On the Colbeck–Renner Theorem

Klaas Landsman

Institute for Mathematics, Astrophysics, and Particle Physics
Faculty of Science, Radboud University Nijmegen
landsman@math.ru.nl

November 13, 2015

Abstract
In three papers Colbeck and Renner (Nature Communications 2:411, (2011); Phys. Rev. Lett. 108, 150402 (2012); arXiv:1208.4123) argued that “no alternative theory compatible with quantum theory and satisfying the freedom of choice assumption can give improved predictions.” We give a more precise version of the formulation and proof of this remarkable claim. Our proof broadly follows theirs, which relies on physically well motivated axioms, but to fill in some crucial details certain technical assumptions have had to be added, whose physical status seems somewhat obscure.

1 Introduction
The claim by Colbeck and Renner that “no alternative theory compatible with quantum theory and satisfying the freedom of choice assumption can give improved predictions” [4, 5, 6] has attracted considerable attention (see e.g. the review [10]), some of which has been rather critical [7, 8, 9]. The aim of this paper is to give a watertight proof of their theorem, including a statement of precise, mathematically formulated assumptions.

Our proof broadly follows the dazzling reasoning of Colbeck and Renner, except that some of their theoretical physics style heuristic arguments have been replaced by rigorous mathematics. However, if this had been a routine exercise in mathematical physics we would not have taken the effort. The point of our analysis is to show that additional assumptions are necessary to make the proof work, so that the theorem is weaker than it may appear to be at first sight: it does not show that quantum mechanics is complete, but that (informative) extensions are subject to (possibly undesirable) constraints.

Indeed, apart from three physically natural (and unavoidable) assumptions, namely Compatibility with Quantum Mechanics, Parameter Independence (the latter being a well-known hidden variable version of the no-signaling axiom), and what we call Product Extension, we also need three assumptions that are satisfied by quantum mechanics itself but might seem somewhat unnatural if imposed on a hidden variable theory, viz. Continuity of Probabilities, Unitary Invariance, and what we call Schmidt Extension. We also replaced the original probabilistic setting, in which almost everything (including even the quantum state) was treated as a random variable, by a more conventional hidden variable theory perspective (which circumvents some unnecessary controversies [7, 11]). Our approach differs significantly from interesting recent work of Leegwater [9], which has a similar goal.
2 Notation

A hidden variable theory \( \mathcal{T} \) underlying quantum mechanics yields probabilities

\[
P(Z_1 = z_1, \ldots, Z_n = z_n|\lambda) \equiv P(\vec{Z} = \vec{z}|\lambda)
\]

for the possible outcomes \( \vec{z} = (z_1, \ldots, z_n) \) of a measurement of any family \( \vec{Z} = (Z_1, \ldots, Z_n) \) of commuting hermitian operators on any Hilbert space \( H \) (here assumed to be finite dimensional for simplicity), given an arbitrary parameter \( \lambda \in \Lambda \) (i.e., the ‘hidden variable’), where \( \Lambda \) is some Borel space\(^1\). Being ‘classical’ probabilities, these numbers are \textit{a priori} only supposed to satisfy \( 0 \leq P(\vec{Z} = \vec{z}|\lambda) \leq 1 \) and \( \sum_{\vec{z}} P(\vec{Z} = \vec{z}|\lambda) = 1 \), where the sum is over all possible outcomes. It will follow from the assumptions below that necessarily \( z_i \in \sigma(Z_i) \) (i.e., the spectrum of \( Z_i \)) for each \( i = 1, \ldots, n \), in the sense that \( P(\vec{Z} = \vec{z}|\lambda) = 0 \) if this is not the case. Families of operators \( \vec{Z}_c \) (all defined on the same \( H \)) are indexed by some parameter \( c \in C \), called the “setting” of the experiment\(^2\).

An important special case will be the bipartite setting \( H = H_1 \otimes H_2 \), where Alice and Bob measure hermitian operators \( X \) and \( Y \) on \( H_1 \) and \( H_2 \), respectively, so that \( n = 2 \), \( Z_1 = X \otimes 1_{H_2} \), and \( Z_2 = 1_{H_1} \otimes Y \). We then write \( z_1 = x \), \( z_2 = y \), and \( c = (a, b) \), so that we typically look at expressions like \( P(X_a = x, Y_b = y|\lambda) \). The other case of interest will simply be \( n = 1 \) with \( Z_1 \equiv Z \), \( z_1 \equiv z \); indeed, this will be the case in the statement of the theorem (the bipartite case playing a role only in the proof, though a crucial one!)

