Compatible quantum states and inside information

C. M. Caves and R. Schack

2005 August 6

Modified a bit 2005 December 1

One-way inside information added on 2006 June 9

The goal of this document is (i) to reformulate Brun-Finkelstein-Mermin (BFM) compatibility in terms of the notion of inside information, (ii) to formulate the notion of maximal belief as the situation where no other party with BFM-compatible beliefs has any inside information, and (iii) to reformulate the notion of maximal belief as the situation where no other party has one-way inside information.

First we have to recall how to define probabilities in terms of betting odds. If a party is willing to buy or sell the lottery ticket "Pay \$1 if E" for \$$q$, this *defines* that party's probability for event E to be $p(E) = q$. Of course, the same party would be willing to sell a ticket on the same event for any amount $\geq$ \$$q$ or to buy a ticket on the same event for any amount $\leq$ \$$q$.

Now consider two parties, A and B, who assign different probabilities, $p_A(E)$ and $p_B(E)$, to the occurrence of E. Assume for the moment that $p_B(E) \leq p_A(E)$. Clearly, A and B can agree on a bet in which A buys from B a ticket for any amount \$$q$ satisfying $p_B(E) \leq q \leq p_A(E)$, and this is the only sort of transaction regarding E that both parties can agree to. The mutually agreeable bets are characterized by a flow of tickets from lower probability to higher probability.

Now we can define what is meant by inside information. Party B is said to have *inside information* about event E, relative to A, if A is willing to agree to a bet on E that B believes to be a sure win. This occurs in two circumstances: (i) B is certain E cannot occur, while A believes E to be possible, i.e., $p_A(E) > 0 = p_B(E)$, or (ii) B is certain E will occur, while A thinks there is a chance it will not, i.e., $p_A(E) < 1 = p_B(E)$. In the former case, A will agree to buy a ticket for \$$q$ with $0 < q \leq p_A(E)$, and B is certain that he will retain the \$$q$ because E will not occur. In the latter case, A will agree to sell a ticket for \$$q$ with $p_A(E) \leq q < 1$, and B is certain that he will be able to cash the ticket in for \$1 when E occurs. Notice that E is of type (i) if and only if $\neg E$ is of type (ii).

Let's now assume in the standard way that there is an exclusive and exhaustive sample space of primary events (atoms) and that the possible events are sets of atomic events. It would not be unusual for A to have inside information relative to B about one event and for B to have inside information relative to A about another event; indeed, this is precisely what we would expect in many circumstances. There is, however, a more awkward situation in which each party has inside information relative to the other about the same event. This occurs when one party believes the event is certain to occur, and the other believes it is impossible. These are starkly contradictory beliefs, so we refer to this situation as *contradictory inside information*. It is clear that two parties have contradictory inside information if and only if their atomic probability assignments do not overlap.

We are now ready to define compatibility: *N parties have compatible beliefs if there exists a state of belief Z such that no party has any inside information relative to Z.* It follows immediately that the parties have compatible beliefs if and only if the supports of their atomic probability assignments (the support of an atomic probability assignment is the set of atomic alternatives that have nonzero probability) have nonempty intersection and thus that this is a simple reformulation of BFM compatibility. To see this, suppose first that there is a Z such that no party has inside information relative to Z. This implies that no party assigns zero probability to any atom to which Z assigns nonzero probability, so the intersection of the parties' supports includes the support of Z's probability assignment. Suppose now that the parties' atomic probabilities have supports with a nonempty intersection. Any probability assignment that is restricted to the intersection can serve as an expression of Z's state of belief, it being clear that no party can assign zero probability to an event to which Z assigns nonzero probability and no party can assign unity probability to an event to which Z assigns subunity probability.

A belief Z defined by a set of compatible beliefs is a candidate belief structure for the situation in which all parties pool their beliefs. We can specialize further to the particular case where Z is an expression of maximal belief: *a state of belief Z is said to be maximal if no other party whose state of belief is compatible with Z has any inside information relative to Z*. It is immediately clear that a belief is maximal if and only if it corresponds to certainty for a particular atom. To see this, notice first that if Z assigned nonzero probability to more than one atom, then an assignment of unity probability to one of these atoms would be compatible and would have inside information relative to Z. Suppose now that Z is certain about the occurrence of a particular atom. Any compatible belief must assign nonzero probability to that atom, thus ruling out having any inside information.

All this generalizes straightforwardly to quantum mechanics. The only differences are that states of belief are translated into density-operator assignments instead of probabilities and that when we talk about one party's having inside information relative to another, we are thinking about all possible measurements. Thus we define compatible beliefs and maximal beliefs in exactly the same way as above, keeping in mind only these two differences in what the definitions mean.

Let's deal first with compatibility from this point of view. To make our task easier, we introduce the notation that $\mathcal{N}(\rho)$ and $\mathcal{S}(\rho)$ denote the null subspace and support of a density operator ρ. We want to show that the beliefs of N parties, expressed in density operators ρ_α, $\alpha = 1, \ldots, N$, are compatible if and only if the intersection of the supports $\mathcal{S}(\rho_\alpha)$ is nontrivial, i.e., not zero-dimensional. We thus demonstrate that this notion of compatibility is a rewrite of BFM compatibility. It is useful to recall that the intersection of the supports is the orthocomplement of the span of union of the null subspaces.

