Quantum Computing and Hidden Variables I: Mapping Unitary to Stochastic Matrices

Scott Aaronson[*]

Abstract

This paper initiates the study of hidden variables from the discrete, abstract perspective of quantum computing. For us, a hidden-variable theory is simply a way to convert a unitary matrix that maps one quantum state to another, into a stochastic matrix that maps the initial probability distribution to the final one in some fixed basis. We list seven axioms that we might want such a theory to satisfy, and then investigate which of the axioms can be satisfied simultaneously. Toward this end, we construct a new hidden-variable theory that is both robust to small perturbations and indifferent to the identity operation, by exploiting an unexpected connection between unitary matrices and network flows. We also analyze previous hidden-variable theories of Dieks and Schrödinger in terms of our axioms. In a companion paper, we will show that actually *sampling* the history of a hidden variable under reasonable axioms is at least as hard as solving the Graph Isomorphism problem; and indeed is probably intractable even for quantum computers.

1 Introduction

Quantum mechanics lets us calculate the probability that (say) an electron will be found in an excited state if measured at a particular time. But it is silent about *multiple-time* or *transition* probabilities: that is, what is the probability that the electron will be in an excited state at time t_1, given that it was in its ground state at an earlier time t_0? The usual response is that this question is meaningless, unless of course the electron was *measured* (or otherwise known with probability 1) to be in its ground state at t_0. A different response—pursued by Schrödinger [22], Bohm [5], Bell [3], Nelson [19], Dieks [10], and others—treats the question as provisionally meaningful, and then investigates how one might answer it mathematically. Specific attempts at answers are called “hidden-variable theories.”

The appeal of hidden-variable theories is that they provide one possible solution to the measurement problem. For they allow us to apply unitary quantum mechanics to the entire universe (including ourselves), yet still discuss the probability of a future observation conditioned on our current observations. Furthermore, they let us do so without making any assumptions about decoherence or the nature of observers. For example, even if an observer were placed in coherent superposition, that observer would still have a sequence of definite experiences, and the probability of any such sequence could be calculated.

This paper initiates the study of hidden variables from a quantum computing perspective. We restrict our attention to the simplest possible setting: that of discrete time, a finite-dimensional

[*] University of California, Berkeley. Email: aaronson@cs.berkeley.edu. Supported by an NSF Graduate Fellowship and by DARPA grant F30602-01-2-0524.

Hilbert space, and a fixed orthogonal basis. Within this setting, we reformulate known hidden-variable theories due to Dieks [10] and Schrödinger [22], and also introduce a new theory based on network flows. However, our main contribution is the *axiomatic approach* that we use. We propose seven axioms for hidden-variable theories in our setting, and then compare theories against each other based on which of the axioms they satisfy. A central question in this approach is which subsets of axioms can be satisfied simultaneously.

In a companion paper [1], we will make the connection to quantum computing explicit, by proving that under any hidden-variable theory that satisfies three reasonable axioms (called symmetry, indifference, and robustness), the ability to examine one's entire "history" through a quantum system would entail the ability to solve the Graph Isomorphism problem in polynomial time. What makes this result surprising is that, in the so-called oracle or black-box model, sampling histories would *not* entail the ability to solve NP-complete problems in polynomial time. We thus obtain the first good example of a computational model that appears "slightly" more powerful than the usual quantum computing model.

This paper lays the groundwork for the computational results of [1], in particular by showing that there *exists* a hidden-variable theory satisfying the symmetry, indifference, and robustness axioms.

The paper is organized as follows. Section 1.1 formally defines hidden-variable theories in our sense; then Section 1.2 contrasts these theories with related ideas such as Bohmian mechanics and modal interpretations. Section 1.3 addresses the most common objections to our approach: for example, that the implicit dependence on a fixed basis is unacceptable.

In Section 2, we introduce seven possible axioms for hidden-variable theories. These are symmetry under permutation of basis states; indifference to the identity operation; robustness to small perturbations; "block robustness," a weaker version of robustness; commutativity with respect to spacelike-separated unitaries; commutativity for the special case of product states; and invariance under decomposition of mixed states into pure states. Ideally, a theory would satisfy all of these axioms. However, we show in Section 3 that no theory satisfies both indifference and commutativity; no theory satisfies both indifference and a stronger version of robustness; no theory satisfies indifference, robustness, and decomposition invariance; and no theory satisfies a stronger version of decomposition invariance. The proofs of two of these results use the same geometric facts that underlie the Bell inequalities.

In Section 4 we shift from negative to positive results. Section 4.1 presents a hidden-variable theory called the *flow theory* or $\mathcal{FT}$, which is based on the Max-Flow-Min-Cut theorem from combinatorial optimization. The idea is to define a network of "pipes" from basis states at an initial time to basis states at a final time, and then route as much probability mass as possible through these pipes. The capacity of each pipe depends on the corresponding entry of the unitary acting from the initial to final time. To find the probability of transitioning from basis state $|i\rangle$ to basis state $|j\rangle$, we then determine how much of the flow originating at $|i\rangle$ is routed along the pipe to $|j\rangle$. Our main results are that $\mathcal{FT}$ is well-defined and that it is robust to small perturbations. Since $\mathcal{FT}$ trivially satisfies the indifference axiom, this implies that the indifference and robustness axioms can be satisfied simultaneously, which was not at all obvious *a priori*. The flow theory also satisfies symmetry, but not product commutativity, scalar invariance, or decomposition invariance.

Section 4.2 presents a second theory that we call the *Schrödinger theory* or $\mathcal{ST}$, since it is based on a pair of integral equations introduced in a 1931 paper of Schrödinger [22]. Schrödinger conjectured, but was unable to prove, the existence and uniqueness of a solution to these equations; the problem was not settled until the work of Nagasawa [18] in the 1980's. In our discrete setting the problem is simpler, and we give a self-contained proof of existence using a matrix scaling technique due to Sinkhorn [23]. The idea is as follows: we want to convert a unitary matrix that maps one quantum state to another, into a nonnegative matrix whose i^{th} column sums to the initial probability of basis state $|i\rangle$, and whose j^{th} row sums to the final probability of basis state $|j\rangle$. To do so, we first replace each entry of the unitary matrix by its absolute value, then normalize each column to sum to the desired initial probability, then normalize each row to sum to the desired final probability. But then the columns are no longer normalized correctly, so we normalize them *again*, then normalize the rows again, and so on. We show that this iterative process converges, from which it follows that $\mathcal{ST}$ is well-defined. We also show that $\mathcal{ST}$ satisfies the symmetry, indifference, and product commutativity axioms; and violates the decomposition invariance axiom. We conjecture that $\mathcal{ST}$ satisfies the robustness axiom; proving that conjecture is the main open problem of the paper. We conclude in Section 5.

1.1 Hidden-Variable Theories

Suppose we have an $N \times N$ unitary matrix U, acting on a state

$$|\psi\rangle = \alpha_1 |1\rangle + \cdots + \alpha_N |N\rangle,$$

where $|1\rangle, \ldots, |N\rangle$ is a standard orthogonal basis. Let

$$U|\psi\rangle = \beta_1 |1\rangle + \cdots + \beta_N |N\rangle.$$

Then can we construct a stochastic matrix S, which maps the vector of probabilities

$$\overrightarrow{p} = \begin{bmatrix} |\alpha_1|^2 \\ \vdots \\ |\alpha_N|^2 \end{bmatrix}$$

induced by measuring $|\psi\rangle$, to the vector

$$\overrightarrow{q} = \begin{bmatrix} |\beta_1|^2 \\ \vdots \\ |\beta_N|^2 \end{bmatrix}$$

induced by measuring $U|\psi\rangle$? Trivially yes. The following matrix maps *any* vector of probabilities to $\overrightarrow{q}$, ignoring the input vector $\overrightarrow{p}$ entirely:

$$S_{\mathcal{PT}} = \begin{bmatrix} |\beta_1|^2 & \cdots & |\beta_1|^2 \\ \vdots & & \vdots \\ |\beta_N|^2 & \cdots & |\beta_N|^2 \end{bmatrix}.$$

Here $\mathcal{PT}$ stands for *product theory.* The product theory corresponds to a strange picture of physical reality, in which memories and records are completely unreliable, there being no causal connection between states of affairs at earlier and later times.

