APPPHYS225 - Thursday 6 November 2008

Suppose we are given a set of possible quantum states, $\aleph = \{\rho_1, \rho_2, \ldots, \rho_N\}$, for an input system A. A *cloning map* E_C is a map on the input system A and a target system B, such that for a fixed initial target state Σ_B we have

$$E_C(\rho_{iA} \otimes \Sigma_B) = \rho_{iA} \otimes \rho_{iB}.$$

We will see that such cloning is impossible unless $\aleph$ contains only mutually orthogonal states.

A *broadcasting map* E_B is a map on the input system A and a target system B, such that for a fixed initial target state Σ_B we have

$$E_B(\rho_{iA} \otimes \Sigma_B) = \tilde{\rho}_{iAB},$$

where

$$\mathrm{Tr}_A[\tilde{\rho}_{iAB}] = \rho_{iB}, \quad \mathrm{Tr}_B[\tilde{\rho}_{iAB}] = \rho_{iA}.$$

It turns out that broadcasting is only possible when $\aleph$ contains only states that commute with each other.

Note that we can define *classical* cloning and broadcasting by restricting the input states to density matrices that are all diagonal in a fixed basis. In general, in order to be physical (allowed by quantum mechanics), cloning/broadcasting maps must be implementable via

$$E_{C/B}(\rho_{iA} \otimes \Sigma_B) = \mathrm{Tr}_C\left[\mathbf{U}(\rho_{iA} \otimes \Sigma_B \otimes \Upsilon_C)\mathbf{U}^\dagger\right],$$

where C is an ancillary system prepared in the initial state Υ_C and $\mathbf{U}$ is a unitary operator that jointly evolves all three systems. In what follows we will restrict our attention to input sets $\aleph$ that contain only two states, but the conclusions can easily be extended to larger sets.

Pure state cloning in quantum and classical models

In this section we follow the discussion of H. P. Yuen, "Amplification of quantum states and noiseless photon amplifiers," Phys. Lett. 113A, **405** (1986).

Restricting our attention first to two pure input states $\aleph = \{|\Phi_1\rangle\langle\Phi_1|, |\Phi_2\rangle\langle\Phi_2|\}$ and true cloning, we search for conditions under which the following transformation is possible:

$$|\Phi_{iA}\rangle \otimes |\alpha_{1B}\rangle \otimes |\beta_{1C}\rangle \mapsto |\Phi_{iA}\rangle \otimes |\Phi_{iB}\rangle \otimes |\gamma_{iC}\rangle,$$
$$|\Phi_{iA}\rangle \otimes |\Phi_{iB}\rangle \otimes |\gamma_{iC}\rangle = \mathbf{U}|\Phi_{iA}\rangle \otimes |\alpha_{1B}\rangle \otimes |\beta_{1C}\rangle.$$

Here A is the input system, B is the target system, and C is an ancillary system that may be used to assist in the cloning operation. The unitary operator $\mathbf{U}$ describes joint evolution of systems A, B and C under the influence of some (possibly time-dependent) coupling Hamiltonian. Note that the target system is prepared in some initial state $|\alpha_{1B}\rangle$ that must be independent of the input state, and that the ancilla may in general be left in some 'side-effect' state $|\gamma_{iC}\rangle$ that could depend on the input state. Note that initial entanglement between the target state and ancilla can be lumped into $\mathbf{U}$.

The proof that only orthogonal pure states are clonable follows from taking a simple inner product. Working on the right-hand side of the above equation,

$$(\mathbf{U}|\Phi_{2A}\rangle \otimes |\alpha_{1B}\rangle \otimes |\beta_{1C}\rangle)^{\dagger}(\mathbf{U}|\Phi_{1A}\rangle \otimes |\alpha_{1B}\rangle \otimes |\beta_{1C}\rangle) = \langle \Phi_2|\Phi_1\rangle,$$

while on the left-hand side,

$$(|\Phi_{2A}\rangle \otimes |\Phi_{2B}\rangle \otimes |\gamma_{2C}\rangle)^{\dagger}(|\Phi_{1A}\rangle \otimes |\Phi_{1B}\rangle \otimes |\gamma_{1C}\rangle) = (\langle \Phi_2|\Phi_1\rangle)^2\langle \gamma_2|\gamma_1\rangle.$$

