Quantum Information Processing Final Report

Sharmila Duppala, Mackenzie Kong-Sivert, Juan Luque

Fall 2019

1 Introduction

Quantum information and computing has an interesting notion of proofs in complexity theory. In this project, we limit ourselves to QMA, a quantum analogue of the NP class with bounded error polynomial time verifier rather than a deterministic one. The notion of proof and an efficient verification is extended to the quantum setting along with a growing list of complete problems and different variants of the QMA (which might or might not be equal to the class QMA). As a preliminary study, we have studied an introduction to the QMA covering the quantum proofs, definitions of efficient quantum verification, the formalization of the class QMA illustrated using the group non-membership problem in quantum setting. Few QMA complete problems like (a, b)-QCS (Quantum Circuit Satisfiability) and the first QMA-complete problem, the local Hamiltonian problem are discussed. We would like to look further into the proof of the QMA completeness for local hamiltonian problem by [VW15] which is intuitively the quantum analogue of the Cook-Levin theorem. The error reduction procedures in classical verification can be handled by running the polynomial time verification procedure multiple times which doesn't exceed a polynomial time and the error bound improves up to required threshold value. However understanding the error reduction procedures seems like the core for the QMA. In subsequent readings we include understanding of the procedures like parallel error reduction and witness preserving error reduction.

The main topic we like to delve into is one of the variants of the QMA called Unentangled quantum proofs (QMA(2)) where a proof splits into two unentangled parts with respect to some bi-partition of the input (proof) k-qubits. Its not known if these two classes are equal or not. We would like to read the first paper on this [KMY01] which introduces quantum "multiple-Merlin"-Arthur proof systems in which Arthur uses multiple quantum proofs unentangled with each other for his verification. This paper also discusses the necessary and sufficient conditions to reduce a QMA(t) ($t \geq 3$) to QMA(2). This paper also says that having multiple provers doesn't increase the power of the QMAs in the case of soundness (in classical setting this class is called co-NP). The paper [HM13] solves some basic questions in this class which is QMA(t)= QMA(2) for ($t \geq 3$). Understanding more about this class by reading the above state of art papers is our short term goal.

With this project, we aim to read about the past research that has been done into quantum Merlin-Arthur structures, learn about the current state of research, and make some developments of our own. We have been guided towards some resources that may be useful to us in achieving this aim, and we have found some additional resources through our own efforts. Our first task, therefore, will be to sort through these sources and the information and insights they have to offer.

Upon closer inspection to these sources we will be better prepared to narrow down on specific outcome goals for the research project. For now topics we are interested in pursuing include: QMA(2), separability problem (testing whether a given quantum state is separable).

2 Preliminaries

The following are some preliminaries that are needed to understand quantum complexity. The notion of complexity is well defined in classical context and can be extended to quantum in the setting of prover and verifer. Usually, while doing complexity theory, we look at the decision problems where the output is binary, yes or no. This is because it makes analysis easier and without loss of generality, any optimization problem can also be restated as a decision problem. Using this, we can define a general function that can be used in the analysis $f : \{0,1\}^n \to \{0,1\}$ where $\{0,1\}^n$ is the set of all binary strings of length n. This can also be formulated in terms of formal languages where we can define a language, L for function f, where the input strings $x \in L$ iff $f(x) = 1$ i.e, $L = \{x : f(x) = 1\}$. Some examples of these languages can be PRIMES = $\{x$: x encodes a prime number$\}$ or FACTORING = $\{(x, y) : x$ has a factor between 2 and $y\}$. PRIMES is a natural decision problem, whereas FACTORING should be returning prime factor. But this works as we can use binary search to find y in time proportional to logarithmic of input size. We define some important classical complexity classes and understand the relationship between them. Then we proceed by observing how these classes behave when extended into a quantum setting.

2.1 Complexity Classes

Definition 2.1 (BPP)**.** *A language L belongs to BPP if the problem $x \in L$ is decidable in* poly(n) *time by a randomized algorithm.*

Henceforth, a randomized algorithm means a standard Turing machine that has access to a 'coin flipper', which can output 0 or 1 each with probability $\frac{1}{2}$.

We do not know whether there is a true random number generator in classical context. Hence we cannot say if P=BPP. But we can say P $\subseteq$ BPP. Decision, for this class, is usually taken to mean that $\Pr[output = 1 \mid x \in L] \geq \frac{3}{4}$ and $Pr[output = 0 \mid x \notin L] \leq \frac{1}{4}$. We see that the fractions 3/4 and 1/4 are arbitrary and can be amplified using the error amplification trick below.
We can see that $P \subseteq BPP$ is trivially true as any randomized algorithm can

run a deterministic algorithm by simply not flipping the coin or ignoring the coin flips.