In this paper, quantum-mechanical states will just be unit vectors \( \psi \in H \). The corresponding prediction for the above probabilities, i.e., the ‘Born rule’, is given by \([13]\)

\[
P_\psi(\vec{Z} = \vec{z}) = \langle \psi, E_{\vec{Z}}(\vec{z})\psi \rangle,
\]

(2.1)

where \( E_{\vec{Z}}(\vec{z}) = \prod_{i=1}^n E_{Z_i}(z_i) \), in which \( E_{Z_i}(z_i) \) is the spectral projection on the eigenspace \( H_{z_i} \subset H \) of \( Z_i \) (i.e., \( Z_i\psi = z_i\psi \) iff \( \psi \in H_{z_i} \)). As detailed in \([13]\) \( \mathcal{T} \) assigns a probability measure \( \mu_\psi \) on \( \Lambda \) to each state \( \psi \). The following notation occurs throughout the paper:

\[
P_\psi(\vec{Z} = \vec{z}|\lambda) = \alpha(\lambda),
\]

(2.2)

with \( \alpha : \Lambda \to [0,1] \) an explicitly given measurable function (often constant). This means\(^3\)

\[
P(\vec{Z} = \vec{z}|\lambda) = \alpha(\lambda) \quad \text{for almost every } \lambda \quad \text{with respect to the measure } \mu_\psi
\]

Since this notation renders equalities like

\[
P_\psi(\vec{Z} = \vec{z}|\lambda) = P_\varphi(\vec{Z}' = \vec{z}'|\lambda),
\]

(2.3)

ambiguous (where \( \psi, \varphi \) are states in \( H \)), we explicitly define \((2.3)\) as the double implication

\[
P_\psi(\vec{Z} = \vec{z}|\lambda) = \alpha(\lambda) \iff P_\varphi(\vec{Z}' = \vec{z}'|\lambda) = \alpha(\lambda).
\]

This notation also appears in our final pair of conventions: for \( \varepsilon \to 0 \) we write

\[
\psi \approx \varphi \iff (1 - \varepsilon) \leq |\langle \psi, \varphi \rangle| \leq 1;
\]

(2.4)

\[
P_\psi(\vec{Z} = \vec{z}|\lambda) \approx P_\varphi(\vec{Z}' = \vec{z}'|\lambda) \iff P_\psi(\vec{Z} = \vec{z}|\lambda) = P_\varphi(\vec{Z}' = \vec{z}'|\lambda) + O(\sqrt{\varepsilon}).
\]

(2.5)

\(^1\)This generality, which is not a common feature of hidden variable theories (and as such is already a significant assumption), is necessary for the Colbeck–Renner argument to work.

\(^2\)Colbeck and Renner look at the setting \( c \) as the value of some random variable \( C \), but this is controversial \([11]\); for us, \( C \) is simply the subset in which \( c \) takes values.

\(^3\)Colbeck and Renner treat \( \psi \) as a random variable and hence interpret \( P_\psi(\vec{Z} = \vec{z}|\lambda) \) as a probability conditioned on knowing (that) \( \psi \). We do not do so, yet our mathematical unfolding of \([222]\) is similar.

\(^4\)In other words, there is a subset \( \Lambda' \subset \Lambda \) such that \( \mu_\psi(\Lambda') = 0 \) and \( P_\psi(\vec{Z} = \vec{z}|\lambda) = \alpha(\lambda) \) holds for any \( \lambda \in \Lambda \setminus \Lambda' \). If \( \Lambda \) is finite, this means that the equality holds for any \( \lambda \) for which \( \mu_\psi(\{\lambda\}) > 0 \).
The assumptions in our reformulation of the Colbeck–Renner Theorem are as follows.

**CQ** Compatibility with Quantum Mechanics: for any unit vector \( \psi \in H \), the theory \( T \) yields a state \( \mu_\psi \) (i.e., a probability measure on \( \Lambda \)) such that (cf. (2.1))

\[
\int_{\Lambda} d\mu_\psi(\lambda) P(\vec{Z} = \vec{z}|\lambda) = P_\psi(\vec{Z} = \vec{z}).
\] (3.6)

**UI** Unitary Invariance: for any unit vector \( \psi \in H \) and unitary operator \( U \) on \( H \)

\[
P_{U\psi}(\vec{Z} = \vec{z}|\lambda) = P_\psi(U^{-1}\vec{Z}U = \vec{z}|\lambda).
\] (3.7)

**CP** Continuity of Probabilities: If \( \psi \approx \varphi \), then \( P_\psi(\vec{Z} = \vec{z}|\lambda) \approx P_\varphi(\vec{Z} = \vec{z}|\lambda) \).

