INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

On the Hardness of Disentanglers and Quantum de Finetti Theorems

F. G. Jeronimo *A. V. Moura*

Technical Report - IC-14-17 - Relatório Técnico

October - 2014 - Outubro

On the Hardness of Disentanglers and Quantum de Finetti Theorems

Fernando Granha Jeronimo [*] Arnaldo Vieira Moura [†]

Abstract

Entanglement has a dual role in quantum computation and information. It is an important resource in protocols such as quantum teleportation and superdense coding. On the other hand, it can potentially reduce the soundness in quantum Multi-prover Merlin-Arthur proof systems. Thus, understanding and controlling entanglement is of primary importance. To achieve this goal a super-operator capable of breaking entanglement, called a disentangler, has been proposed, together with a variety of quantum de Finetti Theorems. In this work, we study some limits of these approaches using computational hardness notions. We rule out the existence of some disentanglers and de Finetti Theorems based on some plausible hardness assumptions.

1 Introduction

Entanglement is an important resource in quantum information processing. It is a fundamental ingredient in protocols such as teleportation and superdense coding [1]. Nonetheless, there are situations in which the lack of entanglement may lead to better resource usage. This duality becomes evident in the context of Multi-prover Merlin-Arthur complexity complexity classes, denoted by QMA(k) where k is the number of unentangled provers [2]. We know that there are a variety of protocols in QMA(2) for treating NP-complete problems, and that use only a logarithmic number of qubits with respect to the input size [3] [4] [5] [6]. But unentanglement promises seem hard to enforce both quantumly and classically. For instance, the expressive power of QMA(2) is not yet well understood, as it ranges from QMA [7] to the powerful NEXP class [8]. In this work, we investigate the potential limits of approaches for breaking and controlling entanglement. We do that by making use of some computational hardness results.

A quantum state that is not entangled is said to be separable. In the case of a mixed state σ^{AB} for two subsystems A and B, it is separable if it can be written as $\sigma^{AB} = \sum p_i \sigma_i^A \otimes \sigma_i^B$, where p_i is a probability distribution [9]. Even though the set of separable states forms a convex set, finding the state that maximizes the Hilbert-Schmidt inner product of a positive

[*] This work was supported in part by FAPESP 2013/20661-1. F. G. Jeronimo is with the Institute of Computing, University of Campinas, Campinas, SP Brazil (e-mail: fegranha@gmail.com).

[†] A. V. Moura is with the Institute of Computing, University of Campinas, Campinas, SP Brazil (e-mail: arnaldo@ic.unicamp.br).

semi-definite matrix M and separable state σ^{AB} is NP-hard when the error is an inverse polynomial in the input [10]. This is known as the Best Separable State (BSS) problem, and it is closely related to the Weak Membership Problem for a set of separable states [11]. Since quantum states with polynomially many qubits are objects of Hilbert spaces of exponential size, optimizing the classical description of separable quantum states may easily become a NEXP-hard problem.

Instead of dealing with the classical description of quantum states, an alternative approach would be to explore quantum ways of breaking entanglement. Aaronson et al. were the first to propose a disentangler which is a quantum channel capable of approximating any separable state within an error δ in trace norm, and with output guaranteed to be always ϵ-close to a separable state, also in the trace norm [12]. They proved that there is no perfect disentangler when the errors δ and ϵ are set to zero. We extend their disentangler definition by considering the computational complexity of the quantum channel as well as the relationship of the input and output dimensions. This will allow us to associate computational hardness results to the existence of some disentanglers.

Computational hardness results are useful to unveil how hard it is to solve a certain problem by implying that its solution would also solve problems known or believed to be hard. The NP-hardness is perhaps the most important example, and problems in this class are widely believed to be intractable [13]. Another classical hardness class stems from the hypothesis that $3SAT$ has no sub-exponential time algorithm, also known as the Exponential Time Hypothesis (ETH) [14]. Here, we explore two quantum hardness notions: the hypothesis that $3SAT$ can not be solved in quantum polynomial time (the BQP class) and the belief that the best quantum algorithm for this problem requires $\Omega(2^{\sqrt{n}})$ time.

