Weyl Covariant Channel

Let's consider some n that's a positive integer. Then let's consider $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ (addition and multiplication modulo n turns this into a ring.

Consider the nth roots of unity $\omega = \exp(2\pi i/n)$.

We will define the following operators

$$U = \sum_{a \in \mathbb{Z}_n} E_{a+1,a}$$

$U|a\rangle = |a+1\rangle$

$$V = \sum_{a \in \mathbb{Z}_n} \omega^a E_{a,a}$$

$V|a\rangle = \omega^a |a\rangle$

Now we'll define

$$W_{a,b} = U^a V^b \quad \text{for} \quad (a, b \in \mathbb{Z}_n)$$

These $W_{a,b}$s are the discrete Weyl operators (generalized Pauli operators).

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

Note that sometimes people add a phase to the definition of the Weyl operators. It doesn't change anything. This is a pretty special collection of operators.

1. All Weyl operators are unitary.
2. They form an orthogonal basis.

Let's check to see if these things are true.

Imagine that we have

$$\begin{aligned} \langle W_{a,b}, W_{c,d} \rangle &= Tr(V^{-b} U^{-a} U^c V^d) \\ &= Tr(U^{c-a} V^{d-b}) \quad \text{by the cyclic property of the trace} \end{aligned}$$

The trace is equal to zero if $a \neq 0$. If $a = 0$ and $b = 0$ then the trace is identity. If $a = 0$ and $b \neq 0$ then the trace will be zero because we'll be summing all the roots of unity.

There's an easy way to see why the sum of all the roots of unity is zero.

$$\begin{aligned} \sum_{c=0}^{n-1} &= \sum_{c=0}^{n-1} \left(\omega^b\right)^c \\ &= \frac{\omega^{bn} - 1}{\omega^b - 1} = 0 \end{aligned}$$

Thus

$$Tr(U^{c-a}V^{d-b}) = \begin{cases} n & \text{if } c = a \text{ and } d = b \\ 0 & \text{if 0 or } \omega \end{cases} \tag{1}$$

We can also show that $VU = \omega UV$ because $W_{a,b}W_{c,d} = \omega^{bc}W_{a+c,b+d}$
We can consider channels of the form

$$\Phi(X) = \sum_{a,b)\in\mathbb{Z}_n\times\mathbb{Z}_n} p(a,b)W_{a,b}XW_{a,b}^*$$

for $p \in P(\mathbb{Z}_n \times \mathbb{Z}_n)$ a probability vector are called **Weyl-covariant channels**. These are interesting channels.

Complete Depolarizing Channel: A Weyl-Covariant Channel

Consider the following channel: The completely depolarizing channel:

$$\Omega(X) = Tr(X)\frac{\mathbb{1}}{n}$$

for every $X \in L(\mathbb{C}^{\mathbb{Z}_n})$ is a Weyl-covariant channel.

$$\begin{aligned}
\Omega(X) &= \frac{1}{n^2}\sum_{(a,b)\in\mathbb{Z}_n\times\mathbb{Z}_n} W_{a,b}XW_{a,b}^* \\
J(\Omega) &= \frac{1}{n^2}\sum_{a,b} vec(W_{a,b})vec(W_{a,b})^* \\
&= \frac{1}{n}\mathbb{1}\times\mathbb{1}
\end{aligned}$$

Now we've filled in a missing detail from last week. The completely depolarizing channel is a completely mixed channel.

Consider another example: The completely dephasing channel

Complete Dephasing Channel: A Weyl-Covariant Channel

Consider the completely dephasing channel

$$\Delta(X) = \sum_{a\in\mathbb{Z}_n} X(a,a)E_{a,a}$$

$$\begin{aligned}
\Delta(X) &= \frac{1}{n}\sum_{b\in\mathbb{Z}_n} W_{0,b}XW_{0,b}^* \\
&= \frac{1}{n}\sum_{b\in\mathbb{Z}_n} V^bXV^-b
\end{aligned}$$

$\Delta(E_{c,d}) = \frac{1}{n}\sum_b \omega^{b,c}\omega^{-db}E_{c,d}$. Rewriting this slightly: $\frac{1}{n}\sum_b \omega^{b(c-d)}E_{c,d}$.

So, now:

$$\Delta(E_{c,d}) = \begin{cases} E_{c,c} & \text{if } c = d \\ 0 & \text{if } c \neq d \end{cases}$$

Application of Majorization

Schur's Theorem

Let $\mathcal{X} = \mathbb{C}^n$ and let $H = Herm(\mathbb{C}^n)$. We will define $u \in \mathcal{X}$ as $u(k) = H(k,k)$ for each $k = 1, \ldots, n$. It holds that $\lambda(H) \succ u$.

Proof: We have $H \succ \Delta(H)$. This holds by definition. Because Δ is mixed unitary this holds. Therefore, the vector of eigenvalues of H majorizes $\lambda(\Delta(H)) = u$ since Δ diagonalizes H (we can just read the eigenvalues off of the diagonal).

