Lecture 6: Further remarks on measurements and channels

In this lecture we will discuss a few loosely connected topics relating to measurements and channels. These discussions will serve to illustrate some of the concepts we have discussed in previous lectures, and are also an opportunity to introduce a few notions that will be handy in future lectures.

6.1 Measurements as channels and nondestructive measurements

We begin with two simple points concerning measurements. The first explains how measurements may be viewed as special types of channels, and the second introduces the notion of nondestructive measurements (which were commented on briefly in Lecture 3).

6.1.1 Measurements as channels

Suppose that we have a measurement $\mu : \Gamma \rightarrow \mathrm{Pos}(\mathcal{X})$ on a register X. When this measurement is performed, X ceases to exist, and the measurement result is transmitted to some hypothetical observer that we generally think of as being external to the system being described or considered.

We could, however, imagine that the measurement outcome is stored in a new register Y, whose classical state set is chosen to be Γ, rather than imagining that it is transmitted to an external observer. Taking this point of view, the measurement μ corresponds to a channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$, where

$$\Phi(X) = \sum_{a \in \Gamma} \langle \mu(a), X \rangle \, E_{a,a}$$

for every $X \in \mathrm{L}(\mathcal{X})$. For any density operator $\rho \in \mathrm{D}(\mathcal{X})$, the output $\Phi(\rho)$ is "classical" in the sense that it is a convex combination of states of the form $E_{a,a}$, which we identify with the classical state a for each $a \in \Gamma$.

Of course we expect that Φ should be a valid channel, but let us verify that this is so. It is clear that Φ is linear and preserves trace, as

$$\mathrm{Tr}(\Phi(X)) = \sum_{a \in \Gamma} \langle \mu(a), X \rangle \, \mathrm{Tr}(E_{a,a}) = \sum_{a \in \Gamma} \langle \mu(a), X \rangle = \langle \mathbb{1}_{\mathcal{X}}, X \rangle = \mathrm{Tr}(X)$$

for every $X \in \mathrm{L}(\mathcal{X})$. To see that Φ is completely positive we may compute the Choi-Jamiołkowski representation

$$J(\Phi) = \sum_{b,c \in \Sigma} \sum_{a \in \Gamma} \langle \mu(a), E_{b,c} \rangle \, E_{a,a} \otimes E_{b,c} = \sum_{a \in \Gamma} E_{a,a} \otimes \left(\sum_{b,c \in \Sigma} \langle \mu(a), E_{b,c} \rangle \, E_{b,c} \right) = \sum_{a \in \Gamma} E_{a,a} \otimes \mu(a)^{\mathsf{T}},$$

where we have assumed that $\mathcal{X} = \mathbb{C}^{\Sigma}$. Each $\mu(a)$ is positive semidefinite, and so $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, which proves that Φ is completely positive.

An alternate way to see that Φ is indeed a channel is to use Naimark's theorem, which implies that $\mu(a) = A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A$ for some isometry $A \in \mathrm{U}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$. It holds that

$$\Phi(X) = \sum_{a \in \Gamma} \langle A^*(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a})A, X \rangle E_{a,a} = \sum_{a \in \Gamma} E_{a,a} \operatorname{Tr}_{\mathcal{X}} (AXA^*) E_{a,a},$$

which is the composition of two channels: $\Phi = \Delta\Psi$, where $\Psi(X) = \operatorname{Tr}_{\mathcal{X}}(AXA^*)$ and

$$\Delta(Y) = \sum_{a \in \Gamma} E_{a,a} Y E_{a,a}$$

is the *completely dephasing channel* (which effectively zeroes out all off-diagonal entries of a matrix and leaves the diagonal alone). The composition of two channels is a channel, so we have that Φ is a channel.

6.1.2 Nondestructive measurements

Sometimes it is convenient to consider measurements that do not destroy registers, but rather leave them in some state that may depend on the measurement outcome that is obtained from the measurement. We will refer to such processes as *non-destructive measurements*.