In the remaining three axioms, \( H = H_1 \otimes H_2 \), and \( X \) and \( Y \) are hermitian operators on \( H_1 \) and \( H_2 \), respectively (identified with operators \( X \otimes 1_{H_2} \) and \( 1_{H_1} \otimes Y \) on \( H \) as appropriate).

**PI** Parameter Independence:

\[
\sum_{y \in \sigma(Y)} P(X = x, Y = y|\lambda) = P(X = x|\lambda); \quad (3.8)
\]

\[
\sum_{x \in \sigma(X)} P(X = x, Y = y|\lambda) = P(Y = y|\lambda). \quad (3.9)
\]

**PE** Product Extension: for any pair of states \( \psi_1 \in H_1, \psi_2 \in H_2 \),

\[
P_{\psi_1}(X = x|\lambda) = P_{\psi_1 \otimes \psi_2}(X = x|\lambda). \quad (3.10)
\]

**SE** Schmidt Extension: if \( e_i \in H_1 \) \((i = 1, \ldots, \dim(H))\) are eigenstates of \( X \), then for arbitrary orthogonal states \( u_i \in H_2 \) and arbitrary coefficients \( c_i > 0 \) with \( \sum_i c_i^2 = 1 \),

\[
P_{\sum_i c_i e_i}(X = x|\lambda) = P_{\sum_i c_i e_i \otimes u_i}(X = x|\lambda). \quad (3.11)
\]

Comments. All assumptions are satisfied by quantum mechanics itself (seen as a ‘hidden’ variable theory, with the state \( \psi \) as the ‘hidden’ variable \( \lambda \)). In the broader context of hidden variable theories, **CQ** seems unavoidable in any such discussion, and also **PI** and **PE** have convincing physical plausibility. Unfortunately, the other assumptions are purely technical and have solely been invented to carry out certain steps in the proof.

In particular, although **UI**, **CP**, and **SE** represent the essence of quantum mechanics itself, these assumptions are far from self-evident for a hidden variable theory. Moreover, the former two are quite unsatisfactory, in that they do not merely constrain the probabilities \( P(\vec{Z} = \vec{z}|\lambda) \) of \( T \): they rather involve an interplay between these probabilities and the supports of the measures \( \mu_\psi \) and \( \mu_{U\psi} \). We challenge the reader to economize this!

---

\(^3\)As the notation indicates, \( \mu_\psi \) depends on \( \psi \) only and hence is independent of \( Z \) and \( z \). From the point of view of \( T \), a quantum state is a probability measure on \( \Lambda \), so one might even write \( \psi \) for \( \mu_\psi \).

\(^6\)This assumption may be replaced by its main consequence, i.e., Lemma [1.2] below.

\(^7\)In words, this assumptions states that the probabilities for Alice’s measurement outcomes, given \( \lambda \), are not only independent of Bob’s choice of his observable \( Y \), but are even independent of his existence altogether, as they are given by the expression that \( T \) yields for Alice’s experiment alone (and likewise for Bob). This slightly generalizes the usual Parameter Independence in the context of Bell’s Theorem [3]. Note that in our form **PI** only makes sense because (2.1) and (3.6) imply that for \( P_\psi(\vec{Z} = \vec{z}|\lambda) \) to be nonzero (in the sense of (2) we must have \( z_i \in \sigma(Z_i) \) for each \( i \).
4 Theorem and proof

Our reformulation of the Colbeck–Renner Theorem, then, is as follows.

**Theorem 4.1** If some hidden variable-theory $\mathcal{T}$ satisfies CQ, UI, CP, PI, PE, and SE, then for any (finite-dimensional) Hilbert space $H$, state $\psi \in H$, and observable $Z$ on $H$,

$$P_{\psi}(Z = z|\lambda) = P_{\psi}(Z = z).$$

(4.12)

We first assume (without loss of generality) that $Z$ is nondegenerate as a hermitian matrix, in that it has distinct eigenvalues $(z_1, \ldots, z_{\dim(H)})$. This assumption will be justified at the end of the proof. The proof consists of three steps:

1. The theorem holds for $H = \mathbb{C}^2$ and any pair $(Z, \psi)$ for which

$$P_{\psi}(Z = z_1) = P_{\psi}(Z = z_2) = 1/2.$$  

(4.13)

This only requires assumptions CQ, PI, and SE.

2. The theorem holds for $H = \mathbb{C}^l$, $l < \infty$ arbitrary, and any pair $(Z, \psi)$ for which

$$P_{\psi}(Z = z_1) = \cdots = P_{\psi}(Z = z_l) = 1/l.$$  

(4.14)

This is just a slight extension of step 1 and uses the same three assumptions.

