CS 598QC Report

A distribution testing oracle separation between QMA and QCMA

Aman Singh

May 11, 2024

1 QMA vs QCMA

QMA is defined as the class of problems which can be solved using a BQP machine with an untrusted quantum proof of polynomially many qubits. On the other hand, QCMA defines a similar class of problems with the only difference being that the proof is a classical bit string of polynomially many bits. However, as with any interesting complexity classes, showing an unconditional separation between these classes is extremely hard. This is because P $\subseteq$ QCMA $\subseteq$ QMA $\subseteq$ PSPACE, and showing a language $L \in$ QMA but L $\notin$ QCMA would imply P $\neq$ PSPACE. So, a more approachable task would be to show a problem that is in QMA^O but not in QCMA^O for some oracle O.

For an n-bit boolean function O, a problem L^O is in the class QMA$^O(c,s)$ if there exist a uniform family of quantum circuits A^O which has oracle access to O through the unitary U^O that maps $U^O(|x,b\rangle) = |x, b \oplus O(x)\rangle$ for all $x \in \{0,1\}^n$ and is such that

- For each YES instance O, there is a $poly(n)$-qubit quantum state $|\zeta\rangle$ such that $A^O(|\zeta\rangle)$ accepts with probability greater than or equal to c.
- For each NO instance O, for all $poly(n)$-qubit quantum states $|\zeta\rangle$ the circuit $A^O(|\zeta\rangle)$ accepts with probability less than or equal to s.

QCMA$^O(c,s)$ is defined in a similar way except that the proof is a $poly(n)$ bit classical string. It is easy to show that the class QMA$^O(c,s)$ = QMA$^O(1-2^{-poly(n)}, 2^{-poly(n)})$ if $c - s \geq 1/poly(n)$. So, we collectively call all these equivalent complexity classes QMA^O. And similarly for QCMA^O.

Showing that QMA$^O \neq$ QCMA^O would give us evidence for the conjecture that quantum proofs are more powerful than classical proofs. A proof of such a statement would give us a no-go theorem for proving QMA = QCMA. Specifically, oracle separations tell us if a relativizing proof technique can't be used to prove the specific complexity classes same. It turns out that this too is difficult to prove and the current results we have prove oracle separations using different, non-standard oracle models.

It is interesting to note that what has also been conjectured is that QMA = QCMA in [2]. The reason behind this conjecture is that the verifier of the k-Local Hamiltonian Problem only tests the quantum

state to the reduced density matrices of five qubits. And perhaps if such states that are specified by short-range entanglement can be efficiently generated, then the k-Local Hamiltonian Problem can be proved to be in QCMA. This would imply QCMA = QMA as the k-Local Hamiltonian Problem is QMA-complete.

2 Prior Work

2.1 Unitary Oracle Separation

The first work which made progress in this problem was [1]. This showed that there is a quantum unitary oracle relative to which the classes are different. The gold standard of oracle separations is a classical binary function on n bits $f : \{0,1\}^n \to \{0,1\}$. Such a unitary oracle separation tells us that a proof for QMA = QCMA would have to use quantumly non-relativizing techniques.

The problem which is used to show the separation is to compute if the unitary oracle U on n qubits is the identity, i.e., $U = I$ or if it is a reflection across an unknown plane, i.e., $U = I - |\psi\rangle\langle\psi|$ for some secret state $|\psi\rangle$. It is easy to see that if the secret state is given as proof in the QMA algorithm, the verifier can decide if the unitary is identity or reflection. However, if the proof is limited to a polynomial-length string, it is difficult to see how it could distinguish between the unitaries using only polynomially many queries to the oracle. Observe that if there was no prover, this problem is equivalent to Grover's search which demands $\Omega(2^{n/2})$ oracle queries. The paper proves that any QCMA algorithm solving the problem with a m bit proof requires at least $\Omega(\sqrt{2^n/(m+1)})$ queries to the unitary oracle.

2.2 CPTP-map Oracle Separation

In [5], the problem they consider for showing a separation is the Preimage Checking problem. The Preimage Checking problem is a promise problem where. Here, given oracle access to a permutation on N^2 objects, the problem is to decide if the preimage of the first N elements under the permutation is either mostly even or mostly odd.

