Pooling quantum states obtained by indirect measurements

Robert W. Spekkens and H. M. Wiseman

Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom

Centre for Quantum Computer Technology, Centre for Quantum Dynamics, School of Science, Griffith University, Brisbane, 4111 Australia

(Dated: Dec. 20, 2006)

We consider the pooling of quantum states when Alice and Bob each share one part of a tripartite system and, on the basis of measurements on their respective shares, each infer a quantum state for the third subsystem S. We denote the conditioned states which Alice and Bob assign to S by $\alpha$ and $\beta$ respectively, while the unconditioned state of S is $\rho$. The state assigned by an overseer, who has all the data available to Alice and Bob, is $\omega$. The overseer is told only $\alpha$, $\beta$, and $\rho$. We show that under certain special circumstances, this information is enough for her to reconstruct $\omega$ by the formula $\omega \propto \alpha \rho^{-1} \beta$. Specifically, we show that this reconstruction is possible when the initial tripartite state is pure or when it is a mixture of product states that are orthogonal on S.

I. INTRODUCTION

In the approach to quantum theory wherein a quantum state encodes an observer’s knowledge of a system, different observers may assign different quantum states. It is then natural to ask which pairs of quantum states are compatible in the sense that they can be simultaneously assigned by a pair of observers. Another natural question concerns pooling: what is the quantum state that ought to be assigned to a system by someone who learns only the quantum states assigned to it by two distinct observers?

The way in which we have just posed the pooling problem — the standard way to do so — presumes that no further assumptions need to be specified in order for there to be a unique solution. That this is not necessarily the case becomes clear when we examine carefully the notion of pooling states of knowledge in classical probability theory. Such an analysis is particularly appropriate given that the problem of pooling quantum states was originally conceived as an analogue of classical pooling.

The classical pooling result may be stated in the following way. Suppose that Alice and Bob share a prior probability distribution $p(s)$ over a space of hypotheses. Suppose further that the data they acquire before updating their distributions is obtained independently. Specifically, if $a$ denotes Alice’s data and $b$ denotes Bob’s data, then these are assumed to be conditionally independent given $s$:

$$p(a,b|s) = p(a|s)p(b|s). \quad (1.1)$$

In these circumstances, Alice, upon learning $a$, updates her description from $p(s)$ to $p(s|a) \propto p(a)p(s)$ and Bob, upon learning $b$, updates his description from $p(s)$ to $p(s|b) \propto p(b)p(s)$.

A third party who has access to both data $a$ and $b$, whom we shall call the overseer and name Oswald, would update his description from $p(s)$ to $p(s|a,b)$, where

$$p(s|a,b) \propto \frac{p(s|a)p(s|b)}{p(s)}, \quad (1.2)$$

as one easily verifies by applying Bayes’ theorem to Eq. (1.1). In fact, Eq. (1.2) holds only for those values of $s$ for which $p(s) > 0$; for values of $s$ for which $p(s) = 0$, Oswald assigns $p(s|a,b) = 0$. The important point to note is that the overseer’s probability distribution depends only on the prior distribution and Alice’s and Bob’s posterior distributions. Thus, another party, who only has knowledge of these three distributions, can reconstruct Oswald’s distribution. This person, whom we shall call the pooler and name Penelope, does not need to know any additional details of how Alice and Bob came to update the prior in the way that they did.

However, the formula (1.2) does not hold in general. A specific counterexample is provided in Sec. II C. In such cases, Oswald, who is aware of how the data was acquired, can still use Bayes’ theorem to update his distribution. But Penelope, who only has the prior distribution and Alice’s and Bob’s posterior distributions at her disposal, does not have enough information to reconstruct Oswald’s state of knowledge. It is only under special circumstances, such as Alice’s and Bob’s data being conditionally independent, that she is able to do so.

