# The Pursuit For Uniqueness: Extending Valiant-Vazirani Theorem to the Probabilistic and Quantum Settings
*preliminary version*

Dorit Aharonov * Michael Ben-Or † Fernando G.S.L. Brandão ‡ Or Sattath §

October 27, 2008



**Abstract**

Valiant-Vazirani showed in 1985 [VV85] that solving NP with the promise that "yes" instances have only one witness is powerful enough to solve the entire NP class (under randomized reductions).

We are interested in extending this result to the quantum setting. We prove extensions to the classes Merlin-Arthur (MA) and Quantum-Classical-Merlin-Arthur (QCMA) [AN02]. Our results have implications on the complexity of approximating the ground state energy of a quantum local Hamiltonian with a unique ground state and an *inverse polynomial* spectral gap. We show that the estimation, to within polynomial accuracy, of the ground state energy of poly-gapped 1-D local Hamiltonians is QCMA-hard, under randomized reductions. This is in strong contrast to the case of constant gapped 1-D Hamiltonians, which is in NP [Has07]. Moreover, it shows that unless QCMA can be reduced to NP by randomized reductions, there is no classical description of the ground state of every poly-gapped local Hamiltonian which allows the calculation of expectation values efficiently.

Finally, we discuss a few obstacles towards establishing an analogous result to the class Quantum-Merlin-Arthur (QMA). In particular, we show that random projections fails to provide a polynomial gap between two witnesses.

# 1 Introduction and Results

## 1.1 Extending Valiant-Vazirani

One of the properties of the class NP is that the number of witnesses might vary from zero to exponentially many. How hard is it to distinguish between "no" instances and "yes" instances that have a unique witness? One might think that such a problem is easier than solving NP. In a celebrated result, Valiant and Vazirani [VV85] showed that access to an oracle which can decide between "no" and "unique yes" instances is enough to solve the NP-complete problem SAT, with high probability, using randomized reductions [1].

The classes MA, QCMA [AN02] and QMA [KVS+02] are probabilistic and quantum analogues of NP. Informally, we say a problem is in MA if for every "yes" instance there is a witness which makes the verifier to accept with high probability (e.g. in the range (2/3, 1)), while for "no" instances he only accepts with a small

*School of Computer Science and Engineering, The Hebrew University, Jerusalem, Israel. doria@cs.huji.ac.il.
†School of Computer Science and Engineering, The Hebrew University, Jerusalem, Israel. benor@cs.huji.ac.il.
‡Institute for Mathematical Sciences, Imperial College London. fernando.brandao@imperial.ac.uk
§School of Computer Science and Engineering, The Hebrew University, Jerusalem, Israel. sattath@cs.huji.ac.il.

[1] A promise problem A is reducible to B by a randomized reduction, if there exists a probabilistic polynomial Turing Machine (TM) $M$ and a polynomial $p$ s.t.:

- completeness: $x \in \mathrm{A}_{yes} \Rightarrow Pr_r(M(x,r) \in \mathrm{B}_{yes}) \geq 1/p(|x|)$
- perfect soundness: $x \in \mathrm{A}_{no} \Rightarrow \forall r\ M(x,r) \in \mathrm{B}_{no}$

where $r$ are the random bits of the TM $M$. We denote this by $A \preceq_R B$.

probability (e.g. in (0, 1/3)), no matter which witness is given to him. The class QCMA is defined in a similar manner, but now the verifier can use a quantum computer to decide whether to accept or not. In QMA, in turn, not only does the verifier use a quantum computer to check the proof, but also the proof itself is a quantum state composed of a polynomial (in the input size) number of qubits.

We can ask a similar question to that of Valiant and Vazirani about each of these classes: given access to an oracle that can only decide between "no" instances and "yes" instances which have a unique solution for MA, QCMA, or QMA, can we solve complete problems for those classes, with high probability? The quantum related questions are also motivated by physical questions about ground states of local Hamiltonians. We provide some interesting implications in this direction, which we will soon describe.

In this paper we partially solve these questions: we present a generalization of the Valiant-Vazirani result to MA and QCMA. We also discuss some obstructions towards establishing a similar result to QMA, which is left as an open problem.

We define UMA and UQCMA as the restrictions of MA and QCMA, respectively, to instances with a unique witness. Roughly speaking, in a "yes" instance of a problem in UMA or UQCMA, *one* proof convinces the verifier with probability larger than e.g. 2/3, while any other witness makes him accept with probability of at most $1/3$. In a "no" instance, the verifier accepts any witness with probability at most 1/3. Our two main results are:

**Theorem 1** *MA* $\overset{R}{=}$ *UMA* [2].

**Theorem 2** *UQCMA* $\overset{R}{=}$ *QCMA*.

The proofs of both theorems rely heavily on the Valiant-Vazirani construction [VV85, AB09], which can be divided into three components:

1. We could guess the size of the accepting witness set, and use a random "filter" with a certain degree of screening, which is determined by the set size. If we guess correctly, then with constant probability, exactly one witness will pass the filter.

2. We notice that it is not crucial to guess the exact size of the set - and a multiplicative approximation is enough. In this way, the possible number of guesses is reduced from exponentially many in the previous component, to linear (in the length of the witness).

3. we replace the random "filter" with a pseudo random "filter" - a universal hash function - without loosing any of the properties. These pseudo-random objects have the advantage of an efficient description, unlike truly random sets.

The probabilistic setting of MA and QCMA raises a new difficulty: on "yes" instances there might be an exponentially larger number of witnesses in the gap-interval (e.g. $(1/3, 2/3)$) than in the "yes" interval $(2/3, 1)$. Thus, a random choice of one of the witnesses - in the spirit of the Valiant-Vazirani approach - would, with overwhelming large probability, fail to choose a witness from the "yes" interval. The main idea in overcoming this obstacle is to divide the "gap" interval into polynomially many smaller intervals, and argue that in at least one of them, the number of witnesses inside it is not much larger than the number of witnesses in the intervals above it.

We can also define the class UQMA - a unique variant of QMA - with the hope of proving the analogous result. It is defined as follows: the conditions for a "no" instance are the same as in QMA, but for a "yes" instance, we demand that there exists a $|\psi\rangle$ which is accepted above the "yes"-threshold, and all states $|\phi\rangle$ orthogonal to it are accepted with probability below the "no"-threshold. Before we proceed to show that an analogous result for QMA is probably impossible to achieve using similar techniques to the ones we employ, we use this definition together with Theorem 2 to derive interesting implications.

---

[2]We say that the class $C_1$ is included in $C_2$ under randomized reduction, and denote it by $C_1 \overset{R}{\subseteq} C_2$ if for every $L_1 \in C_1$ there exists $L_2 \in C_2$ s.t. $C_1 \preceq_R C_2$.

## 1.2 Implications to Ground State and Hamiltonian Complexity

We say a Hamiltonian, acting on $n$ $d$-dimensional particles, is $k$-local if it can be written as a sum of $\mathsf{poly}(n)$ terms which act non-trivially at most on $k$ sites.

**Definition 3** $k$-LOCAL HAMILTONIAN*: We are given a $k$-local Hamiltonian on $n$ qubits $H = \sum_{j=1}^{r} H_j$ with $r = \mathsf{poly}(n)$. Each $H_j$ has a bounded operator norm $||H_j|| \leq \mathsf{poly}(n)$. We are also given two constants $a$ and $b$ with $b - a \geq 1/\mathsf{poly}(n)$. In "yes" instances, the smallest eigenvalue of $H$ is at most $a$. In "no" instances, it is larger than $b$. We should decide which one is the case.*

In a seminal work, Kitaev showed that the 5-LOCAL HAMILTONIAN problem is complete for QMA [Kit99]. Improvements in parameters (dimensionality and locality) were given in [KR03, KKR06, OT05], leading to the QMA-completeness of 1-D 2-LOCAL HAMILTONIAN [AGIK07], which is the variant of the original problem to one-dimensional nearest-neighbors Hamiltonians (with $d = 12$). The importance of these results stems not only from the fact that LOCAL HAMILTONIAN is probably the most representative QMA-complete problem, but also from the key role of local Hamiltonians and their ground-state energy in physics.

An important parameter when dealing with the complexity of ground states and local Hamiltonians is the *spectral gap* of local Hamiltonians, given by the difference of the ground and the first excited energy levels, $\Delta := \lambda_1(H) - \lambda_0(H)$. When the spectral gap is constant, the Hamiltonian is said to be gapped. When it is inverse polynomial, we say the Hamiltonian is poly-gapped.

What are the implications of a gap for the LOCAL HAMILTONIAN problem? A groundbreaking result by Hastings shows that ground states of 1-D gapped Hamiltonians have an efficient classical description, as a Matrix-Product-State (MPS) of polynomial bond dimension [Has07][3]. Since expectation values of local observables of an MPS can be calculated in polynomial time in the number of sites and in its bond dimension (see e.g. [PGVWC06]), Hastings' result implies that 1-D CONSTANT-GAP LOCAL HAMILTONIAN (the restriction of the original problem to 1-D gapped Hamiltonians) belongs to NP.

It has been asked whether such efficient descriptions might exist for the ground state of 1-D poly gapped Hamiltonians. We show that using Theorem 2, and some more work, one can deduce that the answer to this question is negative (under some reasonable complexity assumption). The reasoning is as follows.

We define the UNIQUE LOCAL HAMILTONIAN problem to be similar to the LOCAL HAMILTONIAN problem, where the conditions for a "no" instance are the same, but for a "yes" instance we demand that there exists a $|\psi\rangle$ with energy below the low-threshold, and all other eigenvalues are above the upper-threshold. We also define the UNIQUE 1-D 2-LOCAL HAMILTONIAN in a similar manner.

It is not difficult to show (by observing that the construction used in [AGIK07] preserves the uniqueness) that:

**Lemma 4** UNIQUE 1-D 2-LOCAL HAMILTONIAN *is UQMA-Complete.*

Together with Theorem 2, which implies that $\mathsf{QCMA} \overset{R}{\subseteq} \mathsf{UQCMA} \subseteq \mathsf{UQMA}$, we have

**Theorem 5** UNIQUE 1-D 2-LOCAL HAMILTONIAN *is QCMA-hard, under randomized reductions.*

From Theorem 5 we can deduce the following "no-go" corollary for the ground state of poly-gapped Hamiltonians. Consider any set of states which are (i) described by $\mathsf{poly}(n)$ parameters and (ii) from which one can efficiently compute expectation values of local observables. Matrix-Product-States are an example of such a set, and several others have recently been proposed [APD+06, Vid07, HKH+08]. We can show:

**Theorem 6** *Ground states of 1-D poly gapped local Hamiltonians cannot be approximated to inverse polynomial accuracy by states satisfying properties (i) and (ii), unless $\mathsf{QCMA} \overset{R}{=} \mathsf{NP}$.*

[3] A state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes n}$ has an MPS representation with bond dimension $D$ if it can be written as

$$|\psi\rangle = \sum_{i_1,...,i_n=1}^{d} \mathrm{tr}(A^{[1]}_{i_1} ... A^{[n]}_{i_n}) |i_1, ..., i_n\rangle, \tag{1}$$

with $A^{[k]}_i$ $D \times D$ matrices. Note that only $ndD^2$ complex numbers are needed to specify the state.

