Quantum Computing and Hidden Variables II: The Complexity of Sampling Histories

Scott Aaronson*

Abstract

This paper shows that, if we could examine the entire history of a hidden variable, then we could efficiently solve problems that are believed to be intractable even for quantum computers. In particular, under any hidden-variable theory satisfying a reasonable axiom called "indifference to the identity," we could solve the Graph Isomorphism and Approximate Shortest Vector problems in polynomial time, as well as an oracle problem that is known to require quantum exponential time. We could also search an N-item database using $O\left(N^{1/3}\right)$ queries, as opposed to $O\left(N^{1/2}\right)$ queries with Grover's search algorithm. On the other hand, the $N^{1/3}$ bound is optimal, meaning that we could probably *not* solve NP-complete problems in polynomial time. We thus obtain the first good example of a model of computation that appears *slightly* more powerful than the quantum computing model.

1 Introduction

It is often stressed that hidden-variable theories, such as Bohmian mechanics, yield exactly the same predictions as ordinary quantum mechanics. On the other hand, these theories describe a different picture of physical reality, with an additional layer of dynamics beyond that of a state vector evolving unitarily. This paper addresses a question that, to our knowledge, had never been raised before: *what is the computational complexity of simulating that additional dynamics?* In other words, if we could examine a hidden variable's entire history, then could we solve problems in polynomial time that are intractable even for quantum computers?

We present strong evidence that the answer is yes. The Graph Isomorphism problem asks whether two graphs G and H are isomorphic; while given a basis for a lattice $\mathcal{L} \in \mathbb{R}^n$, the Approximate Shortest Vector problem asks for a nonzero vector in $\mathcal{L}$ within a $\sqrt{n}$ factor of the shortest one. We show that both problems are efficiently solvable by sampling a hidden variable's history, provided the hidden-variable theory satisfies a reasonable axiom that we call "indifference to the identity operation." By contrast, despite a decade of effort, neither problem is known to lie in BQP, the class of problems solvable in quantum polynomial time with bounded error probability.[1] Thus, if we let DQP (Dynamical Quantum Polynomial-Time) be the class of problems solvable in our new model, then this already provides circumstantial evidence that BQP is strictly contained in DQP.

However, the evidence is stronger than this. For we actually show that DQP contains an entire *class* of problems, of which Graph Isomorphism and Approximate Shortest Vector are special

*University of California, Berkeley. Email: aaronson@cs.berkeley.edu.

[1] See www.complexityzoo.com for more information about the complexity classes mentioned in this paper.

cases. Computer scientists know this class as *Statistical Zero Knowledge*, or SZK. Furthermore, in previous work [2] we showed that "relative to an oracle," SZK is not contained in BQP. This is a technical concept implying that any proof of $\mathsf{SZK} \subseteq \mathsf{BQP}$ would require techniques unlike those that are currently known. Combining our result that $\mathsf{SZK} \subseteq \mathsf{DQP}$ with the oracle separation of [2], we obtain that $\mathsf{BQP} \neq \mathsf{DQP}$ relative to an oracle as well. Given computer scientists' longstanding inability to separate basic complexity classes, this is nearly the best evidence one could hope for that sampling histories yields more power than standard quantum computation.

Besides solving SZK problems, we also show that by sampling histories, one could search an unordered database of N items for a single "marked item" using only $O\left(N^{1/3}\right)$ database queries. By comparison, Grover's quantum search algorithm [11] requires $\Theta\left(N^{1/2}\right)$ queries, while classical algorithms require $\Theta\left(N\right)$ queries.[2] On the other hand, we also show that our $N^{1/3}$ upper bound is the best possible—so even in the histories model, one cannot search an N-item database in $(\log N)^c$ steps for some fixed power c. This implies that $\mathsf{NP} \not\subset \mathsf{DQP}$ relative to an oracle, which in turn suggests that DQP is *still* not powerful enough to solve NP-complete problems in polynomial time. Note that while Graph Isomorphism and Approximate Shortest Vector are in NP, it is strongly believed that they are not NP-complete.

At this point we should address a concern that many readers will have. Once we extend quantum mechanics by positing the "unphysical" ability to sample histories, isn't it completely unsurprising if we can then solve problems that were previously intractable? We believe the answer is no, for three reasons.

First, almost every change that makes the quantum computing model more powerful, seems to make it *so much* more powerful that NP-complete and even harder problems become solvable efficiently. To give some examples, NP-complete problems can be solved in polynomial time using a nonlinear Schrödinger equation, as shown by Abrams and Lloyd [4]; using closed timelike curves, as shown by Bacon [6]; or using a measurement rule of the form $|\psi|^p$ for any $p \neq 2$, as shown by us [3]. It is also easy to see that we could solve NP-complete problems if, given a quantum state $|\psi\rangle$, we could request a classical description of $|\psi\rangle$, such as a list of amplitudes or a preparation procedure.[3] By contrast, ours is the first independently motivated model we know of that seems more powerful than quantum computing, but only *slightly* so.[4] Moreover, the striking fact that unordered search in our model takes about $N^{1/3}$ steps, as compared to N steps classically and $N^{1/2}$ quantum-mechanically, suggests that DQP somehow "continues a sequence" that begins with P and BQP. It would be interesting to find a model in which search takes $N^{1/4}$ or $N^{1/5}$ steps.

The second reason our results are surprising is that, given a hidden variable, the distribution over its possible values at any *single* time is governed by standard quantum mechanics, and is therefore efficiently samplable on a quantum computer. So if examining the variable's history confers any extra computational power, then it can only be because of *correlations* between the variable's values at different times.

The third reason is our criterion for success. We are not saying merely that one can solve Graph Isomorphism under *some* hidden-variable theory; or even that, under any theory satisfying

[2] For readers unfamiliar with asymptotic notation: $O\left(f\left(N\right)\right)$ means "at most order $f\left(N\right)$," $\Omega\left(f\left(N\right)\right)$ means "at least order $f\left(N\right)$," and $\Theta\left(f\left(N\right)\right)$ means "exactly order $f\left(N\right)$."

[3] For as Abrams and Lloyd [4] observed, we can so arrange things that $|\psi\rangle = |0\rangle$ if an NP-complete instance of interest to us has no solution, but $|\psi\rangle = \sqrt{1-\varepsilon}\,|0\rangle + \sqrt{\varepsilon}\,|1\rangle$ for some tiny ε if it has a solution.