The lessons of classical pooling for quantum pooling are several. Firstly, we have seen that in the one case where the pooler can reconstruct the overseer’s posterior distribution, she needs to make use of not only Alice and Bob’s distributions, but also the prior distribution. Consequently, it is likely that in the quantum case she will require not only Alice’s and Bob’s quantum states, but also the “prior” quantum state — the one that they both assigned prior to the measurements. Secondly, in order to tackle the pooling problem, it has been useful to imagine an overseer who knows every aspect of the protocol and the collected data, because his posterior is guaranteed to be uniquely specified by Bayes’ theorem. This suggests that in the quantum case, we ought to again consider an overseer who knows every aspect of the protocol and the collected data, because the quantum state that the overseer must assign after the measurements — the “posterior” quantum state — will be uniquely specified by quantum theory (through the quantum update rule).
If this state is a function of Alice’s state, Bob’s state, and the prior state, and nothing more, then a pooler who is given these three can succeed in reconstructing Oswald’s posterior state. Thirdly, we expect that there are limited circumstances in which the pooler can succeed in this fashion. The quantum analogue of Alice and Bob having conditionally independent data will be one such circumstance.

Most of the previous work on pooling has not taken this approach. Typically, the prior quantum state is not specified in the problem, nor is it specified how Alice and Bob acquired their data \[2, 4, 5\]; the notion of pooling that is discussed in these papers is therefore distinct from the one considered here. On the other hand, Jacobs \[3, 6\] and Brun in Ref. \[7\] have emphasized the importance of the method of data acquisition for pooling knowledge about a system, have taken care to specify a prior quantum state (they both assume a completely mixed state), and have used the device of an observer who has all the information (an overseer) to evaluate pooling strategies. The pooling problem that Jacobs considers is nonetheless compatible, and we expect that there are limited circumstances in which the pooler can succeed in reconstructing Oswald’s state, in analogy to Eq. (1.2). This is illustrated in Fig. 1. We then show that our formula fails in more general cases, as one would expect. We discuss the relation of our results to state compatibility, and generalize our results to the case of arbitrarily many parties.

II. POOLING QUANTUM STATES FROM INDIRECT MEASUREMENTS

The scenario we consider is as follows \[13\]. There is a tripartite system \(ABS\) for which Alice possesses the \(A\) share and Bob possesses the \(B\) share. They both initially describe the tripartite system by the (possibly mixed) quantum state \(W\) defined on \(\mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^S\), and thus they both initially describe the third system \(S\) by the same reduced state \(\rho \equiv \text{Tr}_{AB}(W)\). Alice makes a generalized measurement on \(A\), and Bob makes a generalized measurement on \(B\). After registering the outcome of her measurement, Alice updates her description of the system \(S\) to a new quantum state which we denote by \(\alpha\). Likewise, after registering the outcome of his measurement, Bob updates his description of \(S\) to a new quantum state which we denote by \(\beta\). Quantum theory uniquely specifies how Alice and Bob ought to update their descriptions. (Strictly speaking, Alice only requires the reduction of \(W\) to \(AS\) and Bob only requires the reduction to \(BS\), as is indicated schematically in Fig. 1)

The overseer, Oswald, knows everything there is to know: the initial state \(W\), what measurements Alice and Bob made, and the outcomes they obtained. After learning all of this information, the overseer updates his description of \(S\) to the state \(\omega\). Again, quantum theory uniquely specifies how the overseer ought to update his description.

![Fig. 1: Schematic of the pooling problem we consider. All parties seek to update the quantum state they assign to system \(S\) based on the information they acquire. Each party has access to only certain information, represented by the contents of the circle in which he or she is enclosed. All information about \(S\) is ultimately derived from indirect measurements on \(S\), that is, measurements upon systems \((A\) and \(B)\) that are correlated with \(S\). The prior knowledge about \(A\), \(B\), and \(S\) of the different parties derives from a single tripartite state, but each party has the reduced state for only those systems contained in his or her circle. Alice performs a measurement on \(A\) (represented by a POVM \(\{E_a\}\)) with outcome \(a\), and updates her state for \(S\) to \(\alpha\). Bob does likewise, \textit{mutatis mutandis}. Oswald, the overseer, learns everything known to Alice and Bob and updates his state to \(\omega\). Penelope, the pooler, learns only the manner in which Alice and Bob update their states. The question we address is: what state should she assign to \(S\)?]
The pooler, Penelope, is not given any information about what measurements are made by Alice and Bob, nor their outcomes. Rather, she is told only the identity of the initial quantum state for $S$ as well as the quantum states that Alice and Bob assign to $S$ at the end of their measurements. In other words, the pooler is given only $\rho$, $\alpha$, and $\beta$. Her task is to “pool” the information contained in $\alpha$ and $\beta$ (and possibly also $\rho$) to obtain a single quantum state that will represent what she predicts about the outcomes of future experiments on $S$.