The reason is that "yes" instances of the UNIQUE 1-D 2-LOCAL HAMILTONIAN are poly-gapped, and therefore such a description would place UNIQUE 1-D 2-LOCAL HAMILTONIAN in NP.

To further analyze the complexity of the local Hamiltonian problem for poly-gapped Hamiltonians, we introduce a variant of the UQMA class, which we call poly-gapped QMA (PGQMA), as follows: in both "yes" and "no" instances we require there is a gap (given by a pre-determined quantity larger than an inverse polynomial in the input size) from the witness which accept with the largest probability to all the others. We show that the problem 1-D POLY-GAP LOCAL HAMILTONIAN, in which the Hamiltonians are promised to be poly-gapped, is complete for the class. We also present a simple randomized reduction from any UQMA problem to a PGQMA, which implies

**Theorem 7** 1-D POLY-GAP LOCAL HAMILTONIAN *is QCMA-hard, under randomized reductions.*

We thus see that, unless BQP $=$ QCMA [4], the determination of the ground energy of poly-gapped 1-D local Hamiltonians is an intractable problem for quantum computation. Note that this conclusion cannot be drawn from the previous lower bounds on the complexity of the problem [AGIK07, SCV08]. Indeed, the results of [AGIK07] concerning adiabatic quantum computation with a 1-D poly-gapped Hamiltonian indirectly imply that 1-D POLY-GAP LOCAL HAMILTONIAN is BQP-hard[5], while in [SCV08] the problem was shown to be hard for the class UP $\cap$ Uco-NP (the intersection of unique NP with unique co-NP), whose relation with BQP is unknown.

## 1.3 Impossibility Results for UQMA

Finally, we examine the UQMA case. We show that attempting to apply the brute force analogue of the previous proofs in the case of UQMA, we already fail in the first (inefficient) component. A new idea seems to be required, if an extension of the Valiant-Vazirani approach is possible at all for QMA.

To show this we construct a simple family of QMA "yes" instances which we believe captures the difficulty of the problem.

**Example 1** *Let $C$ be a quantum circuit on $l$ qubits, with the property that there exists a subspace $V$ of dimension 2, s.t.* $\forall|\psi\rangle \in V,\ Pr(C\ accepts\ |\psi\rangle) = 1$, *and* $\forall|\psi\rangle \in V^{\perp},\ Pr(C\ accepts\ |\psi\rangle) = 0$.

In the classical case, the analogous example of two solutions is easy to deal with by choosing a "filter" (hash-function) that screens about half of the witnesses. The natural quantum analogue to try, is to use a random projection that will reject half of the space. In proposition 1 we prove that such a transformation (even if it can be implemented efficiently) does not create an inverse polynomial gap between the two states in the subspace $V$: with probability exponentially close to 1, regardless of the dimensionality of the random projection, all states in $V$ will be accepted with probabilities exponentially close to each other.

The reason for this is that the projection of every $N$-dimensional vector on a $d$-dimensional random subspace is concentrated around $\frac{d}{N}$, with a standard deviation of order $\frac{\sqrt{d}}{N}$, for a sufficiently large $N$. Therefore, regardless of how we choose $d$, we always get that the gap is less than $\frac{1}{\sqrt{N}}$, which is exponentially small. Hence, the behavior of random sets - the filters in the classical setting - is very different from the behavior of random subspaces, the natural quantum analogue.

One might hope that a more refined measurement would help. In fact [Sen06] has shown that the two distributions resulting from applying a random von Neumann measurement on two arbitrary orthogonal states have a constant total variation distance with all but exponentially small probability. This sounds promising; Moreover, a similar effect can be achieved efficiently by quantum $t$-designs as shown by [AE07]. Unfortunately, a constant total variation distance between two distributions does not imply an efficient method to distinguish

[4] BQP is the class of problems which can be efficiently solved, with high probability, by a quantum computer

[5] The construction of [AGIK07] for adiabatic quantum computation with one-dimensional Hamiltonians provides a way to encode the outcome of any polynomial quantum computation into the expectation value of a measurement, in the computational basis, of the first site of the ground state of a 1-D poly-gapped local hamiltonian, with a zero ground state energy. By adding a small perturbation to the Hamiltonian, penalizing the first site when it is not in the zero state, and with a strength much smaller than the spectral gap, but still inverse polynomial in the number of sites, we can readily conclude that this construction shows that 1-D POLY-GAP LOCAL HAMILTONIAN is BQP-hard

between them; this problem is tightly related to complete problems for the complexity class SZK, which are not known to have a quantum polynomial time algorithm. Thus, the problem of whether UQMA $\stackrel{R}{=}$ QMA remains wide open.

### 1.4 Organization of the paper

The structure of the rest of the paper is as follows: in Section 2.1 we present the definitions. Section 3 reviews the proof of the Valiant-Vazirani Theorem, while Sections 4 and 5 contain the extension of the theorem to the classes MA and QCMA, respectively. In section 6 we discuss some alternate definitions of the class UQMA, and complete problems for this class. We also show that the two classes are equivalent, under randomized reductions. Finally, in section 7 we prove impossibility results regarding extending our results to QMA using similar ideas.

## 2 Definitions

We start by defining a few standard complexity classes which we will consider throughout the paper. Then we turn to the definition of unique versions of MA, QCMA, and QMA, which to the best of our knowledge, have not been formalized before.

### 2.1 Background Definitions

**Definition 8 (Nondeterministic Polynomial (NP))** *A language $L \in$ NP if there exists a Turing Machine (TM) $M$ which runs in polynomial time in its first argument s.t.:*

1. $x \in L \Rightarrow \exists y\ s.t.\ M(x,y)\ accepts.$
2. $x \notin L \Rightarrow \forall y\ M(x,y)\ rejects.$

**Definition 9 (Unique Nondeterministic Polynomial (UP))** *A promise problem $L = (L_{yes}, L_{no}) \in$ UP if there exists a Turing Machine (TM) $M$ which is polynomial in its first argument s.t.:*

1. $x \in L_{yes} \Rightarrow \exists y\ s.t.\ M(x,y)\ accepts$ *and* $\forall y' \neq y\ M(x,y')\ rejects.$
2. $x \in L_{no} \Rightarrow \forall y\ M(x,y)\ rejects.$

**Definition 10 (Merlin-Arthur (MA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ MA if there exists a probabilistic polynomial TM $M$ which is polynomial in its first argument, and its random bits are denoted by the string $r$, s.t.:*

1. $x \in L_{yes} \Rightarrow \exists y\ s.t.\ Pr_r(M(x,y,r)\ accepts) \geq 2/3.$
2. $x \in L_{no} \Rightarrow \forall y\ Pr_r(M(x,y,r)\ accepts) \leq 1/3.$

**Definition 11 (Quantum Classical Merlin-Arthur (QCMA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ QCMA if there exists a polynomial quantum circuit $U_x$ which can be computed in $poly(|x|)$ time, having $l(x)$ qubits as input and requiring $m(x)$ ancilla qubits initialized to $|0^m\rangle$, such that*

1. $x \in L_{yes} \Rightarrow \exists y\ s.t.\ \|\Pi_1 U_x(|y\rangle \otimes |0^m\rangle)\|^2 \geq 2/3.$
2. $x \in L_{no} \Rightarrow \forall y\ \|\Pi_1 U_x(|y\rangle \otimes |0^m\rangle)\|^2 \leq 1/3.$

*$\Pi_1$ is the projection onto $|1\rangle$ in the first qubit, i.e. $\Pi_1 := |1\rangle\langle 1| \otimes I_{l+m-1}$. We write $l = l(x)$ and $m = m(x)$ when $x$ can be understood from the context.*

**Definition 12 (Quantum Merlin-Arthur (QMA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ QMA if there exists a polynomial quantum circuit $U_x$ which can be computed in $poly(|x|)$ time, having $l(x)$ qubits as input and requiring $m(x)$ ancilla qubits initialized to $|0^m\rangle$, s.t.*

1. $x \in L_{yes} \Rightarrow \exists |\psi\rangle \ s.t. \ \|\Pi_1 U_x(|\psi\rangle \otimes |0^m\rangle)\|^2 \geq 2/3$.
2. $x \in L_{no} \Rightarrow \forall |\psi\rangle \ \|\Pi_1 U_x(|\psi\rangle \otimes |0^m\rangle)\|^2 \leq 1/3$.

$\Pi_1$ *is the projection onto $|1\rangle$ in the first qubit.*

## 2.2 New Definitions

We now describe the analogue unique versions for the classes MA and QCMA and QMA.

**Definition 13 (Unique Merlin-Arthur (UMA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ UMA if there exists a probabilistic TM $M$ which is polynomial in its first argument s.t.:*

1. $x \in L_{yes} \Rightarrow \exists y \ s.t. \ Pr_r(M(x, y, r) \ accepts) \geq 2/3$ *and* $\forall y' \neq y$, $Pr_r(M(x, y', r) \leq 1/3$.
2. $x \in L_{no} \Rightarrow \forall y \ Pr_r(M(x, y, r) \ accepts) \leq 1/3$.

**Definition 14 (Unique Quantum Classical Merlin-Arthur (UQCMA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ UQCMA if there exists a polynomial quantum circuit $U_x$ which can be computed in $poly(|x|)$ time, having $l(x)$ qubits as input and requiring $m(x)$ ancilla qubits initialized to $|0^m\rangle$, such that*

1. $x \in L_{yes} \Rightarrow \exists y \ s.t. \ \|\Pi_1 U_x(|y\rangle \otimes |0^m\rangle)\|^2 \geq 2/3$ *and* $\forall y' \neq y$, $\|\Pi_1 U_x(|y'\rangle \otimes |0^m\rangle)\|^2 \leq 1/3$
2. $x \in L_{no} \Rightarrow \forall y \ \|\Pi_1 U_x(|y\rangle \otimes |0^m\rangle)\|^2 \leq 1/3$.

