Study of Unentanglement in Quantum Computers

Rayan Chikhi

February 20th 2008 - June 20th 2008

M2RI Internship

Massachusetts Institute of Technology
Department of Mechanical Engineering

Ecole Normale Supérieure de Cachan, Antenne de Bretagne
Département Informatique et Télécommunications

Université de Rennes 1
Institut de Formation Supérieure en Informatique et Communication

Abstract

This report explains the research work done during a February-June 2008 internship at MIT under the supervision of Scott Aaronson and Seth Lloyd. It exposes some necessary background knowledge in quantum mechanics, quantum computing and quantum complexity theory, and then focuses on the work conducted during this internship. The subject of this internship is to study two important classes of quantum problems, QMA and $\mathsf{QMA(2)}$, which consist of all languages that can be verified using respectively one and two unentangled quantum proofs. Whether these classes are equal or distinct is an open problem of great interest in quantum computing. To prove that they are the same, one can possibly simulate $\mathsf{QMA(2)}$ problems in QMA using a quantum operation called a disentangler. However, it has been conjectured that polynomial disentanglers do not exist, and therefore this approach fails. In this report, we investigate this conjecture and give two results: in a specific situation, when exponential precision is required, this conjecture holds as long as $\mathsf{P} \neq \mathsf{NP}$. Moreover, in the same situation, we show that the conjecture could be proven unconditionally using a stronger hypothesis.

Introduction

We have witnessed a growing interest in quantum computation over the last decade. While the superiority of quantum computers over classical ones is not yet confirmed by practical experiment, theoretical results predict it to some extent. Efficient algorithms such as Shor's factoring algorithm [25] have encouraged us to believe that there exists many algorithms that perform faster on quantum computers. Quantum complexity theorists are currently investigating this question, in terms of complexity classes.

A quantum complexity class of interest is the class of Quantum Merlin-Arthur problems (QMA), the quantum counterpart of NP. Every problem in this class can be formulated as such: Arthur, a quantum computer, is provided a certificate for his problem by Merlin, an all-knowing computer, and he has to verify it in polynomial time with high success probability. In classical Merlin-Arthur problems, whether Merlin provides one or two certificates does not help Arthur. However in quantum instances, providing two un-correlated quantum certificates defines a problem that belongs to a possibly strictly larger complexity class ($\mathsf{QMA(2)}$). Whether $\mathsf{QMA(2)} \neq \mathsf{QMA}$ has been an open problem since 2001, cited by many authors [21, 20, 2] as highly relevant for our understanding of quantum computing. If we knew that $\mathsf{QMA(2)} \neq \mathsf{QMA}$, it would mean that there exists mathematical statements that can only be verified with two quantum proofs; no matter how polynomially long it is, one proof would never suffice.

During this internship, we studied this problem and gave formal evidence supporting the claim that $\mathsf{QMA(2)} \neq \mathsf{QMA}$. More precisely, we focused on showing that a natural approach to prove that $\mathsf{QMA}(2) = \mathsf{QMA}$ fails. This approach is formulated in [1]: if there exists a polynomial-time procedure that maps every quantum certificate to a sufficiently good approximation of two un-correlated quantum certificates, then Arthur can simulate a $\mathsf{QMA}(2)$ protocol in QMA, and $\mathsf{QMA}(2) = \mathsf{QMA}$. Such procedure is called an (ϵ, δ)-*disentangler*, where ϵ and δ are approximation parameters that we later define more formally. In the same publication, it was established that $(0, 0)$-disentanglers do not exist in any finite dimension.

The authors then list two open problems:

- Can we prove that (ϵ, δ)-disentanglers only exist if the input space is exponentially larger than the output space?
- Can we at least show this for $(\epsilon, 0)$ or $(0, \delta)$-disentanglers?

We give elements of answer to both of these questions. We show that polynomial-input, exponential-error disentanglers do not exist if we assume that $\mathsf{P} \neq \mathsf{NP}$. We prove that, given a disentangler, one can efficiently solve a hard quantum separability problem. We finally give an unconditional result for exponential-error disentanglers, by showing that the (ϵ, δ), $(\epsilon, 0)$ and $(0, \delta)$ cases are equivalent.

Since the approach to prove that $\mathsf{QMA}(2) = \mathsf{QMA}$ relies on the existence of constant-error disentanglers, both questions remain open. Our results nevertheless provide a step towards the study of disentanglers.

The rest of this paper is organized as follows:

Section 1	Introduction to quantum mechanics
Section 2	Introduction to quantum computing and quantum complexity theory
Section 3	Definition and motivation of our problem, and related results
Section 4	Our results and discussion

1 Quantum Mechanics for Computer Scientists

Before introducing our problem, one should first be familiar with the underlying theories, in increasing order of abstraction: quantum mechanics, quantum computing and quantum complexity. We begin with an introduction to quantum mechanics which only requires the reader to know basic mathematical concepts such as vector spaces and probabilities.

1.1 Basics of Quantum Mechanics

From a computer science point of view, quantum mechanics can essentially be treated as a generalization of probability theory to complex values [3, 24]. To give an intuition of this, consider a single bit described by classical probabilities as a random variable being 0 with probability α and 1 with probability β. Classical probabilities impose $\alpha + \beta = 1$.

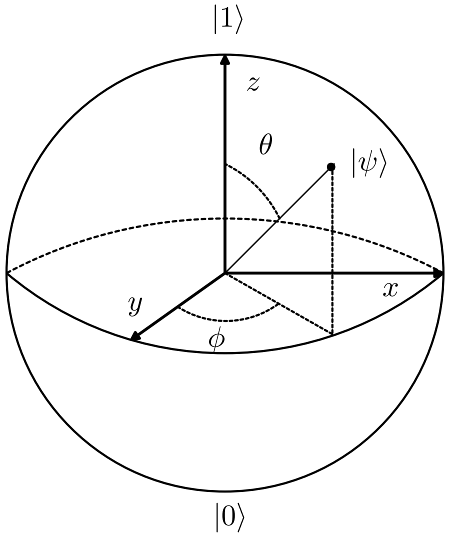

Figure 1: Representation of a qubit in superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ using the Bloch sphere. This representation allows a three-dimensional view of a four-dimensional object. By multiplying $|\psi\rangle$ by an unobservable phase factor, α can be made a real number, and therefore only three real parameters are needed to describe the qubit. The Bloch sphere representation corresponds to $\alpha = cos(\theta/2)$ and $\beta = e^{i\phi}sin(\theta/2)$. The coordinates are: $x = sin(\theta)sin(\phi)$, $y = sin(\theta)cos(\phi)$, $z = cos(\theta)$.

Quantum mechanics tells us that there exists physical entities similar to the bit that admit complex probability weights (α, β) where $|\alpha|^2 + |\beta|^2 = 1$. This leads to the definition of a *qubit* with two states $|0\rangle$ and $|1\rangle$, which is said to exist in a *superposition* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α, β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$ (see Figure 1). However, the superposition cannot be seen: any attempt to measure the qubit state will permanently affect it to $|0\rangle$ with probability $|\alpha|^2$ or to $|1\rangle$ with probability $|\beta|^2$. Therefore, unlike bits, we can never recover the description of a qubit (knowledge of α and β) by measuring its value.

1.2 Quantum Formalism

After having exposed some intuition on quantum mechanics, we now introduce the quantum formalism as well as the fundamental postulates. This can help gain a better understanding of why qubits behave the way we described them.

Postulate 1 An isolated physical system is a complex vector space with inner product (that is, a Hilbert space $\mathcal{H}$). It is completely described by the *pure state vectors*, which are unit vectors, noted $|\psi\rangle$.

