Math seminar @ Shanghai university.

1. Short tour of Q.M & Q.I.T.
2. Decoupling approach.
3. Main result. (decoupling with unitary design)
4. Proof ideas.
5. Conclusion & open problems.

1. Short tour of Q.M. & Q.I.T.

1-1. Three axioms of Q.M.

Axiom 1.

- Physical system = Hilbert space $\mathcal{H}$ ($d := \dim \mathcal{H} < \infty$)
- State: $\{\rho \in \mathrm{Her}(\mathcal{H})$ s.t. $\rho \geq 0$ & $\mathrm{Tr}\,\rho = 1\} =: \mathcal{S}(\mathcal{H})$
  - Pure state $\psi \iff \mathrm{rank}\,\psi = 1$. ($\psi = |\psi\rangle\langle\psi|$ where $|\psi\rangle \in \mathcal{H}$ & $\langle\psi| = (|\psi\rangle)^\dagger$).
  - Mixed state $\rho \iff \mathrm{rank}\,\rho > 1$.
- Two systems $\underset{\rho^A}{\mathcal{H}^A}$ & $\underset{\sigma^B}{\mathcal{H}^B} \Rightarrow$ Whole: $\underbrace{\mathcal{H}^A \otimes \mathcal{H}^B}_{\rho^{AB}}$.
  - Maximally entangled state: $|\Phi\rangle^{AB} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |e_i\rangle^A \otimes |f_i\rangle^B$ (Basis) ($d = \min\{d_A, d_B\}$)

    no classical counterpart & resource of Q.I.T.

Axiom 2.

- Dynamics = completely positive (CP) & trace preserving (TP) map.

$\mathcal{J}^{A\to B} : \mathcal{L}(\mathcal{H}^A) \to \mathcal{L}(\mathcal{H}^B)$

$$\begin{cases} \text{CP} \iff \forall \rho^{AC} \geq 0,\ (\mathcal{J}^{A\to B} \otimes \mathrm{id}^C)(\rho^{AC}) \geq 0. \\ \text{TP} \iff \mathrm{Tr}[\mathcal{J}^{A\to B}(\rho^A)] = \mathrm{Tr}[\rho^A]. \end{cases}$$

E.g.)

- Unitary dynamics: $U \rho U^\dagger$. (U is unitary).
- Partial trace: $AB \to A$. "Forget B"

$$\mathrm{Tr}_B[\rho^{AB}] := \sum_{j=1}^{d_B} (I^A \otimes \langle e_j|^B)\, \rho^{AB}\, (I^A \otimes \underbrace{|e_j\rangle^B}_{\text{Basis in } \mathcal{H}^B}).$$

Axiom 3. Measurement ---- skip.

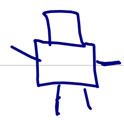
1-2. Q.I.T

Goal of Q.I.T.

Based on the 3 axioms of Q.M.,
what information processing can we do ?

e.g.) • Sending info. (internet)
• computation etc....

Sending Q. info.

Alice  $\rho \xrightarrow[\mathcal{N}^{A\to B}_{CPTP}]{\text{send !!}} \mathcal{N}^{A\to B}(\rho) \neq \rho$ Bob 

→ :-), if gets ρ from $\mathcal{N}^{A\to B}(\rho)$
:-(, otherwise.

Find a pair of CPTP maps $(\mathcal{E}^{\hat{A}\to A}, \mathcal{D}^{B\to\hat{A}})$ s.t.

