When quantum memory is useful for dense coding

Ryuji Takagi

University of Tokyo

Joint work with **Masahito Hayashi**

[Letters in Mathematical Physics 114, 88 (2024)]

Why am I talking about this at resource workshop?

Question: In dense coding, when does receiver want to possess quantum memory?

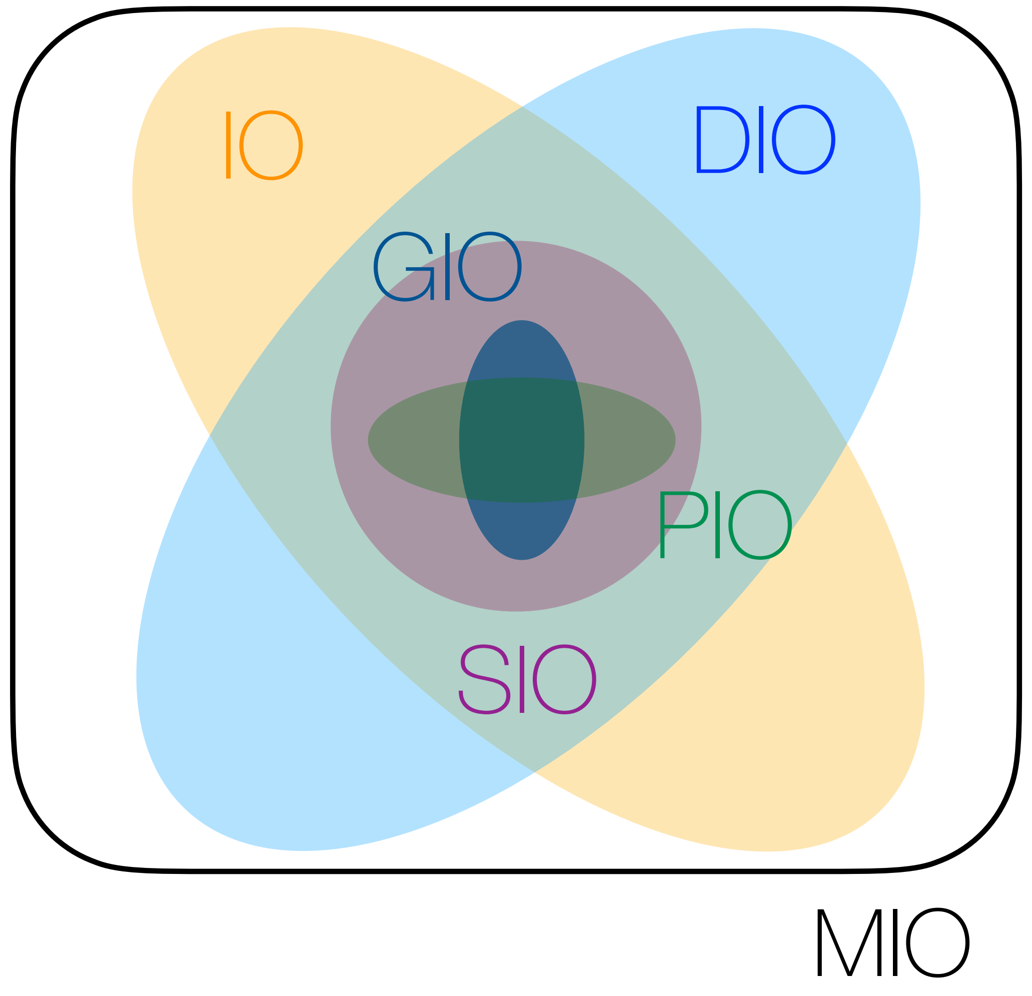
- Operational significance of entanglement from the perspective of quantum memory

- Application of resource theory of (speakable) coherence

  Started by a fundamental motivation: how to quantify superposition?

  Operational significance unclear: zoo of free operations

  Physical significance unclear: artificial preferred basis (c.f. asymmetry)