By analogy with the classical case, we expect that the quantum pooling problem only has a solution when Alice’s and Bob’s data satisfy some condition of independence. Although we do not determine the most general condition here, we do illustrate two simple cases in which the quantum pooling problem can be solved. Case 1 is where $W$ is a pure tripartite state. Case 2 is where $W$ is a separable mixed state of the form $W = \sum_s p(s) (\sigma_s \otimes \tau_s \otimes |s\rangle \langle s|)$, where the $|s\rangle$ are orthonormal vectors on $W$ and the $\sigma_s$ and $\tau_s$ are normalized (possibly mixed) quantum states defined on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

We show that in both cases, Oswald’s quantum state $\omega$ can be written as a simple function of $\alpha$, $\beta$, and $\rho$, namely,

$$\omega \propto \alpha \rho^{-1} \beta \quad (2.1)$$

$$= \beta \rho^{-1} \alpha, \quad (2.2)$$

where $\rho^{-1}$ is the inverse of $\rho$ on its support $|\Psi\rangle$. To obtain the precise form of $\omega$, one need only normalize the right-hand side of this expression. Penelope can obviously construct this state, and so in these cases, she succeeds in the pooling task.

A. Case 1

Let the dimension of $\mathcal{H}^X$ be denoted $d_X$, where $X = A, B, S$, and suppose that $W \equiv |\Psi\rangle \langle \Psi|$.

By the Choi-Jamiolkowski isomorphism $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \sum_{e,f} \sum_{i=1}^{d_A} \sum_{f=1}^{d_B} |e,f\rangle \otimes (\sqrt{\rho} U |e,f\rangle). \quad (2.3)$$

Here $\{|e,f\rangle\}$ is a complete orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$, and $U$ is an isometry from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_S$ (i.e., $U^\dagger U = I^A \otimes I^B$). In the case that $d_A = d_B = d$, $U$ can be represented by a unitary operator $U$.

Alice’s generalized measurement can be represented by a positive-operator-valued-measure (POVM) $\{E_a\}$. If she gets result $a$ then the relevant POVM element (also called an effect) is the positive operator $E_a \otimes I$ on $\mathcal{H}_A \otimes \mathcal{H}_B$. She updates her description of $S$ from $\rho$ to

$$\alpha \propto \text{Tr}_{AB}[\{E_a \otimes I\}|\Psi\rangle \langle \Psi|] \quad (2.4)$$

$$= \sum_{e,f \neq e,f'} \langle e', f' | E_a \otimes I | e, f \rangle \sqrt{\rho} U |e, f\rangle \langle e', f'| U^\dagger \sqrt{\rho}$$

$$= \sqrt{\rho} U (E_a \otimes I)^T U^\dagger \sqrt{\rho}, \quad (2.5)$$

where $A^T$ is the transpose of $A$ in the basis $|e, f\rangle$ and where we have made use of the completeness of this basis. Note that the update rule for indirect measurements has the POVM element sandwiched between square roots of the state. This is the opposite of what occurs with direct measurements where the state is typically sandwiched between square roots of the POVM element. Eq. (2.5) is the generalization of the Hughston-Jozsa-Wootters theorem $[8]$ to POVM measurements $[10, 11]$. The trace of the right-hand-side of Eq. (2.5) is the probability for Alice to have obtained the result she did, and $\alpha$ is simply the right-hand-side divided by this quantity.

