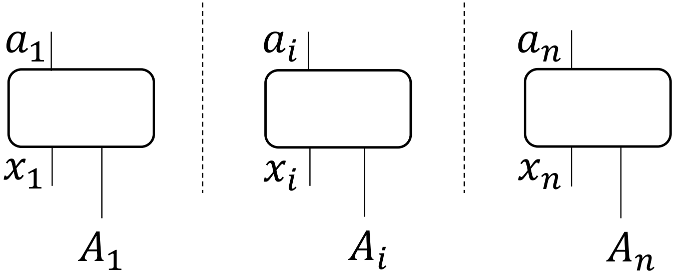
Security based on quantum extremality - from no-signaling assemblages to channel steering with information leakage

Michał Banacki

International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk
joint work with R. Rmanathan, R. Ravell-Rodríguez, and P. Horodecki

QIMG2023, Foundations and Developments of Quantum Information Theory, September 18-22, 2023

Bell-type scenario



Probabilistic description of an experiment with n parties, m measurements, and k outcomes, where $\mathbf{x}_n = (x_1, \ldots, x_n)$ and $\mathbf{a}_n = (a_1, \ldots, a_n)$, is given by

$$P = \{p(\mathbf{a}_n|\mathbf{x}_n)\}_{\mathbf{a}_n,\mathbf{x}_n} .$$

Relationship between sets of correlations

$\mathbf{NS}(n, m, k)$ - polytope of no-signaling correlations

$\mathbf{Q}(n, m, k)$ - convex sets of quantum correlations

$\mathbf{LOC}(n, m, k)$ - polytope of local correlations

$$\mathbf{LOC}(n, m, k) \subsetneq \mathbf{Q}(n, m, k) \subsetneq \mathbf{NS}(n, m, k)$$

Theorem ([RTHH16])

Consider any Bell-type experiment given by n, m, k. Let $P \in \mathbf{NS}(n, m, k)$ be an extreme point in $\mathbf{NS}(n, m, k)$ such that $P \notin \mathbf{LOC}(n, m, k)$. In that case $P \notin \mathrm{cl}(\mathbf{Q}(n, m, k))$.

Relationship between sets of correlations

$\mathbf{NS}(n, m, k)$ - polytope of no-signaling correlations

$\mathbf{Q}(n, m, k)$ - convex sets of quantum correlations

$\mathbf{LOC}(n, m, k)$ - polytope of local correlations

$$\mathbf{LOC}(n, m, k) \subsetneq \mathbf{Q}(n, m, k) \subsetneq \mathbf{NS}(n, m, k)$$

Theorem ([RTHH16])

Consider any Bell-type experiment given by n, m, k. Let $P \in \mathbf{NS}(n, m, k)$ be an extreme point in $\mathbf{NS}(n, m, k)$ such that $P \notin \mathbf{LOC}(n, m, k)$. In that case $P \notin \mathrm{cl}(\mathbf{Q}(n, m, k))$.

Relationship between sets of correlations

$\mathbf{NS}(n, m, k)$ - polytope of no-signaling correlations

$\mathbf{Q}(n, m, k)$ - convex sets of quantum correlations

$\mathbf{LOC}(n, m, k)$ - polytope of local correlations

$$\mathbf{LOC}(n, m, k) \subsetneq \mathbf{Q}(n, m, k) \subsetneq \mathbf{NS}(n, m, k)$$

Theorem ([RTHH16])

Consider any Bell-type experiment given by n, m, k. Let $P \in \mathbf{NS}(n, m, k)$ be an extreme point in $\mathbf{NS}(n, m, k)$ such that $P \notin \mathbf{LOC}(n, m, k)$. In that case $P \notin \mathrm{cl}(\mathbf{Q}(n, m, k))$.

Relationship between sets of correlations

$\mathbf{NS}(n, m, k)$ - polytope of no-signaling correlations

$\mathbf{Q}(n, m, k)$ - convex sets of quantum correlations

$\mathbf{LOC}(n, m, k)$ - polytope of local correlations

$$\mathbf{LOC}(n, m, k) \subsetneq \mathbf{Q}(n, m, k) \subsetneq \mathbf{NS}(n, m, k)$$

Theorem ([RTHH16])

Consider any Bell-type experiment given by n, m, k. Let $P \in \mathbf{NS}(n, m, k)$ be an extreme point in $\mathbf{NS}(n, m, k)$ such that $P \notin \mathbf{LOC}(n, m, k)$. In that case $P \notin \mathrm{cl}(\mathbf{Q}(n, m, k))$.

