Quantum Computing and Dynamical Quantum Models

Scott Aaronson
University of California, Berkeley
aaronson@cs.berkeley.edu

A *dynamical quantum model* assigns an eigenstate to a specified observable even when no measurement is made, and gives a stochastic evolution rule for that eigenstate. Such a model yields a distribution over classical histories of a quantum state. We study what can be computed by sampling from that distribution, i.e., by examining an observer's entire history. We show that, relative to an oracle, one can solve problems in polynomial time that are intractable even for quantum computers; and can search an N-element list in order $N^{1/3}$ steps (though not fewer).

Given a system with known Hamiltonian and initial state, nonrelativistic quantum theory specifies the probability of measuring an observable in a given eigenstate at each time $t \geq 0$. It does not, however, yield multiple-time or transition probabilities [1, 2, 3, 4]: that is, what is the probability that an observable assumes value $|\psi_2\rangle$ at t_2, given that it assumed $|\psi_1\rangle$ at an earlier time t_1 (though was not measured at t_1)?

This question, we argue, is not easily ignored in scenarios wherein a Hamiltonian H is coherently applied to a system that contains an observer. Granting the possibility of macroscopic coherence, one might try to avoid the question as follows. In a typical experiment, one keeps records of observations. If the records were stored where H could not affect them, then they would inhibit the interference that H would otherwise produce. If, on the other hand, records were not kept, or were themselves subject to H, then at time t_2 one would lose the right to ask which eigenstate was observed at t_1, since at t_2 this event has no meaning outside of records available at t_2. The difficulty with this account is that it is unclear what a 'prediction' could mean without some notion of multiple-time probabilities independent of records. Indeed, the 'outcome of an experiment,' the 'output of a computation,' and the 'utility of a decision' all seem to presuppose an observer or collection of observers persisting over time. (See [2, p.126] and [5, p.135-6] for related criticisms.)

The question of multiple-time probabilities arises in any interpretation of quantum theory that treats observers as physical systems that can be placed in superposition. This includes many-worlds interpretations, modal interpretations, and the Bohm interpretation, though not 'explicit-collapse' interpretations. The Bohm interpretation asserts an answer to our question, but applies only to a particular setting: it assumes not only the form of the guiding equation, but also a state space (the positions and momenta of particles in Euclidean space) and a preferred observable (position). We take a more abstract perspective, which allows arbitrary finite state spaces, and does not commit to any one observable or dynamics.

In this Letter we initiate the study of multiple-time probabilities from the standpoint of quantum computing. Our main result is that an observer, if given access to past eigenstates, could solve problems efficiently that are believed to be intractable even for quantum computers. Although such access is not permitted by quantum theory, an observer might wish to *calculate* a probable history of eigenstates, given a dynamics, initial state, and Hamiltonian. Under weak assumptions, we show that this task is infeasible even for moderately-sized systems, meaning those for which a quantum computer could efficiently sample eigenstates at *single* times.

We define a *dynamical quantum model* to be a function which, given a pure or mixed state ρ in N dimensions, a unitary U acting on ρ, and a von Neumann observable V with N possible outcomes, specifies (for all i, j) a probability p_{ij} that V assumes

value i before U is applied to ρ (time t_1), and j after U is applied (time t_2). The p_{ij}'s must marginalize to the single-time probabilities implied by quantum theory: that is, the diagonal entries of $V\rho V^{-1}$ at t_1, and of $VU\rho U^{-1}V^{-1}$ at t_2. It is immediate that there exists a dynamical model (the simplest one, which we call the *product dynamics* or $\mathcal{PD}$, takes the distribution over V at t_2 to be independent of that at t_1), and that there are infinitely many nonequivalent models.

Let a quantum computer have initial state $|0\rangle^{\otimes n}$, and suppose we apply a sequence $\mathcal{U} = (U_1, \ldots, U_T)$ of unitary operations, each of which can be implemented in BQP, or bounded-error quantum polynomial time. (See [6] for background on BQP and other computational complexity classes.) Let V be the observable corresponding to the standard (computational) basis. We consider a *history* $H = (v_1, \ldots, v_T)$ of V, which chooses a particular eigenstate of V at each time step: namely, v_k immediately after U_k is applied to the state $U_{k-1} \cdots U_1 |0\rangle^{\otimes n}$. Then any dynamics $\mathcal{D}$ yields a distribution $\Omega(\mathcal{U}, \mathcal{D})$ over histories. Observe that Ω is a Markov distribution; that is, each v_k is independent of the other v_l's conditioned on v_{k-1} and v_{k+1}. Sampling a history from Ω is at least as difficult as simulating a polynomial-time quantum computation, for sampling from the marginal distribution over any v_k is equivalent to simulating a standard-basis measurement of $U_k \cdots U_1 |0\rangle^{\otimes n}$. But could sampling a history enable one to solve problems that are intractable even for quantum computers?