A different way to understand and control entanglement is through quantum de Finetti Theorems. Given a permutation invariant state $\rho_{A_1 \ldots A_n}$ on n subsystems of dimension $|A|$, a generic de Finetti Theorem bounds the distance of a reduced state $\rho_{A_1 \ldots A_k}$ on k ($k \leq n$) subsystems and a separable state. This distance is usually a function of k, n and $|A|$. Moreover, this distance can be measured using different norms such as the standard trace norm, the **SEP** norm and the fully one-way **LOCC** norm [15] [16]. Using the connection of disentanglers with de Finetti Theorems, it is possible to establish a hardness result on how the error scales with the number n in the **SEP** norm. Given the hardness assumption that $3SAT$ requires $\Omega(2^{\sqrt{n}})$ quantum time, this distance decreases at best as an inverse polynomial in n.

2 Preliminaries

A disentangler is a quantum channel capable of breaking entanglement. It has numerous applications in quantum information, quantum computing and quantum complexity. For instance, the existence of a certain efficient disentangler can be used to show the collapse QMA(2) = QMA. We extend the disentangler definition of Aaronson et al., to take into account the input and output dimensions, as shown next.

Definition 2.1 (Adapted from [12]). *Let $\mathcal{H}$ and $\mathcal{K}$ be two finite-dimensional Hilbert spaces. Then given a super-operator $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$, we say Φ is an (ϵ, δ, f)-disentangler if* *(i)* $\Phi(\rho)$ *is* ϵ*-close to a separable state for every* ρ*,*

(ii) for every separable state σ*, there exists a* $\rho \in \mathcal{H}$ *such that* $\Phi(\rho)$ *is* δ*-close to* σ*, and*

(iii) $\log(\dim(\mathcal{H})) = f(\log(\dim(\mathcal{K})))$*, where* $f : \mathbb{R}^+ \to \mathbb{R}^+$*.*

In the previous definition, closeness is measured with respect to the trace distance. However, it is also possible to use distances based on other norms such as **SEP** and the fully one-way **LOCC**. We denote by Φ^M, the restriction of Φ when the distance is measured according to the measurement class M.

We briefly describe three measurement classes: parallel one-way LOCC ($\mathbf{LOCC}_1^{||}$), **LOCC** and **SEP** as defined in [15]. They described the allowed measurement operators that are sometimes operationally motivated such as $\mathbf{LOCC}_1^{||}$ and **LOCC**. The $\mathbf{LOCC}_1^{||}$ class comprises all measurements that can be performed first on a subsystem A, and according to its outcome, an appropriate measurement M_i is used on a subsystem B. Such an operator can be written as:

$$M = \sum_i \alpha_i \otimes M_i,$$

where $\{\alpha_i\}$ forms a positive operator-valued measure (POVM) and $0 \leq M_i \leq I$ for each i. The more general class **LOCC** comprises measurements on subsystems that can be implemented using a finite number of local measurements and classical communication. In terms of operators, it can be inductively described as

$$\begin{aligned} M &= \sum_i (\sqrt{E_i} \otimes I) M_i (\sqrt{E_i} \otimes I), \quad \text{or} \\ M &= \sum_i (I \otimes \sqrt{E_i}) M_i (I \otimes \sqrt{E_i}), \end{aligned}$$

where $\{E_i\}$ satisfies $\sum_i E_i \leq I$ and $\{M_i\} \in \mathbf{LOCC}$. The **SEP** operator is even more expressive. It can be defined as

$$M = \sum_i M_i^A \otimes M_i^B$$

for positive semi-definite rank one matrices M_i^A and M_i^B. We have the following inclusion of measurement classes

$$\mathbf{LOCC}_1^{||} \subseteq \mathbf{LOCC} \subseteq \mathbf{SEP}.$$

As in [16], it is possible to associate with every POVM $\{M_x\}$ and state ρ the new state $\mathcal{M}(\rho) = \sum_x \operatorname{Tr}(M_x \rho)|x\rangle\langle x|$. Using this definition, it is possible to write the norm of a class of operator M as

$$\|\rho - \sigma\|_M = \max_{\mathcal{M} \in M} \|\mathcal{M}(\rho) - \mathcal{M}(\sigma)\|_1 .$$

Note this norm has the operational interpretation as the optimum bias that can be achieved by an operator of the class M when distinguishing ρ and σ, given one of them with uniform probability. This is the same operational interpretation of the trace norm [17].