$$\left\| \mathcal{D}^{B\to\hat{A}} \circ \mathcal{N}^{A\to B} \circ \mathcal{E}^{\hat{A}\to A}(\rho^{\hat{A}}) - \rho^{\hat{A}} \right\|_1 \leq \varepsilon.$$

where $\|X\|_1 = \mathrm{Tr}\sqrt{X^\dagger X}$.   error

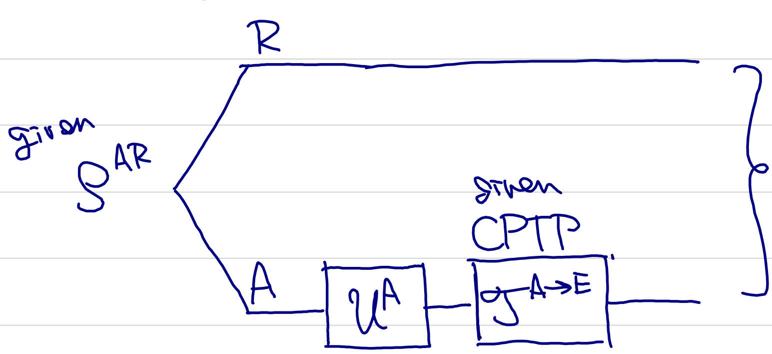
what if
• $\rho^{\hat{A}} = (\rho^{\hat{a}})^{\otimes N}$ for large N : asymptotic situation ⟹ Q. Shannon theory
• A & B share M.E.S. ⟹ entanglement assisted.
⋮ many variants

⟸ Various "entropies" determine if $\exists(\mathcal{E}, \mathcal{D})$.

2. Decoupling approach.

- Schumacher & Westmoreland '02.
- Devetak '05
- Devetak & Winter '04 etc...

<u>Decoupling protocol.</u>



$$= \mathcal{T}^{A\to E}(\mathcal{U}^A \rho^{AR} \mathcal{U}^{A\dagger}) \overset{?}{\approx} \tau^E \otimes \rho^R$$

State is "decoupled"

$\rho^R = \mathrm{Tr}_A[\rho^{AR}]$

τ^E: arbitrary state

If $\exists$ such a $\mathcal{U}^A$, ρ^A can be sent reliably via $\mathcal{N}^{A\to B}$ within error ϵ.

associated with $\mathcal{T}^{A\to E}$ (complementary channel of $\mathcal{T}$)

In short, decoupling $\Rightarrow$ sending a state.

↳ The Haar measure does the job!!

$\boxed{\begin{array}{l}\textbf{Thm} \text{ One-shot decoupling theorem [Dupuis et al. '10]} \\[6pt] \mathbb{E}_{U^A \sim \mathrm{Haar}}\left[\| \mathcal{T}^{A\to E}(U^A \rho^{AR} U^{A\dagger}) - \rho^R \otimes \tau^E \|_1 \right] \leq 2^{-\frac{1}{2}(H_{min}(A|E)_\tau + H_{min}(A|R)_\rho)} \\[6pt] \text{where } \begin{cases} \tau^{AE} := (\mathrm{id}^A \otimes \mathcal{T}^{A'\to E})(\Phi^{AA'}) \\ H_{min}(A|C)_\sigma := -\log_2 \min\{ \mathrm{Tr}[\omega^C] : \omega^C \geq 0,\ \sigma^{AC} \leq I^A \otimes \omega^C \} \end{cases} \\[6pt] \qquad\qquad \text{"conditional min-entropy" of } \sigma^{AC}, \in [-d_A, d_A] \end{array}}$

$\Rightarrow$ If $H_{min}(A|E)_\tau + H_{min}(A|R)_\rho \gg 1$, then decoupled by Haar.

↳ In the asymptotic limit, necessary & sufficient for sending states !!

$\Rightarrow$ Nearly optimal !!

The Haar measure (on $\mathcal{U}(d)$) is very important in Q.I.T.

↳ Even by Q. Computer, sampling takes $\Theta(2^d)$ time

too long.....

3. Decoupling with less random unitary

$\Rightarrow$ unitary design.

For a prob. measure ν on $\mathcal{U}(d)$ & $t \in \mathbb{N}$,

$$\forall X \in \mathcal{L}(\mathcal{H}^{\otimes t}), \quad \mathcal{G}_\nu^{(t)}(X) := \mathbb{E}_{U\sim\nu}[U^{\otimes t} X U^{\dagger\otimes t}].$$

↳ contains the t-th order moments of U & $U^\dagger$.

Def.)