Suppose first that there is a state of belief Z, represented by density operator σ, such that no party has any inside information relative to Z. Assume that $\mathcal{N}(\rho_\alpha)$ is not contained in $\mathcal{N}(\sigma)$. This implies that there is a vector $|\phi\rangle \in \mathcal{N}(\rho_\alpha)$ that is not in $\mathcal{N}(\sigma)$ and thus not orthogonal to $\mathcal{S}(\sigma)$. Considered as an outcome of a measurement, $|\phi\rangle$ has zero probability according to party α and nonzero probability according to Z, thus giving party α inside information about this outcome. We can conclude that the null subspaces of all the parties—and, hence, also the span of these null spaces—is contained in $\mathcal{N}(\sigma)$ and thus that the intersection of the supports $\mathcal{S}(\rho_\alpha)$ contains the nontrivial subspace $\mathcal{S}(\sigma)$.

Suppose now that the intersection of the supports $\mathcal{S}(\rho_\alpha)$ is a nontrivial subspace $\mathcal{S}$, and let Z be any state of belief whose density operator has support $\mathcal{S}$. A measurement outcome that has zero probability according to party α must correspond to a POVM element that is orthogonal to $\mathcal{S}(\rho_\alpha)$. The POVM element is thus orthogonal to $\mathcal{S}$ and has zero probability according to Z. A measurement outcome that has unit probability according to party α must have a POVM element that is the sum of the projector onto $\mathcal{S}(\rho_\alpha)$ and a POVM element orthogonal to $\mathcal{S}(\rho_\alpha)$. The outcome thus has unit probability according to Z. We conclude that no party has inside information relative to Z.

It might be a tiny surprise that we can phrase BFM compatibility in this way. At first sight it might seem that the requirement of no inside information for all measurements means only that for all measurements, the supports of the parties' probabilities have nonempty intersection. This is the requirement for post-Peierls (PP) compatibility, so it's clear that it cannot give BFM compatibility. The difference is that PP compatibility doesn't care whether the overlapping supports for different measurements are consistent with a single density operator, whereas for BFM compatibility such consistency is required. This is a nice way of phrasing the difference between BFM and PP compatibility.

We're now ready for maximal beliefs, and we want to show that a state of belief is maximal if and only if it corresponds to a pure state. This is really easy. Notice first that if $\mathcal{S}(Z)$ were more than one-dimensional, any assignment of a pure state in $\mathcal{S}(Z)$ would be compatible and would have inside information relative to Z. Suppose now that Z assigns a pure state $|\psi\rangle$. Any compatible belief must assign a density operator whose support contains $|\psi\rangle$, thus ruling out having any inside information by the argument above.

So at last we have come to a suitable Bayesian way of encapsulating the property that is shared by unit probability for a classical atomic alternative and quantum pure states: both are the unique expression of the firm belief that compatible belief structures have no inside information.

So far, this document has proceeded by first defining compatible beliefs and then defining maximal beliefs in terms of compatible beliefs, but we can instead go straight to maximal beliefs by defining what might be called one-way inside information. To define this notion, consider two parties, A and B, who assign density operators ρ_A and ρ_B, with supports $\mathcal{S}_A$ and $\mathcal{S}_B$ and null subspaces $\mathcal{N}_A$ and $\mathcal{N}_B$. The key result we need is that B has inside information relative to A if and only if $\mathcal{S}_A$ is not a subset of $\mathcal{S}_B$.

To prove this result in the forward direction, assume that $\mathcal{S}_A$ is not a subset of $\mathcal{S}_B$, which implies that $\mathcal{N}_B$ is not a subset of $\mathcal{N}_A$. Thus there exists a state vector $|\phi\rangle \in \mathcal{N}_B$ that is not in $\mathcal{N}_A$. Considered as an outcome of a measurement, $|\phi\rangle$ has zero probability according to B and nonzero probability according to A, thus giving B inside information about this outcome.

To prove the key result in the opposite direction, assume that $\mathcal{S}_A$ is a subset of $\mathcal{S}_B$. A measurement outcome that has zero probability according to B must correspond to a POVM element that is orthogonal to $\mathcal{S}_B$. The POVM element is thus orthogonal to $\mathcal{S}_A$ and has zero probability according to A. A measurement outcome that has unit probability according to B must have a POVM element that is the sum of the projector onto $\mathcal{S}_B$ and a POVM element orthogonal to $\mathcal{S}_B$. The outcome thus has unit probability according to A. We conclude that B does not have inside information relative to A and, hence, that if B does have inside information relative to A, then $\mathcal{S}_A$ is not a subset of $\mathcal{S}_B$.

We can now introduce the notion of one-way inside information. We say that B has *one-way inside information* relative to A if B has inside information relative to A, but A does not have inside information relative to B. It is a trivial consequence of the key result that B has one-way inside information relative to A if and only if $\mathcal{S}_B$ is a proper subset of $\mathcal{S}_A$.

We now define maximal belief: *a state of belief Z is said to be maximal if no other party has one-way inside information relative to Z.* It is obvious that Z is maximal if and only if the corresponding quantum state is a pure state or, classically, one atomic alternative has probability 1. This way of characterizing maximal belief permits us to say why we have more confidence in the probabilities that come from a pure-state assignment than in classical probabilities or the probabilities from a mixed-state assignment: pure-state probabilities come from a belief structure that is incompatible with any other party having inside information that goes only one way. That's the real content of the statement that we trust a quantum coin toss more than a classical one or a pseudo-random-number generator.

Moreover, we again have a suitable Bayesian way of stating the property that is shared by unit probability for a classical atomic alternative and quantum pure states: both are the unique expression of the firm belief that no other party has one-way inside information.