[4] One can define other, less motivated, models with the same property by allowing "non-collapsing measurements" of quantum states, but these models are very closely related to ours. Indeed, a key ingredient of our results will be to show that certain kinds of non-collapsing measurements can be *simulated* using histories.

the indifference axiom, there exists an algorithm to solve it; but rather that there exists a *single* algorithm that solves Graph Isomorphism under any theory satisfying indifference. Thus, we must consider even theories that are specifically designed to thwart such an algorithm.

But what is the motivation for our results? The first motivation is that, within the community of physicists who study hidden-variable theories such as Bohmian mechanics, there is great interest in actually *calculating* the hidden-variable trajectories for specific physical systems [15, 12]. Our results show that, when many interacting particles are involved, this task might be fundamentally intractable, even if a quantum computer is available. The second motivation is that, in classical computer science, studying "unrealistic" models of computation has often led to new insights into realistic ones; and likewise we expect that the DQP model could lead to new results about standard quantum computation. Indeed, in a sense this has already happened. For our result that $\mathsf{SZK} \not\subset \mathsf{BQP}$ relative to an oracle [2] grew out of work on the BQP versus DQP question. Yet the "quantum lower bound for the collision problem" underlying that result provided the first evidence that cryptographic hash functions could be secure against quantum attack, and ruled out a large class of possible quantum algorithms for Graph Isomorphism, Approximate Shortest Vector, and related problems.

1.1 Outline of Paper

The precise definition of a hidden-variable theory that we use in this paper was developed in a companion paper [1]. Familiarity with [1] is helpful but not essential for understanding this paper. In Section 2, we review the relevant concepts from [1], and then formally define DQP as the class of problems solvable by a classical polynomial-time algorithm with access to a "history oracle." Given a sequence of quantum circuits as input, this oracle returns a sample from a corresponding distribution over histories of a hidden variable, according to some hidden-variable theory $\mathcal{T}$. The oracle can choose $\mathcal{T}$ "adversarially," subject to two constraints: $\mathcal{T}$ must be robust to small errors (since otherwise the definition of DQP could depend on the choice of gate set), and it must satisfy the indifference axiom.

So what is the indifference axiom, then? Intuitively it says that, given a bipartite state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ (entangled or unentangled), if a unitary operation acts only on the $\mathcal{H}_A$ part of $|\psi\rangle$ (i.e. has the form $U \otimes I$), then the hidden-variable transitions can also only involve the $\mathcal{H}_A$ part. Note that this is quite different from *locality* in the sense of Bell's theorem: the probability of transitioning between two basis states $|x_A\rangle \otimes |x_B\rangle$ and $|y_A\rangle \otimes |x_B\rangle$ can depend on the complete state $|\psi\rangle$; all we require is that if $x_B \neq y_B$, then the probability of transitioning between $|x_A\rangle \otimes |x_B\rangle$ and $|y_A\rangle \otimes |y_B\rangle$ is zero. Indifference is a substantive axiom, and is violated (for example) by Bohmian mechanics. However, to us it simply expresses the idea that, if we have a state such as $(|a\rangle + |b\rangle + |c\rangle + |d\rangle)/2$, and a partial measurement yields a new state

$$\frac{|a\rangle + |b\rangle}{2} |R_{ab}\rangle + \frac{|c\rangle + |d\rangle}{2} |R_{cd}\rangle ,$$

where $|R_{ab}\rangle$ and $|R_{cd}\rangle$ denote two configurations of a recording apparatus, then so long as we leave the recording apparatus alone, all further hidden-variable transitions should be between $|a\rangle$ and $|b\rangle$ or between $|c\rangle$ and $|d\rangle$, not between (say) $|a\rangle$ and $|c\rangle$. If we abandoned this axiom, then we would need some other way to rule out the degenerate hidden-variable theory, which takes the hidden-variable values at different times to be completely independent of one another. Were this "product theory" allowed, we would have $\mathsf{DQP} = \mathsf{BQP}$ for trivial reasons.

An earlier version of this paper required another axiom—*symmetry* under permutations of basis states—which seems much harder to justify than indifference. However, we have since been able to eliminate the dependence of our algorithms on the symmetry axiom.

Section 3 establishes the most basic facts about DQP: for example, that BQP $\subseteq$ DQP, and that DQP is independent of the choice of gate set. Then Section 4 presents the "juggle subroutine," a crucial ingredient in both main algorithms of the paper. Given a state of the form $(|a\rangle + |b\rangle)/\sqrt{2}$ or $(|a\rangle - |b\rangle)/\sqrt{2}$, the goal of this subroutine is to "juggle" a hidden variable between $|a\rangle$ and $|b\rangle$, so that when we inspect the hidden variable's history, both $|a\rangle$ and $|b\rangle$ are observed with high probability. The difficulty is that this needs to work under *any* indifferent hidden-variable theory.

Next, Section 5 combines the juggle subroutine with a technique of Valiant and Vazirani [19] to prove that SZK $\subseteq$ DQP, from which it follows in particular that Graph Isomorphism and Approximate Shortest Vector are in DQP. Then Section 6 applies the juggle subroutine to search an N-item database in $O\left(N^{1/3}\right)$ queries, and also proves that this $N^{1/3}$ bound is optimal. We conclude in Section 7 with some directions for further research.

2 The Computational Model

We now explain our model of computation, building our way up to the complexity class DQP. Our starting point is the definition of *hidden-variable theory* that we gave in [1]. To recap from that paper: for us a hidden-variable theory is simply a family of functions $\{S_N\}_{N\in\{1,2,\ldots\}}$, where each S_N maps an $N \times N$ density matrix ρ and an $N \times N$ unitary matrix U onto an $N \times N$ stochastic matrix $S = S_N(\rho, U)$. In this paper, ρ will always be a pure state of $l = \log_2 N$ qubits. That is, $\rho = |\psi\rangle\langle\psi|$ where

$$|\psi\rangle = \sum_{x\in\{0,1\}^l} \alpha_x |x\rangle .$$

What is essential is that S map the probability distribution induced by measuring $|\psi\rangle$ in the computational basis $\{|x\rangle\}_{x\in\{0,1\}^l}$, onto the probability distribution induced by measuring $U|\psi\rangle$ in that same basis. More formally, let $(M)_{xy}$ denote the entry in the x^{th} column and y^{th} row of matrix M, and let

$$U|\psi\rangle = \sum_{x\in\{0,1\}^l} \beta_x |x\rangle .$$

Then we require that for all $y \in \{0,1\}^l$,

$$\sum_{x\in\{0,1\}^l} (S)_{xy} |\alpha_x|^2 = |\beta_y|^2 .$$

It is clear that there are infinitely many theories satisfying the above marginalization axiom; the simplest one is the *product theory* $\mathcal{PT}$, which sets $(S)_{xy} = |\beta_y|^2$ for all x, y. To narrow down the choices, in [1] we proposed seven additional axioms that we might want any hidden-variable theory to satisfy. We then showed that, although not all of the axioms can be satisfied simultaneously, two of the most important ones—called indifference and robustness—*can* be satisfied simultaneously.