Postulate 2 The evolution of a closed quantum system is described by an unitary operator

U ($U^\dagger U$ is the identity[1]). Between time instants t_1 and t_2, $t_1 < t_2$, the state vector $|\psi_1\rangle$ is related to $|\psi_2\rangle$ by an unitary U, depending only on t_1 and t_2,

$$|\psi_2\rangle = U\,|\psi_1\rangle\,.$$

Postulate 3 The system can be measured by a collection $\{M_n\}$ of *measurement operators* that satisfies the completeness relation: $\sum_i M_i^\dagger M_i = I$. The operator index refers to the measurement outcome (ie. M_i measures the outcome i). If the state of the system is $|\psi\rangle$, then the result i occurs with probability

$$p(i) = \langle\psi|\, M_i^\dagger M_i\,|\psi\rangle$$

where $\langle\psi|$ is $|\psi\rangle^\dagger$, the dual vector of $|\psi\rangle$. Immediately after the measurement, the state of the system becomes

$$\frac{M_i\,|\psi\rangle}{\sqrt{p(i)}}$$

Postulate 4 The state space of a composite system (a system made up of two or more distinct systems) is the tensor product[2] of the state spaces of the component systems. For instance, if each component system is in the state $|\psi_i\rangle$, $i = 1,..,n$, the composite system is in the state $|\psi_i\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

Postulate 1 tells us that qubit superpositions exist, as a qubit is described by a two-dimensional state space. Postulate 2 is more commonly known in a refined formulation that describes the evolution of a system in continuous time. In that case, Postulate 2 is the Schrödinger equation:

$$i\hbar\frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle\,,$$

where H is an Hermitian operator (the *Hamiltonian*) and $\hbar$ is Planck's constant. However, it suffices to consider the discrete formulation of Postulate 2 for the study of quantum computing.

Postulate 3 is the reason why we never observe superpositions in everyday life. When the state of the system is measured by any experimental device, for example an eye, it collapses with certain probability to a state modified by the measurement outcome.

The intuition behind Postulate 3 and 4 can be easily seen using vector notation. Suppose $|\psi_1\rangle$ and $|\psi_2\rangle$ are defined as:

[1] $U^\dagger = (U^T)^*$, the complex transpose and conjugate (also called Hermitian adjoint) of U

[2] Definition of vector tensor product is given below, and at the same time an intuition of this postulate is provided.

$$|\psi_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, |\psi_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

$(a_i)_i$ and $(b_i)_i$ are complex coordinates, then $|\psi_1\rangle \otimes |\psi_2\rangle$ is a $n \times m$ vector defined by:

$$|\psi_1\rangle \otimes |\psi_2\rangle := \begin{pmatrix} a_1 |\psi_2\rangle \\ \vdots \\ a_n |\psi_2\rangle \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_m \\ a_2 b_1 \\ \vdots \\ a_n b_m \end{pmatrix}$$

If we consider the square of the coordinates $(a_i)_i$ of $|\psi_1\rangle$ as a probability distribution (the fact that $|\psi_1\rangle$ is an unit vector for the inner product norm hints us to do so) and see $|\psi_1\rangle$ as a superposition of basis states $(|i\rangle)_i$, $|\psi_1\rangle = \sum_{i=1}^{n} a_i |i\rangle$, the state $|i\rangle$ has probability $|a_i|^2$ of being observed. This is consistent with Postulate 3, because what we have just done is implicitely define a complete family of measurements, $M_i = |i\rangle \langle i|$.

Similarly, we define a second basis $(|i'\rangle)_j$ such that $|\psi_2\rangle = \sum_{i=1}^{m} b_i |i'\rangle$. Then $|\psi_1\rangle \otimes |\psi_2\rangle$ is a superposition where the state $|1\rangle \otimes |1'\rangle$, also noted $|11'\rangle$ for simplicity, has probability $|a_1 b_1|^2$ of being observed. Therefore, the tensor product defines a "natural superposition principe" for quantum mechanics.

We suggest to refer to [24] for a complete introduction to the postulates of quantum mechanics and quantum formalism.

The next section presents a selection of more advanced concepts in quantum mechanics. They will be used to establish our results, later in this report. For better understanding, we provide an illustration of these concepts in Section 1.4.

1.3 Quantum States and Superoperators

A useful mathematical tool to describe quantum states are **mixed** states, which are ensembles of pure states. A system is in the mixed state $\{|\psi_i\rangle, p_i\}_{i=1..n}$ if it is in the pure state $|\psi_i\rangle$ with probability p_i. Let N be the dimension of $\mathcal{H}$. Mixed states are conveniently represented by a **density matrix**, which is a complex positive semidefinite (all eigenvalues greater than or equal to zero) $N \times N$ matrix of trace 1, defined by

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| .$$

A pure state $|\psi\rangle$ is represented by $\rho = |\psi\rangle \langle\psi|$. We denote by $\mathcal{D}(\mathcal{H})$ the set of density matrices of states in the complex Hilbert space $\mathcal{H}$. A revelant basis for $\mathcal{D}(\mathcal{H})$ is $\{|e_i\rangle \langle e_j| \, , i, j = 1, .., N\}$ where $(|e_i\rangle)_i$ is an orthonormal basis of $\mathcal{H}$, which can be identified with $\mathbb{C}^N$ or $\mathbb{R}^{2N}$, and therefore induce a matrix notation.

Note that the postulates of quantum mechanics can be reformulated with density matrices instead of pure states. Density matrices describe a quantum syatem whose state is not completely known, which is the most common scenario encountered in quantum mechanics. This is the reason why this formalism is used in any result involving quantum computation.

We now introduce the concept of separability for density matrices, which plays a central role in quantum computing, and specially in the problems we consider.

Consider a quantum system $\mathcal{H}$ described by two subsystems $\mathcal{H}_1$ and $\mathcal{H}_2$. By the fourth postulate of quantum mechanics, the Hilbert space describing this system is $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Let $N = \dim \mathcal{H}_1 \dim \mathcal{H}_2$, then $\mathcal{H}$ is a N-dimensional space consisting of elements of the form:

$$\sum_{|h_1\rangle \in \mathcal{H}_1, |h_2\rangle \in \mathcal{H}_2} \alpha_{h_1,h_2}(|h_1\rangle \otimes |h_2\rangle)$$

The state ρ acting on the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is called **separable** if

$$\rho = \sum_{i=1}^{k} p_i \rho_i^{(1)} \otimes \rho_i^{(2)}$$

where $\{p_i\}_i$ are probabilities and $\rho_i^{(k)}$ are states on $\mathcal{H}_k$.

A state which is not separable is **entangled**.

The most general type of operation on quantum states, in other words a discrete-time transformation of the physical system, can be described by a linear map called a **superoperator**:

$$\begin{aligned} \Phi : \ & \mathcal{H} \to \mathcal{H}' \\ & \rho \mapsto \rho' \end{aligned}$$

Note that $\Phi : \ \mathcal{H} \to \mathcal{H}'$ is notation abuse, as ρ is a density matrix representing an ensemble of pure states in $\mathcal{H}$. The correct definition is $\Phi : \ \mathcal{M}_{\mathcal{H}} \to \mathcal{M}'_{\mathcal{H}}$, but the former is shorter and often used in the literature [1].

Two commonly used distances measures are the Frobenius distance and the trace distance, which are equivalent as long as the Hilbert spaces we consider are finite-dimensional, and defined from the following norms. (ρ^* denotes the complex conjugate of ρ, and $tr(M)$ is the sum of diagonal elements of M)

Frobenius norm $||\rho||_F = \sqrt{tr(\rho^* \rho)}$

Trace norm $||\rho||_{tr} = tr(\sqrt{\rho^* \rho})$

The trace norm is very useful in quantum mechanics for the following reason: if two density matrices are close in trace distance, then a quantum measurement performed on those quantum states will result in probability distributions which are close together in the classical sense (for two probability distributions $(p_x)_x$ and $(q_x)_x$, $D(p,q) = \sum_x |p_x - q_x|$) [24]. Therefore, states close in trace distance are indistinguishable by measurement.

1.4 Entanglement

An intuition for the definition of entanglement is provided in [31], and is summarized here. Consider two different laboratories which are doing a quantum experiment. In laboratory A (resp. B), the quantum system is described by a state ρ_A (resp. ρ_B) acting on $\mathcal{H}_A$ (resp. $\mathcal{H}_B$). Therefore, by the fourth postulate of quantum mechanics, the global state of the experimental system is not in a classical product ($\mathcal{H}_A \times \mathcal{H}_B$) form, but is in a tensor product form $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. An operation performed by laboratory A can be described by a function (superoperator) of the form $\Phi_A \otimes \mathbb{1}$, and equivalently $\mathbb{1} \otimes \Phi_B$ for laboratory B. In 1935, Einstein, Podolsky and Rosen [11] noticed that if the global state of the system is chosen suitably, then an operation in laboratory A can change the system state in laboratory B.