Similarly, if the POVM that Bob measures is $\{F_b\}$, the effect corresponding to the result $b$ is

$$I \otimes F_b \quad (2.6)$$

Then he updates his description of $S$ from $\rho$ to

$$\beta \propto \sqrt{\rho} U (I \otimes F_b)^T U^\dagger \sqrt{\rho}. \quad (2.7)$$

The overseer, upon being told Alice’s and Bob’s outcomes, updates his description of $S$ from $\rho$ to

$$\omega \propto \sqrt{\rho} U (E_a \otimes F_b)^T U^\dagger \sqrt{\rho}. \quad (2.8)$$

It follows from the above results that

$$\omega \propto \sqrt{\rho} U (I \otimes F_b)^T (E_a \otimes I)^T U^\dagger \sqrt{\rho} \quad (2.9)$$

Here we have made use of the fact that $U^\dagger U$ is the identity operator on $\mathcal{H}_A \otimes \mathcal{H}_B$, the fact that $(AB)^T = B^T A^T$, and the fact that $\sqrt{\rho} \rho^{-1} \sqrt{\rho}$ is the identity operator on $\mathcal{H}^S$. This last fact presumes that $\rho$ has full rank on $\mathcal{H}^S$. If this is not the case, we can simply redefine $\mathcal{H}^S$ to be the support of $\rho$ and repeat the proof.

Thus we have shown that Penelope should pool the states according to Eq. (2.1). The proof of the second identity (2.2) is identical, except that the order of $(I \otimes F_b)$ and $(E_a \otimes I)$ (which commute) is inverted in the first line of Eq. (2.3).

B. Case 2

In case 2, the joint quantum state is a separable mixed state of the form

$$W = \sum_s p(s) (\sigma_s \otimes \tau_s \otimes |s\rangle \langle s|). \quad (2.10)$$
It follows that the initial state of system $S$ is
\begin{equation}
\rho = \sum_s p(s) |s\rangle \langle s|.
\end{equation}

When Alice's measurement reveals the outcome associated with the effect $E_a \otimes I$, she updates her description of $S$ to
\begin{equation}
\alpha = \sum_s p(a|s) |s\rangle \langle s|,
\end{equation}
where
\begin{equation}
p(s|a) \propto p(s) \text{Tr}_A(E_a \sigma_s).
\end{equation}

Similarly, when Bob's measurement reveals the outcome associated with the effect $I \otimes F_b$, he updates his description of $S$ to
\begin{equation}
\beta = \sum_s p(b|s) |s\rangle \langle s|,
\end{equation}
where
\begin{equation}
p(s|b) \propto p(s) \text{Tr}_B(F_b \tau_s).
\end{equation}

Oswald, upon learning $a$ and $b$, updates his description to
\begin{equation}
\omega = \sum_s p(s|a,b) |s\rangle \langle s|,
\end{equation}
where
\begin{equation}
p(s|a,b) \propto p(s) \text{Tr}_A(E_a \sigma_s) \text{Tr}_B(F_b \tau_s).
\end{equation}

Noting that $p(s|a,b) \propto p(s|a)p(s|b)/p(s)$ and that $\alpha$, $\beta$, and $\rho$ commute, it follows that Penelope can construct $\omega$ from $\alpha$, $\beta$, and $\rho$ according to Eq. (2.1) or Eq. (2.2).

C. Other cases

It is not difficult to show that Eq. (2.1) does not hold for arbitrary $W$. It suffices to consider the tripartite state $W = \sum_{a,b,s} q(a,b,s) |a\rangle \langle a| \otimes |b\rangle \langle b| \otimes |s\rangle \langle s|$, where $|a\rangle$, $|b\rangle$, and $|s\rangle$ form orthonormal bases for systems $A$, $B$ and $S$. For the case of measurements $E_a = |a\rangle \langle a|$ and $F_b = |b\rangle \langle b|$, it is clear that the problem becomes essentially classical. Specifically, Eqs. (2.12), (2.14) and (2.16) hold, but where $p(s)$, $p(s|a)$, $p(s|b)$ and $p(s|a,b)$ are now defined from $q(a,b,s)$. Given that $\alpha$, $\beta$, and $\rho$ commute, the condition for the quantum pooling formula, $\omega \propto \alpha \rho^{-1} \beta$, to hold is that the classical pooling formula, $p(s|a,b) \propto p(s|a)p(s|b)/p(s)$, holds. However, as mentioned in the introduction, there are joint probability distributions $q(a,b,s)$ for which the latter fails. The following is an example.