Let us restate those two axioms in the present context. *Indifference* says that if U is generalized block-diagonal (i.e. a permutation of a block-diagonal matrix), then S is also generalized block-diagonal with the same block structure or some refinement thereof. So in particular, if $|\psi\rangle$ belongs

to a tensor-product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and if U acts only on $\mathcal{H}_A$ (i.e. never maps a basis state $|x_A\rangle \otimes |x_B\rangle$ to $|y_A\rangle \otimes |y_B\rangle$ where $x_B \neq y_B$), then $S(|\psi\rangle, U)$ acts only on $\mathcal{H}_A$ as well. *Robustness* says that S is insensitive to small perturbations of $|\psi\rangle$ or U. To make this intuition formal, we call a theory robust if for all $b > 0$, there exists $c > 0$ such that for all l, all pairs of states $|\psi\rangle = \sum_{x \in \{0,1\}^l} \alpha_x |x\rangle$ and $\left|\widetilde{\psi}\right\rangle = \sum_{x \in \{0,1\}^l} \widetilde{\alpha}_x |x\rangle$ such that $\left\langle \psi | \widetilde{\psi} \right\rangle \geq 1 - 2^{-cl}$, and all U and $\widetilde{U}$ such that $\left| (U)_{xy} - \left(\widetilde{U}\right)_{xy} \right| \leq 2^{-cl}$ for all x, y, we have

$$\left| (S)_{xy} |\alpha_x|^2 - \left(\widetilde{S}\right)_{xy} |\widetilde{\alpha}_x|^2 \right| \leq 2^{-bl}$$

for all x, y, where $S = S(|\psi\rangle, U)$ and $\widetilde{S} = S\left(\left|\widetilde{\psi}\right\rangle, \widetilde{U}\right)$.

It is easy to show that the product theory $\mathcal{PT}$ satisfies robustness but not indifference. In [1], we analyzed three other hidden-variable theories: the *Dieks theory* $\mathcal{DT}$, which satisfies indifference but not robustness; the *flow theory* $\mathcal{FT}$, which satisfies both indifference and robustness; and the *Schrödinger theory* $\mathcal{ST}$, which satisfies indifference, and which we conjecture satisfies robustness. The details of those theories are mostly irrelevant for this paper. Indeed, our algorithms will work under *any* hidden-variable theory that satisfies the indifference axiom. On the other hand, if we take into account that even in theory (let alone in practice), a generic unitary cannot be represented exactly with a finite universal gate set, only approximated arbitrarily well, then we also need the robustness axiom. Thus, a key result from [1] that we rely on is that there *exists* a hidden-variable theory (namely $\mathcal{FT}$) satisfying both indifference and robustness.

Let a quantum computer have the initial state $|0\rangle^{\otimes l}$, and suppose we apply a sequence $\mathcal{U} = (U_1, \ldots, U_T)$ of unitary operations, each of which is implemented by a polynomial-size quantum circuit. Then a *history* of a hidden variable through the computation is a sequence $H = (v_0, \ldots, v_T)$ of basis states, where v_t is the variable's value immediately after U_t is applied (thus $v_0 = |0\rangle^{\otimes l}$). Given any hidden-variable theory $\mathcal{T}$, we can obtain a probability distribution $\Omega(\mathcal{U}, \mathcal{T})$ over histories by just applying $\mathcal{T}$ repeatedly, once for each U_t, to obtain the stochastic matrices

$$S\left(|0\rangle^{\otimes l}, U_1\right), \quad S\left(U_1 |0\rangle^{\otimes l}, U_2\right), \quad \ldots \quad S\left(U_{T-1} \cdots U_1 |0\rangle^{\otimes l}, U_T\right).$$

Note that $\Omega(\mathcal{U}, \mathcal{T})$ is a Markov distribution; that is, each v_t is independent of the other v_i's conditioned on v_{t-1} and v_{t+1}. Admittedly, $\Omega(\mathcal{U}, \mathcal{T})$ could depend on the precise way in which the combined circuit $U_T \cdots U_1$ is "sliced" into component circuits $U_1, \ldots, U_T$. But as we showed in [1], such dependence on the granularity of unitaries is unavoidable in any hidden-variable theory other than $\mathcal{PT}$.

Given a hidden-variable theory $\mathcal{T}$, let $\mathcal{O}(\mathcal{T})$ be an oracle that takes as input a positive integer l, and a sequence of quantum circuits $\mathcal{U} = (U_1, \ldots, U_T)$ that act on l qubits. Here each U_t is specified by a sequence $\left(g_{t,1}, \ldots, g_{t,m(t)}\right)$ of gates chosen from some finite universal gate set $\mathcal{G}$. The oracle $\mathcal{O}(\mathcal{T})$ returns as output a sample $(v_0, \ldots, v_T)$ from the history distribution $\Omega(\mathcal{U}, \mathcal{T})$ defined previously. Now let A be a deterministic classical Turing machine that is given oracle access to $\mathcal{O}(\mathcal{T})$. The machine A receives an input x, makes a single oracle query to $\mathcal{O}(\mathcal{T})$, then produces an output based on the response. We say a set of strings L is in DQP if there exists an A such that for all sufficiently large n and inputs $x \in \{0,1\}^n$, and all theories $\mathcal{T}$ satisfying the indifference and robustness axioms, A correctly decides whether $x \in L$ with probability at least $2/3$, in time polynomial in n.

Let us make some remarks about the above definition. There is no real significance in our requirement that A be deterministic and classical, and that it be allowed only one query to $\mathcal{O}(\mathcal{T})$. We made this choice only because it suffices for our upper bounds; it might be interesting to consider the effects of other choices. However, other aspects of the definition are not arbitrary. The order of quantifiers matters; we want a single A that works for *any* hidden-variable theory satisfying indifference and robustness. Also, we require A to succeed only for sufficiently large n since by choosing a large enough robustness parameter c, an adversary might easily make A incorrect on a finite number of instances.

