2006

Conditional Density Operators and the Subjectivity of Quantum Operations

Matthew S. Leifer
Chapman University, leifer@chapman.edu

Recommended Citation

Leifer, M.S., 2006. Conditional Density Operators and the Subjectivity of Quantum Operations. *AIP Conference Proceedings*, 889, 172—186. doi:10.1063/1.2713456

Conditional Density Operators and the Subjectivity of Quantum Operations

Comments

This is an author-prepared, prepublication version of a paper that was presented at Foundations of Probability and Physics 4 in 2006 and was later published in *AIP Conference Proceedings*, vol. 889, edited by G. Adenier, C. A. Fuchs and A. Yu. Khrennikov, pp. 172—186 (2007). DOI: 10.1063/1.2713456

Conditional Density Operators and the Subjectivity of Quantum Operations

M. S. Leifer[1,2]

[1]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada, N2L 2Y5*
[2]*Centre for Quantum Computing, Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, UK*

Abstract. Assuming that quantum states, including pure states, represent subjective degrees of belief rather than objective properties of systems, the question of what other elements of the quantum formalism must also be taken as subjective is addressed. In particular, we ask this of the dynamical aspects of the formalism, such as Hamiltonians and unitary operators. Whilst some operations, such as the update maps corresponding to a complete projective measurement, must be subjective, the situation is not so clear in other cases. Here, it is argued that all trace preserving completely positive maps, including unitary operators, should be regarded as subjective, in the same sense as a classical conditional probability distribution. The argument is based on a reworking of the Choi-Jamiołkowski isomorphism in terms of "conditional" density operators and trace preserving completely positive maps, which mimics the relationship between conditional probabilities and stochastic maps in classical probability.

Keywords: Jamiołkowski isomorphism, subjective probability, quantum conditional probability
PACS: 03.65.Ta

1. INTRODUCTION

In recent years, Caves, Fuchs and Shack (CFS) have argued that all quantum states, including pure states, should be taken to represent subjective degrees of belief rather than objective properties of systems [6, 4, 15, 18, 5], in close analogy to the radical probabilist view of classical probabilities [26, 12]. The purpose of this article is not to debate the merits of this view, which have been extensively discussed elsewhere [23, 24, 17, 16, 19], but rather to investigate its consequences for the rest of the quantum formalism. In particular, we address the question of whether quantum dynamics, variously expressed as Hamiltonians, unitary operators and Trace Preserving Completely Positive (TPCP) maps, should also be taken to represent subjective degrees of belief. We argue that this is the case for *all* TPCP maps, in the same sense that all conditional probabilities are subjective in the radical probabilist view of classical probability.

CFS have already argued that *some* CP maps must be taken as subjective [5]. For example, consider a non-destructive measurement in an orthonormal basis. In the orthodox approach to quantum theory, on obtaining an outcome corresponding to a pure state $|\psi\rangle$, the state of the system is updated to $|\psi\rangle$, regardless of the initial state of the system. However, for CFS there can never be a situation in which two agents are compelled to assign the same state to a system, even if they have access to exactly the same data. As in radical probabilism, provided the two agents start with distinct enough prior beliefs, they need never converge on a common set of beliefs, regardless of how much data they share[1]. Thus, the projector $|\psi\rangle\langle\psi|$ corresponding to the measurement outcome must be subjective, depending as it does on an analysis of the workings of the measurement device, and this analysis may differ for the two agents. There are also clearly situations in which the subjectivity of quantum states can infect quantum operations. For example, suppose that two agents both agree on the unitary evolution that applies to a joint system composed of a system of interest and its environment. They will generally use different dynamical maps to describe the evolution of the system of interest alone, by virtue of the fact that that they may assign different initial states to the environment.

The situation is less clear when considering a unitary operation on the system of interest alone, since in this case the environmental state is irrelevant to the action of the operation on the system, and unitary operations do not cause convergence of distinct states. Thus, unlike the previously discussed cases, the subjectivity of unitary operations cannot

[1] Of course, in practical situations it is often reasonable to assume that the agents don't hold such singular beliefs, and then their views can be expected to converge. Nevertheless, as a point of principle, incompatible beliefs are not labeled as irrational *a priori*.

be argued directly from the subjectivity of quantum states. Therefore, it would not be inconsistent for CFS to hold onto the objectivity of unitary operations, which might be tempting, since the specification of a Hamiltonian seems to encode the objective content of our most successful physical laws. However, Fuchs has rejected this road, and argues that all TPCP maps, including unitary operations, are analogous to conditional probabilities and so they should be taken to represent subjective degrees of belief [15, 18, 16]. This view could also be seen as implicit in the de Finetti theorem for quantum operations [21, 20], which does not single out unitary operations for any special treatment.

Here, we significantly strengthen the case for the subjectivity of all TPCP maps by demonstrating a thoroughgoing analogy between TPCP maps and conditional probabilities, of the type needed to make Fuchs' arguments compelling to adherents of the CFS view. In fact, we argue for a reconsideration of the domain of applicability of bipartite quantum states themselves. Instead of assuming that they are always descriptions of a pair of distinct systems, we argue that they can also be used to describe the same system at two distinct instances of time in a "prepare and measure" scenario. That this can be done in special cases has been known for quite a while in the context of quantum cryptography [3], where prepare and measure schemes are regularly traded for entanglement based schemes in proofs of the security of quantum key distribution [34], and this correspondence is generalized here. There does not seem to be any substantive difference in the role played by the bipartite state in the two scenarios, so we argue that if the state is taken to be subjective in one context, then it should also be subjective in the other. From this, the subjectivity of all quantum operations may be inferred. No doubt, this conclusion will seem unappealing to many hard-nosed physicists. If unitary operations cannot be taken as objective then neither can Hamiltonians, and it seems that we may be in danger of losing the objectivity of physical laws altogether. I argue that this fear is unfounded and rests on the same sort of category error as the identification of certainty with a subjective probability equal to one [5].