Consider the case where the domain of $a$, $b$ and $s$ is the real line, so that sums are replaced by integrals. Let
\begin{equation}
q(a,b,s) = G(s; 0, \sigma^2)G(b; s, \Delta^{-2})G(a; b, \infty),
\end{equation}
where $G(x; \bar{x}, \sigma^{-2})$ is a Gaussian distribution in $x$ with mean $\bar{x}$ and variance $\sigma^{-2}$. Eq. (2.18) describes a situation where the system is described by a Gaussian random variable $s$ with zero mean and variance $\sigma^{2}$, where $b$ is a noisy copy of $s$, with the noise having a variance of $\Delta^{2}$, and where $a$ is a perfect copy of $b$ (because $G(x; y, \infty) = \delta(x-y)$ is the Dirac delta-function). It is easy to verify that
\begin{equation}
p(s|a,b) = p(s|a) = p(s|b) = G(s; b, \sigma^{-2} + \Delta^{-2}),
\end{equation}
where $b = a$ (otherwise, $p(s|a,b)$ is not well-defined). On the other hand, the classical pooling formula (1.2) yields
\begin{equation}
\frac{p(s|a)p(s|b)}{p(s)} = \frac{G(s; b, 2\sigma^{-2} + 2\Delta^{-2})}{G(s; 0, \sigma^{-2})} \propto G(s; b', \sigma^{-2} + 2\Delta^{-2})
\end{equation}
where $b' \neq b$ unless $b = 0$. Clearly this is different from $p(s|a,b)$, and in particular it is always narrower. Intuitively, the reason that such a narrowing (representing an increase in certainty about $s$) is spurious is that it counts the same data twice.

It is clear therefore that Eq. (2.1) does not hold in general. Nonetheless, it is likely that there are other choices of $W$, besides the two we have considered above, for which Eq. (2.1) holds true. We leave identifying the most general form of $W$ for which this is the case as a problem for future research.

D. The connection to compatibility

Two classical probability distributions are compatible if and only if their supports on the space of hypotheses (the regions to which they assign non-zero probability) have some overlap. The same concept was applied to quantum states by Brun, Finkelstein and Mermin (BFM) [1]: two quantum states are compatible if and only if the intersection of their supports on the Hilbert space is not null [18]. This condition is equivalent to the requirement that one can find a quantum state that appears with non-zero weight in some convex decomposition of $\alpha$ and also in some convex decomposition of $\beta$. Specifically, there must exist a state $\omega$ and nonzero weights $p$ and $q$ such that
\begin{equation}
\alpha = p\omega + (1-p)\alpha', \quad \beta = q\omega + (1-q)\beta'
\end{equation}
for some states $\alpha'$ and $\beta'$.

It is easy to verify that a pair of quantum states for $S$ that are acquired by indirect measurements (that is, by measurements of systems $A$ and $B$ that are correlated with $S$) are compatible according to the BFM criteria. It suffices to note that as Eqs. (2.5), (2.7) and (2.8), or as Eqs. (2.12), (2.14) and (2.16), one can infer that there exist nonzero probabilities $p$ and $q$ such that $\alpha - p\omega \geq 0$ and $\beta - q\omega \geq 0$, which in turn implies that there exist quantum states $\alpha'$ and $\beta'$ satisfying Eq. (2.22).
This also demonstrates that $\omega$ lies in the intersection of the supports of Alice’s and Bob’s states. Consequently, $\omega$ is incompatible with all states that are incompatible with either Alice’s or Bob’s states. This requirement for pooling has been previously emphasized by Jacobs and by Herbut.