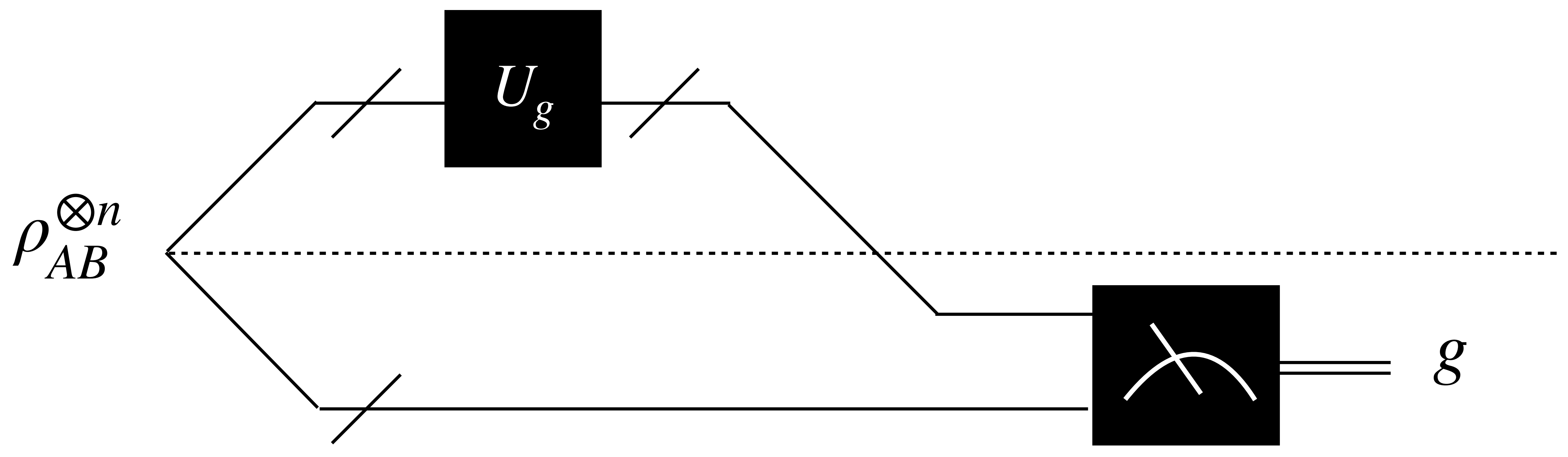


We find that the analysis of free operations (GIO!) is closely related to dense coding

Standard setting of dense coding

Classical message $k \in \mathscr{K}_n$ encoded in an group element $g \in G \times \cdots \times G = G^n$

Encode $g \in G^n$ onto a state $\rho_{AB}^{\otimes n}$ by applying a group representation $\{U_g\}_{g \in G^n}$



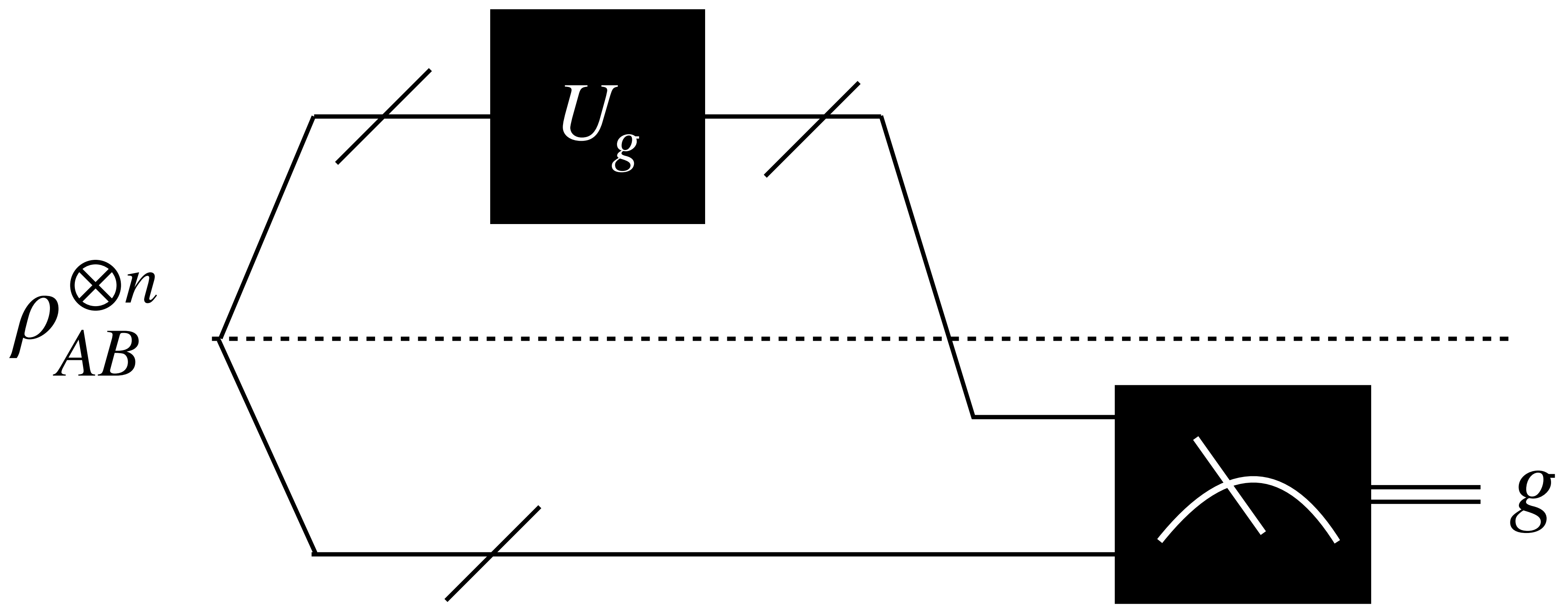
Capacity: rate of classical bits that can be reliably sent

$$\boxed{C_c(\rho_{AB}) = \sup_p S\left(\sum_{g \in G} p_g U_g \rho_{AB} U_g^\dagger\right) - \sum_{g \in G} p_g S(U_g \rho_{AB} U_g^\dagger) = D(\rho_{AB} \| \mathscr{G}_A(\rho_{AB}))}$$