Relationship between sets of correlations

$\mathbf{NS}(n, m, k)$ - polytope of no-signaling correlations

$\mathbf{Q}(n, m, k)$ - convex sets of quantum correlations

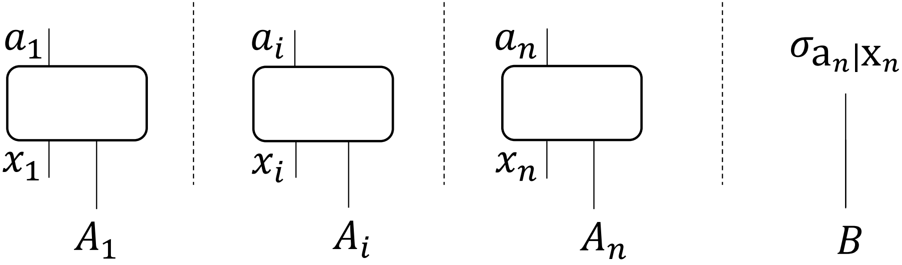
$\mathbf{LOC}(n, m, k)$ - polytope of local correlations

$$\mathbf{LOC}(n, m, k) \subsetneq \mathbf{Q}(n, m, k) \subsetneq \mathbf{NS}(n, m, k)$$

Theorem ([RTHH16])

Consider any Bell-type experiment given by n, m, k. Let $P \in \mathbf{NS}(n, m, k)$ be an extreme point in $\mathbf{NS}(n, m, k)$ such that $P \notin \mathbf{LOC}(n, m, k)$. In that case $P \notin \mathrm{cl}(\mathbf{Q}(n, m, k))$.

Steering scenario

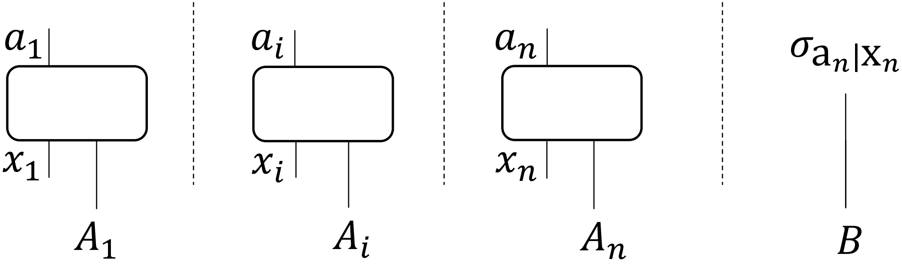


Probabilistic description of an experiment with n parties, m measurements, and k outcomes, where $\mathbf{x}_n = (x_1, \ldots, x_n)$ and $\mathbf{a}_n = (a_1, \ldots, a_n)$, is given by

$$\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}.$$

Remark: One can consider steering in an infinite dimensional setting of C*-algebras [B23].

Steering scenario



Probabilistic description of an experiment with n parties, m measurements, and k outcomes, where $\mathbf{x}_n = (x_1, \ldots, x_n)$ and $\mathbf{a}_n = (a_1, \ldots, a_n)$, is given by

$$\Sigma = \left\{ \sigma_{\mathbf{a}_n|\mathbf{x}_n} \right\}_{\mathbf{a}_n, \mathbf{x}_n}.$$

Remark: One can consider steering in an infinite dimensional setting of C*-algebras [B23].

Quantum, local and no-signaling assemblages

Collection of subnormalized states $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ form a *quantum assemblage* if it can be realized as

$$\sigma_{\mathbf{a}_n|\mathbf{x}_n} = \mathrm{Tr}_{A_1\ldots A_n}(M^{(A_1)}_{a_1|x_1} \otimes \ldots M^{(A_n)}_{a_n|x_n} \otimes \mathbb{1}\rho_{A_1\ldots A_n B}).$$

Additionally, we say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is a *local assemblages* if

$$\sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sum_j q_j p^{(1)}_j(a_1|x_1)\ldots p^{(n)}_j(a_n|x_n)\sigma_j$$

where $q_i \geq 0, \sum_j q_j = 1$, and σ_j are some states of trusted subsystem B. Finally, $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is a *no-signaling assemblage* if

$$\sum_{a_j, j\notin I} \sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sigma_{a_{i_1}\ldots a_{i_s}|x_{i_1}\ldots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sigma,$$

for any set of indexes $I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$ and some state σ on B.