From a broader perspective, this work suggests that it may be possible to cleanly separate the probabilistic and statistical parts of the quantum formalism from those that depend on its particular physical realization. Despite the fact that the abstract formalism of quantum theory looks like a noncommutative generalization of classical probability, it still does not quite achieve a full separation, because it is necessary to know whether two events refer to distinct physical systems or to the same system at two different times in order to know how to combine them, i.e. whether to use the tensor product or a dynamical map. In this respect, quantum theory is in closer analogy to the theory of stochastic process [13] than it is to abstract Kolmogorov probability theory [27], since the latter is independent of any identification of events in an abstract sample space with physical events in spacetime. We believe that a more Kolmogorovian formulation of quantum theory would offer new insights into quantum information protocols, as well as clarifying foundational issues, and regard the current work as a step towards such a formalism.

The remainder of this paper is structured as follows. In section 2 the finite dimensional C^*-algebraic formalism of quantum theory is briefly reviewed. In section 3, the "conditional density operator" is introduced, which is the main tool for relating bipartite quantum states to TPCP maps. In section 4, the Choi-Jamiołkowski isomorphism is discussed. Whilst this is well-known, we give a novel presentation in which the isomorphism is taken to relate *conditional* density operators to TPCP maps, rather than relating unnormalized bipartite states to general CP maps as in usual presentations [25, 10, 36, 1, 37, 22]. Section 4.1 gives the traditional operational interpretation of the isomorphism in terns of noisy gate teleportation and section 4.2 gives a different operational interpretation by which the analogy to the role of conditional probability in classical stochastic processes is made clear. In section 5, the argument for the subjectivity of quantum operations is given and in §6, we argue that the subjectivity of quantum operations does not imply the subjectivity of physical laws. Finally, section 7 contains a summary and conclusions.

The technical results presented here generalize those of previously published work [29] from the finite dimensional Hilbert space formalism to finite dimensional C^* algebras. The current treatment places greater emphasis on the role of the conditional density operator, which we hope clarifies the physical interpretation given in [29].

2. PRELIMINARIES

For present purposes it is convenient to work in the C^*-algebraic formalism for quantum theory. This facilitates the comparison between classical probability and quantum theory, since the former is obtained whenever the algebra is commutative. Because we are concerned mainly with conceptual matters, it is convenient to specialize to finite dimensional algebras in order to avoid analytical complications. Any such algebra can be thought of as the algebra of block-diagonal matrices on a finite dimensional Hilbert space, once a basis for the latter is fixed. Hence, the most general algebra we are concerned with is

$$\mathfrak{A} = \mathfrak{B}(\mathbb{C}^{d_1}) \oplus \mathfrak{B}(\mathbb{C}^{d_2}) \oplus \ldots \oplus \mathfrak{B}(\mathbb{C}^{d_n}), \tag{1}$$

where $\mathfrak{B}(\mathscr{H})$ is the algebra of bounded operators on a Hilbert space $\mathscr{H}$.

Two important special cases are the classical commutative algebras, $\mathfrak{B}(\mathbb{C})^{\oplus n}$, which are diagonal, and the irreducible "full quantum" algebras, $\mathfrak{B}(\mathbb{C}^d)$. States on an algebra are usually defined as positive linear functionals $\omega : \mathfrak{A} \to \mathbb{C}$ that satisfy $\omega(I) = 1$, where I is the identity operator in $\mathfrak{A}$. In the finite dimensional case, these can be replaced by density matrices $\rho \in \mathfrak{A}$ that are positive and have unit trace via the identification $\omega(A) = \mathrm{Tr}(A\rho)$ for all $A \in \mathfrak{A}$. Given two independent subsystems corresponding to algebras $\mathfrak{A}_A$ and $\mathfrak{A}_B$, the combined system corresponds to the tensor product $\mathfrak{A}_A \otimes \mathfrak{A}_B$, which coincides with a Cartesian product of sample spaces in the case where both algebras are classical, and the usual tensor product of Hilbert spaces when both algebras are irreducible. Given a state on the tensor product $\rho_{AB} \in \mathfrak{A}_A \otimes \mathfrak{A}_B$, the reduced states $\rho_A \in \mathfrak{A}_A$ and $\rho_B \in \mathfrak{A}_B$ are given by $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B = \mathrm{Tr}_A(\rho_{AB})$.

The most general dynamics of a system is given by a linear map $\mathscr{E}_{B|A} : \mathfrak{A}_A \to \mathfrak{A}_B$, where the input and output systems are generally allowed to be different. Here, this is taken to be a map acting on density operators, i.e. we are working in a Schrödinger picture, which is unproblematic in finite dimensions. The map should be *Completely Positive* (CP), meaning that $\mathscr{E}_{B|A} \otimes \mathscr{I}_C : \mathfrak{A}_A \otimes \mathfrak{A}_C \to \mathfrak{A}_B \otimes \mathfrak{A}_C$ is a positive map for all finite dimensional algebras $\mathfrak{A}_C$, and where $\mathscr{I}_C : \mathfrak{A}_C \to \mathfrak{A}_C$ is the identity map on $\mathfrak{A}_C$. Furthermore, if no measurements are performed then the map should be *Trace Preserving* (TP) in order to maintain the normalization of density operators.

3. CONDITIONAL DENSITY OPERATOR

In classical probability, the conditional probability of an event Y, given an event X is defined as

$$P(Y|X) = \frac{P(X \cap Y)}{P(X)}, \tag{2}$$

wherever $P(X) \neq 0$ and is undefined otherwise. Defining an analog of this for general C^*-algebraic theories is a tricky problem, and there are several alternative possibilities. Here, we only deal with a special case, which is however the most important for practical applications. Consider a tensor product of two classical algebras $\mathfrak{A}_A \otimes \mathfrak{A}_B$ with corresponding bases $\{|j\rangle_A\}, \{|k\rangle_B\}$ in which the operators are diagonal. A state ρ_{AB} on this algebra can be written in terms of its diagonal components $(\rho_{AB})_{jk,jk}$ as

$$\rho_{AB} = \sum_{jk} (\rho_{AB})_{jk,jk} \, |j\rangle \langle j|_A \otimes |k\rangle \langle k|_B \,, \tag{3}$$

and the reduced state on system A is given by $\rho_A = \mathrm{Tr}_B(\rho_{AB})$, with diagonal components $(\rho_A)_{jj} = \sum_k (\rho_{AB})_{jk,jk}$. Now, the conditional probability that system B is in state $|k\rangle_B$, given that system A is in state $|j\rangle_A$ is given by $\frac{(\rho_{AB})_{jk,jk}}{(\rho_A)_{j,j}}$, provided $(\rho_A)_{j,j}$ is nonzero. This can be written as a matrix of conditional probabilities, given by

$$(\rho_{B|A})_{jk,jk} = \frac{(\rho_{AB})_{jk,jk}}{(\rho_A)_{j,j}}, \tag{4}$$

or in operator notation

$$\rho_{B|A} = \left(\rho_A^{-1} \otimes I_B\right) \rho_{AB}, \tag{5}$$

where I_B is the identity operator in $\mathfrak{A}_B$. Here, care must be taken when ρ_A is not of full rank, in which case we may restrict the domain of $\rho_{B|A}$ to the support of $\rho_A^{-1} \otimes I_B$. An alternative is to define the generalized inverse of ρ_A to have the same eigenspaces as ρ_A, with eigenvalue zero on the null eigenspace of ρ_A and reciprocal eigenvalues on all other eigenspaces. This is the approach we adopt throughout.

