Bipartite unitary operators inducing special classes of quantum channels

Ion Nechita

CNRS, LPT Toulouse

joint work with Tristan Benoist, Julien Deschamps and Clément Pellegrini

Grenoble, May 9th 2016

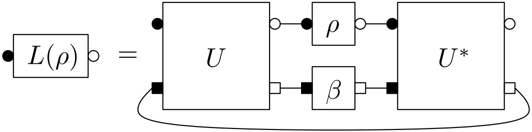
Stinespring dilation for quantum channels

Theorem

Any quantum channel $L : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$ *(i.e. completely positive, trace preserving linear map) can be written as*

$$L(\rho) = [\mathrm{id} \otimes \mathrm{Tr}]\left(U(\rho \otimes \beta)U^*\right)$$

for some environment of size k *(*$k = n^2$ *suffices), a quantum state* $\beta \in \mathcal{M}_n^{1,+}(\mathbb{C})$ *and a global unitary operator* $U \in \mathcal{U}_{nk}$*.*



Stinespring dilation for quantum channels

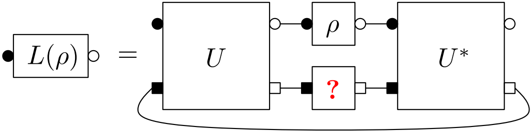
Theorem

Any quantum channel $L : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$ (i.e. completely positive, trace preserving linear map) can be written as

$$L(\rho) = [\mathrm{id} \otimes \mathrm{Tr}]\,(U(\rho \otimes \beta)U^*)$$

for some environment of size k ($k = n^2$ suffices), a quantum state $\beta \in \mathcal{M}_n^{1,+}(\mathbb{C})$ and a global unitary operator $U \in \mathcal{U}_{nk}$.

- What if we do not know / have access to β, the state of the environment ?



The main problem

$$L_{U,\beta}(\rho) := [\mathrm{id} \otimes \mathrm{Tr}]\left(U(\rho \otimes \beta)U^*\right)$$

Our mantra

Given a family $\mathcal{L}$ of quantum channels, characterize the set

$$\mathcal{U}_{\mathcal{L}} := \{U \in \mathcal{U}_{nk} \ : \ \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta} \in \mathcal{L}\}.$$

The main problem

$$L_{U,\beta}(\rho) := [\mathrm{id} \otimes \mathrm{Tr}]\left(U(\rho \otimes \beta)U^*\right)$$

Our mantra

Given a family $\mathcal{L}$ of quantum channels, characterize the set

$$\mathcal{U}_{\mathcal{L}} := \{U \in \mathcal{U}_{nk} \ : \ \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta} \in \mathcal{L}\}.$$

- If the set $\mathcal{L}$ is unitarily invariant, i.e.

  $$L \in \mathcal{L} \iff \forall V_{1,2} \in \mathcal{U}_n,\ V_1 L(V_2 \cdot V_2^*) V_1^* \in \mathcal{L},$$

  then the set $\mathcal{U}_{\mathcal{L}}$ is invariant by local unitary multiplication:

  $$U \in \mathcal{U}_{\mathcal{L}} \iff \forall V_{1,2} \in \mathcal{U}_n, \forall W_{1,2} \in \mathcal{U}_k,\ (V_1 \otimes W_2)U(V_2 \otimes W_2) \in \mathcal{U}_{\mathcal{L}}.$$

The main problem

$$L_{U,\beta}(\rho) := [\mathrm{id} \otimes \mathrm{Tr}]\left(U(\rho \otimes \beta)U^*\right)$$

Our mantra

Given a family $\mathcal{L}$ of quantum channels, characterize the set

$$\mathcal{U}_{\mathcal{L}} := \{U \in \mathcal{U}_{nk} \ : \ \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta} \in \mathcal{L}\}.$$

- If the set $\mathcal{L}$ is unitarily invariant, i.e.

$$L \in \mathcal{L} \iff \forall V_{1,2} \in \mathcal{U}_n,\ V_1 L(V_2 \cdot V_2^*) V_1^* \in \mathcal{L},$$