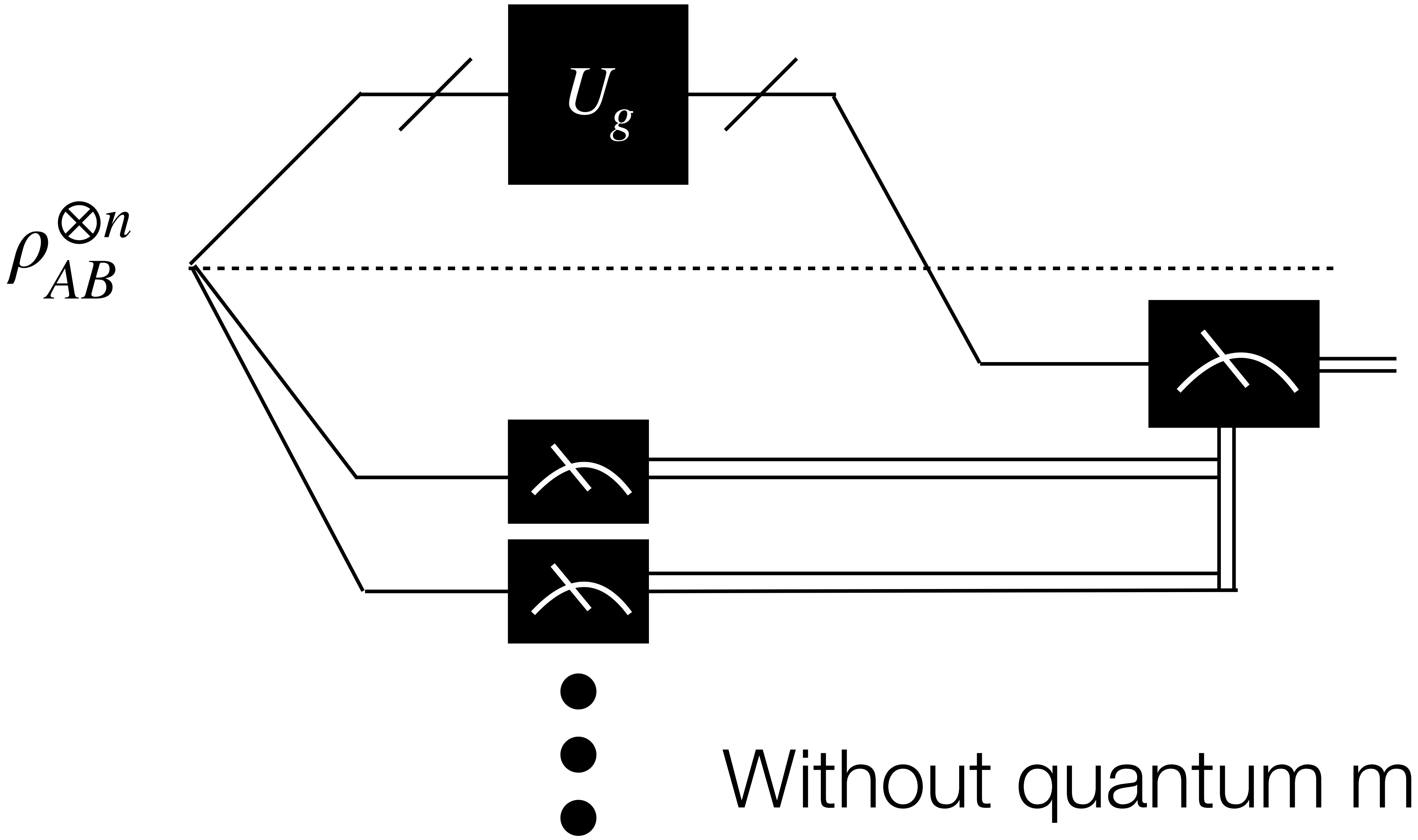
$$\mathscr{G}(\,\cdot\,) = \frac{1}{|G|} \sum_{g \in G} U_g \cdot U_g^\dagger$$

"Group twirling"

Dense coding without quantum memory



With full quantum memory



Without quantum memory

Bob measures his side immediately after ρ_{AB} is distributed.