$\Pi_1$ *is the projection onto $|1\rangle$ in the first qubit.*

**Definition 15 (Unique Quantum Merlin-Arthur (UQMA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ UQMA if there exists a polynomial quantum circuit $U_x$ which can be computed in $poly(|x|)$ time, having $l(x)$ qubits as input and requiring $m(x)$ ancilla qubits initialized to $|0^m\rangle$, s.t.*

1. $x \in L_{yes} \Rightarrow \exists |\psi\rangle \|\Pi_1 U_x(|\psi\rangle \otimes |0^m\rangle)\|^2 \geq 2/3$ *and* $\forall |\phi\rangle \perp |\psi\rangle$, $\|\Pi_1 U_x(|\phi\rangle \otimes |0^m\rangle)\|^2 \leq 1/3$
2. $x \in L_{no} \Rightarrow \forall |\psi\rangle \ \|\Pi_1 U_x(|\psi\rangle \otimes |0^m\rangle)\|^2 \leq 1/3$.

# 3 The Valiant-Vazirani Proof Revisited

In this section, we review the results of [VV85]. We divide the proof into three components, so that we can better understand which components of the original construction fail in the probabilistic and quantum setting. The main result proved by Valiant and Vazirani can be stated as follows:

**Theorem 16** *[VV85] If UP $\subseteq$ RP $\Rightarrow$ NP $\subseteq$ RP.*

The standard proof of the theorem works with the well known NP-complete problem SAT. We will not use it, as there is no simple variant of SAT which is complete for the classes MA and QCMA.

**Definition 17 (TRIVIAL NP PROBLEM (TNPP))** *The words in $L$ are tuples, $\langle V, x, l, t\rangle$, where V is a description of a deterministic Turing machine, x is a string of length n, and $l, t \in \mathbb{N}$, given in unary.*

*$\langle V, x, l, t\rangle \in L$ if there exists a $y$ with $|y| = l$ s.t. $V(x, y)$ accepts in $t$ steps.*

It can easily be seen that TNPP is NP-Complete. The following promise problem is a "unique" version of TNPP.

**Definition 18 (UNIQUE-NP PROMISE PROBLEM (UNPPP))** *The promise problem is $L = (L_{yes}, L_{no})$. The words in $L$ are tuples, $\langle V, x, l, t\rangle$, where V is a description of a deterministic Turing machine, x is a string of length n, and $l, t \in \mathbb{N}$, given in unary.*

*$\langle V, x, l, t\rangle \in L_{yes}$ if there exists exactly one string $y$ s.t. $|y| = l$ and $V(x, y)$ accepts in $t$ steps. $\langle V, x, l, t\rangle \in L_{no}$ if for all strings $y$ s.t. $|y| = t$, $V(x, y)$ does not accept in $t$ steps.*

## 3.1 Proof Sketch

We begin with an instance $\hat{I}$ and a language $L \in NP$, and we should decide if $\hat{I} \in L$. The first step is to use the completeness of $TNPP$ to find an instance $I = \langle V, x, l, t\rangle$ with the property $\hat{I} \in L \iff I \in TNPP$.

There are three main components in the proof, which we shall, now, explain.

**Component 1: The right random "filter" for the right size**

Let $W$ be the set of accepting witnesses: $W := \{y : |y| = l \; and \; V(x,y) \; accepts \; in \; t \; steps\}$, and let $|W| = w$. Notice that $I \in TNPP \iff w \neq 0$.

**Definition 19 (R-restriction)** *Let $R$ be a set of strings, each one of them of size $l$, with the property that there is an algorithm that answers whether $y \in R$ in exactly $T$ time steps. Given a Turing machine $V$, we call the following Turing machines the $R$-restriction of V, and denote it by $V_R$:*

1. *If $y \notin R$, Reject. Otherwise, Continue.*
2. *Run $V$ on $(x, y)$.*

We see the $R$-restriction as a filter added to the original problem, because the new machine accepts only accepting witnesses of the original machine, which belong to the set $R$.

Let us denote by $I'$ the instance $\langle V_R, x, l, t + T\rangle$. Component 1 takes the filter $R$ to be a random set, where each string in $\{0,1\}^l$ is chosen independently with probability $w^{-1}$. Notice that the Turing machine $V_R$ might not have a short description, because in order to decide whether $y \in R$, all the elements of $R$ should somehow be "hard-wired" to the machine. If $|R|$ is exponential in $l$, then by using Kolmogorov Theory arguments[CTWI06], there is no short description for such a circuit, therefore the description of $V_R$ will not be short. Therefore, the mapping between $I$ to $I'$ is not efficient. This drawback will be circumvent in component 3.

We claim that $I'$ will be in $UNPPP_{yes}$ with probability $\Omega(1)$. Let $W' = \{y : |y| = l$ and $V_R(x, y)$ accepts in $t+T$ steps$\}$. Defining $W = \{w_1, ..., w_{|W|}\}$,

$$\begin{aligned} Pr(I' \in UNPPP_{yes}) &= Pr(|W'| = 1) \\ &= Pr(|W \cap R| = 1) \\ &= Pr\left(\bigcup_{i=1}^{w} (w_i \in R \cap_{j \neq i} w_j \notin R)\right) \\ &= w\frac{1}{w}(1 - \frac{1}{w})^{w-1} \\ &\geq 1/e. \end{aligned} \tag{2}$$

The first equality follows from $I' \in UNPPP \iff w' = 1$ and the second from $W' = W \cap R$. The third is a direct consequence of the definition of $w_i$. The fourth stems from the facts that the events in the line above are all disjoint, and using the definition of the set $R$. Therefore, querying the oracle with $\langle V', x, l, t + t'\rangle$ results in a "yes" with probability of at least $\frac{1}{e}$.

Using this idea, we create $2^l$ instances, $I_1, ..., I_{2^l}$, one for every possible value of $w$: $I_j = \langle V_j, x, l, t + t'\rangle$. We claim:

**Lemma 20** *(Completeness) If $I \in TNPP$, then there exists a $j$ for which, with probability $\Omega(1)$ over the choice of $R$, $I_j \in UNPPP_{yes}$. (Soundness) If $I \notin TNPP$, then all the $I_j$ are in $UNPPP_{no}$.*

**Proof:** Completeness: Follows from the previous argument: one of the $I_j$'s is $I_w$. $I_w \in UNPPP_{yes}$ with probability of at least $1/e$. Soundness: $I \notin TNPP \Rightarrow W = \emptyset$. As $W_j = W \cap R_j$, $W_j = \emptyset$, and therefore $I_j \in UNPPP_{no}$. ■

Our algorithm consists of querying $UNPPP$ with $I_1, ..., I_{2^l}$. If one of the results is yes, we accept. The completeness asserts that for a "yes" instance, we accept with constant probability. The soundness asserts that we always reject in "no" instances.

**Component 2: Approximated "filter" also works**

The second component concerns the fact that we do not know the value $w$ and, therefore, in order to use the algorithm given in component 1, we need exponentially many queries to the $UNPPP$ oracle. The key to the solution is to realize that being wrong about the size of $w$ by a constant factor, only changes the probability of having a unique solution by another constant factor.

More explicitly, we transform our instance $I$ into a polynomial number of random instances: $I_1, I_2, ..., I_l$. These instances are formed by choosing random sets $R_k$ again; but now, each element is taken with probability $\frac{1}{2^k}$.

A similar statement to Lemma 20 also holds here. To analyze the completeness of the protocol, we notice that for some $k$, $2^k \leq w \leq 2^{k+1}$. Hence, for such $k$,

$$\begin{aligned} Pr(I_k \in UNPPP_{yes}) &= Pr(|W_k| = 1) \\ &= Pr(|W \cap R_k| = 1) \\ &= Pr\left(\bigcup_{i=1}^{w}(y_i \in W \cap_{j\neq i} y_j \notin W)\right) \\ &= w\frac{1}{2^k}(1-\frac{1}{2^k})^{w-1} \\ &\geq (1-\frac{1}{2^k})^{2^{k+1}-1} \geq e^{-2}. \end{aligned}$$

Therefore, when asking the oracle $l-1$ queries, at least one of the answers will be "yes", with probability of at least $1/e^2$. The soundness analysis uses the same argument as in component 1.

**Component 3: Approximated pseudo random filter is just as good**

The third component deals with the inefficiency of randomness: a random and exponential large set $R$ cannot be determined by a polynomial description. The solution is to replace the randomness by a suitable notion of pseudo-randomness. In this case, the pseudo-random objects of interest are pairwise independent universal hash functions [AB09].

**Definition 21 (pairwise independent hash functions)** *A family of functions $\mathbb{H}_{n,m}$ where each $h \in \mathbb{H}$, $h : \{0,1\}^n \to \{0,1,\}^m$, is called a pairwise independent universal family of hash-functions if:*

1. $$\forall y_1 \neq y_2 \in A,\ \forall a, b \in B, \quad Pr_{h\sim_{\mathcal{U}}\mathbb{H}}(h(y_1) = a \text{ and } h(y_2) = b) = \frac{1}{2^{2m}}$$

2. *There exists a Turing Machine $PRINT\text{-}H$ s.t. for every $n, m \in \mathbb{N}$ and $j \in \mathbb{H}_{n,m}$, $PRINT\text{-}H(n,m,j)$ prints a description of another Turing machine, which computes $h_j \in \mathbb{H}_{n,m}$. By abuse of notation, we also denote the Turing machine which computes $h_j$ by $h_j$. The printing is done in $poly(n,m)$ time.*

3. *The running time of each $h \in \mathbb{H}_{n,m}$ is bounded by some $poly(n,m)$ time.*

Note that this probability is the same as if the map $h$ was random, although $h$ has a short description (unlike a random function which has no compact description).

Instead of choosing $R_k$ to be a random set, we pick a random universal hash function $h_k$ from the set $H_{l,k+2}$; The set $R_k$ is $h_k^{-1}(0) = \{y|h_k(y) = 0\}$. Evaluating $h_k(y)$ is polynomial in $l$, and therefore, step 1 of $V_k$ takes only polynomial time. To conclude, our algorithm is described in Alg. 1.

**Input**: The tuple $\langle V, x, l, t\rangle$.
**Output**: if $x \in TNPP$ accept with some constant probability, if $x \notin TNPP$ reject (with probability 1)

1 **foreach** $k \in [l]$ **do**
2   Sample a hash-function uniformly at random $h_k \sim_{\mathcal{U}} \mathbb{H}_{l,k+2}$ and let $R_k = h_k^{-1}(0)$
3   Denote by $V_k$ the $R_k$-restriction of $V$.
4   Query the $UNPPP$ oracle with $I_k = \langle V_k, x, l, t + T_{l,k+2}\rangle$, and put the result in $r_k$. [a]
5 **end**
6 **if** $\exists k \; s.t. \; r_k = 1$ **then**
7   accept
8 **else**
9   reject
10 **end**

**Algorithm 1**: TNPP solver, which uses polynomially many queries to UNPPP

[a]We will denote by $T_{a,b}$ the running time of $h(y)$ where $h \in \mathbb{H}_{a,b}$. We need the reasonable assumption that the running time is the same for all $h$'s and $y$'s and that it is an easy to compute function. We changed the time $t$ to be $t + T_{l,i+2}$, because the machine $V_k(x, y)$ needs to do one evaluation of the hash function, compared to the machine $V$.