For instance, consider the following situation, where both laboratories each have a single quantum bit. The global state of the system is chosen to be a superposition of pure states of qubits:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

Suppose that laboratory A measures its qubit on the basis $(|0\rangle_A, |1\rangle_A)$. This measurement corresponds to an operator of the form $\Phi_A \otimes \mathbb{1}$. By the third postulate of quantum mechanics, the state of the system will collapse to either $|0\rangle_A \otimes |0\rangle_B$ or $|1\rangle_A \otimes |1\rangle_B$, depending on the outcome of the measurement done at A. After, if laboratory B decides to do a similar measurement on its qubit, instead of finding that qubit B is $|0\rangle_B$ or $|1\rangle_B$ with probability 1/2, the outcome will always be the same as laboratory A. This holds even if both laboratories are arbitrarily far apart!

By taking advantage of this effect, it is possible with elementary quantum operations to transfert any given state in laboratory A to laboratory B, providing both of them are initially in a suitable global state. This led to the discovery of quantum teleportation [8], in 1993.

2 Quantum Computing

2.1 Quantum Computers

The quantum computer is a new computational model that has not been fully physically implemented yet. Since a classical computer is built using electrical circuits made of wires and logic gates, a quantum computer is defined with wires and elementary quantum gates over qubits, as described in [24]. Using a certain subset of quantum gates, it has been proved that quantum computers can simulate classical computers. A natural question arises: are they more powerful?

Some evidence tends to confirm that quantum computers are indeed more powerful than classical computers, however no formal proof exists. For instance, the quantum factoring algorithm [25] discovered by Shor in 1994 has a quantum polynomial time complexity, while known classical implementations of integer factoring have at best an exponential running time; yet, a polynomial classical algorithm may exist. Efficient quantum algorithms have been discovered for other problems, such as Grover's quantum search with quadratic speed-up [14] and Simon's hidden subgroup algorithm with exponential speed-up [26]. However, none of these problems have been proven to be classically unsolvable in polynomial time, so the problem remains: we do not know whether quantum computers are (exponentially) more powerful than classical computers.

In the last two decades, researchers have been interested in the new field of quantum complexity theory, to formally understand how powerful quantum computers are compared to classical computers.

2.2 Quantum Complexity Theory

Defining a quantum equivalent to the classical complexity theory is not straightforward. It is not obvious that Turing machines have a quantum counterpart, one reason is that qubits are not deterministic!

Quantum Turing machines were first defined by Deutsch [10] in 1985, then slightly modified by Bernstein and Vazirani [9]. Due to the nature of qubits, quantum Turing machines (QTM) are probabilistic, ie. acceptance of an initial configuration occurs with a certain probability. Therefore, QTM are the quantum equivalent of probabilistic Turing machines [3], and can be used to define quantum complexity classes similarly to classical probabilistic ones. We first review some relevant probabilistic classes in classical complexity theory.

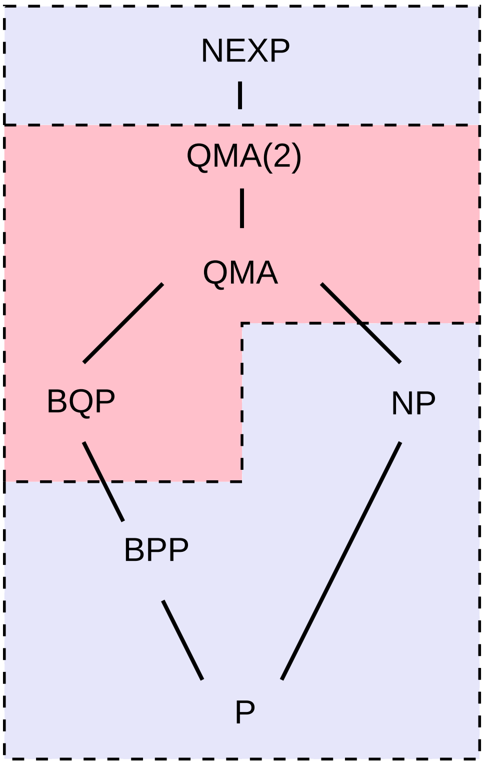

Figure 2: Known inclusions between complexity classes (note that some of them could be equalities). Classical complexity classes are in blue, quantum classes in red.

We define P as the class of all decision problems that are solvable by deterministic Turing machines in polynomial time. One could note that a large amount of decision problems that are not in P can still be solved efficiently, using a randomized algorithm, ie. a polynomial-time algorithm that outputs the correct answer with probability of at least 2/3. The complexity class of such problems is named BPP [3], after Bounded-error Probabilistic Polynomial-time.

In the same fashion, we define BQP the class of decision problems that can be solved in quantum polynomial time, with a correct answer probability at least 2/3. Whether BQP $\neq$ BPP is an open problem; solving it would tell us whether quantum computer are more powerful than classical computers.

This is the purpose of quantum complexity theory: discovering relations between complexity classes could immediately tell us what kind of problems can be efficiently solved with a quantum computer. For instance, Shor's algorithm gave evidence that NP $\cap$ co-NP problems (a class that contains the integer factoring problem) could be solved in quantum polynomial time. Known inclusions between the complexity classes we have seen (and some others to be introduced in the next section) are shown Figure 2.

2.3 Oracles

A useful tool in (quantum and classical) complexity theory, when one fails to prove relationship between two complexity classes, are *oracles*: one can give evidence of such relationship by proving a stronger result, such as "if problem X was easy to solve, then these complexity classes A and B are equal (resp. distinct)". Such assumption is called *relativization*, the problem or class of problems involved in the hypothesis are indifferently named oracle.

Formally, an oracle is defined as a black-box that solves a specific problem in constant time. We define A^{U} the complexity class of problems which belong to A if they are given an oracle that solves U. For instance, it is obvious that $\mathsf{NP} \subset \mathsf{P}^{\mathsf{NP}}$. Oracles have been applied to classical complexity theory to study the $\mathsf{P} = \mathsf{NP}$ question: Baker, Gill, and Solovay [6] showed that there exists an oracle A relative to which $\mathsf{P} = \mathsf{NP}$, and another oracle B relative to which $\mathsf{P} \neq \mathsf{NP}$. Therefore, oracles established that proving $\mathsf{P} \neq \mathsf{NP}$ will require *un-relativization* techniques, ie. techniques that are not affected by the presence of an oracle.

Quantum oracles have recently been introduced in [2] as a quantum generalization of classical oracles. Similarly, they model a quantum subroutine to which the quantum algorithm has black-box access. Examples of quantum oracles are given in the next section.

Proving an oracle separation, subset or equality can give some insight on the actual, non-relativized, relation between two classes. In the context of our internship, we seek to prove a quantum oracle separation between $\mathsf{QMA(2)}$ and QMA.

3 Quantum Merlin Arthur

In this section we introduce the class of problems that have recently gained attention within the quantum community, Quantum Merlin-Arthur (QMA) problems. They define a quantum analog of NP for quantum computers. Characterization of QMA problems will help us understand the limitations of quantum computing the same way we commonly see NP as a barrier for classical computers.

We first give a short introduction to this generalization. The complexity class NP can be viewed as an *interactive proof system* [12], ie. a prover and a verifier such that:

- The prover has unlimited computational power to compute a polynomial-size *proof* (also called *certificate*) according to the input.
- The verifier receives the proof and determines its validity in polynomial time. It accepts the proof (ie. answers "yes" to the decision problem) if and only if it is valid.

Merlin-Arthur problems have been introduced by Babai [4] in 1985 to generalize this interpretation of NP to a probabilistic viewer, instead of a deterministic one. This relates to our knowledge that randomized algorithms are more powerful than polynomial ones, ie. $\mathsf{P} \subset$

BPP. In MA problems, Merlin is the unbounded prover and Arthur has the computing power of randomized algorithms to verify proofs.