3. The theorem holds in general. This requires all assumptions (as well as step 2).

The first step is mathematically straightforward but physically quite deep, depending on chained Bell inequalities [2], and is due to [6] (we will give a slightly simplified proof below). The second step is easy. The third step, relying on the technique of embezzlement [12], is highly nontrivial. This is step that our analysis mainly attempts to clarify.

**Step 1**

Let $H = \mathbb{C}^2$, with basis $(e_1, e_2)$ of eigenvectors of $Z$, so that $\psi \in \mathbb{C}^2$ may be written as

$$\psi = (e_1 + e_2)/\sqrt{2}.$$  

(4.15)

Without loss of generality, we may assume that $z_1 = 1$ and $z_2 = -1$. We now relabel $Z$ as $Z_0$ and extend it to a family of operators $(Z_k)_{k=0,1,\ldots,2N-1}$ by fixing an integer $N > 1$, putting $\theta_k = k\pi/2N$, and defining

$$Z_k = [\theta_{k+\pi}] - [\theta_k],$$  

(4.16)

where, for any angle $\theta \in [0, 2\pi]$, the operator $[\theta] = |\theta\rangle\langle\theta|$ is the orthogonal projection onto the subspace (ray) spanned by the unit vector

$$|\theta\rangle = \sin(\theta/2) \cdot e_1 + \cos(\theta/2) \cdot e_2.$$  

(4.17)

In the corresponding bipartite setting, we have observables $X_k \equiv Z_k \otimes 1_2$ and $Y_k \equiv 1_2 \otimes Z_k$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$, as well as a maximally correlated (Bell) state $\psi_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$, given by

$$\psi_{AB} = \frac{1}{\sqrt{2}}(e_1 \otimes e_1 + e_2 \otimes e_2).$$  

(4.18)
Using assumptions PI and SE, we then have, for $i = 1, 2$ $z_1 = 1$, and $z_2 = -1$,

$$P_\psi(Z = z_i|\lambda) = P_{\psi_{AB}}(X_0 = z_i|\lambda).$$  \hspace{1cm} (4.19)

The quantum-mechanical prediction is

$$P_{\psi_{AB}}(X_0 = 1) = P_{\psi_{AB}}(X_0 = -1) = \frac{1}{2}. \hspace{1cm} (4.20)$$

As in [9], our goal is to show that also

$$P_{\psi_{AB}}(X_0 = 1|\lambda) = P_{\psi_{AB}}(X_0 = -1|\lambda) = \frac{1}{2}. \hspace{1cm} (4.21)$$

To this effect we introduce the combination of probabilities

$$I^{(N)}(\lambda) = P(X_0 = Y_{2N-1}|\lambda) + \sum_{a \in A_N, b \in B_N, |a-b|=1} P(X_a \neq Y_b|\lambda), \hspace{1cm} (4.22)$$

where $A_N = \{0, 2, \ldots, 2N-2\}$ and $B_N = \{1, 3, \ldots, 2N-1\}$. The inequality \[9\]

$$|P(X_a = x_i|\lambda) - P(Y_b = x_i|\lambda)| = |P(X_a = x_i, Y_b = x_i|\lambda) + P(X_a = x_i, Y_b \neq x_i|\lambda) - P(X_a \neq x_i, Y_b = x_i|\lambda) - P(X_a \neq x_i, Y_b \neq x_i|\lambda)| \leq P(X_a \neq x_i, Y_b \neq x_i|\lambda)$$

where $i = 1, 2$, and we used PI, implies a further inequality: since $X_{2N} = -X_0$,

$$|P(X_0 = 1|\lambda) - P(X_0 = -1|\lambda)| = |P(X_0 = 1|\lambda) - P(X_{2N} = 1|\lambda)| \leq \sum_{a,b,|a-b|=1} |P(X_a = 1|\lambda) - P(Y_b = 1|\lambda)|$$

Integrating this with respect to the measure $\mu_{\psi_{AB}}$ and using CQ gives

$$\int_\Lambda d\mu_{\psi_{AB}}(\lambda) |P(X_0 = 1|\lambda) - P(X_0 = -1|\lambda)| \leq \int_\Lambda d\mu_{\psi_{AB}}(\lambda) I^{(N)}(\lambda) = I_{\psi_{AB}}^{(N)}.$$

A routine calculation shows that the quantum-mechanical prediction $I_{\psi_{AB}}^{(N)}$ is given by

$$I_{\psi_{AB}}^{(N)} = 2N \sin^2(\pi/4N), \hspace{1cm} (4.25)$$

so that

$$\lim_{N \to \infty} I_{\psi_{AB}}^{(N)} = 0. \hspace{1cm} (4.26)$$

Letting $N \to \infty$ in (4.21) therefore yields (4.21). From (4.19) we then obtain (4.13).
Step 2