It hence suffices to prove lemma 20 in order to show $\mathsf{UP} \subseteq \mathsf{RP} \Rightarrow \mathsf{NP} \subseteq \mathsf{RP}$, because then Alg. 1 is in $\mathsf{RP}$. First, we need to show that the algorithm takes polynomial time. The only suspect is step 1. The preparation of the description $V_k$ takes polynomial time, as in the definition of hash function (definition 21).

Soundness: In the case that $I \notin TNPP$, then by the soundness of lemma 20, all the $r_k$'s in step 1 are false, and, therefore, in step 1 the condition does not hold, so we always reject.

Completeness: By combining the assumption that $UNPPP$ is in $\mathsf{RP}$, and the completeness of lemma 20, we have that if $I \in TNPP$, then with probability $\Omega(1)$ over the choice of $h_k$, $I_k \in UNPPP_{yes}$, and therefore for that $k$ the query in step 1 will return "accept" with probability $2/3$. Therefore, the overall probability of accepting is at least $\frac{2}{3}\Omega(1) = \Omega(1)$.

**Proof of Lemma 20:** Soundness: Same argument as before.

Completeness: We make use of the following lemma:

**Lemma 22** *Let $W \subset \{0,1\}^n$ of size $w$, such that $2^k \leq w \leq 2^{k+1}$, and let h be a random universal hash function from the set $\mathbb{H}_{l,k+2}$, which is a set of functions from $\{0,1\}^l$ to $\{0,1\}^{k+2}$. Then,*

$$Pr\left(|h^{-1}(0) \cap W| = 1\right) \geq 1/8.$$

.

We prove this lemma in Appendix A. Note that $I_k = \langle V_k, x, y, l, t + T_{l,k+2}\rangle \in UNPPP_{yes}$ is equivalent to $|W_k| = 1$. We have that $W_k = W \cap R_k = W \cap h_k^{-1}(0)$ and Lemma 22 tells us that $|h_k^{-1}(0) \cap W| = 1$ with probability at least $1/8$ over the choice of $h$.

The fact that the description of $V_k$ is efficient makes sure that step 1 of Alg. 1 only takes polynomial time. All the other steps can be easily seen to take polynomial time as well. ■

## 4 Valiant-Vazirani Extended to the Class MA

In this section we prove Theorem 1, which can also be formulated as:

**Theorem 23** *$\mathsf{UMA} \in \mathsf{RP} \Longrightarrow \mathsf{MA} \in \mathsf{RP}$.*

**Definition 24 (Trivial MA Promise Problem (TMAPP))** TMAPP $= (L_{yes}, L_{no})$. *The words in* TMAPP *are tuples, $\langle V, x, p_1, p_2, l, t\rangle$, where V is a description of a probabilistic Turing machine, x is a string of length n, and $0 \leq p_1 < p_2 \leq 1$, where $p_2 - p_1 \geq 1/poly(n)$, and $l, t \in \mathbb{N}$, given in unary.*

$\langle V, x, p_1, p_2, l, t\rangle \in L_{yes}$ *if there exists a string* $y$ *s.t.* $|y| = l$ *and* $Pr(V(x,y)\ accepts\ in\ t\ steps) \in$ "$yes - interval$".

$\langle V, x, p_1, p_2, l, t\rangle \in L_{no}$ *if for all strings* $y$ *of length* $l$, $Pr(V(x,y)\ accepts\ in\ t\ steps) \in$ "$no - interval$".

It can be easily seen that TMAPP is MA-Complete.

We start with a language $L \in$ MA and an instance $I'$ and we should decide whether $I' \in L$ or not. The first step, as was done in the $NP$ case, is to use the completeness of TMAPP, and reduce it to the question whether $\hat{I} = \langle \hat{V}, x, p_1, p_2, l, t\rangle \in \text{TMAPP}_{yes}$ or $\hat{I} \in \text{TMAPP}_{no}$.

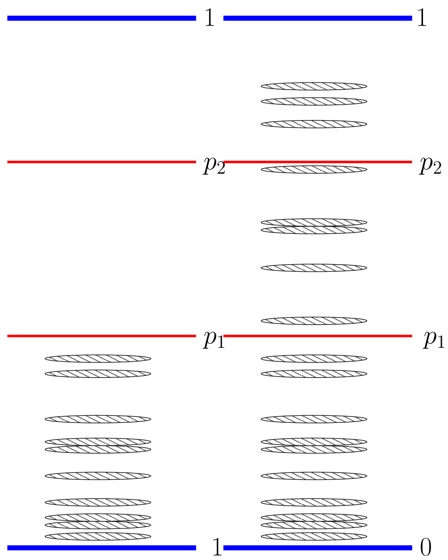


Figure 1: Typical "no" and "yes" instances
The y-axis is probability. The ellipses are all the $2^l$ different witnesses of a specific instance. The red lines outline the boundaries,$[p_1, p_2]$ - the maximal acceptance probability of a MA instance are promised not to be in that interval. The left one is a "no" instance, the maximal probability of acceptance is less than $p_1$. The right one is a "yes" instance, because the maximal probability of acceptance is greater than $p_2$.

Hence, our goal is to create a transformation which takes a $\text{TMAPP}_{yes}$ instance (right side of Fig. 1) to a $\text{UMAPP}_{yes}$ instance (Fig. 2) with constant probability, and a $\text{TMAPP}_{no}$ instance to a $\text{UMAPP}_{no}$ instance (left side of Fig. 1) with probability 1. We divide the potential witnesses into 3 groups, by their probability of acceptance:

$$\begin{aligned} Y_{no} &= \{y|\ |y| = l\ and\ Pr(\hat{V}(x,y)\ accepts\ in\ t\ steps) \in \text{“}no - interval''\} \\ Y_{gap} &= \{y|\ |y| = l\ and\ Pr(\hat{V}(x,y)\ accepts\ in\ t\ steps) \in \text{“}gap - interval''\} \\ Y_{yes} &= \{y|\ |y| = l\ and\ Pr(\hat{V}(x,y)\ accepts\ in\ t\ steps) \in \text{“}yes - interval''\} \end{aligned} \tag{3}$$

Let us look at the $R$-restriction of $V$, $V_R$, where $R$ is a random set and each element in $[2^l]$ is taken with some probability $p$. We denote it by $I' = \langle V_R, x, p_1, p_2, l, t + t'\rangle$, where $t'$ is the time taken for the machine $V_R$ to make its first step. Define $Y'_{yes}, Y'_{gap}, Y'_{no}$ for $I'$, as was done for $\hat{I}$ in Equation 3. For every $y$ of length $l$, denote by $f(y) = Pr(V(x,y)\ accepts\ in\ t\ steps)$, and $f'(y) = Pr(V'(x,y)\ accepts\ in\ t + t'\ steps)$.

**Observation 25**

$$f'(y) = \begin{cases} 0 & \text{if } y \notin R \\ f(y) & \text{if } y \in R \end{cases}$$

*Therefore,* $Y'_{yes} = Y_{yes} \cap R$ *and* $Y'_{gap} = Y_{gap} \cap R$.

Using the same method as in the NP case clearly fails, as we explicitly show in the following section.

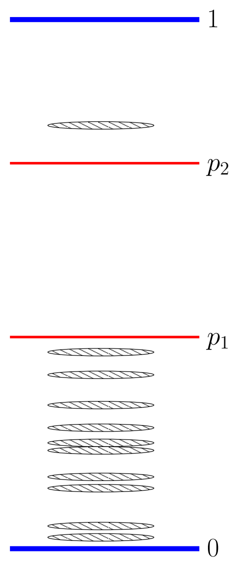


Figure 2: A “unique yes” instance
There is exactly one witness which is accepted with probability greater than $p_2$, and all others are accepted with probability smaller than $p_1$.

### 4.1 Problems with the first component

We present an instance that shows the failure of implementing component 1 in the probabilistic case. The example is a $I^{problematic} = \langle V^{problematic}, x, p_1, p_2, l, t\rangle \in$ TMAPP$_{yes}$ instance which can be seen in Fig.3, with the property that $|Y_{yes}^{problematic}| = 2, |Y_{gap}^{problematic}| = 2^l - 2$ and $|Y_{no}^{problematic}| = 0$.

Because the size of the set $Y_{gap}$ is exponentially bigger than $Y_{yes}$, we cannot “filter” - by using the random set $R$ - one element from $Y_{yes}$ and none from $Y_{gap}$ with non-negligible probability: Suppose we pick the size of $R$ by the set $W_0$, so each element is chosen with probability $1/2$. With probability $\Omega(1)$ exactly one element will be chosen from $W_0$, but about half of the elements of $W_1$ will also be chosen. Therefore, it fails to hold the second property of a UMAPP$_{yes}$ instance. If we pick elements in $R$ by the size $W_1$, which means that each element is picked with probability $\frac{1}{2^l-2}$ then with probability $(1 - \frac{1}{2^l-2})^2$ (which is exponentially close to one), no element will be picked from $W_0$, therefore it fails to hold the first property of a UMAPP$_{yes}$ instance.

### 4.2 the fourth component

The missing property in the example of section 4.1 is formalized in the next definition:

**Definition 26 (“lightweight-gap” instance)** *An instance $I = \langle V, x, p_1, p_2, l, t\rangle$ is a “lightweight-gap” TMAPP$_{yes}$ instance if it is a TMAPP$_{yes}$ instance, and $|Y_{gap}| \leq 3|Y_{yes}|$.*

Lemma 30 explains how this kind of instances does not have the problem that was shown in section 4.1. But first we will see how to create a very simple transformation which takes a general TMAPP$_{yes}$ instance to a “lightweight-gap” TMAPP$_{yes}$ instance:

**Lemma 27** *Let $\hat{I}$ be a TMAPP instance. There exists an efficient transformation that maps $\hat{I}$ to several instances $I_1, ..., I_{l-2}$ with the following properties:*

- *If $\hat{I} \in$ TMAPP$_{yes}$ then $\exists k\ s.t.\ I_k$ is a “lightweight-gap” TMAPP$_{yes}$ instance.*
- *If $\hat{I} \in$ TMAPP$_{no}$ then $\forall k\ I_k \in$ TMAPP$_{no}$ instance.*

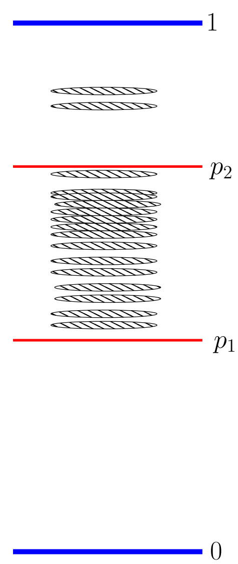


Figure 3: A problematic ma-instance: it has numerous witnesses with probability inside the "gap-interval" and very few in the "yes-interval".

