PHYS 7895: Quantum Information Theory Fall 2015

Lecture 12 — October 5, 2015

Prof. Mark M. Wilde *Scribe: Mark M. Wilde*

1 Overview

In the last lecture, we discussed the exciting protocols of super-dense coding and teleportation. We also showed how to construct qudit extensions of these protocols.

In this lecture, we explore coherent version of these protocols, which illustrate how they are inverses of one another. This development is useful for what we do later in quantum Shannon theory. We then go on to define the notion of a purification of a density operator.

2 Motivation for Coherent Communication

We introduced three protocols in the previous lecture: entanglement distribution, teleportation, and super-dense coding. The last two of these protocols, teleportation and super-dense coding, are perhaps more interesting than entanglement distribution because they demonstrate insightful ways for combining all three unit resources to achieve an information-processing task.

It appears that teleportation and super-dense coding might be "inverse" protocols with respect to each other because teleportation arises from super-dense coding when Alice and Bob "swap their equipment." But there is a fundamental asymmetry between these protocols when we consider their respective resource inequalities. Recall that the resource inequality for teleportation is

$$2\left[c \to c\right] + \left[qq\right] \geq \left[q \to q\right], \tag{1}$$

while that for super-dense coding is

$$\left[q \to q\right] + \left[qq\right] \geq 2\left[c \to c\right]. \tag{2}$$

The asymmetry in these protocols is that they are not *dual under resource reversal.* Two protocols are dual under resource reversal if the resources that one consumes are the same that the other generates and vice versa. Consider that the super-dense coding resource inequality in (2) generates two classical bit channels. Glancing at the left hand side of the teleportation resource inequality in (1), we see that two classical bit channels generated from super-dense coding are not sufficient to generate the noiseless qubit channel on the right hand side of (1)—the protocol requires the consumption of noiseless entanglement in addition to the consumption of the two noiseless classical bit channels.

Is there a way for teleportation and super-dense coding to become dual under resource reversal? One way is if we assume that *entanglement is a free resource.* This assumption is strong and we may have difficulty justifying it from a practical standpoint because noiseless entanglement is extremely fragile. It is also a powerful resource, as the teleportation and super-dense coding protocols demonstrate. But in the theory of quantum communication, we often make assumptions such as this one—such assumptions tend to give a dramatic simplification of a problem. Continuing with our development, let us assume that entanglement is a free resource and that we do not have to factor it into the resource count. Under this assumption, the resource inequality for teleportation becomes

$$2\,[c \to c] \geq [q \to q]\,, \tag{3}$$

and that for super-dense coding becomes

$$[q \to q] \geq 2\,[c \to c]\,. \tag{4}$$

Teleportation and super-dense coding are then dual under resource reversal under the "free-entanglement" assumption, and we obtain the following *resource equality*:

$$[q \to q] = 2\,[c \to c]\,. \tag{5}$$

The above assumptions are useful for finding simple ways to make protocols dual under resource reversal, and we will exploit them later in our proofs of various capacity theorems in quantum Shannon theory. But it turns out that there is a more clever way to make teleportation and super-dense coding dual under resource reversal. In this chapter, we introduce a new resource—the *noiseless coherent bit channel*. This resource produces "coherent" versions of the teleportation and super-dense coding protocols that are dual under resource reversal. The payoff of this coherent communication technique is that we can exploit it to simplify the proofs of various coding theorems of quantum Shannon theory. It also leads to a deeper understanding of the relationship between the teleportation and super-dense coding protocols from the previous chapter.