Definition 2.2 (MA)**.** *A language L is in MA if there exists a polynomial time randomized verifier V such that*

- *(**Completeness**) $\forall x \in L$, $\exists z$ such that $\Pr[V(x,z)=1] \geq 2/3$*
- *(**Soundness**) $\forall x \notin L$, we have that $\forall z$, $\Pr[V(x,z)=1] \leq 1/3$.*

with $x \in \{0,1\}^n$ and proof $z \in \{0,1\}^{\mathrm{poly}(n)}$.

As MA is an extension of NP we have NP $\subseteq$ MA. Further, it is easy to observe that BPP $\subseteq$ MA since Arthur can simply ignore Merlin and solve the problem himself.

Now we make the transition to classes allowing the usage of Quantum Circuits.

Definition 2.3 (BQP)**.** *A language L belongs to the complexity class BQP if the decision problem has a quantum circuit Q that can be constructed in polynomial time satisfying*

- *(**Completeness**) $\forall x \in L$, $\Pr[Q(x)=1] \geq 2/3$*
- *(**Soundness**) $\forall x \notin L$, $\Pr[Q(x)=1] \leq 1/3$.*

It is also easy to see that BPP $\subseteq$ BQP (Bounded error, Quantum, Polynomial) since a quantum circuit can efficiently simulate a randomized algorithm. The relation between BQP and QMA is elaborated on in the next section.

Definition 2.4 (EXP)**.** *A language L is in the complexity class EXP if it is decidable by a deterministic algorithm in time $O(2^{\mathrm{poly}(n)})$.*

This next class is just an extension of EXP where we relax the deterministic requirement of the solver. Equivalently it can be defined in terms of having a deterministic verifier running in time poly(n).

Definition 2.5 (NEXP)**.** *A language L is in the complexity class NEXP if, and only if, there exists a deterministic verifier V that runs in time $2^{\mathrm{poly}(n)}$ and it satisfies*

- *(**Completeness**) If $x \in L$, $\exists y$ of length $2^{\mathrm{poly}(n)}$ such that $V(x,y)=1$*
- *(**Soundness**) If $x \notin L$, $\forall y$ of length $2^{\mathrm{poly}(n)}$ such that $V(x,y)=0$.*

NEXP is a trivial upper bound for QMA(2) (defined below) and also the best known upper bound of it.

3 QMA and the amplification problem

Instead of using Turing machines as a standardized model to define a verifier machine, we use

Definition 3.1 (QMA(c,s))**.** *A language L belongs to QMA(c,s)if there exists a BQP verifier V. That is,*

- ***(Completeness)*** *$\forall x \in L$, there exists a quantum state $|\psi\rangle$ such that $\Pr[V(x, |\psi\rangle) = 1] \geq c$*
- ***(Soundness)*** *$\forall x \notin L$, for all quantum states $|\psi\rangle$, $\Pr[V(x, |\psi\rangle) = 1] < s$*

where each proof $|\psi\rangle$ is $\text{poly}(x)$ qubits long.

One of the classes that we are interested in QMA (Quantum Merlin Arthur), an analogue of NP and MA. This class characterized the languages that can be solved using a quantum randomized circuit in polynomial time using a polynomial size proof. Similar to the famous results in the classical counterparts from the side of error amplification, we have results on error amplification in the quantum context as well. It is known that QMA is robust with respect to error bounds [KSVV02] which is stated formally in the theorem below.

Theorem 3.1. *Let $a, b : N \to [0, 1]$ and $q \in \text{poly}(n)$ satisfy,*

$$a(n) - b(n) \geq \frac{1}{q(n)}$$

for all $n \in \mathbb{N}$ then QMA(a,b) $\subseteq$ QMA($1 - 2^{-r}, 2^{-r}$) for every $r \in \text{poly}(n)$.

(The proof of theorems will be revisted for rigorous understanding in the next iteration of study). Marriott et.al, in [MW05] proves that for a single proof QMA, that completeness and soundness errors can be reduced exponentially without increasing the size of Merlin's proof. This reduction technique is also called witness preserving error reduction. This is formally stated as the theorem below.

Theorem 3.2. *Strong error reduction Let $a, b : N \to [0, 1]$ and $q \in \text{poly}(n)$ satisfy,*

$$a(n) - b(n) \geq \frac{1}{q(n)}$$

for all $n \in \mathbb{N}$ then $QMA_m(a, b) \subseteq QMA_m(1-2^{-r}, 2^{-r})$ for every $r, m \in \text{poly}(n)$.

Two applications of Theorem 3.2 are also stated in [MW05]. The first is a simplified proof that QMA is contained in the class PP i.e, $QMA \subseteq PP$ and $QMA_{\log} = BQP$. The proofs of this are also involved and will be rigorously understood in the next iteration of the study.

