that is similar to Lemma 5.1 stated in (13). However, it requires the commutation relation $[\Pi^S, \tau] = 0$ to hold on the total system A while the assumptions in Lemma 5.1 only impose a condition on subsystem S.

5.1 Iterative min-entropy smoothing

In this section we show how conjecture 3.1 can be proved for two parties by iteratively smoothing the min-entropy over all subsystems. The techniques admit a natural generalization to the setting with more parties solving a restricted form of conjecture 3.1 in this case. This result can be used to conclude conjecture 3.1 for a three party system in a pure state. Finally, we analyze the simplest case where the iterative approach fails to provide a simultaneous min-entropy smoother, which is the three party system in a mixed state.

5.1.1 Two parties

In this section we give proof for conjecture 3.1 in the case of two parties consisting of quantum systems A_1 and A_2. We note that the multiparty typicality conjecture, which is the special case when ρ is a tensor power state, was proved in [2] and subsequently in [3] for two parties. We provide here a proof in the more general one-shot setting which is hopefully more transparent.

Theorem 5.2 (Quantum case of conjecture 3.1 for two parties)**.** *Let $\rho \in \mathcal{S}_{\leq}(A_1A_2)$, $\varepsilon > 0$. There exists $\sigma \in \mathcal{S}_{\leq}(A_1A_2)$ such that*

$$\begin{aligned} \mathbf{H}_{\min}(S)_\sigma &\geq \mathbf{H}^{\varepsilon}_{\min}(S)_\rho \text{ for all } S \in \{A_1, A_2, A_1A_2\}, && (43)\\ P(\rho,\sigma) &\leq 3\sqrt{2\varepsilon}. && (44) \end{aligned}$$

Before starting with the proof, we make the following basic observation

Lemma 5.3. *Let $\rho \in \mathcal{S}_{\leq}(A_1A_2)$, $\mathcal{E}_{A_2\to A_2}$ be a quantum evolution on A_2. Then, $(\mathcal{I}_{A_1} \otimes \mathcal{E}_{A_2\to A_2}(\rho))_{A_1} \leq \rho_{A_1}$.*

This Lemma is simply proved by considering an operator-sum representation, $\mathcal{E}_{A_2}(\cdot) = \sum_k E_k \cdot E_k^\dagger$ with $P_{A_2} = \sum_k E_k^\dagger E_k \leq \mathbb{1}_{A_2}$,

$$\begin{aligned} \rho_{A_1} - (\mathcal{E}_{A_2}(\rho))_{A_1} &= ((\mathbb{1}_{A_2} - P_{A_2})\rho)_{A_1} \\ &= (\sqrt{\mathbb{1}_{A_2} - P_{A_2}}\rho\sqrt{\mathbb{1}_{A_2} - P_{A_2}})_{A_1} \geq 0, \end{aligned}$$

where we used the cyclicity of the partial trace in operators acting only on the system being traced out. We are now ready for the proof of Theorem 5.2.

Proof We start by defining σ. Define $\Pi^S \in \mathcal{P}(S)$, $\Pi^S \leq \mathbb{1}_S$ for $S \in \{A_1, A_2, A_1A_2\}$ such that in the order listed

$$\begin{aligned} \mathbf{H}_{\min}(A_1A_2)_{\Pi^{A_1A_2}\sigma^{A_1A_2}\Pi^{A_1A_2}} &= \mathbf{H}^{\varepsilon,D}_{\min}(A_1A_2)_{\sigma^{A_1A_2}}, && (45)\\ \mathbf{H}_{\min}(A_2)_{\Pi^{A_2}\sigma^{A_2}\Pi^{A_2}} &= \mathbf{H}^{\varepsilon,D}_{\min}(A_2)_{\sigma^{A_2}}, && (46)\\ \mathbf{H}_{\min}(A_1)_{\Pi^{A_1}\sigma^{A_1}\Pi^{A_1}} &= \mathbf{H}^{\varepsilon,D}_{\min}(A_1)_{\sigma^{A_1}}, && (47)\\ D((\sigma^S)_S, \Pi^S(\sigma^S)_S\Pi^S) &\leq \varepsilon \;\forall S \in \{A_1, A_2, A_1A_2\} && (48) \end{aligned}$$

where we abbreviated $\sigma^{A_1A_2} := \rho$, $\sigma^{A_2} := \Pi^{A_1A_2}\sigma^{A_1A_2}\Pi^{A_1A_2}$ and $\sigma^{A_1} := \Pi^{A_2}\sigma^{A_2}\Pi^{A_2}$ and finally $\sigma := \Pi^{A_1}\sigma^{A_1}\Pi^{A_1}$. Note that the superscript does not refer to the system on which the operator acts, it is just a label to keep track which Π^S is to be applied next. In particular, we have $\sigma^S \in \mathcal{S}_{\leq}(A_1A_2)$ for all $S \in \{A_1, A_2, A_1A_2\}$. Also, we used smoothing with respect to the trace distance to assume that the optimizers have the form $\Pi\rho\Pi$ with $\Pi \leq \mathbb{1}$ positive, but note that we have $\mathbf{H}^{\varepsilon,D}_{\min} \geq \mathbf{H}^{\varepsilon}_{\min}$.

Now, let us show the min-entropy smoothing property (43). On the total system A_1A_2, this follows using submultiplicativity of $\|\cdot\|_\infty$,

$$\begin{aligned} \|\sigma\|_\infty &= \|\Pi^{A_1} \otimes \Pi^{A_2}\sigma^{A_2}\Pi^{A_1} \otimes \Pi^{A_2}\|_\infty \\ &\leq \|\Pi^{A_1} \otimes \Pi^{A_2}\|_\infty\|\sigma^{A_2}\|_\infty\|\Pi^{A_1} \otimes \Pi^{A_2}\|_\infty \qquad (49)\\ &\leq \|\sigma^{A_2}\|_\infty, \end{aligned}$$

since $\Pi^{A_1} \leq \mathbb{1}_{A_1}$, $\Pi^{A_2} \leq \mathbb{1}_{A_2}$. On subsystem A_2, by Lemma 5.3, we have $(\Pi^{A_1}\sigma^{A_2}\Pi^{A_1})_{A_2} \leq (\sigma^{A_2})_{A_2}$. We infer

$$\begin{aligned}\sigma_{A_2} &= \Pi^{A_2}\,\mathrm{tr}_{A_1}(\Pi^{A_1}\sigma^{A_2}\Pi^{A_1})\Pi^{A_2} \\ &\leq \Pi^{A_2}(\sigma^{A_2})_{A_2}\Pi^{A_2}.\end{aligned} \tag{50}$$