3 Definition of Coherent Communication

We begin by introducing the coherent bit channel as a classical channel that has "quantum feedback" (in a particular sense). Recall that a classical bit channel is equivalent to a dephasing channel that dephases in the computational basis with dephasing parameter $p = 1/2$. The CPTP map corresponding to this completely dephasing channel is as follows:

$$\mathcal{N}(\rho) = \frac{1}{2}\left(\rho + Z\rho Z\right). \tag{6}$$

An isometric extension $U^{\mathcal{N}}_{A\to BE}$ of the above channel then follows:

$$U^{\mathcal{N}}_{A\to BE} = \frac{1}{\sqrt{2}}\left(I_{A\to B} \otimes |+\rangle_E + Z_{A\to B} \otimes |-\rangle_E\right), \tag{7}$$

where we choose the orthonormal basis states of the environment E to be $|+\rangle$ and $|-\rangle$ (recall that we have unitary freedom in the choice of the basis states for the environment). It is straightforward to show that the isometry $U^{\mathcal{N}}_{A\to BE}$ is as follows by expanding the operators I and Z and the states $|+\rangle$ and $|-\rangle$:

$$U^{\mathcal{N}}_{A\to BE} = |0\rangle_B\langle 0|_A \otimes |0\rangle_E + |1\rangle_B\langle 1|_A \otimes |1\rangle_E. \tag{8}$$

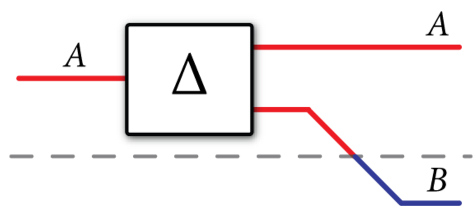

Figure 1: This figure depicts the operation of a coherent bit channel. It is the "coherification" of a classical bit channel in which the sender A has access to the environment's output.

Thus, a classical bit channel is equivalent to the following map, with its action extended by linearity:

$$|i\rangle_A \to |i\rangle_B |i\rangle_E : i \in \{0,1\}\,. \tag{9}$$

A coherent bit channel is similar to the above classical bit channel map, with the exception that we assume that Alice somehow regains control of the environment of the channel:

$$|i\rangle_A \to |i\rangle_B |i\rangle_A : i \in \{0,1\}\,. \tag{10}$$

"Coherence" in this context is also synonymous with linearity—the maintenance and linear transformation of superposed states. The coherent bit channel is similar to classical copying because it copies the basis states while maintaining coherent superpositions. We denote the resource of a coherent bit channel as follows:

$$[q \to qq]\,. \tag{11}$$

Figure 1 provides a visual depiction of the coherent bit channel.

Exercise 1. *Show that the following resource inequality holds:*

$$[q \to qq] \geq [c \to c]\,. \tag{12}$$

That is, devise a protocol that generates a noiseless classical bit channel with one use of a noiseless coherent bit channel.

4 Implementations of a Coherent Bit Channel

How might we actually implement a coherent bit channel? The simplest way to do so is with the aid of a local CNOT gate and a noiseless qubit channel. The protocol proceeds as follows (Figure 2 illustrates the protocol):

1. Alice possesses an information qubit in the state $|\psi\rangle_A \equiv \alpha|0\rangle_A + \beta|1\rangle_A$. She prepares an ancilla qubit in the state $|0\rangle_{A'}$.
2. Alice performs a local CNOT gate from qubit A to qubit A'. The resulting state is

$$\alpha|0\rangle_A|0\rangle_{A'} + \beta|1\rangle_A|1\rangle_{A'}. \tag{13}$$

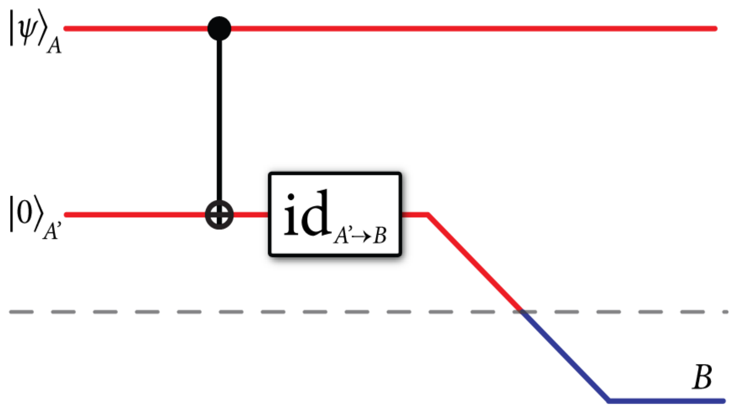

Figure 2: A simple protocol to implement a noiseless coherent channel with one use of a noiseless qubit channel.