Formally, a non-destructive measurement on a space $\mathcal{X}$ is a function

$$\nu : \Gamma \to \mathrm{L}(\mathcal{X}) : a \mapsto M_a,$$

for some finite, non-empty set of measurement outcomes Γ, that satisfies the constraint

$$\sum_{a \in \Gamma} M_a^* M_a = \mathbb{1}_{\mathcal{X}}.$$

When a non-destructive measurement of this form is applied to a register X that has reduced state $\rho \in \mathrm{D}(\mathcal{X})$, two things happen:

1. Each measurement outcome $a \in \Gamma$ occurs with probability $\langle M_a^* M_a, \rho \rangle$.
2. Conditioned on the measurement outcome $a \in \Gamma$ occurring, the reduced state of the register X becomes
$$\frac{M_a \rho M_a^*}{\langle M_a^* M_a, \rho \rangle}.$$

Let us now observe that non-destructive measurements really do not require new definitions, but can be formed from a composition of an operation and a measurement as we defined them initially. One way to do this is to follow the proof of Naimark's theorem. Specifically, let $\mathcal{Y} = \mathbb{C}^{\Gamma}$ and define an operator $A \in \mathrm{L}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ as

$$A = \sum_{a \in \Gamma} M_a \otimes e_a.$$

We have that

$$A^* A = \sum_{a \in \Gamma} M_a^* M_a = \mathbb{1}_{\mathcal{X}},$$

which shows that A is a linear isometry. Therefore, the mapping $X \mapsto AXA^*$ from $\mathrm{L}(\mathcal{X})$ to $\mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ is a channel. Now consider that this operation is followed by a measurement of $\mathcal{Y}$ with respect to the standard basis. Each outcome $a \in \Gamma$ appears with probability

$$\langle \mathbb{1}_{\mathcal{X}} \otimes E_{a,a}, A\rho A^* \rangle = \langle M_a^* M_a, \rho \rangle,$$

and conditioned on the outcome $a \in \Gamma$ appearing, the state of X becomes

$$\frac{\mathrm{Tr}_{\mathcal{Y}}\left[(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a}) A \rho A^*\right]}{\langle \mathbb{1}_{\mathcal{X}} \otimes E_{a,a}, A \rho A^* \rangle} = \frac{M_a \rho M_a^*}{\langle M_a^* M_a, \rho \rangle}$$

as required.

Viewing a nondestructive measurement as a channel, along the same lines as in the previous subsection, we see that it is given by

$$\Phi(X) = \sum_{a \in \Gamma} M_a X M_a^* \otimes E_{a,a} = \sum_{a \in \Gamma} (M_a \otimes e_a) X (M_a \otimes e_a)^*,$$

which is easily seen to be completely positive and trace-preserving using the Kraus representation characterization from the previous lecture.

6.2 Convex combinations of channels

Next we will discuss issues relating to the structure of the set of channels $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ for a given choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$.

Let us begin with the simple observation that convex combinations of channels are also channels: for any choice of channels $\Phi_0, \Phi_1 \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$, and any real number $\lambda \in [0, 1]$, it holds that

$$\lambda \Phi_0 + (1 - \lambda) \Phi_1 \in \mathrm{C}(\mathcal{X}, \mathcal{Y}).$$

One may verify this in different ways, one of which is to consider the Choi-Jamiołkowski representation:

$$J(\lambda \Phi_0 + (1 - \lambda) \Phi_1) = \lambda J(\Phi_0) + (1 - \lambda) J(\Phi_1).$$

Given that Φ_0 and Φ_1 are completely positive, we have $J(\Phi_0), J(\Phi_1) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, and because $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$ is convex it follows that

$$J(\lambda \Phi_0 + (1 - \lambda) \Phi_1) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}).$$

Thus, $\lambda \Phi_0 + (1 - \lambda) \Phi_1$ is completely positive. The fact that $\lambda \Phi_0 + (1 - \lambda) \Phi_1$ preserves trace is immediate by linearity. One could also verify the claim that $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ is convex somewhat more directly, by considering the definition of complete positivity.