Applying Lemma 2.2 on the monotonicity of the smooth min-entropy we find

$$\begin{aligned}\mathbf{H}_{\min}(A_2)_\sigma &\geq \mathbf{H}_{\min}(A_2)_{\Pi^{A_2}\sigma^{A_2}\Pi^{A_2}} \\ &= \mathbf{H}_{\min}^{\varepsilon,D}(A_2)_{\sigma_2^A} \\ &\geq \mathbf{H}_{\min}^{\varepsilon,D}(A_2)_\rho\end{aligned} \tag{51}$$

where the second line follows by definition of Π^{A_2} in (46) and the third line from $\sigma^{A_2} \leq \rho$. For subsystem A_1, observe that by Lemma 5.3 it follows that

$$(\sigma^{A_2})_{A_1} \geq \mathrm{tr}_{A_2}(\Pi^{A_2}\sigma^{A_2}\Pi^{A_2}).$$

The right hand side of this expression equals $(\sigma^{A_1})_{A_1}$ by (47) so that by definition of σ and Lemma 2.2 we find

$$\begin{aligned}\mathbf{H}_{\min}(A_1)_\sigma &= \mathbf{H}_{\min}^{\varepsilon,D}(A_1)_{\sigma^{A_1}} \\ &\geq \mathbf{H}_{\min}^{\varepsilon,D}(A_1)_{\sigma^{A_2}} \\ &\geq \mathbf{H}_{\min}^{\varepsilon,D}(A_1)_\rho\end{aligned}$$

using $\sigma_{A_2} \leq \rho$ again in the last step. This concludes the proof of the min-entropy smoothing properties of σ.

To compute the distance $P(\rho,\sigma)$, we use the triangle inequality

$$\begin{aligned}P(\rho,\sigma) \leq\ & P(\sigma^{A_1A_2}, \Pi^{A_1A_2}\sigma^{A_1A_2}\Pi^{A_1A_2}) \\ &+ P(\sigma^{A_2}, \Pi^{A_2}\sigma^{A_2}\Pi^{A_2}) \\ &+ P(\sigma^{A_1}, \Pi^{A_1}\sigma^{A_1}\Pi^{A_1}).\end{aligned} \tag{52}$$

By the fact that $\Pi^S\sigma^S\Pi^S$ by Lemma 5.1 are isometric extensions of their reduced states on subsystem S relative to σ^S for both $S = A_1$ and A_2 the second and third term on the right hand side of (52) can be re-expressed such that

$$\begin{aligned}P(\rho,\sigma) \leq\ & P(\sigma^{A_1A_2}, \Pi^{A_1A_2}\sigma^{A_1A_2}\Pi^{A_1A_2}) \\ &+ P((\sigma^{A_2})_{A_2}, \Pi^{A_2}(\sigma^{A_2})_{A_2}\Pi^{A_2}) \\ &+ P((\sigma^{A_1})_{A_1}, \Pi^{A_1}(\sigma^{A_1})_{A_1}\Pi^{A_1}) \leq 3\sqrt{2\varepsilon}\end{aligned}$$

where the last inequality follows from the relation (1) and (48). □

We emphasize that in contrast to the proof of Corollary 4.2 this proof does not construct a min-entropy smoother σ close to ρ that fulfills $\sigma \leq \rho$. Note

that we found in chapter 4 that such a state σ can in general lie far off from ρ if ρ is pure. Instead of imposing an operator inequality on σ, it is obtained by iteratively smoothing ρ on all subsystems according to a particular order. The order has to respect the inclusion among subsystems since otherwise we could not have applied the submultiplicativity argument (49) to show that the min-entropy smoothing on one-party subsystems does not reduce the min-entropy of the total system. Furthermore, to show that the smoothing of other subsystems does not decrease the min-entropy on a fixed one-party system, we used that two subsystems are either disjoint or fully contained in one or the other. As we shall see in the following section, the argument presented in the proof of Theorem 5.2 can be naturally generalized to more parties.

5.1.2 Non-overlapping subsystems

We apply the technique of iterative smoothing from the proof of Theorem 5.2 to prove a restricted form of conjecture 3.1 in case of an m-party system $A = A_1 \cdots A_m$ where the subsystems $\mathcal{K}$ under consideration do not mutually overlap.

Theorem 5.4 (Quantum case of conjecture 3.1 for non-overlapping subsystems)**.** *Let $\rho \in \mathcal{S}_{\leq}(A)$, $\varepsilon > 0$. Let $\mathcal{K} \subset 2^{\{A_1,\ldots,A_m\}} \setminus \{\emptyset\}$ be such that*

$$\forall S, T \in \mathcal{K} : (S \subset T) \vee (T \subset S) \vee (S \cap T = \emptyset) \tag{53}$$

There exists a state σ that satisfies

$$\begin{aligned} \mathbf{H}_{\min}(S)_\sigma &\geq \mathbf{H}_{\min}^{\varepsilon,D}(S)_\rho \; \forall S \in \mathcal{K}, \\ P(\rho,\sigma) &\leq |\mathcal{K}|\sqrt{2\varepsilon}. \end{aligned} \tag{54}$$

Proof Let $(S^i)_{i\in\{1,\ldots,|\mathcal{K}|\}}$ be an ordering of $\mathcal{K}$ that respects the inclusion, $S^i \not\supset S^j$ for all $1 \leq i < j \leq |\mathcal{K}|$. Define $\Pi^{S^j} \in \mathcal{P}(S)$, $\Pi^{S^j} \leq \mathbb{1}_S$ iteratively in decreasing order in $j = |\mathcal{K}|, |\mathcal{K}|-1, \ldots, 1$ such that

$$\mathbf{H}_{\min}(S^j)_{\Pi^{S^j}\sigma^{S^j}\Pi^{S^j}} = \mathbf{H}_{\min}^{\varepsilon,D}(S^j)_{\sigma^{S^j}}, \tag{55}$$

$$D(\sigma^{S^j}, \Pi^{S^j}\sigma^{S^j}\Pi^{S^j}) \leq \varepsilon, \tag{56}$$

holds, where $\sigma^{S^j} := (\prod_{i=j+1}^{|\mathcal{K}|}\Pi^{S^i})\rho(\prod_{i=j+1}^{|\mathcal{K}|}\Pi^{S^i})^\dagger$ for all $1 \leq j \leq |\mathcal{K}|-1$, $\sigma^{S^{|\mathcal{K}|}} = \rho$.