3 Basic Results

Having defined the complexity class DQP, in this short section we establish its most basic properties. First of all, it is immediate that BQP $\subseteq$ DQP; that is, sampling histories is at least as powerful as standard quantum computation. For v_1, the first hidden-variable value returned by $\mathcal{O}(\mathcal{T})$, can be seen as simply the result of applying a polynomial-size quantum circuit U_1 to the initial state $|0\rangle^{\otimes l}$ and then measuring in the standard basis.

A key further observation is the following.

Proposition 1 *Any universal gate set yields the same complexity class* DQP*. By universal, we mean here that any unitary matrix (real or complex) can be approximated, without the need for ancilla qubits.*

Proof. Let $\mathcal{G}$ and $\widehat{\mathcal{G}}$ be universal gate sets, and let U be a circuit made of poly(n) gates from $\mathcal{G}$. Then the Solovay-Kitaev Theorem [13, 14] implies that we can approximate U to accuracy (say) 2^{-nl} by using poly$(n,l) =$ poly(n) gates from $\widehat{\mathcal{G}}$, which act on the same set of qubits as U does. Furthermore, the approximating circuit can be efficiently constructed. Now from the definition of robustness, for all $\mathcal{T}$ there exists a $c > 0$ such that, if we approximate each $U_t \in \mathcal{U}$ to accuracy 2^{-cl}, then the distribution over histories seen by A is statistically indistinguishable from what it would have been were the U_t's represented exactly. (This occurs when $b = 3$ for example.) Clearly $2^{-nl} \ll 2^{-cl}$ for sufficiently large n. ■

Unfortunately, the best upper bound on DQP we have been able to show is DQP $\subseteq$ EXP; that is, any problem in DQP is solvable in deterministic exponential time. The proof is trivial, but is the one place in the paper that relies on a specific hidden-variable theory from [1]. Let $\mathcal{T}$ be the flow theory $\mathcal{FT}$, with the slight modification that we omit the step from [1] of symmetrizing over all permutations of basis states. Then by using the Ford-Fulkerson algorithm [10], we can clearly construct the requisite maximum flows in time polynomial in 2^l (hence exponential in n), and thereby calculate the probability of each possible history $(v_1, \ldots, v_T)$ to suitable precision. If we include the symmetrization step, then we only know how to calculate these probabilities in *probabilistic* exponential time.

4 The Juggle Subroutine

This section presents a crucial subroutine that will be used in both algorithms of this paper: the algorithm for simulating statistical zero knowledge in Section 5, and the algorithm for search in $N^{1/3}$ queries in Section 6. Given an l-qubit state $|\psi\rangle = (|a\rangle + |b\rangle)/\sqrt{2}$ that is an equal superposition of

two unknown basis states, the goal of the juggle subroutine is to learn both a and b. The name arises because our strategy will be to "juggle" a hidden variable, so that if it starts out at $|a\rangle$ then with non-negligible probability it transitions to $|b\rangle$, and vice versa. Inspecting the entire history of the hidden variable will then reveal both a and b, as desired. The difficulty is that we need a *single* subroutine that does this under *all* hidden-variable theories satisfying the indifference axiom—even theories that are designed specifically to thwart such a subroutine. To meet this difficulty, we will apply a pair of unitaries to $|\psi\rangle$ that force the hidden variable to "forget" whether it started at $|a\rangle$ or $|b\rangle$. We will then invert those unitaries to return the state to $|\psi\rangle$, at which point the hidden variable must be unequal to its initial value with probability 1/2.

We now give the subroutine. The first unitary, U_1, consists of Hadamard gates on $l-1$ qubits chosen uniformly at random, and the identity operation on the remaining qubit, i. Next U_2 consists of a Hadamard gate on qubit i. Finally U_3 consists of Hadamard gates on all l qubits. Let $a = a_1 \ldots a_l$ and $b = b_1 \ldots b_l$. Then since $a \neq b$, we have $a_i \neq b_i$ with probability at least $1/l$. Assuming that occurs, the state

$$U_1 |\psi\rangle = \frac{1}{2^{l/2}} \left(\sum_{z \in \{0,1\}^l \,:\, z_i = a_i} (-1)^{a \cdot z - a_i z_i} |z\rangle + \sum_{z \in \{0,1\}^l \,:\, z_i = b_i} (-1)^{b \cdot z - b_i z_i} |z\rangle \right)$$

assigns nonzero amplitude to all 2^l basis states. Then $U_2 U_1 |\psi\rangle$ assigns nonzero amplitude to 2^{l-1} basis states $|z\rangle$, namely those for which $a \cdot z \equiv b \cdot z \,(\mathrm{mod}\, 2)$. Finally $U_3 U_2 U_1 |\psi\rangle = |\psi\rangle$.

Let v_t be the value of the hidden variable after U_t is applied. Then assuming $a_i \neq b_i$, we claim that v_3 is independent of v_0. So in particular, if $v_0 = |a\rangle$ then $v_3 = |b\rangle$ with 1/2 probability, and if $v_0 = |b\rangle$ then $v_3 = |a\rangle$ with 1/2 probability. To see this, observe that when U_1 is applied, there is no interference between basis states $|z\rangle$ such that $z_i = a_i$, and those such that $z_i = b_i$. So by the indifference axiom, the probability mass at $|a\rangle$ must spread out evenly among all 2^{l-1} basis states that agree with a on the i^{th} bit, and similarly for the probability mass at $|b\rangle$. Then after U_2 is applied, v_2 can differ from v_1 only on the i^{th} bit, again by the indifference axiom. So each basis state of $U_2 U_1 |\psi\rangle$ must receive an equal contribution from probability mass originating at $|a\rangle$, and probability mass originating at $|b\rangle$. Therefore v_2 is independent of v_0, from which it follows that v_3 is independent of v_0 as well.

Unfortunately, the juggle subroutine only works with probability $1/(2l)$—for it requires that $a_i \neq b_i$, and even then, inspecting the history $(v_0, v_1, \ldots)$ only reveals both $|a\rangle$ and $|b\rangle$ with probability 1/2. Furthermore, the definition of DQP does not allow more than one call to the history oracle. However, all we need to do is pack multiple subroutine calls into a single oracle call. That is, choose U_4 similarly to U_1 (except with a different value of i), and set $U_5 = U_2$ and $U_6 = U_3$. Do the same with U_7, U_8, and U_9, and so on. Since $U_3, U_6, U_9, \ldots$ all return the quantum state to $|\psi\rangle$, the effect is that of multiple independent juggle attempts. With $2l^2$ attempts, we can make the failure probability at most $(1 - 1/(2l))^{2l^2} < e^{-l}$.