So we would like S to depend on U itself somehow, not just on $|\psi\rangle$ and $U|\psi\rangle$. Indeed, ideally S would be a function *only* of U, and not of $|\psi\rangle$. But this is impossible, as the following example shows. Let U be a $\pi/4$ rotation, and let $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Then $U|+\rangle = |1\rangle$ implies that

$$S(|+\rangle, U) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix},$$

whereas $U\left|-\right\rangle = \left|0\right\rangle$ implies that

$$S\left(\left|-\right\rangle, U\right) = \left[\begin{array}{cc} 1 & 1 \\ 0 & 0 \end{array}\right].$$

On the other hand, it is easy to see that, if S can depend on $\left|\psi\right\rangle$ as well as U, then there are infinitely many choices for the function $S\left(\left|\psi\right\rangle, U\right)$. Every choice reproduces the predictions of quantum mechanics perfectly when restricted to single-time probabilities. So how can we possibly choose among them? Our approach in Sections 2 and 4 will be to write down axioms that we would like S to satisfy, and then investigate which of the axioms can be satisfied simultaneously.

Formally, a *hidden-variable theory* is a family of functions $\{S_N\}_{N\geq 1}$, where each S_N maps an N-dimensional mixed state ρ and an $N\times N$ unitary matrix U onto a singly stochastic matrix $S_N\left(\rho, U\right)$. We will often suppress the dependence on N, and use subscripts such as $\mathcal{PT}$ or $\mathcal{FT}$ to indicate the theory in question. Also, if $\rho = \left|\psi\right\rangle\left\langle\psi\right|$ is a pure state we may write $S\left(\left|\psi\right\rangle, U\right)$ instead of $S\left(\left|\psi\right\rangle\left\langle\psi\right|, U\right)$.

Let $(M)_{ij}$ denote the entry in the i^{th} column and j^{th} row of matrix M. Then $(S)_{ij}$ is the probability that the hidden variable takes value $\left|j\right\rangle$ after U is applied, conditioned on it taking value $\left|i\right\rangle$ before U is applied. At a minimum, any theory must satisfy the following marginalization axiom: for all $j\in\{1,\ldots,N\}$,

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

This says that after U is applied, the hidden variable takes value $\left|j\right\rangle$ with probability $\left(U\rho U^{-1}\right)_{jj}$, which is the usual Born probability.

Often it will be convenient to refer, not to S itself, but to the matrix $P\left(\rho, U\right)$ of joint probabilities whose (i,j) entry is $(P)_{ij} = (S)_{ij}(\rho)_{ii}$. The i^{th} column of P must sum to $(\rho)_{ii}$, and the j^{th} row must sum to $\left(U\rho U^{-1}\right)_{jj}$. Indeed, we will define the theories $\mathcal{FT}$ and $\mathcal{ST}$ by first specifying the matrix P, and then setting $(S)_{ij} := (P)_{ij}/(\rho)_{ii}$. This approach has the drawback that if $(\rho)_{ii} = 0$, then the i^{th} column of S is undefined. To get around this, we adopt the convention that

$$S\left(\rho, U\right) := \lim_{\varepsilon\rightarrow 0^+} S\left(\rho_\varepsilon, U\right)$$

where $\rho_\varepsilon = (1-\varepsilon)\rho + \varepsilon I$ and I is the $N\times N$ maximally mixed state. Technically, the limits

$$\lim_{\varepsilon\rightarrow 0^+}\frac{\left(P\left(\rho_\varepsilon, U\right)\right)_{ij}}{(\rho_\varepsilon)_{ii}}$$

might not exist, but in the cases of interest to us it will be obvious that they do.

1.2 Comparison with Previous Work

Before going further, we should contrast our approach with previous approaches to hidden variables, the most famous of which is Bohmian mechanics [5]. Our main criticism of Bohmian mechanics is that it commits itself to a Hilbert space of particle positions and momenta. Furthermore, it is crucial that the positions and momenta be *continuous*, in order for particles to evolve deterministically. To see this, let $\left|L\right\rangle$ and $\left|R\right\rangle$ be discrete positions, and suppose a particle is in state $\left|L\right\rangle$ at time t_1, and state $\left(\left|L\right\rangle + \left|R\right\rangle\right)/\sqrt{2}$ at a later time t_2. Then a hidden variable representing the position would have entropy 0 at t_1, since it is always $\left|L\right\rangle$ then; but entropy 1 at t_2, since it is

$|L\rangle$ or $|R\rangle$ both with 1/2 probability. Therefore the earlier value cannot determine the later one.[1] It follows that Bohmian mechanics is incompatible with the belief that all physical observables are discrete. But in our view, there are strong reasons to hold that belief, which include black hole entropy bounds; the existence of a natural minimum length scale (10^{-33} cm); results on area quantization in quantum gravity [21]; the fact that many physical quantities once thought to be continuous have turned out to be discrete; the infinities of quantum field theory; the implausibility of analog "hypercomputers"; and conceptual problems raised by the independence of the continuum hypothesis.

Of course there exist stochastic analogues of Bohmian mechanics, among them Nelsonian mechanics [19] and Bohm and Hiley's "stochastic interpretation" [6]. But it is not obvious why we should prefer these to other stochastic hidden-variable theories. From a quantum-information perspective, it is much more natural to take an abstract approach—one that allows arbitrary finite-dimensional Hilbert spaces, and that does not rule out any transition rule *a priori*.

Stochastic hidden variables have also been considered in the context of modal interpretations; see Dickson [8], Bacciagaluppi and Dickson [2], and Dieks [10] for example. However, the central assumptions in that work are extremely different from ours. In modal interpretations, a pure state evolving unitarily poses no problems at all: one simply rotates the hidden-variable basis along with the state, so that the state always represents a "possessed property" of the system in the current basis. Difficulties arise only for mixed states; and there, the goal is to track a whole set of possessed properties. By contrast, our approach is to fix an orthogonal basis, then track a single hidden variable that is an element of that basis. The issues raised by pure states and mixed states are essentially the same.

Finally we should mention the consistent-histories interpretation of Griffiths [16] and Gell-Mann and Hartle [14]. This interpretation assigns probabilities to various histories through a quantum system, so long as the "interference" between those histories is negligible. Loosely speaking, then, the situations where consistent histories make sense are precisely the ones where the question of transition probabilities can be avoided.

1.3 Objections

Hidden-variable theories, as we define them, are open to several technical objections. For example, we required transition probabilities for only one orthogonal observable. What about other observables? The problem is that, according to the Kochen-Specker theorem, we cannot assign consistent values to all observables at any *single* time, let alone give transition probabilities for those values. This is an issue in any setting, not just ours. The solution we prefer is to postulate a fixed orthogonal basis of "distinguishable experiences," and to interpret a measurement in any other basis as a unitary followed by a measurement in the fixed basis. As mentioned in Section 1.2, modal interpretations opt for a different solution, which involves sets of bases that change over time with the state itself. It might be interesting to combine the approaches.