First, we shall prove property (54) of σ for a fixed subsystem $S^j \in \mathcal{K}$. Note that all S^i, $1 \leq i < j$, are either subsystems of S^j or do not intersect S^j. In the first case, we apply the submultiplicativity property of $\|\cdot\|_\infty$ as in (49) to show that the corresponding Π^{S^i} do not increase the largest eigenvalue of $((\prod_{1\leq i<j, S^i\not\subset S^j}\Pi^{S^i})\sigma^{S^j}(\prod_{1\leq i<j, S^i\not\subset S^j}\Pi^{S^i})^\dagger)_{S^j}$. In the second case, we use Lemma 5.3 to deduce that the quantum operation $\tau \mapsto \Pi^{S^i}\tau\Pi^{S^i}$ can only decrease a state $\tau \in \mathcal{S}_{\leq}(A)$ on S^j for all $1 \leq i < j$ with $S^i \not\subset S^j$.

It remains to show $(\sigma^{S^j})_{S^j} \leq \rho_{S^j}$ in order to apply Lemma 2.2 on the monotonicity of the smooth min-entropy. For this purpose choose the subsequence $(S^{i_l})_{1\leq l\leq L}$ of all subsystems in $(S^i)_{i\in\{j,\ldots,|\mathcal{K}|\}}$ that contain S^j (preserving the order of the sequence). We can then show the inequality $(\sigma^{S^{i_l}})_{S^{i_l}} \leq \rho_{S^{i_l}}$ by induction over l, establishing $(\sigma^{S^{i_l}})_{S^{i_l}} \leq (\sigma^{S^{i_{l+1}}})_{S^{i_l}}$ for all $1 \leq l \leq L-1$ in the induction step. Since all subsystems S^i, $i_l < i < i_{l+1}$, are disjoint with S^{i_l}, we can apply Lemma 5.3 to obtain $(\sigma^{S^{i_l}})_{S^{i_l}} \leq (\Pi^{S^{i_{l+1}}}\sigma^{S^{i_{l+1}}}\Pi^{S^{i_{l+1}}})_{S^{i_l}}$. Chaining this with the well-known inequality $\Pi^{S^{i_{l+1}}}(\sigma^{S^{i_{l+1}}})_{S^{i_{l+1}}}\Pi^{S^{i_{l+1}}} \leq (\sigma^{S^{i_{l+1}}})_{S^{i_{l+1}}}$ reduced to subsystem S^{i_l} proves the induction step. The base step involves proving $(\sigma^{S^{i_L}})_{S^{i_L}} \leq \rho_{S^{i_L}}$ which is either a trivial statement or again follows by Lemma 5.3 applied on S^{i_L}. Thus by an application of Lemma 2.2 we find that $\mathbf{H}_{\min}^{\varepsilon,D}(S^j)_\rho \leq \mathbf{H}_{\min}(S^j)_{\Pi^{S^j}\sigma^{S^j}\Pi^{S^j}} \leq \mathbf{H}_{\min}(S^j)_\sigma$ where we have included the results from the first paragraph in the last inequality.

The proof of the distance estimate (54) is analogous to the two party case, again making use of the fact that $\Pi^S\sigma^S\Pi^S$ is an isometric extension of its S-marginal relative to σ^S by Lemma 5.1.

$$\begin{aligned} P(\rho,\sigma) &\leq \sum_{S\in\mathcal{K}} P(\sigma^S, \Pi^S\sigma^S\Pi^S) \\ &= \sum_{S\in\mathcal{K}} P((\sigma^S)_S, \Pi^S(\sigma^S)_S\Pi^S) \\ &\leq |\mathcal{K}|\sqrt{2\varepsilon} \end{aligned}$$

□

Since the iterative smoothing procedure as presented in the above proof is rank non-increasing, that is $\operatorname{rank}\sigma \leq \operatorname{rank}\rho$, the statement of Theorem 5.4 can be slightly generalized for pure states. As a consequence, conjecture 3.1 is satisfied on a three party system if its state is pure. Moreover, the distance estimate (54) can be improved in certain cases. To formulate these results in the following Corollary, we introduce an equivalence relation on the set $2^{\{A_1,\ldots,A_m\}} \setminus \{\emptyset\}$ of subsystems of A via

$$\mathcal{K} \sim \mathcal{K}' \Leftrightarrow \forall S \in \mathcal{K} : S \in \mathcal{K}' \vee S^c \in \mathcal{K}'.$$

Corollary 5.5. *Let $\rho \in \mathcal{S}_\leq(A)$ be pure, $\varepsilon > 0$ and $\mathcal{K} \subset 2^{\{A_1,\ldots,A_m\}} \setminus \{\emptyset\}$. If there exists $\mathcal{K}' \sim \mathcal{K}$ that is non-overlapping (53), then there is a pure state σ that satisfies*

$$\mathbf{H}_{\min}(S)_\sigma \geq \mathbf{H}_{\min}^{\varepsilon,D}(S)_\rho \; \forall S \in \mathcal{K} \cup \{T^c | T \in \mathcal{K}\}, \tag{57}$$

$$P(\rho,\sigma) \leq |\mathcal{K}'|\sqrt{2\varepsilon}. \tag{58}$$

Proof Construct σ as in the proof of Theorem 5.4 applied to $\mathcal{K}'$ instead of $\mathcal{K}$. Observe that σ is pure. Then, by the Schmidt decomposition the eigenvalues of

σ_S, σ_{S^c} as well as ρ_S, ρ_{S^c} for $S \in \mathcal{K}$ are identical (with equal multiplicity) which implies

$$\mathbf{H}_{\min}(S^c)_\sigma = \mathbf{H}_{\min}(S)_\sigma \geq \mathbf{H}^{\varepsilon,D}_{\min}(S)_\rho = \mathbf{H}^{\varepsilon,D}_{\min}(S^c)_\rho$$

□

5.1.3 The three-party case

We shall now analyze the simplest case where the iterative smoothing approach fails. In the previous section we found that conjecture 3.1 is satisfied for a three party system if its state is pure. It is, however, unknown, whether a similar result holds for mixed states on a three-party system. Note that similarly we had shown in Corollary 4.2 that conjecture 3.1 is satisfied if all parties are independent, but could not deduce the statement for arbitrary separable states.

To see why our proof techniques fail in the case of three parties and for the sake of completeness, we shall here present another, more elementary proof of theorem 5.4 using a purification point of view. As a side-effect this proof shows that the iterative definition of the smoothing from the proof of Theorem 5.4 can be relaxed in favour of the iterative application of the smoothing defined for the initial state ρ of the system.