To separate this question from any particular dynamics, we introduce a complexity class DQP, or dynamical quantum polynomial-time. Informally, DQP consists of those problems solvable in polynomial time by sampling histories under *any* dynamical model, so long as it satisfies locality and symmetry conditions to be discussed. We then show that $\mathsf{SZK} \subseteq \mathsf{DQP}$, where SZK, statistical zero knowledge, is a classical complexity class containing several problems that have resisted efficient quantum algorithms—including graph isomorphism, nonabelian hidden subgroup, and approximate shortest lattice vector. Already this suggests that $\mathsf{BQP} \neq \mathsf{DQP}$, i.e., that our dynamical quantum computing model is strictly more powerful than the usual quantum computing model. However, we give stronger evidence, of the kind typically sought in computer science. We recently obtained [7] a lower bound of order $n^{1/5}$ on the number of oracle queries needed by a quantum computer to solve the 'collision problem,' that of deciding whether a function $f : \{1, \ldots, n\} \to \mathbb{Z}$ is one-to-one or two-to-one. (Shi [8] has improved this bound to order $n^{1/3}$, which is optimal.) But the collision problem, which abstractly models SZK, can be solved in a *constant* number of queries using a dynamical model. Formalizing this intuition, we show in [7] that there exists an oracle A for which $\mathsf{SZK}^A \not\subseteq \mathsf{BQP}^A$, and therefore $\mathsf{BQP}^A \neq \mathsf{DQP}^A$.

As is usual in quantum computing, we assume a Hilbert space $\mathcal{H}_N$ of finite dimension N, and discretize time into steps of equal length τ. Other authors [1] have considered dynamics in a continuous-time setting. It might be thought that our restriction to discrete time introduces a drawback, that the dynamics depend not just on the initial state and Hamiltonian but also on the choice of τ. For example, two Hadamard gates applied in succession seem to correspond to two random transitions when considered separately, but to a permutation (namely the identity permutation) when considered jointly. However, an analogous problem occurs in the continuous-time setting. There, letting $t \to 0$ be the length of a time interval being considered, there is still a free parameter $d\tau/dt$ on which the dynamics depend.

For simplicity, we consider the dynamics of only a single time-independent observable V, and assume those dynamics at each time t to depend only on the state and Hamiltonian at t (it is easy to show that they cannot depend on the Hamiltonian only). By the Kochen-Specker theorem we cannot assign values noncontextually to

every observable, let alone specify their transition probabilities. We could consider a subset S of observables that contains no Kochen-Specker contradiction, but even then we could not apply a dynamical model independently to each observable in S without in general violating noncontextuality. The case of time-dependent observables was considered in [1] and elsewhere.

Formally, a dynamical quantum model is fully characterized by a family of functions, $\{\mathcal{D}_N\}_{N\geq 1} : \mathcal{H}_N \times U(N)^2 \rightarrow S(N)$, which map a pure or mixed state $\rho \in \mathcal{H}_N$, a unitary $U \in U(N)$, and an orthonormal basis $V = v_1, \ldots, v_N \in U(N)$ onto a singly stochastic matrix $S \in S(N)$. We sometimes suppress the dependence on N. Let $(M)_{ij}$ denote the entry in the i^{th} column and j^{th} row of M. Then $(S)_{ij}$ is the probability that the observable corresponding to V takes value v_j after U is applied to ρ, conditioned on V taking value v_i before U is applied. Any dynamics must satisfy the conditions of *unitary invariance*—for all unitary changes of basis W,

$$\mathcal{D}(\rho, U, V) = \mathcal{D}\left(W\rho W^{-1}, WUW^{-1}, WVW^{-1}\right),$$

and *marginalization*—for all $j \in \{1, \ldots, N\}$,

$$\sum_i (S)_{ij} (\rho)_{ii} = \left(U\rho U^{-1}\right)_{jj}.$$

Because of invariance, we will henceforth take $V = I$ and consider $\mathcal{D}$ as a function of ρ and U only.