The action of a quantum channel Φ on a state ρ^A can be described by a unitary operator U^{AE} acting on it and the environment which is initialized with $|0\rangle\langle 0|^E$ followed by tracing out all subsystems in AE but for a subset B. This action is described as

$$\sigma^B = \Phi(\rho^A) = \mathrm{Tr}_{\backslash B}(U^{AE}\rho^A \otimes |0\rangle\langle 0|^E U^{AE\dagger}).$$

One important observation is that the environment can always be modeled with quadratically many qubits as in system A [17].

We measure the time complexity of a channel Φ using the implementation of U^{AE}, in the same way that we measure the complexity of quantum circuits by the number of elementary gate operations it uses, taken from a fixed universal set such as $\{\mathbf{H}, \mathbf{T}, \mathbf{CNOT}\}$ [18].

It is possible to restrict item *(ii)* of Definition 2.1 to apply only to states σ with certain properties, instead of to arbitrary separable states. One important class of separable states is given by

$$\sigma = \int \psi \otimes \psi d\mu(\psi),$$

where μ is a probability measure over density matrices of a given size. Note that this type of state arises in several quantum de Finetti Theorems [19] [20]. The restriction of a disentangler Φ to require only approximation to states of this form in item *(ii)* is denoted $\Phi_=$.

We make use of the following amplification Theorem of Watrous and Marriott in which QMA with an inverse polynomial completeness soundness gap can be amplified to an exponential small error using the same witness.

Theorem 2.2 ([21]). *Let $c, s : \mathbb{N} \to [0,1]$, and $g \in poly$ with*

$$c(n) - b(n) \geq \frac{1}{g(n)}$$

for all $n \in \mathbb{N}$. Then $\mathrm{QMA}(1, c(n), s(n))_m \subseteq \mathrm{QMA}(1, 1 - 2^{-r(n)}, 2^{-r(n)})_m$ for every m and $r \in poly$. Moreover, the proof size m remains unchanged in the amplification.

Harrow and Montanaro showed that QMA(k) collapses to QMA(2).

Lemma 2.3 (From [15]). *For any m, $k \in \mathbb{N}$ and $0 \leq s < c \leq 1$,*

$$\mathrm{QMA}(k, c, s)_m \subseteq \mathrm{QMA}_{km}(2, c', s')^{\mathbf{SEP}}$$

where $c' = \frac{1+c}{2}$ and $s' = 1 - \frac{(1-s)^2}{100}$. Further, for any language L in $\mathrm{QMA}_{km}(2, c', s')^{\mathbf{SEP}}$ and any input $x \in L$, the two witness may be considered equal without loss of generality.

3 Disentanglers

We know that there is no disentangler in which $\epsilon = \delta = 0$ from [12]. In this section we study the computational hardness when $\epsilon, \delta > 0$, and show that, under certain hardness assumptions, even allowing an exponential time channel with respect to the number of output qubits n_{out}, there is no disentangler that acts on $poly(n_{out})$ input qubits and has error $\epsilon = \delta < \frac{k}{2^{n_{out}}}$, for some constant k.

The next lemma shows how to use a (ϵ, δ, f)-disentangler with certain properties to guarantee $\mathrm{QMA}(2) \subseteq \mathrm{QMA}(1)_m$. Note that m suffers an increase that depends on f.

Lemma 3.1. *For functions $f, l : \mathbb{N} \to \mathbb{N}$ and $c, s : \mathbb{N} \to [0, 1]$ satisfying $c(n) - s(n) \geq \frac{1}{g(n)}$ where g is a polynomial, we have*

$$\mathrm{QMA}(2, c(n), s(n))_{l(n)} \subseteq \mathrm{QMA}(1)_{f(l(n))},$$

assuming there is a polynomial time (ϵ, δ, f)-disentangler Φ with $\epsilon = \delta \leq \frac{1}{4g(n)}$.