It is also not difficult to see that the set $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ is compact for any choice of complex Euclidean spaces $\mathcal{X}$ and $\mathcal{Y}$. This may be verified by again turning to the Choi-Jamiołkowski representation. First, we observe that the set

$$\{P \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}) \,:\, \mathrm{Tr}(P) = \dim(\mathcal{X})\}$$

is compact, by essentially the same reasoning (which we have discussed previously) that shows the set $\mathrm{D}(\mathcal{Z})$ to be compact (for every complex Euclidean space $\mathcal{Z}$). Second, the set

$$\{X \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{X}) \,:\, \mathrm{Tr}_{\mathcal{Y}}(X) = \mathbb{1}_{\mathcal{X}}\}$$

is closed, for it is an affine subspace (in this case given by a translation of the kernel of the partial trace on $\mathcal{Y}$). The intersection of a compact set and a closed set is compact, so

$$\{P \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}) \,:\, \mathrm{Tr}_{\mathcal{Y}}(P) = \mathbb{1}_{\mathcal{X}}\}$$

is compact. Continuous mappings map compact sets to compact sets, and the mapping

$$J^{-1} : \mathrm{L}(\mathcal{Y} \otimes \mathcal{X}) \to \mathrm{T}(\mathcal{X}, \mathcal{Y})$$

that takes $J(\Phi)$ to Φ for each $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is continuous, so we have that $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ is compact.

6.2.1 Choi's theorem on extremal channels

Let us now consider the extreme points of the set $\mathrm{C}(\mathcal{X},\mathcal{Y})$. These are the channels that cannot be written as proper convex combinations of distinct channels. The extreme points of $\mathrm{C}(\mathcal{X},\mathcal{Y})$ can, in some sense, be viewed as being analogous to the pure states of $\mathrm{D}(\mathcal{X})$, but it turns out that the structure of $\mathrm{C}(\mathcal{X},\mathcal{Y})$ is more complicated than $\mathrm{D}(\mathcal{X})$. A characterization of the extreme points of this set is given by the following theorem.

Theorem 6.1 (Choi)**.** *Let $\{A_a : a \in \Sigma\} \subset \mathrm{L}(\mathcal{X},\mathcal{Y})$ be a linearly independent set of operators and let $\Phi \in \mathrm{C}(\mathcal{X},\mathcal{Y})$ be a quantum channel that is given by*

$$\Phi(X) = \sum_{a\in\Sigma} A_a X A_a^*$$

for all $X \in \mathrm{L}(\mathcal{X})$. The channel Φ is an extreme point of the set $\mathrm{C}(\mathcal{X},\mathcal{Y})$ if and only if

$$\{A_b^* A_a : (a,b) \in \Sigma\times\Sigma\}$$

is a linearly independent set of operators.

Proof. Let $\mathcal{Z} = \mathbb{C}^\Sigma$, and define $M \in \mathrm{L}(\mathcal{Z},\mathcal{Y}\otimes\mathcal{X})$ as

$$M = \sum_{a\in\Sigma} \operatorname{vec}(A_a) e_a^*.$$

Given that $\{A_a : a \in \Sigma\}$ is linearly independent, it holds that $\ker(M) = \{0\}$. It also holds that

$$MM^* = \sum_{a\in\Sigma} \operatorname{vec}(A_a)\operatorname{vec}(A_a)^* = J(\Phi).$$