c.f. [Hayashi, Wang, PRX Quantum '22] for the case of LOCC decoder

If Bob measures with basis $\mathscr{B} = \{|k\rangle\}_k$, they share

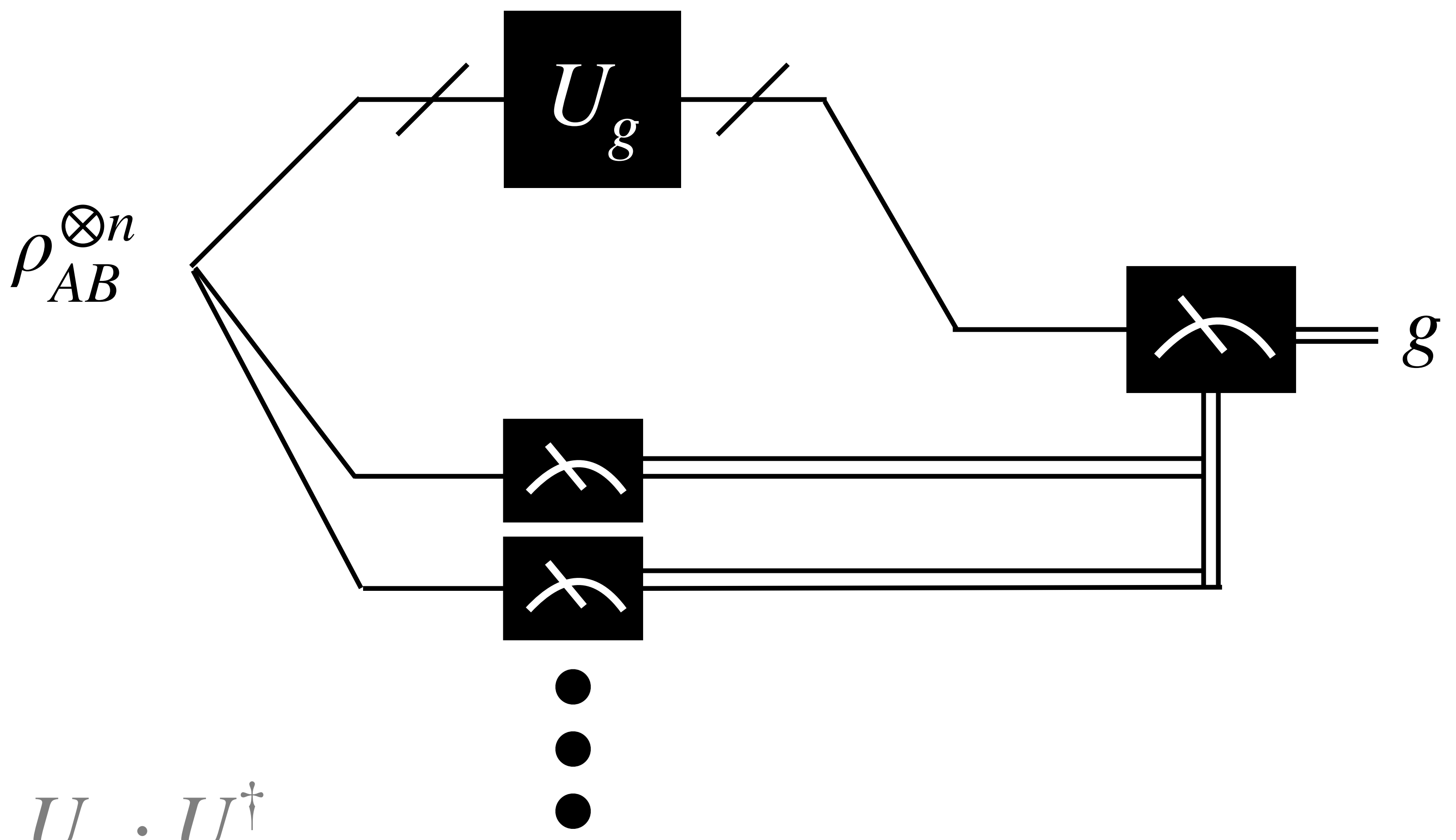
$$\mathscr{B}_B(\rho_{AB}) = \sum_k \langle k|\rho_{AB}|k\rangle \otimes |k\rangle\langle k| = \sum_k p_k\, \rho_{AB|k}$$

$$p_k = \mathrm{Tr}_A \langle k|\rho_{AB}|k\rangle$$

$$\rho_{AB|k} = \frac{1}{p_k}\langle k|\rho_{AB}|k\rangle \otimes |k\rangle\langle k|$$

Capacity with and without quantum memory

$$\mathscr{B}_B(\rho_{AB}) = \sum_k \langle k|\rho_{AB}|k\rangle \otimes |k\rangle\langle k| = \sum_k p_k\, \rho_{AB|k}$$



Capacity with this shared state

$$C_c(\mathscr{B}_B(\rho_{AB})) = D(\mathscr{B}_B(\rho_{AB})\|\mathscr{G}_A \circ \mathscr{B}_B(\rho_{AB}))$$
$$= D(\mathscr{B}_B(\rho_{AB})\|\mathscr{B}_B \circ \mathscr{G}_A(\rho_{AB}))$$

$$\mathscr{G}(\,\cdot\,) = \frac{1}{|G|}\sum_{g\in G} U_g \cdot U_g^\dagger$$

$$\boxed{C_c(\rho_{AB}) = D(\rho_{AB}\|\mathscr{G}_A(\rho_{AB})) \geq D(\mathscr{B}_B(\rho_{AB})\|\mathscr{B}_B \circ \mathscr{G}_A(\rho_{AB})) = C_c(\mathscr{B}_B(\rho_{AB}))}$$

with memory

without memory

data processing

When the equality holds, Bob does not need to hold a quantum memory.

Q-memory-uselessness

Example: $G = \mathbb{Z}_l$, $U_g = \sum_i |g+i\rangle\langle i|$, $\rho_{AB} = |\Phi_{AB}\rangle\langle\Phi_{AB}|$, $|\Phi_{AB}\rangle = \frac{1}{\sqrt{l}}\sum_{i=1}^{l}|ii\rangle$

Capacity with memory $\quad C_c(\rho_{AB}) = S(\mathcal{G}_A(\Phi_{AB})) = \log l$

This capacity can be achieved without quantum memory

$$U_g \otimes \mathbb{I}|\Phi_{AB}\rangle = \frac{1}{\sqrt{l}}\sum_i |i+g\rangle|i\rangle$$

- Bob measures with computational basis and get i
- Bob measures the received qubit with computational basis and get $i+g$

$\longrightarrow$ Bob can reconstruct g

If $C_c(\rho_{AB}) = C_c(\mathscr{B}_B(\rho_{AB}))$, we say that ρ_{AB} is $\mathscr{B}$**-q-memory useless.**

If ρ_{AB} is $\mathscr{B}$-q-memory useless for some basis $\mathscr{B}$, ρ_{AB} is **q-memory useless.**

Can we characterize q-memory uselessness?