Quantum, local and no-signaling assemblages

Collection of subnormalized states $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ form a *quantum assemblage* if it can be realized as

$$\sigma_{\mathbf{a}_n|\mathbf{x}_n} = \mathrm{Tr}_{A_1\ldots A_n}(M^{(A_1)}_{a_1|x_1} \otimes \ldots M^{(A_n)}_{a_n|x_n} \otimes \mathbb{1}\rho_{A_1\ldots A_n B}).$$

Additionally, we say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is a *local assemblages* if

$$\sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sum_j q_j p_j^{(1)}(a_1|x_1)\ldots p_j^{(n)}(a_n|x_n)\sigma_j$$

where $q_i \geq 0, \sum_j q_j = 1$, and σ_j are some states of trusted subsystem B.
Finally, $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is a *no-signaling assemblage* if

$$\sum_{a_j, j\notin I} \sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sigma_{a_{i_1}\ldots a_{i_s}|x_{i_1}\ldots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sigma,$$

for any set of indexes $I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$ and some state σ on B.

Quantum, local and no-signaling assemblages

Collection of subnormalized states $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ form a *quantum assemblage* if it can be realized as

$$\sigma_{\mathbf{a}_n|\mathbf{x}_n} = \mathrm{Tr}_{A_1\ldots A_n}(M^{(A_1)}_{a_1|x_1} \otimes \ldots M^{(A_n)}_{a_n|x_n} \otimes \mathbb{1}\rho_{A_1\ldots A_n B}).$$

Additionally, we say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is a *local assemblages* if

$$\sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sum_j q_j p^{(1)}_j(a_1|x_1)\ldots p^{(n)}_j(a_n|x_n)\sigma_j$$

where $q_i \geq 0, \sum_j q_j = 1$, and σ_j are some states of trusted subsystem B. Finally, $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is a *no-signaling assemblage* if

$$\sum_{a_j, j\notin I} \sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sigma_{a_{i_1}\ldots a_{i_s}|x_{i_1}\ldots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \sigma_{\mathbf{a}_n|\mathbf{x}_n} = \sigma,$$

for any set of indexes $I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$ and some state σ on B.

Relationship between sets of assemblages

$\mathbf{nsA}(n, m, k, d_B)$ - convex set of no-signaling assemblages

$\mathbf{qA}(n, m, k, d_B)$ - convex set of quantum assemblages

$\mathbf{lA}(n, m, k, d_B)$ - convex set of local assemblages

$$\mathbf{lA}(n, m, k, d_B) \subsetneq \mathbf{qA}(n, m, k, d_B) \subset \mathbf{nsA}(n, m, k, d_B)$$

Remark: There is no post-quantum steering for $n = 1$ [G89,HJW93].

Main question: Is there a possibility of quantum realization of extreme yet non-local point in $\mathbf{nsA}(n, m, k, d_B)$ for non-trivila case?

Relationship between sets of assemblages

nsA(n, m, k, d_B) - convex set of no-signaling assemblages

qA(n, m, k, d_B) - convex set of quantum assemblages

lA(n, m, k, d_B) - convex set of local assemblages

$$\mathbf{lA}(n, m, k, d_B) \subsetneq \mathbf{qA}(n, m, k, d_B) \subset \mathbf{nsA}(n, m, k, d_B)$$

Remark: There is no post-quantum steering for $n = 1$ [G89,HJW93].

Main question: Is there a possibility of quantum realization of extreme yet non-local point in **nsA**(n, m, k, d_B) for non-trivila case?

Relationship between sets of assemblages

$\mathbf{nsA}(n, m, k, d_B)$ - convex set of no-signaling assemblages

$\mathbf{qA}(n, m, k, d_B)$ - convex set of quantum assemblages

$\mathbf{lA}(n, m, k, d_B)$ - convex set of local assemblages

$$\mathbf{lA}(n, m, k, d_B) \subsetneq \mathbf{qA}(n, m, k, d_B) \subset \mathbf{nsA}(n, m, k, d_B)$$

Remark: There is no post-quantum steering for $n = 1$ [G89,HJW93].

Main question: Is there a possibility of quantum realization of extreme yet non-local point in $\mathbf{nsA}(n, m, k, d_B)$ for non-trivila case?