Another objection is that the probability of transitioning from basis state $|i\rangle$ at time t_1 to basis state $|j\rangle$ at time t_2 might depend on how finely we divide the time interval between t_1 and t_2. In other words, for some state $|\psi\rangle$ and unitaries V, W, we might have

$$S(|\psi\rangle, WV) \neq S(V|\psi\rangle, W)\, S(|\psi\rangle, V)$$

[1] Put differently, Bohm's conservation of probability result breaks down because the "wavefunctions" at t_1 and t_2 are degenerate, with all amplitude concentrated on finitely many points. But in a discrete Hilbert space, *every* wavefunction is degenerate in this sense!

(a similar point was made by Gillespie [15]). Indeed, this is true for any hidden-variable theory other than the product theory $\mathcal{PT}$. To see this, observe that for all unitaries U and states $|\psi\rangle$, there exist unitaries V, W such that $U = WV$ and $V|\psi\rangle = |1\rangle$. Then applying V destroys all information in the hidden variable (that is, decreases its entropy to 0); so if we then apply W, then the variable's final value must be uncorrelated with the initial value. In other words, $S(V|\psi\rangle, W) S(|\psi\rangle, V)$ must equal $S_{\mathcal{PT}}(|\psi\rangle, U)$. It follows that to any hidden-variable theory we must associate a time scale, or some other rule for deciding when the transitions take place.

In our defense, let us point out that exactly the same problem arises in *continuous*-time stochastic hidden-variable theories. For if a state $|\psi\rangle$ is governed by the Schrödinger equation $d|\psi\rangle/dt = iH_t|\psi\rangle$, and a hidden variable's probability distribution $\overrightarrow{p}$ is governed by the stochastic equation $d\overrightarrow{p}/d\tau = A_\tau \overrightarrow{p}$, then there is still an arbitrary parameter $d\tau/dt$ on which the dynamics depend.

Finally, it will be objected that we have ignored special relativity. In Section 2 we will define a *commutativity axiom*, which informally requires that the stochastic matrix S not depend on the temporal order of spacelike separated events. Unfortunately, we will see that when entangled states are involved, commutativity is irreconcilable with another axiom that seems even more basic. The resulting nonlocality has the same character as the nonlocality of Bohmian mechanics—that is, one cannot use it to send superluminal signals in the usual sense, but it is unsettling nonetheless.

2 Axioms for Hidden-Variable Theories

We now state seven axioms that we would like hidden-variable theories to satisfy.

Symmetry. A theory is symmetric if it is invariant under relabeling of basis states: that is, if for all ρ, U and all permutation matrices Q,

$$Q^{-1} S(\rho, U) Q = S\left(Q^{-1}\rho Q, Q^{-1} U Q\right).$$

All theories discussed in this paper are symmetric.

Indifference. Suppose we partition the basis states into 'blocks,' between which U can never produce interference. Call an ordered pair $\langle I, J\rangle$ of subsets of $\{1,\ldots,N\}$ a *block* if $(U)_{ij} = 0$ for all $i \in I$ and $j \notin J$, as well as all $i \notin I$ and $j \in J$. Also, call $\langle I, J\rangle$ a *minimal block* if $|I| = |J|$ and no $\langle I^*, J^*\rangle$ with $I^* \subset I$ and $J^* \subset J$ is a block. Note that if $\langle I_1, J_1\rangle, \ldots, \langle I_m, J_m\rangle$ are the minimal blocks, then both $\{I_1,\ldots,I_m\}$ and $\{J_1,\ldots,J_m\}$ are partitions of $\{1,\ldots,N\}$. We say a theory is indifferent if it never produces interference between minimal blocks—that is, if $(S)_{ij} = 0$ for all i, j in different minimal blocks. In particular, indifference implies that given any state ρ in a tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$, and any unitary U that acts only on $\mathcal{H}_A$ (that is, is the identity on $\mathcal{H}_B$), the stochastic matrix $S(\rho, U)$ acts only on $\mathcal{H}_A$ as well.

Robustness. A theory is robust if it is insensitive to small errors in a state or unitary (which, in particular, implies continuity). Suppose we obtain $\widetilde{\rho}$ and $\widetilde{U}$ by making small changes to ρ and U respectively. Then for all polynomials p, there should exist a polynomial q such that for all N,

$$\left\| P\left(\widetilde{\rho}, \widetilde{U}\right) - P(\rho, U) \right\| \leq \frac{1}{p(N)}$$

where $\|M\| = \max_{ij} \left|(M)_{ij}\right|$, whenever $\|\widetilde{\rho} - \rho\| \leq 1/q(N)$ and $\left\|\widetilde{U} - U\right\| \leq 1/q(N)$. Robustness has an important advantage for quantum computing: if a hidden-variable theory is robust then the set of gates used to define the unitaries $U_1, \ldots, U_T$ is irrelevant, since by the Solovay-Kitaev

Theorem (see [20]), any universal quantum gate set can simulate any other to a precision ε with $O\left(\log^{c} 1/\varepsilon\right)$ overhead.

Block Robustness. Unfortunately, one of the theories that we wish to study does not satisfy robustness. We therefore define a weaker notion of robustness that this theory satisfies. We say a hidden-variable theory is *block robust* if robustness holds for all modifications $\rho, U \rightarrow \widetilde{\rho}, \widetilde{U}$ such that U and $\widetilde{U}$ have the same set $\langle I_1, J_1\rangle, \ldots, \langle I_m, J_m\rangle$ of minimal blocks.

Commutativity. Let ρ_{AB} be a bipartite state, and let U_A and U_B act only on subsystems A and B respectively. Then commutativity means that the order in which U_A and U_B are applied is irrelevant:

$$S\left(U_A \rho_{AB} U_A^{-1}, U_B\right) S\left(\rho_{AB}, U_A\right) = S\left(U_B \rho_{AB} U_B^{-1}, U_A\right) S\left(\rho_{AB}, U_B\right).$$

Product Commutativity. A theory is product commutative if it satisfies commutativity for all separable pure states $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$.

Decomposition Invariance. A theory is decomposition invariant if

$$S\left(\rho, U\right) = \sum_{i=1}^{N} p_i S\left(\left|\psi_i\right\rangle \left\langle \psi_i\right|, U\right)$$

for every decomposition

$$\rho = \sum_{i=1}^{N} p_i \left|\psi_i\right\rangle \left\langle \psi_i\right|$$

of ρ into pure states. Theorem 2, part (ii) will show that the analogous axiom for $P\left(\rho, U\right)$ is unsatisfiable.

2.1 Comparing Hidden-Variable Theories

To fix ideas, let us compare some hidden-variable theories with respect to the above axioms. We have already seen the product theory $\mathcal{PT}$ in Section 1.1. It is easy to show that $\mathcal{PT}$ satisfies symmetry, robustness, commutativity, and decomposition invariance. However, we consider $\mathcal{PT}$ unsatisfactory because it violates indifference: even if a unitary U acts only on the first of two qubits, $S_{\mathcal{PT}}\left(\rho, U\right)$ will readily produce transitions between (say) $|00\rangle$ and $|01\rangle$, or between $|01\rangle$ and $|10\rangle$.

Recognizing this problem, Dieks [10] proposed an alternative theory that in our terminology corresponds to the following.[2] First find the minimal blocks $\langle I_1, J_1\rangle, \ldots, \langle I_m, J_m\rangle$ of U. Then apply the product theory separately to each minimal block; that is, if i and j belong to the same block $\langle I, J\rangle$ then set

$$\left(S\right)_{ij} = \frac{\left(U\rho U^{-1}\right)_{jj}}{\sum_{\widehat{j}\in J}\left(U\rho U^{-1}\right)_{\widehat{j}\widehat{j}}},$$

and otherwise set $\left(S\right)_{ij} = 0$. The resulting *Dieks theory*, $\mathcal{DT}$, clearly satisfies indifference. However, it does not satisfy robustness (or even continuity), since the set of minimal blocks can change if we replace '0' entries in U by arbitrarily small nonzero entries.