The oracle model we consider is a random in-place permutation oracle. This is a CPTP map which acts on density matrices. So, if there is a set of permutations $\bar{\sigma}$, the oracle would be

$$\mathbb{P}_\sigma(\rho) = \frac{1}{|\bar{\sigma}|}\sum_{\sigma\in\bar{\sigma}} P_\sigma \rho P_\sigma^\dagger$$

Here, for every σ, the in-place permutation oracle P_σ is defined as $P_\sigma(|i\rangle) = |\sigma(i)\rangle$.
(Note: The reason for randomizing the choice of permutation unitaries is that it is difficult to prove a separation without assuming structure on the classical witness. This is very similar to the reason for using distribution over classical oracles in the main result.)

This problem is in QMA as for permutation oracle σ, the preimage state $|S_\sigma\rangle$ where $S_\sigma = \{i : \sigma(i) \in [N]\}$ and a subset state $|S\rangle$ is defined to be $(1/\sqrt{|S|})\sum_{i\in S}|i\rangle$ can work as a witness. This is because for a valid witness, $P_\sigma(|S_\sigma\rangle) = |[N]\rangle$. Applying Hadamard gate on the first n qubits and

measuring on the standard basis is an easy way to verify the state after application of the in-place permutation oracle. We can also just measure the witness state on the standard computational basis and based on whether the answer is odd or ever, we would know if most of the preimages were odd or even with good probability.

However, we don't believe this problem is in QCMA as without the whole exponential-sized preimage subset, it is tough to see if it could work. The paper delves into the proof of this, which uses techniques that are actually similar to the main result discussed in the report. Briefly, the steps in the proof that no QCMA procedure can solve the Preimage Checking problem are:

1. As there are far more oracles than possible classical witnesses, there must be one classical witness $w*$ corresponding to a large number of oracles.
2. Each oracle is associated with a subset (preimage). So we have a large set of subsets that corresponds to $w*$. The proof shows that if we have a set of subsets of some large size, we can always find a subset of the original set that has a nice structure.
   (Note: this nice structure is called being $\alpha-$distributed. This nice set of subsets has a core that is in each subset and the rest of the elements are in a small fraction of subsets. This again is very similar to the definition of a sunflower in the main result.)
3. An adversary bound is applied to the subset with a nice structure to show that the number of queries needed is exponential.
4. Proof is completed using standard diagonalization argument.

3 Distribution Testing Oracle

The work done in [7] was the first to use a classical oracle in contrast to the previous works using quantum oracles. However, this also does not give us a n-bit boolean function oracle but does manage to prove a QMA-QCMA separation using a distribution of oracles.

3.1 Problem

The main problem analysed in the paper and used for proving the separation is the Expander Distinguishing Problem. This is a promise problem where, given oracle access to a graph G, the problem is to decide if the graph has a single connected component or multiple connected components. Each connected component of the graph is promised to be a α-expander. This problem can also be reformulated as deciding if the second highest eigenvalue of the normalized adjacency matrix of G, $\lambda_2 = 1$ or $\lambda_2 \leq 1 - \alpha$.

Oracle access to the graph is given via its adjacency matrix. The number of vertices in the graph is $N = 2^n$. The graph $G = (V, E)$ we consider will be undirected, d-regular and d-colored. Each edge from a vertex has a different color from all the other edges connected to the edge. So, the adjacency function is described as $G_c : V \times [d] \to V$. Similarly, quantum access to the classical function G_c is provided by the following oracle unitary A

$$G|v,k,z\rangle = |v,k,z \oplus G_c(v,k)\rangle$$

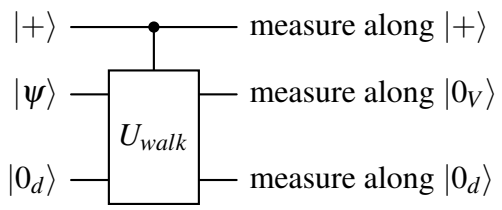
The $(\alpha, \zeta)-$Expander Distinguishing Problem is a promise problem where the input is an oracle G as described above. The problem is to distinguish between the cases described below, promised that one holds.