For $\varepsilon > 0$, an ε-approximate unitary t-design is a prob. measure $\nu^{(t)}$ on $\mathcal{U}(d)$ s.t.

$$\| \mathcal{G}_{\nu}^{(t)} - \mathcal{G}_{Haar}^{(t)} \|_{\diamond} \leq \varepsilon .$$

↑ completely bounded norm.

Remark). ε-app. unitary t-designs can be efficiently generated by Q. computers.

[Cleve et al '15, Nakata et al '17].

↳ Decoupling.

Thm One-shot decoupling with designs [Szehr et al '13]

$$\mathbb{E}_{\underset{\sim}{\mathcal{U}^A \sim \nu_{des.}}} \left[\| \mathcal{T}^{A \to E} (\mathcal{U}^A \rho^{AR} \mathcal{U}^{A\dagger}) - \rho^R \otimes \tau^E \|_1 \right]$$

↑ ε-app. 2-design.

$$\leq \sqrt{1 + 4 \varepsilon d_A^4} \; 2^{-\frac{1}{2}(H_{min}(A|E)_{\tau} + H_{min}(A|R)_{\rho})}$$

$\Rightarrow$ $O(1/d_A^4)$-app 2-designs achieve decoupling at the same rate as Haar!!

Is $\varepsilon = O(1/d_A^4)$ necessary for decoupling?

↳ We construct a random unitary, which

1. is an $\Theta(d_A^{-2})$-approximate 2-design.
2. achieves decoupling at the same rate as Haar.

3. Decoupling with worse-approx. unitary 2-design.

Main idea: to use "random diagonal-unitaries" in the "complementary" real bases.

Def

Random diagonal unitary (RDU) in the basis E is

$$D^E := \mathrm{diag}_E(e^{i\theta_1}, e^{i\theta_2}, \cdots\cdots, e^{i\theta_d})$$

where each $\theta_j \in [0, 2\pi)$ (random).

Def.

A pair of two bases ($E = \{|e_j\rangle\}$, $F = \{|f_j\rangle\}$ is "complementary" & "real" if

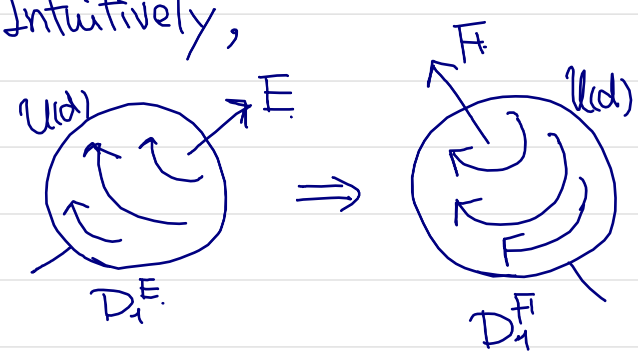
$$\forall i, j \in [1, d], \quad \langle e_j | f_i \rangle = \pm \frac{1}{\sqrt{d}}.$$

Note: "Real" assumption may not be important.

For $l \in \mathbb{N}$, define $D[l] := D^E_{l+1} D^F_l D^E_l \cdots\cdots D^F_1 D^E_1$

all are independent

↳ Intuitively,



$\Rightarrow$ repeat $\approx l$ times.

Thm 1. [Nakata et al '17]

$D[\ell]$ is an ε-approximate unitary 2-design where

$$\frac{2}{d^\ell}\left(1-\frac{1}{d-1}\right) \le \varepsilon \le \frac{2}{d^\ell}\left(1+\frac{2}{d-1}\right).$$

Thm 2. [Nakata et al '17]

$$\mathbb{E}_{D[\ell]} \left\| \mathcal{N}^{A\to E}\left(D^A_{[\ell]}\, \rho^{AR}\, D^{A\dagger}_{[\ell]}\right) - \tau^E \otimes \rho^R \right\|_1$$
$$\le \sqrt{1+8\, d_A^{2-\ell}}\ 2^{-\frac{1}{2}\left(H_{min}(A|E)_\tau + H_{min}(A|R)_\rho\right)}$$

As a consequence, we obtain that

$$\begin{cases} ① \ D[2] \text{ is a } \Theta(d^{-2})\text{-approx. unitary 2-design.} \\ ② \ D[2] \text{ achieves decoupling at the same rate as Haar.} \end{cases}$$

$\Rightarrow$ $O(d^{-4})$-app. design is in general not necessary for decoupling.