Group representation

Consider the group G and projective unitary representation $\{U_g\}_{g\in G}$ acting on $\mathscr{H}_A$.

$$\mathscr{H}_A = \bigoplus_{\lambda\in\hat{G}} \mathscr{H}_\lambda \otimes \mathscr{M}_\lambda$$

$\hat{G}$: subset of irreducible representations

$\mathscr{H}_\lambda$: representation space $\mathscr{M}_\lambda$: multiplicity space

Let Π_λ be a projection onto $\mathscr{H}_\lambda \otimes \mathscr{M}_\lambda$, and

$$q_\lambda := \mathrm{Tr}\left[(\Pi_\lambda \otimes \mathbb{I}_B)\,\rho_{AB}\right]$$

$$\rho_\lambda := \frac{1}{q_\lambda}(\Pi_\lambda \otimes \mathbb{I}_B)\rho_{AB}(\Pi_\lambda \otimes \mathbb{I}_B)$$

Then, we get $\mathscr{G}_A(\rho_{AB}) = \bigoplus_{\lambda\in\hat{G}} q_\lambda \frac{\mathbb{I}_\lambda}{d_\lambda} \otimes \mathrm{Tr}_{\mathscr{H}_\lambda}(\rho_\lambda)$

$$\boxed{C_c(\rho_{AB}) = H(q) + \sum_{\lambda\in\hat{G}} q_\lambda \left(\log d_\lambda + S(\mathrm{Tr}_{\mathscr{H}_\lambda}\rho_\lambda)\right) - S(\rho_{AB})}$$

$$C_c(\rho_{AB}) = D(\rho_{AB}\|\mathscr{G}_A(\rho_{AB}))$$

Characterization of q-memory-uselessness

We here focus on pure resource state $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$

Suppose that unitary representation is multiplicity-free, i.e., $\mathscr{H}_A = \bigoplus_{\lambda\in\hat{G}} \mathscr{H}_\lambda$

e.g., cyclic group $G = \mathbb{Z}_l \quad U_g = \sum_{j=0}^{l-1} |j+g\rangle\langle j|$

Each irrep is one-dimensional and gains different phase under group action.

$|\psi_{AB}\rangle$ is q-memory-useless if and only if $|\psi_{AB}\rangle$ has the form

$$|\psi_{AB}\rangle = \sum_{\lambda\in\hat{G}} \sqrt{q_\lambda}\,|\psi_\lambda\rangle \otimes \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}} |k\rangle \qquad |\psi_\lambda\rangle \in \mathscr{H}_\lambda$$

for some probability distributions $\{q_\lambda\}_\lambda$ and $\{p_k\}_k$.

Characterization of q-memory-uselessness

Equivalently, let us write the resource state as

$$|\psi_{AB}\rangle = \sum_{\lambda\in\hat{G}} \sqrt{q_\lambda}\,|\psi_\lambda\rangle\,|v_\lambda\rangle$$

$$|\psi_{AB}\rangle = \sum_{\lambda\in\hat{G}} \sqrt{q_\lambda}\,|\psi_\lambda\rangle \otimes \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}}|k\rangle$$

Then, we have the following characterization.

$|\psi_{AB}\rangle$ is q-memory-useless if and only if $|v_\lambda\rangle$ can be written in the form

$$|v_\lambda\rangle = \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}}|k\rangle \quad \lambda \in \hat{G}$$

for some basis $\{|k\rangle\}_k$ and phases $\{e^{i\theta_{\lambda,k}}\}_{\lambda,k}$ for all $\lambda \in \hat{G}$.

The problem is whether $|v_1\rangle, \ldots, |v_l\rangle$ with $l := |\hat{G}|$ admits this form.

Characterization of q-memory-uselessness

$|v_1\rangle, \ldots, |v_l\rangle$ with $l := |\hat{G}|$ admits $|v_\lambda\rangle = \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}} |k\rangle$ • • • ★

When does ★ happen? One case: when $\{|v_\lambda\rangle\}_\lambda$ are orthogonal. Take

$$|k\rangle = \frac{1}{\sqrt{l}} \sum_{s=1}^{l} e^{i\frac{2\pi ks}{l}} |v_s\rangle \quad k = 1,\ldots,l$$

and $|l+1\rangle, \ldots, |d_B\rangle$ to be orthogonal to $|v_1\rangle, \ldots, |v_l\rangle$.

Another case: when $l = 2$. Choose $\{|1\rangle, |2\rangle\}$ satisfying

$$|v_1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \qquad |v_2\rangle = \frac{1}{\sqrt{2}}(e^{i(\theta'+\theta)}|1\rangle + e^{i(\theta'-\theta)}|2\rangle) \qquad e^{i\theta'}\cos\theta = \langle v_1 | v_2\rangle$$

Can we get a general characterization of when ★ happens?

Characterization with Gram matrix

$|v_1\rangle, \ldots, |v_l\rangle$ with $l := |\hat{G}|$ admits $|v_\lambda\rangle = \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}} |k\rangle$ • • • ☆

$V = (|v_1\rangle, \ldots, |v_l\rangle)$ set of vectors $\longrightarrow$ $J(V)_{ij} := \langle v_i | v_j \rangle$ Gram matrix of V

★ holds iff there exists a set $U = (|u_1\rangle, \ldots, |u_l\rangle)$ of vectors such that

$|u_\lambda\rangle = \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}} |\tilde{k}\rangle \quad \lambda = 1, \ldots, l$ for the computational basis $\{|\tilde{k}\rangle\}_k$, and

$J(V) = J(U)$ "Vectors with the same Gram matrix are connected by a unitary."