In the general noncommutative case, it should be clear that eq. (5) can be generalized in many different ways, due to the fact that $\rho_A^{-1} \otimes I_B$ and ρ_{AB} need not commute. In doing so, one should bear in mind the various possible applications of conditional probability (e.g. the updating of probabilities by Bayesian conditionalization, in stochastic processes, and in information theory) and check that the chosen generalization is useful for describing sensible quantum analogs of at least some of these. The alternative, to focus on formal mathematical properties of conditional probability, may also be a useful approach, but is unlikely to lead to applicable concepts on its own. In this regard, the following generalization suggests itself as particularly interesting[2]:

$$\rho_{B|A} = \left(\rho_A^{-\frac{1}{2}} \otimes I_B\right) \rho_{AB} \left(\rho_A^{-\frac{1}{2}} \otimes I_B\right). \tag{6}$$

This equation may be inverted to obtain

$$\rho_{AB} = \left(\rho_A^{\frac{1}{2}} \otimes I_B\right) \rho_{B|A} \left(\rho_A^{\frac{1}{2}} \otimes I_B\right). \tag{7}$$

Note that $\rho_{B|A}$ is a positive operator, since it is of the form $A^\dagger A$ for $A = \rho_A^{-\frac{1}{2}} \otimes I_B \rho_{AB}^{\frac{1}{2}}$, but is not a density operator because it does not have unit trace. In fact, $\mathrm{Tr}_B\left(\rho_{B|A}\right) = I_{\mathrm{supp}(\rho_A)}$, where $I_{\mathrm{supp}(\rho_A)}$ is the projector onto the support of ρ_A, so the trace of $\rho_{B|A}$ is the rank of ρ_A. In the classical case, this corresponds to the fact that the matrix of conditional probabilities $(\rho_{B|A})_{jk,jk}$ must give a valid probability distribution for each value of j, i.e. $\sum_k (\rho_{B|A})_{jk,jk} = 1$.

In line with the earlier warning, it should be checked that this definition of a quantum conditional density operator actually plays a role in applications. In §4.2, it is shown that the relation between conditional density operators and TPCP maps is analogous to the relation between conditional probabilities and stochastic matrices in a classical stochastic process. The conditional density operator is also related to Fuchs' proposal for a quantum analog of Bayesian conditionalization [15, 18], and the analog of Bayes' rule, $\rho_{B|A} = \rho_A^{-\frac{1}{2}} \otimes \rho_B^{\frac{1}{2}} \rho_{A|B} \rho_A^{-\frac{1}{2}} \otimes \rho_B^{\frac{1}{2}}$, is relevant to the problem of pooling quantum states, both of which are described in forthcoming work [30].

4. THE CHOI-JAMIOŁKOWSKI ISOMORPHISM

The central tool used in the arguments below is the isomorphism discovered by Jamiołkowski [25], and developed by Choi [10], between Completely Positive maps $\mathfrak{A}_A \to \mathfrak{A}_B$ and (generally unnormalized) states in $\mathfrak{A}_A \otimes \mathfrak{A}_B$[3]. For present purposes, it is convenient to formulate it as an isomorphism between *Trace-Preserving* Completely Positive maps $\mathfrak{A}_A \to \mathfrak{A}_B$ and *conditional* density operators in $\mathfrak{A}_A \otimes \mathfrak{A}_B$. This formulation gives greater intuition about the physical meaning of the isomorphism, as shown in §4.2.

We begin with the case where $\mathfrak{A}_A = \mathfrak{B}(\mathbb{C}^{d_A})$ and $\mathfrak{A}_B$ is a general finite dimensional algebra, and then generalize to the case of general finite dimensional $\mathfrak{A}_A$ below. Let $\mathscr{E}_{B|A} : \mathfrak{A}_A \to \mathfrak{A}_B$ be a TPCP map. To define the isomorphism, we begin with the $\mathscr{E}_{B|A} \to \rho_{B|A}$ direction. Let $\mathfrak{A}_{A'}$ be another copy of the algebra $\mathfrak{A}_A$, i.e. $\mathfrak{A}_{A'} = \mathfrak{A}_A = \mathfrak{B}(\mathbb{C}^{d_A})$. The isomorphism is dependent on an arbitrary choice of basis for $\mathbb{C}^{d_A}$, so let $\{|j\rangle_A\}$ be such a basis and define the "maximally entangled" conditional state vector on $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_A}$ as

$$\left|\Phi^+\right\rangle_{A'|A} = \sum_{j=1}^{d_A} |jj\rangle_{A'A}. \tag{8}$$

This is so called because when one uses eq. (7) to combine the conditional state $\rho^+_{A'|A} = |\Phi^+\rangle_{A'|A} \langle\Phi^+|_{A'|A}$ with a maximally mixed marginal state $\rho_A = \frac{I_A}{d_A}$, where I_A is the identity operator in $\mathfrak{A}_A$, one obtains a properly normalized maximally entangled state $\rho^+_{AA'} = |\Phi^+\rangle_{AA'} \langle\Phi^+|_{AA'}$, where $|\Phi^+\rangle_{AA'} = \frac{1}{\sqrt{d_A}} |\Phi^+\rangle_{A'|A}$. However, note that $\rho^+_{A'|A}$ generally does not yield a maximally entangled state when combined with an arbitrary reduced state ρ_A.