Proof. We show how to transform a $\mathrm{QMA}(2, c(n), s(n))_{l(n)}$ verifier into a $\mathrm{QMA}(1)_{f(l(n))}$. Let $L \in \mathrm{QMA}(2, c(n), s(n))_{l(n)}$ verifier. If $x \in L$, there is a witness $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ and a state ρ such that $\Phi(\rho) = \psi'$ is δ-close to this witness. In the $\mathrm{QMA}(1)_{f(l(n))}$ protocol, the prover sends this state ρ with $f(l(n))$ qubits. The verifier applies the disentangler obtaining the approximation ψ' with which the original QMA(2) protocol is executed. It is clear that the completeness is at least $c(n) - \delta$ since $\Phi(\rho)$ is δ-close to $|\psi\rangle$. Otherwise, if $x \notin L$, no matter the state ρ sent by the prover, it will be ϵ-close to a separable state making the final soundness at most $s(n) + \epsilon$. The completeness soundness gap becomes

$$c(n) - s(n) - \delta - \epsilon \geq \frac{1}{g(n)} - \frac{1}{2g(n)} = \frac{1}{2g(n)},$$

that is still inversely polynomial, completing the proof. □

A $\mathrm{QMA}(1)_m$ protocol can be simulated in time $O(poly(n)2^{2m})$ where n is the input size. This result, adapted from Watrous and Marriott [21], plays a crucial role in our hardness results for some disentanglers. It is stated as

Lemma 3.2. *Let $L \in \mathrm{QMA}(1)_m$, and $x \in \{0, 1\}^n$. Deciding if $x \in L$ can be done in $O(poly(n)2^{2m})$ quantum time.*

Proof. We explore the proof $\mathrm{QMA}_{O(\log(n))} \subseteq \mathrm{BQP}$ [21]. Firstly, some notation. Let L be a language in QMA_m where m denotes the witness size. Let x be an input string and A_x be the associated verifier circuit acting on $k + m$ qubits, where k is the number of ancilla qubits, a polynomial in the size of the input. The amplification procedure of Theorem 2.2 allows us to assume, without loss of generality, that if $x \in L$ then there is witness $|\psi\rangle$ that satisfies

$$\Pr[A_x \text{ accepts } |\psi\rangle] \geq 1 - 2^{-m-2},$$

and if $x \notin L$, for all states $|\psi\rangle$ we have

$$\Pr[A_x \text{ accepts } |\psi\rangle] \leq 2^{-m-2}.$$

We associate to every x a $2^m \times 2^m$ matrix Q_x as follows

$$Q_x = (I_m \otimes \langle 0^k|)A_x^\dagger \Pi_1 A_x (I_m \otimes |0^k\rangle),$$

where Π_1 is the projector on the subspace that has the accepting qubit of A_x equal to 1. Note that Q_x corresponds to a positive semidefinite matrix of an efficient implementable measurement, as A_x is a polynomial time circuit.

The eigenvalues of Q_x are the associated acceptance probability of their respective eigenvectors. Therefore, if $x \in L$, then $\mathrm{Tr}(Q_x) \geq 1 - 2^{-m-2} \geq \frac{3}{4}$ as there exist at least one state (eigenvector) that accepts with probability at least $1 - 2^{-m-2}$. Otherwise, all eigenvalues are at most 2^{-m-2}, resulting in $\mathrm{Tr}(Q_x) \leq 2^m 2^{-m-2} \leq \frac{1}{4}$. It is possible to build a BQP circuit B that decides if $L \in \mathrm{QMA}_m$ by applying the measurement Q_x to the totally mixed state on m qubits. In this case, the acceptance probability of B is

$$\Pr[B \text{ accepts}] = \mathrm{Tr}(Q_x 2^{-m} I_m) = 2^{-m}\,\mathrm{Tr}(Q_x).$$

The completeness soundness gap $g(n)$ is 2^{-m-1}. We can repeat B a certain number of times, say N, in order to amplify this gap. Using the Chernoff bound to achieve a constant error probability ϵ_c, the value N must satisfy

$$N \geq \frac{1}{g^2} \ln(\frac{1}{\sqrt{\epsilon_c}}),$$

resulting in a time complexity $O(poly(n)2^{2m})$, given that the QMA_m verifier runs in time $poly(n)$. □

The $\mathrm{QMA}(2)_{\log(n)}$ protocol for $3SAT$ that has the largest completeness soundness gap is due to Le Gall et al., it is our starting point to show the hardness of some disentanglers.

Theorem 3.3 (GNN [6]).

$$3SAT \in \mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{npolylog(n)}))_{O(\log(n))}$$

Let $\frac{1}{g(n)}$ denote the completeness soundness gap. The proof size $l(n)$ satisfies

$$\log(tg(n)) \leq l(n) \leq t' \log(n)$$

for constants t, t' and $n > 1$.