Hence we require

$$(\langle \Phi_2|\Phi_1\rangle)^2\langle \gamma_2|\gamma_1\rangle = \langle \Phi_2|\Phi_1\rangle,$$

which means that either $\langle \Phi_2|\Phi_1\rangle = 0$, in which case the input states are orthogonal,

$$\langle \Phi_2|\Phi_1\rangle\langle \gamma_2|\gamma_1\rangle = 1.$$

Since both inner products have magnitude less than or equal to $1,$ this can only be satisfied if $|\langle \gamma_2|\gamma_1\rangle| = |\langle \Phi_2|\Phi_1\rangle| = 1$ and $\arg\langle \gamma_2|\gamma_1\rangle + \arg\langle \Phi_2|\Phi_1\rangle = 0.$ But if $|\langle \Phi_2|\Phi_1\rangle| = 1$ then $|\Phi_1\rangle$ and $|\Phi_2\rangle$ represent the same state. Hence we find that pure states can be cloned only if they are either identical (completely indistinguishable) or orthogonal (perfectly distinguishable).

It is similarly straightforward to prove that orthogonal pure states can always be cloned by a unitary transformation. In fact the ancillary system is unnecssary as the required mapping can be achieved via

$$|\Phi_{iA}\rangle \otimes |\Phi_{iB}\rangle = \mathbf{U}|\Phi_{iA}\rangle \otimes |\alpha_{1B}\rangle.$$

So what is this magic operator $\mathbf{U}$? We can start by guessing

$$\tilde{\mathbf{U}} = |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\Phi_{1B}\rangle\langle \alpha_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\Phi_{2B}\rangle\langle \alpha_{1B}|,$$

where without loss of generality we can assume $|\alpha_{1B}\rangle \in \mathrm{span}\{|\Phi_{1B}\rangle, |\Phi_{2B}\rangle\},$ but we find that this candidate is not actually unitary:

$$\tilde{\mathbf{U}}^{\dagger} = |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\alpha_{1B}\rangle\langle \Phi_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\alpha_{1B}\rangle\langle \Phi_{2B}|,$$

$$\tilde{\mathbf{U}}^{\dagger}\tilde{\mathbf{U}} = |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\alpha_{1B}\rangle\langle \alpha_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\alpha_{1B}\rangle\langle \alpha_{1B}|,$$

$$\tilde{\mathbf{U}}\tilde{\mathbf{U}}^{\dagger} = |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\Phi_{1B}\rangle\langle \Phi_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\Phi_{2B}\rangle\langle \Phi_{2B}|.$$

Based on this however we can guess that a simple augmentation is required,

$$\begin{aligned}\mathbf{U} = {} & |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\Phi_{1B}\rangle\langle \alpha_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\Phi_{2B}\rangle\langle \alpha_{1B}| \\ & + |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\Phi_{2B}\rangle\langle \alpha_{2B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\Phi_{1B}\rangle\langle \alpha_{2B}|,\end{aligned}$$

where $\langle \alpha_{2B}|\alpha_{1B}\rangle = 0$ and $|\alpha_{2B}\rangle \in \mathrm{span}\{|\Phi_{1B}\rangle, |\Phi_{2B}\rangle\}.$ Then we have

$$\begin{aligned}\mathbf{U}^{\dagger} = {} & |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\alpha_{1B}\rangle\langle \Phi_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\alpha_{1B}\rangle\langle \Phi_{2B}| \\ & + |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\alpha_{2B}\rangle\langle \Phi_{2B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\alpha_{2B}\rangle\langle \Phi_{1B}|, \\ \mathbf{U}^{\dagger}\mathbf{U} = {} & |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\alpha_{1B}\rangle\langle \alpha_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\alpha_{1B}\rangle\langle \alpha_{1B}| \\ & + |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\alpha_{2B}\rangle\langle \alpha_{2B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\alpha_{2B}\rangle\langle \alpha_{1B}|, \\ \mathbf{U}\mathbf{U}^{\dagger} = {} & |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\Phi_{1B}\rangle\langle \Phi_{1B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\Phi_{2B}\rangle\langle \Phi_{2B}| \\ & + |\Phi_{1A}\rangle\langle \Phi_{1A}| \otimes |\Phi_{2B}\rangle\langle \Phi_{2B}| + |\Phi_{2A}\rangle\langle \Phi_{2A}| \otimes |\Phi_{1B}\rangle\langle \Phi_{1B}|.\end{aligned}$$