To start, note that conjecture 3.1 can equivalently be restated in terms of pure states if one adds a purifying system R to A. Let $\psi \in AR$ thus be a purification of $\rho \in \mathcal{S}_\leq(A)$, let $\varepsilon > 0$. For a non-overlapping collection $\mathcal{K} \subset 2^{\{A_1,\ldots,A_m\}} \setminus \{\emptyset\}$ we define the set of operators $\{\Pi^S\}_{S\in\mathcal{K}}$ such that

$$\begin{aligned} \mathbf{H}_{\min}(S)_{\Pi^S\psi} &= \mathbf{H}^{\varepsilon,D}_{\min}(S)_\psi & (59)\\ D((\Pi^S\psi)_S, \psi_S) &\leq \varepsilon. & (60)\end{aligned}$$

Next, we pick an arbitrary ordering $(S^i)_{1\leq i\leq|\mathcal{K}|}$ of the set $\mathcal{K}$ that respects the inclusion, $S^i \not\supset S^j$ if $i < j$. Then the state

$$\phi = \left(\prod_{i=1}^{|\mathcal{K}|} \Pi^{S^i}\right)\psi \tag{61}$$

is claimed to satisfy (54). To see this, observe that the Schmidt decomposition $|\psi\rangle = \sum_i \sqrt{\lambda_i}\,|i\rangle_S \otimes |i\rangle_{AR\setminus S}$ induces a unitary $G = \sum_i |i\rangle_{AR\setminus S}\langle i|_S$ between the supports of ψ_S and $\psi_{AR\setminus S}$ for every $S \subset A$. Since Π^S is diagonal in the eigenbasis $\{|i\rangle_S\}_i$ of ψ_S we may act on ψ equivalently by $\tilde{\Pi}^S := G \circ \Pi^S \circ G^{-1} = \Pi^{AR\setminus S} \in \mathcal{P}(AR \setminus S)$ to obtain the same result,

$$\Pi^S\psi = \tilde{\Pi}^S\psi.$$

The crucial difference here is that $\tilde{\Pi}^S$ only acts on the complementary system of S in AR. This turns out to be very useful in proving the min-entropy smoothing

property of ϕ on a fixed subsystem S^i. Precisely, we iteratively replace all operators Π^{S^j}, $S^i \subset S^j$ by $\tilde{\Pi}^{S^j}$ in decreasing order in j. For this purpose, let $(j_l)_{1\leq l\leq L} \subset \{i+1,\ldots,|\mathcal{K}|\}$ be the increasing sequence that enumerates all subsystems containing S^i. Note that we have the ordering $S^{j_1} \subset \cdots \subset S^{j_L}$ by the non-overlapping condition (53). We then find

$$\begin{aligned}\prod_{l=1}^{L} \Pi^{S^{j_l}} \psi &= \left(\prod_{l=1}^{L-1} \Pi^{S^{j_l}}\right) \tilde{\Pi}^{S^{j_L}} \psi \\ &= \tilde{\Pi}^{S^{j_L}} \left(\prod_{l=1}^{L-1} \Pi^{S^{j_l}}\right) \psi \\ &= \ldots = \tilde{\Pi}^{S^{j_L}} \cdots \tilde{\Pi}^{S^{j_1}} \psi.\end{aligned} \tag{62}$$

Thus, we can move Π^{S^i} next to ψ in the definition of ϕ with only positive operators that are $\leq \mathbb{1}$ acting either on systems complementary to S^i in AR or subsystems of S^i applied afterwards,

$$\phi = \left(\prod_{l=1}^{i-1} \Pi^{S^l}\right) \underbrace{\left(\prod_{l=i+1, S^l \not\supset S^i}^{|\mathcal{K}|} \Pi^{S^l}\right) \left(\prod_{l=i+1, S^l \supsetneq S^i}^{|\mathcal{K}|} \tilde{\Pi}^{S^l}\right)^{\dagger}}_{=:\hat{\Pi}^{S^i},\, \|\hat{\Pi}^{S^i}\|_\infty \leq \mathbb{1}} \Pi^{S^i} \psi. \tag{63}$$

As shown in the proof of Theorem 5.4 the submultiplicativity property and Lemma 5.3 ensure that the first product can only decrease the state $\Pi^{S^i}\psi$ on S^i while $\hat{\Pi}^{S^i}$ can only decrease the state $\Pi^{S^i}|\psi\rangle\langle\psi|_{S^i}\Pi^{S^i}$. This proves the min-entropy smoothing property of ϕ on all subsystems in $\mathcal{K}$. Note that this property also holds on all subsystems of AR complementary to those in $\mathcal{K}$ by the fact that ϕ is pure.

To obtain the distance estimate in (54) we proceed by

$$\begin{aligned}P(\psi,\phi) &\leq \sum_{i=1}^{|\mathcal{K}|} P\left(\prod_{j=i}^{|\mathcal{K}|} \Pi^{S^j}\psi,\ \prod_{j=i+1}^{|\mathcal{K}|} \Pi^{S^j}\psi\right) \\ &\leq \sum_{i=1}^{|\mathcal{K}|} P\left(\hat{\Pi}^{S^i}\Pi^{S^i}\psi, \hat{\Pi}^{S^i}\psi\right) \leq \sum_{i=1}^{|\mathcal{K}|} P(\Pi^{S^i}\psi,\psi) \\ &= \sum_{i=1}^{|\mathcal{K}|} P((\Pi^{S^i}\psi)_{S^i}, \psi_{S^i}) \leq |\mathcal{K}|\sqrt{2\varepsilon},\end{aligned}$$

where we used the expression obtained in (63) and the monotonicity of the purified distance as well as Lemma 5.1 and finally (1) in the last row.

It is apparent, that such a proof cannot be conducted in general for $m = 3$ when $\mathcal{K}$ is overlapping. Purifying the state of the system we obtain $\psi \in AR$. We may now consider $\mathcal{K} = \{A_1A_2, A_2A_3\}$. The state ϕ analogously defined to (61) would then take the form