As a final remark, it is easy to see that the juggle subroutine works equally well with states of the form $|\psi\rangle = (|a\rangle - |b\rangle)/\sqrt{2}$. This will prove useful in Section 6.

5 Simulating SZK

Our goal is to show that SZK $\subseteq$ DQP. Here SZK, or Statistical Zero Knowledge, was originally defined as the class of all problems that possess a certain kind of "zero-knowledge proof protocol"—

that is, a protocol between an omniscient prover and a verifier, by which the verifier becomes convinced of the answer to a problem, yet without learning anything else about the problem. However, for our purposes this cryptographic definition of SZK is irrelevant. For Sahai and Vadhan [16] have given an alternate and much simpler characterization: a problem is in SZK if and only if it can be reduced to a problem called Statistical Difference, which involves deciding whether two probability distributions are close or far.

More formally, let P_0 and P_1 be functions that map n-bit strings to n-bit strings, and that are specified by classical polynomial-time algorithms. Let Λ_0 and Λ_1 be the probability distributions over $P_0(x)$ and $P_1(x)$ respectively, if $x \in \{0,1\}^n$ is chosen uniformly at random. Then the problem is to decide whether $\|\Lambda_0 - \Lambda_1\|$ is less than $1/3$ or greater than $2/3$, given that one of these is the case. Here

$$\|\Lambda_0 - \Lambda_1\| = \frac{1}{2} \sum_{y \in \{0,1\}^n} \left| \Pr_{x \in \{0,1\}^n} [P_0(x) = y] - \Pr_{x \in \{0,1\}^n} [P_1(x) = y] \right|$$

is the variation distance between Λ_0 and Λ_1.

To illustrate, let us show that Graph Isomorphism is in SZK. Given two graphs G_0 and G_1, take Λ_0 to be the uniform distribution over all permutations of G_0, and Λ_1 to be uniform over all permutations of G_1. This way, if G_0 and G_1 are isomorphic, then Λ_0 and Λ_1 will be identical, so $\|\Lambda_0 - \Lambda_1\| = 0$. On the other hand, if G_0 and G_1 are non-isomorphic, then Λ_0 and Λ_1 will be perfectly distinguishable, so $\|\Lambda_0 - \Lambda_1\| = 1$. Since Λ_0 and Λ_1 are clearly samplable by polynomial-time algorithms, it follows that any instance of Graph Isomorphism can be expressed as an instance of Statistical Difference. For a proof that Approximate Shortest Vector is in SZK, we refer the reader to Aharonov and Ta-Shma [5].

Our proof will use the following "amplification lemma" from [16]:[5]

Lemma 2 (Sahai and Vadhan) *Given efficiently-samplable distributions Λ_0 and Λ_1, we can construct new efficiently-samplable distributions Λ'_0 and Λ'_1, such that if $\|\Lambda_0 - \Lambda_1\| \leq 1/3$ then $\|\Lambda'_0 - \Lambda'_1\| \leq 2^{-n}$, while if $\|\Lambda_0 - \Lambda_1\| \geq 2/3$ then $\|\Lambda'_0 - \Lambda'_1\| \geq 1 - 2^{-n}$.*

In particular, Lemma 2 means we can assume without loss of generality that either $\|\Lambda_0 - \Lambda_1\| \leq 2^{-n^c}$ or $\|\Lambda_0 - \Lambda_1\| \geq 1 - 2^{-n^c}$ for some constant $c > 0$.

Having covered the necessary facts about SZK, we can now proceed to the main result.

Theorem 3 $\mathsf{SZK} \subseteq \mathsf{DQP}$.

Proof. We show how to solve Statistical Difference by using a history oracle. For simplicity, we start with the special case where P_0 and P_1 are both one-to-one functions. In this case, the circuit sequence $\mathcal{U}$ given to the history oracle does the following: it first prepares the state

$$\frac{1}{2^{(n+1)/2}} \sum_{b \in \{0,1\}, x \in \{0,1\}^n} |b\rangle |x\rangle |P_b(x)\rangle .$$

It then applies the juggle subroutine to the joint state of the $|b\rangle$ and $|x\rangle$ registers, taking $l = n+1$. Notice that by the indifference axiom, the hidden variable will never transition from one value of

[5] Note that in this lemma, the constants $1/3$ and $2/3$ are not arbitrary; it is important for technical reasons that $(2/3)^2 > 1/3$.

$P_b(x)$ to another—exactly as if we had *measured* the third register in the standard basis. All that matters is the reduced state $|\psi\rangle$ of the first two registers, which has the form $(|0\rangle|x_0\rangle + |1\rangle|x_1\rangle)/\sqrt{2}$ for some x_0, x_1 if $\|\Lambda_0 - \Lambda_1\| = 0$, and $|b\rangle|x\rangle$ for some b, x if $\|\Lambda_0 - \Lambda_1\| = 1$. We have already seen that the juggle subroutine can distinguish these two cases: when the hidden-variable history is inspected, it will contain two values of the $|b\rangle$ register in the former case, and only one value in the latter case. Also, clearly the case $\|\Lambda_0 - \Lambda_1\| \leq 2^{-n^c}$ is statistically indistinguishable from $\|\Lambda_0 - \Lambda_1\| = 0$ with respect to the subroutine, and likewise $\|\Lambda_0 - \Lambda_1\| \geq 1 - 2^{-n^c}$ is indistinguishable from $\|\Lambda_0 - \Lambda_1\| = 1$.