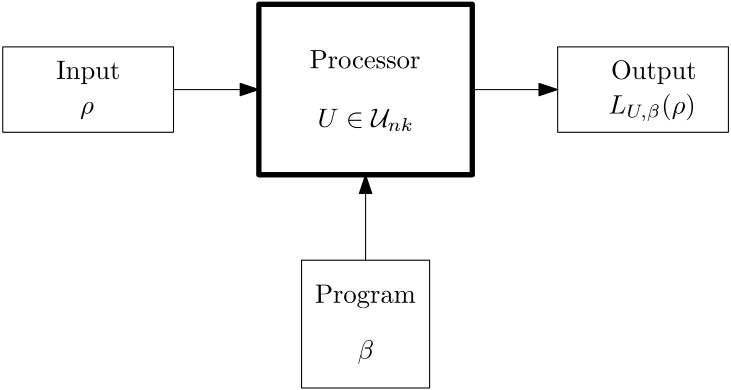
then the set $\mathcal{U}_{\mathcal{L}}$ is invariant by local unitary multiplication:

$$U \in \mathcal{U}_{\mathcal{L}} \iff \forall V_{1,2} \in \mathcal{U}_n, \forall W_{1,2} \in \mathcal{U}_k,\ (V_1 \otimes W_2) U (V_2 \otimes W_2) \in \mathcal{U}_{\mathcal{L}}.$$

1. $\mathcal{L}_{aut} = \{V \cdot V^*\}_{V \in \mathcal{U}_n}$
2. $\mathcal{L}_{const} = \{\text{constant channels}\}$
3. $\mathcal{L}_{unital} = \{L \ : \ L(I) = I\}$
4. $\mathcal{L}_{mixed} = \mathrm{conv}\{V \cdot V^*\}_{V \in \mathcal{U}_n}$
5. $\mathcal{L}_{diag} = \{L \ : \ L(\mathrm{diag}) \subseteq \mathrm{diag}\}$
6. $\mathcal{L}_{tens} = \{L \ : \ L(\mathcal{M}_d(\mathbb{C}) \otimes I_r) \subseteq \mathcal{M}_d(\mathbb{C}) \otimes I_r\}$

Processor / program point of view

- Bužek, Ziman and collaborators study the same problem, under a different name



Lemma (Equivalent processors)

Two processors $U, V \in \mathcal{U}_{nk}$ are equivalent, i.e. for all programs $\beta \in \mathcal{M}_k^{1,+}(\mathbb{C})$, $L_{U,\beta} = L_{V,\beta}$, iff there exists $W \in \mathcal{U}_k$ s.t. $U = (I_n \otimes W)V$.

Unitary conjugations

$$\mathcal{U}_{aut} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta}(\rho) = V_\beta \rho V_\beta^*\}$$

Theorem

We have $\mathcal{U}_{aut} = \{V \otimes W \,:\, V \in \mathcal{U}_n,\, W \in \mathcal{U}_k\}$.
For $U = V \otimes W,\ L_{U,\beta}(\rho) = V\rho V^*$.

Unitary conjugations

$$\mathcal{U}_{aut} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta}(\rho) = V_\beta \rho V_\beta^*\}$$

Theorem

We have $\mathcal{U}_{aut} = \{V \otimes W \;:\; V \in \mathcal{U}_n,\; W \in \mathcal{U}_k\}$.
For $U = V \otimes W$, $L_{U,\beta}(\rho) = V \rho V^*$.

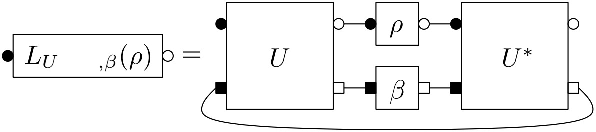
$$\mathcal{U}_{single} := \{U \in \mathcal{U}_{nk} \,|\, \text{the set } \{L_{U,\beta} \;:\; \beta \in \mathcal{M}_k^{1,+}(\mathbb{C})\} \text{ has 1 element}\}.$$

In other words, $U \in \mathcal{U}_{single}$ iff the channel $L_{U,\beta}$ does not depend on β, the state of the environment.