3.1 MA, QMA Classes

The complexity class MA is defined as the class of problems which can be solved by a Merlin-Arthur protocol:

- Merlin is a NP machine that computes a polynomial-size proof which is sent to Arthur.
- Arthur is a BPP machine which must verify the proof and accept it with probability at least 2/3 if it is true, or at most 1/3 if it is false.

It is straightforward to establish that NP $\subset$ MA [4], considering that P $\subset$ BPP.

Using the same intuition as MA, a natural generalization of NP to quantum computers leads to the definition of QMA [30]: Merlin computes a polynomial-size *quantum proof* and Arthur is a BQP machine. Formally, a quantum proof is a quantum register (ie. n qubits), which is the direct translation of the fact that a classical proof consists of n bits. It has been conjectured [21] that due to the *entanglement* (quantum correlation) that occurs between qubits, two quantum proofs of n unentangled qubits given separately could be more powerful than a single combined one. This leads us to define QMA(2) accordingly. QMA(2) consists of QMA problems where two unentangled proofs are provided by Merlin instead of one.

This is the subject of our internship: we aim at characterizing the expressive power of two quantum proofs, ie. whether QMA(2) equals QMA. This problem is motivated by the conjecture seen above, which led to the very definition of QMA(2). At first glance, one might think that quantum proofs are ”only” more powerful than classical proofs because qubits give exponentially more information than bits. Furthermore, one has never discovered a problem that can be solved with a quantum proof but not with a classical proof. However in the next section, we cite a publication that shows evidence that there might exist one, by using the concept of oracles defined before.

Eventually, proving that QMA(2) $\neq$ QMA would tell us that the power of quantum states is not only exponentiality, but also unentanglement.

3.2 Related work on QMA

In this section, we cover the state-of-the-art publications that are related to the QMA complexity class, with particular interest given to the ones that also concern QMA(2).

A reader who has only moderate tolerance for complexity theory may want to skip this section and continue reading from Section 4.

3.2.1 QMA and Classical Complexity

Many results are known about QMA: it is contained in PP [23], the class of decision problems solvable by a (classical) probabilistic Turing Machine in polynomial time, with an error probability less than 1/2. This result means that Quantum Merlin-Artur problems can only be "as hard" as problems that admit a classical probabilistic algorithm that gives the right answer with probability more than 1/2.

However, QMA is not likely to be equal to PP. Since PP is believed to be strictly larger than NP, this would establish that quantum computers flavor of NP (QMA) is more powerful than NP. For instance, it has been established that if QMA equals PP, then PP contains PH [28], where PH is a large class that generalize NP and co-NP, formally defined by all problems of the form "given an input x, does there exist a y such that for all z, there exists w.. such that $\phi(x, y, z, w, ..)$". Since the latter is strongly believed to be false [28], QMA is believed to be strictly contained in PP. This tells us that quantum NP problems are not impossible to solve with a classical computer: there always exists a classical probabilistic algorithm for them. The catch is that its acceptance probability may be arbitrarily close to 1/2.

QMA contains of course MA, but there also exists an oracle relative to which MA is strictly contained in QMA [30]. This result is another evidence of the power of quantum computers over classical computers.

These results give us a clear picture of where QMA stands in the classical complexity inclusion tree: above MA, and below PP. The question whether $\mathsf{QMA(2)} \subset \mathsf{PP}$ has, to the best of our knowledge, never been asked.

3.2.2 QMA and QCMA

In the previous section, we mentioned evidence of separation between quantum proofs and classical proofs. The class QCMA is defined as a subclass of QMA where a classical proof is given instead of a quantum one. Studying the power of two quantum proofs is intrinsically linked with the $\mathsf{QMA} \neq \mathsf{QCMA}$ question. If we could establish that a quantum proof does not give more information than a classical proof, then we could use the fact that receiving two classical proofs instead of one makes no difference; because we could just concatenate them [21]. In other words, $\mathsf{QMA(2)} = \mathsf{QMA}$ may be partially answered if one showed that $\mathsf{QMA} = \mathsf{QCMA}$. However, this is not likely to happen, considering the following.

In recent work [2], Aaronson and Kuperberg give evidence that $\mathsf{QMA} \neq \mathsf{QCMA}$ by building a quantum oracle relative to which this result holds. Whether a classical oracle separation can be achieved is still an open problem. The authors study the only candidate for such separation known in the literature, the Group Non-Membership (GNM) problem, proved to be in QMA [30] (for reference, this was the problem used to prove an oracle separation between MA and QMA in the previous chapter) . They give evidence that GNM is in QCMA, and therefore it could not be used to establish a classical separation between QMA and

QCMA. They furthermore conjecture that classical oracle separation can still be achieved and sketch a methodology to build a classical oracle from a quantum one.

3.2.3 QMA(2) and QMA

Since its introduction in 2001, the QMA(2) $\neq$ QMA question has not received much attention until recently. It has been first formulated by Kobayashi et al. in [21], where evidence that QMA(2) $\neq$ QMA were given. The authors show that quantum measurements cannot distinguish quantum correlation. However, this is not a strong complexity theoretic evidence, as Arthur can still apply quantum operations to Merlin's state without measuring it.

Recently, Aaronson et al. [1] showed that QMA(k) equals QMA(2) for any $k \geq 3$ if we assume the Additivity Conjecture, which is widely believed to be true in the quantum information theory community. This result means that providing any number of quantum proofs greater than 3 is strictly equivalent to providing only two quantum proofs. However, the proof breaks down for QMA(2) = QMA.

In [21], a soundness condition under which QMA(2) = QMA is given: Arthur has to accept a wrong proof with probability zero (but he can still decline correct proofs with probability lower than 1). Finally, evidence that QMA(2) $\subset$ PSPACE under a strong amplification conjecture is given in [1].

3.2.4 QMA-completeness

A few problems are known to be QMA-complete. In the context of our internship, these problems as such cannot help us, since we would rather be interested in QMA(2)-complete problems, but none exists to the best of our knowledge. However, they could give us hints on how to create a problem that would be in QMA(2) $\setminus$ QMA. We list some known QMA-complete problems:

- 2,3,5,8-local Hamiltonian problems, quantum analogues of SAT [18]. Interestingly, we note two facts: completeness proofs among k-local flavors use very different techniques; 3-local Hamiltonian can be modified to create a QCMA-complete problem (note that this does not prove QCMA = QMA).

- N-representability, a complex physics problem where one wants to minimize total energy while conserving specific properties of density matrices represented by N-particle wave functions [22]. A variant called "N-representability of pure states" is in QMA(2), but not known to be in QMA.

- Quantum clique [7].

- Quantum identity, ie. deciding whether a quantum circuit acts almost like the identity function, which can also be modified to create a QCMA-complete problem [22].

4 Our Results

We now present the approaches we used to investigate the $\mathsf{QMA(2)} \neq \mathsf{QMA}$ problem. This section makes use of the concepts introduced in Section 1.3. To avoid considering different norms, we slightly modify the definition of disentangler as introduced in [1]. In the following, we say that a state is *ϵ-close* to another if their Frobenius distance is less than ϵ.

Definition 1 ((ϵ, δ)-disentangler). *Let H and K be two finite-dimensional Hilbert spaces. Then given a superoperator $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$, Φ is an (ϵ, δ)-disentangler if*

1. *$\Phi(\rho)$ is ϵ-close to a separable state for every ρ, and*
2. *for every separable state σ, there exists a ρ such that $\Phi(\rho)$ is δ-close to σ.*

We now state the natural approach exposed in [1] to prove that $\mathsf{QMA(2)} = \mathsf{QMA}$. The authors note that, if for sufficiently small constants ϵ, δ there exists an (ϵ, δ)-disentangler with $\log \dim \mathcal{H} = O(\text{poly}(\log \dim \mathcal{K}))$, and if it can be implemented in quantum polynomial time, then $\mathsf{QMA(2)} = \mathsf{QMA}$. However, the following conjecture compromises this approach.