In Section 4 we will introduce two other hidden-variable theories, the flow theory $\mathcal{FT}$ and the Schrödinger theory $\mathcal{ST}$. The following table lists which axioms the four theories satisfy.

[2] Dieks (personal communication) says he would no longer defend this theory.

	$\mathcal{PT}$ (Product)	$\mathcal{DT}$ (Dieks)	$\mathcal{FT}$ (Flow)	$\mathcal{ST}$ (Schrödinger)
Symmetry	Yes	Yes	Yes	Yes
Indifference	No	Yes	Yes	Yes
Robustness	Yes	No	Yes	?
Block Robustness	Yes	Yes	Yes	?
Commutativity	Yes	No	No	No
Product Commutativity	Yes	Yes	No	Yes
Decomposition Invariance	Yes	Yes	No	No

If we could prove that $\mathcal{ST}$ satisfies robustness, then the above table together with the impossibility results of Section 3 would completely characterize which of the axioms can be satisfied simultaneously.

3 Impossibility Results

This section shows that certain sets of axioms cannot be satisfied by any hidden-variable theory. We first show that the failure of $\mathcal{DT}$, $\mathcal{FT}$, and $\mathcal{ST}$ to satisfy commutativity is inherent, and not a fixable technical problem.

Theorem 1 *No hidden-variable theory satisfies both indifference and commutativity.*

Proof. Assume indifference holds, and let our initial state be $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Suppose U_A applies a $\pi/8$ rotation to the first qubit, and U_B applies a $-\pi/8$ rotation to the second qubit. Then

$$U_A|\psi\rangle = U_B|\psi\rangle = \frac{1}{\sqrt{2}}\left(\cos\frac{\pi}{8}|00\rangle - \sin\frac{\pi}{8}|01\rangle + \sin\frac{\pi}{8}|10\rangle + \cos\frac{\pi}{8}|11\rangle\right),$$

$$U_A U_B|\psi\rangle = U_B U_A|\psi\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle + |11\rangle\right).$$

Let v_t be the value of the hidden variable after t unitaries have been applied. Let E be the event that $v_0 = |00\rangle$ initially, and $v_2 = |10\rangle$ at the end. If U_A is applied before U_B, then the unique 'path' from v_0 to v_2 consistent with indifference sets $v_1 = |10\rangle$. So

$$\Pr[E] \leq \Pr[v_1 = |10\rangle] = \frac{1}{2}\sin^2\frac{\pi}{8}.$$

But if U_B is applied before U_A, then the probability that $v_0 = |11\rangle$ and $v_2 = |10\rangle$ is at most $\frac{1}{2}\sin^2\frac{\pi}{8}$, by the same reasoning. Thus, since v_2 must equal $|10\rangle$ with probability $1/4$, and since the only possibilities for v_0 are $|00\rangle$ and $|11\rangle$,

$$\Pr[E] \geq \frac{1}{4} - \frac{1}{2}\sin^2\frac{\pi}{8} > \frac{1}{2}\sin^2\frac{\pi}{8}.$$

We conclude that commutativity is violated. ■

Let us remark on the relationship between Theorem 1 and Bell's Theorem. Any hidden-variable theory that is "local" in Bell's sense would immediately satisfy both indifference and commutativity. However, the converse is not obvious, since there might be nonlocal information in the states $U_A|\psi\rangle$ or $U_B|\psi\rangle$, which an indifferent commutative theory could exploit but a local one could not. Theorem 1 rules out this possibility, and in that sense is a strengthening of Bell's Theorem.

The next result places limits on decomposition invariance.

Theorem 2

(i) No theory satisfies indifference, robustness, and decomposition invariance.

(ii) No theory has the property that

$$P(\rho, U) = \sum_{i=1}^{N} p_i P(|\psi_i\rangle\langle\psi_i|, U)$$

for every decomposition $\sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|$ *of* ρ.

Proof.

(i) Suppose the contrary. Let

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$
$$|\varphi_\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle.$$

Then for every θ not a multiple of $\pi/2$, we must have

$$S(|\varphi_{-\theta}\rangle, R_\theta) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix},$$
$$S\left(\left|\varphi_{\pi/2-\theta}\right\rangle, R_\theta\right) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

So by decomposition invariance, letting $I = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2$ denote the maximally mixed state,

$$S(I, R_\theta) = S\left(\frac{|\varphi_{-\theta}\rangle\langle\varphi_{-\theta}| + \left|\varphi_{\pi/2-\theta}\right\rangle\left\langle\varphi_{\pi/2-\theta}\right|}{2}, R_\theta\right) = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

and therefore

$$P(I, R_\theta) = \begin{bmatrix} \frac{(\rho)_{00}}{2} & \frac{(\rho)_{11}}{2} \\ \frac{(\rho)_{00}}{2} & \frac{(\rho)_{11}}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{bmatrix}.$$

By robustness, this holds for $\theta = 0$ as well. But this is a contradiction, since by indifference $P(I, R_0)$ must be half the identity.

(ii) Reminiscent of Theorem 1. Suppose the contrary; then

$$P\left(I, R_{\pi/8}\right) = \frac{P\left(|0\rangle, R_{\pi/8}\right) + P\left(|1\rangle, R_{\pi/8}\right)}{2}.$$

So considering transitions from $|0\rangle$ to $|1\rangle$,

$$\left(P\left(I, R_{\pi/8}\right)\right)_{01} = \frac{\left(P\left(|0\rangle, R_{\pi/8}\right)\right)_{11} + 0}{2} = \frac{1}{2}\sin^2\frac{\pi}{8}.$$

But

$$P\left(I, R_{\pi/8}\right) = \frac{P\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/8}\right) + P\left(\left|\varphi_{5\pi/8}\right\rangle, R_{\pi/8}\right)}{2}$$

also. Since $R_{\pi/8}\left|\varphi_{\pi/8}\right\rangle = \left|\varphi_{\pi/4}\right\rangle$, we have

$$\begin{aligned}
\left(P\left(I, R_{\pi/8}\right)\right)_{01} &\geq \frac{1}{2}\left(P\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/8}\right)\right)_{01} \\
&\geq \frac{1}{2}\left(\frac{1}{2} - \left(P\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/8}\right)\right)_{11}\right) \\
&\geq \frac{1}{2}\left(\frac{1}{2} - \sin^2\frac{\pi}{8}\right) \\
&> \frac{1}{2}\sin^2\frac{\pi}{8}
\end{aligned}$$

which is a contradiction.

■

Notice that all three conditions in Theorem 2, part (i) were essential—for $\mathcal{PT}$ satisfies robustness and decomposition invariance, $\mathcal{DT}$ satisfies indifference and decomposition invariance, and $\mathcal{FT}$ satisfies indifference and robustness.

Our last impossibility result says that no hidden-variable theory satisfies both indifference and "strong continuity," in the sense that for all $\varepsilon > 0$ there exists $\delta > 0$ such that $\left\|\widetilde{\rho} - \rho\right\| \leq \delta$ implies $\left\|S\left(\widetilde{\rho}, U\right) - S\left(\rho, U\right)\right\| \leq \varepsilon$. To see this, let

$$\begin{aligned}
U &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}, \\
\rho &= \sqrt{1-2\delta^2}\left|0\right\rangle + \delta\left|1\right\rangle + \delta\left|2\right\rangle, \\
\widetilde{\rho} &= \sqrt{1-2\delta^2}\left|0\right\rangle + \delta\left|1\right\rangle - \delta\left|2\right\rangle.
\end{aligned}$$

Then by indifference,

$$S\left(\rho, U\right) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \qquad S\left(\widetilde{\rho}, U\right) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

This is the reason why we defined robustness in terms of the joint probabilities matrix P rather than the stochastic matrix S. On the other hand, note that by giving up indifference, we *can* satisfy strong continuity, as is shown by $\mathcal{FT}$.

