Separating QMA from QCMA with a Classical Oracle

John Bostanci* Jonas Haferkamp† Mark Zhandry‡

Abstract

We show that there exists a classical oracle relative to which QMA, the class of languages that can be decided by an efficient quantum verifier with a quantum witness, is separate from QCMA, the analogous class with a *classical* witness. Our separating oracle is derived from a new quantum query complexity problem called *spectral Forrelation*, which is the task of estimating the spectral norm of a "Forrelation" matrix between two sets that are accessible through membership queries. We prove that for a specific way of sampling random instances of the spectral Forrelation problem, any QCMA verifier will fail to decide the problem. As a part of our proof, we show that *relative-error* approximately k-wise independent functions are indistinguishable from uniformly random functions to quantum algorithms that make fewer than $k/2$ queries.

*Columbia University
†Harvard University
‡NTT Research

Contents

1 Introduction

The problem of finding a standard oracle separation between QMA (the class of problems that can be verified with a quantum computer and quantum proof) and QCMA (the class of problems that can be verified with a quantum computer and *classical* proof) is a central open problem in the field of quantum query complexity, and the first question mentioned in Aaronson's list of open problems in the field [Aar21]. The question of separating QMA from QCMA is, in some sense, similar to the following question:

Do quantum witnesses offer more power than classical witnesses?

This question was first posed by [AN02], and partially answered by [AK07], which provided a *quantum* oracle separation between the two classes.

However, one can argue that the quantum oracle separation of [AK07] does not fully resolve the question of an oracle separation between QMA and QCMA. First, classical oracle separations are considered more standard in the community, and so it is natural to ask for such a separation. More importantly, the oracle separation tells us less than we would desire from a resolution to this question. In particular, the problem of QMA versus QCMA asks whether *useful properties*[1] of the quantum witnesses can be written down using a number of bits polynomial in the number of qubits of the witness. It could be the case that if QMA = QCMA, the QCMA verifier for a QMA-complete problem would not be receiving a "verbatim" description of the quantum witness, e.g. a circuit preparing it, but rather some other classical information derived from the original quantum witness and instance. However, the oracle separation of [AK07] essentially enforces that the only useful property of the ground state is its full classical description, as the separating problem seems to require that the verifier knows about a specific Haar random state[2]. By forcing the oracle to be classical, one hopes to identify more meaningful reasons why useful properties – beyond the full description of a quantum witnesses – should be hard to write down. A final reason for studying the problem of a classical oracle separation is that the question lies in the rich field of quantum query complexity and has been linked to open questions in quantum cryptography, such as the existence of quantum money [Lut11, NZ24] and pseudo-randomness against quantum adversaries [LMY24]. One hopes that finding a classical oracle separation between QMA and QCMA will provide an improved understanding of these fields.

An early candidate classical oracle separation was given by [Lut11], but the candidate lacked a proof. More recently, a number of results have made progress towards the goal of a classical oracle separation by proving separations under different restrictions on how the oracle is accessed. [FK15] showed a separation assuming that the classical oracle is an "in-place permutation oracle", a non-standard model where the oracle irreversibly permutes the input state. [NN24] showed a separation assuming the QCMA witness is required to be independent of certain choices made in constructing the oracle. A very recent line of work has used quantum advantage relative to unstructured oracles [YZ24] to separate QMA from QCMA: [Liu22, LLPY23] gave a separation assuming the verifier can only make classical oracle queries, and more recently [BK24] gave a separation which allows the verifier to make quantum queries, but assumes the adaptivity of the

[1] By "useful" we mean useful to a specific QMA verifier, but this is not meant as a formal statement.

[2] The notion of "knowing" the state is intuitive, rather than formal, due to the result of [INN+21], where it is shown that having an oracle that solves the separating problem of [AK07] does not allow one to synthesize the state specified by the oracle.

queries is sub-logarithmic. Despite this recent progress, a standard classical oracle separation that makes no constraints on how the oracle is accessed or how the witness is created still remains open.

The central challenge in separating QMA from QCMA relative to a classical oracle seems to be the following. Consider a language in QMA $\setminus$ QCMA and consider measuring the QMA witness in the computational basis. The resulting string must *not* be accepted by the QMA verifier, otherwise it would be a classical witness for the language, putting it in QCMA. Therefore, in some sense, the QMA verifier needs to verify that the witness is in superposition. In order for such verification using only a classical oracle, existing approaches require highly structured oracles. But then to actually prove that the language is outside of QCMA, we need a quantum query complexity lower-bound, and the techniques we have are often not amenable to highly structured oracles. Additionally, any witness would naturally be treated as a form of oracle-dependent advice about the oracle, and most quantum query complexity techniques are not very good at distinguishing between quantum advice and classical advice. In other words, if a typical technique succeeded in proving that a language is outside of QCMA and it can not distinguish between quantum and classical advice, it would likely show the language it outside of QMA as well, failing to give a separation.

Motivated by this seemingly dual requirement of having to apply quantum query complexity tools to highly structured oracles, a pair of works, [Zha24] (which this work subsumes) and [LMY24], have shown connections between the QMA versus QCMA problem and *pseudorandomness* against quantum adversaries. [LMY24] propose a conjecture about the pseudorandomness of δ-dense permutations, and prove that this implies a classical oracle separation between QMA and QCMA. Previously, [GLLZ21] prove that the δ-dense conjecture implies the long-standing Aaronson-Ambainis (AA) conjecture [AA09], meaning the AA conjecture would need to be resolved in order to make the separation in [LMY24] unconditional. We nevertheless believe that the results and the statistical conjecture of [LMY24] remain interesting, even in light of this result, since showing that the oracle of [LMY24] works to separate QCMA and QMA (either through their conjecture about δ-dense permutations or by different means) would provide an alternate oracle separation that sheds light on the Aaronson-Ambainis conjecture, which we do not believe our oracle separation does.

Our Work. We resolve this line of work by separating QMA and QCMA relative to a standard classical oracle. Our oracle separation is based on a new quantum query complexity problem, and appears much less structured than prior work[3], and is more amenable to existing quantum query complexity techniques. In particular, we prove that our distribution over oracles satisfies a strong notion of being an approximate k-wise independent distribution, and prove that this notion of relative error k-wise independence is indistinguishable from truly random distributions even to quantum adversaries.

Organization. In Section 4, we show that distributions over functions satisfying closeness to k-wise independent functions in a *relative* sense are indistinguishable from random functions to quantum query algorithms. This fact is crucial to our proof and we believe that it may be of independent interest to readers, but the proof is self contained and uses separate techniques than the rest of the paper, so a reader who is only interested in the oracle separation may take the result for granted and read past this section. In Section 5, we define the spectral Forrelation problem, which is the oracle-input problem we study. We also construct hard instances of the spectral Forrelation problem, relative-error Fourier-independent distributions. Finally, in Section 6, we show how relative-error

[3]Although this is an intuitive statement, rather than a formal one

Fourier independent distributions imply an oracle separation between QMA and QCMA using the properties of relative-error Fourier-independent distributions and the result of Section 4.

2 Technical overview

In this section, we provide a high level overview of our separating oracle and the proof that it provides a separation between QMA and QCMA.

2.1 Our separating oracle: spectral Forrelation

For two sets S and $U \subseteq [N]$, we can define a "Forrelation" matrix over $\mathbb{Z}_N$ to be $\mathrm{F}_{S,U} = \Pi_U \cdot \mathsf{QFT}_N \cdot \Pi_S$, where QFT_N is the quantum Fourier transform over $\mathbb{Z}_N$ and $\Pi_S = \sum_{x \in S} |x\rangle\langle x|$, $\Pi_U = \sum_{x \in U} |x\rangle\langle x|$ are the projectors onto the elements of S and U respectively. Then the (α, β)-SpectralForrelation problem is the problem of, given access to membership oracles for (S, U) as "input", to determine whether $\|\mathrm{F}_{S,U}\|^2$ is larger than β, or smaller than α promised that one of these two is the case, where $\|A\|^2 = \max_{\||\psi\rangle\|=1} \{\langle\psi| A^\dagger A |\psi\rangle\}$ is the squared spectral norm of A. We will typically take $\beta - \alpha$ to be inverse-polynomial. See Section 5.1 for a formal definition of (α, β)-SpectralForrelation. We will often abuse notation and refer to S (and U) as both the set and the membership oracle for the set.

There is a natural QMA verifier for the (α, β)-SpectralForrelation problem (for inverse polynomial gap), which receives a state $|\psi\rangle$, measures that is entirely supported on elements of S, then applies the QFT to the state and measures whether the resulting state is supported on U, accepting if both membership checks accept. It is clear to see that this verifier, given the top eigenvalue of $\mathrm{F}_{S,U}$, accepts YES instances with probability β, and that for all states, this verifier accepts NO instances with probability at most α. Note that this can be amplified to the standard $(\frac{2}{3}, \frac{1}{3})$-definition of QMA for any inverse polynomial promise gap.

Remark 2.1. The name SpectralForrelation comes from the observation that the task of estimating the spectral norm of $\Pi_U \cdot \mathsf{QFT} \cdot \Pi_S$ is reminiscent of the Forrelation problem [AA15, Aar10], which is roughly the task of estimating $\langle +^n | U_f \cdot \mathsf{QFT} \cdot U_g | +^n \rangle$, where U_f and U_g are the phase oracles corresponding to two Boolean functions (and the QFT in the original Forrelation problem is over $\mathbb{Z}_2^n$). Both tasks require estimating some notion of correlation between a function and the Fourier transform of another function, although spectral Forrelation involves a maximization over all input states whereas the Forrelation problem has a fixed starting state.

2.2 Spectral Forrelation does not have QCMA verifiers

The bulk of our work is showing that there are instances of $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation that can not be solved by QCMA verifiers (although α could be taken to be any number with inverse-polynomial gap from β, and β could be taken to be any constant less than $\frac{3}{4}$). Our basic ideas for finding these instances is as follows. We first sample a set $S \subseteq [N]$ where N is exponentially-sized in the input size n. S will be chosen to only contain a negligible fraction of $[N]$, but still be super-polynomial sized. We will also sample a random state $|\psi\rangle = \sum_{y \in S} \alpha_y |y\rangle$ supported on S. The state will be our witness state for the $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation problem.

To construct U, let $|\hat{\psi}\rangle$ be the quantum Fourier transform applied to $|\psi\rangle$. Observe that if $|\psi\rangle$ has support on a single point y, then $|\hat{\psi}\rangle$ will have uniform amplitude on all points in $[N]$

(though with complex phases on these points). On the other hand, for a random $|\psi\rangle$ with support on the large set S, the amplitudes on different points will vary. Concretely, while the expected squared-amplitude on any point $z \in [N]$ is $1/N$, there is a reasonable chance that it could be, say, smaller than $1/2N$ or larger than $2/N$. We will choose U to be a subset of $[N]$ consisting of points where $|\hat{\psi}\rangle$ has squared-amplitude somewhat larger than $1/N$. Then we will have that the total squared-amplitude of $|\hat{\psi}\rangle$ on points in U is roughly $3/4$ (making this a YES instance of the spectral Forrelation problem), while $|U|/N$ is roughly $1/2$. In this case, the QFT of any *classical string* y will only have squared-amplitude on U of $1/2$. Thus, in some sense U certifies that $|\psi\rangle$ is in superposition over classical inputs (as opposed to a single classical input). We will also see that for our way of sampling U, (S', U) will be a NO instance of $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation for all S' whose size is smaller than a fixed super-polynomial function, which will be important for showing QCMA hardness.

We now need a way to argue that these instances of $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation do not have QCMA witnesses. For now, let us simply focus on the problem of determining whether S is suitably large or not. As noted before, there are no witnesses when S is small, so if a QCMA verifier can not distinguish between a large and small S (for the same U), they will not be able to solve the $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation problem. We previously showed that a single classical string $y \in S$ cannot serve as a witness, but this alone does not preclude some more clever way of attesting to S being large. In particular, the witness w could contain several points of S. Worse, perhaps queries to U may reveal a significant amount of information about S, which may help in deciding if S is large or small.

Consider a hypothetical QCMA verifier V which is given a classical witness w, and makes quantum queries to S, U, and accepts in the case where S is large. We want to show that we can replace S with a small set S' that V will still accept with too high a probability, meaning it incorrectly claims that (S', U) is in the language, despite S' being small. To that end, we will chose S' to be all points in S that are also "heavy" among the queries V makes to S. That is, points $y \in S$ such that the query amplitude in V's quantum queries to S is above some inverse-polynomial threshold. As the total query amplitude of all points is just the number of queries of V and hence polynomial, the number of heavy y is also polynomial. Hence, this set S' is small. We can also construct S' efficiently: for each heavy y, running V and measuring a random query will have an inverse polynomial chance of producing y. By repeating this process a polynomial number of times, we can collect all heavy queries.

By why should S and S' be indistinguishable to V? By standard quantum query analysis, if V can distinguish S from S', then it's queries must place significant amplitude on $S \setminus S'$. By measuring a random query, we therefore obtain with significant probability, a $y \in S \setminus S'$. But since y is not heavy, repeating this process many times will product many different y. This means that if V can distinguish S from S', it must actually be able to generate essentially arbitrarily large (but still polynomial) numbers of $y \in S$. Denote the number of y that V is able to generate by L.

Verifiers that do not query U. Let us first consider a hypothetical verifier that makes no queries to U. In this case, we can argue that any distinguishing V actually violates known query complexity results for multiple Grover search. In particular, [HM23] show that any algorithm making polynomially-many queries to a random sparse S can not produce L points in S except with probability bounded by 2^{-L} (see Lemma 3.5 for a precise statement). Now, this result assumes that no advice is provided about S, but the witness w counts as advice. Fortunately, we can handle this advice using the strong exponential lower bound provided by [HM23]. Consider running the

process above to generate S' with a *random* w' instead of the real witness w. If the verifier actually distinguishes between S and S' when given witness w, in the event that $w' = w$, the process will produce L points in S. This happens with probability $2^{-|w|}$. By setting $L \gg |w|$ (since L can be an arbitrarily large polynomial), we therefore obtain an algorithm with no advice that produces L points in S with probability $2^{-|w|} \gg 2^{-L}$, contradicting the hardness of multiple Grover search.