3. Alice transmits qubit A' to Bob with one use of a noiseless qubit channel $\text{id}_{A'\to B}$. The resulting state is
$$\alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|1\rangle_B, \tag{14}$$
and it is now clear that Alice and Bob have implemented a noiseless coherent bit channel as defined in (10).

The above protocol implements the following resource inequality:
$$[q \to q] \geq [q \to qq]\,, \tag{15}$$
demonstrating that quantum communication generates coherent communication.

Exercise 2. *Show that the following resource inequality holds:*
$$[q \to qq] \geq [qq]\,. \tag{16}$$
That is, devise a protocol that generates a noiseless ebit with one use of a noiseless coherent bit channel.

We now have the following chain of resource inequalities:
$$[q \to q] \geq [q \to qq] \geq [qq]\,. \tag{17}$$
Thus, the power of the coherent bit channel lies in between that of a noiseless qubit channel and a noiseless ebit.

5 Coherent Dense Coding

In the previous section, we gave a protocol that implements a noiseless coherent bit channel. We now introduce a different method for implementing two coherent bit channels that makes more judicious use of available resources. We name it *coherent super-dense coding* because it is a coherent version of the super-dense coding protocol.

The protocol proceeds as follows (Figure 3 depicts the protocol):

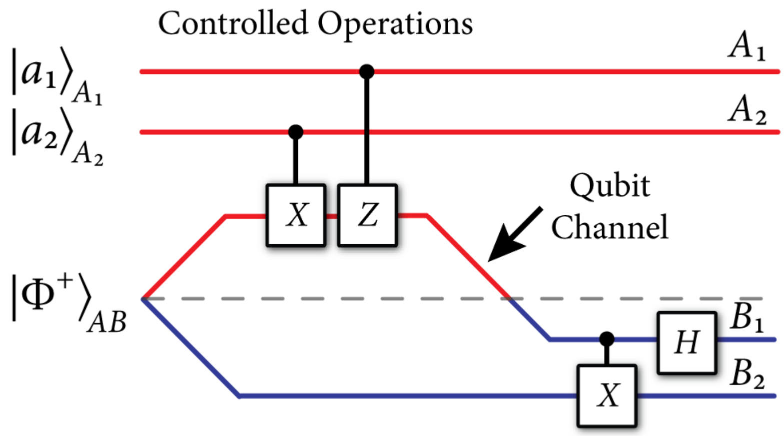

Figure 3: This figure depicts the protocol for coherent super-dense coding.

1. Alice and Bob share one ebit in the state $|\Phi^+\rangle_{AB}$ before the protocol begins.

2. Alice first prepares two qubits A_1 and A_2 in the state $|a_1\rangle_{A_1}|a_2\rangle_{A_2}$ and prepends this state to the ebit. The global state is as follows:

$$|a_1\rangle_{A_1}|a_2\rangle_{A_2}|\Phi^+\rangle_{AB}, \tag{18}$$

where a_1 and a_2 are binary-valued. This preparation step is reminiscent of the super-dense coding protocol (recall that, in the super-dense coding protocol, Alice has two classical bits she would like to communicate).

3. Alice performs a CNOT gate from register A_2 to register A and performs a controlled-Z gate from register A_1 to register A. The resulting state is as follows:

$$|a_1\rangle_{A_1}|a_2\rangle_{A_2} Z_A^{a_1} X_A^{a_2}|\Phi^+\rangle_{AB}. \tag{19}$$

4. Alice transmits the qubit in register A to Bob. We rename this register as B_1 and Bob's other register B as B_2.

5. Bob performs a CNOT gate from his register B_1 to B_2 and performs a Hadamard gate on B_1. The final state is as follows:

$$|a_1\rangle_{A_1}|a_2\rangle_{A_2}|a_1\rangle_{B_1}|a_2\rangle_{B_2}. \tag{20}$$