4. Proof ideas.

Need to consider $\mathcal{G}^{(2)}_{D[\ell]}(\xi) = \mathbb{E}\left[D_{[\ell]}^{\otimes 2}\ \xi\ D_{[\ell]}^{\dagger\otimes 2} \right]$

$$D_{[\ell]} = D^E_{\ell+1} \prod_{i=1}^{\ell} D^F_i D^E_i = \prod_{i=1}^{\ell} \left(D^E_i D^F_i D^E_i\right) \leftarrow \text{all independent.}$$

$$\mathcal{G}^{(2)}_{D[\ell]} = \Big(\underbrace{\mathcal{G}^{(2)}_{D^E} \circ \mathcal{G}^{(2)}_{D^F} \circ \mathcal{G}^{(2)}_{D^E}}_{=:\ \mathcal{R}} \Big)^\ell \quad \text{where } \mathcal{G}^{(2)}_{D^W}(\xi) = \mathbb{E}\left[D^{W\otimes 2}\ \xi\ D^{W\dagger\otimes 2}\right]$$

$=: \mathcal{R}. \leftarrow$ main target.

Lemma.

The l repetitions of $\mathcal{R}^l$ is given by

$$\mathcal{R}^l = (1-p_l)\,\mathcal{G}^{(2)}_{\mathrm{Haar}} + p_l\,\mathcal{C}_l$$

where $p_l = \Theta(d^{-l})$ & $\mathcal{C}_l$ is a unital CPTP map.

$\mathcal{C}_l(I) = I$.

↑ $\mathcal{R}^l$ is a prob. mixture of $\mathcal{G}^{(2)}_{\mathrm{Haar}}$ & $\mathcal{C}_l$!!

Proof of Thm 1.

- $\| \mathcal{R}^l - \mathcal{G}^{(2)}_{\mathrm{Haar}} \|_\diamond \le p_l \| \mathcal{C}_l - \mathcal{G}^{(2)}_{\mathrm{Haar}} \|_\diamond \le 2 p_l$.
- $\| \quad " \quad - \quad " \quad \|_\diamond \ge \| \mathcal{R}^l(\rho) - \mathcal{G}^{(2)}_{\mathrm{Haar}} \|_1$ for $\forall \rho \in \mathcal{S}(\mathcal{H}^{\otimes 2})$

Proof of Thm 2.

Using some trick, $\exists\, \mathcal{T}, \tilde{\rho}, \tilde{\tau}$ st.

$$\left(\mathbb{E}_D \| \mathcal{N}^{A\to E}(D^A \rho^{AR} D^{A\dagger}) - \tau^E \otimes \rho^R \|_1 \right)^2$$

$$\le \mathbb{E}_D \| \mathcal{T}^{A\to E}(D^A \tilde{\rho}^{AR} D^{A\dagger}) - \tilde{\tau}^E \otimes \tilde{\rho}^R \|_2^2$$

$\|X\|_2^2 = \mathrm{Tr}[X^\dagger X]$

$$= \mathbb{E}_D\left[\mathrm{Tr}[(\mathcal{T}^{A\to E}(\quad))^2] \right] - \mathrm{Tr}[(\tilde{\tau}^E)^2]\,\mathrm{Tr}[(\tilde{\rho}^R)^2].$$

$$= \mathrm{Tr}\left[(\mathcal{T}^{A\to E}(D^A \tilde{\rho}^{AR} D^{A\dagger}))^{\otimes 2} (\mathbb{F}^{EE'} \otimes \mathbb{F}^{RR'}) \right]$$

$= \sum_{i,j} |e_i\rangle\langle e_j|^E \otimes |e_j\rangle\langle e_i|^{E'}$

(SWAP operator).