Remark 2.2. The argument above inherently uses the fact that the witness is classical. If V had a quantum witness/advice, running it even once and measuring a random query to find a $y \in S$ would potentially destroy the witness, meaning further runs of V are not guaranteed to produce any points in S. This is the key place in the proof where we distinguish between classical and quantum witnesses.

Verifiers that query a k-wise independent U. The above strategy does not work for handling queries to U. The reason is that U takes potentially N bits (which is exponential in the input size) to describe, meaning treating U as advice would require setting $L \gg N$, at which point the bounds from [HM23] do not apply.

However, we can first assume that U is k-wise independent for a super-polynomial k, even conditioned on S (but not $|\psi\rangle$, whose correlation with U is crucial for the correctness of our QMA verifier). A result of [Zha15] shows that a k-wise independent U is perfectly indistinguishable from a uniformly random U for all quantum query algorithms making at most $k/2$ queries. Since k is super-polynomial, we thus obtain perfect indistinguishability against all polynomial-query algorithms, including our process for generating many points in S. Consequently, the process succeeds in generating L points in S even in U is replaced by a uniformly random U independent of S. But such a U can be simulated without knowledge of S at all, and thus the lower bound of [HM23] actually applies to algorithms making queries to the uniformly random U. Thus, under the assumption that U is k-wise independent, we can justify QCMA hardness.

Verifiers that query relative error ϵ-approximate k-wise independent U. Our U will not be exactly k-wise independent, but we will be able to show that U satisfies a very strong notion of *relative error* approximate k-wise independence, even conditioned on S. In particular, we mean that for every subset $T \subseteq [N]$ of size at most k, and every subset $R \subseteq T$, we have that for some negligible ϵ,

$$(1-\epsilon) \cdot 2^{-|T|} \leq \Pr[T \cap U = R] \leq (1+\epsilon) \cdot 2^{-|T|}.$$

The issue in our previous argument is that [Zha15] only applies to the case of *perfect* k-wise independence, and there are even counter-examples showing this kind of result can not hold for *additive error* approximate k-wise independence. However, the story is different for relative errors. In particular, we show that our notion of relative error approximate independence implies that the $k/2$'th moment operators of U and a uniformly random function satisfy a relative error bound in CP ordering. This, combined with the idea of [SHH24] for showing that relative error bounds in CP ordering are indistinguishable to quantum query adversaries, implies that our U *are* indistinguishable from a uniformly random function to all polynomial-query algorithms. Thus, we can apply the previous argument, swapping out U for a uniformly random function and applying the lower bound from [HM23].

3 Preliminaries and notation

A function $f(n) \leq n^{O(1)}$ is *polynomial* and $f(n) \geq n^{-O(1)}$ is inverse polynomial. Functions $f(n) \geq n^{\omega(1)}$ are superpolynomial and $f(n) \leq n^{-\omega(1)}$ are negligible. We will sometimes use the notation $\mathrm{negl}(n)$ to denote an unspecified negligible function in n.

Let $\mathsf{Bernoulli}_p$ denote the distribution over $\{0,1\}$ which outputs 1 with probability p. Let $\mathsf{Bernoulli}_p^N$ denote the distribution over $\{0,1\}^N$ consisting of N iid samples from $\mathsf{Bernoulli}_p$. We will associate $\{0,1\}^N$ with subsets of $[N]$, where $S \subseteq [N]$ is associated with the vector $\mathbf{v}$ such that $v_x = 1$ if $x \in S$. We will also associate $\{0,1\}^N$ (and hence also subsets of $[N]$) with functions from $[N]$ to $\{0,1\}$, where S is associated with its indicator function f, where $f(x)$ is 1 if and only if $x \in S$.

A joint distribution $X_1, \cdots X_n$ is k-wise independent if, for each subset T of size at most k, $(X_i)_{i\in T}$ are independent random variables. $X_1, \cdots, X_n$ is k-wise *uniform* independent if each $(X_i)_{i\in T}$ are independent uniform random variables over their respective domains.

Complex Normal Distribution. Let $\mathcal{N}^{\mathbb{C}}_{\mu,\sigma}$ denote complex normal distribution with width σ. The probability density function of this distribution is given by $\Pr[x \leftarrow \mathcal{N}^{\mathbb{C}}_{\mu,\sigma}] = \frac{1}{\pi\sigma^2} e^{-|x-\mu|^2/\sigma^2}$.

Two basic identities that will be useful when computing integrals involving complex normal distributions are the following. Let $\mathbf{v}$ is a vector of n complex numbers, $\mathbf{M}$ is a complex $n \times n$ matrix, and $\int_{\mathbb{C}} d\mathbf{v}$ means to integrate over all complex vectors $\mathbf{v}$. Then

$$\int_{\mathbb{C}} e^{-\mathbf{v}^\dagger \mathbf{M} \mathbf{v}} d\mathbf{v} = \frac{\pi}{\det(\mathbf{M})} \qquad \int_{\mathbb{C}} |v_1|^2 |v_2|^2 e^{-\mathbf{v}^\dagger \mathbf{M} \mathbf{v}} d\mathbf{v} = \frac{\pi^2 \mathrm{Tr}(\mathbf{M})^2}{4 \det(\mathbf{M})^3} \text{ for } n = 2$$

Quantum computation. We assume the reader is familiar with the basics of quantum computation and quantum query models. Recall that in the standard model for making quantum queries to a classical oracle $\mathcal{O}$, the algorithm submits a state $\sum_{x,y,z} \alpha_{x,y,z} |x,y,z\rangle$, and receives back $\sum_{x,y,z} \alpha_{x,y,z} |x, y \oplus \mathcal{O}(x), z\rangle$. We will make use of the quantum Fourier transform, denoted QFT_N, defined on computational basis states as $|y\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{z\in\mathbb{Z}_N} e^{i2\pi yz/N} |z\rangle$ for $y \in \mathbb{Z}_N$. We will usually drop the subscript N as it will be clear from context. For a quantum state $|\psi\rangle$, we will typically let $|\hat{\psi}\rangle$ be shorthand for $\mathsf{QFT}|\psi\rangle$. For a state $|\psi\rangle$, we use the notation $\||\psi\rangle\|$ to denote the 2-norm, $\sqrt{\langle\psi|\psi\rangle}$. For an operator A, we use the notation $\|A\|$ to denote the spectral norm (sometimes called the operator norm), $\max_{\||\psi\rangle\|=1} \{\|A|\psi\rangle\|\}$, and $\|A\|_1$ to denote the 1-norm, $\mathrm{Tr}(|A|)$. We also use the notation $\mathrm{Re}(\alpha)$ to denote the real component of a complex number α.

3.1 Defining QMA and QCMA relative to oracles

We can consider two types of oracle versions of complexity classes, and in particular QMA/QCMA. The first, and the typical way to define these classes, is to specify an infinite oracle $\mathcal{O} : \{0,1\}^* \to \{0,1\}$, and define the classes QMA/QCMA relative to $\mathcal{O}$. The second version, which is typically easier to work with, is to consider a variant of QMA/QCMA where the instance itself is an exponentially-sized oracle $\mathcal{X} : \{0,1\}^n \to \{0,1\}$. Fortunately, we show that a QMA/QCMA separation for one variant immediately gives such a separation for the other variant. Thus, it suffices to prove a separation for whichever variant is most convenient.

Definition 3.1 (Oracle-Aided QMA/QCMA)**.** *For a function $\mathcal{O} : \{0,1\}^* \to \{0,1\}$, an oracle decision problem is a subset $\mathsf{L}^{\mathcal{O}} \subseteq \{0,1\}^*$ which depends on $\mathcal{O}$. We say that $\mathsf{L}^{\mathcal{O}}$ is in $\mathsf{QMA}^{\mathcal{O}}$ if there exists a polynomial-time oracle-aided quantum algorithm $V^{\mathcal{O}}$ and polynomial p such that:*

- *For every $x \in \mathsf{L}^{\mathcal{O}}$ of length n, there exists a state $|\psi\rangle$ on $p(n)$ qubits such that $\Pr[V^{\mathcal{O}}(x, |\psi\rangle) = 1] \geq 2/3$. In this case, we say that $V^{\mathcal{O}}$* accepts *x.*
- *For every $x \notin \mathsf{L}^{\mathcal{O}}$ of length n, and for any state $|\psi\rangle$ on $p(n)$ qubits, $\Pr[V^{\mathcal{O}}(x, |\psi\rangle) = 1] \leq 1/3$. In this case, we say that $V^{\mathcal{O}}$* rejects *x.*

$\mathsf{QCMA}^{\mathcal{O}}$ *is defined analogously, except that the states $|\psi\rangle$ are required to be classical.*

Definition 3.2 (Oracle-Input QMA/QCMA)**.** *Let $\mathcal{U} = \{\mathcal{U}_n\}_{n \in \mathbb{Z}^+}$ where $\mathcal{U}_n$ are sets of strings $\mathcal{X}$ of length $2^{n^{\Theta(1)}}$, interpreted as functions from $\mathcal{X} : [n^{\Theta(1)}] \to \{0,1\}$. An oracle-input promise language is a subset $\mathsf{OI\text{-}L} \subseteq \mathcal{U}$. An oracle-input promise language $\mathsf{OI\text{-}L} \subseteq \mathcal{U}$ is in* OI-QMA *if there exists a polynomial-time oracle-aided quantum algorithm V and polynomial p such that:*

- *For every $\mathcal{X} \in \mathsf{OI\text{-}L} \cap \mathcal{U}_n$, there exists a $|\psi\rangle$ on $p(n)$ qubits such that $\Pr[V^{\mathcal{X}}(|\psi\rangle) = 1] \geq 2/3$.*
- *For every $\mathcal{X} \in \mathcal{U}_n \setminus \mathsf{OI\text{-}L}$, and for any state $|\psi\rangle$ on $p(n)$ qubits, $\Pr[V^{\mathcal{X}}(|\psi\rangle) = 1] \leq 1/3$.*

OI-QCMA *is defined analogously, except that the states $|\psi\rangle$ are required to be classical.*

Note that the constants $1/3, 2/3$ in Definitions 3.1 and 3.2 are arbitrary, and can be replaced with a, b for any a, b such that $a \geq 2^{-\mathrm{poly}(n)}, b \leq 1 - 2^{-\mathrm{poly}(n)}$, and $b - a \geq 1/\mathrm{poly}(n)$ without changing the classes.

Given any countable collection of oracles $\mathcal{O}_1, \mathcal{O}_2, \cdots$ which may have finite or infinite domains, we can construct a single oracle $\mathcal{O} : \{0,1\}^* \to \{0,1\}$ by setting $\mathcal{O}(j, x) = \mathcal{O}_j(x)$, where (j, x) is some encoding of pairs $(j, x) \in \{0,1\}^* \times \{0,1\}^*$ into strings in $\{0,1\}^*$. We can likewise convert $\mathcal{O}$ back into $\mathcal{O}_1, \mathcal{O}_2, \cdots$. Therefore, we will take the definitions of QMA, QCMA, OI-QMA, OI-QCMA to allow for verifiers making queries to countable collections of oracles.

This next theorem is proved in Section A following a standard diagonalization argument, and shows that is suffices to give a separation for either variant of QMA, QCMA.

Theorem 3.3. *There exists a classical oracle $\mathcal{O}$ such that $\mathsf{QCMA}^{\mathcal{O}} \neq \mathsf{QMA}^{\mathcal{O}}$ if and only if* OI-QCMA $\neq$ OI-QMA.

The style of oracle separation between QMA and QCMA given in [AK07] follows that of Definition 3.1, except that they use a quantum oracle instead of a classical oracle. They do not formally define the oracle-input versions of OI-QMA and OI-QCMA or a general result like Theorem 3.3, but their proof implicitly uses similar concepts. In particular, they first define a universe of quantum oracles: namely, those that are either the identity or reflect around a Haar random state. They then show that the two cases can be efficiently distinguished via a quantum witness, but not a classical witness. This is effectively showing a separation between OI-QMA and OI-QCMA, except using quantum oracles instead of classical oracles. They then extend this to give a quantum oracle $\mathcal{Q}$ separating $\mathsf{QMA}^{\mathcal{Q}}$ from $\mathsf{QCMA}^{\mathcal{Q}}$. This can be seen as roughly corresponding to a transformation like in Theorem 3.3.

One slight non-triviality in generalizing their techniques to give a general equivalence is that a separation between OI-QMA and OI-QCMA only needs to show that, for any potential QCMA verifier, there is *some* instance that the verifier answers incorrectly. This is indeed how our separation is constructed. In contrast, [AK07] show that almost all instances will fool any QCMA verifier. This stronger separation is crucially used when constructing the oracle $\mathcal{Q}$ separating $\mathsf{QMA}^{\mathcal{Q}}$ from $\mathsf{QCMA}^{\mathcal{Q}}$,

as they can basically choose $\mathcal{Q}$ to be random from the appropriate universe of oracles. In order to get a general equivalence for arbitrary separations, including those like ours where the instance depends on the verifier, we have to work a bit harder and incorporate a diagonalization argument. Fortunately, this is standard.

3.2 Some useful quantum lemmas

Here we state some lemmas related to quantum query complexity that will be useful in our proof.