The above protocol implements two coherent bit channels: one from A_1 to B_1 and another from A_2 to B_2. You can check that the protocol works for arbitrary superpositions of two-qubit states on A_1 and A_2—it is for this reason that this protocol implements two coherent bit channels. The resource inequality corresponding to coherent super-dense coding is

$$[qq] + [q \to q] \geq 2\,[q \to qq]. \tag{21}$$

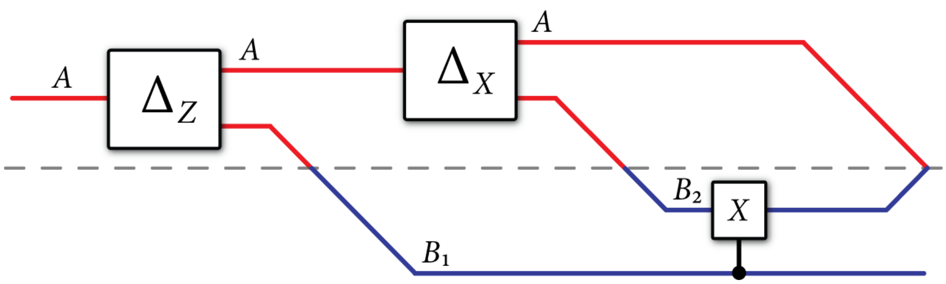

Figure 4: This figure depicts the protocol for coherent teleportation.

6 Coherent Teleportation

We now introduce a coherent version of the teleportation protocol that we name *coherent teleportation*. Let a Z coherent bit channel Δ_Z be one that copies eigenstates of the Z operator (this is as we defined a coherent bit channel before). Let an X coherent bit channel Δ_X be one that copies eigenstates of the X operator:

$$\Delta_X : |+\rangle_A \rightarrow |+\rangle_A |+\rangle_B, \tag{22}$$
$$|-\rangle_A \rightarrow |-\rangle_A |-\rangle_B . \tag{23}$$

It does not really matter which basis we use to define a coherent bit channel—it just matters that it copies the orthogonal states of some basis.

Exercise 3. *Show how to simulate an X coherent bit channel with a Z coherent bit channel and local operations.*

The protocol proceeds as follows (Figure 4 depicts the protocol):

1. Alice possesses an information qubit $|\psi\rangle_A$ where

$$|\psi\rangle_A \equiv \alpha|0\rangle_A + \beta|1\rangle_A. \tag{24}$$

   She sends her qubit through a Z coherent bit channel:

$$|\psi\rangle_A \quad \underrightarrow{\Delta_Z} \quad \alpha|0\rangle_A|0\rangle_{B_1} + \beta|1\rangle_A|1\rangle_{B_1} \equiv |\tilde{\psi}\rangle_{AB_1}. \tag{25}$$

   Let us rewrite the above state $|\tilde{\psi}\rangle_{AB_1}$ as follows:

$$|\tilde{\psi}\rangle_{AB_1} = \alpha\left(\frac{|+\rangle_A + |-\rangle_A}{\sqrt{2}}\right)|0\rangle_{B_1} + \beta\left(\frac{|+\rangle_A - |-\rangle_A}{\sqrt{2}}\right)|1\rangle_{B_1} \tag{26}$$
$$= \frac{1}{\sqrt{2}}\left[|+\rangle_A (\alpha|0\rangle_{B_1} + \beta|1\rangle_{B_1}) + |-\rangle_A (\alpha|0\rangle_{B_1} - \beta|1\rangle_{B_1})\right]. \tag{27}$$

2. Alice sends her qubit A through an X coherent bit channel with output systems A and B_2:

$$|\tilde{\psi}\rangle_{AB_1} \quad \underrightarrow{\Delta_X} \quad \frac{1}{\sqrt{2}}|+\rangle_A |+\rangle_{B_2} (\alpha|0\rangle_{B_1} + \beta|1\rangle_{B_1})$$
$$+ \frac{1}{\sqrt{2}}|-\rangle_A |-\rangle_{B_2} (\alpha|0\rangle_{B_1} - \beta|1\rangle_{B_1}) . \tag{28}$$