**Proof:** The transformation is the following. We start by applying amplification: We can reduce the instance $\hat{I} = \langle \hat{V}, x, p_1, p_2, l, t \rangle$ to $I = \langle V, x, \frac{1}{l}, 1 - \frac{1}{l}, l, t \rangle$. This is done by using standard error reduction techniques.

**Observation 28** *Let $I_1 = \langle V, x, p_1, p_2, l, t \rangle$ and let $I_2 = \langle V, x, q_1, q_2, l, t \rangle$, where $[q_1, q_2] \subset [p_1, p_2]$.*

- $I_1 \in \text{TMAPP}_{yes} \Rightarrow I_2 \in \text{TMAPP}_{yes}$.
- $I_1 \in \text{TMAPP}_{no} \Rightarrow I_2 \in \text{TMAPP}_{no}$.

The observation follows immediately from the definitions of TMAPP.

The second step of the transformation is the following: we take the instance $I = \langle V, x, \frac{1}{l}, 1 - \frac{1}{l}, l, t \rangle$ and create $l - 2$ instance,$I_1, ..., I_{l-2}$, where $I_j = \langle V, x, \frac{j}{l}, \frac{j+1}{l}, l, t \rangle$. By observation 28, we know that if $I \in \text{TMAPP}_{yes} \Rightarrow \forall k\ I_k \in \text{TMAPP}_{yes}$, and that $I \in \text{TMAPP}_{no} \Rightarrow \forall k\ I_k \in \text{TMAPP}_{no}$.

But in the case of a "yes" instance, the lemma demands a "lightweight-gap" $\text{TMAPP}_{yes}$ instance. This is achieved using the following observation:

**Observation 29 (Existence of lightweight range)** *We define $l$ ranges: $r_j = [\frac{j}{l}, \frac{j+1}{l})$, $1 \leq j \leq l - 1$. We define*

$$Y_j = \{y |\ |y| = l \text{ and } Pr(\hat{V}(x, y) \text{ accepts in } t \text{ steps}) \in r_j\}$$

*If $I = \langle V, x, \frac{1}{l}, 1 - \frac{1}{l}, l, t \rangle \in \text{TMAPP}_{yes}$, then there exists a $j$ s.t. $|Y_j| < 3|Y_{j+1}|$.*

**Proof:** First, notice that $|Y_l| \geq 1$, due to the fact that $I \in \text{TMAPP}_{yes}$. Now, assume that the inequality does not hold for every j, i.e. $|Y_j| \geq 3|Y_{j+1}|$. Then, $|Y_1| \geq 3^{l-1} > 2^l$. The total number of the witnesses is $2^l$. Contradiction. ■

All we need to notice to prove lemma 27 is that if $|Y_j| < 3|Y_{j-1}|$, then $I_j$ is a "lightweight-gap" $\text{TMAPP}_{yes}$ instance. Observation 29 asserts that such a $j$ indeed exists. ■

Until now we have shown how to transform the instance to a "lightweight-gap". The following lemma proves that component 1 works for this kind of instances:

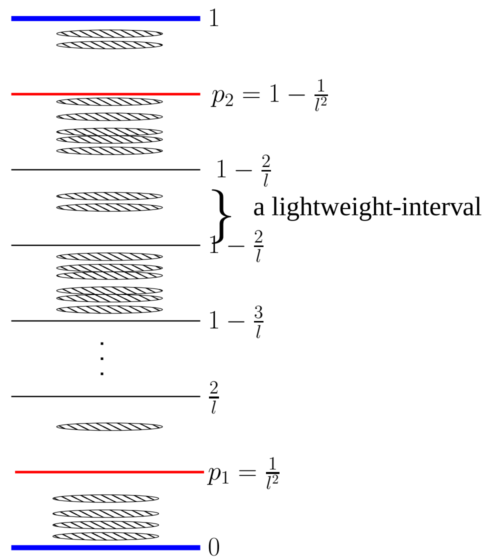


Figure 4: A yes-instance, with its lightweight range.

**Lemma 30** *Suppose $I = \langle V, x, p_1, p_2, l, t\rangle$ is a lightweight-gap* TMAPP$_{yes}$ *instance. Define $I' = \langle V_R, x, p_1, p_2, l, t+t'\rangle$, where $V_R$ is the R-restriction of $V$ where each element in $R$ is taken with probability $p = \frac{1}{|Y_{gap}|+|Y_{yes}|}$. Then, with probability $\Omega(1)$ (over the choice of R), $I'$ is a* UMAPP$_{yes}$ *instance.*

**Proof:**

As was shown in component 1, with probability $\Omega(1)$ exactly one witness will be picked from the set $Y_{yes} \cup Y_{gap}$. The probability that the instance is from the set $Y_{yes}$ is proportional to its size. Therefore $Pr(I' \in \text{UMAPP}_{yes}) = \Omega(1)\frac{|Y_{yes}|}{|Y_{gap}|+|Y_{yes}|} \geq \frac{1}{4}\Omega(1)$. ■

Component 2 works without any change in the probabilistic setting: a constant approximation of the size $|Y_{yes}|$ is sufficient. In order to adapt component 3 to the present case, we need a simple variant of lemma 22:

**Lemma 31** *Let $S \subset \{0,1\}^l$ of size $b$, such that $2^k \leq b \leq 2^{k+1}$, $S_1 \subset S$ of size $a$, and $S_2 = S \setminus S_1$. Let h be picked randomly from the set $\mathbb{H}_{n,k+2}$. Then,*

$$Pr(|h^{-1}(0)\bigcap S_1| = 1 \wedge |h^{-1}(0)\bigcap S_2| = 0] \geq \frac{a}{8b}$$

.

The proof is given in Appendix A. We apply lemma 31 to our construction by setting $S_1 = Y_{yes},\ S_2 = Y_{gap},\ S = S_1 \cap S_2$.

### 4.3 Putting It All Together

Assuming UMAPP $\in$ RP, then algorithm 2, which solves TMAPP, is also in RP.

**Input**: $I = \langle V, x, 1-\frac{1}{l}, \frac{1}{l}, l, t\rangle$, where V is a description of a probabilistic Turing machine, x is a string of length n, and $0 \leq p_1 \leq p_2 \leq 1$, where $p_2 - p_1 \geq 1/poly(n)$, and $l, t \in \mathbb{N}$, given in unary.

**Output**: if $x \in$ TMAPP$_{yes}$ accept with some constant probability, if $x \in$ TMAPP$_{no}$ reject (with probability 1)

**foreach** $k \in [l-2]$ **do**
  Define $I_k = \langle V, x, \frac{k}{l}, \frac{k+1}{l}, l, t\rangle$.
  **foreach** $b \in [l]$ **do**
    Sample a hash-function in random $h_b \in \mathbb{H}_{n,b+2}$. Denote by $R_b = h_b^{-1}(0)$
    Create the $R_b$-restriction of $V$, $V_b$:
    **if** $h_b(y) \neq 0$ **then**
      **return** *"no"*
    **else**
      $result \leftarrow$ Run (simulate) $V(x,y)$
      **return** *result*
    **end**
    Define $I_{k,b} = \langle V_b, x, \frac{k}{l}, \frac{k+1}{l}, l, t + T_{l,b+2}\rangle$.[a]
    Query the UMAPP oracle with $I_{k,b}$ and put the result in $r_{k,b}$ .
  **end**
**end**
**if** $\exists k, b\ s.t.\ r_{k,b} = 1$ **then**
  accept
**else**
  reject
**end**

**Algorithm 2**: TMAPP solver, which uses polynomially many queries to UMAPP

[a] We will denote by $T_{a,b}$ the running time of $h(y)$ where $h \in \mathbb{H}_{a,b}$. We need the reasonable assumption that the running time is the same for all $h$'s and $y$'s and that it is an easy to compute function. We have changed the time $t$ to be $t + T_{l,i+2}$ because the machine $V_k(x,y)$ needs to do one evaluation of the hash function, compared to the machine $V$, and therefore we need the additional time.

That the algorithm takes polynomial time can be seen in the same manner as the NP case. For the soundness, we have that $\forall k, b\ I \in$ TMAPP$_{no} \Rightarrow I_{k,b} \in$ TMAPP$_{no}$, by using observation 28 and observation 25. Because a TMAPP$_{no}$ instances is also a UMAPP$_{no}$ instance, step 2 will always output 0, and therefore in step 2 we will always reject. Finally, let us analyze the completeness of the protocol. We know that $I \in$ TMAPP$_{yes}$. According to lemma 27, for some $k$, $I_k$ is a "lightweight-gap" TMAPP$_{yes}$ instance. Define $Y^k_{yes}, Y^k_{gap}$ for $I_k$ in similar manner to Equation (3). According to lemma 31, with $S_1 = Y^k_{yes},\ S_2 = Y^k_{gap},\ S = S_1 \cap S_2$, we have that $I_{k,b} \in$ UMAPP$_{yes}$, for a $b$ such that $2^b \leq Y_k \leq 2^{b+1}$, with probability $\frac{1}{24}$.

# 5 Valiant-Vazirani Extended to the class QCMA

The proof of Theorem 2 is identical to the MA case.

Theorem 2 can also be formulated as:

**Theorem 32** *UQCMA $\in$ RP $\Longrightarrow$ QCMA $\in$ RP.*

We define the QCMA analogue of TMAPP and UMAPP to be:

**Definition 33 (TQCMAPP)** TQCMAPP $= (L_{yes}, L_{no})$. *The words in* TQCMAPP *are tuples, $\langle U, p_1, p_2\rangle$ where $U$ is a description of a quantum circuit, with input of size $l$, s.t.:*

1. $\langle U, p_1, p_2 \rangle \in L_{yes}$ *if there exists a string* $y$ *of length l, s.t.* $Pr(U \; accepts \; |y\rangle) \in$ "$yes - interval$".

2. $\langle U, p_1, p_2 \rangle \in L_{no}$ *if for all strings* $y$ *of length l* $Pr(U \; accepts \; |y\rangle) \in$ "$no - interval$".