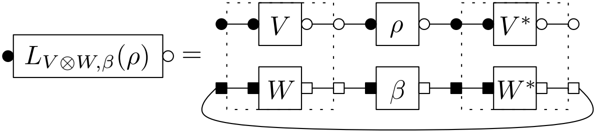
Proposition

We have $\mathcal{U}_{single} = \mathcal{U}_{aut} = \{V \otimes W\}$.

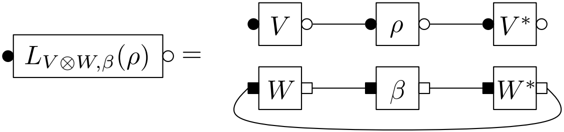
Unitary conjugations



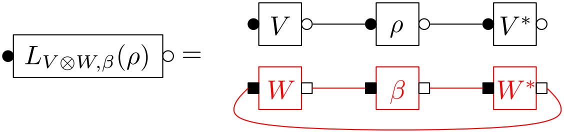
Unitary conjugations



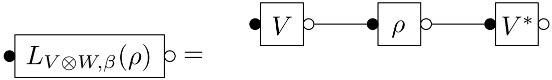
Unitary conjugations



Unitary conjugations



Unitary conjugations



Constant channels

$$\mathcal{U}_{const} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta} \text{ is a constant channel}\}.$$

Theorem

If $k \neq rn$ for $r = 1, 2, \ldots$, then $\mathcal{U}_{const}$ is empty. If $k = r \cdot n$ for some positive r, then

$$\mathcal{U}_{const} = \{(I_n \otimes V)(F_n \otimes I_r)(I_n \otimes W) \,:\, V, W \in \mathcal{U}_k\},$$

where $F_n \in \mathcal{U}_{n^2}$ denotes the flip operator.
For $U \in \mathcal{U}_{const}$ as above, $L_{U,\beta}(\rho) = [\mathrm{id}_n \otimes \mathrm{Tr}_r](W \beta W^*)$.

Constant channels

$$\mathcal{U}_{const} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta} \text{ is a constant channel}\}.$$

Theorem

If $k \neq rn$ for $r = 1, 2, \ldots$, then $\mathcal{U}_{const}$ is empty. If $k = r \cdot n$ for some positive r, then

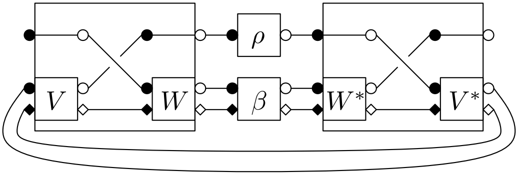
$$\mathcal{U}_{const} = \{(I_n \otimes V)(F_n \otimes I_r)(I_n \otimes W) \,:\, V, W \in \mathcal{U}_k\},$$

where $F_n \in \mathcal{U}_{n^2}$ denotes the flip operator.
For $U \in \mathcal{U}_{const}$ as above, $L_{U,\beta}(\rho) = [\mathrm{id}_n \otimes \mathrm{Tr}_r](W \beta W^*)$.

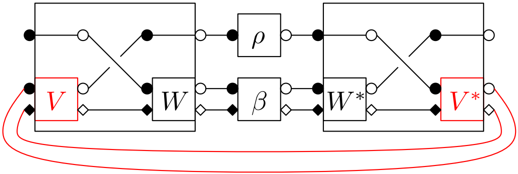
Corollary

If $n = k$, then $\mathcal{U}_{const} = F_n \cdot \mathcal{U}_{aut} = F_n \cdot \{V \otimes W \,:\, V, W \in \mathcal{U}_n\}$.