Next, we define the conditional state $\rho_{B|A}$ associated with the map $\mathscr{E}_{B|A}$ via

$$\rho_{B|A} = \mathscr{E}_{B|A'} \otimes \mathscr{I}_A\left(\rho^+_{A'|A}\right), \tag{9}$$

where $\mathscr{I}_A$ is the identity CP-map on system A. Note that here $\mathscr{E}_{B|A'}$ is acting on the ancillary system A', transforming it into system B. It is straightforward to check that $\rho_{B|A}$ is a valid conditional state, which is transformed into a valid joint state ρ_{AB} when it is combined with any reduced density operator ρ_A in $\mathfrak{A}_A$ via eq. (7).

[2] As pointed out by Cerf and Adami [7, 8, 9], another definition of note is $\rho_{B|A} = \lim_{n\to\infty}\left(\rho_A^{-\frac{1}{2n}} \otimes I_B \rho_{AB}^{\frac{1}{n}} \rho_A^{-\frac{1}{2n}} \otimes I_B\right)^n$, since this allows the von Neumann conditional entropy to be expressed as $S(B|A) = -\mathrm{Tr}\left(\rho_{AB} \log \rho_{B|A}\right)$ in analogy to the classical expression for conditional Shannon entropy.

[3] Jamiołkowski and Choi both take $\mathfrak{A}_A = \mathfrak{B}(\mathbb{C}^d)$, but the extension to general finite dimensional algebras is straightforward as shown below

For the $\rho_{B|A} \rightarrow \mathscr{E}_{B|A}$ direction, note that the action of $\mathscr{E}_{B|A}$ on an arbitrary state $\sigma_A \in \mathfrak{A}_A$ may be recovered from $\rho_{B|A}$ via

$$\mathscr{E}_{B|A}(\sigma_A) = \mathrm{Tr}_{AA'}\left(\left(\rho^+_{A'|A} \otimes I_B\right)\left(\sigma_A \otimes \rho_{B|A'}\right)\right), \tag{10}$$

which is easily checked by expanding the states in the basis used to define the isomorphism. Note that the state $\rho_{B|A}$ is pure iff the TPCP map $\mathscr{E}_{B|A}$ is an isometry, and in the case where $\mathfrak{A}_A = \mathfrak{A}_B$, this means that $\mathscr{E}_{B|A}$ is unitary.

Finally, we briefly explain how to extend the isomorphism to the case where $\mathfrak{A}_A$ is an arbitrary finite dimensional algebra. The problem is that, for a general algebra of the form $\mathfrak{A}_A = \mathfrak{B}(\mathbb{C}^{d_1}) \oplus \mathfrak{B}(\mathbb{C}^{d_2}) \oplus \ldots \oplus \mathfrak{B}(\mathbb{C}^{d_n})$, $\mathfrak{A}_A \otimes \mathfrak{A}_{A'}$ does not contain the conditional state $\rho^+_{A'|A}$, since $|\Phi^+\rangle_{A'|A}$ is a superposition of all basis states of the form $|jj\rangle_{AA'}$, and this is ruled out for any algebra which is the direct sum of more than one irreducible component. To resolve this, note that $\mathfrak{A}_A$ may be embedded in $\mathfrak{B}(\mathbb{C}^{d_1+d_2+\ldots+d_n})$ by associating operators in $\mathfrak{A}_A$ with block-diagonal matrices in $\mathfrak{B}(\mathbb{C}^{d_1+d_2+\ldots+d_n})$. The action of $\mathscr{E}_{B|A}$ is not well defined on this algebra, since its domain is $\mathfrak{A}_A$, but this can be dealt with by introducing the projection map $\mathscr{P} : \mathfrak{B}(\mathbb{C}^{d_1+d_2+\ldots+d_n}) \rightarrow \mathfrak{A}_A$, which can be written in the form

$$\mathscr{P}(\rho) = \sum_{j=1}^{n} P_j \rho P_j, \tag{11}$$

where P_j is the projector onto the factor $\mathbb{C}^{d_j}$ in $\mathbb{C}^{d_1+d_2+\ldots+d_n}$. Now, $\mathscr{E}_{B|A'}$ may be replaced with $\tilde{\mathscr{E}}_{B|A'} = \mathscr{E}_{B|A'} \circ \mathscr{P}_{A'}$ in eq. (9), and this map is well defined on $\mathfrak{B}(\mathbb{C}^{d_1+d_2+\ldots+d_n})$. Since $\mathscr{P}$ is idempotent, one may additionally replace $\rho^+_{A'|A}$ with

$$\tilde{\rho}^+_{A'|A} = \mathscr{I}_A \otimes \mathscr{P}_{A'}(\rho_{A'|A}) \tag{12}$$

in eqs. (9) and (10), which is a well-defined conditional state in $\mathfrak{A}_A \otimes \mathfrak{A}_{A'}$. The actions of $\tilde{\mathscr{E}}_{B|A'}$ and $\mathscr{E}_{B|A'}$ on this state are identical, so we obtain

$$\rho_{B|A} = \mathscr{E}_{B|A'} \otimes \mathscr{I}_A\left(\tilde{\rho}^+_{A'|A}\right) \tag{13}$$

and

$$\mathscr{E}_{B|A}(\sigma_A) = \mathrm{Tr}_{AA'}\left(\tilde{\rho}^+_{A'|A} \otimes I_B \sigma_A \otimes \rho_{B|A'}\right), \tag{14}$$

as the generalized version of the isomorphism.