**Definition 34 (UQCMAPP)** UQCMAPP $= (L_{yes}, L_{no})$. *The words in* UQCMAPP *are tuples,* $\langle U, p_1, p_2 \rangle$ *where* $U$ *is a description of a quantum circuit, with input of size* $l$*, s.t.:*

1. $\langle U, p_1, p_2 \rangle \in L_{yes}$ *if there exists a string* $y$ *of length l, s.t.* $Pr(U \; accepts \; |y\rangle) \in$ "$yes - interval$" *and* $\forall y' \neq y \; Pr(U \; accepts \; |y\rangle) \in$ "$no - interval$".

2. $\langle U, p_1, p_2 \rangle \in L_{no}$ *if for all strings* $y$ *of length l* $Pr(U \; accepts \; |y\rangle) \in$ "$no - interval$".

All the steps realized previously can also be done here: We begin with a language $L \in$ QCMA and an instance $I'$, and we need to decide whether $I' \in L$ or not. We use the completeness of TQCMAPP to reduce it to the question whether $\hat{I} = \langle \hat{U}, p_1, p_2 \rangle \in L$ or not. Notice that in order to use component 4, and apply lemma 27, we need to perform gap amplification, i.e. to transform $\langle \hat{U}, p_1, p_2 \rangle$ to $\langle U, \frac{1}{l}, 1 - \frac{1}{l} \rangle$. This is not a problem, because standard amplification works also for QCMA: Given $y$ we can create several copies of it without worrying about the "no cloning theorem", by measuring $y$ in the standard basis, without disturbing $|y\rangle$.

The TQCMAPP solver appears in Alg. 3.

**Input**: $I = \langle U, \frac{1}{l}, 1 - \frac{1}{l} \rangle$, where $U$ is a description of a Quantum Circuit, and $0 \leq p_1 \leq p_2 \leq 1$, where $p_2 - p_1 \geq 1/poly(n)$

**Output**: if $x \in$ TMAPP$_{yes}$ accept with some constant probability, if $x \in$ TMAPP$_{no}$ reject (with probability 1)

**foreach** $k \in [l-2]$ **do**
    Define $I_k = \langle U, \frac{k}{l}, \frac{k+1}{l} \rangle$.
    **foreach** $b \in [l]$ **do**
        Sample a hash-function in random $h_b \in \mathbb{H}_{n,b+2}$. Denote by $R_b = h_b^{-1}(0)$
        Create the $R_b$-restriction of $U$, $U_b$, which is implemented by a quantum circuit:
        **if** $h_b(y) \neq 0$ **then**
            **return** *"no"*
        **else**
            $result \leftarrow$ Run the circuit $U$ on the state $|y\rangle$,
            **return** *result*
        **end**
        Define $I_{k,b} = \langle U_b, \frac{k}{l}, \frac{k+1}{l}, \rangle$.
        Query the UQCMAPP oracle with $I_{k,b}$ and put the result in $r_{k,b}$ .
    **end**
**end**
**if** $\exists k, b \; s.t. \; r_{k,b} = 1$ **then**
    accept
**else**
    reject
**end**

**Algorithm 3**: TQCMAPP solver, which uses polynomially many queries to UQCMAPP

Soundness and Completeness follow from the same arguments used in the MA case. This ends the proof of Theorem 2.

# 6 The Robustness of UQMA

## 6.1 Discussion about QMA and the Marriott-Watrous Formalism

In this section we discuss the robustness of our definition of unique QMA and prove Lemma 4.

From Definition 12 we see that for a given QMA verification scheme and a state $|\psi\rangle$, its probability of acceptance is:

$$Pr(\text{verifier accepts } |\psi\rangle) = \|\Pi_1 U_x(I \otimes |0^m\rangle)|\psi\rangle\|^2$$

A useful operator in this context, as defined in [MW05], is the following

$$Q = (I_m \otimes \langle 0^m|)U^\dagger \Pi_1 U(I \otimes |0^m\rangle). \tag{4}$$

Note that

$$Pr(\text{verifier accepts } |\psi\rangle) = \langle\psi|Q|\psi\rangle. \tag{5}$$

As $Q$ is Hermitian, there is a basis of orthonormal eigenvectors $\{|\psi_i\rangle\}_{i=1}^{2^l}$ for which $Q = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$, where $\lambda_i(Q) \geq \lambda_{i+1}(Q)$ are the eigenvalues of $Q$. Note that by knowing the eigenvectors and eigenvalues of $Q$ we can find out the acceptance probability of every witness in a simple way

$$\begin{aligned} \langle\psi|Q|\psi\rangle &= \sum_{i,j} a_i^* a_j \langle\psi_i|Q|\psi_j\rangle \\ &= \sum_{i,j} a_i^* a_j \lambda_j \langle\psi_i|\psi_j\rangle = \sum_i |a_i|^2 \lambda_i, \end{aligned} \tag{6}$$

where $a_i = \langle\psi_i|\psi\rangle$.

Let us consider another possible definition of the class UQMA.

**Definition 35 (UQMA)** *A promise problem $L = (L_{yes}, L_{no}) \in$ UQMA if there exists a polynomial quantum circuit $U_x$ which can be computed in $poly(|x|)$ time, having $l(x)$ qubits as input and requiring $m(x)$ ancilla qubits initialized to $|0^m\rangle$, s.t.*

1. $x \in L_{yes} \Rightarrow \lambda_1(Q) \geq 2/3$ *and* $\lambda_2(Q) \leq 1/3$.
2. $x \in L_{no} \Rightarrow \lambda_1(Q) \leq 1/3$.

*Where $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_{2^{l(x)}}$ are the eigenvalues of $Q$.*

**Lemma 36 (Equivalence of Definitions 15 and 35)** *A language $L = (L_{yes}, L_{no}) \in$ UQMA according to Definition 15 $\Longleftrightarrow L \in$ UQMA according to Definition 35*

**Proof:** We start proving that given a $I \in L_{yes}$ according to Definition 15, it is also in $L_{yes}$ according to Definition 35. We now from Definition 15 that there is state $|\psi\rangle$ which is accepted with probability of at least $2/3$. According to Eq. (5), the acceptance probability of $|\psi\rangle$ is $\langle\psi|Q|\psi\rangle = p \geq 2/3$. From Eq. (6), in turn, we see that $p$ can be written as a convex combination of the $\lambda$'s. Therefore, $\lambda_1 \geq 2/3$.

We now prove that $\lambda_2 \leq 1/3$. Denote by $V$ the subspace spanned by the eigenvectors with eigenvalue greater than $1/3$. Note that $\forall|\phi\rangle \in V$ $\langle\phi|Q|\phi\rangle > 1/3$. If $dim(V) \geq 2$, there must exist a $|\phi\rangle \in V$ orthogonal to $|\psi\rangle$ and, therefore, the acceptance probability of $|\phi\rangle$ is greater than $1/3$, which is in contradiction to the properties of an $L_{yes}$ instance according to definition 15.

The other directions is straightforward. ■

We now turn to the proof of Lemma 4. Let us start with the precise definition of the problem UNIQUE 1-D 2-LOCAL HAMILTONIAN:

**Definition 37** UNIQUE 1-D 2-LOCAL HAMILTONIAN*: We are given a 2-local Hamiltonian on $n$ $d$-dimensional sites $H = \sum_{j=1}^r H_j$ with $r =$ poly$(n)$ arranged in a line. Each $H_j$ has a bounded operator norm $||H_j|| \leq$ poly$(n)$. We are also given two constants $a$ and $b$ with $b - a \geq 1/$poly$(n)$. In "yes" instances, the smallest eigenvalue of $H$ is at most $a$ and all the other eigenvalues are above $b$. In "no" instances, the smallest eigenvalue is larger than $b$. We should decide which one is the case.*

We now prove Lemma 4. That the problem is in UQMA can be seen by the following verification procedure. We expect as a proof the unique ground state of $H$. Given a witness $|\psi\rangle$, we use the phase estimation algorithm (see e.g. Ref. [WZ06]) to determine, within inverse polynomial accuracy $\delta$ with exponentially high probability, its energy, i.e. $\langle\psi|H|\psi\rangle$. Case it is smaller than $a+\delta$, we accept; otherwise we reject. It is clear that in "yes" instances, there is one witness which is accepted with probability exponentially close to one (the ground state of $H$), while any state orthogonal to it is accepted only with an exponentially small probability (which is the probability that the phase estimation does not give the correct answer).

The hardness of the problem for UQMA is a simple application of the construction of [AGIK07], which presents a reduction from any problem in QMA to 1-D 2-LOCAL HAMILTONIAN with $d = 12$. The details of the construction are not important here. We only note that the low-lying eigenvectors of the Hamiltonian considered are well approximated, within an inverse polynomial, to a class of states parametrized by all possible proofs - called history states - with the property that two orthogonal proofs give raise to two orthogonal history states. Moreover, the probability of acceptance of a given proof is imprinted in the energy of the associated history state - again up to inverse polynomial accuracy. It is then clear that a problem in UQMA will give raise to valid instance of UNIQUE 1-D 2-LOCAL HAMILTONIAN, since in "yes" instances of the problem (which is the only case we must analyze), the second eigenvalue of the Hamiltonian, which is well approximated by the energy of the history state associated to the witness which has the *second* highest probability of acceptance, will be separated from the ground state energy by a constant factor.

## 6.2 Yet Another New Class and its Equivalence To UQMA

One might define a similar class to QMA, with the additional promise of the gap of its acceptance probability.

**Definition 38 (Poly-Gapped QMA (PGQMA))** *A promise problem $L = (L_{yes}, L_{no}) \in$ GQMA if there exists a polynomial $\delta(|x|)$, and a polynomial quantum circuit $U_x$ which can be computed in $poly(|x|)$ time, having $l(x)$ qubits as input and requiring $m(x)$ ancilla qubits initialized to $|0^m\rangle$, s.t.*

1. $x \in L_{yes} \Rightarrow \lambda_1(Q) \geq 2/3$ *and* $(\lambda_1(Q) - \lambda_2(Q)) \geq \delta(|x|)$.
2. $x \in L_{no} \Rightarrow \lambda_1 \leq 1/3$ *and* $(\lambda_1(Q) - \lambda_2(Q)) \geq \delta(|x|)$.

*Where $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_{2^{l(x)}}$ are the eigenvalues of the operator $Q$, defined in Eq. (4).*

The above definition is motivated by the LOCAL HAMILTONIAN problem, with the additional promise that the spectral gap of the Hamiltonian is inverse polynomial. Its one dimensional version is defined as follows.