4 Specific Theories

This section presents the main results of the paper, which concern two nontrivial examples of hidden-variable theories: the flow theory in Section 4.1, and the Schrödinger theory in Section 4.2.

4.1 Flow Theory

The idea of the flow theory is to convert a unitary matrix into a weighted directed graph, and then route probability mass through that graph like oil through pipes. Given a unitary U, let

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_N \end{bmatrix} = \begin{bmatrix} (U)_{11} & \cdots & (U)_{N1} \\ \vdots & & \vdots \\ (U)_{1N} & \cdots & (U)_{NN} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix},$$

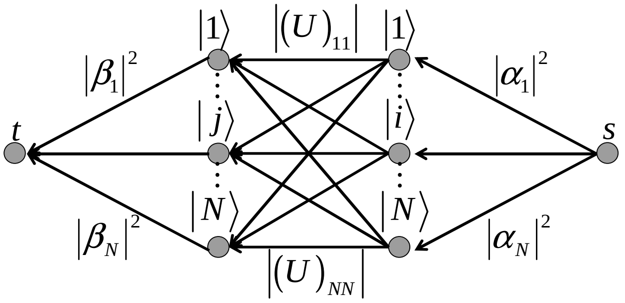

Figure 1: A network (weighted directed graph with source and sink) corresponding to the unitary U and state $|\psi\rangle$

where for the time being

$$|\psi\rangle = \alpha_1 |1\rangle + \cdots + \alpha_N |N\rangle,$$
$$U|\psi\rangle = \beta_1 |1\rangle + \cdots + \beta_N |N\rangle$$

are pure states. Then consider the network G shown in Figure 1. We have a source vertex s, a sink vertex t, and N input and N output vertices labeled by basis states $|1\rangle, \ldots, |N\rangle$. Each edge of the form $(s, |i\rangle)$ has capacity $|\alpha_i|^2$, each edge $(|i\rangle, |j\rangle)$ has capacity $\left|(U)_{ij}\right|$, and each edge $(|j\rangle, t)$ has capacity $|\beta_j|^2$. A natural question is how much probability mass can flow from s to t without violating the capacity constraints. Rather surprisingly, we show that one unit of mass (that is, all of it) can. Interestingly, this result would be false if edge $(|i\rangle, |j\rangle)$ had capacity $\left|(U)_{ij}\right|^2$ (or even $\left|(U)_{ij}\right|^{1+\varepsilon}$) instead of $\left|(U)_{ij}\right|$. We also show that there exists a mapping from networks to maximum flows in those networks, that is *robust* in the sense that a small change in edge capacities produces only a small change in the amount of flow through any edge.

The proofs of these theorems use classical results from the theory of network flows (see [7] for an introduction). In particular, let a *cut* be a set of edges that separates s from t; the *value* of a cut is the sum of the capacities of its edges. Then a fundamental result called the *Max-Flow-Min-Cut Theorem* [11] says that the maximum possible amount of flow from s to t equals the minimum value of any cut.

Theorem 3 *One unit of flow can be routed from s to t in G.*

Proof. By the above, it suffices to show that any cut C in G has value at least 1. Let A be the set of $i \in \{1, \ldots, N\}$ such that $(s, |i\rangle) \notin C$, and let B be the set of j such that $(|j\rangle, t) \notin C$. Then C must contain every edge $(|i\rangle, |j\rangle)$ such that $i \in A$ and $j \in B$, and we can assume without loss of generality that C contains no other edges. So the value of C is

$$\sum_{i \notin A} |\alpha_i|^2 + \sum_{j \notin B} |\beta_j|^2 + \sum_{i \in A,\ j \in B} \left|(U)_{ij}\right|.$$

Therefore we need to prove the matrix inequality

$$\left(1 - \sum_{i \in A} |\alpha_i|^2\right) + \left(1 - \sum_{j \in B} |\beta_j|^2\right) + \sum_{i \in A,\ j \in B} \left|(U)_{ij}\right| \geq 1,$$

or

$$1 + \sum_{i\in A,\ j\in B} \left|(U)_{ij}\right| \geq \sum_{i\in A} |\alpha_i|^2 + \sum_{j\in B} |\beta_j|^2 .$$

Let U be fixed, and consider the maximum of the right-hand side over all $|\psi\rangle$. Since

$$\beta_j = \sum_i (U)_{ij} \alpha_i,$$

this maximum is equal to the largest eigenvalue λ of the positive semidefinite matrix

$$\sum_{i\in A} |i\rangle \langle i| + \sum_{j\in B} |u_j\rangle \langle u_j|$$

where for each j,

$$|u_j\rangle = (U)_{1j} |1\rangle + \cdots + (U)_{Nj} |N\rangle .$$

Let H_A be the subspace of states spanned by $\{|i\rangle : i \in A\}$, and let H_B be the subspace spanned by $\{|u_j\rangle : j \in B\}$. Also, let $L_A(|\psi\rangle)$ be the length of the projection of $|\psi\rangle$ onto H_A, and let $L_B(|\psi\rangle)$ be the length of the projection of $|\psi\rangle$ onto H_B. Then since the $|i\rangle$'s and $|u_j\rangle$'s form orthogonal bases for H_A and H_B respectively, we have

$$\begin{aligned}\lambda &= \max_{|\psi\rangle} \left(\sum_{i\in A} |\langle i|\psi\rangle|^2 + \sum_{j\in B} |\langle u_j|\psi\rangle|^2 \right) \\ &= \max_{|\psi\rangle} \left(L_A(|\psi\rangle)^2 + L_B(|\psi\rangle)^2 \right).\end{aligned}$$

So letting θ be the angle between H_A and H_B,

$$\begin{aligned}\lambda &= 2\cos^2 \frac{\theta}{2} \\ &= 1 + \cos\theta \\ &\leq 1 + \max_{|a\rangle\in H_A,\ |b\rangle\in H_B} |\langle a|b\rangle| \\ &= 1 + \max_{\substack{|\gamma_1|^2+\cdots+|\gamma_N|^2=1 \\ |\delta_1|^2+\cdots+|\delta_N|^2=1}} \left| \left(\sum_{i\in A} \gamma_i \langle i| \right) \left(\sum_{j\in B} \delta_j |u_j\rangle \right) \right| \\ &\leq 1 + \sum_{i\in A,\ j\in B} \left|(U)_{ij}\right|\end{aligned}$$

which completes the theorem. ■

Observe that Theorem 3 still holds if U acts on a mixed state ρ, since we can write ρ as a convex combination of pure states $|\psi\rangle\langle\psi|$, construct a flow for each $|\psi\rangle$ separately, and then take a convex combination of the flows.

Using Theorem 3, we now define the flow theory $\mathcal{FT}$. Let $F(\rho, U)$ be the set of maximum flows for ρ, U—representable by $N \times N$ arrays of real numbers f_{ij} such that $0 \leq f_{ij} \leq \left|(U)_{ij}\right|$ for all i, j, and also

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

Clearly $F(\rho, U)$ is a convex polytope, which Theorem 3 asserts is nonempty. Form a maximum flow $f^*(\rho, U) \in F(\rho, U)$ as follows: first let f_{11}^* be the maximum of f_{11} over all $f \in F(\rho, U)$. Then let f_{12}^* be the maximum of f_{12} over all $f \in F(\rho, U)$ such that $f_{11} = f_{11}^*$. Continue to loop through all i, j pairs in lexicographic order, setting each f_{ij}^* to its maximum possible value consistent with the $(i-1)N + j - 1$ previous values.

