Recap

- $\mathcal{N}: A \to B$ quantum channel, G group with unitary reps U_g on $\mathcal{H}_A$, V_g on $\mathcal{H}_B$. $\mathcal{N}$ is called (G, U_g, V_g)-covariant, if

$$V_g \mathcal{N}(\cdot) V_g^\dagger = \mathcal{N}(U_g \cdot U_g^\dagger) \quad \text{for all } g \in G.$$

- Let $|A| = |B| = d$. If $\mathcal{N}: A \to B$ is $(\mathcal{U}(d), U, U)$-covariant ("natural representation of $\mathcal{U}(d)$"), then $\mathcal{N}$ is a depolarizing channel:

$$\mathcal{N}(X) = (1-q) X + q \operatorname{tr}(X) \frac{1}{d} \mathbb{1}_d,$$

where $q = \frac{f - d^2}{1 - d^2}$ with $f = \langle \gamma | \tau^{\mathcal{N}} | \gamma \rangle$

- Proof used structure of so-called "Werner states":

If $R = (U \otimes U) R (U \otimes U)^\dagger$ for all $U \in \mathcal{U}(d)$, then

$$R = x \mathbb{1}_{AB} + y F_{AB} \quad \text{for some } x, y \in \mathbb{C}.$$

- Ways to prove this statement: (Part of) Schur-Weyl duality

Let $R \in B((\mathbb{C}^d)^{\otimes N})$: If $R = U^{\otimes N} R (U^\dagger)^{\otimes N}$ for all $U \in \mathcal{U}(d)$,

then $R = \sum_{\pi \in S_N} c_\pi P_\pi$, where P_π acts on $(\mathbb{C}^d)^{\otimes N}$ by

permuting tensor factors: $P_\pi \bigotimes_{i=1}^N |\psi_i\rangle = \bigotimes_{i=1}^N |\psi_{\pi^{-1}(i)}\rangle$

- Alternatively: brute-force argument (easy for $d = 2$)

§3.2 Channel twirling

$\mathcal{N}: A \to B$, G group with U_g on $\mathcal{H}_A$, V_g on $\mathcal{H}_B$ unitary representations

→ how do we impose (G, U_g, V_g)-covariance on $\mathcal{N}$?

i) G finite:

$$\mathcal{N}_G = \frac{1}{|G|} \sum_{g \in G} V_g^\dagger \, \mathcal{N}(U_g \cdot U_g^\dagger) \, V_g$$

Prop 20 $\mathcal{N}_G$ is (G, U_g, V_g)-covariant.

Proof: Recall proof of Prop 17: $(\mathbb{1}_A \otimes U_g)|\gamma\rangle = (U_g^T \otimes \mathbb{1}_{A'})|\gamma\rangle$

transpose trick (ricochet lemma)

$$\Rightarrow \tilde{\tau} = \tau^{\mathcal{N}_G} = \frac{1}{|G|} \sum_{g \in G} (\bar{U}_g \otimes V_g) \, \tau^{\mathcal{N}} \, (\bar{U}_g \otimes V_g)^\dagger \qquad (*)$$

Prop 17: $\mathcal{N}_G$ is (G, U_g, V_g)-covariant iff

$$\tilde{\tau} = (\bar{U}_g \otimes V_g) \, \tilde{\tau} \, (\bar{U}_g \otimes V_g)^\dagger \quad \forall g \in G.$$

$g \in G$: $(\bar{U}_g \otimes V_g) \, \tilde{\tau} \, (\bar{U}_g \otimes V_g)^\dagger$ $\qquad \bar{U}_g \bar{U}_h \otimes V_g V_h$

$$\overset{(*)}{=} \frac{1}{|G|} \sum_{h \in G} (\bar{U}_g \otimes V_g)(\bar{U}_h \otimes V_h) \, \tau^{\mathcal{N}} \, (\bar{U}_h \otimes V_h)^\dagger (\bar{U}_g \otimes V_g)^\dagger$$

$U_{gh} = U_g U_h$ ↘

$$= \frac{1}{|G|} \sum_{h \in G} (\bar{U}_{gh} \otimes V_{gh}) \, \tau^{\mathcal{N}} \, (\bar{U}_{gh} \otimes V_{gh})^\dagger$$

$h \mapsto gh$ for fixed g is a bijection G.

$$= \frac{1}{|G|} \sum_{h \in G} (\bar{U}_h \otimes V_h)\, \tau^N\, (\bar{U}_h \otimes V_h)^\dagger$$

$$\overset{(*)}{=} \widehat{\tau} \qquad \square$$

·) G is not finite → averaging operation?

Let G be a locally compact group (every point in G has a compact neighborhood)

Then exists a unique (up to normalization) measure μ on G called the Haar measure satisfying:

1a) Left-invariance: $\mu(gS) = \mu(S)$ $\forall g \in G$, $S \subseteq G$ Borel set

- OR -

1b) Right-invariance: $\mu(Sg) = \mu(S)$ $\forall g \in G$, $S \subseteq G$ Borel set

2) $\mu(K) < \infty$ for $K \subseteq G$ compact

G compact: ·) G locally compact and $\mu(G) < \infty$ (take $\mu(G) = 1$)

·) Haar measure is <u>both</u> left- and right-invariant

Define the Haar integral $\int_G d\mu(g)\, f(g)$ → averaging operation!