Conjecture 1 (Watrous Conjecture). *For all constants ϵ, $\delta < 1$, any (ϵ, δ)-disentangler requires* $\dim \mathcal{H} = 2^{\Omega(\dim \mathcal{K})}$.

It was proven in [1] that $(0, 0)$-disentanglers do not exist in any finite dimension, and the general case was left as an open question. In this section, we study (ϵ, δ)-disentanglers, where ϵ and δ depend on the dimension of the system.

4.1 Ruling Out Exponential-Error Approximate Disentanglers

We show that the existence of exponential-error disentanglers (in terms of ϵ and δ depending exponentially on $n = \log(\dim \mathcal{K})$, the number of qubits that describe the state space $\mathcal{K}$) is unlikely, as evidenced by the following theorem.

Theorem 4.1. *Suppose there exists a (ϵ, δ)-disentangler $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ with the following properties:*

1. $\dim \mathcal{H} = \textit{poly}(\dim \mathcal{K})$
2. $1/\epsilon = O(\textit{poly}(\dim \mathcal{K}))$ *and* $1/\delta = O(\textit{poly}(\dim \mathcal{K}))$

then $\mathsf{P} = \mathsf{NP}$.

We easily see that this result only concerns exponential-error disentanglers: when $1/\epsilon$ is set to be $O(\text{poly}(\dim \mathcal{K}))$, it is bounded by $2^{O(\text{poly}(n))}$ but not necessarily by $O(\text{poly}(n))$. The same reasoning applies to δ.

4.1.1 Proof of Theorem 4.1

We prove that the existence of such Φ enables us to solve two NP-hard problems, namely approximate separability and weak separation, in polynomial time.

Let us first define the approximate separability problem, (WMEM($S_{M,N}$)), which is a special case of the weak membership problem (WMEM(K)) for any compact and convex set K [13].

Definition 2 (Weak membership problem for K (WMEM(K))). *Given a rational vector $p \in \mathbb{R}^n$ and a rational $\delta > 0$, assert either that*

$$p \in S(K, \delta), \text{ or,} \tag{1}$$

$$p \notin S(K, -\delta) \tag{2}$$

where $S(K,\delta) := \cup_{x\in K} B(x,\delta)$ and $S(K,-\delta) := \{x \mid B(x,\delta) \subseteq K\}$.

Intuitively, $S(K,\delta)$ is the set of points that "almost belong to K" and $S(K,-\delta)$ is the set of points that are "deep in K".

It was proven that WMEM(K) is a NP-hard problem when $1/\delta$ is exponentially large (as a function of M and N) and $N \leq M \leq N(N-1)/2$ [15]. However, since $S_{M,N}$ is the set of separable states in $M \otimes N$, $\dim M$ is already exponentially large in terms of the number of qubits in the system ($n = \log_2 \dim M$). Therefore, such $1/\delta$ value would correspond to a superexponential-error disentangler, of less interest than exponential-error ones. Still, it is a first step towards proving a stronger result for exponential-error disentanglers.

To achieve a reduction to WMEM($S_{M,N}$), we use a well-studied class of algorithms: semidefinite programs [27]. The most general definition of semidefinite programs is as follows.

Definition 3 (Semidefinite Program (SDP)). *Given the vector $c \in R^m$ and Hermitian matrices $F_i \in \mathbb{C}^{n\times n}, i \in [|0,m|]$,*

$$\begin{aligned} \textit{minimize} \quad & c^T x \\ \textit{subject to:} \quad & F(x) \geq 0, \end{aligned}$$

where $F(x) = F_0 + \sum_{i=1}^m x_i F_i$.

Semidefinite programs can be solved efficiently in polynomial time $O(m^2 n^{2.5})$ [27].

Proposition 1. *Suppose there exists a (ϵ,δ)-disentangler $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ with the following properties:*

1. $\dim \mathcal{H} = \mathit{poly}(\dim \mathcal{K})$

2. $1/\epsilon = O(2^{(\dim \mathcal{K})})$ *and* $1/\delta = O(2^{(\dim \mathcal{K})})$

then WMEM($S_{N,N}$) can be solved in polynomial time.

Proof. The following SDP is used to solve an instance (ρ, δ') of WMEM$(S_{N,N})$ when a (ϵ, δ)-disentangler Φ with $\dim \mathcal{H} = poly(\dim \mathcal{K})$ and $\max(\epsilon, \delta) \leq \delta'$ is given.

$$\begin{aligned} \textit{minimize} \quad & ||\Phi(\sigma) - \rho||_{tr} \\ \textit{subject to:} \quad & \sigma \geq 0 \\ & tr(\sigma) = 1 \end{aligned}$$

Depending on the result of this SDP, answer $\rho \in S(S_{N,N}, \delta')$ if $min||\Phi(\sigma) - \rho||_{tr} \leq \delta' - \max(\epsilon, \delta)$; and $\rho \notin S(K, -\delta')$ otherwise. □

By making further use of Φ it is possible to solve an even harder problem than WMEM$(S_{M,N})$, namely WSEP$(S_{M,N})$, which is NP-hard for polynomial values of $1/\delta$ [17] (and therefore is related to exponential-error disentanglers). Again, this is a special case of a more general problem (WSEP(K)).

Definition 4 (Weak separation problem for K (WSEP(K))). *Given a rational vector $p \in \mathbb{R}^n$ and a rational $\delta > 0$, either*

- *assert that $p \in S(K, \delta)$, or,*

- *find a rational vector $c \in \mathbb{R}^n$ with $||c||_\infty = 1$ such that $c^T x < c^T p$ for every $x \in K$.*

where $S(K, \delta) := \cup_{x \in K} B(x, \delta)$

This problem not only asks whether p is weakly in K, but it also requires to provide a separating hyperplane (c) if it is not. With some effort, it can be proved that if we can solve WSEP then we can solve WMEM [13].

We prove that our disentangler Φ is powerful enough to solve the weak separation problem WSEP$(S_{M,N})$.

Proposition 2. *Suppose there exists a (ϵ, δ)-disentangler $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ with the following properties:*

1. $\dim \mathcal{H} = poly(\dim \mathcal{K})$

2. $1/\epsilon = O(poly(\dim \mathcal{K}))$ *and* $1/\delta = O(poly(\dim \mathcal{K}))$

then WSEP($S_{N,N}$) can be solved in polynomial time.

Proof. Consider an instance (ρ, δ') of WSEP$(S_{N,N})$. The following polynomial-time algorithm is used to solve the problem:

- Solve (ρ, δ') as an instance of WMEM$(S_{N,N})$.
- If the result is $p \in S(K, \delta')$, then terminate.
- If not, find c as the result of the following SDP:

$$\begin{array}{rc} \textit{maximize} & \rho^T c \\ \textit{subject to:} & \Phi(x)^T c + \delta < \rho^T c \\ & x \geq 0 \\ & tr(x) = 1 \\ & ||c||_\infty = 1 \end{array}$$

Such vector c always exists as a consequence of the Hahn-Banach theorem applied to the bounded convex set $S_{N,N}$. For every $\sigma \in S_{N,N}$, since Φ is a (ϵ, δ)-disentangler, there exists $x \in \mathcal{H}$ such that $||\sigma - \Phi(x)|| \leq \delta$. It follows that c verifies $\sigma^T c < \Phi(x)^T c + \delta < \rho^T c$, hence $c^T \sigma < c^T p$ for all $\sigma \in S_{N,N}$, and the algorithm terminates correctly. □

Theorem 4.1 follows from this proposition and the fact that WSEP$(S_{N,N})$ is NP-hard with polynomial error.

4.1.2 Discussion

We note that Theorem 4.1 was also independently known by Watrous, in unpublished works [29]. We should also stress that while our results only help ruling out exponential-error disentanglers and not other flavors, this is because little is known about the hardness of approximating separable states with logarithmic (corresponding to a polynomial number of qubits, hence polynomial-error disentangler) or constant error.