- YES: G has connected components of size at most $\leq \zeta$ and each component is α-expanding
- NO: G is an α-expander with a single connected component

In the paper, they take α to be a constant $\alpha = 1/(2 \cdot 10^8)$ and $\zeta \approx N^{9/10}$.

3.2 QMA algorithm

The $(\alpha, \zeta)-$Expander Distinguishing Problem can be solved by a simple QMA protocol with access to the oracle G through the unitary U_{walk} and proof state $|\psi\rangle$. Consider the following circuit



Here U_{walk} is a unitary that computes $U_{walk}|j,k\rangle|ancilla\rangle = |G_c(j,k),k\rangle|ancilla\rangle$ by accessing the adjacency list oracle unitary G twice. Additionally,

$$|0_d\rangle = (1/\sqrt{d}) \sum_{colors} |k\rangle$$
$$|0_V\rangle = (1/\sqrt{N}) \sum_{vertices} |j\rangle$$

We accept if the measurement along the control and control yields 1 but yields 0 along the witness. In all other cases, the circuit rejects. For the completeness, the paper shows that if G is a YES instance, there is a witness $|\psi\rangle$ of the form

$$|\psi_S\rangle = \sqrt{\frac{|T|}{N}}|S\rangle - \sqrt{\frac{|S|}{N}}|T\rangle$$

that accepts with probability 1. Here S is a connected component and $T = V - S$. The states $|S\rangle, |T\rangle$ are subset states meaning $|S\rangle = (1/\sqrt{|S|})\sum_{v\in S}|v\rangle$ and similarly for $ketT$. The reason for this is that: the probability of measuring $|+\rangle, |0_d\rangle$ is

$$Pr[+,0_d] = 1/4 + 1/4(\langle\psi|A^2|\psi\rangle) + 1/2(\langle\psi|A|\psi\rangle)$$

where A is the normalized adjacency matrix. And the above state $|\psi_s\rangle$ is an eigenvector of A with value 1 while also being perpendicular to $|0_V\rangle$.

For soundness, the paper shows using a proof by contradiction that the probability that the circuit accepts is at most $\leq 1 - \alpha/4$.

3.3 Non-deterministic Oracle Distinguishing Problem

The paper's authors do not prove that any QCMA circuit can't solve the $(\alpha, \zeta)-$Expander Distinguishing Problem. However, they manage to show that no QCMA circuit can solve the problem assuming the prover can only send in witness strings that depend only on subsets of vertices and not the edges. However, we can't assume the proof structure if we were to prove a separation. So, we can also present the result as an oracle separation if we allow a non-standard oracle model.

We consider distributions B_S and B_{NO} over graphs. B_S is a distribution over YES instance graphs such that there is a connected component C where $C \subseteq S$ and the size of S is slightly more than $N^{9/10}$. B_{NO} is a distribution over NO instance graphs. The problem now is to design an algorithm that can distinguish these distributions assuming that it is promised to be one of them. This is the non-deterministic Oracle Distinguishing Problem.

The catch is that the witness can only depend on the distribution and not the actual graph. The algorithm, though, still has oracle access to the graph. So, a QMA(c,s) algorithm solves the distribution version of the Expander Distinguishing Model if there exists a quantum circuit A^G such that

- For every YES instance distribution B_S, there exists a quantum state $|\psi\rangle$ of $poly(n)$ qubits such that
$$E_{G \in B_S} \ Pr[A^G(|\psi\rangle) accepts] \geq c$$
- For every NO instance distribution B_{NO}, for all quantum states $|\psi\rangle$ of $poly(n)$ qubits
$$E_{G \in B_{NO}} \ Pr[A^G(|\psi\rangle) accepts] \leq s$$

A QCMA(c,s) would have to satisfy the same conditions as above but with a $poly(n)$ length classical string as proof.

As the witness in the QMA algorithm $|\psi_S\rangle$ depends only on the vertex subset that forms a connected component, and the distribution gives the prover information about such a subset, the same algorithm works. Note that the subset S is only a superset of some connected component C, but it is close enough that it works out. For the QCMA algorithm, however, the same witness has to work for many graphs which only share a subset in common. This means the witness can only depend on the subset S, which is what we wanted.

3.4 Lower Bounds for QCMA algorithm

In this section, we list the steps used to prove that there is no QCMA protocol for solving the distributional Expander Distinguishing Problem by contradiction. Before that, we define a few useful terms.