3. Bob then performs a CNOT gate from qubit B_1 to qubit B_2. Consider that the action of the CNOT gate with the source qubit in the computational basis and the target qubit in the $+/-$ basis is as follows:

$$|0\rangle|+\rangle \rightarrow |0\rangle|+\rangle, \tag{29}$$
$$|0\rangle\,|-\rangle \rightarrow |0\rangle\,|-\rangle\,, \tag{30}$$
$$|1\rangle|+\rangle \rightarrow |1\rangle|+\rangle, \tag{31}$$
$$|1\rangle\,|-\rangle \rightarrow -\,|1\rangle\,|-\rangle\,, \tag{32}$$

so that the last entry catches a phase of π ($e^{i\pi} = -1$). Then this CNOT gate brings the overall state to

$$\frac{1}{\sqrt{2}}\left[|+\rangle_A\,|+\rangle_{B_2}\,(\alpha|0\rangle_{B_1} + \beta|1\rangle_{B_1}) + |-\rangle_A\,|-\rangle_{B_2}\,(\alpha|0\rangle_{B_1} + \beta|1\rangle_{B_1})\right]$$
$$= \frac{1}{\sqrt{2}}\left[|+\rangle_A\,|+\rangle_{B_2}\,|\psi\rangle_{B_1} + |-\rangle_A\,|-\rangle_{B_2}\,|\psi\rangle_{B_1}\right] \tag{33}$$
$$= \frac{1}{\sqrt{2}}\left[|+\rangle_A\,|+\rangle_{B_2} + |-\rangle_A\,|-\rangle_{B_2}\right]|\psi\rangle_{B_1} \tag{34}$$
$$= \left|\Phi^+\right\rangle_{AB_2}|\psi\rangle_{B_1}. \tag{35}$$

Thus, Alice teleports her information qubit to Bob, and both Alice and Bob possess one ebit at the end of the protocol.

The resource inequality for coherent teleportation is as follows:

$$2[q \rightarrow qq] \geq [qq] + [q \rightarrow q]. \tag{36}$$

7 The Coherent Communication Identity

The fundamental result of this chapter is the *coherent communication identity*:

$$2[q \rightarrow qq] = [qq] + [q \rightarrow q]. \tag{37}$$

We obtain this identity by combining the resource inequality for coherent super-dense coding in (21) and the resource inequality for coherent teleportation in (36). The coherent communication identity demonstrates that coherent super-dense coding and coherent teleportation are dual under resource reversal—the resources that coherent teleportation consumes are the same as those that coherent super-dense coding generates and vice versa.

The major application of the coherent communication identity is in noisy quantum Shannon theory. We will find later that its application is in the "upgrading" of protocols that output private classical information. Suppose that a protocol outputs private classical bits. The super-dense coding protocol is one such example, as we argued before. Then it is possible to upgrade the protocol by making it coherent, similar to the way in which we made super-dense coding coherent by replacing conditional unitary operations with controlled unitary operations.

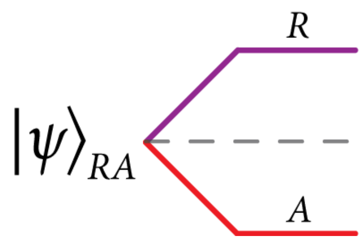

Figure 5: This diagram depicts a purification $|\psi\rangle_{RA}$ of a density operator ρ_A. The above diagram indicates that the reference system R is generally entangled with the system A. An interpretation of the purification theorem is that the noise inherent in a density operator ρ_A is due to entanglement with a reference system R.

8 Purification

Suppose we are given a density operator ρ_A on a system A. Every such density operator has a *purification*, as defined below and depicted in Figure 5:

Definition 4 (Purification)**.** *A purification of a density operator $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ is a pure bipartite state $|\psi\rangle_{RA} \in \mathcal{H}_R \otimes \mathcal{H}_A$ on a reference system R and the original system A, with the property that the reduced state on system A is equal to ρ_A in* (39)*:*

$$\rho_A = \mathrm{Tr}_R \{|\psi\rangle\langle\psi|_{RA}\}\,. \tag{38}$$

Suppose that a spectral decomposition for the density operator ρ_A is as follows:

$$\rho_A = \sum_x p_X(x)|x\rangle\langle x|_A. \tag{39}$$

We claim that the following state $|\psi\rangle_{RA}$ is a purification of ρ_A:

$$|\psi\rangle_{RA} \equiv \sum_x \sqrt{p_X(x)}\,|x\rangle_R\,|x\rangle_A, \tag{40}$$

where the set $\{|x\rangle_R\}_x$ of vectors is some set of orthonormal vectors for the reference system R. The next exercise asks you to verify this claim.