$$\phi = \Pi^{A_1A_2}\Pi^{A_2A_3}\psi$$

up to a permutation of the order in which $\Pi^{A_1A_2}$ and $\Pi^{A_2A_3}$ are applied. The problem now is that $\tilde{\Pi}^{A_2A_3}$ cannot be moved past $\Pi^{A_1A_2}$, hence we cannot apply $\Pi^{A_1A_2}$ to ψ directly. It is not known, whether $\Pi^{A_2A_3}$ manipulates ψ such that ϕ does not smooth the min-entropy of ψ on A_1A_2. Moreover, the non-commutativity of $\Pi^{A_1A_2}$ and $\Pi^{A_2A_3}$ also prevents us from applying the argument used for the distance estimate above. Returning to a genuinely iterative scheme as in section 5.1.2 would solve this problem. We may thus redefine $\Pi^{A_1A_2}$ such that $(\Pi^{A_1A_2}\Pi^{A_2A_3}\psi)_{A_1A_2}$ is the $\varepsilon + D((\Pi^{A_2A_3}\psi)_{A_1A_2}, \psi_{A_1A_2})$ close $\mathbf{H}_{\min}$-smoother of $(\Pi^{A_2A_3}\psi)_{A_1A_2}$. While the resulting state ϕ formally has the right min-entropy on A_1A_2, we introduced an unknown parameter $D((\Pi^{A_2A_3}\psi)_{A_1A_2}, \psi_{A_1A_2})$. There is no reasonable bound known on this quantity since it is unknown how large the distance between $\Pi^{A_2A_3}\psi$ and ψ has to be chosen so that the state ϕ has larger min-entropy than $\mathbf{H}_{\min}^{\varepsilon,D}(A_2A_3)_\psi$ on A_2A_3. Concretely, the fact that $A_1A_2 \not\subset A_2A_3$ prohibits an application of the submultiplicativity of $\|\cdot\|_\infty$ to $\Pi^{A_1A_2}$ on subsystem A_2A_3. To summarize, the inherent non-commutativity of quantum min-entropy smoothing on different subsystems prevents an iterative approach from succeeding.

We conclude this section with an analysis of a special three-party case, where conjecture 3.1 can actually be proved by iterative techniques. Let A_1 be independent from A_2A_3, let $\mathcal{K} = \{A_1A_2, A_2A_3, A_1A_3\}$. Choose a purification $\psi = \psi'_{A_1R_1} \otimes \psi''_{A_2A_3R_2}$. Writing $\Pi^{A_1A_j} = \sum_i |i\rangle\langle i|_{A_1} \otimes \Pi^{A_1A_j}_{A_j,i}$, $\Pi^{A_1A_j}_{A_j,i} \leq \mathbb{1}_{A_j}$ and $\Pi_{A_1A_2,i} := \Pi^{A_1A_2}_{A_2,i} \otimes \Pi^{A_1A_3}_{A_3,i}$ we find on A_2A_3

$$\begin{aligned}
\|\phi_{A_2A_3}\|_\infty &= \|\sum_i \langle i|\,\psi'_{A_1}\,|i\rangle\,\Pi_{A_1A_2,i}\Pi^{A_2A_3}\psi''_{A_2A_3}\Pi^{A_2A_3}\Pi_{A_1A_2,i}\|_\infty \\
&\leq \sum_i \langle i|\,\psi'_{A_1}\,|i\rangle\,\underbrace{\|\Pi_{A_1A_2,i}\Pi^{A_2A_3}\psi''_{A_2A_3}\Pi^{A_2A_3}\Pi_{A_1A_2,i}\|_\infty}_{\leq\|\Pi^{A_2A_3}\psi''_{A_2A_3}\Pi^{A_2A_3}\|_\infty} \\
&\leq \|\Pi^{A_2A_3}\psi_{A_2A_3}\Pi^{A_2A_3}\|_\infty
\end{aligned}$$

On subsystem A_1A_j, $2 \leq j \leq 3$, we find that ϕ is min-entropy smoothing since the operators Π^S with $A_1A_j \neq S \subset A$ can be replaced iteratively by operators acting only a subsystem of $AR_1R_2 \setminus S$ by the techniques described in this section. Note that the structure of the purification ψ gives more freedom to replace operators acting on it by ones that act on different subsystems. Moreover, $\Pi^{A_1A_2}$ and $\Pi^{A_1A_3}$ commute. Then an application of Lemma 5.3 implies the min-entropy smoothing of ϕ on A_1A_j. The distance part is similar. We leave it to the reader.

5.2 Minimization in the positive semi-definite cone

Motivated by the failure of the iterative smoothing approach in the general quantum case, we consider an alternative proof ansatz for conjecture 3.1 in this section. The idea is to first construct a set of isometric extensions of min-entropy smoothing states on subsystems relative to the state of the system. Then the minimum of this set in the positive semi-definite cone is taken. In this manner, we are

able to rederive the result that follows from Corollary 4.2 in the classical case. Subsequently, we discuss the difficulties arising in an attempted generalization to the quantum setting.

5.2.1 The classical result

For the purpose of finding a isometric extension of a classical state relative to a given reference state on a classical-quantum (cq) system in the trace distance we prove the following Lemma.

Lemma 5.6. *Let XA be a classical-quantum system, $\rho \in \mathcal{S}_{\leq}(XA)$, $\sigma \in \mathcal{S}_{\leq}(X)$. There exists an extension $\bar{\sigma} \in \mathcal{S}_{\leq}(XA)$ to the total system with $\bar{\sigma}_X = \sigma$ and $D(\rho, \bar{\sigma}) = D(\rho_X, \sigma)$.*

Proof Note that the trace of a density operator is independent of the subsystem under consideration. Therefore, it suffices to find an extension $\bar{\sigma}$ to the total system that satisfies $\|\rho - \bar{\sigma}\|_1 = \|\rho_X - \sigma\|_1$. For this purpose we write ρ in cq-form,

$$\rho = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_A^{X=x},$$

where $\{|x\rangle\}$ denotes the classical basis of X and $\rho_A^{X=x}$ is the normalized state of system A conditioned on the event $X = x$. If $P_X(x) = 0$ then $\rho_A^{X=x}$ can be any normalized density operator. Let $\sigma = \sum_x Q_X(x)|x\rangle\langle x|$ be a spectral decomposition. Then the state

$$\bar{\sigma} := \sum_x Q_X(x)|x\rangle\langle x| \otimes \rho_A^{X=x} \tag{64}$$

is a cq-extension of σ to the total system with

$$\begin{aligned}
\|\rho - \bar{\sigma}\|_1 &= \|\sum_x (P_X(x) - Q_X(x))|x\rangle\langle x| \otimes \rho_A^{X=x}\|_1 \\
&= \sum_x |P_X(x) - Q_X(x)| \| |x\rangle\langle x| \otimes \rho_A^{X=x}\|_1 \\
&= \|\rho_X - \sigma\|_1
\end{aligned}$$

where the second line follows from the orthogonality of the support of $|x\rangle\langle x| \otimes \rho_A^{X=x}$ for different x and positive homogeneity of the trace norm. The third line is a consequence of the normalization of $\rho_A^{X=x}$. □

With the aid of this Lemma, we can prove conjecture 3.1 for classical states.