Lemma 3.4 ([BBBV97, Theorems 3.1 and 3.3]). *Let A be a quantum algorithm running making q queries to an oracle O. Let M_V denote the total magnitude squared of elements $y \in V$ in all queries made by A. Let $\epsilon > 0$ and let V be a set of inputs. If we modify O into an oracle O' which is identical to O except possibly on inputs in V, then $|\Pr[A^O() = 1] - \Pr[A^{O'}() = 1]| \leq 4\sqrt{qM_V}$.*

Lemma 3.5 ([HM23, Theorem 5.5]). *Let $p \in [0, 1]$. There is a constant $C \leq 48e$ such that the following is true. The success probability of finding K marked items in a random function $S : [N] \to \{0, 1\}$ where $S(x) = 1$ with probability p for each $x \in [N]$ is at most $(Cp(Q/K)^2)^K$ for any algorithm making $Q \geq K$ quantum queries to S.*

4 Indistinguishability of relative error k-wise independent functions

Here, we give a notion of a distribution being "close" to k-wise independent, for a relative error. The usual notion of "biased" or "almost" k-wise independence asks that every k-wise marginal is additively ϵ-close to uniform, for a negligible ϵ. This notion of closeness to k-wise independence is indistinguishable from a truly random distribution to any classical-query algorithm making at most k queries. However, it is not hard to come up with counterexamples showing that the notion of closeness is *not* sufficient for an analogous quantum statement. Consider the following example.

Example. *Consider the distribution over functions implied by the hidden shift problem (also known as Simon's problem).*

$$\textsc{HiddenShift} = \text{uniform}\left(\{f : \{0,1\}^n \mapsto \{0,1\}^n : \exists s \in \{0,1\}^n . f(x) = f(x \oplus s)\}\right) .$$

It is known that on every choice of k queries, the output of a random function from HiddenShift is $\left(\frac{2k}{2^{n+1}-k^2}\right)$-close to the output of a random permutation [Cle11]. It is further known that for all k, a random permutation is $O(\frac{k^2}{2^n})$-approximate k-wise independent [CN08].[4] *Since the additive errors in the k-wise independence add, HiddenShift is $O\left(\frac{k}{2^n-k^2} + \frac{k^2}{2^n}\right)$-approximate k-wise independent for all k. Setting $k = 2^{n/3}$, we find that HiddenShift is a $O(2^{-n/3})$-approximate $2^{n/3}$-wise independent distribution of functions.*

However, Simon's algorithm [Sim97] is a quantum query algorithm that distinguishes HiddenShift from a uniformly random permutation (or function) using $O(n)$ queries to the function.

We therefore give a much stronger notion of being close to k-wise independent, and show that it is sufficient to fool quantum query adversaries that make $k/2$ quantum queries to the approximately k-wise independent distribution.

[4] Note that these papers prove distinguishing bounds on unbounded classical adversaries that make k queries, but as noted before this exactly corresponds to the additive approximate error from a uniformly random function

Definition 4.1. *We say that a distribution over subsets U of $[N]$ is (k,ϵ)-wise independent with relative error if, for every set $T \subseteq [N]$ of size at most k and every subset $R \subseteq T$, it holds that*

$$(1-\varepsilon)2^{-|T|} \leq \Pr[T \cap U = R] \leq (1+\varepsilon)2^{-|T|}\,.$$

The main result of this section is following theorem:

Theorem 4.2. *Let U be drawn from a $(2k,\varepsilon)$-wise independent distribution in the sense of Definition 4.1. Then, for all quantum algorithms that make k queries to an oracle $\mathcal{O}_U$, the output state of the quantum algorithm when U is sampled from an exactly $2k$-wise independent function is at most ε-far in trace distance.*

Proof. We will use that the relevant moment super-operators satisfy relative errors in CP (complete positivity) ordering similar to the definition of relative error approximate designs as introduced in Ref. [BHH16]. The rest of the proof will then follow as in the proof of Lemma 5 in Ref. [SHH24]. Relative errors in CP ordering are equivalent to the following operator inequalities:

$$\begin{aligned}
(1-\varepsilon) \mathop{\mathbb{E}}_{U\sim\text{unif}} \left[(\mathcal{O}_U^{\otimes k} \otimes \mathrm{id}) \, |\Omega\rangle\langle\Omega| \, (\mathcal{O}_U^{\dagger,\otimes k} \otimes \mathrm{id}) \right] \\
\leq \mathop{\mathbb{E}}_{U\sim\nu} \left[(\mathcal{O}_U^{\otimes k} \otimes \mathrm{id}) \, |\Omega\rangle\langle\Omega| \, (\mathcal{O}_U^{\dagger,\otimes k} \otimes \mathrm{id}) \right] \\
\leq (1+\varepsilon) \mathop{\mathbb{E}}_{U\sim\text{unif}} \left[(\mathcal{O}_U^{\otimes k} \otimes \mathrm{id}) \, |\Omega\rangle\langle\Omega| \, (\mathcal{O}_U^{\dagger,\otimes k} \otimes \mathrm{id}) \right] . \qquad (1)
\end{aligned}$$

where $|\Omega\rangle = \sum_{\vec{x},\vec{a}} |\vec{x},\vec{a}\rangle \otimes |\vec{x},\vec{a}\rangle$ is the (un-normalized) maximally entangled state. Here, $\vec{x} \in \{0,1\}^{nk}, \vec{a} \in \{0,1\}^k$. Then we compute

$$\begin{aligned}
\mathop{\mathbb{E}}_{U\sim\nu} \left[(\mathcal{O}_U^{\otimes k} \otimes \mathrm{id}) \, |\Omega\rangle\langle\Omega| \, (\mathcal{O}_U^{\dagger,\otimes k} \otimes \mathrm{id}) \right] &= \sum_{\substack{\vec{x},\vec{y}\in\{0,1\}^{nk} \\ \vec{a},\vec{b}\in\{0,1\}^k}} \mathop{\mathbb{E}}_{U\sim\nu} \left[|\vec{x}, U(\vec{x}) \oplus \vec{a}, \vec{x}, \vec{a}\rangle\langle \vec{y}, U(\vec{y}) \oplus \vec{b}, \vec{y}, \vec{b}| \right] \\
&= \sum_{S\subset[k]} \sum_{\substack{\vec{x},\vec{y}\in\{0,1\}^{nk} \\ \vec{a},\vec{b}\in\{0,1\}^k \\ y_i = x_i, \forall i\in S \\ \& \; y_j \neq x_j \forall j \notin S}} \mathop{\mathbb{E}}_{U\sim\nu} \left[|\vec{x}, U(\vec{x}) \oplus \vec{a}, \vec{x}, \vec{a}\rangle\langle \vec{y}, U(\vec{y}) \oplus \vec{b}, \vec{y}, \vec{b}| \right] ,
\end{aligned}$$

where we used the notation $U(\vec{x}) := (U(x_1), \ldots, U(x_k))$. Let us consider the summands for each set S individually. Without loss of generality, and for simplicity, fix a set S of size ℓ and consider the following:

$$\begin{aligned}
&\sum_{\substack{\vec{x},\vec{y}\in\{0,1\}^{nk} \\ y_i = x_i, \forall i\in S \\ \& \; y_j \neq x_j \forall j \notin S}} \sum_{\vec{a},\vec{b}\in\{0,1\}^k} \mathop{\mathbb{E}}_{U\sim\nu} \left[|\vec{x}, U(\vec{x}) \oplus \vec{a}, \vec{x}, \vec{a}\rangle\langle \vec{y}, U(\vec{y}) \oplus \vec{b}, \vec{y}, \vec{b}| \right] \\
&= \sum_{\substack{\vec{x},\vec{y}\in\{0,1\}^{nk} \\ y_i = x_i, \forall i\in S \\ \& \; y_j \neq x_j \forall j \notin S}} \sum_{\substack{\vec{s}\in\{0,1\}^{\ell}, \vec{q},\vec{r}\in\{0,1\}^{k-\ell} \\ \vec{a},\vec{b}\in\{0,1\}^k}} \Pr_{U\sim\nu} [\forall i \in S, j \notin S.\; U(x_i) = s_i, U(x_j) = q_j, U(y_j) = r_j] \\
&\qquad \cdot |\vec{x}, \vec{s} \oplus \vec{a}_{1,\ell}, \vec{q} \oplus \vec{a}_{\ell+1,k}, \vec{x}, \vec{a}\rangle\langle \vec{y}, \vec{s} \oplus \vec{b}_{1,\ell}, \vec{r} \oplus \vec{b}_{\ell+1,k}, \vec{y}, \vec{b}| \,,
\end{aligned}$$

where we denote by $\vec{a}_{i,j}$ the $j-i+1$ dimensional vector that contains the entries $a_i, \ldots, a_j$. We group the terms into Hermitian operators of the form:

$$\begin{aligned}
&\Pr_{U\sim\nu}\left[\forall i \in S, j \notin S.\ U(x_i) = s_i, U(x_j) = q_j, U(y_j) = r_j\right] \\
&\qquad \cdot \Big(|\vec{x}, \vec{s} \oplus \vec{a}_{1,\ell}, \vec{q} \oplus \vec{a}_{\ell+1,k}, \vec{x}, \vec{a}\rangle\langle \vec{y}, \vec{s} \oplus \vec{b}_{1,\ell}, \vec{r} \oplus \vec{b}_{\ell+1,k}, \vec{y}, \vec{b}| \\
&\qquad + |\vec{y}, \vec{s} \oplus \vec{b}_{1,\ell}, \vec{r} \oplus \vec{b}_{\ell+1,k}, \vec{y}, \vec{b}\rangle\langle \vec{x}, \vec{s} \oplus \vec{a}_{1,\ell}, \vec{q} \oplus \vec{a}_{\ell+1,k}, \vec{x}, \vec{a}| \Big) .
\end{aligned}$$

Then we can split the term as follows

$$\begin{aligned}
M_+ + M_- = \Big(&|\vec{x}, \vec{s} \oplus \vec{a}_{1,\ell}, \vec{q} \oplus \vec{a}_{\ell+1,k}, \vec{x}, \vec{a}\rangle\langle \vec{y}, \vec{s} \oplus \vec{b}_{1,\ell}, \vec{r} \oplus \vec{b}_{\ell+1,k}, \vec{y}, \vec{b}| \\
&+ |\vec{y}, \vec{s} \oplus \vec{b}_{1,\ell}, \vec{r} \oplus \vec{b}_{\ell+1,k}, \vec{y}, \vec{b}\rangle\langle \vec{x}, \vec{s} \oplus \vec{a}_{1,\ell}, \vec{q} \oplus \vec{a}_{\ell+1,k}, \vec{x}, \vec{a}| \Big)
\end{aligned}$$

into a positive (M_+) and a negative part (M_-). Then,

$$\begin{aligned}
&\min\{(1+\varepsilon)^{-1}, (1-\varepsilon)\} 2^{-\ell-2(k-\ell)}(M_+ + M_-) \\
&\quad \leq \Pr_{U\sim\nu}\left[\forall i \in S, j \notin S.\ U(x_i) = s_i, U(x_j) = q_j, U(y_j) = r_j\right](M_+ + M_-) \\
&\quad \leq \max\{(1+\varepsilon), (1-\varepsilon)^{-1}\} 2^{-\ell-2(k-\ell)}(M_+ + M_-) .
\end{aligned}$$

Here we use the fact that ν is relative-error ϵ-approximately $2k$-wise independent, and the fact that there are at most $2k$ entries specified in the probability. Both inequalities extend to the full sum. The operator inequality in Equation (1) now follows from observing that $2^{-\ell-2(k-\ell)}(M_+ + M_-)$ corresponds to the uniform case.

We can now proceed to show that this operator inequality implies indistinguishability for any quantum algorithm that only queries $k/2$ copies of U. The proof is completely analogous to the proof of Lemma 5 in Ref. [SHH24]. For completeness, we repeat the argument here: Any quantum algorithm that makes k queries can be applies a sequence of unitaries $W_1, \ldots, W_k$ alternating with queries to the oracle $\mathcal{O}$ to $|0^{n+m}\rangle$, where m denotes the number of ancilla qubits. We denote the outcome state of this procedure by

$$|\psi_U\rangle = W_{k+1} \cdot \prod_{i=1}^{k} ((\mathcal{O} \otimes \mathrm{id}_m) \cdot W_i) \, |0^{n+m}\rangle \ .$$

We can now write $|\psi_U\rangle$ as

$$|\psi_U\rangle = (\mathrm{id}_{n+m} \otimes \langle\Omega|) \, |\Psi_U\rangle \ ,$$

for two unnormalized states (and here we use capital greek letters to denote un-normalized states)

$$\begin{aligned}
|\Psi_U\rangle &:= \sum_{\vec{x},\vec{y}\in\{0,1\}^{kn}} W_{k+1} \cdot \prod_{i=1}^{k} ((|y_i\rangle\langle x_i| \otimes \mathrm{id}_m) \cdot W_i) \, |0^{n+m}\rangle \otimes (U^{\otimes k} \otimes \mathrm{id}_{nk}) \, |\vec{x}, \vec{y}\rangle \\
|\Omega\rangle &:= \sum_{\vec{z}\in\{0,1\}^{kn}} |\vec{z}, \vec{z}\rangle \, .
\end{aligned}$$

Here, Ω is the (un-normalized) maximally entangled state, as before, but the number of qubits is not necessarily the same as before. This "parallelizes" the application of the queried unitaries $\mathcal{O}$, which allows us to compare the uniformly random oracle to $\mathcal{O}$ with the set U drawn from ν. Relative errors are necessary to overcome the large normalization factors.