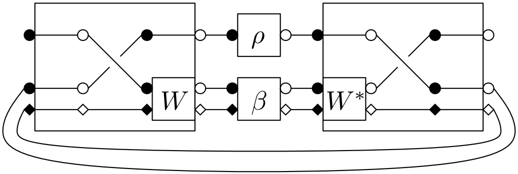
Constant channels



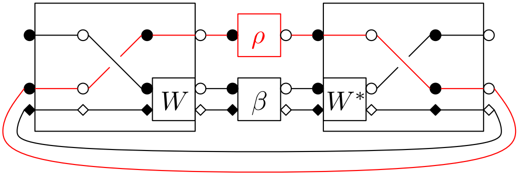
Constant channels



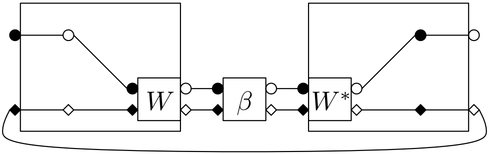
Constant channels



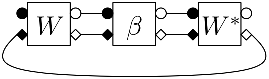
Constant channels



Constant channels



Constant channels



Unital channels

$$\mathcal{U}_{unital} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta}(I) = I\}$$

Theorem

One has

$$\mathcal{U}_{unital} = \mathcal{U}_{nk} \cap \mathcal{U}_{nk}^{\Gamma}$$

where $A^{\Gamma} = [\mathrm{id} \otimes \mathrm{transp}](A)$ denotes the partial transposition of A. In other words, $U \in \mathcal{U}_{unital}$ iff both U and U^{Γ} are unitary operators.

Unital channels

$$\mathcal{U}_{unital} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}), L_{U,\beta}(I) = I\}$$

Theorem

One has

$$\mathcal{U}_{unital} = \mathcal{U}_{nk} \cap \mathcal{U}_{nk}^{\Gamma}$$

where $A^{\Gamma} = [\mathrm{id} \otimes \mathrm{transp}](A)$ *denotes the partial transposition of A. In other words,* $U \in \mathcal{U}_{unital}$ *iff both U and* U^{Γ} *are unitary operators.*

- $\mathcal{U}_{aut} = \{V \otimes W \,:\, V, W \in \mathcal{U}_n\} \subseteq \mathcal{U}_{unital}$.
- If $n > 1$, then $\mathcal{U}_{const} \cap \mathcal{U}_{unital} = \emptyset$.
- $\mathcal{U}_{unital}$ is a non-smooth algebraic variety. The dimension of the enveloping tangent space of $\mathcal{U}_{unital}$ is generically $nk(n + k - 1)$.

- Although it is easy to check whether a given U is an element of $\mathcal{U}_{unital}$, we do not know how to parametrize or to sample from $\mathcal{U}_{unital}$.
- We conjecture that the following algorithm produces (random) elements from $\mathcal{U}_{unital}$

Sampling from $\mathcal{U}_{unital}$

1. **Input:** Integers n, k and an error parameter $\varepsilon > 0$.
2. Start with a Haar distributed unitary random unitary operator $U \in \mathcal{U}_{nk}$.
3. While $\|U^\Gamma (U^\Gamma)^* - I_{nk}\|_2 > \varepsilon$, repeat the next step:
4. $U \leftarrow \mathrm{Pol}(U^\Gamma)$, where $\mathrm{Pol}(X)$ is the unitary operator V appearing in the polar decomposition of X: $X = VP$ with $P \geq 0$.
5. **Output:** U, an operator at distance at most ε from $\mathcal{U}_{unital}$.

Block diagonal unitary matrices

Block-diagonal (or control) unitary operators wrt the system A (resp. B)

$$\mathcal{U}^{A}_{block-diag} = \{U \in \mathcal{U}_{nk} \mid U = \sum_{i=1}^{k} U_i \otimes e_i f_i^*,$$

$$\text{with } U_i \in \mathcal{U}_n \text{ and } \{e_i\}, \{f_i\} \text{ orthonormal bases in } \mathbb{C}^k\}$$