We now consider the general case, where P_0 and P_1 need not be one-to-one. Our strategy is to reduce to the one-to-one case, by using a well-known hashing technique of Valiant and Vazirani [19]. Let $\mathcal{D}_{n,k}$ be the uniform distribution over all affine functions mapping $\{0,1\}^n$ to $\{0,1\}^k$, where we identify those sets with the finite fields $\mathbb{F}_2^n$ and $\mathbb{F}_2^k$ respectively. What Valiant and Vazirani showed is that, for all subsets $A \subseteq \{0,1\}^n$ such that $2^{k-2} \leq |A| \leq 2^{k-1}$, and all $s \in \{0,1\}^k$,

$$\Pr_{h \in \mathcal{D}_{n,k}} \left[\left| A \cap h^{-1}(s) \right| = 1 \right] \geq \frac{1}{8}.$$

As a corollary, the expectation over $h \in \mathcal{D}_{n,k}$ of

$$\left| \left\{ s \in \{0,1\}^k : \left| A \cap h^{-1}(s) \right| = 1 \right\} \right|$$

is at least $2^k/8$. It follows that, if x is drawn uniformly at random from A, then

$$\Pr_{h,x} \left[\left| A \cap h^{-1}(h(x)) \right| = 1 \right] \geq \frac{2^k/8}{|A|} \geq \frac{1}{4}.$$

This immediately suggests the following algorithm for the many-to-one case. Draw k uniformly at random from $\{2, \ldots, n+1\}$; then draw $h_0, h_1 \in \mathcal{D}_{n,k}$. Have $\mathcal{U}$ prepare the state

$$\frac{1}{2^{(n+1)/2}} \sum_{b \in \{0,1\}, x \in \{0,1\}^n} |b\rangle |x\rangle |P_b(x)\rangle |h_b(x)\rangle,$$

and then apply the juggle subroutine to the joint state of the $|b\rangle$ and $|x\rangle$ registers, ignoring the $|P_b(x)\rangle$ and $|h_b(x)\rangle$ registers as before.

Suppose $\|\Lambda_0 - \Lambda_1\| = 0$. Also, given a value $s = P_b(x)$, let $A_0 = P_0^{-1}(s)$ and $A_1 = P_1^{-1}(s)$, and suppose $2^{k-2} \leq |A_0| = |A_1| \leq 2^{k-1}$. Then

$$\Pr_{s,h_0,h_1} \left[\left| A_0 \cap h_0^{-1}(s) \right| = 1 \wedge \left| A_1 \cap h_1^{-1}(s) \right| = 1 \right] \geq \left(\frac{1}{4} \right)^2,$$

since the events $\left| A_0 \cap h_0^{-1}(s) \right| = 1$ and $\left| A_1 \cap h_1^{-1}(s) \right| = 1$ are independent of each other conditioned on s. Assuming both events occur, as before the juggle subroutine will reveal both $|0\rangle|x_0\rangle$ and $|1\rangle|x_1\rangle$ with high probability, where x_0 and x_1 are the unique elements of $A_0 \cap h_0^{-1}(s)$ and $A_1 \cap h_1^{-1}(s)$ respectively. By contrast, if $\|\Lambda_0 - \Lambda_1\| = 1$ then only one value of the $|b\rangle$ register will ever be observed. Again, replacing $\|\Lambda_0 - \Lambda_1\| = 0$ by $\|\Lambda_0 - \Lambda_1\| \leq 2^{-n^c}$, and $\|\Lambda_0 - \Lambda_1\| = 1$ by $\|\Lambda_0 - \Lambda_1\| \geq 1 - 2^{-n^c}$, can have only a negligible effect on the history distribution.

Of course, the probability that the correct value of k is chosen, and that $A_0 \cap h_0^{-1}(s)$ and $A_1 \cap h_1^{-1}(s)$ both have a unique element, could be as low as $1/(16n)$. To deal with this, we simply

increase the number of calls to the juggle subroutine by an $O(n)$ factor, drawing new values of k, h_0, h_1 for each call. We pack multiple subroutine calls into a single oracle call as described in Section 4, except that now we uncompute the entire state (returning it to $|0\cdots 0\rangle$) and then recompute it between subroutine calls. A final remark: since the algorithm that calls the history oracle is deterministic, we "draw" new values of k, h_0, h_1 by having $\mathcal{U}$ prepare a uniform superposition over all possible values. The indifference axiom justifies this procedure, by guaranteeing that within each call to the juggle subroutine, the hidden-variable values of k, h_0, and h_1 remain constant. ■

Let us end this section with some brief remarks about the oracle result of [2]. Given a function $g : \{0,1\}^n \rightarrow \{0,1\}^n$, the *collision problem* is to decide whether g is one-to-one or two-to-one, given that one of these is the case. The question is, how many queries to g are needed to solve this problem (where a query just returns $g(x)$ given x)? It is not hard to see that $\Theta\left(2^{n/2}\right)$ queries are necessary and sufficient for classical randomized algorithms. What we showed in [2] is that $\Omega\left(2^{n/5}\right)$ queries are needed by any *quantum* algorithm as well. Subsequently Shi [17] managed to improve the quantum lower bound to $\Omega\left(2^{n/3}\right)$ queries, thereby matching an upper bound of Brassard, Høyer, and Tapp [9]. On the other hand, the collision problem is easily reducible to the Statistical Difference problem, and is therefore solvable in polynomial time by sampling histories. This is the essence of the statement that $\mathsf{BQP} \neq \mathsf{DQP}$ relative to an oracle.

6 Search in $N^{1/3}$ Queries

Given a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$, the database search problem is simply to find a string x such that $f(x) = 1$. We can assume without loss of generality that this "marked item" x is unique.[6] We want to find it using as few queries to f as possible, where a query returns $f(y)$ given y.

Let $N = 2^n$. Then classically, of course, $\Theta(N)$ queries are necessary and sufficient. By querying f in superposition, Grover's algorithm [11] finds x using $O\left(N^{1/2}\right)$ queries, together with $\widetilde{O}\left(N^{1/2}\right)$ auxiliary computation steps (here the $\widetilde{O}$ hides a factor of the form $(\log N)^c$). Bennett et al. [8] showed that any quantum algorithm needs $\Omega\left(N^{1/2}\right)$ queries.

In this section, we show how to find the marked item by sampling histories, using only $O\left(N^{1/3}\right)$ queries and $\widetilde{O}\left(N^{1/3}\right)$ computation steps. Formally, the model is as follows. Each of the quantum circuits $U_1, \ldots, U_T$ that algorithm A gives to the history oracle $\mathcal{O}(\mathcal{T})$ is now able to query f. Suppose U_t makes q_t queries to f; then the total number of queries made by A is defined to be $Q = q_1 + \cdots + q_T$. The total number of *computation* steps is at least the number of steps required to write down $U_1, \ldots, U_T$, but could be greater.