An interesting point can be made if we discuss the NP-hardness of WMEM$(S_{M,N})$ with constant-error:

- If WMEM$(S_{M,N})$ is NP-hard with constant-error, then Theorem 4.1 directly implies that constant-error (ϵ, δ)-disentanglers do not exist unless $\mathsf{P} = \mathsf{NP}$. Therefore, we would have strong evidence supporting Conjecture 1 and the disentangler approach to prove $\mathsf{QMA(2)} = \mathsf{QMA}$ would fail.
- If WMEM$(S_{M,N})$ is tractable with constant-error, it means that there exists an efficient algorithm that decides the separability of a state with constant-error. Arthur could

then use it to tell whether Merlin sends him an entangled state, and therefore does not need to rely on the QMA(2) promise that the state is separable. This supports the intuition that QMA(2) = QMA.

However, all the separability algorithms with constant approximation parameter that we are aware of have an exponential complexity [17].

4.2 Equivalence of Exponential-error Disentanglers

We have established the following result: to show the non-existence of exponential-error disentanglers unconditionnally, it suffices to prove it for any of those cases: (ϵ, δ), $(\epsilon, 0)$ or $(0, \delta)$.

4.2.1 Results

In this section, we use the following definitions and notations:

$\mathcal{H}$, $\mathcal{K}$ are respectively the input (output) Hilbert spaces of a disentangler

$\mathcal{D}(\mathcal{H})$ is the set of density operators in $\mathcal{H}$

S is the set of separables operators in $\mathcal{D}(\mathcal{K} \otimes \mathcal{K})$

d is the dimension of $\mathcal{K} \otimes \mathcal{K}$, $d := (\dim \mathcal{K})^2$

ρ^* is $I/(\dim \mathcal{K})^2$, the maximally mixed state[3] where I is the identity operator, and can be shown to be the center of S

δS is the boundary[4] of S

Let Φ be an (ϵ,0)-disentangler $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ and $\dim(\mathcal{H})$ is finite. Recall that the image of an (ϵ,0)-disentangler contains S. Let $\rho \in \mathcal{D}(\mathcal{H})$, and define $p(\Phi(\rho))$ as the point that belongs to the line $(\rho^*, \Phi(\rho))$ and that lies on the boundary δS of S. (ie. intersection of $\{(1-x)\Phi(\rho) + x\rho^*, x \in [0,1]\}$ and δS).

If $\Phi(\rho)$ is always very close to $p(\Phi(\rho))$, we could apply a small transformation to Φ to make its own image included in S, and hopefully obtain a $(0, \delta)$-disentangler. An illustration of this idea is provided in Figure 3.

The problem is, intuitively, that S could have very long spikes. The first lemma shows that, since there exists two balls B_1, B_2 such that $B_1 \subset S \subset B_2$, the image of Φ is either inside S, or not too far away from the boundary of S.

[3] In this section, ρ^* is not the complex conjugate of ρ, but is a specific state (the maximally mixed state) that has nothing to do with ρ. This misleading notation is commonly used.

[4] The notation δS is widely used, and has nothing to do with the δ of (ϵ, δ)-disentanglers.

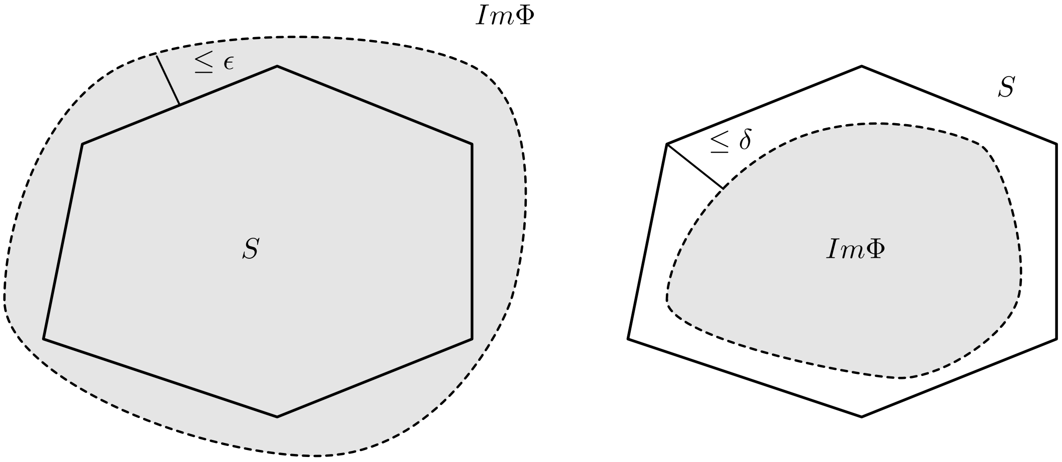

Figure 3: Sketch of an $(\epsilon, 0)$-disentangler and a $(0, \delta)$-disentangler. The gray region represents the image of the disentangler, which is a convex set. The set of separable states, S, is a convex and bounded set. This sketch is overly simplified and inaccurately represents high-dimensional objects.

Lemma 1.

$$||\Phi(\rho) - \rho^*|| \leq \alpha\epsilon + ||p(\Phi(\rho)) - \rho^*||$$

where $\alpha^2 := (R_2^2+\epsilon^2)/R_1^2$, $R_2 = \sqrt{(d-1)/d}$ *being the radius of the smallest ball containing* S *and* $R_1 = \sqrt{1/(d(d-1))}$ *the radius of the largest ball contained in* S *(both of them centered at* ρ^**, Gurvits results [16]), thus* $\alpha \leq \sqrt{2}d$*.*

The proof of all lemmas are left to the Appendix. Define $\tilde{\Phi}_{\epsilon'} = (1-\epsilon')\Phi + \epsilon'\rho^*$. Is it a $(0, \delta)$-disentangler? In other words, by how much do we have to "squeeze" the image of Φ so that if lies completely in S?

The following lemma gives a lower bound for ϵ'.

Lemma 2.

$$||((1-\epsilon')\Phi(\rho) + \epsilon'\rho^*) - \rho^*|| \leq ||p(\Phi(\rho)) - \rho^*||$$

if $\epsilon' \geq (1 + \dfrac{R_1}{\alpha\epsilon})^{-1}$

Define $\epsilon' := (1 + \dfrac{R_1}{\alpha\epsilon})^{-1}$, then we compare how far the image of $\tilde{\Phi}_{\epsilon'}$ is from Φ.

Lemma 3.

$$||(1-\epsilon')\Phi(\rho) + \epsilon'\rho^* - \Phi(\rho)|| \leq \alpha^2\epsilon$$

Since Φ is a $(\epsilon, 0)$-disentangler, $\tilde{\Phi}_{\epsilon'}$ is a $(0, (\alpha^2+1)\epsilon)$-disentangler.

Theorem 4.2. *Let* $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ *be an (*ϵ*,0)-disentangler. Then, we can construct a* $(0, \delta)$*-disentangler with* $\delta = (2(\dim\mathcal{K})^2 + 1)\epsilon$*.*

In the next theorem, we prove that an inverse transformation is also possible. For this, we need to show that the image of a $(0,\epsilon)$-disentangler is not only close to every separable states, but contains all the separables states except those close to the border of S. Then, we apply a similar transformation as before to obtain a $(\delta, 0)$-disentangler.

The following proposition, which can also be of independant interest, tells us that the image of a $(0, \epsilon)$ disentangler contains all the separable states that are not too close to δS.

Proposition 3. *Let $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ be an (0,ϵ)-disentangler. Then, any state of the form*

$$\rho = x\rho^* + (1-x)\sigma,$$

where $\sigma \in \delta S$ and $x \in [0, \frac{\epsilon}{R_1}]$ belongs to the image of Φ, ie. there exists ρ' s.t $\Phi(\rho') = \rho$.

Let $\epsilon_0 = \frac{\epsilon}{R_1}$. Again, $p(\Phi(\rho))$ is the point that belongs to the line $(\rho^*, \Phi(\rho))$ and that lies on the boundary of S. (ie. the intersection of $\{(1-x)\Phi(\rho) + x\rho^*, x \in [0,1]\}$ and δS).