**Definition 39** 1-D POLY-GAP LOCAL HAMILTONIAN*: We are given a 2-local Hamiltonian on $n$ $d$-dimensional sites $H = \sum_{j=1}^{r} H_j$ with $r =$ poly$(n)$ arranged in a line. Each $H_j$ has a bounded operator norm $||H_j|| \leq$ poly$(n)$. We are also given three constants $a$, $b$ and $\Delta$ with $b-a, \Delta \geq 1/$poly$(n)$. We have the promise that the spectral gap of $H$ is larger than $\Delta$. In "yes" instances, the smallest eigenvalue of $H$ is at most $a$. In "no" instances, the smallest eigenvalue is larger than $b$. We should decide which one is the case.*

As in the unique case, we can show

**Lemma 40** 1-D POLY-GAP LOCAL HAMILTONIAN*is PGQMA-Complete.*

The proof is completely analogous to the reasoning we provided for Lemma 4. In order to prove Theorem 7, we need the following result.

**Lemma 41** *PGQMA $\stackrel{R}{=}$ UQMA.*

**Proof:** We first show that UQMA $\subset$ PGQMA. This inclusion is not immediate because of the following reason: If $I \in L_{no} \in$ UQMA, then we know that $\lambda_1(Q) \leq 1/3$, but we do not know whether $(\lambda_1(Q) - \lambda_2(Q)) \geq \delta$.

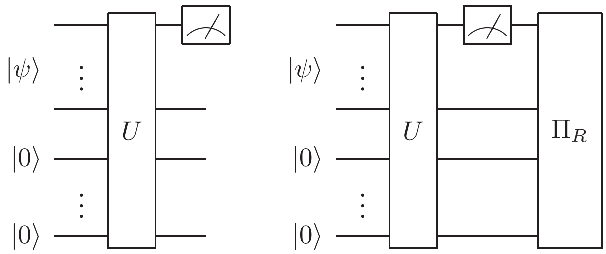


Figure 5: A quantum R-restriction. On the left: a general description of a QMA verification scheme. On the right: its $R$-restriction, where $\Pi_R$ is the projection on the subspace $R$. The state is accepted only if in both measurements the outcome was 1.

In order to resolve this issue, we use the amplification property of QMA, and change the "no"-probability to be $1/3 - \delta$ instead of $1/3$: so we have $\lambda_1(Q) \leq 1/3 - \delta$. Then, by a simple construction which we shall explain in the sequel, we add a single state which is accepted with probability $1/3$, having $\lambda_1(Q) = 1/3$ and $\lambda_2(Q) \leq 1/3 - \delta$, which provides the necessary gap.

Adding the $1/3$-eigenvalue is done by changing the circuit: we append another qubit to the input qubits, and measure it in the beginning of the circuit. If its state is 0, then we proceed as before. If it is 1, we measure all other input qubits in the computational basis. If all of them are 1, we accept with probability 1/3. Otherwise we reject. A simple calculation shows that the action of such a procedure is exactly as we want: it adds one $1/3$-eigenvalue, and $2^l - 1$ 0-eigenvalues, which do not concern us.

We now show that PGQMA $\overset{R}{\subseteq}$ UQMA. This is again not immediate, as case $I \in L_{yes} \in$ PGQMA, we know that $\lambda_1(Q) \geq 2/3$, but we do not know whether $\lambda_2(Q)$ is below the "no"-probability. For this we use the fact that $\mathsf{UQMA}_{1/3,2/3} = \mathsf{UQMA}_{a,b}$, where $(b-a) \geq 1/poly$. We know that for a $I \in L_{yes}$ there exists a for which $\lambda_1(Q) \geq 2/3 + (j+1)\frac{\delta}{2}$ and $\lambda_2(Q) \leq 2/3 + j\frac{\delta}{2}$. So, we give the circuit as a $\mathsf{UQMA}_{2/3+j\frac{\delta}{2},2/3+(j+1)\frac{\delta}{2}}$ problem, for $j = 1, \ldots, \lfloor j \rfloor$, and for at least one $j$, it will be in $L_{yes}$. Thus by picking $j$ at random, we get the required property. It is also easy to see that we have soundness in the above construction. ■

# 7 The QMA Case

## 7.1 Random Projections Fail to Create Inverse Polynomial Gap

As mentioned earlier, we have divided the proof of the Valiant-Vazirani Theorem into 3 components. Component 1 solves the problem in the simple case where the number of the accepting witnesses is known; Component 2 improves it by observing that the size of the set can be only approximated, without a considerable effect on the probability of acceptance; Finally, Component 3 shows that we may achieve the same results by using a two-universal hash function instead of a random function, rendering the reduction efficient.

In this section we show that even in the case where the number of solutions is known, as in component 1, we cannot - at least in the most direct approach - create a transformation that maps it to a "unique instance". The main difficulty in the QMA case is that we do not know in which basis to operate. Notice that if there exists a description (which Merlin can supply) of how to efficiently transform a standard basis state to one of the states that is accepted with probability greater than $2/3$, then the problem is in QCMA.

Let us define a possible quantum analogue of a $R$-restriction. A natural generalization is - instead of restricting to witnesses which belong to some set $R$ - to project onto some subspace $R$; We call this procedure a quantum $R$-restriction. As we did in the discussion of component 1, we will not consider the efficiency of implementing the restriction. A diagram of a general circuit and its $R$-restriction is given in Figure 7.1.

While the relevant operator for the original verification is $Q = (I_l \otimes \langle 0^m|)U^\dagger \Pi_1 U(I_l \otimes |0^m\rangle)$, after the the $R$-restriction it is given by $Q_R = (I_m \otimes \langle 0^m|)U^\dagger \Pi_1 \Pi_R \Pi_1 A(I_m \otimes |0^k\rangle)$, where $\Pi_R$ is a projection onto the subspace $R$. The quantum analogue of component 1 consists of taking the subspace $R$ to be a random subspace of dimension $d$, chosen accordingly to the Haar measure, for some convenient $d$. The next proposition shows that this approach, unfortunately, fails.

**Proposition 1** *For every $\epsilon > 0$, with probability larger than $1-\epsilon$, applying the quantum random $R$-restriction, with arbitrary $d$, to example 1 creates an instance with a gap smaller than $\epsilon^{-1}2^{-l/2+2}$.*

**Proof:** As the verification circuit already rejects any state in the orthogonal complement of the two-dimensional subspace $V$, it is clear that we only have to analyze the gap created on states in $V$.

A rank $d$ random projector can be written as $UP_dU^\dagger$, where $U$ is a unitary drawn from the Haar measure and $P_d := \sum_{j=1}^{d} |j\rangle\langle j|$. Let $m_V(U,d) := \max_{|\psi\rangle \in V} \langle\psi|UP_dU^\dagger|\psi\rangle - \langle\psi^\perp|UP_dU^\dagger|\psi^\perp\rangle$, where $|\psi^\perp\rangle$ is the - up to a phase - unique orthogonal vector to $|\psi\rangle$ in $V$. We consider the following quantity, which gives the expectation value of the gap created by applying the random $R$-projection defined by $UP_dU^\dagger$:

$$\mathbb{E}_{U\sim\text{Haar}}(m_V(U,d)) = \int_{U(2^l)} dU m_V(U,d), \tag{7}$$

where the integral is taken over the Haar measure of the unitary group $U(2^l)$.

Let $\{|0\rangle, |1\rangle\}$ be a basis for $V$. Note that $m_V(U,d)$ is given by the difference of the maximum $\lambda_{\max}$ and minimum $\lambda_{\min}$ eigenvalues of the following matrix

$$V_{U,k} := \begin{pmatrix} \langle 0|UP_dU^\dagger|0\rangle & \langle 0|UP_dU^\dagger|1\rangle \\ \langle 1|UP_dU^\dagger|0\rangle & \langle 1|UP_dU^\dagger|1\rangle \end{pmatrix}$$

By Gersgorin disc Theorem ([BB97] p. 244), we find

$$|\lambda_{\max}(V_{U,k}) - \lambda_{\min}(V_{U,k})| \leq |\langle 0|UP_dU^\dagger|0\rangle - \langle 1|UP_dU^\dagger|1\rangle| + 2|\langle 0|UP_dU^\dagger|1\rangle|,$$

from which follows that

$$\int_{U(2^l)} dU m_V(U,d) \leq \int_{U(2^l)} dU |\langle 0|UP_dU^\dagger|0\rangle - \langle 1|UP_dU^\dagger|1\rangle| + 2\int_{U(2^l)} dU |\langle 0|UP_dU^\dagger|1\rangle|.$$

Applying Lemma 42 to each of the two terms in the R.H.S. of the equation above,

$$\int_{U(2^l)} dU m_V(U,d) \leq \sqrt{\frac{2k(2^l-k)}{(2^l+1)2^l(2^l-1)}} + 2\sqrt{\frac{k(2^l-k)}{(2^l+1)2^l(2^l-1)}} \leq 2^{-l/2+2},$$

for any $1 \leq k \leq 2^l$. To complete the proof, note that by Markov's inequality,

$$\int_{U: m_V(U,d)\geq\lambda} dU \leq 2^{-l/2+2}/\lambda,$$

for every $\lambda > 0$. Setting $\lambda = 2^{-l/2+2}/\epsilon$, we find that with probability

$$\int_{U: m_V(U,d)<\lambda} dU = 1 - \int_{U: m_V(U,d)\geq\lambda} dU \geq 1-\epsilon,$$

$m_V(U,d)$ is smaller than $2^{-l/2+2}/\epsilon$. ■

**Lemma 42** *For any traceless operator $X \in \mathcal{B}(\mathbb{C}^N)$,*

$$\int_{U(N)} dU |tr(UP_kU^\dagger X)| \leq \sqrt{\frac{k(k-K)tr(X^\dagger X)}{(N+1)N(N-1)}}, \tag{8}$$

*where $P_k := \sum_{j=1}^{k} |j\rangle\langle j|$.*

**Proof:** From the convexity of the square function,

$$\left(\int_{U(N)} dU|\mathrm{tr}(UP_kU^\dagger X)|\right)^2 \leq \int_{U(N)} dU|\mathrm{tr}(UP_kU^\dagger X)|^2.$$

To compute the R.H.S. of the equation above, we first note that

$$\begin{aligned}\int_{U(N)} dU|\mathrm{tr}(UP_kU^\dagger X)|^2 &= \int_{U(N)} dU\mathrm{tr}(U^{\otimes 2}P_k^{\otimes 2}(U^\dagger)^{\otimes 2}X\otimes X^\dagger) \\ &= \mathrm{tr}(\left(\int_{U(N)} dUU^{\otimes 2}P_k^{\otimes 2}(U^\dagger)^{\otimes 2}\right)X\otimes X^\dagger). \qquad (9)\end{aligned}$$

By Schur's Lemma [FH91],

$$\begin{aligned}\int_{U(N)} dUU^{\otimes 2}P_k^{\otimes 2}(U^\dagger)^{\otimes 2} &= \mathrm{tr}\left(P_k^{\otimes 2}(\mathbb{I}-\mathrm{SWAP})\right)\frac{\mathbb{I}-\mathrm{SWAP}}{N(N-1)} \\ &+ \mathrm{tr}\left(P_k^{\otimes 2}(\mathbb{I}+\mathrm{SWAP})\right)\frac{\mathbb{I}+\mathrm{SWAP}}{N(N+1)} \\ &= \frac{k(k-1)}{N(N-1)}(\mathbb{I}-\mathrm{SWAP}) + \frac{k(k+1)}{N(N+1)}(\mathbb{I}+\mathrm{SWAP}),\end{aligned}$$

where SWAP if the swap operator and we used that $\mathrm{tr}(\mathrm{SWAP}(P_k\otimes P_k)) = \mathrm{tr}(P_k^2) = \mathrm{tr}(P_k) = k$. Then, from Eq. (9),

$$\int_{U(D)} dU\mathrm{tr}(UP_kU^\dagger X)^2 = \mathrm{tr}(X^\dagger X)\left(\frac{k(k+1)}{N(N+1)} - \frac{k(k-1)}{N(N-1)}\right),$$

from which the lemma easily follows. ■

## 7.2 Using a Many-Outcome Measurement

In the previous section we tried to solve example 1 by applying the most natural idea that comes to mind: do a random 2-outcome measurement, and see if one state can "pass" the projection with an amount which is not negligible, compared to the other state on the subspace. We found out that such a procedure fails. In this section, we analyze the use a many-outcome measurement. We begin by applying a measurement in a random basis (or, to put it differently, by applying a random unitary according to the Haar measure, and then measuring in the standard basis). This, of course, cannot be done efficiently, but we will deal with it later.