Three additional conditions we desire are *symmetry*, *robustness*, and *locality*. We say that $\mathcal{D}$ is symmetric if it is invariant under relabeling of basis states: more precisely, for all permutation matrices P and Q,

$$\mathcal{D}\left(P\rho P^{-1}, QUP^{-1}\right) = Q\mathcal{D}(\rho, U) P^{-1}.$$

Also, $\mathcal{D}$ is robust if it is insensitive to sufficiently small errors (which, in particular, implies continuity): for all polynomials p, there exists a polynomial q such that for all N, $\rho \in \mathcal{H}_N$, and $U \in U(N)$,

$$\|\mathcal{D}_N(\rho, U) - \mathcal{D}_N(\rho^*, U^*)\| \leq 1/p(N)$$

where $\|M\| = \max_{ij} \left|(M)_{ij}\right|$, whenever $\|\rho - \rho^*\| \leq 1/q(N)$ and $\|U - U^*\| \leq 1/q(N)$. Robustness will not be needed for our results, but is often demanded of a computational model.

In the interest of generality, we did not assume $\mathcal{H}_N$ to have a particular tensor product structure. Thus, we define locality by partitioning the basis states into 'blocks,' between which U can never produce interference. Call $L \subseteq \{1, \ldots, N\}$ a *block* if $(U)_{ik} = 0$ for all $i \in L$ and $k \notin L$, and a *minimal block* if no $L^* \subset L$ is a block. Note that the minimal blocks are disjoint. Then $\mathcal{D}$ is local if it acts separately on each minimal block: more formally,

$$(S)_{ij} = \mathcal{D}_{|L|}(\rho_L, U_L)$$

for all minimal blocks L and $i, j \in L$, where U_L is the $L \times L$ submatrix of U, and ρ_L is the $L \times L$ submatrix of ρ normalized to have trace 1. We do not claim that the locality condition implies relativistic causality. For example, if ρ_{AB} is a bipartite state and U_A and U_B act only on A and B respectively, then locality does not imply *commutativity* in the sense that

$$\begin{aligned}&\mathcal{D}\left(U_A\rho_{AB}U_A^{-1}, U_B\right)\mathcal{D}(\rho_{AB}, U_A)\\ &= \mathcal{D}\left(U_B\rho_{AB}U_B^{-1}, U_A\right)\mathcal{D}(\rho_{AB}, U_B).\end{aligned}$$

We raise as an open question whether there exists a dynamical model satisfying robustness, locality, and commutativity. See [3] for a more detailed analysis of causality in dynamical models.

The product dynamics $\mathcal{PD}$ is unsatisfactory because it does not satisfy locality. Dieks [4] proposed partitioning the basis vectors into minimal blocks and applying $\mathcal{PD}$ separately to each. The resulting *Dieks dynamics*, $\mathcal{DD}$, satisfies locality and commutativity, but not robustness, since the minimal blocks are sensitive to arbitrarily small changes to U.

We introduce a dynamical model, the *Schrödinger dynamics* or $\mathcal{SD}$, that satisfies robustness and locality. Commutativity is satisfied for unentangled states but not for entangled ones. Constructing $\mathcal{SD}$ involves solving a system of nonlinear equations, which were first studied in the continuous case by Schrödinger [9]. The existence and uniqueness of a solution was shown under broad conditions by Nagasawa [10]. In the discrete case, where the problem is known as (r, c)-*scaling*, efficient algorithms are known for finding the solution ([11] and references therein).

The idea is repeatedly to tweak U to bring it closer to a stochastic matrix that satisfies the marginalization condition. The first step is to replace each entry of U by its squared magnitude, obtaining $U^{(0)}$ such that $\left(U^{(0)}\right)_{ij} = \left|(U)_{ij}\right|^2$. We wish to make the i^{th} column of the matrix sum to $(\rho)_{ii}$, and the j^{th} row sum to $\left(U\rho U^{-1}\right)_{jj}$ for all $i, j \in \{1, \ldots, N\}$. The stochastic matrix S mapping $\mathrm{diag}\,(\rho)$ to $\mathrm{diag}\left(U\rho U^{-1}\right)$ is then readily obtained by normalizing each column to sum to 1. Here 'normalizing' means multiplying by a scalar.