Theorem 5.7. *Let $\rho \in \mathcal{S}_{\leq}(A)$ be a classical state on an m-party system $A = A_1 \cdots A_m$, let $\mathcal{K} \subset 2^{\{A_1,\ldots,A_m\}} \setminus \emptyset$. For $\varepsilon > 0$ there exists a classical state $\sigma \in \mathcal{S}_{\leq}(A)$ such that*

$$\begin{aligned}
\mathbf{H}_{\min}(S)_\sigma &\geq \mathbf{H}_{\min}^{\varepsilon,D}(S)_\rho && (65)\\
D(\rho, \sigma) &\leq |\mathcal{K}|\varepsilon && (66)
\end{aligned}$$

Proof We explicitly construct a state σ that satisfies (65), (66). For every $S \in \mathcal{K}$, let $\omega^S \in B_\varepsilon^D(\rho_S)$ be such that $\mathbf{H}_{\min}(S)_{\omega^S} = \mathbf{H}_{\min}^{\varepsilon,D}(S)_\rho$. Since ω^S and ρ are classical, by Lemma 5.6 the state ω^S can be isometrically extended relative to ρ to a classical state $\bar{\omega}^S \in \mathcal{S}_\leq(A)$. Define the joint minimum σ of the set $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ on the space of classical states via

$$\sigma := \sum_{i_1,\ldots,i_m} (\min_{S\in\mathcal{K}} \langle i_1,\ldots,i_m|\,\bar{\omega}^S\,|i_1,\ldots,i_m\rangle)|i_1\rangle\langle i_1|_{A_1}\cdots|i_m\rangle\langle i_m|_{A_m}, \quad (67)$$

By definition, it follows $\sigma \leq \bar{\omega}^S$ for every $S \in \mathcal{K}$. By positivity of the partial trace this relation inherits to subsystem S, where it is equivalent to $\sigma_S \leq \omega^S$ and therefore implies (65).

To bound the distance consider a partition of the classical basis

$$\{|i_1,\ldots,i_m\rangle_{A_1\cdots A_m}\}_{1\leq i_k\leq d_{A_k}} = \bigsqcup_{S\in\mathcal{K}} K^S$$

into disjoint subsets where $|i_1,\ldots,i_m\rangle_{A_1\cdots A_m}$ can only lie in K^S if

$$\langle i_1,\ldots,i_m|\,\bar{\omega}^S\,|i_1,\ldots,i_m\rangle = \min_{T\in\mathcal{K}} \langle i_1,\ldots,i_m|\,\bar{\omega}^T\,|i_1,\ldots,i_m\rangle\,.$$

Define the corresponding complete set of orthogonal projections $\{\Pi^S|\,\mathrm{supp}\,\Pi^S = \mathrm{Span}\,K^S\}_{S\in\mathcal{K}}$ onto mutually orthogonal subspaces of A. We then find $\rho = \sum_{T\in\mathcal{K}} \Pi^T\rho\Pi^T$ and $\sigma = \sum_{S\in\mathcal{K}} \Pi^S\bar{\omega}^S\Pi^S$, which gives rise to

$$\begin{aligned} D(\rho,\sigma) &= D(\sum_{T\in\mathcal{K}} \Pi^T\rho\Pi^T, \sum_{S\in\mathcal{K}} \Pi^S\bar{\omega}^S\Pi^S) \\ &= \sum_{S\in\mathcal{K}} D(\Pi^S\rho\Pi^S, \Pi^S\bar{\omega}^S\Pi^S) \\ &\leq \sum_{S\in\mathcal{K}} D(\rho,\bar{\omega}^S) \\ &\leq |\mathcal{K}|\varepsilon \end{aligned} \quad (68)$$

Here, the second line is a consequence of the fact that by definition $\{\Pi^S\}_{S\in\mathcal{K}}$ project onto mutually orthogonal subspaces of A as well as $\rho \geq \bar{\omega}^S$ for all $S \in \mathcal{K}$ to obtain equality. In the third line, the monotonicity property of D (2) for the trace non-increasing CPM $\tau \to \Pi^S\tau\Pi^S$ was used. □

Note that the inequality in the third line of (68) makes especially transparent why the example presented in chapter 4 saturates the distance bound (66). Namely, this inequality becomes an equality if ρ and $\bar{\omega}^S$ differ only on $\mathrm{supp}\Pi^S$.

5.2.2 Generalization to the quantum setting

It is worth investigating a possible generalizations of the minimum-based approach to the quantum setting. Recall in this context, that the iterative smoothing in section

5.1.3 failed to yield a proof of conjecture 3.1 in the general quantum case due to the non-commutativity of the min-entropy smoothing operation for overlapping subsystems. Such a difficulty could be avoided if we, instead, take a minimium over a set of extensions $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ of min-entropy smoothing states on subsystems in the positive semidefinite sense.

However, there are two basic problems with this generalization of the classical idea to the quantum setting. First, we cannot apply Lemma 5.6 to conclude the existence of an extension $\bar{\omega}^S$ of the state $\omega^S \in B^D_\varepsilon(\rho_S)$ that is equally close to ρ on the total system. This is, however, easily solved if we use the purified distance instead of the trace distance in the definition of the smooth min-entropy, $\mathbf{H}_{\min}(S)_{\omega^S} = \mathbf{H}^{\varepsilon,P}_{\min}(S)_\rho$. In particular, know by Lemma 5.1 that $\Pi^S\rho\Pi^S$ is an isometric extension of $\omega^S = \Pi^S\rho_S\Pi^S$ relative to ρ. For ease of notation, we may thus due to (1) for the remainder of this section assume that $\bar{\omega}^S \in B^{\|\cdot\|_1}_\varepsilon(\rho)$ holds for all $S \in \mathcal{K}$.

The other more important issue is that the collection $\{\bar{\omega}^S\}_{S\in\mathcal{K}} \in B^P_\varepsilon(\rho)$ in general may not admit a positive semidefinite minimum $\sigma \in \mathcal{S}_\leq(A)$ close to ρ. Precisely, the inequality $\sigma \leq \tau$ implies $\mathrm{supp}\sigma \subset \mathrm{supp}\tau$ since

$$\forall\ |\alpha\rangle \in \ker\tau : 0 = \langle\alpha|\,\tau\,|\alpha\rangle \geq \langle\alpha|\,\sigma\,|\alpha\rangle = \|\sqrt{\sigma}\,|\alpha\rangle\,\|^2 \tag{69}$$

from which it follows that $\ker\tau \subset \ker\sigma$. Therefore, if the common support $\bigcap_{S\in\mathcal{K}}\mathrm{supp}\bar{\omega}^S = \{0\}$ is the trivial subspace the unique positive semidefinite minimum of $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ is $\sigma = 0$. This is always the case when the collection $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ contains two pure states that do not lie on the same complex line in A. Moreover, we have already seen in chapter 4 that the closest extension σ of a min-entropy smoothing state of a subsystem that satisfies $\sigma \leq \rho$ can generally be arbitrarily close to 0. Therefore, the positive semidefinite minimum condition alone tends to be too rigid to be yield a close candidate state to satisfy conjecture 3.1.