- A (μ, ζ, t)-sunflower Λ is a set of subsets of V with the property that, first, there is a subset $F \subset V$ such that for all $S \in \Lambda$ we have that $F \subset S$ and $|S \leq t$. This is the core of the sunflower. Second, any vertex v in the sunflower that is not in the core F appears in a small fraction of the subsets, i.e., $Pr_{S \in \Lambda}[v \in S] \leq (\zeta/N)^{1-\mu}$.

- The paper defines distributions (and a way to generate them) $P_{M,1}$ which is an (effectively) uniform distribution over NO instances. $P_{M,l}(F)$ is an (effectively) uniform distribution over YES instances with high probability. This distribution also has the property that there is a connected component C such that $F \subseteq C$.
- B_S is restriction of $P_{M,l}(\{\})$ to graphs such that there is a $C \subseteq S$.
- H_Λ is a distribution over graphs where a subset S is uniformly sampled from Λ and then a graph is sampled from B_S.
- $\textcircled{F}$ is a called the ideal sunflower with core F. It is the set of subsets of size ζ but such that for each subset S, $F \subseteq S$. $H_{\textcircled{F}}$ is defined similarly - it is a distribution over graphs where a subset S is uniformly sampled from $\textcircled{F}$ and then a graph is sampled from B_S.
- B_{NO} is essentially just $P_{M,1}$ ($P_{M,1}$ is not a uniform distribution but can be made so using the un-queryable random bits trick)

We assume that there is a QCMA protocol distinguishing B_S and B_{NO}. The implications of this assumption are

1. From a counting argument, there is a sunflower Λ such that a BQP oracle machine distinguishes B_S for $S \in \Lambda$ from $P_{M,1}$.
2. This directly implies that a BQP oracle machine distinguishes H_Λ from $P_{M,1}$.
3. As no BQP oracle machine can distinguish H_Λ and $H_{\textcircled{F}}$, it implies that a BQP oracle machine distinguishes $H_{\textcircled{F}}$ from $P_{M,l}(F)$.
4. As $H_{\textcircled{F}}$ and $P_{M,l}(F)$ are statistically close, it implies that a BQP oracle machine distinguishes $P_{M,l}(F)$ from $P_{M,1}$.
5. With some modifications to the parameters, the above implies that a BQP oracle machine distinguishes $P_{M,l}(\{\})$ from $P_{M,1}$. This is the standard Expander Distinguishing Problem.

But we know that no BQP oracle machine can solve the Expander Distinguishing Problem from prior work ([3]) that proves the claim by the polynomial method. So, we have our contradiction as we manage to show the existence of a BQP oracle machine that solves the Expander Distinguishing Problem assuming a QCMA protocol for solving the distributed version of the Expander Distinguishing Problem.

The proof technique here seems similar to the prior work in [5]. Indeed it is, the authors remark that this result is an application of QCMA lower bounding techniques developed in the work [5] to the expander distinguishing problem (for BQP machines) originally studied in [3], resulting in proving an even stronger oracle separation between QCMA and QMA.

3.5 Problems with subset witness

There is clearly a problem with assuming a structure on the witness of the QCMA algorithm as the prover can send any sort of string as the proof. In this section, we see why assuming the classical proof to be a subset structure may not be the best idea for the Expander Distinguising Problem.

Consider a random d-regular graph with each connected component having n vertices. The probability of three randomly chosen vertices forming a triangle is around $(d/n)^3$. So the expected value of the number of triangles in a graph with z connected components will be

$$E[\text{no. of triangles}] \approx \frac{d^3}{n^3} \cdot \binom{n}{3} \cdot z \approx zd^3$$

So in the Expander Distinguising Problem, a YES instance would have many more triangles in expectation than a NO instance which would only have d^3, i.e., a constant number of triangles. The classical proof here could just be a list of some $poly(n)$ many triangles in the graph, and this can be easily verified as well.

Although the above witness would work in expectation, there can be triangle-free YES and NO instances that could still separate QCMA and QMA. However, there may be other combinatorial structures that could distinguish YES and NO instances and proving a lower bound against all of them is difficult. Despite these challenges, the authors of [7] conjecture that the Expander Distinguishing Problem is not in QCMA and hence is a candidate gold-standard oracle separation.