Let $H = \mathbb{C}^l$ and let $(e_i)_{i=1}^l$ be an orthonormal basis of eigenvectors of $Z$, with corresponding eigenvalues $z_i$, and phase factors for the eigenvectors $e_i$ such that $c_i > 0$ in the expansion

$$\psi = \sum_i c_i e_i. \quad (4.27)$$

Of course, $\sum_i c_i^2 = 1$. The case of interest will be $c_1 = \cdots = c_l / l$, but first we merely assume that $c_1 = c_2$ (the same reasoning applies to any other pair), with $z_1 = 1$ and $z_2 = -1$ (which involves no loss of generality either and just simplifies the notation). The other coefficients $c_i (i > 2)$ may or may not be equal to $c_1$.

Generalizing (4.21), we will show that

$$P_\psi (Z = 1 | \lambda) = P_\psi (Z = -1 | \lambda). \quad (4.28)$$

This shows that if two Born probabilities defined by some quantum state $\psi$ are equal, then the underlying hidden variable probabilities (conditioned on $\psi$) must be equal, too. Eq. (4.14) immediately follows from this result by taking all $c_i$ to be equal.

Given step 1, the derivation of (4.28) is a piece of cake. We again pass to the bipartite setting, introducing two copies $H_A = H_B = \mathbb{C}^l$ of $H$, and define the correlated state

$$\psi_{AB} = \sum_i c_i \cdot e_i \otimes e_i \quad (4.29)$$

in $H_A \otimes H_B$. Eq. (4.19) again follows from assumptions PI and SE. Throughout the argument of step 1, we now replace each probability $P(X_a = x, Y_b = y | \lambda)$ by a corresponding probability $P^{(1)}(X_a = x, Y_b = y | \lambda)$, defined as the conditional probability

$$P^{(1)}(X_a = x, Y_b = y | \lambda) = \frac{P(X_a = x, Y_b = y | |x| = |y| = 1, \lambda)}{P(|x| = |y| = 1 | \lambda)}, \quad (4.30)$$

for all $\lambda$ for which $P(|x| = |y| = 1 | \lambda) > 0$, whereas

$$P^{(1)}(X_a = x, Y_b = y | \lambda) = 0 \quad (4.31)$$

whenever $P(|x| = |y| = 1 | \lambda) = 0$. The same argument then yields (4.21), with $P$ replaced by $P^{(1)}$ but with the same right-hand side; see \[7\] §3.2 for this calculation. As in step 1,

$$P_{\psi_{AB}}^{(1)}(X_0 = 1 | \lambda) = P_{\psi_{AB}}^{(1)}(X_0 = -1 | \lambda), \quad (4.32)$$

which implies that

$$P_{\psi_{AB}}(X_0 = 1 | \lambda) = P_{\psi_{AB}}(X_0 = -1 | \lambda), \quad (4.33)$$

either because both sides vanish (if $P(|x| = |y| = 1 | \lambda) = 0$), or because (in the opposite case) the denominator $P(|x| = |y| = 1 | \lambda)$ cancels from both sides of (4.32).

Combined with (4.19), eq. (4.33) proves (4.28) and hence establishes step 2.
Step 3

We continue to use the notation established at the beginning of step 2, especially (4.27). As in step 1, we introduce two copies $H_A = H_B = \mathbb{C}^d$ of $H$, as well as two states

$$\psi_{AB} = \sum_i c_i \cdot e_i \otimes e_i \in H_A \otimes H_B; \quad (4.34)$$

$$\psi''_{AB} = \kappa_n \otimes \epsilon'_i \otimes \epsilon'_i \otimes \psi_{AB} \in H''_A \otimes H''_B; \quad (4.35)$$

where $\kappa_n$ is given by (A.69), $H'' = H'' \otimes H' \otimes H$, and we have notationally ignored the obvious permutations of factors in the tensor product.