Block diagonal unitary matrices

Block-diagonal (or control) unitary operators wrt the system A (resp. B)

$$\mathcal{U}^{A}_{block-diag} = \{U \in \mathcal{U}_{nk} \mid U = \sum_{i=1}^{k} U_i \otimes e_i f_i^*,$$

with $U_i \in \mathcal{U}_n$ and $\{e_i\}, \{f_i\}$ orthonormal bases in $\mathbb{C}^k\}$

$$\mathcal{U}^{B}_{block-diag} = \{U \in \mathcal{U}_{nk} \mid U = \sum_{i=1}^{n} e_i f_i^* \otimes U_i,$$

with $U_i \in \mathcal{U}_k$ and $\{e_i\}, \{f_i\}$ orthonormal bases in $\mathbb{C}^n\}$

Block diagonal unitary matrices

Block-diagonal (or control) unitary operators wrt the system A (resp. B)

$$\mathcal{U}^{A}_{block-diag} = \{U \in \mathcal{U}_{nk} \mid U = \sum_{i=1}^{k} U_i \otimes e_i f_i^*,$$

with $U_i \in \mathcal{U}_n$ and $\{e_i\}, \{f_i\}$ orthonormal bases in $\mathbb{C}^k\}$

$$\mathcal{U}^{B}_{block-diag} = \{U \in \mathcal{U}_{nk} \mid U = \sum_{i=1}^{n} e_i f_i^* \otimes U_i,$$

with $U_i \in \mathcal{U}_k$ and $\{e_i\}, \{f_i\}$ orthonormal bases in $\mathbb{C}^n\}$

More generally, $U \in \mathcal{U}^{A}_{block-diag}$ iff

$$U = \sum_{i=1}^{r} U_i \otimes R_i,$$

where U_i are unitary operators acting on $\mathbb{C}^n$ and R_i are partial isometries $R_i : \mathbb{C}^k \to \mathbb{C}^k$ such that $\sum_{i=1}^{r} R_i R_i^* = \sum_{i=1}^{r} R_i^* R_i = I_k$. Moreover, the decomposition is unique, up to the permutation of the terms in the sum and $\mathbb{C}U_i \neq \mathbb{C}U_j$ for $i \neq j$.

Block diagonal unitary matrices

Proposition

If $n = 2$, then

$$\mathcal{U}^{B}_{block-diag} \subseteq \mathcal{U}^{A}_{block-diag}.$$

In particular, when $n = k = 2$, we have

$$\mathcal{U}^{A}_{block-diag} = \mathcal{U}^{B}_{block-diag}.$$

Block diagonal unitary matrices

Proposition

If $n = 2$, then

$$\mathcal{U}^B_{block-diag} \subseteq \mathcal{U}^A_{block-diag}.$$

In particular, when $n = k = 2$, we have

$$\mathcal{U}^A_{block-diag} = \mathcal{U}^B_{block-diag}.$$

$$\begin{aligned}
\mathcal{U}^B_{block-diag} \ni U &= e_1 f_1^* \otimes U_1 + e_2 f_2^* \otimes U_2 \\
&= (I \otimes U_1)\left[e_1 f_1^* \otimes I + e_2 f_2^* \otimes (U_1^* U_2)\right] \\
&= (I \otimes U_1)\left[e_1 f_1^* \otimes \left(\sum_{i=1}^{k} g_i g_i^*\right) + e_2 f_2^* \otimes \left(\sum_{i=1}^{k} \lambda_i g_i g_i^*\right)\right] \\
&= (I \otimes U_1)\sum_{i=1}^{k}(e_1 f_1^* + \lambda_i e_2 f_2^*) \otimes g_i g_i^* \\
&= (I \otimes U_1)\sum_{i=1}^{k} W_i \otimes g_i g_i^* = \sum_{i=1}^{k} W_i \otimes h_i g_i^* \in \mathcal{U}^A_{block-diag}.
\end{aligned}$$

Mixed quantum channels

$$\mathcal{U}_{mixed} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\; L_{U,\beta} \in \mathrm{conv}\{V \cdot V^*\}_{V \in \mathcal{U}_n}\}$$

$$= \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\; L_{U,\beta}(X) = \sum_{i=1}^{r(\beta)} p_i(\beta) U_i(\beta) X U_i(\beta)^*\}$$