3.6 More details about QCMA non-inclusion proof

In this section, we say some more things about the proof of the distributed Expander Distinguishing problem not being in QCMA. The flow of the proof was outlined in a previous section and we talk about each step in more detail here.

1. *From a counting argument, there is a sunflower Λ such that a BQP oracle machine distinguishes B_S for $S \in \Lambda$ from $P_{M,1}$.*

Let's say that the proof is q-bit long. The total number of YES distributions this works for is $\binom{N}{\zeta}$ (as each YES distribution is defined by a subset of vertices). So, the most common witness w would work for $2^{-q}\binom{N}{\zeta}$ subsets, i.e., it can distinguish these many YES and NO distributions. When we have these many subsets, we can build a set of subsets with a sunflower structure - here we can build a $\Lambda = (\mu, \zeta, 2q/(\mu \log(N/\zeta)))$-sunflower. So, if we fix the witness to the algorithm we get a BQP oracle machine that distinguishes B_S for $S \in \Lambda$ from $P_{M,1}$.

2. *This directly implies that a BQP oracle machine distinguishes H_Λ from $P_{M,1}$.*

There exists a BQP oracle machine that distinguishes B_S for $S \in \Lambda$ from $P_{M,1}$. As it works for all B_S, it also would work if we sample graphs from H_Λ. So, a BQP oracle machine distinguishes H_Λ from $P_{M,1}$.

3. *As no BQP oracle machine can distinguish H_Λ and $H_{\textcircled{F}}$, it implies that a BQP oracle machine distinguishes $H_{\textcircled{F}}$ from $P_{M,l}(F)$.*

The reason why no BQP oracle machine can distinguish H_Λ and $H_{\textcircled{F}}$ is because of an adversary bound. The main lemma proved here is

For $\delta \leq 1/4$, any quantum query algorithm $(1-\delta)-$distinguishing the distributions H_Λ and $H_{\textcircled{F}}$ where Λ is a $(\mu, \zeta, 2q/(\mu \log(N/\zeta)))$-sunflower and F is the corresponding core, requires

$$\geq \frac{1}{2}(1-2\sqrt{2\delta(1-2\delta)})(1-4\delta)\sqrt{\left(\frac{N}{\zeta}\right)^{1-\mu}} \text{ queries}$$

The proof proceeds by first showing that the adversary bounds can be applied to a distribution over oracles that store a permutation that maps the set S to a known set $U = [\zeta]$ and its inverse. More precisely it shows that the distribution Π_Λ which is a uniform distribution of permutations that map $S \in \Lambda$ to U can only be distinguished from $\Pi_{\textcircled{F}}$ using exponentially many queries.

It then goes on to show an exponential query lower bound between distributions of graphs G_Λ and $G_{\textcircled{F}}$. Here G_Λ is formed by first uniformly sampling a graph G that has a connected component U. Then π is sampled from Π_Λ and $\pi(G)$ is output. The distribution $G_{\textcircled{F}}$ is similarly defined. It finally just translates this result into a proof of the main lemma by doing a more detailed analysis of the previous two exponential lower bounds.

4. *As $H_{\textcircled{F}}$ and $P_{M,l}(F)$ are statistically close, it implies that a BQP oracle machine distinguishes $P_{M,l}(F)$ from $P_{M,1}$.*

Both these distributions are extremely close. $H_{\textcircled{F}}$ is just when you uniformly sample from distribution B_S where S is a ζ sized subset chosen uniformly from N vertices given that is contains the F. $P_{M,l}(F)$ is a distribution over graphs that is chosen in a particular way described by the paper so that with high probability ($\geq 1 - O(N^{-3})$) the graph contains ζ sized connected components, but it is guaranteed to contain F in all the connected components. It is shown that the statistical difference among these distributions is $O(N^{-3})$, so we can just replace $H_{\textcircled{F}}$ with $P_{M,l}(F)$ in the argument.