Since $\text{span}\{|\alpha_{1B}\rangle, |\alpha_{2B}\rangle\} = \text{span}\{|\Phi_{1B}\rangle, |\Phi_{2B}\rangle\}$, we have

$$|\Phi_{1A}\rangle\langle\Phi_{1A}| + |\Phi_{2A}\rangle\langle\Phi_{2A}| = \mathbf{1}^A,$$
$$|\Phi_{1B}\rangle\langle\Phi_{1B}| + |\Phi_{2B}\rangle\langle\Phi_{2B}| = |\alpha_{1B}\rangle\langle\alpha_{1B}| + |\alpha_{2B}\rangle\langle\alpha_{2B}| = \mathbf{1}^B,$$

and thus $\mathbf{U}$ is indeed unitary.

We recognize from the form of our cloning unitary transformation that the following measurement-based procedure would also do the trick. First perform a projective measurement with operation elements $\{\mathbf{A}_1 = |\Phi_{1A}\rangle\langle\Phi_{1A}|,\ \mathbf{A}_2 = |\Phi_{2A}\rangle\langle\Phi_{2A}|\}$ on the input system. If the result corresponding to $\mathbf{A}_1$ is obtained prepare the target system in state $|\Phi_{1B}\rangle$, and if the result corresponding to $\mathbf{A}_2$ is obtained prepare the target system in state $|\Phi_{2B}\rangle$. Clearly this kind of approach is possible if and only if the input states are orthogonal. We also note in this context that it's a good thing (for the consistency of quantum probability theory) that non-orthogonal states *can't* be cloned, because if they could you would have an easy way of distinguishing non-orthogonal input states with arbitrarily small probability of error—simply clone the input system a large number of times, and repeat (for example) an optimal projective measurement on successive copies until your overall probability of error is as small as you like.

If $\langle\Phi_{2A}|\Phi_{1A}\rangle = 0$ then $\{|\Phi_{1A}\rangle, |\Phi_{2A}\rangle\}$ represent an orthonormal basis for a two-dimensional subspace of the A Hilbert space. It follows that in this basis, the density operators have matrix representations

$$|\Phi_{1A}\rangle\langle\Phi_{1A}| \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |\Phi_{2A}\rangle\langle\Phi_{2A}| \leftrightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

The state matrices thus look like those of a classical probability model with $\Omega_A = \{\omega_{1A}, \omega_{2A}\}$. Clearly we can 'clone' pure states of any classical model by first measuring the configuration of A precisely and then preparing B in the identical configuration. Of course the quantum cloning scenario, even with $\aleph$ containing only orthogonal pure states, cannot actually be mapped to an equivalent classical probability model because we place no restrictions on the class of observables that might be measured after the cloning map is applied.

Classical broadcasting

What about mixed states of a classical probability model? Recall that in the classical context a pure state is represented by a probability distribution function $m(\bullet)$ that takes value 1 on one configuration and 0 on the others; a mixed state is any other function $m(\bullet)$ such that $m^2(\bullet) \neq m(\bullet)$. We'll see below that arbitrary classical mixed states cannot be cloned, but it is in fact possible to broadcast arbitrary classical mixed states. We have actually already seen a procedure that accomplishes this, in our earlier discussion of classical teleportation.

We consider an input system with $\Omega_A = \{\omega_{1A}, \omega_{2A}\}$, a target system with $\Omega_B = \{\omega_{2A}, \omega_{2B}\}$ and an ancillary system with $\Omega_C = \{\omega_{1C}, \omega_{2C}\}$. Let the input system be prepared in an arbitrary mixed state,

$$m_A(\omega_{1A}) = p_{1A}, \quad m_A(\omega_{2A}) = p_{2A}.$$

We start by preparing the target and ancillary systems in the correlated state

$$m_{BC}(\omega_{1B} \times \omega_{1C}) = m_{BC}(\omega_{2B} \times \omega_{2C}) = \frac{1}{2},$$
$$m_{BC}(\omega_{1B} \times \omega_{2C}) = m_{BC}(\omega_{2B} \times \omega_{1C}) = 0,$$

so that our set of three systems start out in the joint state

$$m_{ABC}(\omega_{iA} \times \omega_{jB} \times \omega_{kC}) = m_A(\omega_{iA}) m_{BC}(\omega_{jB} \times \omega_{kC}).$$