We can subsequently pull out the $U^{\otimes k}$ in the purifying register to get the following

$$|\Psi_U\rangle = (\mathrm{id}_{n+m} \otimes U^{\otimes k} \otimes \mathrm{id}_{kn}) |\Psi_{\mathrm{id}}\rangle \ .$$

where $|\Psi_{\mathrm{id}}\rangle$ is the corresponding un-normalized state corresponding to if the algorithm had queried the identity instead of U. Then we can compute the average outcome state

$$\mathop{\mathbb{E}}_{U\sim\nu} [|\psi_U\rangle\langle\psi_U|] = (\mathrm{id}_{n+m} \otimes \langle\Omega|)(\mathrm{id}_{n+m} \otimes \Phi_\nu \otimes \mathrm{id}_{kn})(|\Psi_{\mathrm{id}}\rangle\langle\Psi_{\mathrm{id}}|)(\mathrm{id}_{n+m} \otimes |\Omega\rangle) \,,$$

where we abuse notation and use id_{kn} to represent the identity channel on kn qubits, and $\Phi_\nu(\cdot) := \mathbb{E}_{U\sim\nu}\left[\mathcal{O}_U^{\otimes k}(.)\mathcal{O}_U^{\dagger,\otimes k}\right]$. Then, the inequality Equation (1) readily implies the operator inequality

$$(1-\varepsilon) \mathop{\mathbb{E}}_{U\sim\nu} [|\psi_U\rangle\langle\psi_U|] \leq \mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \leq (1+\varepsilon) \mathop{\mathbb{E}}_{U\sim\nu} [|\psi_U\rangle\langle\psi_U|] \ .$$

We can now complete the proof of Theorem 4.2:

$$\begin{aligned}
&\left\| \mathop{\mathbb{E}}_{U\sim\nu} [|\psi_U\rangle\langle\psi_U|] - \mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \right\|_1 \\
&\quad = \max_{0\leq M_+, M_- \leq 1} \mathrm{Tr}\Bigg(M_+ \left[\mathop{\mathbb{E}}_{U\sim\nu} [|\psi_U\rangle\langle\psi_U|] - \mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \right] \\
&\qquad\qquad - M_- \left[\mathop{\mathbb{E}}_{U\sim\nu} [|\psi_U\rangle\langle\psi_U|] - \mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \right] \Bigg) \\
&\quad \leq \max_{0\leq M_+, M_- \leq 1} \varepsilon \left(\mathrm{Tr}\left(M_+ \left[\mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \right] \right) + \mathrm{Tr}\left(M_- \left[\mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \right] \right) \right) \\
&\quad = 2\varepsilon \left\| \mathop{\mathbb{E}}_{U\sim\mathrm{unif}} [|\psi_U\rangle\langle\psi_U|] \right\|_1 \\
&\quad = 2\varepsilon \,.
\end{aligned}$$

The definition of the trace distance as half of the one-norm distance concludes the proof. □

5 Spectral Forrelation and Fourier-independent distributions

Here, we define the *spectral Forrelation* problem, and then construct a certain "nice" type of distribution, which we call *relative-error Fourier-independent* (REFI) distributions. We will see that REFI distributions are a distribution of instances of the $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation problem that are hard for QCMA verifiers.

5.1 The spectral Forrelation problem

Here we define the spectral Forrelation problem more generally than presented in Section 2. We first define what it means for two sets to be Forrelated.

Definition 5.1 (Forrelation matrix of two sets)**.** *Let $S, U \subseteq [N]$ be two subsets. Then we define the* Forrelation matrix *of S and U to be*

$$\mathrm{F}_{S,U} = \Pi_U \cdot \mathsf{QFT} \cdot \Pi_S \,,$$

where $\Pi_S = \sum_{x \in S} |x\rangle\langle x|$ and similarly for U.

Definition 5.2 (Spectrally Forrelated sets)**.** *Let $\eta \in [0,1]$ and $N = 2^{n^{\Theta(1)}}$, then we say that two sets $S, U \subseteq [N]$ are* η-Spectrally Forrelated *if*

$$\|\mathrm{F}_{S,U}\|^2 \geq \eta \,.$$

Note that we use the squared spectral norm, as it will correspond to the probability of a measurement accepting on some state.

Now we define the spectral Forrelation problem. Since we hope that (α, β)-SpectralForrelation will be a useful concept outside the context of this paper, the preceding definition is made in a more general way than we need in this paper.

Definition 5.3 (The spectral Forrelation problem)**.** *Let $\alpha < \beta : \mathbb{N} \mapsto [0,1]$ and fix $N(n) = 2^n$, then the (α, β)-spectral Forrelation problem, (α, β)-SpectralForrelation, is an oracle-input promise language. For every $n \in \mathbb{Z}^+$, we define the universe to consist of tuples (S, U), where $S \in \{0,1\}^{N(n)}$ and $U \in \{0,1\}^{N(n)}$ are interpreted as membership oracles for sets $S, U \subseteq [N(n)]$, such that one of the following holds:*

$$\|\mathrm{F}_{S,U}\|^2 \geq \beta \quad \text{or} \quad \|\mathrm{F}_{S,U}\|^2 \leq \alpha \,.$$

Then (α, β)-SpectralForrelation is the subset of $\mathcal{U}$ corresponding to tuples (S, U) in such that $\|\mathrm{F}_{S,U}\|^2 \geq \beta$.

As stated before, this definition is slightly more general than we need, and in the rest of this paper we will primarily be concerned with the $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation problem.

5.2 Relative-error Fourier-independent distributions

In order to show hardness of the spectral Forrelation problem, we will define a family of "hard" instances of the problem, which we denote by relative-error Fourier-independent distributions. In this section, we define REFI distributions, and present an algorithm that samples them (Algorithm 1).

Definition 5.4 (Relative-error Fourier-independent distribution)**.** *Let $N \in \mathbb{Z}^+$ and $S \subseteq [N]$. We say that a distribution $\mathcal{D}_S$ over pairs $(|\psi\rangle, U)$ is $(k, \epsilon, \delta, \gamma)$-Relative-Error Fourier-Independent (REFI) if the following hold:*

- *$|\psi\rangle$ is a normalized superposition $\sum_{y \in S} \alpha_y |y\rangle$ over elements $y \in S$.*
- *$U \subseteq [N]$, and the marginal distribution of U is (k, ϵ)-wise uniform independent with relative error.*
- *Let $|\hat{\psi}\rangle = \mathsf{QFT}|\psi\rangle$ be the quantum Fourier transform of $|\psi\rangle$. Then except with probability δ over the choice of $|\psi\rangle$, $\langle\hat{\psi}|\Pi_U|\hat{\psi}\rangle \geq \frac{1}{2} + \gamma$, where Π_U is the projection operator $\sum_{z \in U} |z\rangle\langle z|$.*

We want k to be large (say super-polynomial in $\log N$), ϵ, δ to be small (say negligible in $\log N$), and γ to be not-too-small (non-negligible in $\log N$). Then a REFI distributions is one where (1) $|\psi\rangle$ has support on S, (2) U "looks like" a random set to query-bounded quantum algorithms (via Theorem 4.2), but (3) $|\hat{\psi}\rangle$ is biased toward elements in U. We show that for a set S sampled from $\mathsf{Bernoulli}_p^N$ for a suitable p, we can sample REFI distributions.

Algorithm 1. *Sampling from a REFI distribution, $\mathcal{D}_S$.*

Input: $S \subseteq N$ of size ℓ and parameters $k, \epsilon, \delta, \gamma$.

1. For each $y \in S$, sample $\alpha_y \leftarrow \mathcal{N}^{\mathbb{C}}(0, \sigma)$ for $\sigma\ 1/\sqrt{\ell}$. Let $|\psi\rangle = \sum_{y \in S} \alpha_y |y\rangle$.
2. For each $z \in \mathbb{Z}_N$, let $\beta_z = \sum_{y \in S} e^{i2\pi yz/N} \alpha_y$ and place z into a set U independently with probability $1 - e^{-|\beta_z|^2}$.

Output: $(|\psi\rangle, U)$.

We will show that with high probability, Algorithm 1 produces a REFI distribution when the input is a random set of a suitable size. However, we first provide some intuition and prove some lemmas about the algorithm.

Intuition: By choosing $\sigma = 1/\sqrt{\ell}$, we will show that $|\psi\rangle$ is approximately normalized, so we can think of $|\psi\rangle$ as being essentially a Haar random state with support on S. Let $|\hat{\psi}\rangle = \mathsf{QFT}\,|\psi\rangle$ be the QFT applied to $|\psi\rangle$. Then $|\hat{\psi}\rangle = \sum_{z \in \mathbb{Z}_N} (\beta_z/\sqrt{N})\,|z\rangle$. Thus, the set U that the algorithm outputs will be biased toward containing the points z where β_z is large. In order to show that U is approximately k-wise independent, we will show that the probability of U having intersection R with any set T is related to the inner product between this "almost Haar random" vector $|\psi\rangle$ and fixed matrix that depends on S and the quantum Fourier transform. Then applying matrix concentration inequalities will allow us to get very good bounds on the deviation of this probability from its expected value.

5.3 Technical lemmas

We first prove some useful lemmas and provide notation related to the output distribution $\mathcal{D}_S$ that Algorithm 1 outputs. For a subset $S \subseteq \mathbb{Z}_N$, let $\mathbf{M}^S$ be the $N \times N$ matrix defined as $\mathsf{QFT}^\dagger \circ \Pi_S \circ \mathsf{QFT}$. For another subset T, let $\mathbf{M}_T^S$ be the $|T| \times |T|$ sub-matrix of $\mathbf{M}^S$ consisting of rows and columns whose indices are in T. The following lemma bounds the determinant of the minors of $\mathbf{M}^S$.

Lemma 5.5. *For any $\epsilon > 0$, except with probability at most $2N^2 e^{-\epsilon^2 N^2/8\ell}$ over the choice of random S of size ℓ, $\max_{z \neq z'} |\mathbf{M}^S_{z,z'}| \leq \epsilon$*

Proof. Fix any $z \neq z'$, and consider the random variable $M^S_{z,z'}$ where S is a random set of size ℓ. We write:

$$M^S_{z,z'} = \frac{1}{N} \sum_{y \in S} e^{i2\pi(z-z')y/N} = \frac{1}{N} \sum_{j=1}^{\ell} e^{i2\pi(z-z')y_j/N}$$

where $y_1 \cdots, y_\ell$ range over the elements of S, and are therefore random distinct values in $\mathbb{Z}_N$.

We first look at the real part of $\mathbf{M}^S_{z,z'}$, namely $\frac{1}{N}\sum_{i=1}^{\ell} Y_i$ where $Y_i = \cos(2\pi(z-z')y_i/N)$. For the moment, imagine the y_i being uniform without the distinctness requirement, in which case since $z - z' \neq 0$ the Y_i all become independent random variables bounded to the range $[-1, 1]$. Moreover, the means are zero since $z - z' \neq 0 \bmod N$. Then by Hoeffding's inequality, we have

$$\Pr\left[\left|\sum_{i=1}^{\ell} Y_i\right| \geq t\right] \leq 2e^{-t^2/4\ell}$$

We then observe that switching to distinct y_i cannot make the inequality worse. This is because Hoeffding's inequality still holds when sampling is performed without replacement; in fact even better bounds are possible [Ser74].

We now look at the imaginary part $\frac{1}{N}\sum_{i=1}^{\ell} Y'_i$ where $Y'_i = \sin(2\pi(z-z')y_i/N)$. By identical logic, we have that

$$\Pr\left[\left|\sum_{i=1}^{\ell} Y'_i\right| \geq t\right] \leq 2e^{-t^2/4\ell}$$

Combining the two inequalities with the fact that the real and imaginary parts are orthogonal gives $\Pr[|M^S_{z,z'}| \geq \sqrt{2}t/N] \leq 4e^{-t^2/4\ell}$. Setting $t = \epsilon N/\sqrt{2}$ gives that

$$\Pr\left[\left|M^S_{z,z'}\right| \geq \epsilon\right] \leq 4e^{-\epsilon^2 N^2/8\ell}$$

Taking a union bound over all $\binom{N}{2}$ off-diagonal terms[5] we obtain the lemma. □

Next, we derive an analytic form for the probability that U sampled from Algorithm 1 intersects a fixed set S. This lemma is the main technical lemma that we will use to derive the fact that the disrtibution produced by Algorithm 1 is REFI with high probability, and later show that is close to k-wise independent in relative error.

Lemma 5.6. *Fix subsets S, T, with $|S| = \ell$. Then for all $R \subseteq T$, the following holds*

$$\Pr_{U \leftarrow \mathcal{D}^S}[T \cap U = R] = \frac{\det(\frac{N}{\ell}\mathbf{M}^S_R)}{\det(\mathrm{id} + \frac{N}{\ell}\mathbf{M}^T_S)} = \frac{\det(\frac{N}{\ell}\mathbf{M}^S_R)}{\det(\mathrm{id} + \frac{N}{\ell}\mathbf{M}^S_T)}\,.$$

Proof. Recall that for sampling U we first sample a state $|\psi\rangle$ with support on S and Gaussian coefficients α_z and then exclude a bitstring z from U with probability $e^{-|\beta_z|^2}$, where β_z denotes the Fourier coefficient of z. Then, we find that conditioned on sampling state $|\psi\rangle$,

$$\begin{aligned}
\Pr[T \cap U = R|\,|\psi\rangle] &= \prod_{z\in R}\left(1 - e^{-|\beta_z|^2}\right)\prod_{z\in T\setminus R} e^{-|\beta_z|^2} \\
&= e^{-\sum_{z\in T\setminus R}|\beta_z|^2}\cdot\left(\sum_{L\subseteq R}(-1)^{|L|}\cdot e^{-\sum_{z\in L}|\beta_z|^2}\right) \\
&= \sum_{L\subseteq R}(-1)^{|L|}e^{-\sum_{z\in T\setminus(R\setminus L)}|\beta_z|^2}\,.
\end{aligned}$$

[5] Since M^S is Hermitian, we only need to bound, say, the terms above the diagonal.