Mixed quantum channels

$$\mathcal{U}_{mixed} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta} \in \mathrm{conv}\{V \cdot V^*\}_{V \in \mathcal{U}_n}\}$$

$$= \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta}(X) = \sum_{i=1}^{r(\beta)} p_i(\beta) U_i(\beta) X U_i(\beta)^*\}$$

$$\mathcal{U}_{prob} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta}(X) = \sum_{i=1}^{r} p_i(\beta) U_i X U_i^*$$

$$\text{with } p_i(\beta) \geq 0 \text{ and } \sum_i p_i(\beta) = 1\}$$

Mixed quantum channels

$$\mathcal{U}_{mixed} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta} \in \mathrm{conv}\{V \cdot V^*\}_{V \in \mathcal{U}_n}\}$$

$$= \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta}(X) = \sum_{i=1}^{r(\beta)} p_i(\beta) U_i(\beta) X U_i(\beta)^*\}$$

$$\mathcal{U}_{prob} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta}(X) = \sum_{i=1}^{r} p_i(\beta) U_i X U_i^*$$

$$\text{with } p_i(\beta) \geq 0 \text{ and } \sum_i p_i(\beta) = 1\}$$

$$\mathcal{U}_{prob-lin} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta}(X) = \sum_{i=1}^{r} p_i(\beta) U_i X U_i^*$$

$$\text{with linear } p_i(\beta) \geq 0 \text{ and } \sum_i p_i(\beta) = 1\}$$

Mixed quantum channels

$$\mathcal{U}_{mixed} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\; L_{U,\beta} \in \mathrm{conv}\{V \cdot V^*\}_{V \in \mathcal{U}_n}\}$$

$$= \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\; L_{U,\beta}(X) = \sum_{i=1}^{r(\beta)} p_i(\beta) U_i(\beta) X U_i(\beta)^*\}$$

$$\mathcal{U}_{prob} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\; L_{U,\beta}(X) = \sum_{i=1}^{r} p_i(\beta) U_i X U_i^*$$

$$\text{with } p_i(\beta) \geq 0 \text{ and } \sum_i p_i(\beta) = 1\}$$

$$\mathcal{U}_{prob-lin} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\; L_{U,\beta}(X) = \sum_{i=1}^{r} p_i(\beta) U_i X U_i^*$$

$$\text{with linear } p_i(\beta) \geq 0 \text{ and } \sum_i p_i(\beta) = 1\}$$

We have the following chain of inclusions

$$\mathcal{U}^A_{block-diag} \subseteq \mathcal{U}_{prob-lin} \subseteq \mathcal{U}_{prob} \subseteq \mathcal{U}_{mixed} \subseteq \mathcal{U}_{unital}.$$

Mixed quantum channels

Theorem

For all n, k*, we have* $\mathcal{U}_{prob-lin} = \mathcal{U}^{A}_{block-diag}$.

Mixed quantum channels

Theorem

For all n, k, we have $\mathcal{U}_{prob-lin} = \mathcal{U}^{A}_{block-diag}$.

- Since $\beta \mapsto p_i(\beta)$ are linear, there exists a POVM (M_i) such that $p_i(\beta) = \mathrm{Tr}(M_i \beta)$.
- Prove the M_i's have orthogonal supports.
- Construct a candidate unitary operator $\tilde{U}$.
- Use the lemma on equivalence of processors.

Mixed quantum channels

Theorem

For all n, k, we have $\mathcal{U}_{prob-lin} = \mathcal{U}^{A}_{block-diag}$.

- Since $\beta \mapsto p_i(\beta)$ are linear, there exists a POVM (M_i) such that $p_i(\beta) = \mathrm{Tr}(M_i \beta)$.
- Prove the M_i's have orthogonal supports.
- Construct a candidate unitary operator $\tilde{U}$.
- Use the lemma on equivalence of processors.