For a (ϵ, δ, f)-disentangler Φ, if the errors ϵ and δ are sufficiently small and f does not require the input size to be much larger than the output, it will be possible to use the two previous lemmas to show that $3SAT$ can be decided faster than it is currently know. This is our approach to show the hardness of some disentanglers. The following three Theorems make precise the conditions under which Φ promotes such speedups.

The next theorem treats the case in which the input and output of Φ are linearly related.

Theorem 3.4. *If* $3SAT \notin \text{BQP}$*, then there is no* $O(poly(\dim(\mathcal{K})))$ *time* (ϵ, δ, f)*-disentangler* Φ *with* $f(x) = cx$ *and* $\epsilon, \delta \leq \frac{k}{\dim(\mathcal{K})}$*, for any constant* $c \geq 1$ *and any fixed constant* k*.*

Proof. This proof follows from the GNN protocol for $3SAT$ in Theorem 3.8, and using Lemmas 3.1 and 3.2, as we elaborate next. We show the contrapositive, that is, if a $O(poly(\dim(\mathcal{K})))$ time (ϵ, δ, f)-disentangler Φ exists with $f(x) = cx$ and $\epsilon, \delta \leq \frac{k}{\dim(\mathcal{K})}$ for any $c \geq 1$ and a constant k that we specify latter, then $3SAT$ is in BQP.

Let $g(n) = c(n) - s(n)$ be the completeness soundness gap in the GNN protocol where n denotes the input size. In this protocol, the proof size $l(n)$ is greater than $\log(tg(n))$ for some constant t. Thus, the dimension $\dim(\mathcal{K})$ of the output space is at least $tg(n)$. Since the errors ϵ and δ of Φ are bounded above by $\frac{k}{\dim(\mathcal{K})}$, we can choose a constant k such that $\frac{k}{tg(n)} \leq \frac{1}{4g(n)}$.

Combining the existence of Φ and Lemma 3.1, we conclude that the GNN protocol is in $\text{QMA}_{ct' \log(n)}$ for some constant t', and where $t' \log(n)$ is an upper bound on the witness size in this protocol. Now, using Lemma 3.2 this protocol can be solved in polynomial $O(poly(n) 2^{2ct' \log(n)})$ quantum time, implying that $3SAT$ is in BQP. □

The previous result can be improved under the assumption that there is no quasi-polynomial quantum time ($O(2^{\text{polylog}(n)})$) algorithm for 3SAT. The best quantum algorithm to this date is the Grover unstructured search, with complexity $O(2^{\sqrt{n}})$.

Theorem 3.5. *If there is no quantum algorithm for 3SAT which runs in* $O(2^{polylog(n)})$ *time, then there is no* $O(poly(\dim(\mathcal{K})))$ *time* (ϵ, δ, f)*-disentangler* Φ *with* $f \in poly$ *and* $\epsilon, \delta \leq \frac{k}{\dim(\mathcal{K})}$*, where* k *is a constant.*

Proof. Similar to the proof of Theorem 3.4. But now the simulation of the GNN protocol occurs in $\text{QMA}_{\text{polylog}(n)}$, as the number of input qubits and output qubits of Φ are related by a polynomial. Since the output dimension Φ remains the same as in the previous Theorem, the the same choice of k allows us to use Lemma 3.1 and claim that $3SAT$ is in $\text{QMA}_{\text{polylog}(n)}$. Using Lemma 3.2, we conclude that $3SAT$ that can be solved in $O(poly(n) 2^{\text{polylog}(n)})$ time. □

We can also conjecture that every quantum algorithm to solve any NP-complete problem requires $\Omega(2^{\sqrt{n}})$ time. In this case, the function f in Theorem 3.5 can be improved again as shown by the next theorem.

Theorem 3.6. *If there is no quantum algorithm for 3SAT which runs in* $o(2^{\sqrt{n}})$ *time, then there is no* $O(poly(\dim(\mathcal{K})))$ *time* (ϵ, δ, f)*-disentangler* Φ *with* $f(x) = 2^{\frac{x}{c}}$ *and* $\epsilon, \delta \leq \frac{k}{\dim(\mathcal{K})}$*, for some constants* c *and* k*.*

Proof. Same reasoning as in the last two results. Let the proof size in the GNN protocol be bounded by $t' \log(n)$ for a constant t'. It suffices to choose a constant c such that $2^{\frac{t' \log(n)}{c}} < \frac{\sqrt{n}}{2}$ for every $n > 1$. □

The previous theorem is a step towards proving the following conjecture.