In the following we shall investigate which states ρ admit a positive semidefinite minimum $\sigma \in \mathcal{S}_\leq(A)$ of the ε-ball around them, $\sigma \leq \omega, \forall\omega \in B_\varepsilon(\rho)$ that converges to ρ as $\varepsilon \to 0$. For this purpose, we observe that the topology of the positive semidefinite cone is such that regular operators lie in its interior $\mathrm{int}(\mathcal{P}(A))$ while singular operators lie on its boundary $\partial\mathcal{P}(A)$:

$$\begin{aligned}\mathrm{int}\mathcal{P}(A) &= \{\tau \in \mathcal{P}(A)\big|\mathrm{rank}\tau = \dim\mathcal{H}\}\\ \partial\mathcal{P}(A) &= \{\tau \in \mathcal{P}(A)\big|\mathrm{rank}\tau < \dim\mathcal{H}\}\end{aligned}$$

Consider the minimization over an ε-ball centered $\rho \in \partial\mathcal{P}(A)$, $\varepsilon > 0$. By continuity of the action of unitaries on density operators, we find that $U\rho U^\dagger \in B^{\|\cdot\|_1}_\varepsilon(\rho)$ for U in some open neighborhood $V \subset \mathcal{U}(A)$ of $\mathbb{1}$. Therefore, by argument (69) it follows that $\ker(U\rho U^\dagger) = U\ker\rho \subset \ker\sigma$ for all $U \in V$. This implies that $\sigma = 0$ since the sum of all subspaces $U\ker\rho$, $U \in V$, contains a basis of A. We conclude that there exists no non-zero positive semidefinite minimum σ of any open neighborhood of the unitary orbit around ρ if $\rho \in \partial\mathcal{P}(A)$.

Notably, the situation changes once the state ρ lies in the interior of $\mathcal{P}(\mathcal{H})$. Let $\varepsilon < \lambda_{\min}(\rho)$, so that $B_\varepsilon^{\|\cdot\|_1}(\rho) \subset \operatorname{int}(\mathcal{P}(A))$. Then, we can argue

$$\forall\, \tau \in B_\varepsilon^{\|\cdot\|_1}(\rho) : \rho - \varepsilon \mathbb{1} \leq \tau, \tag{70}$$

hence $\sigma := \rho - \varepsilon\mathbb{1} \geq 0$ is a feasible minimum of $B_\varepsilon^{\|\cdot\|_1}(\rho)$ (in fact the closest achievable to ρ) that converges to ρ: $\|\rho - \sigma\|_1 = \varepsilon \dim A \to 0$ ($\varepsilon \to 0$). Note, however, that the dimension of A enters the distance expression, which renders the state $\rho - \varepsilon\mathbb{1}$ useless for applications.

In particular, the question is whether the distance estimate improves significantly if we define σ to only minimize over the set $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ and replace the states $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ on $\partial\mathcal{P}(A)$ by appropriate ones in $\operatorname{int}\mathcal{P}(A)$. To address the former we can consider

$$\sigma := \rho + \sum_{S\in\mathcal{K}} \{\bar{\omega}^S - \rho\}_-, \tag{71}$$

where $\{O\}_- := f(O)$ only keeps the negative part, $f(x) := x\chi_{(-\infty,0]}$. However, expression (71) does not necessarily define a positive operator if $\lambda_{\min}(\rho) < |\mathcal{K}|\varepsilon$.

To obtain a valid density operator in this case, we may apply a (slightly modified) depolarizing channel

$$\mathcal{E}_p : \tau \to (1-p)\tau + p\frac{\operatorname{tr}\rho - \varepsilon}{\dim A}\mathbb{1}, \tag{72}$$

where $p \in [0,1]$, $\operatorname{tr}\rho - \varepsilon = \inf_{\tau\in B_\varepsilon^{\|\cdot\|_1}(\rho)} \operatorname{tr}\tau$, to the states ρ and $\{\bar{\omega}^S\}_{S\in\mathcal{K}}$ first. Note that $\mathcal{E}_p$ contracts the set of density operators towards a fully mixed state mapping $B_\varepsilon^{\|\cdot\|_1}(\rho)$ to $B_{(1-p)\varepsilon}^{\|\cdot\|_1}(\mathcal{E}_p(\rho))$. To obtain a valid density operator σ replacing $\rho \to \mathcal{E}_p(\rho)$, $\bar{\omega}^S \to \mathcal{E}_p(\bar{\omega}^S)$ in definition (71), we have to choose p such that

$$\underbrace{\lambda_{\min}(\mathcal{E}_p(\rho))}_{=\lambda_{\min}(\rho)+p\frac{\operatorname{tr}\rho-\varepsilon}{\dim A}} \geq \underbrace{\|\sum_{S\in\mathcal{K}} \{\mathcal{E}_p(\bar{\omega}^S) - \mathcal{E}_p(\rho)\}_-\|_1}_{\leq|\mathcal{K}|(1-p)\varepsilon},$$

which is satisfied if $p \geq \frac{|\mathcal{K}|\varepsilon - \lambda_{\min}(\rho)}{|\mathcal{K}|\varepsilon + (\operatorname{tr}\rho-\varepsilon)/\dim A}$. Since the depolarizing channel does not increase the largest eigenvalue of any state in $B_\varepsilon^{\|\cdot\|_1}(\rho)$ on any subsystem of A this state σ will in fact achieve the smooth min-entropies on all subsystems in $\mathcal{K}$ simultaneously. For the distance to ρ we find

$$\|\rho - \sigma\|_1 \leq \underbrace{\|\rho - \mathcal{E}_p(\rho)\|_1}_{=p\|\rho - \frac{\operatorname{tr}\rho-\varepsilon}{\dim A}\mathbb{1}\|_1} + \underbrace{\|\mathcal{E}_p(\rho) - \sigma\|_1}_{\leq\sum_{S\in\mathcal{K}}\|\{\mathcal{E}_p(\bar{\omega}^S)-\mathcal{E}_p(\rho)\}_-\|_1 \leq |\mathcal{K}|(1-p)\varepsilon}. \tag{73}$$

The second term on the RHS is unproblematic since $p \in [0,1]$. The first term, however, gives a value close to $\|\rho - \frac{\operatorname{tr}\rho-\varepsilon}{\dim A}\mathbb{1}\|_1$ since the lower bound on p lies close to 1 for $\varepsilon \gg \frac{1}{|\mathcal{K}|\dim A}$ as is usual in applications. Therefore, such a state

σ generally lies far from ρ and is of little use to actual applications. However, interestingly, we find that $p \to 0$ ($\varepsilon \to 0, \dim A$ fixed), which proves the existence of sequences of simultaneous min-entropy smoothing states that converge to the state ρ of the system in the limit $\varepsilon \to 0$.