$(\mathbb{F} \otimes \mathbb{F})$

$$= \mathrm{Tr}\left[\mathcal{T}^{A\to E \otimes 2}\left(\underbrace{\mathbb{E}_D[(D^A \tilde{\rho}^{AR} D^{A\dagger})^{\otimes 2}]}_{= \mathcal{R}^l(\tilde{\rho}^{AR\otimes 2})} \right) \right] - \bigcirc\bigcirc.$$

Proof of Lemma.

$\mathcal{R} := \mathcal{G}^{(2)}_{DE} \circ \mathcal{G}^{(2)}_{DF} \circ \mathcal{G}^{(2)}_{DE}$: map from $\mathcal{L}(\mathcal{H}^{\otimes 2}) \to \mathcal{L}(\mathcal{H}^{\otimes 2})$.

↳ We expect $\mathcal{R} \approx \mathcal{G}^{(2)}_{Haar}$.

$\forall \xi \in \mathcal{L}(\mathcal{H}^{\otimes 2})$, $\mathcal{G}^{(2)}_{Haar}(\xi) := \mathbb{E}_{\mathcal{U} \sim Haar}[\mathcal{U}^{\otimes 2} \xi \, \mathcal{U}^{\dagger \otimes 2}]$.

Due to the left- & right invariance of Haar,

$\forall V \in \mathcal{U}(d)$, $V^{\otimes 2} \mathcal{G}^{(2)}_{Haar}(\xi) V^{\dagger \otimes 2} = \mathcal{G}^{(2)}_{Haar}(\xi)$.

Shur-Weyl duality ↳ $\mathcal{G}^{(2)}_{Haar}(\xi) = \alpha \underbrace{\Pi_{sym}}_{\text{proj. onto the symmetric subspc.}} + \beta \underbrace{\Pi_{anti}}_{\text{proj. onto anti-sym.}}$

⇒ Consider how $\mathcal{R}$ acts on

- the sym. subspc. ← $\{|e_i\rangle^{\otimes 2}\}$, $\left\{\frac{|e_i\rangle|e_j\rangle + |e_j\rangle|e_i\rangle}{\sqrt{2}}\right\}$ $= |\phi_{ij}\rangle$
- " anti- subspc ← $\{|e_i\rangle|e_j\rangle - |e_j\rangle|e_i\rangle\}$ $= |\psi_{ij}\rangle$.
- off-diagonal parts.

$$\begin{cases} \mathcal{R}(|e_i\rangle\langle e_i|^{\otimes 2}) \approx \left(1 - \frac{1}{d^2}\right)\Pi_{sym} + \Delta. \\ \mathcal{R}(|\phi_{ij}\rangle\langle\phi_{ij}|) \approx \left(1 - \frac{1}{d}\right)\Pi_{sym} + \Delta' \\ \mathcal{R}(|\psi_{ij}\rangle\langle\psi_{ij}|) \approx \left(1 - \frac{1}{d}\right)\Pi_{anti} + \Delta''. \\ \mathcal{R}(\text{off-diagonal}) = 0. \end{cases}$$

⇒ The map $\mathcal{R}^{\ell}$ can be evaluated.

5. Conclusion & open problems.

Decoupling : one of the most important protocols in Q.I.T.

$\leftarrow$ known to be achievable by $\Theta(d^{-4})$-app. uni. 2-des.

not tight!!

$\exists\, \Theta(d^{-2})$-app 2-design that achieves decoupling!!

Open problems.

- Does $\left\{ \begin{array}{l} \Theta(d^{-1})\text{-app } \underbrace{\text{2-design}} \text{ achieve decoupling?} \\ \Theta(1/\log d) \end{array} \right.$

How worse can ε be?

really need 2-design?

Known : 1-design is useless.

$\Longrightarrow$ Can we define t-designs for $t \in \mathbb{R}^+$?

e.g.) Decoupling with 3/2-design etc.

Interesting, but nobody knows how to define 3/2-design ....