For any $\varepsilon > 0$ and given coefficients $c_i$, pick $\epsilon'_i$ in $\mathbb{R}^+$ such that $(\epsilon'_i)^2 \in \mathbb{Q}^+$ and

$$|\epsilon'_i - c_i| < \varepsilon / \dim(H), \quad (4.36)$$

which implies that, in the sense of (2.4), $\sum_i \epsilon'_i e_i \approx \sum_i c_i e_i$. Suppose $\epsilon'_i = \sqrt{p_i/q_i}$, with $p_i, q_i \in \mathbb{N}$ and $\gcd(p_i, q_i) = 1$, and define

$$m_i = p_i \prod_{i' \neq i} q_{i'} \quad (4.37)$$

Consequently, writing $q = 1/\sqrt{\sum_i m_i'}$, the following quotient is independent of $i$:

$$\frac{\epsilon'_i}{\sqrt{m_i}} = q. \quad (4.38)$$

Given the integers $m_i$ thus obtained, we define a unitary operator $U : H'' \rightarrow H''$ by

$$U = \sum_{i=1}^l U^{(m_i)} \otimes P_i, \quad (4.39)$$

where $P_i : H \rightarrow H$ projects onto $e_i$ (that is, $P_i = |e_i\rangle\langle e_i|$ in physics notation) and $U^{(m_i)}$ is defined in (A.66). From this definition (with additional labels to denote the copies $U_A : H''_A \rightarrow H''_A$ and $U_B : H''_B \rightarrow H''_B$) and (A.71) and (4.36), we then obtain the relations

$$1_{H''_A} \otimes 1_{H''_B}(\psi''_{AB}) = \kappa_n \otimes \sum_{i=1}^l c_i \cdot \epsilon''_{iAA'} \otimes \epsilon''_{iBB'}; \quad (4.40)$$

$$U_A \otimes 1_{H''_B}(\psi''_{AB}) = \frac{1}{\sqrt{C(n)}} \sum_{i=1}^l \sum_{k=1}^n \frac{c_i}{e_{ak} \otimes e''_{ik} \otimes \epsilon''_{iAA'} \otimes \epsilon''_{iBB'}}; \quad (4.41)$$

$$1_{H''_A} \otimes U_B(\psi''_{AB}) = \frac{1}{\sqrt{C(n)}} \sum_{i=1}^l \sum_{k=1}^n \frac{c_i}{e_{ik} \otimes e''_{sk} \otimes \epsilon''_{iAA'} \otimes \epsilon''_{iBB'};} \quad (4.42)$$

$$U_A \otimes U_B(\psi''_{AB}) \approx q \cdot \kappa_n \otimes \sum_{i=1}^l \sum_{i'=1}^l m_i \cdot \epsilon_{iAA'} \otimes \epsilon_{iBB'} \quad (4.43)$$

Here

$$\epsilon_{ij} = e_i \otimes e_j \in H \otimes H', \quad (4.44)$$
4 THEOREM AND PROOF

with corresponding copies \( \xi_{ij} \in H_A \otimes H'_A \) and \( \xi_{ij} \in H_B \otimes H'_B \); the right-hand sides of (4.40) - (4.43) have been arranged so as to obtain vectors in the six-fold tensor product

\[ H''_A \otimes H''_B \otimes H_A \otimes H'_A \otimes H_B \otimes H'_B. \]

The following (sub)steps are meant to replace (or justify) the core argument of [6]. We repeatedly invoke the following lemma, whose proof just unfolds the notation (which incorporates the identification of \( X \) with \( X \otimes 1_{H_2} \) and of \( Y \) with \( 1_{H_1} \otimes Y \) as appropriate).

**Lemma 4.2** Assume \( \Pi \) and \( \Pi \). For any pair of unitary operators \( U_1 \) on \( H_1 \) and \( U_2 \) on \( H_2 \), and any unit vector \( \psi \in H_1 \otimes H_2 \), one has

\[
P_{U_1 \otimes U_2}(Y = y|\lambda) = P_{\psi}(Y = y|\lambda); \quad (4.45)
\]

\[
P_{U_1 \otimes U_2}(X = x|\lambda) = P_{\psi}(X = x|\lambda), \quad (4.46)
\]

We now introduce some convenient notation. Since we assume that \( Z \) is nondegenerate, there is a bijective correspondence between its eigenvalues \( Z = z_i \) and its eigenvectors \( e_i \).

Instead of \( P(Z = z_i) \) dressed with whatever parameters \( \psi \) or \( \lambda \), we may then write \( P(e_i) \), where \( Z \) is understood, and analogously for the more complicated operators on tensor products of Hilbert space appearing below. We are now in a position to go ahead:

- From Step 2, using the notation explained below (4.27),

\[
P_q \sum_{i=1}^q \sum_{j=1}^{m_i} \xi_{ij}\xi_{ij}^{BB'}(\xi_{BB'}^{ij}|\lambda) = q^2. \quad (4.47)
\]

- From (3.11) in \( \Pi \) and (4.47),

\[
P_q \sum_{i,j} \xi_{ij}\xi_{ij}^{BB'}(\xi_{BB'}^{ij}|\lambda) = q^2. \quad (4.48)
\]