5. *With some modifications to the parameters, the above implies that a BQP oracle machine distinguishes $P_{M,l}(\{\})$ from $P_{M,1}$. This is the standard Expander Distinguishing Problem.*

In this part, the main claim is that the set of points F from the same connected component is not a helpful witness. This is because, in the case of $P_{M,1}$ and $P_{M,l}(\{\})$ the connected components are expanding and therefore the verifier can just select a random subset of the points from a single connected component by taking a random walk starting from a random point (this is just the expander mixing lemma). So, if a query algorithm exists for distinguishing $P_{M,1}$ and $P_{M,l}(F)$, it can be used as a subroutine for distinguishing $P_{M,1}$ and $P_{M,l}(\{\})$ without any witness F. The formal statement mentioning the exact changes in parameters is:

Suppose there exists some F and a q_1-query quantum algorithm that ε_1-distinguishes the distributions $P_{M,1}$ and $P_{M,l}(F)$. Then there exists a q_2-query quantum algorithm that ε_2-distinguishes the distributions $P_{M,1}$ and $P_{M,l}$ with $q_2 = q_1 + O(N^{3/100})$ and $\varepsilon_2 = \varepsilon_1 - O(N^{-9/200})$.

So, if an algorithm making $o(N^{1/4}/\log N)$ queries existed for distinguishing $P_{M,1}$ and $P_{M,l}(F)$, then as $o(N^{1/4}/\log N) + O(N^{3/100}) = o(N^{1/4}/\log N)$, we would have a $o(N^{1/4}/\log N)$-query algorithm for distinguishing $P_{M,1}$ and $P_{M,l}$. This is not possible due to a proof using the polynomial method from [3]. So, no QCMA protocol distinguishes B_S and B_{NO}.

4 Other work

4.1 Classically accessible classical oracle

In the work [6], the authors show a classical oracle separation between QCMA and QMA. The catch however is that the oracle can only be accessed classically. The problem they use to show this is to check if in a string x of exponential size, at some hard-to-find indices labelled by (r,v) the bits at these locations, i.e., $x_{(r,v)}$ are all 1s or only 1 at a maximum of one-third of the locations.

The indices (r,v) are derived from the Yamakawa-Zhandary problem. This says that there exists a function $f^H : \{0,1\}^m \to \{0,1\}^n$ related to the oracle H. It is easy to invert f^H when given quantum access to H but provably hard with only classical access to H. The relevant indices (r,v) are such that $f^H(r) = v$. So, in the QMA algorithm, the prover can just send the state $|H\rangle$ making it easy to invert f_H and find which locations to query in string/oracle x. However, it is not possible to do this when only given a classical witness. Note that the string/oracle x is only accessed classically in the QMA protocol but for proving the impossibility for QCMA can only be done yet if you assume classical accesses to x.

Using this approach, the paper also manages to show the existence of a separation between QCMA and QMA relative to a distribution over oracles. The oracle here is quantumly accessible too so it matches the result from [7] (main result discussed in the report) using a simpler proof.

4.2 Bounded adaptivity quantum queries

The work [4] improves upon [6]. They show that there exists an oracle separating QCMA and QMA relative to an oracle that is classical and quantumly accessible but there is a bound on the number of rounds of adaptive queries that the algorithm can issue. In each such round, we can query the oracle $poly(n)$ times but only a maximum of $o(\log n/\log\log n)$ rounds are allowed. The problem now is to make this work for fully adaptive queries (even $poly(n)$ rounds allowed).

References

[1] Scott Aaronson and Greg Kuperberg. “Quantum Versus Classical Proofs and Advice”. In: (2006).

[2] Dorit Aharonov and Tomer Naveh. *Quantum NP - A Survey*. 2002.

[3] Andris Ambainis, Andrew M. Childs, and Yi-Kai Liu. “Quantum property testing for bounded-degree graphs”. In: (2010). DOI: 10.1007/978-3-642-22935-0_31.

[4] Shalev Ben-David and Srijita Kundu. *Oracle separation of QMA and QCMA with bounded adaptivity*. 2024.

[5] Bill Fefferman and Shelby Kimmel. *Quantum vs Classical Proofs and Subset Verification*. 2015.

[6] Xingjian Li et al. *Classical vs Quantum Advice and Proofs under Classically-Accessible Oracle*. 2023.

[7] Anand Natarajan and Chinmay Nirkhe. “A distribution testing oracle separation between QMA and QCMA”. In: (2022). DOI: 10.4230/LIPIcs.CCC.2023.22.