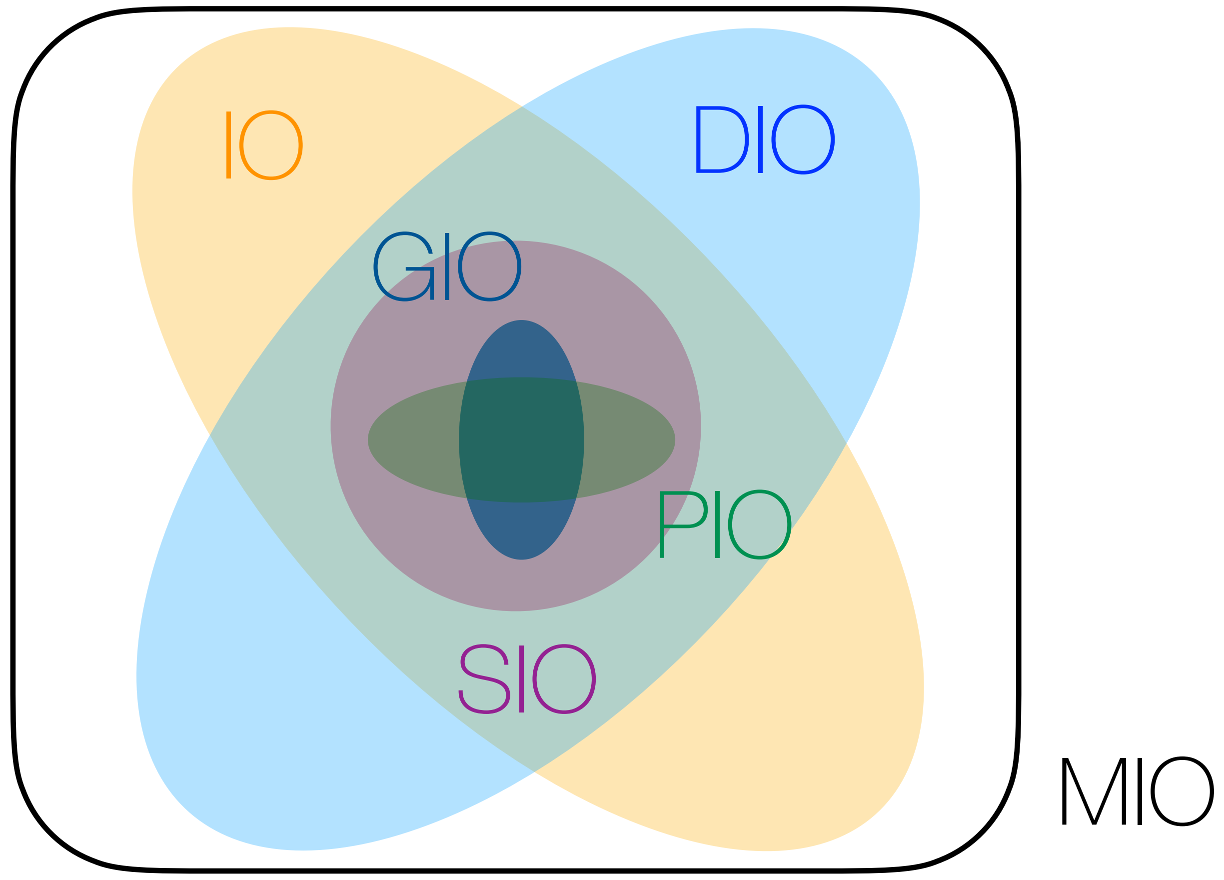
Observation $J(U) = l \sum_{k=1}^{d_B} p_k Z_k |+\rangle\langle+| Z_k^\dagger$ $\quad |+\rangle = \frac{1}{\sqrt{l}} \sum_{\lambda=1}^{l} |\lambda\rangle$ $\quad Z_k = \sum_{\lambda=1}^{l} e^{i\theta_{\lambda,k}} |\lambda\rangle\langle\lambda|$

★ $\Longleftrightarrow$ $|+\rangle$ can be transformed to the state $J(V)/l$ by a probabilistic incoherent unitary!

Genuinely Incoherent Operations (GIO)

$\mathcal{I} = \mathrm{conv}\{\,|i\rangle\langle i|\,\}$: incoherent states

Λ is GIO iff $\Lambda(\sigma) = \sigma, \quad \forall \sigma \in \mathcal{I}$



Characterization of GIO

Λ is GIO iff $\Lambda(\rho) = A \odot \rho$ for some positive semidefinite matrix A with $A_{ii} = 1\ \forall i$

$(X \odot Y)_{ij} = X_{ij}Y_{ij}$: Hadamard product

[de Vicente, Streltsov, J. Phys. A '17]

J is a Gram matrix if and only if $J_{ii} = 1\ \forall i$ and $J \geq 0$

$\longrightarrow$ Every Gram matrix J has one-to-one correspondence with GIO $\Lambda_J(\rho) = J \odot \rho$

Q-memory uselessness with GIO

$|v_1\rangle, \ldots, |v_l\rangle$ with $l := |\hat{G}|$ admits $|v_\lambda\rangle = \sum_{k=1}^{d_B} \sqrt{p_k} e^{i\theta_{\lambda,k}} |k\rangle$ • • • ★

★ $\Longleftrightarrow$ $|+\rangle$ can be transformed to the state $J(V)/l$ by a probabilistic incoherent unitary

Observe that $J(V)/l = J(V) \odot |+\rangle\langle+| = \Lambda_{J(V)}(|+\rangle\langle+|)$ always holds.

i.e., $|+\rangle\langle+|$ can be always transformed to the state $J(V)/l$ by GIO.