The algorithm is iterative. For each $t \geq 0$ we obtain $U^{(2t+1)}$ by normalizing each column i of $U^{(2t)}$ to sum to $(\rho)_{ii}$; likewise we obtain $U^{(2t+2)}$ by normalizing each row j of $U^{(2t+1)}$ to sum to $\left(U\rho U^{-1}\right)_{jj}$. We claim that (1) the limit $U^{(\infty)}$ of this iteration exists, and (2) the resulting diagonal matrices A and B such that $U^{(\infty)} = AU^{(0)}B$ are unique up to scalar multiples. It is known [11] that both claims are implied by the following 'flow condition': there exists a nonnegative matrix M such that $\sum_k (M)_{ik} = (\rho)_{ii}$ for all i, $\sum_k (M)_{kj} = \left(U\rho U^{-1}\right)_{jj}$ for all j, and $(M)_{ij} = 0$ whenever $(U)_{ij} = 0$. Surprisingly, the flow condition always holds if U is unitary (we omit the proof).

Clearly $\mathcal{SD}$ satisfies locality, since $U^{(\infty)}_{ij} = 0$ whenever $U_{ij} = 0$. It is shown in [11] that for any polynomial p, the iterative algorithm converges to within $1/p\,(N)$ precision in polynomial time. Using this one can show that $\mathcal{SD}$ satisfies robustness also.

We now define the complexity class DQP. For a dynamics $\mathcal{D}$, let $\mathcal{O}\,(\mathcal{D})$ be an oracle that takes as input a sequence $\mathcal{U} = (U_1, \ldots, U_T)$ of quantum circuits, and returns as output a sample $(v_1, \ldots, v_T)$ from the history distribution $\Omega\,(\mathcal{U}, \mathcal{D})$ as defined previously. Then let $\mathsf{DQP}\,(\mathcal{D}) = \mathsf{BQP}^{\mathcal{O}(\mathcal{D})}$ (i.e. BQP with oracle access to $\mathcal{O}\,(\mathcal{D})$), and let DQP be the set of languages that are in $\mathsf{DQP}\,(\mathcal{D})$ for all $\mathcal{D}$ satisfying symmetry and locality. Other reasonable classes could be defined—for example, we could allow only classical queries to $\mathcal{O}\,(\mathcal{D})$, or only one query instead of multiple ones—but such distinctions are a subject for complexity theory rather than physics. The best upper bound we know of is $\mathsf{DQP} \subseteq \mathsf{P}^{\#\mathsf{P}}$, from the Dieks dynamics.

Let us see why $\mathsf{SZK} \subseteq \mathsf{DQP}$. Sahai and Vadhan [12] showed that, to simulate SZK, it suffices to solve the following *statistical difference* (SD) problem. Suppose deterministic classical polynomial-time algorithm P_i (for $i \in \{0, 1\}$) returns output $Y_i\,(X) \in \{0, 1\}^{n+1}$ distributed according to $\Lambda_i = (p_{Y,i})$, when given an input X chosen uniformly from $\{0, 1\}^n$. Then decide whether Λ_0 and Λ_1 are 'ε-close' or

'ε-far'—that is, whether

$$\|\Lambda_0 - \Lambda_1\| = \sum_Y |p_{Y,0} - p_{Y,1}| / 2$$

is less than ε or greater than $1-\varepsilon$ for some $\varepsilon > 0$, given that one of these is the case. As an example, let G_0 and G_1 be graphs, and let Λ_i be the uniform distribution over all permutations of G_i. Then Λ_0 and Λ_1 are 0-close (that is, identical) if G_0 and G_1 are isomorphic, and are 0-far (disjoint) otherwise. It follows that testing isomorphism of graphs is reducible to SD, and hence is in SZK.

In the special case where P_0 and P_1 are one-to-one, the DQP algorithm consists simply of three quantum circuits, U_1, U_2, and U_3. First U_1 transforms $|0\rangle^{\otimes n}$ to $(|\Phi_0\rangle + |\Phi_1\rangle)/\sqrt{2}$, where

$$|\Phi_i\rangle = 2^{-n/2} \sum_{X \in \{0,1\}^n} |i\rangle |X\rangle |Y_i(X)\rangle$$

for a control bit $|i\rangle$ (henceforth $|Y_i(X)\rangle$ is abbreviated $|Y\rangle$). Then U_2 applies a bitwise Fourier transform to $|i\rangle|X\rangle$ (that is, a Hadamard gate on each bit), and U_3 does the same, returning the state to $U_1|0\rangle^{\otimes n}$. Intuitively, this is analogous to measuring $|Y\rangle$, and then making multiple 'non-collapsing' measurements of $|i\rangle$ to see whether it contains one value or a superposition of two values. In the former case we conclude that Λ_0 and Λ_1 are ε-far; in the latter that they are ε-close. The technical part is to show that this algorithm works under *any* symmetric local model.