We measure the random variable $\Pi_{AC}(\cdot)$ on $\Omega_A \times \Omega_C,$ defined by

$$\Pi_{AC}(\omega_{1A} \times \omega_{1C}) = \Pi_{AC}(\omega_{2A} \times \omega_{2C}) = +1,$$
$$\Pi_{AC}(\omega_{1A} \times \omega_{2C}) = \Pi_{AC}(\omega_{2A} \times \omega_{1C}) = -1.$$

As we have previously shown and explained in the class notes from 10/31, if we obtain $\Pi_{AC} = +1$ we are left with the conditional joint state

$$m_+(\omega_{1A} \times \omega_{1B} \times \omega_{1C}) = m_A(\omega_{1A}), \quad m_+(\omega_{2A} \times \omega_{2B} \times \omega_{2C}) = m_A(\omega_{2A}),$$
$$m_+(\omega_{iA} \times \omega_{jB} \times \omega_{kC}) = 0, \quad i \neq j \neq k.$$

If $\Pi_{AC} = -1$ we have

$$m_-(\omega_{1A} \times \omega_{2B} \times \omega_{2C}) = m_A(\omega_{1A}), \quad m_-(\omega_{2A} \times \omega_{1B} \times \omega_{1C}) = m_A(\omega_{2A}),$$
$$m_-(\omega_{iA} \times \omega_{jB} \times \omega_{kC}) = 0, \quad \text{otherwise},$$

and we note that we can convert $m_-(\cdot)$ to $m_+(\cdot)$ by applying the transformations $\omega_{1B} \leftrightarrow \omega_{2B}$ and $\omega_{1C} \leftrightarrow \omega_{2C}$ (think of turning coins over without looking at them). Looking at the joint state $m_+(\cdot)$ then, we note that the marginal distributions for A and B are both equal to $m_A(\cdot).$

$$M_A(\omega_{iA}) \equiv \sum_{\omega_{jB},\omega_{kC}} m_+(\omega_{iA} \times \omega_{jB} \times \omega_{kC}) = m_A(\omega_{iA}),$$
$$M_B(\omega_{jB}) \equiv \sum_{\omega_{iA},\omega_{kC}} m_+(\omega_{iA} \times \omega_{jB} \times \omega_{kC}) = m_A(\omega_{jB}),$$

where we have implicitly extended the definition

$$m_A(\omega_{1B}) = m_A(\omega_{1A}) = p_{1A}, \quad m_A(\omega_{2B}) = m_A(\omega_{2A}) = p_{2A}.$$

Note that this is really a broadcasting map and not a cloning map, as the latter would have to give us

$$m_{ABC}(\omega_{iA} \times \omega_{jB} \times \omega_{kC}) \propto m_A(\omega_{iA}) m_A(\omega_{jB}),$$

which would in general have non-zero probability for both $\omega_{1A} \times \omega_{1B}$ and $\omega_{1A} \times \omega_{2B},$ for example.

In this classical context we can easily see that broadcasting will not get us in trouble in terms of the distinguishability or measurability of mixed states. If someone gives a classical system with $\Omega_A = \{\omega_{1A}, \omega_{2A}\}$ prepared with an arbitrary probability distribution function $m_A(\cdot),$ we should not be able to determine $m_A(\cdot)$ by making measurements on the physical system. Any measurement we make can at most yield one bit of information (whether the configuration is ω_{1A} or ω_{2A}), whereas it can take an arbitary number of bits to specify $m_A(\cdot)$ exactly (since $m_A(\omega_{1A})$ and $m_A(\omega_{2A})$ are real numbers). Even after broadcasting, however, we note that no measurement on the $\Omega_A \times \Omega_B \times \Omega_C$ system can yield more than one bit of information since the three systems are perfectly correlated. If true cloning were possible this would not be true, since with something like

$$m_{ABC}(\omega_{iA}\times\omega_{jB}\times\omega_{kC}) \propto m_A(\omega_{iA})m_A(\omega_{jB}),$$

we could actually obtain two bits of information by measuring A and B independently.