Proposition

When $n = 2$, $\mathcal{U}^{A}_{block-diag} = \mathcal{U}_{unital}$, *so we have*

$$\mathcal{U}^{A}_{block-diag} = \mathcal{U}_{prob-lin} = \mathcal{U}_{prob} = \mathcal{U}_{mixed} = \mathcal{U}_{unital}.$$

Non-invariant structures

- We focus next on some classes of channels which depend on some particular choice of basis

$$\mathcal{L}_{diag} = \{L \,:\, L(\mathrm{diag}) \subseteq \mathrm{diag}\}$$
$$\mathcal{L}_{tens} = \{L \,:\, L(\mathcal{M}_d(\mathbb{C}) \otimes I_r) \subseteq \mathcal{M}_d(\mathbb{C}) \otimes I_r\}$$

- We shall study both Schrödinger (quantum channels) and Heisenberg (unital CP maps) pictures

$$L_{U,\beta}(\rho) = [\mathrm{id} \otimes \mathrm{Tr}]\left(U(\rho \otimes \beta)U^*\right)$$
$$T_{U,\beta}(\rho) = [\mathrm{id} \otimes \mathrm{Tr}]\left(U^*(\rho \otimes I_k)U(I_n \otimes \beta)\right)$$

- We write

$$\mathcal{U}_{S,diag} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta} \in \mathcal{L}_{diag}\}$$
$$\mathcal{U}_{H,diag} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ T_{U,\beta} \in \mathcal{L}_{diag}\}$$
$$\mathcal{U}_{S,tens} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta} \in \mathcal{L}_{tens}\}$$
$$\mathcal{U}_{H,tens} := \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ T_{U,\beta} \in \mathcal{L}_{tens}\}$$

Matrices of partial isometries

Definition

An operator $R \in M_{nk}(\mathbb{C}) \cong M_n(M_k(\mathbb{C}))$ is called a matrix of partial isometries if its blocks R_{ij} defined by $R = \sum_{i,j=1}^{n} e_i e_j^* \otimes R_{ij}$ are partial isometries. Let E_{ij} (resp. F_{ij}) be the initial (resp. final) spaces of the partial isometries R_{ij}. R is said to be of type (1,2,3,4) respectively if

1. For all $i \in [n]$, the subspaces $\{E_{ij}\}_{j \in [n]}$ form a partition of $\mathbb{C}^k$;
2. For all $i \in [n]$, the subspaces $\{F_{ij}\}_{j \in [n]}$ form a partition of $\mathbb{C}^k$;
3. For all $j \in [n]$, the subspaces $\{E_{ij}\}_{i \in [n]}$ form a partition of $\mathbb{C}^k$;
4. For all $j \in [n]$, the subspaces $\{F_{ij}\}_{i \in [n]}$ form a partition of $\mathbb{C}^k$.

Lemma

A matrix of partial isometries is unitary iff it is of type (2,3).

Strucutre preserving maps

Theorem

Let $\{e_1, \ldots, e_n\}$ be some fixed basis of $\mathbb{C}^n$ and let diag be the diagonal sub-algebra of $\mathcal{M}_n(\mathbb{C})$. We have

$$\begin{aligned}\mathcal{U}_{H,diag} &= \{\text{matrices of partial isometries of type } (2,3)\} \\ &= \{\text{unitary matrices of partial isometries}\} \\ \mathcal{U}_{S,diag} &= \{\text{matrices of partial isometries of type } (2,3,4)\}\end{aligned}$$

Theorem

In the case of the tensor product algebra, we have (here, $n = dr$)

$$\begin{aligned}\mathcal{U}_{H,tens} &= \{(I_d \otimes V) \cdot (W \otimes I_r), : \ V \in \mathcal{U}_{rk}, \ W \in \mathcal{U}_{dk}\} \\ \mathcal{U}_{S,tens} &= \{(I_d \otimes V^\Gamma) \cdot (W \otimes I_r), : \ V \in \mathcal{U}_{rk} \cap \mathcal{U}_{rk}^\Gamma, \ W \in \mathcal{U}_{dk}\}\end{aligned}$$

Quantum latin squares

- A matrix of partial isometries of type (1,2,3,4), with $n = k$ and $\dim E_{ij} = \dim F_{ij} = 1$ for all i, j, is called a quantum Latin square.