Exercise 5. *Show that the state $|\psi\rangle_{RA}$, as defined in* (40)*, is a purification of the density operator ρ_A, with a spectral decomposition as given in* (39)*.*

Exercise 6 (Canonical purification)**.** *Let ρ_A be a density operator and let $\sqrt{\rho_A}$ be its unique positive semi-definite square root (i.e., $\rho_A = \sqrt{\rho_A}\sqrt{\rho_A}$.) We define the canonical purification of ρ_A as follows:*

$$(I_R \otimes \sqrt{\rho_A})\,|\Gamma\rangle_{RA}\,, \tag{41}$$

where $|\Gamma\rangle_{RA}$ is the unnormalized maximally entangled vector, defined as

$$|\Gamma\rangle_{RA} = \sum_i |i\rangle_R|i\rangle_A. \tag{42}$$

Show that (41) *is a purification of ρ_A.*

8.1 Interpretation of Purifications

The purification idea has an interesting physical interpretation: we can think of the noisiness inherent in a particular quantum system as being due to entanglement with some external reference system to which we do not have access. That is, we can think that the density operator ρ_A arises from the entanglement of the system A with the reference system R and from our lack of access to the system R.

Stated another way, the purification idea gives us a fundamentally different way to interpret noise. The interpretation is that any noise on a local system is due to entanglement with another system to which we do not have access. This interpretation extends to the noise from a noisy quantum channel. We can view this noise as arising from the interaction of the system that we possess with an external environment over which we have no control.

The global state $|\psi\rangle_{RA}$ is a pure state, but a reduced state ρ_A is not a pure state in general because we trace over the reference system to obtain it. A reduced state ρ_A is pure if and only if the global state $|\psi\rangle_{RA}$ is a pure product state.

8.2 Equivalence of Purifications

Theorem 8 below states that there is an equivalence relation between all purifications of a given density operator ρ_A. It is a consequence of the Schmidt decomposition. Before stating it, we need the definition of an isometry:

Definition 7 (Isometry)**.** *Let $\mathcal{H}$ and $\mathcal{H}'$ be Hilbert spaces such that* $\dim(\mathcal{H}) \leq \dim(\mathcal{H}')$. *An isometry V is a linear map from $\mathcal{H}$ to $\mathcal{H}'$ such that $V^\dagger V = I_{\mathcal{H}}$. Equivalently, an isometry V is a linear, norm-preserving operator, in the sense that $\||\psi\rangle\|_2 = \|V|\psi\rangle\|_2$ for all $|\psi\rangle \in \mathcal{H}$.*

An isometry is a generalization of a unitary, because it maps between spaces of different dimensions and is thus generally rectangular and need not satisfy $VV^\dagger = I_{\mathcal{H}'}$. Rather, it satisfies $VV^\dagger = \Pi_{\mathcal{H}'}$, where $\Pi_{\mathcal{H}'}$ is some projection onto $\mathcal{H}'$, because

$$(VV^\dagger)(VV^\dagger) = V(V^\dagger V)V^\dagger = VI_{\mathcal{H}}V^\dagger = VV^\dagger. \tag{43}$$

In later chapters, we repeatedly use the notion of an isometry.