E. Generalization to an arbitrary number of parties

The above results of Secs. II A and II B are straightforward to generalize to an arbitrary number $N$ of parties: Alice, Bob, $\ldots$, Zane. In the context of classical probability theory, if the parties’ data is conditionally independent,

$$p(a, b|s) = p(a|s)p(b|s)\cdots p(z|s)$$

(2.23)

then

$$p(s|a, b, \ldots, z) \propto \frac{p(s|a)p(s|b)\cdots p(s|z)}{p(s)^{N-1}}$$

(2.24)

The quantum pooling formula for $N$ parties, which is the generalization of Eq. (2.1), is

$$\omega = \alpha \rho^{-1}\beta \rho^{-1} \cdots \rho^{-1} \zeta,$$

(2.25)

where $\zeta$ is Zane’s posterior quantum state. By proofs analogous to those presented for the 2-party case, this formula can be shown to apply if the initial $N$-partite quantum state $W$ is pure or of the form $W = \sum_s p(s) (\alpha_s \otimes \beta_s \otimes \cdots \otimes \zeta_s \otimes |s\rangle\langle s|)$.

III. DISCUSSION

Assuming quantum states are states of knowledge, one should sometimes be able to pool the quantum states of different observers. We have argued that it is critical to determine whether, from the prior quantum state and Alice’s and Bob’s posterior quantum states, one can reconstruct the quantum state that would be assigned by an overseer who knew all the details of the experiment and was given all of the data. If this is the case, then the pooled quantum state is simply the state assigned by the overseer. We have considered the scenario wherein Alice and Bob acquire their data by indirect measurements on the system, specifically, by measurements upon distinct ancillas, and have shown two forms of the initial tripartite state for which the pooler can reconstruct the state of the overseer. Finally, we have demonstrated the connection to the notion of compatibility and the generalization to multiple parties.

In the introduction, we noted that conditional independence of Alice’s and Bob’s data, Eq. (1.1), is a sufficient condition for the applicability of the classical pooling formula, Eq. (1.2). It is not, however, a necessary condition. It follows that in seeking the most general conditions under which the quantum pooling formula holds, one is not simply seeking a quantum analogue of conditional independence. Further investigations into these issues are underway.

Acknowledgments

The authors acknowledge stimulating discussions with Robin Blume-Kohout, Todd Brun, Kurt Jacobs, Matt Leifer, and David Poulin. We also acknowledge the organizers of the workshop “Being Bayesian in a Quantum World”, Konstanz, Germany, 2005, where a talk by Todd Brun prompted the current investigation. R.W.S. receives support from the Royal Society and from the European Union through the Integrated Project QAP (IST-3-015848), SCALA (CT-015714), SECOQC, and QIP IRC (GR/S821176/01). H.M.W. is supported by the ARC and the Government of Queensland.

[14] It follows that Alice’s and Bob’s quantum states need not be compatible, rendering the constraints on pooling that one derives from the compatibility constraint inapplicable in this context, a fact which Jacobs acknowledges.
It has previously been considered by Brun, Finkelstein and Mermin [1] in the context of compatibility and by Jacobs [3] in the context of pooling.

The support of an operator $A$ is the span of the eigenspaces of $A$ having non-zero eigenvalue; it is the orthogonal complement of the kernel of $A$. The inverse of $A$ on its support is the operator obtained by replacing the non-zero eigenvalues of $A$ by their inverses.

Actually this case can be assumed without loss of generality: If $d_S > d_{AB}$ then one can redefine $H^S$ to be a $d_{AB}$-dimensional subspace of the original $H_S$ that supports $\rho$. If $d_S < d_{AB}$ then one can add a subspace to $H_S$ so as to increase its dimensionality to $d_{AB}$.

Caves, Fuchs, and Schack, however, dispute the uniqueness of this condition, as well as the one for classical compatibility [12].