Assume first that Φ is not an extreme point of $\mathrm{C}(\mathcal{X},\mathcal{Y})$. It follows that there exist channels $\Psi_0, \Psi_1 \in \mathrm{C}(\mathcal{X},\mathcal{Y})$, with $\Psi_0 \neq \Psi_1$, such that

$$\Phi = \frac{1}{2}\Psi_0 + \frac{1}{2}\Psi_1.$$

Let $P = J(\Phi)$, $Q_0 = J(\Psi_0)$, and $Q_1 = J(\Psi_1)$. As Φ, Ψ_0, and Ψ_1 are channels, one has that $P, Q_0, Q_1 \in \mathrm{Pos}(\mathcal{Y}\otimes\mathcal{X})$ and

$$\operatorname{Tr}_{\mathcal{Y}}(P) = \operatorname{Tr}_{\mathcal{Y}}(Q_0) = \operatorname{Tr}_{\mathcal{Y}}(Q_1) = \mathbb{1}_{\mathcal{X}}.$$

Moreover, as $\frac{1}{2}Q_0 \leq P$, it follows that $\operatorname{im}(Q_0) \subseteq \operatorname{im}(P) = \operatorname{im}(M)$, and therefore there exists a positive semidefinite operator $R_0 \in \mathrm{Pos}(\mathcal{Z})$ for which $Q_0 = MR_0M^*$. By similar reasoning, there exists a positive semidefinite operator $R_1 \in \mathrm{Pos}(\mathcal{Z})$ for which $Q_1 = MR_1M^*$. Letting $H = R_0 - R_1$, one finds that

$$0 = \operatorname{Tr}_{\mathcal{Y}}(Q_0) - \operatorname{Tr}_{\mathcal{Y}}(Q_1) = \operatorname{Tr}_{\mathcal{Y}}(MHM^*) = \sum_{a,b\in\Sigma} H(a,b)\left(A_b^* A_a\right)^{\mathsf{T}},$$

and therefore

$$\sum_{a,b\in\Sigma} H(a,b) A_b^* A_a = 0.$$

Given that $\Psi_0 \neq \Psi_1$, it holds that $Q_0 \neq Q_1$, so $R_0 \neq R_1$, and thus $H \neq 0$. It has therefore been shown that the set $\left\{A_b^* A_a : (a,b) \in \Sigma\times\Sigma\right\}$ is linearly dependent, as required.

Now assume the set $\left\{A_b^* A_a : (a,b) \in \Sigma \times \Sigma\right\}$ is linearly dependent: there exists a nonzero operator $Z \in \mathrm{L}(\mathcal{Z})$ such that

$$\sum_{a,b \in \Sigma} Z(a,b) A_b^* A_a = 0.$$

It follows that

$$\sum_{a,b \in \Sigma} Z^*(a,b) A_b^* A_a = \left(\sum_{a,b \in \Sigma} Z(a,b) A_b^* A_a \right)^* = 0$$

and therefore

$$\sum_{a,b \in \Sigma} H(a,b) A_b^* A_a = 0 \tag{6.1}$$

for both of the choices $H = Z + Z^*$ and $H = iZ - iZ^*$. At least one of the operators $Z + Z^*$ and $iZ - iZ^*$ must be nonzero when Z is nonzero, so one may conclude that the above equation (6.1) holds for a nonzero Hermitian operator $H \in \mathrm{Herm}(\mathcal{Z})$ that is hereafter taken to be fixed. Given that this equation is invariant under rescaling H, there is no loss of generality in assuming $\|H\| \leq 1$.

As $\|H\| \leq 1$ and H is Hermitian, it follows that $\mathbb{1} + H$ and $\mathbb{1} - H$ are both positive semidefinite, and therefore the operators $M(\mathbb{1} + H)M^*$ and $M(\mathbb{1} - H)M^*$ are positive semidefinite as well. Letting $\Psi_0, \Psi_1 \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ be the mappings that satisfy

$$J(\Psi_0) = M(\mathbb{1} + H)M^* \quad \text{and} \quad J(\Psi_1) = M(\mathbb{1} - H)M^*,$$

one therefore has that Ψ_0 and Ψ_1 are completely positive. It holds that

$$\mathrm{Tr}_{\mathcal{Y}}(MHM^*) = \sum_{a,b \in \Sigma} H(a,b) \left(A_b^* A_a\right)^{\mathsf{T}} = \left(\sum_{a,b \in \Sigma} H(a,b) A_b^* A_a \right)^{\mathsf{T}} = 0$$