Conjecture 3.7 (Watrous (from [12]))**.** *For any constants $\epsilon, \delta < 1$, a (ϵ, δ)-disentangler will require* $\dim(\mathcal{H}) = 2^{\Omega(\dim(\mathcal{K}))}$.

It would be interesting if the previous theorem could be scaled down. That is, instead of a $\dim(\mathcal{K})$ dependence, it would show a polylog($\dim(\mathcal{K})$) dependence for both the disentangler complexity and the errors ϵ and δ.

It is possible to use the result QMA(k) = QMA(2), given by Lemma 2.3, to show that the GNN protocol can be transformed into a **SEP** protocol by doubling the message size and squaring the completeness soundness gap.

Theorem 3.8 (SEP GNN (variation of [6]))**.** *We have*

$$3SAT \in \mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{n^2 polylog(n)}))^{\mathbf{SEP}}_{O(\log(n))}.$$

If $g(n) \in \Omega(\frac{1}{n^2 polylog(n)})$ is the completeness soundness gap, then the proof size $l(n)$ satisfies

$$\log(t\sqrt{g(n)}) \leq l(n) \leq t' \log(n)$$

for constants t, t' and $n > 1$.

In Theorems 3.4, 3.5 and 3.6, the norm used to measure distances was the general trace norm. By making $\epsilon = \delta \leq \frac{k}{\dim(\mathcal{K})^2}$, for a suitable constant k, and using the **SEP** version of the GNN protocol in Theorem 3.8, we can see that the same results hold for the more restricted $\Phi^{\mathbf{SEP}}$ disentangler.

4 Connection to the de Finetti Theorems

Quantum de Finetti Theorems provide sufficient conditions that limit the maximum correlations that quantum states on n subsystems may exhibit when considering only k ($k \leq n$) of them. They are important tools to limit the entanglement among these subsystems.

Brandão et al. established the connection of a version of the de Finetti Theorem for parallel **LOCC** to $(\epsilon, 0, f(x) = \frac{tx}{\epsilon^2})$-disentanglers in this norm, where t is a constant [11] [22]. We define a generic de Finetti Theorem based on [16], and observe that it leads to a generic disentangler.

Theorem 4.1 (Generic de Finetti Theorem)**.** *Let $\rho_{A_1 \ldots A_n}$ be a permutation invariant state on $\mathcal{H}_A^{\otimes n}$. Then, for integers $0 \leq k \leq n$, there exists a probability measure μ on density matrices on $\mathcal{H}_A$, and a function g such that*

$$\left\| \rho_{A_1 \ldots A_k} - \int \sigma^{\otimes k} d\mu(\sigma) \right\|_M \leq g(|A|, k, n).$$

This generic theorem implies the existence of the following generic disentangler.

Lemma 4.2. *A de Finetti theorem, in the generic form of Theorem 4.1, implies the existence of a $(\epsilon, 0, f)$-disentangler $\Phi^M_{=}$, and where the error ϵ is given by $g(|A|, k, n)$ with function f satisfying $f(x) = nx$.*

Proof. Let $\rho_{A_1\ldots A_n}$ be a state in $\mathcal{H}_A^{\otimes n}$, and let $k=2$. The disentangler $\Phi_{=}^{M}$ selects uniformly at random one permutation τ in the symmetric group S_n, and permute the systems $A_1\ldots A_n$ according to it. Then, it traces out all of them, except the first two subsystems which we denote by A_1' and A_2'. This action can be described as

$$\Phi_{=}^{M}(\rho_{A_1\ldots A_n}) = \mathrm{Tr}_{\backslash A_1'A_2'}(\sum_{\tau\in S_n}\frac{1}{n!}\tau\rho_{A_1\ldots A_n}\tau^{\dagger}).$$