Theorem 8. *All purifications of a density operator are related by an isometry acting on the purifying system. That is, let ρ_A be a density operator, and let $|\psi\rangle_{R_1A}$ and $|\varphi\rangle_{R_2A}$ be purifications of ρ_A, such that* $\dim(\mathcal{H}_{R_1}) \leq \dim(\mathcal{H}_{R_2})$. *Then there exists an isometry $U_{R_1\to R_2}$ such that*

$$|\varphi\rangle_{R_2A} = (U_{R_1\to R_2} \otimes I_A)\, |\psi\rangle_{R_1A}. \tag{44}$$

Proof. Let first suppose that the eigenvalues of ρ_A are distinct, so that a unique spectral decomposition of ρ_A is as follows:

$$\rho_A = \sum_x p_X(x)|x\rangle\langle x|_A. \tag{45}$$

Then a Schmidt decomposition of $|\varphi\rangle_{R_2A}$ necessarily has the form

$$|\varphi\rangle_{R_2A} = \sum_x \sqrt{p_X(x)}|\varphi_x\rangle_{R_2}|x\rangle_A, \tag{46}$$

where $\{|\varphi_x\rangle_{R_2}\}$ is an orthonormal basis for the R_2 system, and similarly, the Schmidt decomposition of $|\psi\rangle_{R_1A}$ necessarily has the form

$$|\psi\rangle_{R_1A} = \sum_x \sqrt{p_X(x)}|\psi_x\rangle_{R_1}|x\rangle_A. \tag{47}$$

(If it were not the case then we could not have $\mathrm{Tr}_{R_2}\{|\varphi\rangle\langle\varphi|_{R_2A}\} = \mathrm{Tr}_{R_1}\{|\psi\rangle\langle\psi|_{R_1A}\} = \rho_A$, as given in the statement of the theorem.) Given the above, we can take the isometry $U_{R_1\to R_2}$ to be

$$U_{R_1\to R_2} = \sum_x |\varphi_x\rangle_{R_2}\langle\psi_x|_{R_1}, \tag{48}$$

which is an isometry because $U^\dagger U = I_{R_1}$. If the eigenvalues of ρ_A are not distinct, then there is more freedom in the Schmidt decompositions, but here we are free to choose them as above, and then the development is the same. □

This theorem leads to a way of relating all convex decompositions of a given density operator:

Corollary 9. *Let two convex decompositions of a density operator ρ be as follows:*

$$\rho = \sum_{x=1}^{d} p_X(x)|\psi_x\rangle\langle\psi_x| = \sum_{y=1}^{d'} p_Y(y)|\phi_y\rangle\langle\phi_y|, \tag{49}$$

where $d' \leq d$. Then there exists an isometry U such that

$$\sqrt{p_X(x)}|\psi_x\rangle = \sum_y U_{x,y}\sqrt{p_Y(y)}|\phi_y\rangle. \tag{50}$$

Proof. Let $\{|x\rangle_R\}$ be an orthonormal basis for a purification system, with a number of states equal to $\max\{d, d'\}$. Then a purification for the first decomposition is as follows:

$$|\psi\rangle_{RA} \equiv \sum_x \sqrt{p_X(x)}|x\rangle_R \otimes |\psi_x\rangle_A, \tag{51}$$

and a purification of the second decomposition is

$$|\phi\rangle_{RA} \equiv \sum_y \sqrt{p_Y(y)}|y\rangle_R \otimes |\phi_y\rangle_A. \tag{52}$$

From Theorem 8, we know that there exists an isometry U_R such that $|\psi\rangle_{RA} = (U_R \otimes I_A)|\phi\rangle_{RA}$. Then consider that

$$\sqrt{p_X(x)}|\psi_x\rangle_A = \sum_{x'} \sqrt{p_X(x')}\langle x|_R|x'\rangle_R \otimes |\psi_{x'}\rangle_A = (\langle x|_R \otimes I_A)|\psi\rangle_{RA} \tag{53}$$

$$= (\langle x|_R U_R \otimes I_A)|\phi\rangle_{RA} = \sum_y \sqrt{p_Y(y)}\langle x|_R U_R|y\rangle_R|\phi_y\rangle_A \tag{54}$$

$$= \sum_y \sqrt{p_Y(y)}U_{x,y}|\phi_y\rangle_A, \tag{55}$$

where in the last step we have defined $U_{x,y} = \langle x|_R U_R|y\rangle_R$. □