We denote by $T' = T \setminus (R \setminus L)$, and we compute the expression in each term of the sum as follows.

$$e^{-\sum_{z\in T'}|\beta_z|^2} = e^{-N\langle\psi|\mathsf{QFT}^\dagger\cdot\Pi_{T'}\cdot\mathsf{QFT}|\psi\rangle} = e^{-N\langle\psi|\mathbf{M}^{T'}|\psi\rangle}\,.$$

Now let $\mathbf{v}$ be the vector of length ℓ where the y'th entry is α_y. Note that $|\psi\rangle$ is just $\mathbf{v}$ with zeros inserted in each position outside of S. Then we can write

$$\Pr[T \cap U = R|\,|\psi\rangle] = e^{-N\mathbf{v}^\dagger\mathbf{M}_S^{T'}\mathbf{v}}\,.$$

Now evaluating the probability from the theorem statement amounts to integrating the above expression over all states $|\psi\rangle$.

$$\begin{aligned}
\Pr_{U\leftarrow\mathcal{D}^S}[T\cap U = R] &= \frac{1}{(\pi\sigma^2)^\ell}\int_{\mathbb{C}^\ell}\sum_{L\subseteq R}(-1)^{|L|}e^{-N\mathbf{v}^\dagger\mathbf{M}_S^{T'}\mathbf{v}}\mathrm{d}\mathbf{v}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\frac{1}{(\pi\sigma^2)^\ell}\int_{\mathbb{C}^\ell}e^{-N\mathbf{v}^\dagger\mathbf{M}_S^{T'}\mathbf{v}}\mathrm{d}\mathbf{v}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\frac{1}{(\pi\sigma^2)^\ell}\int_{\mathbb{C}^\ell}e^{-\mathbf{v}^\dagger(\sigma^{-2}\mathrm{id}+N\mathbf{M}_S^{T'})\mathbf{v}}d\mathbf{v}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\frac{1}{(\sigma^2)^\ell\det(\sigma^{-2}\mathrm{id}+N\mathbf{M}_S^{T'})}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\frac{1}{\det(\mathrm{id}+N\sigma^2\mathbf{M}_S^{T'})}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\frac{1}{\det(\mathrm{id}+\frac{N}{\ell}\mathbf{M}_{T'}^{S})}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\det\left((\mathrm{id}+\frac{N}{\ell}\mathbf{M}_{T'}^{S})^{-1}\right),
\end{aligned}$$

In order to switch the positions of T' and S, we observe that for all T', $\mathbf{M}_S^T = A^\dagger A$, where A is the $|T'|\times\ell$ sub-matrix of QFT restricted to column indices in S and row indices in T'. Then by the Weinstein–Aronszajn identity, $\det(\mathrm{id}+\frac{N}{\ell}\mathbf{M}_S^{T'}) = \det(\mathrm{id}+\frac{N}{\ell}A^\dagger A) = \det(\mathrm{id}+\frac{N}{\ell}AA^\dagger) = \det(\mathrm{id}+\frac{N}{\ell}\mathbf{M}_{T'}^S)$. Then we use the fact that $\det(AB)=\det(A)\det(B)$ to switch from the inverse of the determinant to the determinant of the inverse. We can now use Jacobi's identity for complementary minors of inverse matrices:

$$\det\left(\left(1+\frac{N}{\ell}\mathbf{M}_{T'}^S\right)^{-1}\right) = \frac{\det\left(\mathrm{id}+\frac{N}{\ell}\mathbf{M}_{T\setminus T'}^S\right)}{\det\left(\mathrm{id}+\frac{N}{\ell}\mathbf{M}_T^S\right)}\,,$$

Finally, we arrive at the expression:

$$\begin{aligned}
\Pr_{U\leftarrow\mathcal{D}^S}[T\cap U=R] &= \sum_{L\subseteq R}(-1)^{|L|}\frac{1}{\det(\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T'})}\\
&= \sum_{L\subseteq R}(-1)^{|L|}\det\left((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T'})^{-1}\right)\\
&= \frac{1}{\det((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T})}\sum_{L\subseteq R}(-1)^{|L|}\det\left((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T\setminus T'})\right)\\
&= \frac{(-1)^{|R|}}{\det((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T})}\sum_{L\subseteq R}(-1)^{|T\setminus T'|}\det\left((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T\setminus T'})\right)\\
&= \frac{(-1)^{|R|}}{\det((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T})}\sum_{L\subseteq R}(-1)^{|R\setminus L|}\det\left((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{R\setminus L})\right)\\
&= \frac{(-1)^{|R|}}{\det((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T})}\det\left(\mathrm{id}-(\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{R})\right)\\
&= \frac{\det\left(\frac{N}{\ell}\mathbf{M}^S_R\right)}{\det((\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_{T})},
\end{aligned}$$

where we used the fact that for all choices of R and L, $T\setminus T' = (L\cup(T\setminus R)) = R\setminus L$ and the identity [Gri20, Corollary 6.164]

$$\det(x\cdot\mathrm{id}+A)=\sum_{r=0}^{m}\left(\sum_{I\subseteq[m],|I|=r}\det(A_I)x^{m-r}\right)$$

for $A=\mathrm{id}+\frac{N}{l}\mathbf{M}^S_T$ and $x=-1$. □

Now we provide upper and lower bounds on the probability that U sampled from Algorithm 1 intersects a fixed set T. The following is a lower bound on the probability.

Lemma 5.7 (Intersection probability lower bound)**.** *For all subsets S, $T\subseteq[N]$, and $R\subseteq T$, except with probability at most $2N^2e^{-\epsilon^2\ell/2}$, the following holds*

$$\frac{1}{1+|T|}\geq\Pr_{U\leftarrow\mathcal{D}_S}[T\cap U=R]\geq 2^{-|T|}(1-|T|^2\epsilon)\,.$$

Proof. Recall that we have the following expression for the intersection probability.

$$\Pr_{U\leftarrow\mathcal{D}_S}[T\cap U=R]=\frac{\det\left(\frac{N}{\ell}\mathbf{M}^S_R\right)}{\det\left(\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_T\right)}\,.$$

Since we are interested in a lower bound, we can first upper bound the determinant in the denominator.

Observe that the diagonal entries in $\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S$ are exactly 2. Indeed, the zth diagonal entry is $1+\frac{N}{\ell}\left(\frac{1}{N}\sum_{x\in S}e^{i2\pi zx}e^{-i2\pi zx}\right)=2$. Moreover, $\frac{N}{\ell}\mathbf{M}^S$ and hence $\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S$ is PSD. Since $\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S_T$ is just a principal minor of $\mathrm{id}+\frac{N}{\ell}\mathbf{M}^S$, it is also PSD with diagonal entries also equal to 2. The determinant is then bounded by the product of the diagonal entries, giving the upper bound.

Now we lower bound the numerator. By Lemma 5.5, the off-diagonal entries of $\mathbf{M}^S$ are bounded by $2\epsilon\ell/N$ except with probability $2N^2e^{-\epsilon^2\ell/2}$. We have already seen that the diagonal entries of $\frac{N}{\ell}\mathbf{M}_T^S$ are exactly 1. The off-diagonal entries of $\frac{N}{\ell}\mathbf{M}_T^S$ are off-diagonal entries from $\mathbf{M}^S$ but scaled by N/ℓ, and are therefore bounded by 2ϵ except with the given probability. By Gershgorin's circle theorem, the eigenvalues are lower-bounded by $(1-|T|\epsilon)$, and therefore the determinant is lower bounded by $(1-|T|\epsilon)^{|T|}$. We get the desired bound by bounding $(1-|T|\epsilon)^{|T|} \geq (1-|T|^2\epsilon)$.

For the upper bound, we can first upper bound the detminant of $\frac{N}{\ell}\mathbf{M}_R^S$ by 1. Then note that the eigenvalues of $\mathrm{id}+\mathbf{M}_T^S$ sum to $2|T|$ and are at least 1. The detminant of this matrix is the product of eigenvalues, which is minimized when the first eigenvalue is $|T|+1$, and the remaining $|T|-1$ are 1, giving the desired upper bound. □

Note that in Lemma 5.7, when $R=\emptyset$, we can tighten the lower bound to be exactly $2^{-|T|}$, since we remove the contribution of $\det(\mathbf{M}_R^S)$. Since the lemma holds for all choices of T, for $|T|=1$ and $R=\emptyset$, we have that $\Pr[T\cap U=\emptyset]=1/2$. This means each z is placed in U with probability exactly $1/2$. By linearity of expectation, $\mathbb{E}[|U|]=N/2$. We can also give tighter upper-bound on the probability with high probability over the choice of S, as in the following lemma.

Lemma 5.8 (Intersection probability upper bound)**.** *For all $\epsilon>0$, except with probability at most $2N^2e^{-\epsilon^2\ell/2}$ over the choice of random subset S of size ℓ, for all subsets T and $R\subseteq T$*

$$\left(\Pr_{U\leftarrow\mathcal{D}_S}[T\cap U=R]\right)^{-1} \geq 2^{|T|}(1-|T|^2\epsilon)\,.$$

In this event, as long as $|T|^2\epsilon\leq 1/2$, we can bound $\Pr_{U\leftarrow\mathcal{D}_S}[T\cap U=R]\leq 2^{-|T|}(1+2|T|^2\epsilon)$.

Proof. Recall that we have the following expression from Lemma 5.6.

$$\left(\Pr_{U\leftarrow\mathcal{D}_S}[T\cap U=R]\right)^{-1} = \frac{\det(\mathrm{id}+\frac{N}{\ell}\mathbf{M}_T^S)}{\det(\frac{N}{\ell}\mathbf{M}_R^S)}\,.$$

Since we are interested in a lower bound, we can first upper bound the determinant of $\frac{N}{\ell}\mathbf{M}_R^S$ by 1 using the the analysis from Lemma 5.7 that shows that the diagonal entries are 1, which upper bounds the determinant by 1 as well. It remains to lower bound the determinant in the numerator.

Assume all the off-diagonal entries of M^S are bounded by $2\epsilon\ell/N$, which by Lemma 5.5 holds except with probability $2N^2e^{-\epsilon^2\ell/2}$. We have already seen that the diagonal entries of $\mathrm{id}+\frac{N}{\ell}\mathbf{M}_T^S$ are exactly 2. The off-diagonal entries of $\mathrm{id}+\frac{N}{\ell}\mathbf{M}_T^S$ are off-diagonal entries from $\mathbf{M}^S$ but scaled by N/ℓ, and are therefore bounded by 2ϵ. By Gershgorin's circle theorem, the eigenvalues are therefore lower-bounded by $2(1-|T|\epsilon)$. The determinant is therefore lower-bounded by this quantity raised to the $|T|$. We obtain the lemma by bounding $(1-|T|\epsilon)^{|T|}\geq(1-|T|^2\epsilon)$. □

Now we bound $\||\psi\rangle\|^2$, showing that $|\psi\rangle$ is approximately normalized.

Lemma 5.9. *Let S be a set of size ℓ and $\epsilon\in(0,1)$. Then except with probability $2e^{-\epsilon^2\ell/8}$, $\||\psi\rangle\|^2\in[1-\epsilon,1+\epsilon]$, where $|\psi\rangle$ is generated as in Algorithm 1.*

Proof. First, $\mathbb{E}[\||\psi\rangle\|^2]=\sum_{y\in S}\mathbb{E}[|\alpha_y|^2]$. Since $\alpha_y\leftarrow\mathcal{N}^{\mathbb{C}}(0,1/\sqrt{\ell})$, the real and imaginary parts are mean-0 normal variables with variance $1/2\ell$. $|\alpha_y|^2$ is therefore distributed as the Chi-squared distribution with two degrees of freedom, scaled by $1/2\ell$, which therefore has expectation $1/\ell$.

Summing over all $y \in S$ gives $\mathbb{E}[\||\psi\rangle\|^2] = 1$. We also see that $\||\psi\rangle\|^2$ is distributed as a Chi-squared distribution with 2ℓ degrees of freedom, scaled by $1/2\ell$. Via concentration inequalities for Chi-squared, we have that

$$\Pr\left[\left|\||\psi\rangle\|^2 - 1\right| \geq 4\sqrt{x/2\ell}\right] \leq 2e^{-x}\,.$$

Setting $\epsilon = 4\sqrt{x/2\ell}$ gives the lemma. □

Now, we bound the probability that (the normalization of) $|\hat{\psi}\rangle$ is accepted by U. Note that $\||\psi\rangle\|^2 = \left\||\hat{\psi}\rangle\right\|^2$.

Lemma 5.10. *For all S of size ℓ and $\epsilon \in (0,1)$, except with probability at most $3(N^{-1}+\ell^2 N^{-2})\epsilon^{-2} + 4N^2 e^{-\ell\epsilon^2/32}$ over the choice of S, U sampled from Algorithm 1, we have*

$$\left|\frac{\langle\hat{\psi}|\Pi_U|\hat{\psi}\rangle}{\||\psi\rangle\|^2} - 3/4\right| \leq \epsilon\,.$$

Recall Π_U is the projection operator $\sum_{z\in U}|z\rangle\langle z|$.