Let $v_k = |i_k\rangle |X_k\rangle |Y\rangle$ be the value of V immediately after U_k is applied. First suppose Λ_0 and Λ_1 are ε-far. Then because P_0 and P_1 are one-to-one, v_1's 'counterpart' $|\neg i_1\rangle \left|X_1^{(\neg)}\right\rangle |Y\rangle$ has zero amplitude in $U_1|0\rangle^{\otimes n}$ with probability at least $1-\varepsilon$, where '$\neg$' denotes negation. In that case, the state of $|i\rangle$ conditioned on $|Y\rangle$ is $|i_1\rangle$. Since U_2 and U_3 do not act on $|Y\rangle$ and U_3U_2 is the identity, it follows by locality that $i_1 = i_3$.

Second, suppose Λ_0 and Λ_1 are ε-close. Define binary vectors $a = i_1 \circ X_1$, $b = \neg i_1 \circ X_1^{(\neg)}$, and $c = i_2 \circ X_2$ in $\mathbb{Z}_2^{n+1}$, where '$\circ$' denotes concatenation. Then $|a\rangle|Y\rangle$ and $|b\rangle|Y\rangle$ have equal amplitude with probability at least $1-\varepsilon$. Recall that the Fourier transform F maps $|a\rangle$ onto $2^{-n/2}\sum_c (-1)^{a \cdot c} |c\rangle$ and similarly for $|b\rangle$. Thus, the only $|c\rangle$ that have nonzero amplitude in $U_2U_1|0\rangle^{\otimes n}$ are those for which $a \cdot c \equiv b \cdot c \pmod 2$. We wish to show that F is symmetric under some permutation of eigenstates that interchanges a with b while leaving c fixed. Suppose we had an invertible matrix M over $\mathbb{Z}_2^{n+1}$ such that $Ma = b$, $Mb = a$, and $M^T c = c$. Then define two permutations σ, τ over binary vectors by $\sigma(a) = Ma$ and $\tau(c) = \left(M^T\right)^{-1} c$, so that

$$\sigma(a) \cdot \tau(c) \equiv a \cdot c \pmod 2$$

for all a, c. Since the (a,c) entry of F is $2^{-(n+1)/2}(-1)^{a \cdot c}$, this implies that F is symmetric under application of σ to its input eigenstates and τ^{-1} to its output eigenstates. We argue that such an M exists so long as a and b are nonzero (which they almost certainly are). For let w and z be unit vectors, and let L be an invertible matrix over $\mathbb{Z}_2^{n+1}$ such that $Lw = a$ and $Lz = b$. Let Q be the permutation matrix that interchanges w and z while leaving all other unit vectors fixed. Then set $M = LQL^{-1}$. Clearly $Ma = b$ and $Mb = a$. Also, $a \cdot c = b \cdot c$ implies $w^T L^T c = z^T L^T c$, so the w and z entries of $L^T c$ are equal, and thus $Q^T\left(L^T c\right) = L^T c$, implying $M^T c = c$.

By the symmetry condition, it follows that $(S)_{ca} = (S)_{cb} = 1/2$, where $(S)_{ca}$ is the probability that $v_3 = |a\rangle|Y\rangle$ and $(S)_{cb}$ that $v_3 = |b\rangle|Y\rangle$, both conditioned on $v_2 = |c\rangle|Y\rangle$. Thus, there is a $1/2$ probability that $i_1 \neq i_3$.

For general P_0 and P_1, we can reduce to the one-to-one case by appending a register $|h(i \circ X)\rangle$ to $|\Phi_i\rangle$, on which U_2 and U_3 do not act. Here h is chosen uniformly at random among all 'hash functions' mapping $\mathbb{Z}_2^{n+1}$ to $\{1, \ldots, K\}$, for some range size K. Let $n_0 = \left|P_0^{-1}(Y)\right|$ be the number of X such that $P_0(X) = Y$, and similarly define n_1. Then assuming that Λ_0 and Λ_1 are ε-close, $|n_0/n_1 - 1| < 4\varepsilon$ with probability at least $3/4$ over the choice of Y, by Markov's inequality. After applying U_1, we apply U_2 and U_3 in succession n times, initially with $K = 1$ and each time thereafter setting K to twice its previous value and recomputing h. Define $a = i_1 \circ X_1$ as before. Then we want there to exist a unique counterpart $b = \neg i_1 \circ X_1^{(\neg)}$ such that $h(a) = h(b)$, but no $a^* = i_1 \circ X_1^*$ such that $h(a) = h(a^*)$. Letting $\alpha = n_1/K$, this joint event (call it E) occurs with probability