- From (3.10) in \( \Pi \) and (4.48),

\[
P_q \sum_{i,j} \xi_{ij}\xi_{ij}^{BB'}(\xi_{BB'}^{ij}|\lambda) = q^2. \quad (4.49)
\]

- From (4.49), \( \Pi \) (whose notation we use), and (4.43),

\[
P_{U_1 \otimes U_2}(\psi^{ij}_{AB})(\xi_{BB'}^{ij}|\lambda) \approx q^2. \quad (4.50)
\]

- From (4.50) and Lemma 4.2 we have

\[
P_{1_{H''_A} \otimes U_2}(\psi^{ij}_{AB})(\xi_{BB'}^{ij}|\lambda) \approx q^2 (j_i = 1, \ldots, m_i), \quad (4.51)
\]

whereas the definition of the indices in question gives

\[
P_{1_{H''_A} \otimes U_2}(\psi^{ij}_{AB})(\xi_{BB'}^{ij}|\lambda) \approx 0 (j_i = m_i + 1, \ldots, m); \quad (4.52)
\]

here the number \( m \) (satisfying \( m \geq m_i \) for all \( i \)) is introduced in the Appendix.

We now start a different argument, to be combined with (4.51) - (4.52) in due course.
4 THEOREM AND PROOF

- From PE, SE, and \([4.27]\), with \(e^i_A \in H_A\) denoting \(e^i \in H\), we have
  \[P_\psi(Z = z_i|\lambda) = P_\psi(e^i|\lambda) = P_{\kappa_n^2 \otimes \sum_i c_i \xi^{i1}_{AA'} \otimes \xi^{i1}_{BB'}}(e^i_A|\lambda).\] \((4.53)\)

- Using Lemma \([4.2], (4.40),\) and \((4.41)\),
  \[P_{\kappa_n^2 \otimes \sum_i c_i \xi^{i1}_{AA'} \otimes \xi^{i1}_{BB'}}(e^i_A|\lambda) = P_{\kappa'A^2 \otimes U_B(\psi''_{AB})}(e^i_A|\lambda),\] \((4.54)\)
  and hence
  \[P_\psi(Z = z_i|\lambda) = P_{\kappa'A^2 \otimes U_B(\psi''_{AB})}(e^i_A|\lambda).\] \((4.55)\)

- From quantum mechanics, notably \((2.1)\), and \((4.42)\), for any \(i' \neq i\) we have
  \[P_{\kappa'A^2 \otimes U_B(\psi''_{AB})}(e^{i'}_A \otimes \xi^{ij}_{BB'}|\lambda) = 0.\] \((4.56)\)

- From CQ and \((4.56)\), for any \(i' \neq i\),
  \[P_{\kappa'A^2 \otimes U_B(\psi''_{AB})}(e^{i'}_A, \xi^{ij}_{BB'}|\lambda) = 0. \] \((4.57)\)

- From PI,
  \[P(e^i_A|\lambda) = \sum_{i,j} P(e^{i'}_A, \xi^{ij}_{BB'}|\lambda); \] \((4.58)\)
  \[P(\xi^{ij}_{BB'}|\lambda) = \sum_{i'} P(e^{i'}_A, \xi^{ij}_{BB'}|\lambda). \] \((4.59)\)

- From \((4.57), (4.58),\) and \((4.59),\)
  \[P_{\kappa'A^2 \otimes U_B(\psi''_{AB})}(e^i_A|\lambda) = \sum_{j_i} P_{\kappa'A^2 \otimes U_B(\psi''_{AB})}(\xi^{ij}_{BB'}|\lambda). \] \((4.60)\)

Finally, from \((4.55), (4.60), (4.51) - (4.52),\) and \((4.38)\) we obtain
  \[P_\psi(Z = z_i|\lambda) \approx \sum_{j_i}^{m_i} q^2 = m_i \cdot q^2 = (c^i)^2.\] \((4.61)\)

Since \(c_i > 0\) we have \(c_i^2 = |c_i|^2\); using \((4.36)\) and letting \(\varepsilon \to 0\) then proves step 3:
  \[P_\psi(Z = z_i|\lambda) = |c_i|^2 = P_\psi(Z = z_i). \] \((4.62)\)

Finally, we remove our standing assumption that the spectrum of \(Z\) be nondegenerate. In the degenerate case one has
  \[P_\psi(Z = z_i) = \sum_{j_i} P_\psi(e_{j_i}), \] \((4.63)\)
where the sum is over any orthonormal basis \((e_{j_i})_{j_i}\) of the eigenspace of \(z_i\). Since each state \(e_{j_i}\) gives the same numerical outcome \(Z = z_i\), probability theory gives for all \(\lambda,
  \[P(Z = z_i|\lambda) = \sum_{j_i} P(e_{j_i}|\lambda). \] \((4.64)\)