4.1. Operational Interpretation in terms of teleportation

There is a standard interpretation of the Choi-Jamiołkowski isomorphism in terms of “noisy gate teleportation”, which is the generalization of a protocol considered in [31] from unitary operations to arbitrary TPCP maps. To describe this, we begin with the case where $\mathfrak{A}_A = \mathfrak{B}(\mathbb{C}^{d_A})$, and combine the conditional states, $\rho_{B|A'}$ and $\rho^+_{A'|A}$, with maximally mixed reduced states, $\rho_{A'} = \frac{I_{A'}}{d_A}$ and $\rho^+_A = \frac{I_A}{d_A}$, via eq. (7), so that the reverse direction of the isomorphism eq. (10) can be rewritten in terms of the properly normalized joint states $\rho_{A'B} = \frac{1}{d_A}\rho_{B|A'}$ and $\rho^+_{AA'} = \frac{1}{d_A}\rho_{A'|A}$ as

$$\mathscr{E}_{B|A}(\sigma_A) = d_A^2 \mathrm{Tr}_{AA'}\left(\rho^+_{AA'} \otimes I_B \sigma_A \otimes \rho_{A'B}\right). \tag{15}$$

Now, suppose that Alice holds a system in an unknown state[4] $\sigma_A \in \mathfrak{A}_A$ and that Alice and Bob share a pair of systems in the state $\rho_{A'B}$. They would like for Bob to end up with his system in the transformed state[5] $\mathscr{E}_{B|A}(\sigma_A)$, using only local operations and classical communication and the state $\rho_{A'B}$ as resources. To achieve this, Alice can make a joint measurement of the systems A and A' in a basis that includes the state ρ^+_{AA}. If the outcome corresponding to this state is obtained, then the procedure is successful, which may be deduced from eq. (15). It is also evident from eq. (15) that the probability of obtaining this successful outcome is $\frac{1}{d_A^2}$. On the other hand, if the $\rho^+_{AA'}$ outcome is not obtained then the procedure fails. In some cases it is still possible for Bob to reconstruct the state $\mathscr{E}_{B|A}(\sigma_A)$ by applying a local

[4] For the subjectivist, the phrase “unknown state” should set alarm bells ringing. It is a shorthand for saying that the system is prepared by Charlie, who then gives it to Alice without revealing any details of the preparation procedure. The “unknown state” is the one assigned by Charlie [4].

[5] Again, it is Charlie’s description of Bob’s state that is being referred to.

operation that depends on Alice's outcome, which she can inform him of via classical communication. In particular, this happens when $\mathscr{E}_{B|A}$ is the identity, in which case we obtain the standard teleportation protocol [2].

This protocol can be straightforwardly generalized to the case where $\mathfrak{A}_A$ is a general finite dimensional algebra. However, the expression for the success probability becomes more complicated because more than one state may be mapped to $\tilde{\rho}^+_{A'|A}$ by the action of $\mathscr{P}_{A'}$. In particular, it can happen that states associated failure outcomes in $\mathfrak{B}(\mathbb{C}^{d_1+d_2+\ldots+d_n})$ are mapped to the success outcome $\tilde{\rho}^+_{A'|A}$ by $\mathscr{P}_{A'}$, which increases the probability of success. As an example, consider the classical algebra $\mathfrak{B}(\mathbb{C}) \oplus \mathfrak{B}(\mathbb{C})$ and its embedding in $\mathfrak{B}(\mathbb{C}^2)$. Here, Alice should make a measurement in the Bell basis

$$\begin{array}{ll} \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right) & \left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle + \left|10\right\rangle\right) \\ \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle - \left|11\right\rangle\right) & \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle - \left|10\right\rangle\right), \end{array} \tag{16}$$

as in the teleportation protocol. Under the projection map $\mathscr{P}_{A'}$,

$$\rho^+_{AA'} = \left|\Phi^+\right\rangle\left\langle\Phi^+\right|_{AA'} \to \tilde{\rho}^+_{AA'} = \frac{1}{2}\left(\left|00\right\rangle\left\langle 00\right| + \left|11\right\rangle\left\langle 11\right|\right)_{AA'}, \tag{17}$$

but $\left|\Phi^-\right\rangle\left\langle\Phi^-\right|_{AA'}$ also gets mapped to the same thing, so these outcomes may be grouped together and the success probability is increased from $1/4$ to $1/2$. Similarly, the failure outcomes $\left|\Psi^\pm\right\rangle\left\langle\Psi^\pm\right|_{AA'}$ both get mapped to $\frac{1}{2}\left(\left|01\right\rangle\left\langle 01\right| + \left|10\right\rangle\left\langle 10\right|\right)_{AA'}$, so these may also be grouped together and Alice's measurement is then just a parity measurement of her two classical bits. In the case where $\mathscr{E}_{B|A}$ is the identity, Bob can recover the correct state by flipping his bit when Alice gets the failure outcome and the whole procedure is simply a classical one-time-pad (Vernam cipher) [35, 33]. The similarity between teleportation and the one-time pad has been remarked upon before [28, 11], but in the algebraic formulation it is more than just a similarity. They both arise from the same isomorphism, so they are, in fact, the same thing.

4.2. Operational interpretation in terms of stochastic processes

The previous interpretation resulted from combining the conditional states with maximally mixed reduced states, so it is natural to ask whether there is any interpretation that results from combining $\rho_{B|A}$ with an arbitrary reduced state ρ_A. Doing so reveals the Choi Jamiołkowski isomorphism to be a generalization of the relationship between stochastic dynamics and conditional probabilities in classical probability theory.

In the classical case, it is a familiar fact that we can always describe the correlations between two random variables by a joint probability distribution, regardless of whether the variables refer to two distinct physical systems or to the same quantity associated with the same system at two distinct times. In the latter case, we are likely to describe the situation as a stochastic process. Initially there is a random variable A, with probability distribution $P(A)$. Then, the system undergoes a stochastic evolution described by a stochastic matrix $\Gamma_{B|A}$, which transforms A into another variable B, with probability distribution $P(B)$. However, $P(A)$ and $\Gamma_{B|A}$ are just convenient summaries of a joint distribution $P(A,B)$, since $\Gamma_{B|A}$ is a matrix of transition probabilities, i.e. conditional probabilities. It is evident that any joint probability distribution $P(A,B)$ may in principle arise in this scenario and also in the case where the variables refer to distinct systems, so that one does not have to know the causal relations between the two variables in advance in order to know that a joint probability distribution is the correct mathematical object to use for describing their correlations.