Define $\tilde{\Phi}_{\epsilon'} = (1+\epsilon')\Phi - \epsilon'\rho^*$. From the following expressions:

$$p(\Phi(\rho)) = (1 + x(\rho))\Phi(\rho) - x(\rho)\rho^*$$
$$\tilde{\Phi}_{\epsilon'}(\rho) = (1+\epsilon')\Phi(\rho) - \epsilon'\rho^*$$

we notice that $\tilde{\Phi}_{\epsilon'}$ contains S iff $\epsilon' \geq x(\rho)$ for all ρ.

Lemma 4. *For all ρ, $x(\rho) \leq \frac{\epsilon_0}{1+\epsilon_0}$.*

Let $\epsilon' = \frac{\epsilon_0}{1+\epsilon_0}$.

Lemma 5.

$$||\tilde{\Phi}_{\epsilon'} - \Phi(\rho)|| \leq \alpha\epsilon,$$

with $\alpha := R_2/R_1$.

Therefore $\tilde{\Phi}_{\epsilon'}$ is a $((\alpha+1)\epsilon, 0)$ disentangler.

Theorem 4.3. *Let $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ be an (0,ϵ)-disentangler. Then, we can construct a $(\delta, 0)$-disentangler with $\delta = (\dim \mathcal{K}^2)\epsilon$.*

Finally, this result can be extended to (ϵ, δ)-disentanglers since Proposition 3 also holds for them.

Theorem 4.4. *Let $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ be an (ϵ, δ)-disentangler. Then, we can construct a $(\gamma, 0)$-disentangler.*

Proof idea.

- Use Proposition 1 to find $\epsilon_0 = \delta/R_1$.

- Define $\tilde{\Phi}_{\epsilon'} = (1+\epsilon')\Phi - \epsilon'\rho^*$.
- Prove that $S \subset \tilde{\Phi}_{\epsilon'}$ for $\epsilon' = \dfrac{\epsilon_0}{1+\epsilon_0}$, fix ϵ'.
- Because the image of Φ can now be ϵ-outside S, $||\tilde{\Phi}_{\epsilon'} - \Phi(\rho)|| \leq \epsilon'(R_2 + \epsilon)$
- $\tilde{\Phi}_{\epsilon'}$ is a $((1+\alpha)\epsilon + \epsilon^2, 0)$ disentangler.

□

4.2.2 Discussion

From these results, it follows that exponential-error disentanglers are equivalent to $(\epsilon, 0)$ or $(0, \delta)$-disentanglers, which have more interesting properties. For instance, a simple example for both of them is provided in [1].

Also, note that our results cannot be easily extended to polynomial-error disentanglers since the radius R_1 depends exponentially on the number of qubits, and is optimal.

Conclusion

In this report, we introduced quantum computing and quantum complexity theory. We then described the class of problems we are interested in, namely QMA, and discussed why studying them would increase our knowledge on the power of quantum computers. Specifically, our internship focuses on the whether QMA(2) equals QMA. We studied an approach to prove that QMA equals QMA(2) by using a quantum operation called disentangler, and gave evidence that such operation is not likely to exist. We obtained the following results:

1. A disentangler on poly(n) qubits that is exponentially precise does not exist unless P =NP. If one succeeds to prove that the problem of deciding whether a quantum state is entangled (WMEM$(S_{M,N})$) is NP-hard with constant error, then no poly(n) qubits disentangler exists unless P =NP.

2. Unconditionally, if we want to show that poly(n)-qubits and exponentially precise (ϵ, δ)-disentanglers do not exist, it suffices to show that $(\epsilon, 0)$ or $(0, \delta)$-disentanglers do not exist.

These results provide a step toward ruling out a proof that QMA equals QMA(2), therefore give an intuition that QMA $\neq$QMA(2). Furthermore, it is conjectured in [1] that the non-existence of poly(n) disentanglers could lead to an oracle separation between QMA and QMA(2).

We conclude by listing open problems for future work:

- Is the approximate separability problem (WMEM($S_{M,N}$)) NP-hard when the parameter δ is constant? If not, is the weak separation problem (WSEP($S_{M,N}$)) also not NP-hard?
- Can we prove (unconditionally) that with poly(n) qubits and exponential $1/\epsilon$ and $1/\delta$, $(\epsilon, 0)$ or $(0, \delta)$-disentanglers do not exist?
- More generally, can Conjecture 1 be proven?
- Then, if Conjecture 1 holds, is there an oracle separation between QMA and $\mathsf{QMA(2)}$?

References

[1] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor, *The power of unentanglement*, (2008).

[2] Scott Aaronson and Greg Kuperberg, *Quantum versus classical proofs and advice*, Theory of Computing **3** (2007), no. 7, 129–157.

[3] Sanjeev Arora and Boaz Barak, *Complexity theory: A modern approach*, Web draft, 2008.

[4] L Babai, *Trading group theory for randomness*, STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing (New York, NY, USA), ACM, 1985, pp. 421–429.

[5] László Babai, *Bounded round interactive proofs in finite groups*, SIAM J. Discret. Math. **5** (1992), no. 1, 88–111.

[6] J. Baker, T. Gill and Solovay, *Relativizations of the p =? np question*, SICOMP: SIAM J. Comput., 1975.

[7] S. Beigi and P. W. Shor, *On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels*, ArXiv e-prints **709** (2007).

[8] C Bennett, G Brassard, C Crepeau, R Jozsa, A Peres, and W Wootters, *Teleporting an unknown quantum state via dual classical and EPR channels*, Phys Rev Lett (1993), 1895–1899.

[9] Ethan Bernstein and Umesh Vazirani, *Quantum complexity theory*, SIAM J. Comput. **26** (1997), no. 5, 1411–1473.

[10] David Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London Ser. A **A400** (1985), 97–117.

[11] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev. **47** (1935), no. 10, 777–780.

[12] S. Goldwasser, S. Micali, and C. Rackoff, *The knowledge complexity of interactive proof systems*, SIAM J. Comput. **18** (1989), no. 1, 186–208.

[13] Martin Grötschel, Lászlo Lovász, and Alexander Schrijver, *Geometric Algorithms and Combinatorial Optimization*, second corrected edition ed., Algorithms and Combinatorics, vol. 2, Springer, 1993 (English).

[14] Lov K. Grover, *A fast quantum mechanical algorithm for database search*, 1996, pp. 212–219.

[15] Leonid Gurvits, *Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement)*, 2002.

[16] Leonid Gurvits and Howard Barnum, *Largest separable balls around the maximally mixed bipartite quantum state*, 2002.

[17] Lawrence M. Ioannou, *Computational complexity of the quantum separability problem*, Quantum Information and Computation **7** (2007), 335.

[18] Julia Kempe, Alexei Kitaev, and Oded Regev, *The complexity of the local hamiltonian problem*, SIAM J. Comput. **35** (2006), no. 5, 1070–1097.

[19] H. Kobayashi and K. Matsumoto, *Towards EXP Upper Bound for Multi-Proof QMA of Perfect Completeness*, ERATO conference on Quantum Information Science (2003).

[20] H. Kobayashi, K. Matsumoto, and T. Yamakami, *Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?*, ArXiv Quantum Physics e-prints (2003).

[21] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami, *Quantum certificate verification: Single versus multiple quantum certificates*, CoRR **quant-ph/0110006** (2001), informal publication.

[22] Y. . Liu, M. Christandl, and F. Verstraete, *N-representability is QMA-complete*, ArXiv Quantum Physics e-prints (2006).

[23] Chris Marriott and John Watrous, *Quantum arthur-merlin games*, CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity (Washington, DC, USA), IEEE Computer Society, 2004, pp. 275–285.

[24] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, October 2000.

[25] Peter W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, IEEE Symposium on Foundations of Computer Science, 1994, pp. 124–134.

[26] David R. Simon, *On the power of quantum computation*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Los Alamitos, CA), Institute of Electrical and Electronic Engineers Computer Society Press, 1994, pp. 116–123.

[27] Lieven Vandenberghe and Stephen Boyd, *Semidefinite programming*, SIAM Rev. **38** (1996), no. 1, 49–95.

[28] Mikhail N. Vyalyi, *Qma=pp implies that pp contains ph*, Electronic Colloquium on Computational Complexity (ECCC) **10** (2003), no. 021.