Definition

A quantum Latin square (QLS) of order n is a matrix $X = (x_{ij})_{i,j=1}^{n}$, where $x_{ij} \in \mathbb{C}^n$ are such that the vectors on each row (resp. column) of X form an orthonormal basis of $\mathbb{C}^n$.

- Each classical latin square L_{ij} and each orthonormal basis $\{e_i\}$ of $\mathbb{C}^n$ induces a QLS by setting $x_{ij} = e_{L_{ij}}$.
- There exist non-classical QLS [Musto, Vicary]:

$$X = \begin{bmatrix} |0\rangle & |1\rangle & |2\rangle & |3\rangle \\ \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) & \frac{1}{\sqrt{5}}(i|0\rangle + 2|3\rangle) & \frac{1}{\sqrt{5}}(2|0\rangle + i|3\rangle) & \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \\ \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) & \frac{1}{\sqrt{5}}(2|0\rangle + i|3\rangle) & \frac{1}{\sqrt{5}}(i|0\rangle + 2|3\rangle) & \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) \\ |3\rangle & |2\rangle & |1\rangle & |0\rangle \end{bmatrix}$$

Sampling quantum Latin squares

- We conjecture that the following algorithm, which generalizes Sinkhorn's classical procedure, produces (random) quantum Latin squares

Non-commutative Sinkhorn algorithm for sampling QLS

1. **Input:** The dimension n and an error parameter $\varepsilon > 0$
2. Start with x_{ij} independent uniform points on the unit sphere of $\mathbb{C}^n$.
3. While X is not an ε-QLS, do the steps (4-6)
4. Define the matrix Y by making the rows of X unitary:
$$\forall i \in [n], \qquad y_{ij} = \mathrm{Pol}\left(\sum_{s=1}^{n} x_{is} e_s^* \right) \cdot e_j .$$
5. Define the matrix Z by making the columns of Y unitary:
$$\forall j \in [n], \qquad z_{ij} = \mathrm{Pol}\left(\sum_{s=1}^{n} y_{sj} e_s^* \right) \cdot e_i .$$
6. $X \leftarrow Z$.
7. **Output:** X, an ε-QLS.

Open questions / work in progress

Question (Mixed channels)

For all values of n, k, we conjecture that $\mathcal{U}^A_{block-diag} = \mathcal{U}_{mixed}$.

Question (Other sets of channels)

Characterize the unitarily invariant sets

$$\mathcal{U}_{PPT} = \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta} \text{ is a PPT channel } \}$$

$$\mathcal{U}_{EB} = \{U \in \mathcal{U}_{nk} \,|\, \forall \beta \in \mathcal{M}_k^{1,+}(\mathbb{C}),\ L_{U,\beta} \text{ is an entanglement breaking channel } \}.$$

Obviously, $\mathcal{U}_{const} \subseteq \mathcal{U}_{EB} \subseteq \mathcal{U}_{PPT}$, *and, if* $n = k$, $\mathcal{U}^A_{block-diag} \cdot F_n \subseteq \mathcal{U}_{EB} \subseteq \mathcal{U}_{PPT}$. *Is there equality ?*

Question (Generating random bipartite unitary operators)

Show that the iterative algorithms for sampling from $\mathcal{U}_{unital}$ *and* $\mathcal{U}_{S,diag}$ *(or* $\mathcal{QLS}$*) converge, and study the distribution of the limit.*

The End

thank you for your attention

- Deschamps, J., N.I., Pellegrini, C. *On some classes of bipartite unitary operators.* Preprint arXiv:1509.06543.
- Benoist, T., N.I. *Unitary operators generating structure-preserving quantum dynamics.* Soon™ on the arXiv.
- Hillery, M., Ziman, M., Bužek, V. *Implementation of quantum maps by programmable quantum processors.* Physical Review A, 66(4), 042302 (2002).
- Musto, B., Vicary, J. *Quantum Latin squares and unitary error bases.* Preprint arXiv:1504.02715.