Relationship between sets of assemblages

$\mathbf{nsA}(n, m, k, d_B)$ - convex set of no-signaling assemblages

$\mathbf{qA}(n, m, k, d_B)$ - convex set of quantum assemblages

$\mathbf{lA}(n, m, k, d_B)$ - convex set of local assemblages

$$\mathbf{lA}(n, m, k, d_B) \subsetneq \mathbf{qA}(n, m, k, d_B) \subset \mathbf{nsA}(n, m, k, d_B)$$

Remark: There is no post-quantum steering for $n = 1$ [G89,HJW93].

Main question: Is there a possibility of quantum realization of extreme yet non-local point in $\mathbf{nsA}(n, m, k, d_B)$ for non-trivila case?

Relationship between sets of assemblages

$\mathbf{nsA}(n, m, k, d_B)$ - convex set of no-signaling assemblages

$\mathbf{qA}(n, m, k, d_B)$ - convex set of quantum assemblages

$\mathbf{lA}(n, m, k, d_B)$ - convex set of local assemblages

$$\mathbf{lA}(n, m, k, d_B) \subsetneq \mathbf{qA}(n, m, k, d_B) \subset \mathbf{nsA}(n, m, k, d_B)$$

Remark: There is no post-quantum steering for $n = 1$ [G89,HJW93].

Main question: Is there a possibility of quantum realization of extreme yet non-local point in $\mathbf{nsA}(n, m, k, d_B)$ for non-trivila case?

Inflexibility of assemblages

We say that $\Sigma = \{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n}$ is an assemblage of pure states if a rank of $\sigma_{\mathbf{a}_n|\mathbf{x}_n}$ is not greater than one for all $\mathbf{a}_n, \mathbf{x}_n$.

For $\Sigma = \{p_{\mathbf{a}_n|\mathbf{x}_n} |\psi_{\mathbf{a}_n|\mathbf{x}_n}\rangle\langle\psi_{\mathbf{a}_n|\mathbf{x}_n}|\}_{\mathbf{a}_n|\mathbf{x}_n}$ define $S_\Sigma \subset \mathbf{nsA}(n, m, k, d_B)$ as a set of all assemblages of the form $\Sigma' = \{q_{\mathbf{a}_n|\mathbf{x}_n} |\psi_{\mathbf{a}_n|\mathbf{x}_n}\rangle\langle\psi_{\mathbf{a}_n|\mathbf{x}_n}|\}_{\mathbf{a}_n|\mathbf{x}_n}$ such that $p_{\mathbf{a}_n|\mathbf{x}_n} = 0$ implies $q_{\mathbf{a}_n|\mathbf{x}_n} = 0$ for arbitrary $\mathbf{a}_n, \mathbf{x}_n$.

Definition ([RBRH20])

We say that $\Sigma = \{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n}$ is inflexible if $S_\Sigma = \{\Sigma\}$.

Inflexibility of assemblages

We say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is an assemblage of pure states if a rank of $\sigma_{\mathbf{a}_n|\mathbf{x}_n}$ is not greater than one for all $\mathbf{a}_n, \mathbf{x}_n$.

For $\Sigma = \left\{p_{\mathbf{a}_n|\mathbf{x}_n}|\psi_{\mathbf{a}_n|\mathbf{x}_n}\rangle\langle\psi_{\mathbf{a}_n|\mathbf{x}_n}|\right\}_{\mathbf{a}_n|\mathbf{x}_n}$ define $S_\Sigma \subset \mathbf{nsA}(n, m, k, d_B)$ as a set of all assemblages of the form $\Sigma' = \left\{q_{\mathbf{a}_n|\mathbf{x}_n}|\psi_{\mathbf{a}_n|\mathbf{x}_n}\rangle\langle\psi_{\mathbf{a}_n|\mathbf{x}_n}|\right\}_{\mathbf{a}_n|\mathbf{x}_n}$ such that $p_{\mathbf{a}_n|\mathbf{x}_n} = 0$ implies $q_{\mathbf{a}_n|\mathbf{x}_n} = 0$ for arbitrary $\mathbf{a}_n, \mathbf{x}_n$.

Definition ([RBRH20])

We say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is inflexible if $S_\Sigma = \{\Sigma\}$.

Inflexibility of assemblages

We say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is an assemblage of pure states if a rank of $\sigma_{\mathbf{a}_n|\mathbf{x}_n}$ is not greater than one for all $\mathbf{a}_n, \mathbf{x}_n$.