Radhakrishnan et al. [RRS05] have shown,

**Theorem 43** *[RRS05] Let $|\psi_1\rangle, |\psi_2\rangle$ be two orthogonal quantum states in $\mathbb{C}^N$. Then,*

$$\mathbb{E}_{\hat{M}}\left(\left\|\hat{M}(|\psi_1\rangle) - \hat{M}(|\psi_2\rangle)\right\|_1\right) = \Omega(1)$$

*where $\hat{M}$ is a orthogonal basis chosen uniformly from the Haar measure.*

A stronger result was presented in Theorem 1 of [Sen06], which implies the same kind of result, but instead of the expectation, it asserts that the same holds with all but an exponentially small probability.

Furthermore, Ambainis and Emerson [AE07] have shown that:

**Theorem 44** *Let $|\psi_1\rangle, |\psi_2\rangle$ be two orthogonal quantum states in $\mathbb{C}^N$. Then,*

$$\left\|\hat{M}(|\psi_1\rangle) - \hat{M}(|\psi_2\rangle)\right\|_1 = \Omega(1)$$

*where $\hat{M}$ is a POVM with respect to an $\epsilon$-approximate (4, 4)-design.*

For our purpose, there is no need to understand what is an $\epsilon$-approximate (4, 4)-design, but only that there exists an efficient construction which enables us to realize the POVM $\hat{M}$ for any constant $\epsilon$. Notice that this is a constant POVM, and for every 2 states, the TVD of the distributions is constant. For more details of how one can implement a 4-design, see Theorem 1 of [AE07]. Although the POVM is constant, it achieves the same result as a random object (many-outcome measurements) but in an efficient way, and therefore we see it as a "pseudo-random" object.

So, how can we take advantage of that? Suppose we had the description of the distribution of $\hat{M}(|\psi_1\rangle)$ and $\hat{M}(|\psi_2\rangle)$. Then we could select a unique witness by accepting only when we measure an outcome $j$ associated to the $j$'s for which $\hat{M}(|\psi_1\rangle)(j) > \hat{M}(|\psi_2\rangle)(j)$. In this way we would get by Theorem 44 that $|\psi_1\rangle$ is accepted with a $\Omega(1)$ probability larger than $|\psi_2\rangle$. Of course this approach does not lead to the solution of the problem, as the promise of having a description of the distributions is too strong.

Indeed, although there is a classical description which would let us distinguish, with high probability, between the two cases, there is no known general way to achieve that which is in BQP. We would like to note that there is a resemblance between this problem and the SZK-Complete given in Ref. [Vad99], where in both problems, it is required to distinguish between two probabilities with some total variation distance.

# 8 Acknowledgments

This work is part of the QIP-IRC supported by EPSRC (GR/S82176/0) as well as the Integrated Project Qubit Applications (QAP) supported by the IST directorate as Contract Number 015848' and was supported by an EPSRC Postdoctoral Fellowship for Theoretical Physics.

# A Proofs

**Proof of Lemma 22:** Let $\{y_1, y_2, ..., y_w\}$ be the elements of $W$.

$$Pr(|h^{-1}(0)\bigcap W| = 1) =$$

$$Pr(\bigcup_{i=1}^{w}(h(y_i) = 0\bigcap_{j\neq i} h(y_j) \neq 0)) \tag{10}$$

$$= \sum_{i=1}^{w} Pr(h(y_i) = 0\bigcap_{j\neq i} h(y_j) \neq 0) \tag{11}$$

$$= \sum_{i=1}^{w} Pr(h(y_i) = 0)Pr(\bigcap_{j\neq i} h(y_j) \neq 0|h(y_i) = 0)$$

$$= \sum_{i=1}^{w} Pr(h(y_i) = 0)(1 - Pr(\bigcup_{j\neq i} h(y_j) = 0|h(y_i) = 0)$$

$$\geq \sum_{i=1}^{w} Pr(h(y_i) = 0)(1 - \sum_{j\neq i} Pr(h(y_j) = 0|h(y_i) = 0) \tag{12}$$

Equation (10) follows from the fact that all the elements in the union of equation (10) are disjoint. Equation (12) follows from the union bound.

Because $h$ is taken from a universal hash function set, we have that $Pr(h(y_i) = 0) = 1/2^{k+2}$, $Pr(h(y_j) = 0|h(y_i) = 0) = 1/2^{k+2}$. It was also given that $w/2^{k+2} > 1/4$ and $w/2^{k+2} \leq 1/2$. So,

$$= w/2^{k+2}(1 - \frac{w-1}{2^{k+2}}) \geq 1/8 \tag{13}$$

■

**Proof of Lemma 31:**

The proof is almost the same: Let $y_1, ..., y_a$ be the elements of $S_1$, and $y_{a+1}, ..., y_b$ the elements of $S_2$. So,

$$Pr(|h^{-1}(0)\bigcap S_1| = 1 \wedge |h^{-1}(0)\bigcap S_2| = 0)$$
$$= Pr(\bigcup_{i=1}^{a}(h(y_i) = 0 \bigcap_{1\leq j\leq b, j\neq i} h(y_j) \neq 0)).$$

The next steps are exactly the same, until we get to:

$$\geq \sum_{i=1}^{a} Pr(h(y_i) = 0)(1 - \sum_{1\leq j\leq b, j\neq i} Pr(h(y_j) = 0|h(y_i) = 0))$$
$$\geq a/2^{k+2}(1 - (b-1)/2^{k+2}) \geq 1/8\frac{a}{b}$$

■

# References


[AB09] S. Arora and B. Barak. Computational Complexity: A Modern Approach. *to appear: http://www. cs. princeton. edu/theory/complexity*, 2009.

[AE07] A. Ambainis and J. Emerson. Quantum t-designs: t-wise independence in the quantum world. *Arxiv preprint quant-ph/0701126*, 2007.

[AGIK07] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. The power of quantum systems on a line. *Arxiv preprint arXiv:0705.4077*, 2007.

[AN02] D. Aharonov and T. Naveh. Quantum NP-A Survey. *Arxiv preprint quant-ph/0210077*, 2002.

[APD+06] S. Anders, MB Plenio, W. Dür, F. Verstraete, and H.J. Briegel. Ground-State Approximation for Strongly Interacting Spin Systems in Arbitrary Spatial Dimension. *Physical Review Letters*, 97(10):107206, 2006.

[BB97] R. Bhatia and R. Bhatia. *Matrix analysis*. Springer New York, 1997.

[CTWI06] T.M. Cover, J.A. Thomas, J. Wiley, and W. InterScience. *Elements of Information Theory*. Wiley-Interscience New York, 2006.

[FH91] W. Fulton and J. Harris. *Representation Theory: A First Course*. Springer, 1991.

[Has07] MB Hastings. An Area Law for One Dimensional Quantum Systems. *JSTAT, P*, 8024, 2007.

[HKH+08] R. Hübener, C. Kruszynska, L. Hartmann, W. Dür, F. Verstraete, J. Eisert, and MB Plenio. Renormalization algorithm with graph enhancement. *Arxiv preprint arXiv:0802.1211*, 2008.

[Kit99] A. Kitaev. Quantum NP. *Talk at AQIP*, 99, 1999.

[KKR06] J. Kempe, A. Kitaev, and O. Regev. The Complexity of the Local Hamiltonian Problem. *SIAM JOURNAL ON COMPUTING*, 35(5):1070, 2006.

[KR03] J. Kempe and O. Regev. 3-Local Hamiltonian is QMA-complete. *Arxiv preprint quant-ph/0302079*, 2003.

[KVS+02] A.Y. Kitaev, M.N. Vyalyi, A.A. Shen, A.Û. Kitaev, and A.H. Šen&. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[MW05] C. Marriott and J. Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[OT05] R. Oliveira and B.M. Terhal. The complexity of quantum spin systems on a two-dimensional square lattice. *Arxiv preprint quant-ph/0504050*, 2005.

[PGVWC06] D. Perez-Garcia, F. Verstraete, MM Wolf, and JI Cirac. Matrix Product State Representations. *Arxiv preprint quant-ph/0608197*, 2006.

[RRS05] J. Radhakrishnan, M. Rotteler, and P. Sen. On the power of random bases in Fourier sampling: Hidden subgroup problem in the Heisenberg group. *Arxiv preprint quant-ph/0503114*, 2005.

[SCV08] N. Schuch, I. Cirac, and F. Verstraete. Computational Difficulty of Finding Matrix Product Ground States. *Physical Review Letters*, 100(25):250501, 2008.

[Sen06] P. Sen. Random Measurement Bases, Quantum State Distinction and Applications to the Hidden Subgroup Problem. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity*, pages 274–287. IEEE Computer Society Washington, DC, USA, 2006.

[Vad99] S.P. Vadhan. A study of statistical zero-knowledge proofs. 1999.

[Vid07] G. Vidal. Entanglement Renormalization. *Physical Review Letters*, 99(22):220405, 2007.

[VV85] LG Valiant and VV Vazirani. *NP is as easy as detecting unique solutions*. ACM Press New York, NY, USA, 1985.

[WZ06] P. Wocjan and S. Zhang. Several natural BQP-Complete problems. *Arxiv preprint quant-ph/0606179*, 2006.