and therefore

$$\mathrm{Tr}_{\mathcal{Y}}(J(\Psi_0)) = \mathrm{Tr}_{\mathcal{Y}}(MM^*) + \mathrm{Tr}_{\mathcal{Y}}(MHM^*) = \mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$$

and

$$\mathrm{Tr}_{\mathcal{Y}}(J(\Psi_1)) = \mathrm{Tr}_{\mathcal{Y}}(MM^*) - \mathrm{Tr}_{\mathcal{Y}}(MHM^*) = \mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}.$$

Thus, Ψ_0 and Ψ_1 are channels. Finally, given that $H \neq 0$ and $\ker(M) = \{0\}$ it holds that $J(\Psi_0) \neq J(\Psi_1)$, so that $\Psi_0 \neq \Psi_1$. As

$$\frac{1}{2} J(\Psi_0) + \frac{1}{2} J(\Psi_1) = MM^* = J(\Phi),$$

one has that

$$\Phi = \frac{1}{2}\Psi_0 + \frac{1}{2}\Psi_1,$$

which demonstrates that Φ is not an extreme point of $\mathrm{C}(\mathcal{X}, \mathcal{Y})$. □

6.2.2 Application of Carathéodory's theorem to convex combinations of channels

For an arbitrary channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$, one may always write

$$\Phi = \sum_{a \in \Gamma} p(a) \Phi_a$$

for some finite set Γ, a probability vector $p \in \mathbb{R}^{\Gamma}$, and $\{\Phi_a : a \in \Gamma\}$ being a collection of extremal channels. This is so because $\mathrm{C}(\mathcal{X}, \mathcal{Y})$ is convex and compact, and every compact and convex set is equal to the convex hull of its extreme points (by the Krein-Milman theorem). One natural question is: how large must Γ be for such an expression to exist? Carathéodory's theorem, which you will find stated in the Lecture 2 notes, provides an upper bound.

To explain this bound, let us assume $\mathcal{X} = \mathbb{C}^{\Sigma}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$. As explained in Lecture 1, we may view the space of Hermitian operators $\mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$ as a real vector space indexed by $(\Gamma \times \Sigma)^2$, and therefore having dimension $|\Sigma|^2 |\Gamma|^2$.

Now, the Choi-Jamiołkowski representation $J(\Phi)$ of any channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ is an element of $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, and is therefore an element of $\mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X})$. Taking

$$\mathcal{A} = \{J(\Psi) : \Psi \in \mathrm{C}(\mathcal{X}, \mathcal{Y}) \text{ is extremal}\} \subset \mathrm{Herm}(\mathcal{Y} \otimes \mathcal{X}),$$

and applying Carathéodory's theorem, we have that every element $J(\Phi) \in \mathrm{conv}(\mathcal{A})$ can be written as

$$J(\Phi) = \sum_{j=1}^{m} p_j J(\Psi_j)$$

for some probability vector $p = (p_1, \ldots, p_m)$ and some choice of extremal channels $\Psi_1, \ldots, \Psi_m$, for $m = |\Sigma|^2 |\Gamma|^2 + 1$. Equivalently, every channel $\Phi \in \mathrm{C}(\mathcal{X}, \mathcal{Y})$ can be written as a convex combination of no more than $m = |\Sigma|^2 |\Gamma|^2 + 1$ extremal channels.

This bound may, in fact, be improved to $m = |\Sigma|^2 |\Gamma|^2 - |\Sigma|^2 + 1$ by observing that the trace-preserving property of channels reduces the dimension of the smallest (affine) subspace in which they may be contained.