Proof. Fix $|\psi\rangle$. We first compute the expectation of $\langle\hat{\psi}|\Pi_U|\hat{\psi}\rangle$ (as U varies) given $|\psi\rangle$. We will actually compute the complement $\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle$

$$\begin{aligned}
\mathbb{E}[\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle] &= \frac{1}{N}\,\mathbb{E}\left[\sum_{z\notin U}|\beta_z|^2\right] \\
&= \frac{1}{N}\sum_{z\in\mathbb{Z}_N}\Pr[z\notin U]\cdot|\beta_z|^2 \\
&= \frac{1}{N}\sum_{z\in\mathbb{Z}_N}|\beta_z|^2 e^{-|\beta_z|^2}\,.
\end{aligned}$$

Now we include the expectation as we vary $|\psi\rangle$, giving:

$$\mathbb{E}[\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle] = \frac{1}{N}\sum_{z\in\mathbb{Z}_N}\mathbb{E}\left[|\beta_z|^2 e^{-|\beta_z|^2}\right]\,.$$

Next, we bound $\mathbb{E}[|\beta_z|^2 e^{-|\beta_z|^2}]$. Since the distribution of α_y are invariant under phase change, we see that β_z is just the sum of ℓ iid variables distributed as $\mathcal{N}^{\mathbb{C}}(0,1/\sqrt{\ell})$. This means each β_z is distributed as $\mathcal{N}^{\mathbb{C}}(0,1)$. Breaking out the real and imaginary parts lets us write

$$\begin{aligned}
\mathbb{E}[|\beta_z|^2 e^{-|\beta_z|^2}] &= \int_{\mathbb{C}}|\beta|^2 e^{-|\beta|^2}\cdot\frac{1}{\pi}e^{-|\beta|^2}\mathrm{d}\beta \\
&= \frac{1}{\pi}\int_{\mathbb{C}}|\beta|^2 e^{-2|\beta|^2}\mathrm{d}\beta \\
&= \frac{1}{\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}(x^2+y^2)e^{-2(x^2+y^2)}\mathrm{d}x\mathrm{d}y \\
&= \frac{1}{4}\,.
\end{aligned}$$

Thus, we have that $\mathbb{E}[\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle] = 1/4$. Now we bound the variance. By carrying out a similar calculation as before, we have:

$$\begin{aligned}
\mathbb{E}\left[\left(\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle\right)^2\right] &= \frac{1}{N^2}\,\mathbb{E}\left[\left(\sum_{z\notin U}|\beta_z|^2\right)\right] \\
&= \frac{1}{N^2}\sum_{z,z'\in\mathbb{Z}_N}\Pr[z,z'\notin U]\cdot|\beta_z|^2\cdot|\beta_{z'}|^2 \\
&= \frac{1}{N^2}\left(\sum_z \Pr[z\notin U]\cdot|\beta_z|^4 + \sum_{z\neq z'}\Pr[z\notin U]\Pr[z'\notin U]\cdot|\beta_z|^2\cdot|\beta_{z'}|^2\right) \\
&= \frac{1}{N^2}\left(\sum_z |\beta_z|^4 e^{-|\beta_z|^2} + \sum_{z\neq z'}|\beta_z|^2\cdot|\beta_{z'}|^2 e^{-|\beta_z|^2-|\beta_{z'}|^2}\right).
\end{aligned}$$

We include the expectation as we vary $|\psi\rangle$. The expectation of $|\beta_z|^4 e^{-|\beta_z|^2}$ becomes

$$\mathbb{E}\left[|\beta_z|^4 e^{-|\beta_z|^2}\right] = \int_{\mathbb{C}}|\beta|^4 e^{-|\beta|^2}\times\frac{1}{\pi}e^{-|\beta|^2}\mathrm{d}\beta = \frac{3}{4}.$$

Meanwhile, to compute the expectation of $|\beta_z|^2\cdot|\beta_{z'}|^2 e^{-|\beta_z|^2-|\beta_{z'}|^2}$, we use that the co-variance matrix of $\beta_z,\beta_{z'}$ is exactly $\mathbf{M}^S_{\{z,z'\}}$. Thus

$$\begin{aligned}
&\mathbb{E}\left[|\beta_z|^2\cdot|\beta_{z'}|^2 e^{-|\beta_z|^2-|\beta_{z'}|^2}\right] \\
&= \int_{\mathbb{C}}\int_{\mathbb{C}}|\beta|^2\cdot|\beta'|^2 e^{-|\beta|^2-|\beta'|^2}\times\frac{1}{\pi^2\det(\mathbf{M}^S_{\{z,z'\}})^2}e^{-\begin{pmatrix}\beta^* & (\beta')^*\end{pmatrix}\cdot\left(\mathbf{M}^S_{\{z,z'\}}\right)^{-1}\cdot\begin{pmatrix}\beta\\ \beta'\end{pmatrix}}\mathrm{d}\beta\mathrm{d}\beta' \\
&= \frac{1}{\pi^2\det\left(\mathbf{M}^S_{\{z,z'\}}\right)^2}\int_{\mathbb{C}}\int_{\mathbb{C}}|\beta|^2|\beta'|^2 e^{-\begin{pmatrix}\beta^* & (\beta')^*\end{pmatrix}\cdot\left[\mathrm{id}+\left(\mathbf{M}^S_{\{z,z'\}}\right)^{-1}\right]\cdot\begin{pmatrix}\beta\\ \beta'\end{pmatrix}}\mathrm{d}\beta\mathrm{d}\beta' \\
&= \frac{1}{\pi^2\det\left(\mathbf{M}^S_{\{z,z'\}}\right)^2}\times\frac{\pi^2\mathrm{Tr}\left(\mathrm{id}+\left(\mathbf{M}^S_{\{z,z'\}}\right)^{-1}\right)^2}{4\det\left(\mathrm{id}+\left(\mathbf{M}^S_{\{z,z'\}}\right)^{-1}\right)^3} \\
&= \frac{\det\left(\mathbf{M}^S_{\{z,z'\}}\right)\mathrm{Tr}\left(\mathrm{id}+\left(\mathbf{M}^S_{\{z,z'\}}\right)^{-1}\right)^2}{4\det\left(\mathrm{id}+\mathbf{M}^S_{\{z,z'\}}\right)^3}.
\end{aligned}$$

Now write $\mathbf{M}^S_{\{z,z'\}} = \begin{pmatrix}1 & \epsilon_{z,z'}\\ \epsilon_{z,z'} & 1\end{pmatrix}$. By Lemma 5.5, we can now bound $|\epsilon_{z,z'}|$ by $\frac{\ell}{4N} < 1/2$, except with probability $2N^2e^{-\ell/32}$. Then we have that

$$\mathbb{E}[|\beta_z|^2\cdot|\beta_{z'}|^2 e^{-|\beta_z|^2-|\beta_{z'}|^2}] = \frac{\left(2-|\epsilon_{z,z'}|^2\right)^2}{\left(1-|\epsilon_{z,z'}|^2\right)\left(4-|\epsilon_{z,z'}|^2\right)^3} \leq \frac{1}{16}(1+|\epsilon_{z,z'}|^2),$$

where the last inequality used that $|\epsilon_{z,z'}| \leq 1/2$.

We therefore have that $\mathbb{E}[(\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle)^2] \leq \frac{1}{16}+\frac{3}{4N}+\frac{1}{16N^2}\sum_{z\neq z'}|\epsilon_{z,z'}|$. Since the mean is $1/4$, the variance is therefore at most $\frac{3}{4N}+\frac{1}{16N^2}\sum_{z\neq z'}|\epsilon_{z,z'}|^2 \leq \frac{3}{4N}+\frac{1}{16N^2}\sum_{z\neq z'}\left(\frac{\ell}{4N}\right)^2 \leq \frac{3}{4N}+\frac{\ell^2}{256N^2}$. We now apply Chebyshev's inequality, to get that

$$\Pr\left[|\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle - 1/4| \geq \epsilon/2\right] \leq \frac{\frac{3}{4N}+\frac{\ell^2}{64N^2}}{(\epsilon/2)^2} + 2N^2 e^{-\ell/32}\,.$$

Now we have that

$$\begin{aligned}
\Pr\left[\left|\frac{\langle\hat{\psi}|\Pi_U|\hat{\psi}\rangle}{\||\psi\rangle\|^2} - 3/4\right| \geq \epsilon\right] &= \Pr\left[\left|\frac{\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle}{\||\psi\rangle\|^2} - 1/4\right| \geq \epsilon\right] \\
&= \Pr\left[\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle \notin \||\psi\rangle\|^2 \times \left[\frac{1}{4}-\epsilon, \frac{1}{4}+\epsilon\right]\right] \\
&\leq \Pr\left[\langle\hat{\psi}|(\mathrm{id}-\Pi_U)|\hat{\psi}\rangle \notin \left[\frac{1}{4}-\epsilon/2, \frac{1}{4}+\epsilon/2\right]\right] \\
&\quad + \Pr\left[\||\psi\rangle\|^2 \notin [1-\epsilon/2, 1+\epsilon/2]\right] \\
&\leq \left(\frac{\frac{3}{4N}+\frac{\ell^2}{64N^2}}{(\epsilon/2)^2} + 2N^2 e^{-\ell/32}\right) + 2e^{-\ell\epsilon^2/32} \\
&\leq 3(N^{-1}+\ell^2 N^{-2})\epsilon^{-2} + 4N^2 e^{-\ell\epsilon^2/32}\,.
\end{aligned}$$

Here going to the second to last line, we combine the analysis in the previous section of this proof and Lemma 5.9. □

5.4 Sampling REFI distributions

Now we proceed with the main theorem of this section.

Theorem 5.11. *For all functions $\epsilon, \delta : \mathbb{Z}^+ \mapsto [0,1]$ and functions $N, k : \mathbb{Z}^+ \mapsto \mathbb{Z}^+$ such that $\delta, 1/k = \mathrm{negl}(n)$, $\epsilon > N^{-1/2}$, $N = 2^{n^{O(1)}}$, set $p = \frac{k^4 \log^2(N)}{N\epsilon^2}$, $\gamma = 1/6$. Then except with negligible probability in $\log(N)$ over a random $S \leftarrow \mathsf{Bernoulli}_{p(n)}^{N(n)}$, Algorithm 1 outputs a $(k(n), \epsilon(n), \delta(n), \gamma)$-REFI distribution $\mathcal{D}_S$ for S for $\delta(n) = O\left(\frac{1}{N} + p^2 + N^2 e^{-pN/2304}\right)$.*

Proof. Let ℓ be the size of S, sampled from $\mathsf{Bernoulli}_p^N$. By the multiplicative Chernoff bound, we have that $\frac{1}{2}pN \leq \ell \leq \frac{3}{2}pN$ except with probability $0.9^{pN} = 0.9^{k^4\log^2(N)/\epsilon^2} = \mathrm{negl}(\log(N))$. Applying Lemma 5.7 and Lemma 5.8 with $\epsilon' = \epsilon(n)/4k^2$ and ℓ either being $\frac{1}{2}pN = \log^2(N)/2(\epsilon')^2$ or $\frac{3}{2}pN = 3\log^2(N)/2(\epsilon')^2$, we have that except with probability at most $O(N^2 e^{-O(\log^2(N))}) = \mathrm{negl}(\log(N))$, both of the following bounds hold for all T with $|T| \leq k$ and $R \subseteq T$.

$$2^{-|T|}(1-\epsilon) \leq \Pr_{U\leftarrow\mathcal{D}_S}[T \cap U = R] \leq 2^{-|T|}(1+\epsilon)\,.$$

This shows that, except with negligible probability, U sampled from $\mathcal{D}_S$ satisfies the (k,ϵ)-wise uniform independence property of Definition 5.4.

The final step is to show that there is a *normalized* state $|\psi\rangle$ satisfying the desired expectation value with $\Pi_U = \sum_{z\in U} |z\rangle\langle z|$. To that end, let $(|\psi\rangle, U) \leftarrow \mathcal{D}_S$, and let $|\psi'\rangle = |\psi\rangle / \||\psi\rangle\|$. From Lemma 5.10 we have that except with probability at most $\delta(n)$ given in this theorems statement, $\langle\hat{\psi}'| \Pi_U |\hat{\psi}'\rangle \geq 2/3$, as desired. □

6 From REFI distributions to an oracle separation

We now show that the spectral Forrelation problem give a separation between OI-QCMA and OI-QMA, using the REFI distribution guaranteed by Theorem 5.11.

6.1 Technical lemmas

We first prove a useful lemma in the proof of our main theorem.

Lemma 6.1. *Let U be sampled from a (k', δ)-wise uniform independent with relative error function and S' be a set that is potentially correlated to U but has size at most v, then except with probability $2N^2 \left(\frac{\sqrt{ek'}}{\epsilon\sqrt{N}}\right)^{k'} + \delta$ over the choice of U, S', it holds that, for any normalized state $|\phi\rangle$ with support on S', $\langle\hat{\phi}|\Pi_U|\hat{\phi}\rangle \leq 1/2 + v\epsilon$, where $|\hat{\phi}\rangle = \mathsf{QFT}|\phi\rangle$.*

Proof. First note that by Theorem 4.2, no quantum algorithm making k' queries can distinguish between U and a truly k-wise uniform independent function except with probability δ. Thus, for the remainder of the proof, we can assume that U is k'-wise uniform independent, at a cost of δ in the probability.