After a random permutation, the state becomes permutation invariant. Hence, the generic de Finetti Theorem 4.1 applies [23]. Let $\rho'_{A_1'A_2'}$ denote the output state. The de Finetti Theorem guarantees that it is ϵ-close where ϵ is given by

$$\epsilon \leq g(|A|, 2, n).$$

Conversely, any separable state $\sigma = \int \psi\otimes\psi d\mu'(\psi)$, where μ' is a measure on density matrices, can be extended to n subsystems $\sigma^n = \int \psi^{\otimes n} d\mu'(\psi)$. This new state is permutation invariant, and its reduced state in A_1' and A_2' is equal to σ. Therefore, the error δ is zero. The input space is $\mathcal{H} = \mathcal{H}_A^{\otimes n}$, and the output space is $\mathcal{K}^{\otimes 2} = \mathcal{H}_a^{\otimes 2}$. Thus $f(x) = nx$. □

Theorem 4.3. *For any constant $p > p_0$, unless there is a $o(2^{\sqrt{n}})$ time quantum algorithm for $3SAT$, the following quantum de Finetti Theorem is impossible.*

Let $\rho_{A_1\ldots A_n}$ be a permutation invariant state on $\mathcal{H}_A^{\otimes n}$. Then, for integers $0 \leq k \leq n$ there exists a probability measure μ on density matrices on $\mathcal{H}_A$ such that

$$\left\|\rho_{A_1\ldots A_k} - \int \sigma^{\otimes k} d\mu(\sigma)\right\|_{\mathbf{SEP}} \leq \frac{poly(k)poly(|A|)}{n^p}.$$

Proof. We show that if the stated de Finetti theorem is possible, then there is (ϵ,δ,f)-disentangler $\Phi_{=}^{\mathbf{SEP}}$ with $f(x) = 2^{\frac{x}{c}}$ and $\epsilon,\delta \leq \frac{k'}{\dim(\mathcal{K})^2}$, for some constants c and k'. Combining this result with the extension of Theorem 3.6 in the **SEP** norm implies that $3SAT$ has a $o(2^{\sqrt{n}})$ time quantum algorithm.

Let the number of output systems k be 2. Let $x = \log(\dim(\mathcal{H}_A))$ and let $n = \frac{2^{\frac{x}{c}}}{x}$. Now, using the de Finetti Theorem we have:

$$\begin{aligned}\left\|\rho_{A_1A_2} - \int \sigma^{\otimes 2} d\mu(\sigma)\right\|_{\mathbf{SEP}} &\leq \frac{poly(2)poly(|A|)}{n^p}\\ &= O(\frac{|A|^a}{2^{\frac{p}{c}x - p\log(x)}})\\ &= O(\frac{2^{ax}}{2^{\frac{p}{c}x - p\log(x)}})\\ &= O(\frac{1}{2^{\frac{p}{c}x - ax - p\log(x)}}),\end{aligned}$$

where a is the maximum degree of $poly(|A|)$.

For any $p > p_0 = c(a+2)$, we have the following upper bound

$$O(\frac{1}{\dim(\mathcal{H}_A)^{2+\varepsilon}}).$$

for any $\varepsilon > 0$ which is asymptotically smaller than $O(\frac{k'}{\dim(\mathcal{H}_A)^2})$. Note that the random permutation takes time at most $O(poly(2^x))$ since the disentangler input size is $O(2^{\frac{x}{c}})$. This leads to a disentangler that contradicts our hardness assumption. □

Note 4.4. *Given the hardness assumption of the previous Theorem, even for the restricted* **SEP** *norm the distance error from a separable state in the de Finetti Theorem does not decrease faster than an inverse polynomial in the number of subsystems n. But this dependence is $\frac{1}{n}$ for the more general trace norm version of the de Finetti Theorem [19] [20].*

Note 4.5. *The previous Theorem holds for a different constant p_0, even if the dependence on the dimension subsystem A is polylogarithmic.*

Note 4.6. *Any proof that* $\mathrm{QMA}(2) \subseteq \mathrm{QMA}$ *that relies only on a de Finetti of the same form as Theorem 4.1 must have a polylogarithmic dependence on A, since the dependence on n in the best case is an inverse polynomial, assuming the hardness assumption.*

5 Conclusion

The starting point of our hardness results for disentanglers and the generic quantum de Finetti Theorem is a protocol for $3SAT$ in $\mathrm{QMA}(2)_{O(\log(n))}$ which has completeness soundness gap $\Omega(\frac{1}{n\mathrm{polylog}(n)})$. One way to strengthen these hardness results would be to devise protocols with larger gaps. For an (ϵ, δ, f)-disentangler, the errors ϵ and δ are directly related to this gap. Therefore, an interesting research direction is to improve this gap, or otherwise show that it is optimum.