We define the joint probabilities matrix P by "symmetrizing" $f^*(\rho, U)$ over permutations of basis states—that is,

$$P(\rho, U) = \frac{1}{N!} \sum_Q Q f^* \left(Q^{-1} \rho Q, Q^{-1} U Q\right) Q^{-1}$$

where Q ranges over all $N \times N$ permutation matrices. As discussed in Section 1.1, given P we can easily obtain the stochastic matrix S by dividing the i^{th} column by $(\rho)_{ii}$, or taking a limit in case $(\rho)_{ii} = 0$. It is easy to check that $\mathcal{FT}$ so defined satisfies the symmetry and indifference axioms.

Showing that $\mathcal{FT}$ satisfies robustness is harder. Our proof is based on the Ford-Fulkerson algorithm [11], a classic algorithm for computing maximum flows that works by finding a sequence of "augmenting paths," each of which increases the flow from s to t by some positive amount.

Theorem 4 *$\mathcal{FT}$ satisfies robustness.*

Proof. Let G be an arbitrary flow network with source s, sink t, and directed edges $e_1, \ldots, e_m$, where each e_i has capacity c_i and leads from v_i to w_i. It will be convenient to introduce a fictitious edge e_0 from t to s with unlimited capacity; then maximizing the flow through G is equivalent to maximizing the flow through e_0. Suppose we produce a new network $\widetilde{G}$ by increasing a single capacity c_{i^*} by some $\varepsilon > 0$. Let f^* be the optimal flow for G, obtained by first maximizing the flow f_0 through e_0, then maximizing the flow f_1 through e_1 holding f_0 fixed, and so on up to f_m. Let $\widetilde{f}^*$ be the maximal flow for $\widetilde{G}$ produced in the same way. We claim that for all $i \in \{0, \ldots, m\}$,

$$\left| \widetilde{f}_i^* - f_i^* \right| \leq \varepsilon.$$

To see that the theorem follows from this claim: first, if f^* is robust under adding ε to c_{i^*}, then it must also be robust under subtracting ε from c_{i^*}. Second, if we change ρ, U to $\widetilde{\rho}, \widetilde{U}$ such that $\|\widetilde{\rho} - \rho\| \leq 1/q(N)$ and $\left\|\widetilde{U} - U\right\| \leq 1/q(N)$, then we can imagine the $N^2 + 2N$ edge capacities are changed one by one, so that

$$\begin{aligned} \left\| f^*\left(\widetilde{\rho}, \widetilde{U}\right) - f^*(\rho, U) \right\| &\leq \sum_{ij} \left| \left| \left(\widetilde{U}\right)_{ij} \right| - \left| (U)_{ij} \right| \right| + \sum_i \left| (\widetilde{\rho})_{ii} - (\rho)_{ii} \right| \\ &\quad + \sum_j \left| \left(\widetilde{U} \widetilde{\rho} \widetilde{U}^{-1} \right)_{jj} - \left(U \rho U^{-1} \right)_{jj} \right| \\ &\leq \frac{4N^2}{q(N)}. \end{aligned}$$

(Here we have made no attempt to optimize the bound.) Third, symmetrizing over all row and column permutations can only decrease $\left\|\widetilde{P} - P\right\|$, not increase it.

We now prove to the claim. To do so we describe an iterative algorithm for computing f^*. First maximize the flow f_0 through e_0, by using the Ford-Fulkerson algorithm [11] to find a maximum flow from s to t. Let $f^{(0)}$ be the resulting flow, and let $G^{(1)}$ be the residual network that corresponds to $f^{(0)}$. For each i, that is, $G^{(1)}$ has an edge $e_i = (v_i, w_i)$ of capacity $c_i^{(1)} = c_i - f_i^{(0)}$, and an edge

$\overline{e}_i = (w_i, v_i)$ of capacity $\overline{c}_i^{(1)} = f_i^{(0)}$. Next maximize f_1 subject to f_0 by using the Ford-Fulkerson algorithm to find "augmenting cycles" from w_1 to v_1 and back to w_1 in $G^{(1)} \setminus \{e_0, \overline{e}_0\}$. Continue in this manner until each of $f_1, \ldots, f_m$ has been maximized subject to the previous f_i's. Finally set $f^* = f^{(m)}$.

Now, one way to compute $\widetilde{f}^*$ is to start with f^*, then repeatedly "correct" it by applying the same iterative algorithm to maximize $\widetilde{f}_0$, then $\widetilde{f}_1$, and so on. Let $\varepsilon_i = \left| \widetilde{f}_i^* - f_i^* \right|$; then we need to show that $\varepsilon_i \leq \varepsilon$ for all $i \in \{0, \ldots, m\}$. The proof is by induction on i. Clearly $\varepsilon_0 \leq \varepsilon$, since increasing c_{i^*} by ε can increase the value of the minimum cut from s to t by at most ε. Likewise, after we maximize $\widetilde{f}_0$, the value of the minimum cut from w_1 to v_1 can increase by at most $\varepsilon - \varepsilon_0 + \varepsilon_0 = \varepsilon$. For of the at most ε new units of flow from w_1 to v_1 that increasing c_{i^*} made available, ε_0 of them were "taken up" in maximizing $\widetilde{f}_0$, but the process of maximizing $\widetilde{f}_0$ could have again increased the minimum cut from w_1 to v_1 by up to ε_0. Continuing in this way,

$$\varepsilon_2 \leq \varepsilon - \varepsilon_0 + \varepsilon_0 - \varepsilon_1 + \varepsilon_1 = \varepsilon,$$

and so on up to ε_m. This completes the proof. ■

That $\mathcal{FT}$ violates decomposition invariance now follows from Theorem 2, part (i). However, it might be helpful to see an explicit counterexample. Let I be the 1-qubit maximally mixed state, and let $R_{\pi/4}$ be a $\pi/4$ rotation. Then $R_{\pi/4} I R_{\pi/4}^{-1} = I$, and

$$S\left(I, R_{\pi/4}\right) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

since the 1/2 unit of flow from $|0\rangle$ all gets routed to $|0\rangle$, and then the 1/2 unit of flow from $|1\rangle$ can only be routed to $|1\rangle$. On the other hand, let $|\varphi_\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$; then $S\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/4}\right)$ and $S\left(\left|\varphi_{5\pi/8}\right\rangle, R_{\pi/4}\right)$ clearly do *not* equal the identity, since $\cos^2(\pi/8)$ units of flow cannot be routed along an edge of capacity only $1/\sqrt{2}$. Therefore

$$S\left(I, R_{\pi/4}\right) \neq \frac{S\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/4}\right) + S\left(\left|\varphi_{5\pi/8}\right\rangle, R_{\pi/4}\right)}{2}.$$

Let us also show that $\mathcal{FT}$ violates product commutativity. Let $|\psi\rangle = \left|\varphi_{\pi/4}\right\rangle \otimes \left|\varphi_{-\pi/8}\right\rangle$ be a 2-qubit initial state, and let $R_{\pi/4}^A$ and $R_{\pi/4}^B$ be $\pi/4$ rotations applied to the first and second qubits respectively. Suppose $R_{\pi/4}^B$ is applied first to change the second qubit from $\left|\varphi_{-\pi/8}\right\rangle$ to $\left|\varphi_{\pi/8}\right\rangle$. Then one can check that $\frac{1}{2}\cos^2\frac{\pi}{8}$ probability mass is routed from $|0\rangle$ to $|0\rangle$, and $\frac{1}{2}\sin^2\frac{\pi}{8}$ from $|1\rangle$ to $|1\rangle$; the $1/\sqrt{2}$ edge capacities never come into play. So $S\left(|\psi\rangle, R_{\pi/4}^B\right)$ is the identity, which implies that

$$S\left(R_{\pi/4}^B|\psi\rangle, R_{\pi/4}^A\right) S\left(|\psi\rangle, R_{\pi/4}^B\right) = S\left(\left|\varphi_{\pi/4}\right\rangle \otimes \left|\varphi_{\pi/8}\right\rangle, R_{\pi/4}^A\right) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