Theorem 4 *In the* DQP *model, we can search a database of N items for a unique marked item using $O\left(N^{1/3}\right)$ queries and $\widetilde{O}\left(N^{1/3}\right)$ computation steps.*

Proof. Assume without loss of generality that $N = 2^n$ with $n|3$, and that each database item is labeled by an n-bit string. Let $x \in \{0,1\}^n$ be the label of the unique marked item. Then the sequence of quantum circuits $\mathcal{U}$ does the following: it first runs $O\left(2^{n/3}\right)$ iterations of Grover's

[6] For if there are multiple marked items, then we can reduce to the unique marked item case by using the Valiant-Vazirani hashing technique described in Theorem 3.

algorithm, in order to produce the n-qubit state $\alpha |x\rangle + \beta \sum_{y \in \{0,1\}^n} |y\rangle$, where

$$\alpha = \sqrt{\frac{1}{2^{n/3} + 2^{-n/3+1} + 1}},$$
$$\beta = 2^{-n/3}\alpha$$

(one can check that this state is normalized). Next $\mathcal{U}$ applies Hadamard gates to the first $n/3$ qubits. This yields the state

$$2^{-n/6}\alpha \sum_{y \in \{0,1\}^{n/3}} (-1)^{x_A \cdot y} |y\rangle |x_B\rangle + 2^{n/6}\beta \sum_{z \in \{0,1\}^{2n/3}} |0\rangle^{\otimes n/3} |z\rangle,$$

where x_A consists of the first $n/3$ bits of x, and x_B consists of the remaining $2n/3$ bits. Let Y be the set of $2^{n/3}$ basis states of the form $|y\rangle |x_B\rangle$, and Z be the set of $2^{2n/3}$ basis states of the form $|0\rangle^{\otimes n/3} |z\rangle$.

Notice that $2^{-n/6}\alpha = 2^{n/6}\beta$. So with the sole exception of $|0\rangle^{\otimes n/3} |x_B\rangle$ (which belongs to both Y and Z), the "marked" basis states in Y have the same amplitude as the "unmarked" basis states in Z. This is what we wanted. Notice also that, if we manage to find any $|y\rangle |x_B\rangle \in Y$, then we can find x itself using $2^{n/3}$ further classical queries: simply test all possible strings that end in x_B. Thus, the goal of our algorithm will be to cause the hidden variable to visit an element of Y, so that inspecting the variable's history reveals that element.

As in Theorem 3, the tools that we need are the juggle subroutine, and a way of reducing many basis states to two. Let s be drawn uniformly at random from $\{0,1\}^{n/3}$. Then $\mathcal{U}$ appends a third register to $|\phi\rangle$, and sets it equal to $|z\rangle$ if the first two registers have the form $|0\rangle^{\otimes n/3} |z\rangle$, or to $|s, y\rangle$ if they have the form $|y\rangle |x_B\rangle$. Disregarding the basis state $|0\rangle^{\otimes n/3} |x_B\rangle$ for convenience, the result is

$$2^{-n/6}\alpha \left(\sum_{y \in \{0,1\}^{n/3}} (-1)^{x_A \cdot y} |y\rangle |x_B\rangle |s, y\rangle + \sum_{z \in \{0,1\}^{2n/3}} |0\rangle^{\otimes n/3} |z\rangle |z\rangle \right).$$

Next $\mathcal{U}$ applies the juggle subroutine to the joint state of the first two registers. Suppose the hidden-variable value has the form $|0\rangle^{\otimes n/3} |z\rangle |z\rangle$ (that is, lies outside Y). Then with probability $2^{-n/3}$ over s, the first $n/3$ bits of z are equal to s. Suppose this event occurs. Then conditioned on the third register being $|z\rangle$, the reduced state of the first two registers is

$$\frac{(-1)^{x_A \cdot z_B} |z_B\rangle |x_B\rangle + |0\rangle^{\otimes n/3} |z\rangle}{\sqrt{2}},$$

where z_B consists of the last $n/3$ bits of z. So it follows from Section 4 that with probability $\Omega(1/n)$, the juggle subroutine will cause the hidden variable to transition from $|0\rangle^{\otimes n/3} |z\rangle$ to $|z_B\rangle |x_B\rangle$, and hence from Z to Y.

The algorithm calls the juggle subroutine $\Theta\left(2^{n/3} n\right) = \Theta\left(N^{1/3} \log N\right)$ times, drawing a new value of s and recomputing the third register after each call. Each call moves the hidden variable from Z to Y with independent probability $\Omega\left(2^{-n/3}/n\right)$; therefore with high probability *some* call does so. Note that this juggling phase does not involve any database queries. Also, as in Theorem 3, "drawing" s really means preparing a uniform superposition over all possible s. Finally, the

probability that the hidden variable ever visits the basis state $|0\rangle^{\otimes n/3}|x_B\rangle$ is exponentially small (by the union bound), which justifies our having disregarded it. ■

A curious feature of Theorem 4 is the tradeoff between queries and computation steps. Suppose we had run Q iterations of Grover's algorithm, or in other words made Q queries to f. Then provided $Q \leq \sqrt{N}$, the marked state $|x\rangle$ would have occurred with probability $\Omega\left(Q^2/N\right)$, meaning that $\widetilde{O}\left(N/Q^2\right)$ calls to the juggle subroutine would have been sufficient to find x. Of course, the choice of Q that minimizes $\max\left\{Q, N/Q^2\right\}$ is $Q = N^{1/3}$. On the other hand, had we been willing to spend $\widetilde{O}\left(N\right)$ computation steps, we could have found x with only a *single* query![7] Thus, one might wonder whether some other algorithm could push the number of queries below $N^{1/3}$, without simultaneously increasing the number of computation steps. The following theorem rules out that possibility.