6 Conclusion

In this work, we transferred Dutil's multiparty typicality conjecture [2] to the one-shot setting using the concept of smooth min-entropies. As a result, we obtained an optimization problem for the min-entropies of different subsystems. A proof of this so-called simultaneous min-entropy smoothing conjecture was obtained for states whose min-entropy smoothing operations commute. This condition is especially satisfied in the classical case, where we derived an optimal distance bound. We demonstrated that there exist classical states whose support can be partitioned into mutually exclusive events, each being strongly atypical on a different subsystem. As a consequence, in general eliminating atypically large probabilities on all subsystems of a classical system simultaneously comes at the cost of an error growing exponentially in the number of parties.

We then addressed the quantum case, proving our one-shot conjecture 3.1 for the case of two parties by iteratively smoothing all subsystems according to an appropriate ordering. This result was generalized to more parties if the subsystems under consideration do not overlap. By the fact that smoothing was implemented as a rank non-increasing operation, we could conclude that conjecture 3.1 is also satisfied on a three party system in a pure state. However, we were not able to generalize this result further to arbitrary mixed states on three parties. Similarly, we could neither conclude our conjecture for general separable states from the fact that it holds for product states. The obstacle in these cases was the fact that it is unknown how smoothing operations for overlapping subsystems affect the min-entropies of the other system.

An alternative approach via minimization in the positive semidefinite cone was then considered. Although we could rederive an earlier result in the classical setting, a generalization of this idea to the quantum case did not succeed. This is due to the fact a state that achieves the smooth min-entropy on a subsystem and is smaller as an operator than the state on the total system generally can lie close to zero. An application of the depolarizing channel could not resolve this issue, however, it demonstrated the existence of sequences of simultaneous min-entropy smoothing states that - although at the wrong rate - converge to the state of the system in the limit where the smoothing parameter tends to zero.

Backed by these observations it is believed that in principle simultaneous min-entropy smoothing may be possible. However, more sophisticated techniques are required to obtain reasonable distance bounds. A potential solution could also come from further analyzing the iterative smoothing method in the three-party case as presented in section 5.1.3. In this context, techniques developed in the study of the quantum marginal problem [11] might be useful. To prove conjecture 3.1 in general it is felt that new insights into the compatibility of simultaneous eigenvalue perturbations on different subsystems might be required.

A further goal of future research should be to elucidate the operational meaning of simultaneous (min-)entropy smoothing. Are there any more fundamental applications than multiparty state merging? In this context, we note that the results

presented in sections 4, 5.1.1 and 5.1.2 with the exception of Theorem 4.3 can be minimally modified to apply to the max-entropy, where $\mathbf{H}_{\max}(\rho) := \log \operatorname{rank} \rho$, $\mathbf{H}^{\varepsilon}_{\max}(\rho) := \min_{\sigma \in B_{\varepsilon}(\rho)} \mathbf{H}_{\max}(\sigma)$. Also, a generalization of the simultaneous min-entropy smoothing conjecture to the conditional setting should be attempted to raise the potential for further applications of this concept, among them the simultaneous decoding conjecture for cq-MACs.

7 Acknowledgements

The author would like to thank Omar Fawzi, who jointly with the author developed the work presented in this thesis, for the many helpful discussions and continuous support. His optimism in the quest for scientific insight is inspiring. The author also would like to thank Renato Renner for offering the possibility to take part in the adventure of scientific research in his group.

References

[1] M. Horodecki et al. *Quantum state merging and negative information*, Communication in Mathematical Physics, 269(1): 107-136 (2007)

[2] N. Dutil, *Multiparty quantum protocols for assisted entanglement distillation*, Ph.D thesis, School of Computer Science, McGill University, Montreal (2011)

[3] J. Nötzel, *A solution to two party typicality using representation theory of the symmetric group*, arXiv:1209.5094v1 [quant-ph] (2012)

[4] R. Renner, *Security of quantum key distribution*, Ph.D. thesis, ETH Zürich (2005)

[5] O. Fawzi et al. *Classical communication over a quantum interference channel* IEEE Transactions on Information Theory, 58(6):3670-3691 (2012)

[6] I. Savov, *Network information theory for classical-quantum channels*, Ph.D. Thesis, School of Computer Science, McGill University (2012)

[7] A. Winter, *The capacity of the quantum multiple-access channel*, IEEE Transactions on Information Theory, 47(7):3069-3065 (2001)

[8] T.-S. Han, K. Kobayashi, *A new achievable rate region for the interference channel*, IEEE Transactions on Information Theory, 27(1): 49-60 (1981)

[9] P. Sen, *Achieving the Han-Kobayashi inner bound for the quantum interference channel by sequential decoding*, IEEE International Symposium on Information Theory (2012), arxiv:1109.0802

[10] H.-F. Chong et al. *A comparison of two achievable rate regions for the interference channel*, Proceedings of the USCD-ITA Workshop, San Diego, California, USA (2006)

[11] A. Klyachko, *Quantum marginal problem and N-representability*, Journal of Physics: Conference Series 36(1):72-86 (2006)

[12] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000, 409-416

[13] M. Tomamichel, *A Framework for Non-Asymptotic Quantum Information Theory*, Ph.D thesis, Institute for Theoretical Physics, ETH Zürich, 2012

[14] A. Uhlmann, *The Transition Probability for States of Star-Algebras*, Ann. Phys., 497(4): 524-532, 1985.

[15] E. Ehrhart, *Sur un problème de géometrie diophantienne linéaire II*, Journal für die reine und angewandte Mathematik, 227 (1967), 25-49

[16] M. Beck, S. Robbins, *Computing the Continuous Discretely - Integer Enumeration in Polyhedra*, Springer, 2007

[17] D. Hensley, *Slicing the cube in* $\mathbb{R}^n$ *and probability*, Proc. Amer. Math. Soc. 73 (1979), 95-100

[18] K. Ball, *Cube slicing in* $\mathbb{R}^n$, Proc. Amer. Math. Soc. 97 (1986) 465-473

[19] C. Zong, *The cube: a window to convex and discrete geometry*, Cambridge University Press (2006)