On the other hand, if $R_{\pi/4}^A$ is applied first to change the state to $|1\rangle \otimes \left|\varphi_{-\pi/8}\right\rangle$, then when $R_{\pi/4}^B$ is applied next, at most $1/\sqrt{2}$ of the $\cos^2\frac{\pi}{8}$ probability mass at $|10\rangle$ can be routed to $|10\rangle$; the rest must go to $|11\rangle$. It follows that

$$S\left(R_{\pi/4}^A|\psi\rangle, R_{\pi/4}^B\right) S\left(|\psi\rangle, R_{\pi/4}^A\right) \neq S\left(R_{\pi/4}^B|\psi\rangle, R_{\pi/4}^A\right) S\left(|\psi\rangle, R_{\pi/4}^B\right).$$

4.2 Schrödinger Theory

Our final hidden-variable theory, which we call the *Schrödinger theory* or $\mathcal{ST}$, is the most interesting one mathematically. The idea—to make a matrix into a stochastic matrix via an iterative process of row and column rescaling—is natural enough that we came upon it independently, only later learning that it originated in a 1931 paper of Schrödinger [22]. Schrödinger gave a pair of functional integral equations that such an iterative process would solve, but was unable to prove that those equations always have a solution. The existence and uniqueness of a solution were shown under broad conditions by Nagasawa [18], building on earlier work of Fortet [12] and Beurling [4]. Our goal is to give what (to our knowledge) is the first self-contained, reasonably accessible presentation of the main result in this area; and to interpret that result in what we think is the correct way: as providing one example of a hidden-variable theory, whose strengths and weaknesses should be directly compared to those of other theories.

Most of the technical difficulties in [4, 12, 18, 22] arise because the stochastic process being constructed involves continuous time and particle positions. Here we eliminate those difficulties by restricting attention to discrete time and to finite-dimensional Hilbert spaces. We thereby obtain a generalized version[3] of a problem that computer scientists know as *(r,c)-scaling of matrices.* Sinkhorn [23] gave an algorithm for the (r,c)-scaling problem, which was shown to run in polynomial time by Franklin and Lorenz [13] (see also Linial, Samorodnitsky, and Wigderson [17]).

As in the case of the flow theory, given a unitary U acting on a state ρ, the first step is to replace each entry of U by its absolute value, obtaining the nonnegative matrix $U^{(0)}$ defined by $\left(U^{(0)}\right)_{ij} := \left|(U)_{ij}\right|$. We then repeatedly tweak $U^{(0)}$ to bring it closer to a joint probabilities matrix $P(\rho,U)$. We want 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 $S(\rho,U)$ is then readily obtained by normalizing each column to sum to 1.

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 $\left(U\rho U^{-1}\right)_{jj}$. More formally,

$$\begin{aligned}\left(U^{(2t+1)}\right)_{ij} &= \frac{(\rho)_{ii}}{\sum_k \left(U^{(2t)}\right)_{ik}} \left(U^{(2t)}\right)_{ij}, \\ \left(U^{(2t+2)}\right)_{ij} &= \frac{\left(U\rho U^{-1}\right)_{jj}}{\sum_k \left(U^{(2t+1)}\right)_{kj}} \left(U^{(2t+1)}\right)_{ij}.\end{aligned}$$

The crucial fact is that the above iteration converges. Our proof will reuse a result about network flows from Section 4.1, in order to define a nondecreasing "progress measure" based on Kullback-Leibler distance.

Theorem 5 *The limit $U^{(\infty)} = \lim_{t\rightarrow\infty} U^{(t)}$ exists.*

Proof. A consequence of Theorem 3 is that for every ρ, U, there exists an $N \times N$ array of nonnegative real numbers f_{ij} such that

(1) $f_{ij} = 0$ whenever $\left|(U)_{ij}\right| = 0$,

[3] In (r,c)-scaling, we are given an invertible real matrix, and the goal is to rescale all rows and columns to sum to 1. The generalized version is to rescale the rows and columns to given values (not necessarily 1).

(2) $f_{i1} + \cdots + f_{iN} = (\rho)_{ii}$ for all i, and

(3) $f_{1j} + \cdots + f_{Nj} = \left(U \rho U^{-1}\right)_{jj}$ for all j.

Given any such array, define a progress measure

$$Z^{(t)} = \prod_{ij} \left(U^{(t)}\right)_{ij}^{f_{ij}},$$

where we adopt the convention $0^0 = 1$. We claim that $Z^{(t+1)} \geq Z^{(t)}$ for all $t \geq 1$. To see this, assume without loss of generality that we are on an odd step $2t+1$, and let $C_i^{(2t)} = \sum_j \left(U^{(2t)}\right)_{ij}$ be the i^{th} column sum before we normalize it. Then

$$\begin{aligned} Z^{(2t+1)} &= \prod_{ij} \left(U^{(2t+1)}\right)_{ij}^{f_{ij}} \\ &= \prod_{ij} \left(\frac{(\rho)_{ii}}{C_i^{(2t)}} \left(U^{(2t)}\right)_{ij} \right)^{f_{ij}} \\ &= \left(\prod_{ij} \left(U^{(2t)}\right)_{ij}^{f_{ij}} \right) \left(\prod_i \left(\frac{(\rho)_{ii}}{C_i^{(2t)}} \right)^{f_{i1} + \cdots + f_{iN}} \right) \\ &= Z^{(2t)} \cdot \prod_i \left(\frac{(\rho)_{ii}}{C_i^{(2t)}} \right)^{(\rho)_{ii}}. \end{aligned}$$

As a result of the $2t^{th}$ normalization step, we had $\sum_i C_i^{(2t)} = 1$. Subject to that constraint, the maximum of

$$\prod_i \left(C_i^{(2t)}\right)^{(\rho)_{ii}}$$

over the $C_i^{(2t)}$'s occurs when $C_i^{(2t)} = (\rho)_{ii}$ for all i—a simple calculus fact that follows from the nonnegativity of Kullback-Leibler distance. This implies that $Z^{(2t+1)} \geq Z^{(2t)}$. Similarly, normalizing rows leads to $Z^{(2t+2)} \geq Z^{(2t+1)}$.

It follows that the limit $U^{(\infty)} = \lim_{t \to \infty} U^{(t)}$ exists. For suppose not; then some $C_i^{(t)}$ is bounded away from $(\rho)_{ii}$, so there exists an $\varepsilon > 0$ such that $Z^{(t+1)} \geq (1+\varepsilon) Z^{(t)}$ for all even t. But this is a contradiction, since $Z^{(0)} > 0$ and $Z^{(t)} \leq 1$ for all t. ■

It is immediate that $\mathcal{ST}$ satisfies symmetry and indifference. Let us show that it satisfies product commutativity as well.