The nondegenerate case of the theorem (which distinguishes the states \(e_{j_i}\)) yields
  \[P_\psi(e_{j_i}|\lambda) = P_\psi(e_{j_i}), \] \((4.65)\)
from which \((4.12)\) follows once again:
  \[P_\psi(Z = z_i|\lambda) = \sum_{j_i} P_\psi(e_{j_i}|\lambda) = \sum_{j_i} P_\psi(e_{j_i}) = P_\psi(Z = z_i). \]
A Embezzlement

We only treat the amazing technique of embezzlement for maximally entangled states (cf. [12] for the general case). We will deal with three Hilbert spaces, namely $H = \mathbb{C}^l$, $H' = \mathbb{C}^m$, and $H'' = \mathbb{C}^n$ (where $n = m^N$ for some large $N$, see below), each with some fixed orthonormal basis $(e_i)_i=1$, $(e'_j)_j=1$, and $(e''_k)_k=1$, respectively. Given a further number $m_i \leq m$, we now list the $nm$ basis vectors $e''_k \otimes e'_j$ of $H'' \otimes H'$ in two different orders:

1. $e''_1 \otimes e'_1, \ldots, e''_1 \otimes e'_1, e''_1 \otimes e'_2, \ldots, e''_1 \otimes e'_m, \ldots, e''_m \otimes e'_1, \ldots, e''_m \otimes e'_m$;

2. $e''_1 \otimes e'_1, \ldots, e''_1 \otimes e'_m, e''_2 \otimes e'_1, \ldots, e''_2 \otimes e'_m, \ldots, e''_m \otimes e'_1, \ldots, e''_m \otimes e'_m$,

where the remaining vectors (i.e., those of the form $e''_k \otimes e'_j$ for $1 \leq k \leq n$ and $j > m_i$) are listed in some arbitrary order.

Define $U^{(m_i)} : H'' \otimes H' \to H'' \otimes H'$ as the unitary operator that maps the first list on the second. We will need the explicit expression

$$U^{(m_i)}(e''_k \otimes e'_j) = e''_{s_k^i} \otimes e'_{j_k^i}, \quad (A.66)$$

where for given $k = 1, \ldots, n$ the numbers $s_k^i = 1, \ldots, n_i$ (where $n_i$ is the smallest integer such that $n im_i \geq n$) and $j_k^i = 1, \ldots, n_i$ are uniquely determined by the decomposition

$$k = (s_k^i - 1)m_i + j_k^i. \quad (A.67)$$

We will actually work with two copies of $H'' \otimes H'$, called $H''_A \otimes H'_A$ and $H''_B \otimes H'_B$, with ensuing copies of $U^{(m_i)}_A$ and $U^{(m_i)}_B$ of $U^{(m_i)}$, and hence, leaving the isomorphism

$$H''_A \otimes H'_A \otimes H''_B \otimes H'_B \cong H''_A \otimes H''_B \otimes H'_A \otimes H'_B$$

implicit, we obtain a unitary operator

$$U^{(m_i)}_A \otimes U^{(m_i)}_B : H''_A \otimes H''_B \otimes H'_A \otimes H'_B \to H''_A \otimes H''_B \otimes H'_A \otimes H'_B. \quad (A.68)$$

The point of all this is that the unit vector $\kappa_n \in H''_A \otimes H''_A$ defined by

$$\kappa_n = \frac{1}{\sqrt{C(n)}} \sum_{k=1}^{n} e''_k \otimes e''_k, \quad (A.69)$$

where $C(n) = \sum_{k=1}^{n} 1/k$, acts as a catalyst in producing the maximally entangled state

$$\varphi = \frac{1}{\sqrt{m_i}} \sum_{j=1}^{m_i} e'_j \otimes e'_j, \quad (A.70)$$

in $H'_A \otimes H'_B$ from the uncorrelated state $e'_1 \otimes e'_1 \in H'_A \otimes H'_B$, in that for any $m_i \leq m$,

$$U^{(m_i)}_A \otimes U^{(m_i)}_B(\kappa_n \otimes e'_1 \otimes e'_1) \overset{\varepsilon/2}{=} \kappa_n \otimes \varphi, \quad (A.71)$$

where $\varepsilon = 1/N$ if $n = m^{2N}$. This follows straightforwardly from (A.68) - (A.70).
Acknowledgement

The author is indebted to Eric Cator, Roger Colbeck, Dennis Dieks, Dennis Hendrikx, and especially Gijs Leegwater for discussions, correspondence, and friendly corrections.

References