6.2.3 Mixed unitary channels

Suppose that $\mathcal{X}$ is a complex Euclidean space and $U \in \mathrm{U}(\mathcal{X})$ is a unitary operator. The mapping $\Psi \in \mathrm{T}(\mathcal{X})$ defined by

$$\Psi(X) = UXU^*$$

for all $X \in \mathrm{L}(\mathcal{X})$ is clearly a channel, and any such channel is called a *unitary channel*. Any channel $\Phi \in \mathrm{C}(\mathcal{X})$ that can be written as a convex combination of unitary channels is said to be a *mixed unitary channel*. (The term *random unitary channel* is more common, but it is easily confused with a different notion whereby one chooses a unitary channel randomly according to some distribution or measure.)

Again let us suppose that $\mathcal{X} = \mathbb{C}^{\Sigma}$. One may perform a similar calculation to the one above to find that every mixed unitary channel can be written as a convex combination of $|\Sigma|^4 - 2|\Sigma|^2 + 2$ unitary channels. The difference between this expression and the one from above comes from considering additional linear constraints satisfied by unitary channels—namely that they are unital in addition to being trace-preserving.

6.3 Discrete Weyl operators and teleportation

Now we will switch gears and discuss something different: the collection of so-called *discrete Weyl operators* and some examples of channels based on them. They also allow us to discuss a straightforward generalization of *quantum teleportation* to high-dimensional systems.

6.3.1 Definition of discrete Weyl operators

For any positive integer n, we define

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\},$$

and view this set as a ring with respect to addition and multiplication defined modulo n. Let us also define

$$\omega_n = \exp(2\pi i/n)$$

to be a principal n-th root of unity, which will typically be denoted ω rather than ω_n when n has been fixed or is clear from the context.

Now, for a fixed choice of n, let $\mathcal{X} = \mathbb{C}^{\mathbb{Z}_n}$, and define two unitary operators $X, Z \in \mathrm{U}(\mathcal{X})$ as follows:

$$X = \sum_{a \in \mathbb{Z}_n} E_{a+1,a} \qquad \text{and} \qquad Z = \sum_{a \in \mathbb{Z}_n} \omega^a E_{a,a}.$$

Here, and throughout this section, the expression $a+1$ refers to addition in $\mathbb{Z}_n$, and similar for other arithmetic expressions involving elements of $\mathbb{Z}_n$. Finally, for any choice of $(a, b) \in \mathbb{Z}_n^2$ we define

$$W_{a,b} = X^a Z^b.$$

Such operators are known as *discrete Weyl operators* (and also as *generalized Pauli operators*).

Let us note a few basic facts about the collection

$$\{W_{a,b} \,:\, (a, b) \in \mathbb{Z}_n^2\}. \tag{6.2}$$

First, we have that each $W_{a,b}$ is unitary, given that X and Z are obviously unitary. Next, it is straightforward to show that

$$\operatorname{Tr}(W_{a,b}) = \begin{cases} n & \text{if } a = b = 0 \\ 0 & \text{otherwise.} \end{cases}$$

This implies that the collection (6.2) forms an orthogonal basis for $\mathrm{L}(\mathcal{X})$, because

$$\langle W_{a,b}, W_{c,d} \rangle = \operatorname{Tr}\left(Z^{-b} X^{-a} X^c Z^d\right) = \operatorname{Tr}\left(X^{c-a} Z^{d-b}\right) = \begin{cases} n & \text{if } (a, b) = (c, d) \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we note the *commutation relation*

$$ZX = \omega XZ,$$

which (for instance) implies

$$W_{a,b} W_{c,d} = (X^a Z^b)(X^c Z^d) = \omega^{bc} X^{a+c} Z^{b+d} = \omega^{bc-ad} (X^c Z^d)(X^a Z^b) = \omega^{bc-ad} W_{c,d} W_{a,b}.$$

6.3.2 Dephasing and depolarizing channels

Two simple examples of mixed unitary channels, where the corresponding unitary operators are chosen to be discrete Weyl operators, are as follows:

$$\Delta(A) = \frac{1}{n}\sum_{a\in\mathbb{Z}_n} W_{0,a} A W_{0,a}^{*} \qquad \text{and} \qquad \Omega(A) = \frac{1}{n^2}\sum_{a,b\in\mathbb{Z}_n} W_{a,b} A W_{a,b}^{*}.$$