$$(1 - 1/K)^{n_0+n_1} \, n_1/K \approx \alpha e^{-2\alpha(1\pm 2\varepsilon)}$$

over the choice of h. This is bounded away from 0 when $\alpha \in [1, 2]$. When E does occur, the analysis for the one-to-one case applies, and establishes that v_1 and its counterpart are both observed with $1/2$ probability.

The algorithm for searching an unordered list of N items in order $N^{1/3}$ queries is conceptually similar. Assume for simplicity that there is a unique marked state $|j\rangle$ that we are trying to find. The first step is to apply $N^{1/3}$ iterations of Grover's search algorithm [13], thereby boosting the probability of observing $|j\rangle$ to order $N^{-1/3}$. The next step is to 'juggle' the observable V as uniformly as possible, so that after order $N^{1/3}$ steps, with high probability V has visited $|j\rangle$ at least once. Then j can be found by inspecting the classical history $(v_1, \ldots, v_T)$. Again the technical part is to show that this can be done in any symmetric local model, and again the primary tools are a hash function (to reduce the problem of juggling V among many eigenstates to that of juggling it between two), and the bitwise Fourier transform (to juggle). Details are omitted due to space limitations.

The $N^{1/3}$ bound is easily seen to be optimal under *any* dynamical model. Bennett et al. [14] showed that, if $\Psi^{(t)}(X)$ is an algorithm's state after t queries to an N-item list X, then by changing one item of X we can obtain a list X^* such that $\left\|\Psi^{(t)}(X) - \Psi^{(t)}(X^*)\right\| \precsim t^2/N$ in trace distance. It follows by the union bound that, if $T \ll N^{1/3}$ queries are made, then the probability that the $X \to X^*$ change affects the history $(v_1, \ldots, v_T)$ is of order $\sum_{t=1}^{T} t^2/N \ll 1$. Hence, there exists an oracle A relative to which NP-complete problems are not efficiently solvable in dynamical models; that is, $\mathsf{NP}^A \not\subseteq \mathsf{DQP}^A(\mathcal{D})$ for any $\mathcal{D}$. This result supports the intuition that dynamical models are somehow more 'physically reasonable' than (for example) nonlinear quantum models, which *would* enable NP-complete and even #P-complete problems to be solved in polynomial time [15]. Although our model grants an observer access to her entire history within a quantum system, it does not allow her to record histories in superposition, or otherwise to influence the system in a way contrary to quantum theory.

I thank Ronald de Wolf, Umesh Vazirani, John Preskill, Guido Bacciagaluppi, Avi Wigderson, and Dennis Dieks for helpful discussions. Supported by an NSF Graduate Fellowship and by DARPA grant F30602-01-2-0524.

References

[1] G. Bacciagaluppi and M. Dickson, *Found. Phys.* 29, 1165(1999).

[2] J. Barrett, *The Quantum Mechanics of Minds and Worlds*, Oxford (1999).

[3] M. Dickson and R. Clifton, in *The Modal Interpretation of Quantum Mechanics*, D. Dieks and P. E. Vermaas (eds), Kluwer (1998).

[4] D. Dieks, *Phys. Rev. A* , 2290(1994). Dieks (personal communication) would no longer defend the model we call DD.
[5] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge (1987).
[6] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge (2000).
[7] S. Aaronson, *Proc. ACM STOC* (2002).
[8] Y. Shi, manuscript (2001). quant-ph/0112086.
[9] E. Schrödinger, *Sitzungsber. Preuss. Akad. Wissen. Phys. Math. Kl.*, 144(1931).
[10] M. Nagasawa, *Prob. Theory and Related Fields* 82, 109(1989).
[11] N. Linial, A. Samorodnitsky, and A. Wigderson, *Combinatorica* 20(4), 545(2000).
[12] A. Sahai and S. Vadhan, *Proc. IEEE FOCS*, 448(1997).
[13] L. K. Grover, *Proc. ACM STOC*, 212(1996).
[14] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, *SIAM J. Comp.* 26(5), 1510(1997).
[15] D. Abrams and S. Lloyd, *Phys. Rev. Lett.* 81, 3992(1998).