For $\Sigma = \left\{p_{\mathbf{a}_n|\mathbf{x}_n}|\psi_{\mathbf{a}_n|\mathbf{x}_n}\rangle\langle\psi_{\mathbf{a}_n|\mathbf{x}_n}|\right\}_{\mathbf{a}_n|\mathbf{x}_n}$ define $S_\Sigma \subset \mathbf{nsA}(n, m, k, d_B)$ as a set of all assemblages of the form $\Sigma' = \left\{q_{\mathbf{a}_n|\mathbf{x}_n}|\psi_{\mathbf{a}_n|\mathbf{x}_n}\rangle\langle\psi_{\mathbf{a}_n|\mathbf{x}_n}|\right\}_{\mathbf{a}_n|\mathbf{x}_n}$ such that $p_{\mathbf{a}_n|\mathbf{x}_n} = 0$ implies $q_{\mathbf{a}_n|\mathbf{x}_n} = 0$ for arbitrary $\mathbf{a}_n, \mathbf{x}_n$.

Definition ([RBRH20])

We say that $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ is inflexible if $S_\Sigma = \{\Sigma\}$.

Extremality of inflexible assemblages

Consider an inflexible assemblage $\Sigma = \{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n} \in \mathbf{nsA}(n, m, k, d_B)$ and define

$$\rho_{\mathbf{a}_n|\mathbf{x}_n} = \begin{cases} 0 & \text{for } \sigma_{\mathbf{a}_n|\mathbf{x}_n} = 0, \\ \frac{\sigma_{\mathbf{a}_n|\mathbf{x}_n}}{\mathrm{Tr}(\sigma_{\mathbf{a}_n|\mathbf{x}_n})} & \text{for } \sigma_{\mathbf{a}_n|\mathbf{x}_n} \neq 0. \end{cases}$$

We introduce the following functional

$$F_\Sigma(\tilde{\Sigma}) = \sum_{\mathbf{a}_n,\mathbf{x}_n} \mathrm{Tr}(\rho_{\mathbf{a}_n|\mathbf{x}_n} \tilde{\sigma}_{\mathbf{a}_n|\mathbf{x}_n}).$$

where $\tilde{\Sigma} = \{\tilde{\sigma}_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n} \in \mathbf{nsA}(n, m, k, d_B)$. One can show that

$$F_\Sigma(\tilde{\Sigma}) \leq m^n$$

for all $\tilde{\Sigma}$ and equality holds if and only if $\tilde{\Sigma} = \Sigma$.

Extremality of inflexible assemblages

Consider an inflexible assemblage $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n} \in \mathbf{nsA}(n, m, k, d_B)$ and define

$$\rho_{\mathbf{a}_n|\mathbf{x}_n} = \begin{cases} 0 & \text{for } \sigma_{\mathbf{a}_n|\mathbf{x}_n} = 0, \\ \frac{\sigma_{\mathbf{a}_n|\mathbf{x}_n}}{\mathrm{Tr}(\sigma_{\mathbf{a}_n|\mathbf{x}_n})} & \text{for } \sigma_{\mathbf{a}_n|\mathbf{x}_n} \neq 0. \end{cases}$$

We introduce the following functional

$$F_\Sigma(\tilde{\Sigma}) = \sum_{\mathbf{a}_n,\mathbf{x}_n} \mathrm{Tr}(\rho_{\mathbf{a}_n|\mathbf{x}_n} \tilde{\sigma}_{\mathbf{a}_n|\mathbf{x}_n}).$$

where $\tilde{\Sigma} = \left\{\tilde{\sigma}_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n} \in \mathbf{nsA}(n, m, k, d_B)$. One can show that

$$F_\Sigma(\tilde{\Sigma}) \leq m^n$$

for all $\tilde{\Sigma}$ and equality holds if and only if $\tilde{\Sigma} = \Sigma$.

Extremality of inflexible assemblages

Consider an inflexible assemblage $\Sigma = \left\{\sigma_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n} \in \mathbf{nsA}(n, m, k, d_B)$ and define

$$\rho_{\mathbf{a}_n|\mathbf{x}_n} = \begin{cases} 0 & \text{for } \sigma_{\mathbf{a}_n|\mathbf{x}_n} = 0, \\ \frac{\sigma_{\mathbf{a}_n|\mathbf{x}_n}}{\mathrm{Tr}(\sigma_{\mathbf{a}_n|\mathbf{x}_n})} & \text{for } \sigma_{\mathbf{a}_n|\mathbf{x}_n} \neq 0. \end{cases}$$