The analog of this in quantum theory would be to always describe correlations between systems described by algebras $\mathfrak{A}_A$ and $\mathfrak{A}_B$ by a joint state $\rho_{AB} \in \mathfrak{A}_A \otimes \mathfrak{A}_B$, regardless of whether $\mathfrak{A}_A$ and $\mathfrak{A}_B$ refer to two distinct systems or to the same system at two distinct times. In the former case, this is indeed what we usually do. However, in the latter case, we normally ascribe a state $\rho_A \in \mathfrak{A}_A$ to the system initially, and then assert that it evolves in time according to the TPCP map $\mathscr{E}_{B|A} : \mathfrak{A}_A \to \mathfrak{A}_B$ to obtain a state $\rho_B \in \mathfrak{A}_B$. This is analogous to the stochastic process description given in the classical case above, but in the quantum case we do not normally associate this with a joint state ρ_{AB}. The Choi-Jamiołkowski isomorphism asserts that a description in terms of a joint state is indeed possible, since the map $\mathscr{E}_{B|A}$ is isomorphic to a conditional state $\rho_{B|A}$ from which a joint state ρ_{AB} can be built by combining with ρ_A via eq. (7). Since we can also go in the other direction, we could equally well describe things just by specifying ρ_{AB}. However, this is not quite enough, since we would like to assert that ρ_{AB} provides an equally useful summary of the probabilistic predictions that may be obtained in this scenario, without having to go back and reconstruct ρ_A and $\mathscr{E}_{B|A}$

via the isomorphism before calculating them. In fact, this is almost the case, but a slight modification is needed and we actually consider the following series of correspondences:

$$(\rho_{AB}) \leftrightarrow \left(\rho_A, \rho_{B|A}\right) \leftrightarrow \left(\rho_A^T, \mathscr{E}_{B|A}\right), \tag{18}$$

where ^{T} denotes the transpose in the basis used to construct the isomorphism. The transpose is related to a time reversal implicit in the construction, which is discussed in [29], but note that if an eigenbasis of ρ_A is used to construct the isomorphism then $\rho_A^T = \rho_A$, so this would be a natural constraint to impose on the construction.

To understand how this works, it is helpful to return briefly to the classical case. If Alice has access to a random variable A and Bob has access to a random variable B, and they ascribe the joint probability distribution $P(A,B)$ to the two variables, then the set of joint probability distributions they can generate by local processing of their variables is the same, regardless of whether Alice and Bob read A and B from distinct physical systems or if Bob's variable comes from the same physical system, sent to him through a noisy channel by Alice. Essentially the same thing is true in the quantum case, although noncommutativity makes things a little more subtle. In the case where ρ_{AB} represents the joint state of two systems, the local processing consists of measurements on $\mathfrak{A}_A$ and on $\mathfrak{A}_B$. However, in the case where it represents the same system at two different times, we have to move to a "prepare and measure" scenario where the local processing consists of a choice of an ensemble preparation for Alice and a measurement for Bob. To describe this, we need to recall the formalism of generalized measurements in quantum theory.

A general measurement can be represented by a Positive Operator Valued Measure (POVM). This is a collection of positive operators $\boldsymbol{M} = \{M_j\}$ in an algebra $\mathfrak{A}$ that sum to the identity $\sum_j M_j = I$. The probability of obtaining the outcome $\boldsymbol{M} = j$ when the system is in state $\rho \in \mathfrak{A}$ is given by the generalized Born rule $\text{prob}(\boldsymbol{M} = j) = \text{Tr}\left(M_j \rho\right)$. It is less commonly appreciated that POVMs can also be used to describe ensemble preparation procedures. This is demonstrated by the following lemma, which is proved in [29].

Lemma: Let ρ be a state in $\mathfrak{A}$. $\{p_j, \rho_j\}$ is an ensemble decomposition of ρ iff there exists a POVM $\boldsymbol{M} = \{M_j\}$ such that $p_j = \text{Tr}\left(M_j \rho\right)$ and $\rho_j = \frac{\sqrt{\rho} M_j \sqrt{\rho}}{\text{Tr}\left(M_j \rho\right)}$.

Therefore, given a state ρ and a POVM $\boldsymbol{M}$, there are two procedures that they could be used to describe. An $\boldsymbol{M}$-*measurement* of ρ is a procedure that takes a system in the state ρ as input and outputs a classical random variable with distribution $\text{prob}(\boldsymbol{M} = j) = \text{Tr}\left(M_j \rho\right)$. Conversely, an $\boldsymbol{M}$-*preparation* of ρ consists of first generating a classical random variable with distribution $\text{prob}(\boldsymbol{M} = j) = \text{Tr}\left(M_j \rho\right)$ and then preparing the corresponding state $\rho_j = \frac{\sqrt{\rho} M_j \sqrt{\rho}}{\text{Tr}\left(M_j \rho\right)}$ as output. We are now in a position to state the main result, which is proved in [29].

Theorem: Let $\rho_{AB} \in \mathfrak{A}_A \otimes \mathfrak{A}_B$ be a state with reduced state $\rho_A \in \mathfrak{A}_A$ and conditional state $\rho_{B|A}$. Let $\mathscr{E}_{B|A}$ be the TPCP map isomorphic to $\rho_{B|A}$ and let ^{T} denote the transpose of an operator taken in the basis used to define the isomorphism. Let $\boldsymbol{N} = \{N_j\}$ be a POVM on $\mathfrak{A}_A$ and let $\boldsymbol{M} = \{M_k\}$ on $\mathfrak{A}_B$. Then, the joint probability of getting outcome j in an $\boldsymbol{N}$-measurement on $\mathfrak{A}_A$ and getting outcome k in an $\boldsymbol{M}$-measurement on $\mathfrak{A}_B$, on a joint system in the state ρ_{AB}, is the same as the joint probability for obtaining the j value of the classical input in an N^T-preparation of ρ_A^T and getting outcome k in an $\boldsymbol{M}$-measurement on $\mathfrak{A}_B$, when the system is evolved according to $\mathscr{E}_{B|A}$ between preparation and measurement. Equivalently,

$$\text{prob}(\boldsymbol{N} = j, \boldsymbol{M} = k) = \text{Tr}_{AB}\left(N_j \otimes M_k \rho_{AB}\right) = \text{Tr}_B\left(M_k \mathscr{E}_{B|A}\left(\sqrt{\rho^T} N_j^T \sqrt{\rho^T}\right)\right). \tag{19}$$