Theorem 5 *In the* DQP *model,* $\Omega\left(N^{1/3}\right)$ *computation steps are needed to search an* N*-item database for a unique marked item. As a consequence, there exists an oracle relative to which* $\mathsf{NP} \not\subset \mathsf{DQP}$*; that is,* NP*-complete problems are not efficiently solvable by sampling histories.*

Proof. Let $N = 2^n$ and $f : \{0,1\}^n \rightarrow \{0,1\}$. Given a sequence of quantum circuits $\mathcal{U} = (U_1, \ldots, U_T)$ that query f, and assuming that $x \in \{0,1\}^n$ is the unique string such that $f(x) = 1$, let $|\psi_t(x)\rangle$ be the quantum state after U_t is applied but before U_{t+1} is. Then the "hybrid argument" of Bennett et al. [8] implies that, by simply changing the location of the marked item from x to x^*, we can ensure that

$$\||\psi_t(x)\rangle - |\psi_t(x^*)\rangle\| = O\left(\frac{Q_t^2}{N}\right)$$

where $\|\ \|$ represents trace distance, and Q_t is the total number of queries made to f by $U_1, \ldots, U_t$. Therefore $O\left(Q_t^2/N\right)$ provides an upper bound on the probability of noticing the $x \rightarrow x^*$ change by monitoring v_t, the value of the hidden variable after U_t is applied. So by the union bound, the probability of noticing the change by monitoring the entire history $(v_1, \ldots, v_T)$ is at most of order

$$\sum_{t=1}^{T} \frac{Q_t^2}{N} \leq \frac{TQ_T^2}{N}.$$

This cannot be $\Omega(1)$ unless $T = \Omega\left(N^{1/3}\right)$ or $Q_T = \Omega\left(N^{1/3}\right)$, either of which implies an $\Omega\left(N^{1/3}\right)$ lower bound on the total number of steps.

To obtain an oracle relative to which $\mathsf{NP} \not\subset \mathsf{DQP}$, we can now use a standard and well-known "diagonalization method" due to Baker, Gill, and Solovay [7] to construct an infinite sequence of exponentially hard search problems, such that any DQP machine fails on at least one of the problems, whereas there exists an NP machine that succeeds on all of them. We omit the details. ■

7 Discussion

Perhaps the most interesting problem left open by this paper is the computational complexity of simulating Bohmian mechanics. We strongly conjecture that this problem, like the hidden-variable problems we have seen, is strictly harder than simulating an ordinary quantum computer.

[7] One should not make too much of this fact; one way to interpret it is simply that the "number of queries" should be redefined as $Q + T$ rather than Q.

The trouble is that Bohmian mechanics does not quite fit in our framework: as discussed in [1], we cannot have deterministic hidden-variable trajectories for discrete degrees of freedom such as qubits. Even worse, Bohmian mechanics violates the continuous analogue of the indifference axiom. On the other hand, this means that by trying to implement (say) the juggle subroutine with Bohmian trajectories, one might learn not only about Bohmian mechanics and its relation to quantum computation, but also about how essential the indifference axiom really is for our implementation.

On the computer science side, a key open problem is to show better upper bounds on DQP. Recall that we were only able to show $\mathsf{DQP} \subseteq \mathsf{EXP}$, by giving a classical exponential-time algorithm to simulate the flow theory $\mathcal{FT}$. Can we improve this to (say) $\mathsf{DQP} \subseteq \mathsf{PSPACE}$? Clearly it would suffice to give a PSPACE algorithm that computes the transition probabilities for some theory $\mathcal{T}$ satisfying the indifference and robustness axioms. On the other hand, this might not be *necessary*—that is, there might be an indirect simulation method that does not work by computing (or even sampling from) the distribution over histories. It would also be nice to pin down the complexities of simulating specific hidden-variable theories, such as $\mathcal{FT}$ and $\mathcal{ST}$.

8 Acknowledgments

I thank Umesh Vazirani, Ronald de Wolf, and an anonymous reviewer for comments on an earlier version of this paper; Antony Valentini and Rob Spekkens for helpful discussions; and Andris Ambainis for correcting an ambiguity in the definition of DQP. Supported by an NSF Graduate Fellowship and by DARPA grant F30602-01-2-0524.

References

[1] S. Aaronson (2004), Quantum computing and hidden variables I: mapping unitary to stochastic matrices, submitted. quant-ph/0408035.

[2] S. Aaronson (2002), Quantum lower bound for the collision problem, *Proc. ACM Symp. on Theory of Computing*, pp. 635–642. quant-ph/0111102.

[3] S. Aaronson (2004), Is quantum mechanics an island in theoryspace?, *Proceedings of the Växjö Conference "Quantum Theory: Reconsideration of Foundations"* (A. Khrennikov, ed.). quant-ph/0401062.

[4] D. S. Abrams and S. Lloyd (1998), Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems, *Phys. Rev. Lett.* 81:3992–3995. quant-ph/9801041.

[5] D. Aharonov and A. Ta-Shma (2003), Adiabatic quantum state generation and statistical zero knowledge, *Proc. ACM Symp. on Theory of Computing*, pp. 20–29. quant-ph/0301023.

[6] D. Bacon (2003), Quantum computational complexity in the presence of closed timelike curves, submitted. quant-ph/0309189.

[7] T. P. Baker, J. Gill, and R. Solovay (1975), Relativizations of the P=?NP question, *SIAM J. Comput.* 4(4):431–442.

[8] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani (1997), Strengths and weaknesses of quantum computing, *SIAM J. Comput.* 26(5):1510–1523. quant-ph/9701001.

[9] G. Brassard, P. Høyer, and A. Tapp (1997), Quantum algorithm for the collision problem, *ACM SIGACT News (Cryptology Column)* 28:14–19. quant-ph/9705002.

[10] L. R. Ford and D. R. Fulkerson (1962), *Flows in Networks*, Princeton.

[11] L. K. Grover (1996), A fast quantum mechanical algorithm for database search, *Proc. ACM Symp. on Theory of Computing*, pp. 212–219. quant-ph/9605043.

[12] E. Guay and L. Marchildon (2003), Two-particle interference in standard and Bohmian quantum mechanics, *J. Phys. A.: Math. Gen.* 36:5617–24. quant-ph/0302085.

[13] A. Yu. Kitaev (1997), Quantum computation: algorithms and error correction, *Russian Math. Surveys* 52(6):1191-1249.

[14] M. Nielsen and I. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge.

[15] C. Philippidis, C. Dewdney, and B. J. Hiley (1979), Quantum interference and the quantum potential, *Nuovo Cimento* 52B:15.

[16] A. Sahai and S. Vadhan (2003), A complete problem for statistical zero knowledge, *J. of the ACM* 50(2):196–249.

[17] Y. Shi (2002), Quantum lower bounds for the collision and the element distinctness problems, *Proc. IEEE Symp. on Foundations of Comp. Sci.*, pp. 513–519. quant-ph/0112086.

[18] A. Valentini (2002), Subquantum information and computation, *Pramana J. Physics* 59(2):269–277. quant-ph/0203049.

[19] L. G. Valiant and V. V. Vazirani (1986), NP is as easy as detecting unique solutions, *Theoret. Comp. Sci.* 47(3):85–93.