References

[1] M. M. Wilde (2013), *Quantum Information Theory* (Cambridge University Press, New York, NY, USA), 1st edition.

[2] H. Kobayashi, K. Matsumoto and T. Yamakami (2003), *Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur?* In T. Ibaraki, N. Katoh and H. Ono, eds., *ISAAC*, Vol. 2906 of *Lecture Notes in Computer Science*, pp. 189–198 (Springer).

[3] H. Blier and A. Tapp (2009), *All languages in np have very short quantum proofs.* Quantum, Nano, and Micro Technologies, First International Conference on, Vol. 0, pp. 34–37.

[4] S. Beigi (2010), *NP vs qma_log(2).* Quantum Information & Computation, Vol. 10(1&2), p. 2.

[5] A. Chiesa and M. A. Forbes (2011), *Improved soundness for qma with multiple provers.* CoRR, Vol. abs/1108.2098.

[6] F. Gall, S. Nakagawa and H. Nishimura (2012), *On qma protocols with two short quantum proofs.* Quantum Information and Computation, Vol. 12(7-8), pp. 589–600.

[7] A. Y. Kitaev, A. H. Shen and M. N. Vyalyi (2002), *Classical and Quantum Computation* (American Mathematical Society, Boston, MA, USA). ISBN 0821832298.

[8] S. Arora and B. Barak (2009), *Computational Complexity: A Modern Approach* (Cambridge University Press, New York, NY, USA), 1st edition. ISBN 0521424267, 9780521424264.

[9] L. M. Ioannou (2007), *Computational complexity of the quantum separability problem.* Quantum Info. Comput., Vol. 7(4), pp. 335–370. ISSN 1533-7146.

[10] S. Gharibian (2010), *Strong np-hardness of the quantum separability problem.* Quantum Info. Comput., Vol. 10(3), pp. 343–360.

[11] F. G. S. L. Brandão, M. Christandl and J. Yard (2011), *A quasipolynomial-time algorithm for the quantum separability problem.* In *STOC*, pp. 343–352.

[12] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman and P. W. Shor (2008), *The power of unentanglement.* Electronic Colloquium on Computational Complexity (ECCC), Vol. 15(051).

[13] M. R. Garey and D. S. Johnson (1990), *Computers and Intractability; A Guide to the Theory of NP-Completeness* (W. H. Freeman & Co., New York, NY, USA). ISBN 0716710455.

[14] R. Impagliazzo and R. Paturi (2001), *On the complexity of k-sat.* J. Comput. Syst. Sci., Vol. 62(2), pp. 367–375.

[15] A. W. Harrow and A. Montanaro (2013), *Testing product states, quantum merlin-arthur games and tensor optimization.* J. ACM, Vol. 60(1), p. 3.

[16] K. Li and G. Smith (2014), *Quantum de finetti theorem measured with fully one-way locc norm.* CoRR, Vol. abs/1408.6829.

[17] M. Nielsen and I. Chuang (2000), *Quantum computation and quantum information.* Cambridge Series on Information and the Natural Sciences (Cambridge University Press). ISBN 9780521635035.

[18] H. Kobayashi, F. Le Gall and H. Nishimura (2013), *Stronger methods of making quantum interactive proofs perfectly complete.* In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ITCS '13, pp. 329–352 (ACM, New York, NY, USA). ISBN 978-1-4503-1859-4.

[19] M. Christandl, R. König, G. Mitchison and R. Renner (2007), *One-and-a-half quantum de finetti theorems.* Communications in Mathematical Physics, Vol. 273(2), pp. 473–498. ISSN 0010-3616.

[20] (2011), *John watrous lecture notes: Theory of quantum information.*

[21] C. Marriott and J. Watrous (2005), *Quantum arthur-merlin games.* Computational Complexity, Vol. 14(2), pp. 122–152.

[22] F. Brandão, M. Christandl and J. Yard (2011), *Faithful squashed entanglement.* Communications in Mathematical Physics, Vol. 306(3), pp. 805–830.

[23] A. W. Harrow (2013), *The church of the symmetric subspace.* CoRR, Vol. abs/1308.6595.