3.1 QMA Completeness

The first problem that is proved to be QMA is complete is the k-local Hamiltonian problem which is the quantum analogue of the MAX-k-SAT which is an NP-complete problem for $k \geq 2$ and is QMA-complete for $k \geq 3$. On the other hand, the 1-local Hamiltonian problem is in P. And the 2-local Hamiltonian problem is QMA-Complete [KKR04].

Definition 3.2. *An operator $H : B^{\otimes n} \rightarrow B^{\otimes n}$, where $B = \{0, 1\}$ on n qubits is a k-local Hamiltonian if H is expressible as $H = \sum_{j=1}^{r} H_j$ where each term is a Hermitian operator acting on at most k qubits.*

Now, we define the local Hamiltonian problem as follows

Definition 3.3. *Given $H_1, H_2, H_3, \ldots, H_r$ local Hamiltonians on n-qubits with $H = \sum_{j=1}^{r} H_j$ with $r \in \text{poly}(n)$. Each of the H_j has the norm bounded by a polynomial in the total number of qubits, i.e, $\|H_j\| = O(\text{poly}(n))$ and its entries are specified by $\text{poly}(n)$ size. In addition, there are two parameters c, s where $c < s$. For Yes instances, the smallest eigenvalue of H is at most c and for a No instance, the smallest eigenvalue of H should be at least s.*

We see that local Hamiltonian problem is a natural extension of the SAT problem, where each clause of the SAT instance, corresponds to one of the local Hamiltonians. All the false assignments to the clause should be penalized, hence the corresponding states of the local Hamiltonian will have positive eigenvalues. The constraints on the clause are being directly applied on the local Hamiltonians which gives the connection for the reduction between the two problems. We observe that a trivial upper bound of QMA is the class EXP. As the Hamiltonian on n-qubit system interactions can be represented using a $2^n x 2^n$ matrix whose smallest eigenvalue can be found in time polynomial in the input's size by the spectral decomposition. Hence we have QMA $\subseteq$ EXP. However, having a $\text{poly}(n)$ number of local Hamiltonians reduces our input size to $\text{poly}(n)$ introducing only $\text{poly}(n)$ constraints which is analogous to the Satisfiability problem.

4 QMA(2) and the power of Unentangled provers

A natural question to ask is, what happens in the case of multiple provers. In case of a classical complexity, multiple proofs are of no significance. However, the case of separable proofs is interesting as we see that QMA(2) $\subseteq$ QMA [] The class QMA(2) is first introduced by Kobayashi in [KMY01] with unentangled provers. Intuitively, multiple provers can help Arthur to make less mistakes. This is analogous to how the police often investigates multiple criminals to uncover the truth. There are some important properties of multiple prover class in quantum setting without any interaction. We discuss them after defining the class.

Definition 4.1 (QMA(2))**.** *A language L belongs to QMA(c,s)if there exists a BQP verifier V. That is,*

- ***(Completeness)*** *$\forall x \in L$, there exist quantum states $|\psi_1\rangle, |\psi_2\rangle$ such that* $\Pr[V(|x\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle) = 1] \geq c$
- ***(Soundness)*** *$\forall x \notin L$, for all quantum states $|\psi_1\rangle, |\psi_2\rangle$, we have* $\Pr[V(|x\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle) = 1] < s$

where each of the proofs $|\psi_1\rangle, |\psi_2\rangle$ is $\text{poly}(x)$ *qubits long.*

4.1 Power of unentanglement

It is conjectured that multiple provers QMA with non entangled promise is more powerful than QMA. Trivial bounds are QMA $\subseteq$ QMA(2) $\subseteq$ NEXP as Arthur can ignore one of the proofs and use only one proof to verify and give the output hence $QMA \subseteq QMA(2)$. $QMA(2) \subseteq NEXP$ comes from guessing exponential-size classical descriptions of the two quantum proofs, which is a trivial upper bound and known best bound. However, an interesting upper bound for it would be $QMA(2) =^? EXP$. Also we can ask if $QMA =^? QMA(2)$. In fact, there is a problem(pure state N-representibility problem) given by Liu et al, in [LCV07] that is in QMA(2) but not in QMA which makes it plausible that the class QMA(2) is strictly larger than QMA.

4.2 Results in QMA(2)

It is known that QMA(k)=QMA(2) which says that k provers can be reduced to 2 provers [HM12]. Other non trivial results include proving that 3SAT can be solved by QMA(2) using $O(\log n)$ size proofs from Merlin and $O(\sqrt{n})$ witnesses. This means that the size of input is $o(n)$, which would classically mean proving that Exponential time Hypothesis given by Impagliazzo and Paturi in [IP01], to be false.