★ $\Longleftrightarrow$ GIO $\Lambda_{J(V)}$ can be implemented by a probabilistic incoherent unitary

When does this happen?

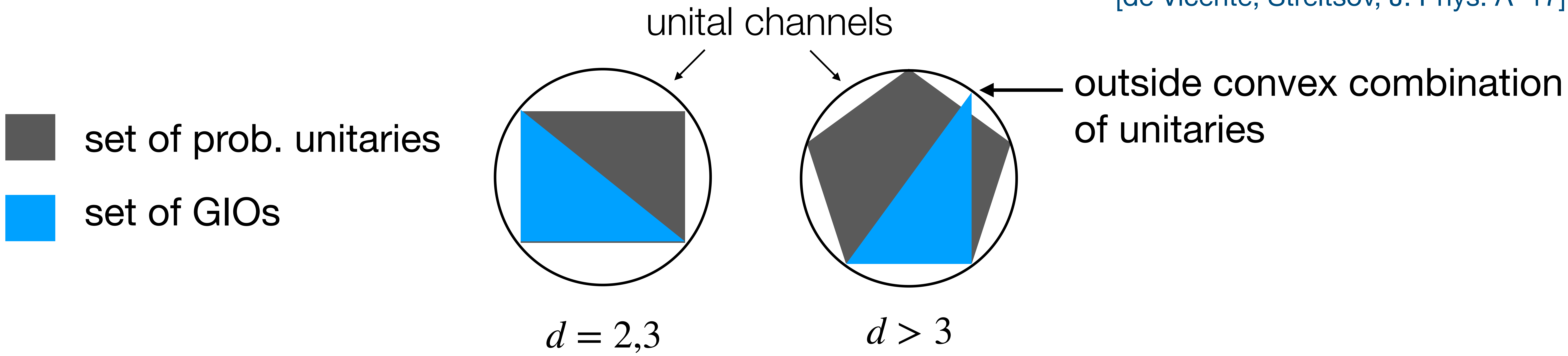
GIO implementable by probabilistic incoherent unitary

Let d be a dimension of the system that GIO operations act on.

When $d = 2{,}3$, every $\Lambda \in \mathcal{O}_{\rm GIO}$ can be implemented by a probabilistic application of incoherent unitaries.

When $d > 3$, there exists $\Lambda \in \mathcal{O}_{\rm GIO}$ that cannot be implemented by a probabilistic applications of incoherent unitaries.

[de Vicente, Streltsov, J. Phys. A ’17]



Application to dense coding

Combining these arguments lead to the following characterization.

If $l = |\hat{G}|$ takes $l = 2,3$, $|\psi_{AB}\rangle$ is always q-memory-useless.

i.e., $C_c(|\psi_{AB}\rangle\langle\psi_{AB}|) = C_c(\mathscr{B}_B(|\psi_{AB}\rangle\langle\psi_{AB}|))$ for every basis $\mathscr{B}_B$ on Bob.

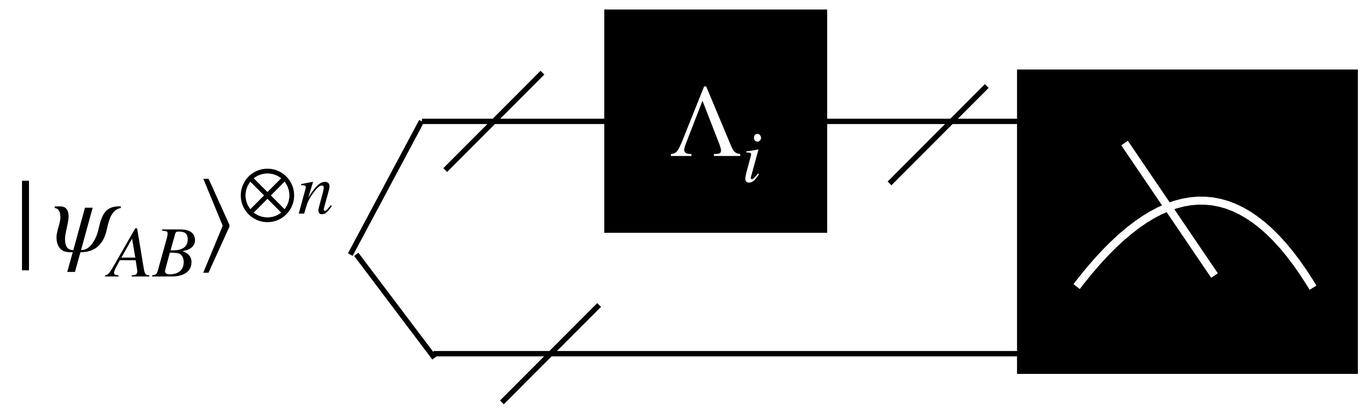
If $l > 3$, there exists a state $|\psi_{AB}\rangle$ such that Bob's quantum memory is useful.

i.e., $C_c(|\psi_{AB}\rangle\langle\psi_{AB}|) > C_c(\mathscr{B}_B(|\psi_{AB}\rangle\langle\psi_{AB}|))$ for some basis $\mathscr{B}_B$ on Bob.