[29] J. Watrous, *Personal communication.*

[30] John Watrous, *Succinct quantum proofs for properties of finite groups*, IEEE Symposium on Foundations of Computer Science, 2000, pp. 537–546.

[31] Karol Zyczkowski and Ingemar Bengtsson, *An introduction to quantum entanglement: a geometric approach*, 2006.

Appendix

Proof of Lemmas

Proof of Lemma 1. Let $\rho \in \mathcal{D}(\mathcal{H})$. Its image by Φ is ϵ-close to a separable state σ. Suppose that it $\Phi(\rho)$ is not inside S. We want to evaluate the distance d between $\Phi(\rho)$ and the intersection I of δS and the line $(\rho^*, \Phi(\rho))$. It is maximal when σ is as far as possible to ρ^*, ie. $||\sigma - \rho^*|| = R_2$.

Since S is convex and contains a ball B of separable states centered at ρ^*, S contains a segment starting at σ and ending at a point tangent to B. Let H be the orthogonal projection of $\Phi(\rho)$ to such segment, on the plane defined by $(\rho^*, \sigma, \Phi(\rho))$.

Using Figure 1, we define $d = ||\Phi(\rho) - I||$, $x = ||\Phi(\rho) - H|| \leq \epsilon$, $h^2 = ||IH|| = d^2 - x^2$, $R^2 = ||I - \rho^*||^2 \leq R_2^2 + \epsilon^2$.

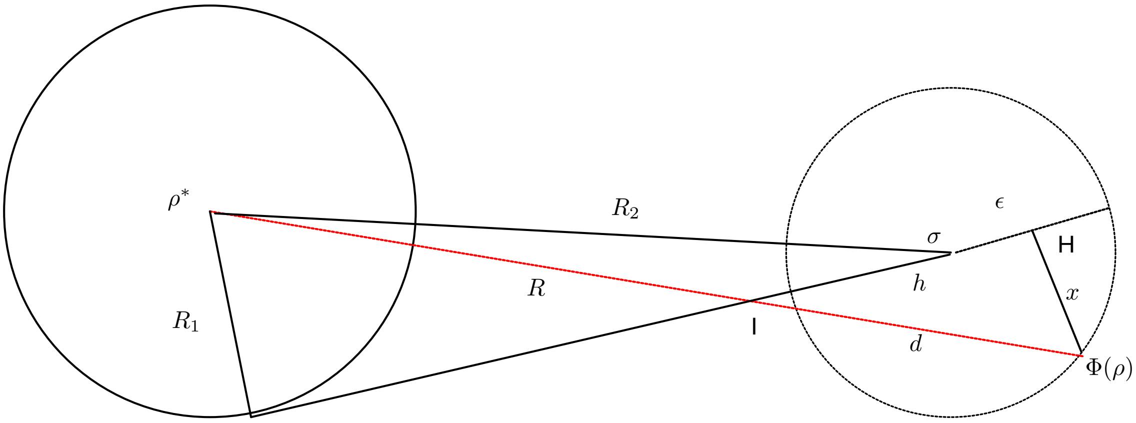

Figure 4: Sketch of geometric argument for Lemma 1

We have the following relation: $\dfrac{x}{R_1} = \dfrac{h}{\sqrt{R^2 - R_1^2} - h}$. Hence,

$$\begin{aligned} h &= \frac{x}{R_1}(\sqrt{R^2 - R_1^2} - h) \\ h(1 + \frac{x}{R_1}) &= \frac{x}{R_1}\sqrt{R^2 - R_1^2} \\ h^2 &\leq (\frac{R^2 - R_1^2}{R_1^2})\epsilon^2 \\ d^2 &\leq (\frac{R_2^2 + \epsilon^2}{R_1^2})\epsilon^2 \\ d^2 &\leq \alpha^2\epsilon^2, \end{aligned}$$

where $\alpha^2 := 2d^2$ since $\dfrac{R_2^2 + \epsilon^2}{R_1^2} = (\dfrac{d-1}{d} + \epsilon^2)(d(d-1)) \leq 2d^2$. □

Proof of Lemma 2.

$$\begin{aligned} ||((1-\epsilon')\Phi(\rho) + \epsilon'\rho^*) - \rho^*|| &\leq (1-\epsilon')||\Phi(\rho) - \rho^*|| \\ &\leq (1-\epsilon')(||\Phi(\rho) - p(\Phi(\rho))|| + ||p(\Phi(\rho)) - \rho^*||) \\ &\leq (1-\epsilon')(\alpha\epsilon + ||p(\Phi(\rho)) - \rho^*||), \end{aligned}$$

by the previous lemma. Therefore

$$||((1-\epsilon')\Phi(\rho) + \epsilon'\rho^*) - \rho^*|| \leq ||p(\Phi(\rho)) - \rho^*||$$

if

$$\begin{aligned}(1-\epsilon')(\alpha\epsilon+||p(\Phi(\rho))-\rho^*||) &\leq ||p(\Phi(\rho))-\rho^*|| \\ (1-\epsilon')\alpha\epsilon &\leq \epsilon'||p(\Phi(\rho))-\rho^*|| \\ \frac{\alpha\epsilon}{\alpha\epsilon+||p(\Phi(\rho))-\rho^*||} &\leq \epsilon'\end{aligned}$$

And by noting that $||p(\Phi(\rho))-\rho^*|| \geq R_1$, we obtain the lower bound. □

Proof of Lemma 3.

$$\begin{aligned}||(1-\epsilon')\Phi(\rho)+\epsilon'\rho^*-\Phi(\rho)|| &= \epsilon'(||\Phi(\rho)-\rho^*||) \\ &\leq \epsilon'(\epsilon+R_2) \\ &\leq \frac{R_2+\epsilon}{1+\dfrac{R_1}{\alpha\epsilon}} \\ &\leq \frac{(R_2+\epsilon)R_2^2\epsilon}{R_2^2\epsilon+R_1^2R_2}\end{aligned}$$

And since $R_2 \geq R_1$, $\dfrac{(R_2+\epsilon)R_2^2\epsilon}{R_2^2\epsilon+R_1^2R_2} \leq \dfrac{(R_2+\epsilon)R_2^2\epsilon}{R_1^2\epsilon+R_1^2R_2}$ and we obtain:

$$\begin{aligned}||(1-\epsilon')\Phi(\rho)+\epsilon'\rho^*-\Phi(\rho)|| &\leq \frac{R_2^2}{R_1^2}\epsilon \\ &\leq \alpha^2\epsilon\end{aligned}$$

□

Proof of Proposition 3. The image of Φ is a convex subset of S. For any state of S, there is a state in the image of Φ which is ϵ-close to it. It suffices to know how far this image can be from the border of S, to get an upper bound on the gap between the image of Φ and S.

Formally, we consider ρ as defined in the hypothesis.

$$||\rho-\sigma|| = x||\rho^*-\sigma|| \leq xR_2$$

Using a geometric argument similar to Lemma 1, we obtain the following bound when ρ is ϵ-close to δS.

$$||\rho-\sigma|| \leq \epsilon\frac{R_2}{R_1}$$

Therefore, for the latter bound to hold for all ρ's, a sufficient condition is $x \leq \epsilon/R_1$.

□

Proof of Lemma 4. This lemma consists in finding $x(\rho)$ as a function of ϵ_0. We re-write $\Phi(\rho)$ as:

$$\Phi(\rho) = \frac{1}{1+x(\rho)}p(\Phi(\rho)) + \frac{x(\rho)}{1+x(\rho)}\rho^*$$

Proposition 3 requires that $\frac{x(\rho)}{1+x(\rho)} \leq \epsilon_0$, then

$$x(\rho) \leq \frac{\epsilon_0}{1+\epsilon_0}.$$

□

Proof of Lemma 5.

$$\begin{aligned} ||\tilde{\Phi}_{\epsilon'} - \Phi(\rho)|| &\leq \epsilon' R_2 \\ &\leq \frac{\epsilon_0 R_2}{1+\epsilon_0} \\ &\leq \frac{R_2}{R_1}\epsilon \end{aligned}$$

□