We can generalize this theorem: Take any complex Euclidean space $\mathcal{X} = \mathbb{C}^\Sigma$, $\{x_a : a \in \Sigma\}$ for $\{x_a : a \in \Sigma\}$ an orthonormal basis of $\mathcal{X}$. For $H \in Herm(\mathcal{X})$ and $u \in \mathcal{X}$ we have $u(a) = x_a^* H x_a$ for each $a \in \Sigma$.

It holds that $\lambda(H) \succ u$. One thing to conclude from this is that if we had some orthornormal basis $\{x_a : a \in \Sigma\}$ and some density operator $\rho \in D(\mathcal{X})$ then $p(a)x_a^*\rho x_a$. This tells us that the $p(a)$ will be at least as mixed up as the vector of eigenvalues. If you measure a density operator, the measurement that yields the least entropy is the one where you have measured with respect to the eigenvectors of ρ.

We may wonder if there exists a converse to this theorem. There does, indeed, exist such a theorem. In other words, assume we have that $\mathcal{X} = \mathbb{C}^\Sigma$ and $H \in Herm(\mathcal{X})$. Consider $v \in \mathcal{X}$ where v is any vector which is majorized by the vector of eigenvalues : $\lambda(H) \succ v$. Does there exist an orthonormal basis that will give us $v(a) = x_a^* H x_a$ for all $a \in \Sigma$? Yes, this theorem was proven by Horn.

Horn's Theorem

The proof for Horn's theorem follows:

$$H = \sum_{a\in\Sigma} w(a) u_a u_a^*$$

is a spectral decomposition. From last time we "know" (theorem unproven) that there must exist a unitary operator U such that

$$Dw = v$$

For $D(a,b) = |U(a,b)|^2$. Now, we'll define

$$V = \sum_{a\in\Sigma} e_a u_a^*$$

and define

$$x_a = V^*U^*Vu_a \quad \text{for each } a \in \Sigma$$

Do these definitions work?

$$\begin{aligned}
x_a^* H x_a &= u_a^* V^* U V H V^* U^* V u_a \\
&= e_a^* U V H V^* U^* e_a \\
&= e_a^* U (\sum_b w(b) E_{b,b}) U^* e_a \\
&= \sum_b w(b) \left| U(a,b) \right|^2 \\
&= \sum_b D(a,b) w(b) \\
&= (Dw)(a) \\
&= v(a)
\end{aligned}$$

This does what we want so we're done! This relies on the fact that the unitary operator U exists. Majorization is discussed well in Bathia/Battia/Batia.

Final Application (for now) of Majorization

The theorem: Let $\rho \in D(\mathcal{X})$ and $\mathcal{X} = \mathbb{C}^\Sigma$ and let $p \in P(\Sigma)$. You might wonder when it's possible to write ρ as a convex combination of pure states using p as a probability vector. There exist a (not-necessarily) orthonormal collection $\{u_a : a \in \Sigma\}$ such that $\rho = \sum\limits_{a\in\Sigma} p(a) u_a u_a^*$ if and only if $\lambda(\rho) \succ p$.

The proof: Assume, first, that $\lambda(\rho) \succ p$. Because this holds we know from Schur-Horn's theorem (particularly the "Horn" part) that there must be some $\{x_a : a \in \Sigma\}$ (orthonormal basis) such that $p(a) = x_a^* \rho x_a$ for all $a \in \Sigma$.

Allow

$$y_a = \sqrt{\rho} x_a \quad \text{for each } a \in \Sigma$$

$||y_a||^2 = \langle y_a, y_a \rangle = x_a^* \sqrt{p} \sqrt{\rho} x_a = p(a)$

Define:

$$u_a = \begin{cases} \frac{y_a}{||y_a||^2} & \text{if } y_a \neq 0 \\ z \quad \text{if } y_a = 0 \end{cases}$$

for z being an arbitrary unit vector.

$$\begin{aligned}\sum_a p(a) u_a u_a^* &= \sum_a y_a y_a^* \\ &= \sum_a \sqrt{p} x_a x_a^* \sqrt{p} \\ &= \sqrt{p} \mathbb{1} \sqrt{p} = \rho\end{aligned}$$

Suppose on the other hand that

$$\rho = \sum_a p(a) u_a u_a^*$$

for some choice of unit vectors $\{u_a : a \in \Sigma\}$.
Now, define:

$$A = \sum_{a \in \Sigma} \sqrt{p(a)} u_a e_a^*$$

Note that

$$AA^* = \sum_a p(a) u_a u_a^* = \rho$$

When you have an expression like it's worth considering what A^*A is.

$$A^*A = \sum_{a,b} \sqrt{p(a)p(b)} (u_a^* u_b) e_a e_b^*$$

so

$$e_a^* A^* A e_a = p(a) \quad \text{by orthonormality of } e_a$$

The ath diagonal entry of A^*A is just $p(a)$. The diagonal entries of A^*A correspond to p. $\lambda(A^*A) \succ p$. But

$$\lambda(p) = \lambda(AA^*) = \lambda(A^*A) \succ p$$

This is what we wanted so we're done!