Cloaning and broadcasting of quantum mixed states

In this section we follow the discussion of H. Barnum *et al.*, "Noncommuting Mixed States Cannot be Broadcast," Phys. Rev. Lett. **76**, 2818 (1996).

Fidelity is a measure of distinguishability for mixed states,

$$F(\rho_1,\rho_2) = \mathrm{Tr}\left[\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}}\,\right],$$

which reduces to the familiar inner product when both states are pure:

$$\begin{aligned}\mathrm{Tr}\left[\sqrt{\rho_1^{1/2}\rho_2\rho_1^{1/2}}\,\right] &\to \mathrm{Tr}\left[\sqrt{|\Psi_1\rangle\langle\Psi_1||\Psi_2\rangle\langle\Psi_2||\Psi_1\rangle\langle\Psi_1|}\,\right]\\ &= |\langle\Psi_1|\Psi_2\rangle|\,\mathrm{Tr}\left[\sqrt{|\Psi_1\rangle\langle\Psi_1|}\,\right]\\ &= |\langle\Psi_1|\Psi_2\rangle|.\end{aligned}$$

In the above expressions, for any positive (Hermitian with non-negative eigenvalues) operator $\mathbf{O}$ the square root $\sqrt{\mathbf{O}}$ or $\mathbf{O}^{1/2}$ denotes the *unique positive square-root* of $\mathbf{O}$, which is the unique matrix $\mathbf{T}$ such that $\mathbf{TT}=\mathbf{O}$ and $\mathbf{T}$ is itself positive. We thus infer that $F(\rho_1,\rho_2)=1$ indicates that the two mixed states are indistinguishable, while $F(\rho_1,\rho_2)=0$ indicates that they are orthogonal. For today's purposes, it is important to note that fidelity has an operational significance as the minimum *overlap* between the probability distributions for measurement results of a POVM applied to either ρ_1 or ρ_2:

$$F(\rho_1,\rho_2) = \min_{\{\mathbf{E}_b\}}\sum_b\sqrt{\mathrm{Tr}[\rho_1\mathbf{E}_b]}\sqrt{\mathrm{Tr}[\rho_2\mathbf{E}_b]}\,.$$

Clearly if ρ_1 and ρ_2 are indistinguishable by means of a given POVM $\{\mathbf{E}_b\}$, the outcome probabilities appearing under the radicals will be identical and therefore the sum over b will simply yield $1.$ If ρ_1 and ρ_2 are perfectly distinguishable by means of a given POVM then the outcome probabilities must be orthogonal, in the sense that only one of $\mathrm{Tr}[\rho_1\mathbf{E}_b]$ or $\mathrm{Tr}[\rho_2\mathbf{E}_b]$ can be non-zero for each b, and the sum over b must therefore yield 0.

Recall that we above derived the impossibility of cloning non-orthogonal pure states by comparing the inner product of cloned states $(|\Phi_{2A}\rangle\otimes|\Phi_{2B}\rangle\otimes|\gamma_{2C}\rangle)^\dagger(|\Phi_{1A}\rangle\otimes|\Phi_{1B}\rangle\otimes|\gamma_{1C}\rangle)$ with its 'implementation' equivalent $(\mathbf{U}|\Phi_{2A}\rangle\otimes|\alpha_{1B}\rangle\otimes|\beta_{1C}\rangle)^\dagger(\mathbf{U}|\Phi_{1A}\rangle\otimes|\alpha_{1B}\rangle\otimes|\beta_{1C}\rangle).$ In the mixed-state case, fidelities take center stage in place of the inner products. Recall the abstract setup for broadcasting or cloning of mixed states,

$$E_{C/B}(\rho_{iA}\otimes\Sigma_B) = \mathrm{Tr}_C\left[\mathbf{U}(\rho_{iA}\otimes\Sigma_B\otimes\Upsilon_C)\mathbf{U}^\dagger\right] \equiv \tilde{\rho}_{iAB}.$$

For cloning we require that $\tilde{\rho}_{iAB}=\rho_{iA}\otimes\rho_{iB}$ while for broadcasting we have the relaxed requirement

$$\mathrm{Tr}_B[\tilde{\rho}_{iAB}] = \rho_{iA}, \quad \mathrm{Tr}_A[\tilde{\rho}_{iAB}] = \rho_{iB}.$$