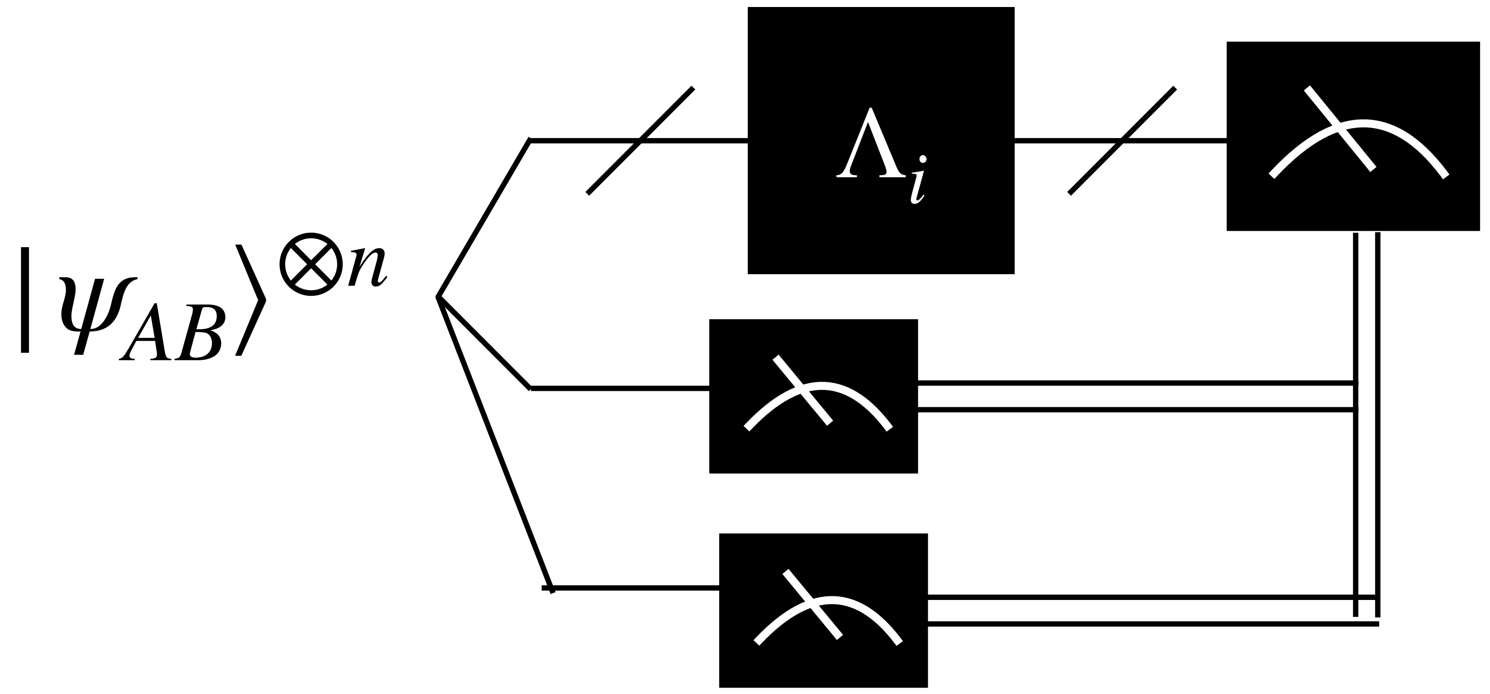
q-memory-uselessness of $|\psi_{AB}\rangle = \sum_{\lambda\in\hat{G}}\sqrt{q_\lambda}\,|\psi_\lambda\rangle|v_\lambda\rangle$ $\iff$ Implementability of $\Lambda_{J(V)} \in \mathscr{O}_{\mathrm{GIO}}$

Implication to channel discrimination

Discriminate whether Λ_1 or Λ_2 applied.



with memory



without memory

e.g., quantum illumination

$\Lambda_1 = (1-p)\,\mathrm{id} + p\mathscr{R}_\tau$ $\quad \Lambda_2 = \mathscr{R}_\tau$ $\quad \mathscr{R}_\tau$: preparation of thermal state τ

Here, we consider a variant of this, where $\Lambda_1 = \mathrm{id} \quad \Lambda_2 = \mathscr{G}$ $\quad \mathscr{G}(\cdot) = \frac{1}{|G|}\sum_{g\in G} U_g \cdot U_g^\dagger$

Error exponent of Type-II error in asymmetric channel discrimination

$$\boxed{D(\psi_{AB}\|\mathscr{G}_A(\psi_{AB})) \geq D(\mathscr{B}_B(\psi_{AB}))\|\mathscr{G}_A \otimes \mathscr{B}_B(\psi_{AB}))}$$

with memory $\qquad$ without memory

Same analysis can carry over!

Summary

- Introduced dense coding where receiver immediately measures out the shared entangled resource, representing the scenario that the receiver does not possess quantum memory.

- Characterized when the receiver's quantum memory becomes useful in terms of the given resource state and group representation.

- It turns out that the problem reduces to the analysis of GIO—whether the given GIO admits the implementation of probabilistic incoherent unitaries.

- Resource theory of coherence could find further applications as an analytical tool?

Thank you!