For a set U', let $\mathbf{M}^{U'} = \mathsf{QFT}^\dagger \cdot \Pi_{U'} \cdot \mathsf{QFT}$. Observe that $(\mathbf{M}^{U'})_{z,z'} = \frac{1}{N}\sum_{y\in\mathbb{Z}_N} e^{i2\pi(z-z')y/N}\xi_y$, where ξ_y is the Boolean value that is 1 if $y \in U'$. Then we have that $(\mathbf{M}^{U'})_{z,z} = |U'|/N$. In expectation, $|U'|/N$ is $1/2$. We now bound how far $|U'|/N$ can deviate from $1/2$. Recall that $|U'|/N = \frac{1}{N}\sum_{y\in\mathbb{Z}_N}\xi_y$. The ξ_y are not truly independent so we cannot use standard concentration inequalities such as Hoeffding's. However, we can use the following somewhat standard bound (e.g. [Tao10]) for the $[-1,1]$-weighted sum of k'-wise independent Boolean random variables:

$$\Pr\left[\left|\frac{1}{N}\sum_{y\in\mathbb{Z}_N}\xi_y - \frac{1}{2}\right| \geq \epsilon/\sqrt{2}\right] \leq 2\left(\frac{\sqrt{ek'}}{\epsilon\sqrt{N}}\right)^{k'}.$$

On the other hand, for $z \neq z'$, taking the expectation over U', we see that $\mathbb{E}_{U'}[(\mathbf{M}^{U'})_{z,z'}] = 0$. We now try to bound the deviation from the expectation, by bounding the real and imaginary parts separately. We see that $\mathrm{Re}[(\mathbf{M}^{U'})_{z,z'}] = \frac{1}{N}\sum_{y\in\mathbb{Z}_N}\cos(2\pi(z-z')y/N)\xi_y$, which is the weighted sum of Boolean random variables ξ_y, where the weights are all in $[-1,1]$. Using the $[-1,1]$-weighted sum of k'-wise independent Boolean random variables again, we have:

$$\Pr\left[\frac{1}{N}\sum_{y\in\mathbb{Z}_N}\cos(2\pi(z-z')y/N)\xi_y \geq \epsilon/\sqrt{2}\right] \leq 2\left(\frac{\sqrt{ek'}}{\epsilon\sqrt{N}}\right)^{k'}$$

Combining with an identical bound on the imaginary part of $(\mathbf{M}^{U})_{z,z'}$, we have that

$$\Pr[|(\mathbf{M}^{U'})_{z,z'}| \geq \epsilon] \leq 4\left(\frac{\sqrt{ek'}}{\epsilon\sqrt{N}}\right)^{k'}$$

By union-bounding over all entries of $\mathbf{M}^U$ (which only needs to count entries on the diagonal and above since $\mathbf{M}$ is Hermitian), we have except for probability at most $2N^2\left(\frac{\sqrt{ek'}}{\epsilon\sqrt{N}}\right)^{k'}$, both (1) for all z that $(\mathbf{M}^U)_{z,z} \in [1/2-\epsilon, 1/2+\epsilon]$ and (2) for all $z \neq z'$ that $|(\mathbf{M}^U)_{z,z'}| \leq \epsilon$.

Now suppose (1) and (2) hold. Now consider a supposed set S' of size v. Let $\mathbf{M}^{U'}_{S'}$ be the $v \times v$ sub-matrix whose row and column indices are in S'. Then by the Gershgorin circle theorem, all eigenvalues of $\mathbf{M}^{U'}_{S'}$ are bounded from above by $1/2 + v\epsilon$. □

6.2 Oracle separation between QMA and QCMA

Now we prove our main result, an oracle separation between QMA and QCMA. We first show that (α,β)-SpectralForrelation is in OI-QMA whenever $\beta - \alpha$ is inverse polynomial.

Theorem 6.2. *(α,β)-SpectralForrelation $\in$ OI-QMA for all inverse polynomial $\beta - \alpha$.*

Proof. An instance of (α,β)-SpectralForrelation will be a tuple (S,U) where $S,U \subseteq [N(n)]$ are given as membership oracles. Our verifier $V^{S,U}(|\psi\rangle)$ will do the following: V will make a query to S on the witness state $|\psi\rangle$ and measuring the output. If it accepts, then V will apply QFT_N to the witness state (which may have changed due to the measurement), and make a query to U, measuring the output. If both queries accept, then V will output 1; if either measurement rejects, then V will output 0.

We can see that on witness state $|\psi\rangle$, $\Pr[V^{S,U}(|\psi\rangle) = 1] = \langle\psi| F^\dagger_{S,U} F_{S,U} |\psi\rangle$, and maximizing this quantity over all $|\psi\rangle$ is exactly $\|F_{S,U}\|^2$. By the definition of (α,β)-SpectralForrelation, the universe $\mathcal{U}$ of valid inputs is the set of pairs (S,U) for which either (1) there exists a state $|\psi\rangle$ such that $\Pr[V^{S,U}(|\psi\rangle) = 1] \geq \beta$, or (2) for all states $|\psi\rangle$, $\Pr[V^{S,U}(|\psi\rangle) = 1] < \alpha$, and $(\alpha,\beta))$-SpectralForrelation $\subseteq \mathcal{U}$ is exactly the set such that $\Pr[V^{S,U}(|\psi\rangle) = 1] \geq \beta$. Thus we conclude that for all YES instances of (α,β)-SpectralForrelation, there exists a state that causes V to accept with probability β and on NO instances V running on all $|\psi\rangle$ accepts with probability at most α. Since $\beta - \alpha$ is inverse polynomial, applying sequential repetition [MW05] we can amplify the gap between YES and NO instances to meet the standard definition of QMA. Thus, we have that (α,β)-SpectralForrelation $\in$ OI-QMA. □

Now we show that $(\frac{7}{12},\frac{2}{3})$-SpectralForrelation $\notin$ OI-QCMA by showing that REFI distributions (Definition 5.4) are decided incorrectly by all QCMA verifiers with overwhelming probability.

Theorem 6.3. *$(\frac{7}{12},\frac{2}{3})$-SpectralForrelation $\notin$ OI-QCMA.*

Proof. We first invoke Theorem 5.11 with $N = 2^n$, $k = 2^{n/10}$, $\epsilon = 2^{-n/4}$ to obtain a distribution over $S \sim \mathsf{Bernoulli}^N_{n^{\log(n)+2}\cdot 2^{-n/10}}$ and $\mathcal{D}_S$, a $(2^{n/20}, 2^{-n/4}, O(n^{2\log(n)+4}\cdot 2^{-n/5})), 1/6)$-REFI distribution for S, except with negligible probability in n. Note that these are YES instances of $(\frac{7}{12},\frac{2}{3})$-SpectralForrelation. We now use this to construct our separation. Note that a valid QCMA verifier will accept YES instances of size n (given a correct witness) with probability at least $\frac{2}{3}$, and accept NO instances with probability at most $\frac{1}{3}$.

We can always assume without loss of generality that there is, say, a fixed quadratic running time t such that the running time of any OI-QCMA verifier is bounded by $t(|x| + |w|)$ where $|x|$ is the instance length and $|w|$ is the witness length. This is accomplished by padding the witness length with 0's that just get ignored by the verifier.

Now let $q(n) = 2^{n/200}$, which we will take as an upper bound on the witness length, and let $Q(n) = q(n)^2 = 2^{n/100}$, which we take to be an upper bound on the number of queries when the witness length is at most $q(n)$. Let $v(n) = O(2^{n/15})$ be the number of "heavy" indices we sampled. We will show that all sets S of size $v(n)$ do *not* correspond to YES instances of $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation.

Suppose toward contradiction that there is such a QMA(2) verifier V_* for the $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation problem. Then there is a classical witness w such that $\Pr[V_*^{S,U}(w) = 1] \geq 2/3$ for the S and U sampled from $\mathcal{D}_S$. We will now construct a different instance (S', U), where S' is constructed from the following algorithm, $\mathsf{GenSmallSet}^{S,U}(w)$.

Algorithm 2. $\mathsf{GenSmallSet}^{S,U}$

Input: Witness w.

1. Initialize $S' = \{\}$, and then repeat the following loop for $i = 1, ..., 2^{n/15}$:
   (a) Run $V_*^{S,U}(w)$ until a randomly chosen query to S, and measure the query, obtaining a string $y_i \in [N]$.
   (b) If $y_i \in S \setminus S'$, add y_i to S'.

Now we prove that this yields an instance that is not in $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation with high probability by showing that V^* must accept (S', U) with probability higher than $1/3$.

Claim 6.4. *Except with negligible probability over the choice of S, U, S', $(S', U) \in \mathcal{U} \setminus (\frac{7}{12}, \frac{2}{3})$-SpectralForrelation.*

Proof. Set $\epsilon = 2^{-n/15}/18$, and set $G := 2 \cdot 2^{2n} \left(\frac{2^{n/15} \cdot 18\sqrt{5e}}{2^{n/2}} \right)^5 = O(2^{-n/6})$. By Lemma 6.1 with $k' = 5$ (and $\delta = N^2 e^{-O(\log^2(N)} \ll G$ from Theorem 5.11), except with probability at most $G + \delta = O(2^{-n/6})$, the following bound holds:

$$\begin{aligned} \max_{\|\Pi_S |\phi\rangle\| = 1} \langle \hat{\phi} | \, \Pi_U \, | \hat{\phi} \rangle &\leq \frac{1}{2} + v\epsilon \\ &\leq \frac{1}{2} + \frac{1}{18} \\ &\leq \frac{7}{12}. \end{aligned}$$

Since this bound holds for any state $|\phi\rangle$, this is exactly an upper bound on the squared spectral norm of $\mathrm{F}_{S,U}$, so we can conclude that (S', U) is a NO instance of $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation. Note that this holds regardless of what S' is, since we only used the fact that it consists of at most $2^{n/15}$ elements. □

We now show, however, that V^* fails to reject (S', U) with high enough probability.

Claim 6.5. *Except with negligible probability over the choice of S, U, w, S', $\Pr[V_*^{S',U}(w) = 1] > \frac{1}{2}$.*

Proof. Observe that the process $\mathsf{GenSmallSet}^{S,U}(w)$ for constructing S' always generates $S' \subseteq S$. Now consider running $S' \leftarrow \mathsf{GenSmallSet}^{S,U'}(w')$, where w' is a random string and U' is a random Boolean function, with both w', U' independent of S. This is an algorithm which makes vQ queries to S (and also to U', but U' can be simulated on its own since it is independent of S). S in turn sampled from $\mathsf{Bernoulli}_p^N$. Finally, the algorithm outputs some subset S' of S. By Lemma 3.5, there is a universal constant C such that

$$\Pr[|S'| \geq K | w', U' \text{ are uniform and independent of } S] \leq (Cp(vQ/K)^2)^K .$$

Now, consider running $S' \leftarrow \mathsf{GenSmallSet}^{S,U'}(w)$. Since $\Pr[w' = w] = 2^{-q}$, this means that with probability 2^{-q}, $\mathsf{GenSmallSet}^{S,U'}(w')$ is actually running $\mathsf{GenSmallSet}^{S,U'}(w)$. Therefore, we have that for all K,

$$\Pr[|S'| \geq K | w' = w] \leq (Cp(vQ/K)^2)^K \times 2^q.$$

We now set $K = vQ\sqrt{2Cp} + q + \log_2(v) + 1$. Then we have that $\Pr[|S'| \geq K | w' = w] \leq 1/2v$. Finally, we consider running $S' \leftarrow \mathsf{GenSmallSet}^{S,U}(w)$, replacing U' with U. Recall that U is $(2^{n/10}, 2^{-n/4})$-wise independent even conditioned on S. Since $2^{n/10} \gg 2vQ = 2^{1+n/15+n/100}$, where vQ is the number of queries made by $\mathsf{GenSmallSet}$ when run on w, we can apply Theorem 4.2 to conclude that $\Pr[|S'| \geq K : U' = U, w' = w] \leq 1/2v + 2^{-n/4} \leq 1/v$, since we chose $v = 2^{n/15}$. Then in particular since $|S'| \leq v$ always, we have that $\mathbb{E}[|S'|] \leq (K-1)\Pr[|S'| < K] + v \Pr[|S'| \geq K] \leq (K-1) + 1 \leq K$.

Let e_j be the probability that $\mathsf{GenSmallSet}$ adds an element y_i to S' in the ith iteration. Then $\sum_{j=1}^{v} e_j = \mathbb{E}[|S'|] \leq K$. We also have that the e_j are monotonically decreasing since the y_i are identically distributed and thus the probability mass outside of the growing S' can only shrink. Thus $e_v \leq K/v$.

For an input $y \in S$, let M_y denote the total magnitude squared of y in all queries made by $V_*^{S,U}(w)$ to oracle S. Then measuring a random choice of the $\leq Q$ queries by V_*, we will obtain y with probability at least M_y/Q. Since $e_v \leq K/v$, this means that by the end of the loop, the expected total query weight of all points in S but not in S' is at most QK/v. By Markov's inequality, we therefore have that the query weight of points in $S \setminus S'$ is at most $\sqrt{QK/v}$, except with probability at most $\sqrt{QK/v}$. Recall that $\sqrt{QK/v}$ is negligible. Therefore, since this probability is negligible, we will therefore assume the total query weight of points in $S \setminus S'$ is at most $\sqrt{QK/v}$.

Lemma 3.4 shows that the difference in acceptance probability between $V_*^{S,U}(w)$ and $V_*^{S',U}(w))$ is at most $4\sqrt{Q \times \sqrt{QK/v}} = 4\sqrt[4]{Q^3K/v}$. Observe that $Q^3K/v = Q^4\sqrt{2Cp} + Q^3(q + \log_2(v))/v$. Plugging in our values for $Q = 2^{n/100}, v = 2^{n/15}, q = 2^{n/200}, p = 2^{-3n/10}$, we find that the difference in acceptance probability is $O(2^{-19n/600})$, which is negligible in n. Hence we have that $\Pr[V_*^{S',U}(w)) = 1] > \frac{2}{3} - \mathrm{negl}(n) > \frac{1}{2}$. □

Claim 6.4 and Claim 6.5 shows that V_* fails to decide $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation, contradicting it being a OI-QCMA verifier. Hence, $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation $\notin$ OI-QCMA. This completes the proof of Theorem 6.3. □

Corollary 6.6. *There exists a classical oracle relative to which* $\mathsf{QMA}^{\mathcal{O}} \neq \mathsf{QCMA}^{\mathcal{O}}$.

Proof. Theorem 6.2 and Theorem 6.3 show that $(\frac{7}{12}, \frac{2}{3})$-SpectralForrelation $\in$ OI-QMA $\setminus$ OI-QCMA. Invoking Theorem 3.3 provides a classical oracle separation between QMA and QCMA. □

Acknowledgements

We thank James Bartusek, Barak Nehoran, and Henry Yuen for helpful discussions on the implications of this work. JB is supported by Henry Yuen's AFORS (award FA9550-21-1-036) and NSF CAREER (award CCF2144219). JH acknowledges funding from the Harvard Quantum Initiative postdoctoral fellowship.