The authors of the paper cited at the beginning of this section derived a cloning/broadcasting fildelity relation

$$F_A(\rho_1,\rho_2) = F(\tilde{\rho}_1,\tilde{\rho}_2) = F_B(\rho_1,\rho_2),$$

where $F(\tilde{\rho}_1,\tilde{\rho}_2)$ is simply the fidelity between the joint states produced by a cloning or broadcasting operation, and $F_A(\rho_1,\rho_2)$ and $F_B(\rho_1,\rho_2)$ are defined as follows:

$$F_A(\rho_1,\rho_2) \equiv \sum_b \sqrt{\mathrm{Tr}[\tilde{\rho}_{1AB}(\mathbf{E}_b^A \otimes \mathbf{1}^B)]}\sqrt{\mathrm{Tr}[\tilde{\rho}_{2AB}(\mathbf{E}_b^A \otimes \mathbf{1}^B)]},$$

$$F_B(\rho_1,\rho_2) \equiv \sum_b \sqrt{\mathrm{Tr}[\tilde{\rho}_{1AB}(\mathbf{1}^A \otimes \mathbf{E}_b^B)]}\sqrt{\mathrm{Tr}[\tilde{\rho}_{2AB}(\mathbf{1}^A \otimes \mathbf{E}_b^B)]}.$$

Here $\{\mathbf{E}_b\}$ is taken to be the optimal POVM for distinguishing states ρ_1 and ρ_2, as in the operational definition of fidelity that we discussed above. Note that in the cloning scenario, in which $\tilde{\rho}_{iAB} = \rho_{iA} \otimes \rho_{iB}$, we immediately obtain a result from the fidelity relation:

$$F_A(\rho_1,\rho_2) = \sum_b \sqrt{\mathrm{Tr}[\rho_{1A} \otimes \rho_{1B}(\mathbf{E}_b^A \otimes \mathbf{1}^B)]}\sqrt{\mathrm{Tr}[\rho_{2A} \otimes \rho_{2B}(\mathbf{E}_b^A \otimes \mathbf{1}^B)]}$$

$$= \sum_b \sqrt{\mathrm{Tr}[\rho_{1A}\mathbf{E}_b^A]}\sqrt{\mathrm{Tr}[\rho_{2A}\mathbf{E}_b^A]}$$

$$= F(\rho_1,\rho_2),$$

$$F(\tilde{\rho}_{1AB},\tilde{\rho}_{2AB}) = F(\rho_{1A} \otimes \rho_{1B},\rho_{2A} \otimes \rho_{2B}) = F^2(\rho_1,\rho_2),$$

where the final equality follows from elementary properties of the tensor product. We thus require for cloning to be possible that $F(\rho_1,\rho_2) = F^2(\rho_1,\rho_2)$, which means that either $F(\rho_1,\rho_2) = 0$ or $F(\rho_1,\rho_2) = 1.$ This reproduces the identical-or-orthogonal criterion that we obtained in the pure state case, with orthogonality here generalized in the mixed-state scenario to perfect distinguishability (via some POVM, as in our discussion of the operational definition of fidelity).

For broadcasting, as opposed to true cloning, the paper we cited above contains a proof that the cloning/broadcasting fidelity relation can only be satisfied if $\rho_1\rho_2 = \rho_2\rho_1$, that is, if the states in $\aleph$ *commute*. Recall that when this condition is satisfied we can find a basis in which the matrix representations of the states are simultaneously diagonalized. In this basis, specified by a set of orthonormal eigenvectors $\{|b\rangle\}$, we have the spectral decompositions

$$\rho_1 = \sum_b \lambda_{1b}|b\rangle\langle b|, \quad \rho_2 = \sum_b \lambda_{2b}|b\rangle\langle b|.$$

We may then construct the broadcasting scheme:

$$\rho_{iA} \otimes \Sigma_B \mapsto \mathbf{U}(\rho_{iA} \otimes \Sigma_B)\mathbf{U}^\dagger,$$

where

$$\Sigma_B = |1_B\rangle\langle 1_B|$$

and

$$\mathbf{U} = |1_A\rangle\langle 1_A| \otimes \mathbf{1}^B + \sum_{b>1} |b_A\rangle\langle b_A| \otimes \left(|b_B\rangle\langle 1_B| + |1_B\rangle\langle b_B| + \sum_{b' \notin \{1,b\}} |b'_B\rangle\langle b'_B| \right),$$
$$\mathbf{U}^\dagger = \mathbf{U}.$$