We introduce the following functional

$$F_\Sigma(\tilde{\Sigma}) = \sum_{\mathbf{a}_n,\mathbf{x}_n} \mathrm{Tr}(\rho_{\mathbf{a}_n|\mathbf{x}_n} \tilde{\sigma}_{\mathbf{a}_n|\mathbf{x}_n}).$$

where $\tilde{\Sigma} = \left\{\tilde{\sigma}_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n} \in \mathbf{nsA}(n, m, k, d_B)$. One can show that

$$F_\Sigma(\tilde{\Sigma}) \leq m^n$$

for all $\tilde{\Sigma}$ and equality holds if and only if $\tilde{\Sigma} = \Sigma$.

Extremality of quantum assemblages

In the simplest non-trivial case $\mathbf{nsA}(2,2,2,d_C)$ we introduce as set of sufficient conditions for inflexibility.

Theorem ([RBRH22])

For any genuine entangled pure state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_C}$ there are PVMs, defined by $P_{a|x}, Q_{b|y}$ when $a,b,x,y = 0,1$, such that

$$\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$$

defines an inflexible assemblage. Moreover, Σ is not local, nor it belongs to the set of biseparable assemblages.

Remark: Self-testing results from F_{Σ} for pure states and projection measurements.

Extremality of quantum assemblages

In the simplest non-trivial case $\mathbf{nsA}(2, 2, 2, d_C)$ we introduce as set of sufficient conditions for inflexibility.

Theorem ([RBRH22])

For any genuine entangled pure state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_C}$ there are PVMs, defined by $P_{a|x}, Q_{b|y}$ when $a, b, x, y = 0, 1$, such that

$$\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$$

defines an inflexible assemblage. Moreover, Σ is not local, nor it belongs to the set of biseparable assemblages.

Remark: Self-testing results from F_Σ for pure states and projection measurements.

Extremality of quantum assemblages

In the simplest non-trivial case $\mathbf{nsA}(2,2,2,d_C)$ we introduce as set of sufficient conditions for inflexibility.

Theorem ([RBRH22])

For any genuine entangled pure state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^{d_C}$ there are PVMs, defined by $P_{a|x}, Q_{b|y}$ when $a, b, x, y = 0, 1$, such that

$$\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$$

defines an inflexible assemblage. Moreover, Σ is not local, nor it belongs to the set of biseparable assemblages.

Remark: Self-testing results from F_Σ for pure states and projection measurements.

Exmaple of steering inequality from inflexibility

Consider a three-qubits GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

Define $\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$ where $P_{0|0} = Q_{0|0} = |+\rangle\langle+|$ and $P_{0|1} = Q_{0|1} = |0\rangle\langle 0|$, i.e.

$$\Sigma_{GHZ} = \frac{1}{4}\left(\begin{array}{cc|cc} |+\rangle\langle+| & |-\rangle\langle-| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ |-\rangle\langle-| & |+\rangle\langle+| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ \hline |0\rangle\langle 0| & |0\rangle\langle 0| & 2|0\rangle\langle 0| & 0 \\ |1\rangle\langle 1| & |1\rangle\langle 1| & 0 & 2|1\rangle\langle 1| \end{array}\right).$$

Σ_{GHZ} is inflexible and not biseparable

$$\mathcal{C}_{\mathbf{IA}} = \sup_{\Sigma\in\mathbf{IA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{4+\sqrt{10}}{2},$$

$$\mathcal{C}_{\mathbf{bisA}} = \sup_{\Sigma\in\mathbf{bisA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{5+\sqrt{5}}{2}.$$

Exmaple of steering inequality from inflexibility

Consider a three-qubits GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

Define $\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$ where $P_{0|0} = Q_{0|0} = |+\rangle\langle+|$ and $P_{0|1} = Q_{0|1} = |0\rangle\langle 0|$, i.e.

$$\Sigma_{GHZ} = \frac{1}{4}\left(\begin{array}{cc|cc} |+\rangle\langle+| & |-\rangle\langle-| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ |-\rangle\langle-| & |+\rangle\langle+| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ \hline |0\rangle\langle 0| & |0\rangle\langle 0| & 2|0\rangle\langle 0| & 0 \\ |1\rangle\langle 1| & |1\rangle\langle 1| & 0 & 2|1\rangle\langle 1| \end{array}\right).$$