5. SUBJECTIVITY OF QUANTUM OPERATIONS

We now turn to the question of what the above result means for the status of quantum operations in the CFS view of quantum theory. The first point is that, when considering the probabilities of local measurements made on a bipartite system, the description we would normally give in terms of a bipartite state ρ_{AB} can always be replaced by a description in terms of the pair $(\rho_A^T, \mathscr{E}_{B|A})$ via eq. (19). The latter description looks just like a "prepare and measure" scenario, in which the TPCP map $\mathscr{E}_{B|A}$ describes the time evolution between preparation and measurement, even though we are "actually" talking about the correlations between two subsystems at a given time. In this context, CFS would assert that the assignment of the state ρ_{AB} *always* represents some agent's degree of belief and is *never* to be thought of as representing an objective state of affairs. Clearly, for this to be true, at least one of ρ_A^T or $\mathscr{E}_{B|A}$ must represent degrees of belief rather than objective facts. In fact, for CFS, *both* ρ_A^T and $\mathscr{E}_{B|A}$ must represent degrees of belief, because they impose no a priori constraints on the degree to which two agents' state assignments may differ, and both ρ_A^T and $\mathscr{E}_{B|A}$ must be allowed to vary in order to obtain an arbitrary ρ_{AB}. In particular, CFS state that ρ_{AB} is subjective even if it is pure[6], and demanding purity of ρ_{AB} is equivalent to demanding that $\mathscr{E}_{B|A}$ is an isometry, and unitary if $\mathfrak{A}_A = \mathfrak{A}_B$. Thus, we already have a case where CFS would have to regard a unitary operation as representing subjective degrees of belief rather than an objective state of affairs.

However, in this case the unitary operation is simply providing part of a description of a bipartite system and the real question is whether unitary operations should be regarded as subjective when they are being used to describe the time evolution of a single system. To argue this case, we introduce a variant of Leibniz's principle of the "identity of indiscernibles" [14]. If the sum total of probabilistic assignments that can be made in one experimental scenario is identical to those that can be made in another scenario, then it is clear that both scenarios should be representable by an identical mathematical formalism. Our principle states that we should ascribe subjectivity and objectivity to the elements of the formalism identically in both cases. In the present context, if we are "really" using $(\rho_A^T, \mathscr{E}_{B|A})$ to describe a "prepare and measure" scenario, then $\mathscr{E}_{B|A}$ does represent a time evolution and the statistical predictions that can be made are identical to those of the bipartite scenario described above. Thus, our principle requires that if $\mathscr{E}_{B|A}$ is subjective in the bipartite scenario, then it is also subjective when used to describe time evolution in the prepare and measure scenario. In particular, for CFS, this has to apply to unitary operations, since they are treated as subjective in the bipartite scenario.

At this point, the subjectivity of unitary operations hangs on whether or not one accepts the principle described above. The main argument for accepting it rests on the virtue of probabilistic abstraction, which is familiar in the classical case. Consider the Kolmogorovian formulation of probability theory, in which we have a sample space of events. This is a purely abstract mathematical theory and no identification between events in the sample space and physical events in spacetime is supposed. Clearly, this is the reason behind the fact that we can describe spacelike and timelike correlated variables via an identical formalism, using joint probability distributions in both cases. Now, subjectivist axiomatizations of probability theory, such as those provided by de Finetti and Savage [12, 32], are focussed on deriving a mathematical representation of degrees of belief in various events from their *logical* relations, rather than anything to do with how those events are embedded in spacetime. This is natural for a theory which is about rational decision making in general, rather than being just about its application in physics, and leads to the abstraction of the theory from the details of causality. If we are really to regard the better part of quantum theory as a "law of thought", as advocated by Fuchs [15, 18], then it seems that we ought to adopt a similar approach as far as possible. The fact that two scenarios entail the same set of possible probability ascriptions, is enough to guarantee their equivalence from the point of view of decision making. Therefore, the two cases should be identified within the abstract theory, and the principle follows.

6. OBJECTIVITY OF PHYSICAL LAWS

Accepting the preceding argument implies that the Hamiltonians and Lagrangians of physics represent subjective degrees of belief, since assuming that we are prepared to regard time intervals as objective, the Hamiltonian of a system uniquely determines the unitary time evolution operator. Our most fundamental physical theories, such as the standard model of particle physics, are essentially postulations of a particular Hamiltonian or Lagrangian, so it might seem that we are in danger of losing the objectivity of physical law altogether.

However, this worry is unfounded, and rests on a similar category error as the identification of objective certainty with probability one [5] (assuming a finite sample space to avoid the necessary caveats about sets of measure zero). To the radical probabilist, these are very distinct assertions. The statement that the probability of an event is equal to one is relative to the particular agent who asserts it. It is verified by observing the agent's decision making behavior, e.g. asking her to enter into a bet on the event and finding out that she is willing to bet her life on it. On the other hand, objective certainty means that the event is sure to occur and can only be verified by empirical observation of the occurrence of the event itself, or by logical deduction from other objective certainties. For the radical probabilist,

[6] The arguments for this will not be rehashed here, but see [5]

agents may make probability one assignments even if the event itself is not an objective certainty because no prior probability assignment is ruled out as irrational a priori. To be sure, a probability one assertion entails a rather strong commitment on the part of the agent, and it does mean that the agent *believes* that the event is certain to occur. In particular, if she believes that it is an objective certainty then she must assign probability one.

The fact that probability one is not identified with objective certainty does not mean that objective facts about the world do not exist, just that they have no representation in probability theory without reference to an agent who believes in them. Similarly, if Hamiltonians are taken as subjective degrees of belief rather than objective physical laws it does not mean that objective physical laws have no bearing on Hamiltonian assignments. Belief in the truth of a particular physical law, can indeed constrain the class of Hamiltonians that an agent may assign. For example, if the Hamiltonian does not respect a particular symmetry principle, such as Lorentz invariance, that the agent believes to be true then it is not a legitimate representative of the agent's beliefs. Here it is the symmetry principle, and not the Hamiltonian itself, that captures the objective content of the physical law.

7. CONCLUSIONS

To summarize, we have argued that if quantum states, including pure states, are to be regarded as representing subjective degrees of belief, then it is natural to regard quantum operations, including unitary ones, as also being subjective. Essentially, if quantum states, including pure states, are more like probability distributions than "states of reality", then quantum operations, including unitary ones, are more like conditional probabilities than objective dynamical laws and should likewise be taken to be subjective.