It is easy to see that the relevant action of $\mathbf{U}$ is to swap $|1_B\rangle$ with $|b_B\rangle$ when system A is in the state $|b_A\rangle$ (it is somewhat like a multi-dimensional controlled-NOT). We first verify that

$$\begin{aligned}
\mathbf{U}^2 &= |1_A\rangle\langle 1_A| \otimes \mathbf{1}^B \\
&\quad + \sum_{b>1} |b_A\rangle\langle b_A| \otimes \left(|b_B\rangle\langle 1_B| + |1_B\rangle\langle b_B| + \sum_{b' \notin \{1,b\}} |b'_B\rangle\langle b'_B| \right)\left(|b_B\rangle\langle 1_B| + |1_B\rangle\langle b_B| + \sum_{b'' \notin \{1,b\}} |b''_B\rangle\langle b''_B| \right) \\
&= |1_A\rangle\langle 1_A| \otimes \mathbf{1}^B + \sum_{b>1} |b_A\rangle\langle b_A| \otimes \left(|b_B\rangle\langle b_B| + |1_B\rangle\langle 1_B| + \sum_{b' \notin \{1,b\}} |b'_B\rangle\langle b'_B| \right) \\
&= \sum_{b=1} |1_A\rangle\langle 1_A| \otimes \mathbf{1}^B + \sum_{b>1} |b_A\rangle\langle b_A| \otimes \mathbf{1}^B \\
&= \mathbf{1}^A \otimes \mathbf{1}^B.
\end{aligned}$$

We then check the action of $\mathbf{U}$,

$$\begin{aligned}
\mathbf{U}(\boldsymbol{\rho}_{iA} \otimes \boldsymbol{\Sigma}_B)\mathbf{U}^\dagger &= \mathbf{U}\left(\sum_b \lambda_{ib} |b_A\rangle\langle b_A| \otimes |1_B\rangle\langle 1_B| \right)\mathbf{U}^\dagger \\
&= \left(\sum_b \lambda_{ib} |b_A\rangle\langle b_A| \otimes |b_B\rangle\langle 1_B| \right)\mathbf{U}^\dagger \\
&= \sum_b \lambda_{ib} |b_A\rangle\langle b_A| \otimes |b_B\rangle\langle b_B|.
\end{aligned}$$

It is easy to see that this correlated joint state satisfies the broadcasting criterion, since we can take our partial traces in the $\{|b\rangle\}$ bases:

$$\begin{aligned}
\mathrm{Tr}_B\left[\sum_b \lambda_{ib} |b_A\rangle\langle b_A| \otimes |b_B\rangle\langle b_B| \right] &= \sum_{b'} \langle b'_B| \left(\sum_b \lambda_{ib} |b_A\rangle\langle b_A| \otimes |b_B\rangle\langle b_B| \right) |b'_B\rangle \\
&= \sum_b \lambda_{ib'} |b'_A\rangle\langle b'_A|,
\end{aligned}$$

and likewise for the partial trace over A.

The proof of the impossibility of perfect broadcasting for states that do not commute is rather technical, so we do not repeat it here. With what you have learned in this class so far you should find the technical content of the paper reasonable accessible, however, so you are encouraged to have a look. In particular, the paper contains a nice derivation of the operational significance of mixed-state fidelity, which sets up a subsequent proof of the impossibility of broadcasting non-commuting mixed states.

Some more recent treatments of the ‘no-broadcasting rheorem’ have appeared in the literature:

- H. Barnum *et al.*, “Generalized No-Broadcasting Theorem,” Phys. Rev. Lett. **99**, 240501 (2007).
- A. Kalev and I. Hen, “No-Broadcasting Theorem and Its Classical Counterpart,” Phys. Rev. Lett. **100**, 210502 (2008).

The first of these makes connections with an interesting new research direction of considering probability theories that are neither quantum nor classical, and shows that the possibility of broadcasting mixed states is in some sense unique to classical probability (as opposed to the impossibility of broadcasting being unique to quantum probability). The second paper utilizes a more information-theoretic approach to proove the no-broadcasting theorem, based on relative entropy.