Σ_{GHZ} is inflexible and not biseparable

$$\mathcal{C}_{\mathbf{IA}} = \sup_{\Sigma\in\mathbf{IA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{4+\sqrt{10}}{2},$$

$$\mathcal{C}_{\mathbf{bisA}} = \sup_{\Sigma\in\mathbf{bisA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{5+\sqrt{5}}{2}.$$

Exmaple of steering inequality from inflexibility

Consider a three-qubits GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

Define $\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$ where $P_{0|0} = Q_{0|0} = |+\rangle\langle+|$ and $P_{0|1} = Q_{0|1} = |0\rangle\langle 0|$, i.e.

$$\Sigma_{GHZ} = \frac{1}{4}\left(\begin{array}{cc|cc} |+\rangle\langle+| & |-\rangle\langle-| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ |-\rangle\langle-| & |+\rangle\langle+| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ \hline |0\rangle\langle 0| & |0\rangle\langle 0| & 2|0\rangle\langle 0| & 0 \\ |1\rangle\langle 1| & |1\rangle\langle 1| & 0 & 2|1\rangle\langle 1| \end{array}\right).$$

Σ_{GHZ} is inflexible and not biseparable

$$\mathcal{C}_{\mathbf{IA}} = \sup_{\Sigma \in \mathbf{IA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{4+\sqrt{10}}{2},$$

$$\mathcal{C}_{\mathbf{bisA}} = \sup_{\Sigma \in \mathbf{bisA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{5+\sqrt{5}}{2}.$$

Exmaple of steering inequality from inflexibility

Consider a three-qubits GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

Define $\sigma_{ab|xy} = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}|\psi\rangle\langle\psi|)$ where $P_{0|0} = Q_{0|0} = |+\rangle\langle+|$ and $P_{0|1} = Q_{0|1} = |0\rangle\langle 0|$, i.e.

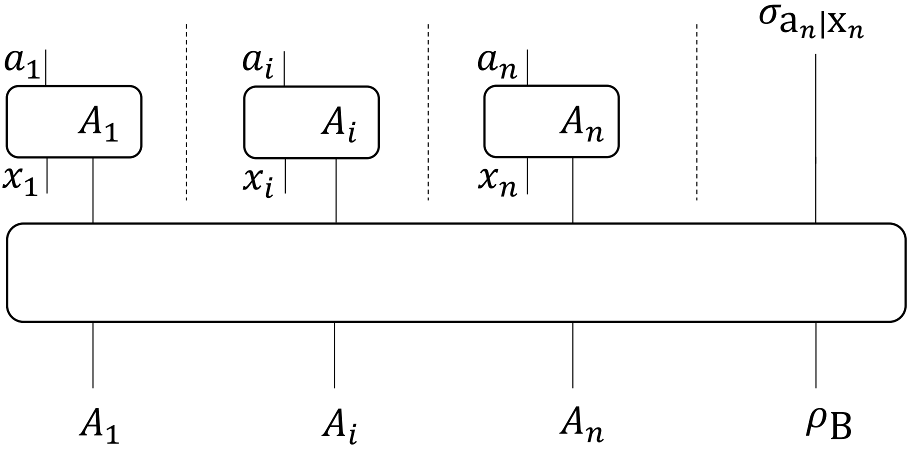
$$\Sigma_{GHZ} = \frac{1}{4}\left(\begin{array}{cc|cc} |+\rangle\langle+| & |-\rangle\langle-| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ |-\rangle\langle-| & |+\rangle\langle+| & |0\rangle\langle 0| & |1\rangle\langle 1| \\ \hline |0\rangle\langle 0| & |0\rangle\langle 0| & 2|0\rangle\langle 0| & 0 \\ |1\rangle\langle 1| & |1\rangle\langle 1| & 0 & 2|1\rangle\langle 1| \end{array}\right).$$

Σ_{GHZ} is inflexible and not biseparable

$$\mathcal{C}_{\mathbf{IA}} = \sup_{\Sigma\in\mathbf{IA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{4+\sqrt{10}}{2},$$

$$\mathcal{C}_{\mathbf{bisA}} = \sup_{\Sigma\in\mathbf{bisA}} F_{\Sigma_{GHZ}}(\Sigma) = \frac{5+\sqrt{5}}{2}.$$

Channel steering



Channel assemblages

Family $\mathcal{L} = \{\Lambda_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n}$ of CP maps $\Lambda_{\mathbf{a}_n|\mathbf{x}_n} : B(H_B) \to B(H_{\tilde{B}})$ defines a *weakly no-signaling channel assemblage* if

$$\sum_{a_j, j \notin I} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda_{a_{i_1} \ldots a_{i_s}|x_{i_1} \ldots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda,$$

for any subset of indexes $I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$ and a CPTP map Λ.