Perhaps more importantly, this work raises the question of whether a formalism for quantum theory could be given that does not require causal relations to be specified a priori. Although quantum theory is often thought to be a kind of generalized probability theory, it is not often formulated at the same level of abstraction as the classical theory. In the usual formulation of quantum theory, when we speak of joint states we are referring to the state of two distinct subsystems and when we speak of correlations between the same system at two different times we use TPCP maps instead. As noted above, this is a closer analog to the classical theory of stochastic processes than it is to a fully abstract probability theory. In the canonical framework for quantum theory, this same issue is manifested in the fact that quantum states are always referred to spakelike hypersurfaces rather than to arbitrary collections of regions in spacetime. In other words, we need to know some minimal information about the causal relations between events before we can even set up the theory. We take the current work as a demonstration that, in fact, joint quantum states need not be exclusively referred to spacelike separated regions, but can also be used to describe the correlations between algebras referring to potentially timelike separated events. This indicates that it may be possible to formulate quantum theory at the same level of abstraction as Kolmogorov probability theory, although much further work is needed to realize this possibility. Having such a formalism would hopefully shed further light on the foundations of quantum theory and quantum information, and may even play a role in the construction of a background independent quantum theory of gravity, wherein there is good reason to suspect that causal relations between events may not be fixed a priori.

Acknowledgments: I would like to thank Rob Spekkens for many interesting discussions on topics related to this work. I would also like to thank Andrei Khrennikov and Chris Fuchs for inviting me to speak at this conference, and for allowing me to fill this article with speculations that may or may not prove meaningful. Research at Perimeter Institute is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MEDT. At Cambridge, this work was supported by the European Commission through QAP, QAP IST-3-015848, and through the FP6-FET Integrated Project SCALA, CT-015714.

REFERENCES

1. P. Arrighi and C. Patricot. On quantum operations as quantum states. *Ann. Phys.*, 311:26–52, 2004.
2. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.
3. C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theroem. *Phys. Rev. Lett.*, 68:557–559, 1992.
4. C. M. Caves, C. A. Fuchs, and R. Schack. Unkown quantum states: the quantum de Finetti representation. *J. Math. Phys.*, 43(9):4537–4559, 2002.

5. C. M. Caves, C. A. Fuchs, and R. Schack. Subjective probability and quantum certainty. quant-ph/0608190, 2006.
6. Carlton M. Caves, Christopher A. Fuchs, and Rüdiger Schack. Quantum probabilities as Bayesian probabilities. *Phys. Rev. A*, 65:022305, 2002. quant-ph/0106133.
7. N. J. Cerf and C. Adami. Negative entropy and information in quantum mechanics. *Phys. Rev. Lett.*, 79(26):5194–5197, December 1997.
8. N. J. Cerf and C. Adami. Quantum information theory of entanglement and measurement. *Physica D*, 120:62–81, 1998.
9. N. J. Cerf and C. Adami. Quantum extension of conditional probability. *Phys. Rev. A*, 60(2):893–897, 1999.
10. M. D. Choi. Completely positive linear maps on complex matrices. *Lin. Alg. Appl.*, 10:285–290, 1975.
11. D. Collins and S. Popescu. A classical analogue of entanglement. *Phys. Rev. A*, 65:032321, 2002. quant-ph/0107082.
12. B. de Finetti. *Theory of Probability*. Wiley, 1974.
13. J. L. Doob. What is a stochastic process? *Amer. Math. Monthly*, 49(10):648–653, December 1942.
14. P. Forrest. The identity of indiscernibles. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, fall 2006 edition edition, http://plato.stanford.edu/archives/fall2006/entries/identity-indiscernible/.
15. C. A. Fuchs. Quantum mechanics as quantum information (and only a little more). quant-ph/0205039, 2002.
16. C. A. Fuchs. Quantum states: W.H.A.T.? http://netlib.bell-labs.com/who/cafuchs/PhaseTransition.pdf, 2002.
17. C. A. Fuchs. *Notes on a Paulian Idea*, volume 4 of *Mathematical Modelling in Physics, Engineering and Cognitive Sciences*. Växjö University Press, 2003. quant-ph/0105039.
18. C. A. Fuchs. Quantum mechanics as quantum information, mostly. *J. Mod. Opt.*, 50:987, 2003.
19. C. A. Fuchs. Darwinism all the way down (probabilism all the way back up). http://netlib.bell-labs.com/who/cafuchs/n-Samizdat2.pdf, 2006.
20. C. A. Fuchs and R. Schack. Unknown quantum states and operations, a Bayesian view. In M. G. A. Paris and J. Rehacek, editors, *Quantum Estimation Theory*. Springer-Verlag, 2004. quant-ph/0404156.
21. C. A. Fuchs, R. Schack, and P. F. Scudo. A de Finetti representation theorem for quantum process tomography. *Phys. Rev. A*, 69:062305, 2004. quant-ph/0307198.
22. R. B. Griffiths. Channel kets, entangled states, and the location of quantum information. *Phys. Rev. A*, 71:042337, 2005.
23. A. Hagar. A philosopher looks at quantum information theory. *Philosophy of Science*, 70:752–775, 2003.
24. A. Hagar. Quantum information: What price realism? *Int. J. Quant. Inform.*, 3(1):165–170, 2005.
25. A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3:275–278, 1972.
26. R. Jeffrey. *Subjective Probability: The Real Thing*. Cambridge University Press, 2004.
27. A. N. Kolmogorov. *Foundations of the Theory of Probability*. Chelsea, 2nd english edition edition, 1950.
28. M. Koniorczyk, T. Kiss, and J. Janszky. Teleportation: from probability distributions to quantum states. *J. Phys. A*, 34:6949–6955, 2001. quant-ph/0011083.
29. M. S. Leifer. Quantum dynamics as an analog of conditional probability. *Phys. Rev. A*, 74:042310, 2006. quant-ph/0606022.
30. M. S. Leifer and R. W. Spekkens. State pooling and a quantum bayes' theorem. in preparation, 2006.
31. M. A. Nielsen and I. L. Chuang. Programmable quantum gate arrays. *Phys. Rev. Lett.*, 79(2):321–324, July 1997.
32. L. J. Savage. *The Foundation of Statistics*. Dover, 2nd rev. edition edition, 1972.
33. C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.
34. P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.
35. G. Vernam. U.S. patent 1,310,719, 1919.
36. F. Verstraete and H. Verschelde. On quantum channels. quant-ph/0202124.
37. K. Życzkowski and I. Bengtsson. On duality between quantum maps and quantum states. *Open Syst. Inf. Dyn.*, 11:3–42, 2004.