We have already encountered Δ in this lecture: it is the completely dephasing channel that zeros out off-diagonal entries and leaves the diagonal alone. To see that this is so, we may compute the action of this channel on the standard basis of $\mathrm{L}(\mathcal{X})$:

$$\Delta(E_{c,d}) = \frac{1}{n}\sum_{a\in\mathbb{Z}_n} W_{0,a} E_{c,d} W_{0,a}^{*} = \left(\frac{1}{n}\sum_{a\in\mathbb{Z}_n}\omega^{a(c-d)}\right) E_{c,d} = \begin{cases} E_{c,d} & \text{if } c = d\\ 0 & \text{if } c \neq d.\end{cases}$$

Alternately we may compute the action on the basis of discrete Weyl operators:

$$\Delta(W_{c,d}) = \frac{1}{n}\sum_{a\in\mathbb{Z}_n} W_{0,a} W_{c,d} W_{0,a}^{*} = \left(\frac{1}{n}\sum_{a\in\mathbb{Z}_n}\omega^{ac}\right) W_{c,d} = \begin{cases} W_{c,d} & \text{if } c = 0\\ 0 & \text{if } c \neq 0.\end{cases}$$

The discrete Weyl operators of the form $W_{c,d}$ for $c = 0$ span precisely the diagonal operators, so we see that this expression is consistent with the one involving the standard basis.

The channel Ω is known as the *completely depolarizing channel*, or the *maximally noisy channel*. We have

$$\Omega(W_{c,d}) = \frac{1}{n^2}\sum_{a,b\in\mathbb{Z}_n} W_{a,b} W_{c,d} W_{a,b}^{*} = \left(\frac{1}{n^2}\sum_{a,b\in\mathbb{Z}_n}\omega^{bc-ad}\right) W_{c,d} = \begin{cases} W_{c,d} & \text{if } (c,d) = (0,0)\\ 0 & \text{otherwise.}\end{cases}$$

The output is always a scalar multiple of $W_{0,0} = \mathbb{1}$. We may alternately write

$$\Omega(A) = \frac{\operatorname{Tr}(A)}{n}\mathbb{1}.$$

For every $\rho \in \mathrm{D}(\mathcal{X})$ we therefore have $\Omega(\rho) = \mathbb{1}/n$, which is the maximally mixed state: nothing but noise comes out of this channel.

6.3.3 Weyl covariant channels

The channels Δ and Ω above exhibit an interesting phenomenon, which is that the discrete Weyl operators are eigenvectors of them, in the sense that $\Delta(W_{a,b}) = \lambda_{a,b} W_{a,b}$ for some choice of $\{\lambda_{a,b}\} \subset \mathbb{C}$ (and likewise for Ω). This property holds for all channels given by convex combinations of unitary channels corresponding to the discrete Weyl operators. In general, channels of this form are called *Weyl covariant channels*. This can be demonstrated using the commutation relations noted above.

In greater detail, let us take $M \in \mathrm{L}\left(\mathbb{C}^{\mathbb{Z}_n}\right)$ to be any operator, and consider the mapping

$$\Phi(A) = \sum_{a,b\in\mathbb{Z}_n} M(a,b) W_{a,b} A W_{a,b}^{*}.$$

We have

$$\Phi(W_{c,d}) = \sum_{a,b\in\mathbb{Z}_n} M(a,b) W_{a,b} W_{c,d} W_{a,b}^* = \left(\sum_{a,b\in\mathbb{Z}_n} M(a,b)\omega^{bc-ad}\right) W_{c,d} = N(c,d) W_{c,d}$$

for

$$N(c,d) = \sum_{a,b\in\mathbb{Z}_n} M(a,b)\omega^{bc-ad}.$$

Alternately, we may write

$$N = V M^{\mathsf{T}} V^*,$$

where

$$V = \sum_{b,c\in\mathbb{Z}_n} \omega^{bc} E_{c,b}$$

is the operator typically associated with the *discrete Fourier transform*.