4.3 Classes of bipartite measurement operators

There's an interesting line of work attempting to understand QMA(2) with restricted verification protocols [HM12]. We say a POVM(M,I-M) has following classes of measurement operators describes operators on $\mathbb{C}^d \otimes \mathbb{C}^d$

1. BELL : Systems are measured locally with no conditioning (independent measurements). $M = \sum_{(i,j)\in S} \alpha_i \otimes \beta_j$ where $\sum_i \alpha_i = I$ and $\sum_j \beta_j = I$ and S is set of pairs of outcomes. The verifier accepts the if we get a state that belong to S after independent local measurements.
2. LOCC1 : It is the set of M that can be realised by measuring the first system and then choosing a measurement on the second system conditional on the outcome of the first measurement. Such M can be written as

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

where where $\sum_i \alpha_i = I$ and $0 \leq M_i \leq 1$ for each i

3. LOCC: It is the set of M that can be realised by alternating partial measurements on the two systems a finite number of times, choosing each measurement conditioned on the previous outcomes. An inductive definition is that M is in LOCC if there exist operators $\{E_i\}, \{Mi\}$ with $\sum_i E_i \leq I$ and each $M_i \in LOCC$ such that either, $M = \sum_i (I \otimes \sqrt{E_i}) M_i (I \otimes \sqrt{E_i})$ or $M = \sum_i (\sqrt{E_i} \otimes I) M_i (\sqrt{E_i} \otimes I)$. For the base case, it suffices to take $I \in LOCC$.

4. SEP: It is the set of M such that

$$M = \sum_i \alpha_i \otimes \beta_i$$

for some positive semidefinite (WLOG rank one) matrices $\{\alpha_i\}, \{\beta_i\}$.

5. ALL: This class has no restrictions on M other than $0 \leq M \leq 1$

Currently, we are at the step of understanding these classes and how each of these restrictions can be used to understand the complexity of QMA(2) by seeing which of them influences the complexity of the class.

4.4 Results under the bipartite measurement operators

BellQMA protocols are a subclass of multi-prover quantum Merlin-Arthur protocols in which the verifier is restricted to perform nonadaptive, unentangled measurements on the quantum states received from each Merlin. Drucker and Chen in [CD10] gives BellQMA proofs of satisfiability problem with m clauses with constant gap in soundness, in which $O(\sqrt{m})$ merlins send proofs of length $o(\log m)$ qubits to Arthur. The below theorem explains the result formally.

Theorem 4.1. *[ABD$^+$08] proved that $3-SAT$ with m clauses can be solved using $\sqrt{m} poly \log m$ Merlins, where each Merlin sends a proof of size $O(\log m)$ qubits with perfect completeness and constant gap in the soundness. There is a BellQMA proof system which, given a 3-SAT instance with m clauses uses $O(\sqrt{m})$ Merlins, each of which sends $O(\log m)$ qubits. The proof system has completeness $1 - \exp\{\Omega(\sqrt{m})\}$ and soundness $1 - \Omega(1)$.*

It is a conjecture proposed by Aaronson et.al, in [ABD$^+$08] which strengthens the fact that 3SAT can have almost the same completeness and a constant soundness gap as above even under Bell measurements.

4.5 Open questions

Is there a non trivial upper bound on the class QMA(2) e.g. like $QMA(2) \subseteq EXP$? More about the QMA(2)-complete problems? More open questions in relation to the measurement operator classes, they will be discussed after the next reading.

References

[ABD+08] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 223–236. IEEE, 2008.

[CD10] Jing Chen and Andrew Drucker. Short multi-prover quantum proofs for sat without entangled measurements. *arXiv preprint arXiv:1011.0716*, 2010.

[HM12] Aram Harrow and Ashley Montanaro. Testing product states,quantum merlin-arthur games and tensor optimization. *ACM, 60(1):1–43*, 2012.

[HM13] Aram W. Harrow and Ashley Montanaro. Testing product states, quantum merlin-arthur games and tensor optimization. *J. ACM*, 60(1):3:1–3:43, February 2013.

[IP01] Russell Impagliazzo and Ramamohan Paturi. On the complexity of k-sat. *Journal of Computer and System Sciences*, 62(2):367–375, 2001.

[KKR04] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem, 2004.

[KMY01] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum certificate verification: Single versus multiple quantum certificates. *arXiv preprint quant-ph/0110006*, 2001.

[KSVV02] Alexei Yu Kitaev, Alexander Shen, Mikhail N Vyalyi, and Mikhail N Vyalyi. *Classical and quantum computation*. Number 47. American Mathematical Soc., 2002.

[LCV07] Yi-Kai Liu, Matthias Christandl, and Frank Verstraete. Quantum computational complexity of the n-representability problem: Qma complete. *Physical review letters*, 98 11:110503, 2007.

[MW05] Chris Marriott and John Watrous. Quantum arthur-merlin games, 2005.

[VW15] Thomas Vidick and John Watrous. *Quantum Proofs*. Foundations and Trends in Theoretical Computer Science, 2015.