References

[AA09] Scott Aaronson and Andris Ambainis. "The need for structure in quantum speedups". In: *arXiv preprint arXiv:0911.0996* (2009) (cit. on p. 4).

[AA15] Scott Aaronson and Andris Ambainis. "Forrelation: A problem that optimally separates quantum from classical computing". In: *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*. 2015, pp. 307–316 (cit. on p. 5).

[Aar10] Scott Aaronson. "BQP and the polynomial hierarchy". In: *Proceedings of the forty-second ACM symposium on Theory of computing*. 2010, pp. 141–150 (cit. on p. 5).

[Aar21] Scott Aaronson. "Open problems related to quantum query complexity". In: *ACM Transactions on Quantum Computing* 2.4 (2021), pp. 1–9 (cit. on p. 3).

[AK07] Scott Aaronson and Greg Kuperberg. "Quantum versus classical proofs and advice". In: *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*. IEEE. 2007, pp. 115–128 (cit. on pp. 3, 9).

[AN02] Dorit Aharonov and Tomer Naveh. "Quantum NP-a survey". In: *arXiv preprint quant-ph/0210077* (2002) (cit. on p. 3).

[BBBV97] Charles H Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. "Strengths and weaknesses of quantum computing". In: *SIAM journal on Computing* 26.5 (1997), pp. 1510–1523 (cit. on p. 10).

[BHH16] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. "Local random quantum circuits are approximate polynomial-designs". In: *Communications in Mathematical Physics* 346 (2016), pp. 397–434 (cit. on p. 11).

[BK24] Shalev Ben-David and Srijita Kundu. "Oracle separation of QMA and QCMA with bounded adaptivity". In: *arXiv preprint arXiv:2402.00298* (2024) (cit. on p. 3).

[Cle11] Richard Cleve. *Classical Lower Bound for Simon's Problem*. 2011. URL: https://cs.uwaterloo.ca/~cleve/courses/F11CS667/SimonClassicalLB.pdf (cit. on p. 10).

[CN08] Donghoon Chang and Mridul Nandi. "A short proof of the PRP/PRF switching lemma". In: *Cryptology ePrint Archive* (2008) (cit. on p. 10).

[FK15] Bill Fefferman and Shelby Kimmel. "Quantum vs classical proofs and subset verification". In: *arXiv preprint arXiv:1510.06750* (2015) (cit. on p. 3).

[GLLZ21] Siyao Guo, Qian Li, Qipeng Liu, and Jiapeng Zhang. "Unifying presampling via concentration bounds". In: *Theory of Cryptography Conference*. Springer. 2021, pp. 177–208 (cit. on p. 4).

[Gri20] Darij Grinberg. "Notes on the combinatorial fundamentals of algebra". In: *arXiv preprint arXiv:2008.09862* (2020) (cit. on p. 18).

[HM23] Yassine Hamoudi and Frédéric Magniez. "Quantum Time–Space Tradeoff for Finding Multiple Collision Pairs". In: *ACM Transactions on Computation Theory* 15.1-2 (2023), pp. 1–22 (cit. on pp. 6, 7, 10).

[INN+21] Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. "Quantum search-to-decision reductions and the state synthesis problem". In: *arXiv preprint arXiv:2111.02999* (2021) (cit. on p. 3).

[Liu22] Qipeng Liu. "Non-uniformity and Quantum Advice in the Random Oracle Model". In: *Cryptology ePrint Archive* (2022) (cit. on p. 3).

[LLPY23] Xingjian Li, Qipeng Liu, Angelos Pelecanos, and Takashi Yamakawa. "Classical vs Quantum Advice and Proofs under Classically-Accessible Oracle". In: *arXiv preprint arXiv:2303.04298* (2023) (cit. on p. 3).

[LMY24] Jiahui Liu, Saachi Mutreja, and Henry Yuen. "QMA vs. QCMA and Pseudorandomness". In: *arXiv preprint arXiv:2411.14416* (2024) (cit. on pp. 3, 4).

[Lut11] Andrew Lutomirski. "Component mixers and a hardness result for counterfeiting quantum money". In: *arXiv preprint arXiv:1107.0321* (2011) (cit. on p. 3).

[MW05] Chris Marriott and John Watrous. "Quantum Arthur–Merlin games". In: *computational complexity* 14.2 (2005), pp. 122–152. DOI: 10.1007/s00037-005-0194-x (cit. on p. 24).

[NN24] Anand Natarajan and Chinmay Nirkhe. "A distribution testing oracle separation between QMA and QCMA". In: *Quantum* 8 (2024), p. 1377 (cit. on p. 3).

[NZ24] Barak Nehoran and Mark Zhandry. "A computational separation between quantum no-cloning and no-telegraphing". In: *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*. Schloss-Dagstuhl-Leibniz Zentrum für Informatik. 2024 (cit. on p. 3).

[Ser74] Robert J Serfling. "Probability inequalities for the sum in sampling without replacement". In: *The Annals of Statistics* (1974), pp. 39–48 (cit. on p. 16).

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. "Random unitaries in extremely low depth". In: *arXiv preprint arXiv:2407.07754* (2024) (cit. on pp. 7, 11, 12).

[Sim97] Daniel R Simon. "On the power of quantum computation". In: *SIAM journal on computing* 26.5 (1997), pp. 1474–1483 (cit. on p. 10).

[Tao10] Terrence Tao. "254a, notes 1: Concentration of measure". In: (2010). URL: https://terrytao.wordpress.com/2010/01/03/254a-notes-1-concentration-of-measure/ (cit. on p. 23).

[YZ24] Takashi Yamakawa and Mark Zhandry. "Verifiable quantum advantage without structure". In: *Journal of the ACM* 71.3 (2024), pp. 1–50 (cit. on p. 3).

[Zha15] Mark Zhandry. "Secure identity-based encryption in the quantum random oracle model". In: *International Journal of Quantum Information* 13.04 (2015), p. 1550014 (cit. on p. 7).

[Zha24] Mark Zhandry. "Toward Separating QMA from QCMA with a Classical Oracle". In: *arXiv preprint arXiv:2411.01718* (2024) (cit. on p. 4).

A Equivalence between oracle-aided and oracle-input separations

In this section, we prove the following theorem which shows that our oracle-input separation implies a classical oracle separation between QCMA and QMA.

Theorem 3.3. *There exists a classical oracle $\mathcal{O}$ such that* $\mathsf{QMA}^{\mathcal{O}} \neq \mathsf{QCMA}^{\mathcal{O}}$ *if and only if* $\mathsf{OI\text{-}QMA} \neq \mathsf{OI\text{-}QCMA}$

Proof. In one direction, assume a classical oracle $\mathcal{O}$ such that $\mathsf{QMA}^{\mathcal{O}} \neq \mathsf{QCMA}^{\mathcal{O}}$. Let $\mathsf{L}^{\mathcal{O}}$ be the separating language, and V a verifier for $\mathsf{L}^{\mathcal{O}}$.

We construct a language $\mathsf{OI\text{-}L}$ as follows. Let $Q(n)$ be a (polynomial) upper bound on the length of queries that V makes to $\mathcal{O}$ when given an instance x of length n. Let $\mathcal{O}_n$ be the portion of $\mathcal{O}$ corresponding to queries of length at most $Q(n)$. Then $|\mathcal{O}_n| \leq 2^{n^{\Theta(1)}}$.

Let $\mathcal{U}_n$ consist of strings of the form $(x, \mathcal{O}_n)$ where x has size n, and let $\mathsf{OI\text{-}L}$ be the set of $(x, \mathcal{O}_n)$ where $x \in \mathsf{L}^{\mathcal{O}}$. We can decide membership in $\mathsf{OI\text{-}L}$ as follows: given a witness state $|\psi\rangle$, first recover x by making n queries to $(x, \mathcal{O}_n)$. Then run $V^{\mathcal{O}_n}(x, |\psi\rangle)$. By our choice of $\mathcal{O}_n$ containing all of $\mathcal{O}$ that gets queried by V, we therefore have that $V^{\mathcal{O}_n}(x, |\psi\rangle)$ is identical to $V^{\mathcal{O}}(x, |\psi\rangle)$. As such, if V correctly decides if $x \in \mathsf{L}^{\mathcal{O}}$, then our verifier correctly decides in $(x, \mathcal{O}_n) \in \mathsf{OI\text{-}L}$. Thus, $\mathsf{OI\text{-}L} \in \mathsf{OI\text{-}QMA}$.

On the other hand, suppose there is a $\mathsf{OI\text{-}QCMA}$ verifier V_* that decides $\mathsf{OI\text{-}L}$. We can then readily obtain a QCMA verifier for $\mathsf{L}^{\mathcal{O}}$. On input instance x and witness w, simulate $V_*^{(x,\mathcal{O}_n)}(w)$ by answering queries to x with the bits of x, and queries to $\mathcal{O}_n$ by forwarding the queries to $\mathcal{O}$. If V_* decides membership in $\mathsf{OI\text{-}L}$, this exactly decides if $x \in \mathsf{L}^{\mathcal{O}}$.

We now turn to the other direction in the statement of Theorem 3.3. Assume that $\mathsf{OI\text{-}QMA} \neq \mathsf{OI\text{-}QCMA}$. Let $\mathcal{U}$ be the universe and $\mathsf{OI\text{-}L} \subseteq \mathcal{U}$ be the separating language, and V the $\mathsf{OI\text{-}QMA}$ verifier for $\mathsf{OI\text{-}L}$.

We construct our oracle $\mathcal{O}$ and associated language $L^{\mathcal{O}}$ as follows. $\mathcal{O}$ will be interpreted as a countably-infinite family of oracles $(\mathcal{X}_{n_i})_{i \in \mathbb{Z}^+}$ for integers $n_i \in \mathbb{Z}^+$. Let $\mathcal{O}_j = (\mathcal{X}_{n_i})_{i \leq j}$. By padding the witness with 0's size appropriately, we can assume that any potential QCMA verifier runs in quadratic time. Let $T_1, T_2, \cdots$ be an enumeration over all oracle-aided quadratic-time quantum algorithms. $\mathcal{O}$ and $\mathsf{L}^{\mathcal{O}}$ will be constructed by constructing $\mathcal{X}_{n_i}$ for $i = 1, 2, \cdots$ as follows: Consider the $\mathsf{OI\text{-}QCMA}$ verifier $V_i^{\mathcal{X}}(w)$ which has $\mathcal{O}_{i-1}$ hard-coded, and runs $T_i^{\mathcal{O}_{i-1},\mathcal{X}}(w)$. Since $\mathcal{O}_{i-1}$ is constant-sized, $V_i^{\mathcal{X}}(w)$ runs in quadratic time (though with a large constant overhead coming from $\mathcal{O}_{i-1}$). Let n_i be an integer and $\mathcal{X}_{n_i} \in \mathcal{U}_{n_i}$ be an instance such that both:

- V_i incorrectly decides $\mathcal{X}_{n_i}$ given classical witnesses/inputs. That is, either $\mathcal{X}_{n_i} \in \mathsf{OI\text{-}L}$ and $V_i^{\mathcal{X}_{n_i}}(w)$ rejects for all w, or $\mathcal{X}_{n_i} \notin \mathsf{OI\text{-}L}$ and there exists a w such that $V_i^{\mathcal{X}_{n_i}}(w)$ accepts.
- n_i is large enough so that the inputs to the function $\mathcal{X}_{n_i}$ are longer than the running time of $T_j^{\mathcal{O}_j}$ on inputs of length n_j for all $j < i$, meaning $T_j^{\mathcal{O}_j}$, and hence V_j, on inputs of length $n_j, j < i$ never query any input that is an input to $\mathcal{X}_{n_i}$.

Such an $\mathcal{X}_{n_i}$ is guaranteed to exist: that *some* $n_i, \mathcal{X}_{n_i}$ exist satisfying the first criteria follows immediately from the fact that $\mathsf{OI\text{-}L} \notin \mathsf{OI\text{-}QCMA}$. Suppose that there is no $n_i, \mathcal{X}_{n_i}$ satisfying the second criteria. This means there are only a finite number of $\mathcal{X}$ where V_i fails to correctly decide. But by hard-coding these bad instances along with the correct solutions, we can obtain a new verifier V_i' which correctly decides $\mathsf{OI\text{-}L}$, contradicting that $\mathsf{OI\text{-}L} \notin \mathsf{QCMA}$.

We then let $\mathsf{L}^{\mathcal{O}}$ consist of the strings 0^{n_i} such that $\mathcal{X}_{n_i} \in \mathsf{OI\text{-}L}$. We immediately see that $\mathsf{L}^{\mathcal{O}} \in \mathsf{QMA}^{\mathcal{O}}$: by making appropriate queries to $\mathcal{O}$, we can simulate the $\mathsf{OI\text{-}QMA}$ verifier $V^{\mathcal{X}_{n_i}}$, thereby deciding membership of 0^{n_i} in $\mathsf{OI\text{-}L}$.

We now show that $\mathsf{L}^{\mathcal{O}} \notin \mathsf{QCMA}^{\mathcal{O}}$. Consider a supposed QCMA verifier V_*. This corresponds to some T_i according to our enumeration. Then we argue that V_* incorrectly decides membership for 0^{n_i}. Indeed, we know that $T_i^{\mathcal{O}}$ in instance 0^{n_i} never queries on $\mathcal{X}_{n_j}$ for $j > i$, by our choice of n_j. Hence, it can be simulated as $T_i^{\mathcal{O}_i}$, or equivalently $T_i^{\mathcal{O}_{i-1},\mathcal{X}_{n_i}}$. Thus, V_* corresponds exactly to the verifier V_i. But we know that V_i incorrectly decides membership for $\mathcal{X}_{n_i}$. Hence, V_* is not a valid QCMA verifier. □