Examples of compact (Lie) groups: $U(d)$, $SU(d)$, $O(d)$, $SO(d)$, $Sp(n)$

$G = U(d)$, φ, ψ unitary rep's on $\mathcal{H}_A$, $\mathcal{H}_S$:

channel twirling: $N_G = \int_G d\mu(U)\, \psi(U)^\dagger\, N(\varphi(U) \cdot \varphi(U)^\dagger)\, \psi(U)$

If G is finite: $\int_G d\mu(g) \to \frac{1}{|G|} \sum_{g \in G}$ counting measure

Prop 21 Let $\mathcal{N}: A \to B$ be a quantum channel, $|A| = |B| = d$.

Then $\mathcal{N}_{U(d)}$ is $(U(d), U, U)$-covariant, and

hence a depolarizing channel:

$$\mathcal{N}_{U(d)}(X) = (1-q)X + q\,\mathrm{tr}(X)\,\frac{1}{d}\mathbb{1}_d$$

where $q = \frac{f - d^2}{1 - d^2}$ with $f = \langle \gamma | \tau^{\mathcal{N}} | \gamma \rangle$.

Proof: $(U(d), U, U)$-covariance of $\mathcal{N}_{U(d)} = \int_{U(d)} dU\, U^\dagger \mathcal{N}(U \cdot U^\dagger) U$

uses same proof as in Prop 20 with $\frac{1}{|G|}\sum_{g \in G} \leftrightarrow \int_{U(d)} dU$,

using left-invariance of Haar measure.

Prop 18
$\Rightarrow$ $\mathcal{N}_{U(d)}(X) = (1-q)X + q\,\mathrm{tr}(X)\,\frac{1}{d}\mathbb{1}_d \qquad q = \frac{f - d^2}{1 - d^2}$

$$f = \langle \gamma | \tau^{\mathcal{N}} | \gamma \rangle = \langle \gamma | (\mathrm{id} \otimes \mathcal{N})(|\gamma\rangle\langle\gamma|) | \gamma \rangle$$

$|\phi^+\rangle = \frac{1}{\sqrt{d}} |\gamma\rangle$: $\langle \phi^+ | \mathrm{id} \otimes \mathcal{N} | \phi^+ \rangle \, | \phi^+ \rangle = F(\mathcal{N})$

entanglement fidelity

$d^2 F = f$

$$f \overset{!}{=} \langle\gamma| id \otimes \mathcal{N}_{\psi(d)}(\gamma) |\gamma\rangle$$

$$= \langle\gamma| \int dU \, (\mathbb{1} \otimes U^\dagger)(id \otimes \mathcal{N}) \big(\underbrace{(\mathbb{1} \otimes U)|\gamma\rangle\langle\gamma|(\mathbb{1} \otimes U^\dagger)}_{(V^T \otimes \mathbb{1})|\gamma\rangle} \big) (\mathbb{1} \otimes U) |\gamma\rangle$$

$$= \int dU \, \langle\gamma| (V^T \otimes U^\dagger) \underbrace{(id \otimes \mathcal{N})(\gamma)}_{= \tau^{\mathcal{N}}} \underbrace{(\bar{V} \otimes U)|\gamma\rangle}_{\mathbb{1} \otimes \underbrace{U(\bar{U})^T}_{= UU^\dagger = \mathbb{1}} |\gamma\rangle}$$

$$= \underbrace{\int dU}_{= 1} \langle\gamma| \tau^{\mathcal{N}} |\gamma\rangle = f \qquad \square$$

§ 3.3 Irreducibly covariant channels and minimum entropy

Recall: ·) a representation (φ, R) of a group G is called irreducible, if $\{0\}$ and R are the only G-invariant subspaces. ($S \subseteq R$ G-inv., if $\varphi(g)s \in S$ $\forall g \in G, s \in S$)

·) Let (φ_1, R_1), (φ_2, R_2) be rep's of a group G.
A linear map $f: R_1 \to R_2$ is called G-linear (G-equivariant), if $f \circ \varphi_1(g) = \varphi_2(g) \circ f$ $\forall g \in G$.

·) Schur's lemma: Let $(\varphi_1, R_1), (\varphi_2, R_2)$ be irreducible,

$f: R_1 \to R_2$ a G-linear map. $\varphi_2(g) \circ f = f \circ \varphi_1(g)$

Then: ·) $R_1 \not\cong R_2$ and $f = 0$

or ·) $R_1 \cong R_2$ and $f = \lambda \, id_{R_1 \to R_2}$ for some $\lambda \in \mathbb{C}$

Lemma 22 An irreducible rep (φ, R) of a compact group G forms a 1-design: $\frac{1}{|G|} \sum_{g \in G} \varphi(g) X \varphi(g)^\dagger = \frac{\mathrm{tr} X}{d} \mathbb{1}_R$, $d = |R|$

$\left(\frac{1}{|G|}\sum_{g\in G} \leftrightarrow \int_G d\mu\right)$ for all $X \in B(R)$.

Proof: Let $Y = \frac{1}{|G|} \sum_{g \in G} \varphi(g) X \varphi(g)^\dagger$.

$\Rightarrow \varphi(g) Y \varphi(g)^\dagger = Y \quad \forall g \in G$ (we've proved this before!)

$\varphi(g) Y = Y \varphi(g)$ $\overset{\text{Schur's lemma}}{\Rightarrow}$ $Y = c \cdot \mathbb{1}_R$ for some $c \in \mathbb{C}$.

($\varphi(g) X \varphi(g)^\dagger \in B(R)$)

$\mathrm{tr} Y = d \cdot c = \frac{1}{|G|} \sum_{g \in G} \underbrace{\mathrm{tr}\left(\varphi(g) X \varphi(g)^\dagger\right)}_{\mathrm{tr} X} = \mathrm{tr} X \Rightarrow c = \frac{\mathrm{tr} X}{d}$.

$d = \dim R$

□