Proposition 6 *$\mathcal{ST}$ satisfies product commutativity.*

Proof. Given a state $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, let $U_A \otimes I$ act only on $|\psi_A\rangle$ and let $I \otimes U_B$ act only on $|\psi_B\rangle$. Then we claim that

$$S\left(|\psi\rangle, U_A \otimes I\right) = S\left(|\psi_A\rangle, U_A\right) \otimes I.$$

The reason is simply that multiplying all amplitudes in $|\psi_A\rangle$ and $U_A |\psi_A\rangle$ by a constant factor α_x, as we do for each basis state $|x\rangle$ of $|\psi_B\rangle$, has no effect on the scaling procedure that produces $S\left(|\psi_A\rangle, U_A\right)$. Similarly

$$S\left(|\psi\rangle, I \otimes U_B\right) = I \otimes S\left(|\psi_B\rangle, U_B\right).$$

It follows that

$$\begin{aligned} S\left(\left|\psi_A\right\rangle, U_A\right) \otimes S\left(\left|\psi_B\right\rangle, U_B\right) &= S\left(U_A\left|\psi_A\right\rangle \otimes \left|\psi_B\right\rangle, I \otimes U_B\right) S\left(\left|\psi\right\rangle, U_A \otimes I\right) \\ &= S\left(\left|\psi_A\right\rangle \otimes U_B\left|\psi_B\right\rangle, U_A \otimes I\right) S\left(\left|\psi\right\rangle, I \otimes U_B\right). \end{aligned}$$

■

On the other hand, let us show that $\mathcal{ST}$ violates decomposition invariance. Using the same notation as in Section 4.1, we have $R_{\pi/8} I R_{\pi/8}^{-1} = I$, $R_{\pi/8}\left|\varphi_{\pi/8}\right\rangle = \left|\varphi_{\pi/4}\right\rangle$, and $R_{\pi/8}\left|\varphi_{5\pi/8}\right\rangle = \left|\varphi_{3\pi/4}\right\rangle$, from which it can be calculated that

$$\begin{aligned} S\left(I, R_{\pi/8}\right) &\approx \left[\begin{array}{cc} 0.707 & 0.293 \\ 0.293 & 0.707 \end{array}\right], \\ S\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/8}\right) &\approx \left[\begin{array}{cc} 0.555 & 0.177 \\ 0.445 & 0.823 \end{array}\right], \\ S\left(\left|\varphi_{5\pi/8}\right\rangle, R_{\pi/8}\right) &\approx \left[\begin{array}{cc} 0.177 & 0.555 \\ 0.823 & 0.445 \end{array}\right]. \end{aligned}$$

Hence

$$S\left(I, R_{\pi/8}\right) \neq \frac{S\left(\left|\varphi_{\pi/8}\right\rangle, R_{\pi/8}\right) + S\left(\left|\varphi_{5\pi/8}\right\rangle, R_{\pi/8}\right)}{2}.$$

5 Discussion

The idea that certain observables in quantum mechanics might have trajectories governed by dynamical laws has reappeared many times: in Schrödinger's 1931 stochastic approach [22], Bohmian mechanics [5], modal interpretations [2, 8, 10], and elsewhere. Yet because all of these proposals yield the same predictions for single-time probabilities, if we are to decide between them it must be on the basis of internal mathematical considerations. A main message of this paper has been that such considerations can actually get us quite far.

To focus attention on the core issues, we restricted attention to the simplest possible setting: discrete time, a finite-dimensional Hilbert space, and a single orthogonal basis. Within this setting, we proposed what seem like reasonable axioms that any hidden-variable theory should satisfy: for example, symmetry under permutation of basis states, robustness to small perturbations, and independence of the temporal order of spacelike-separated events. We then showed that not all of these axioms can be satisfied simultaneously. But perhaps more surprisingly, we also showed that certain subsets of axioms *can* be satisfied for highly nontrivial reasons. In showing that the indifference and robustness axioms can be simultaneously satisfied, Section 4 revealed an unexpected connection between unitary matrices and the classical theory of network flows.

As mentioned previously, the most important open problem is to show that the Schrödinger theory satisfies robustness. Currently, we can only show that the matrix $P_{\mathcal{ST}}(\rho, U)$ is robust to *exponentially* small perturbations, not polynomially small ones. The problem is that if any row or column sum in the $U^{(t)}$ matrix is extremely small, then the (r, c)-scaling process will magnify tiny errors in the entries. Intuitively, though, this effect should be washed out by later scaling steps.

A second open problem is whether there exists a theory that satisfies indifference, as well as commutativity for all separable *mixed* states (not just separable pure states). A third problem is to investigate other notions of robustness—for example, robustness to small *multiplicative* rather than additive errors.

6 Acknowledgments

I thank Umesh Vazirani, Ronald de Wolf, and an anonymous reviewer for comments on an earlier version of this paper; Dorit Aharonov, Guido Bacciagaluppi, John Preskill, and Avi Wigderson for helpful discussions; and Dennis Dieks for correspondence.

References

[1] S. Aaronson (2004), Quantum computing and hidden variables II: the complexity of sampling histories, to appear.

[2] G. Bacciagaluppi and M. Dickson (1999), Dynamics for modal interpretations of quantum theory, *Found. Phys.* 29, pp. 1165–1201. quant-ph/9711048.

[3] J. S. Bell (1987), *Speakable and Unspeakable in Quantum Mechanics*, Cambridge.

[4] A. Beurling (1960), An automorphism of product measures, *Ann. Math.* 72, pp. 189–200.

[5] D. Bohm (1952), A suggested interpretation of the quantum theory in terms of "hidden" variables, *Phys. Rev.* 85, pp. 166–179 (I) and 180–193 (II).

[6] D. Bohm and B. Hiley (1993), *The Undivided Universe: An Ontological Interpretation of Quantum Theory*, Routledge.

[7] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein (2001), *Introduction to Algorithms* (2nd edition), MIT Press.

[8] M. Dickson (2002), Modal interpretations of quantum mechanics, *Stanford Encyclopedia of Philosophy.* http://plato.stanford.edu/entries/qm-modal/.

[9] M. Dickson and R. Clifton (1998), Lorentz-invariance in modal interpretations, in *The Modal Interpretation of Quantum Mechanics*, D. Dieks and P. E. Vermaas (eds), Kluwer, pp. 9–47.

[10] D. Dieks (1994), Modal interpretation of quantum mechanics, measurements, and macroscopic behaviour, *Phys. Rev. A* 49:2290–2300.

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

[12] R. Fortet (1940), Résolution d'un système d'équations de M. Schrödinger, *J. Math Pures et. Appl.* 9, pp. 83–105.

[13] J. Franklin and J. Lorenz (1989), On the scaling of multidimensional matrices, *Linear Algebra Appl.* 114/115, pp. 717–735.

[14] M. Gell-Mann and J. Hartle (1990), Quantum mechanics in the light of quantum cosmology, in *Complexity, Entropy, and the Physics of Information* (W. H. Zurek, ed.), Addison-Wesley.

[15] D. T. Gillespie (1994), Why quantum mechanics cannot be formulated as a Markov process, *Phys. Rev. A* 49:1607.

[16] R. B. Griffiths (1998), Choice of consistent family, and quantum incompatibility, *Phys. Rev. A* 57:1604. quant-ph/9708028.

[17] N. Linial, A. Samorodnitsky, and A. Wigderson (2000), A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents, *Combinatorica* 20(4), pp. 545–568.

[18] M. Nagasawa (1989), Transformations of diffusions and Schrödinger processes, *Prob. Theory and Related Fields* 82, pp. 109–136.

[19] E. Nelson (1985), *Quantum Fluctuations*, Princeton.

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

[21] C. Rovelli and L. Smolin (1995), Discrete of area and volume in loop quantum gravity, *Nucl. Phys.* B442 593. gr-qc/9411005.

[22] E. Schrödinger (1931), Über die umkehrung der naturgesetze, *Sitzungsber. Preuss. Akad. Wissen. Phys. Math. Kl.*, pp. 144–153.

[23] R. Sinkhorn (1964), A relationship between arbitrary positive matrices and doubly stochastic matrices, *Ann. Math. Statist.* 35, pp. 876–879.