6.3.4 Teleportation

Suppose that X, Y_{A}, and Y_{B} are registers, all having classical state set $\mathbb{Z}_n$ for some arbitrary choice of a positive integer n (such as $n = 8,675,309$, which is known as *Jenny's number*). Alice is holding X and Y_{A}, while Bob has Y_{B}. The pair $(\mathsf{Y}_{\mathsf{A}}, \mathsf{Y}_{\mathsf{B}})$ was long ago prepared in the pure state

$$\frac{1}{\sqrt{n}} \operatorname{vec}(\mathbb{1}) = \frac{1}{\sqrt{n}} \sum_{a\in\mathbb{Z}_n} e_a \otimes e_a,$$

while X was recently acquired by Alice. Alice wishes to *teleport* the state of X to Bob by sending him only classical information. To do this, Alice measures the pair $(\mathsf{X}, \mathsf{Y}_{\mathsf{A}})$ with respect to the *generalized Bell basis*

$$\left\{ \frac{1}{\sqrt{n}} \operatorname{vec}(W_{a,b}) \,:\, (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n \right\}. \tag{6.3}$$

She transmits to Bob whatever result $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ she obtains from her measurement, and Bob "corrects" Y_{B} by applying to it the unitary channel

$$\sigma \mapsto W_{a,b} \sigma W_{a,b}^*.$$

We may express this entire procedure as a channel from X to Y_{B}, where the preparation of $(\mathsf{Y}_{\mathsf{A}}, \mathsf{Y}_{\mathsf{B}})$ is included in the description so that it makes sense to view Y_{B} as having been created in the procedure. This channel is given by

$$\Phi(\rho) = \frac{1}{n} \sum_{(a,b)\in\mathbb{Z}_n\times\mathbb{Z}_n} \left(\operatorname{vec}(W_{a,b})^* \otimes W_{a,b}\right) \left(\rho \otimes \frac{1}{n} \operatorname{vec}(\mathbb{1}) \operatorname{vec}(\mathbb{1})^*\right) \left(\operatorname{vec}(W_{a,b}) \otimes W_{a,b}^*\right).$$

To simplify this expression, it helps to note that

$$\operatorname{vec}(\mathbb{1}) \operatorname{vec}(\mathbb{1})^* = \frac{1}{n} \sum_{c,d} \overline{W_{c,d}} \otimes W_{c,d}.$$

We find that

$$
\begin{aligned}
\Phi(W_{e,f}) &= \frac{1}{n^3} \sum_{a,b,c,d \in \mathbb{Z}_n} \left(\operatorname{vec}(W_{a,b})^* \otimes W_{a,b}\right) \left(W_{e,f} \otimes \overline{W_{c,d}} \otimes W_{c,d}\right) \left(\operatorname{vec}(W_{a,b}) \otimes W_{a,b}^*\right) \\
&= \frac{1}{n^3} \sum_{a,b,c,d \in \mathbb{Z}_n} \operatorname{Tr}\left(W_{a,b}^* W_{e,f} W_{a,b} W_{c,d}^*\right) W_{a,b} W_{c,d} W_{a,b}^* \\
&= \frac{1}{n^3} \sum_{a,b,c,d \in \mathbb{Z}_n} \left\langle W_{c,d}, W_{e,f} \right\rangle W_{c,d} \\
&= \frac{1}{n} \sum_{c,d \in \mathbb{Z}_n} \left\langle W_{c,d}, W_{e,f} \right\rangle W_{c,d} \\
&= W_{e,f}
\end{aligned}
$$

for all $e, f \in \mathbb{Z}_n$. Thus, Φ is the identity channel—so the teleportation has worked as expected.