We say that it admits a quantum realization if

$$\Lambda_{\mathbf{a}_n|\mathbf{x}_n}(\cdot) = \mathrm{Tr}_{A_1,\ldots,A_n}(M^{(1)}_{a_1|x_1} \otimes \ldots \otimes M^{(n)}_{a_n|x_n} \otimes \mathbb{1}(\mathcal{E}(\rho_{A_1,\ldots,A_n} \otimes \cdot))).$$

Possible description on the level of assemblages of Choi matrices

$$\mathcal{J}(\Lambda) = \Lambda \otimes \mathrm{id}(|\phi^+_{BB}\rangle\langle\phi^+_{BB}|).$$

Analogous result: Existence of quantum yet non-local extreme points.

Channel assemblages

Family $\mathcal{L} = \{\Lambda_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n}$ of CP maps $\Lambda_{\mathbf{a}_n|\mathbf{x}_n} : B(H_B) \to B(H_{\tilde{B}})$ defines a *weakly no-signaling channel assemblage* if

$$\sum_{a_j, j\notin I} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda_{a_{i_1}\dots a_{i_s}|x_{i_1}\dots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda,$$

for any subset of indexes $I = \{i_1, \dots, i_s\} \subset \{1, \dots, n\}$ and a CPTP map Λ.

We say that it admits a quantum realization if

$$\Lambda_{\mathbf{a}_n|\mathbf{x}_n}(\cdot) = \mathrm{Tr}_{A_1,\dots,A_n}(M^{(1)}_{a_1|x_1} \otimes \dots \otimes M^{(n)}_{a_n|x_n} \otimes \mathbb{1}(\mathcal{E}(\rho_{A_1,\dots,A_n} \otimes \cdot))).$$

Possible description on the level of assemblages of Choi matrices

$$\mathcal{J}(\Lambda) = \Lambda \otimes \mathrm{id}(|\phi^+_{BB}\rangle\langle\phi^+_{BB}|).$$

Analogous result: Existence of quantum yet non-local extreme points.

Channel assemblages

Family $\mathcal{L} = \{\Lambda_{\mathbf{a}_n|\mathbf{x}_n}\}_{\mathbf{a}_n,\mathbf{x}_n}$ of CP maps $\Lambda_{\mathbf{a}_n|\mathbf{x}_n} : B(H_B) \to B(H_{\tilde{B}})$ defines a *weakly no-signaling channel assemblage* if

$$\sum_{a_j, j\notin I} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda_{a_{i_1}\dots a_{i_s}|x_{i_1}\dots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda,$$

for any subset of indexes $I = \{i_1, \dots, i_s\} \subset \{1, \dots, n\}$ and a CPTP map Λ.

We say that it admits a quantum realization if

$$\Lambda_{\mathbf{a}_n|\mathbf{x}_n}(\cdot) = \mathrm{Tr}_{A_1,\dots,A_n}(M^{(1)}_{a_1|x_1} \otimes \dots \otimes M^{(n)}_{a_n|x_n} \otimes \mathbb{1}(\mathcal{E}(\rho_{A_1,\dots,A_n} \otimes \cdot))).$$

Possible description on the level of assemblages of Choi matrices

$$\mathcal{J}(\Lambda) = \Lambda \otimes \mathrm{id}(|\phi^+_{BB}\rangle\langle\phi^+_{BB}|).$$

Analogous result: Existence of quantum yet non-local extreme points.

Channel assemblages

Family $\mathcal{L} = \left\{\Lambda_{\mathbf{a}_n|\mathbf{x}_n}\right\}_{\mathbf{a}_n,\mathbf{x}_n}$ of CP maps $\Lambda_{\mathbf{a}_n|\mathbf{x}_n} : B(H_B) \to B(H_{\tilde{B}})$ defines a *weakly no-signaling channel assemblage* if

$$\sum_{a_j, j\notin I} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda_{a_{i_1}\ldots a_{i_s}|x_{i_1}\ldots x_{i_s}}, \quad \sum_{\mathbf{a}_n} \Lambda_{\mathbf{a}_n|\mathbf{x}_n} = \Lambda,$$

for any subset of indexes $I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$ and a CPTP map Λ.

We say that it admits a quantum realization if

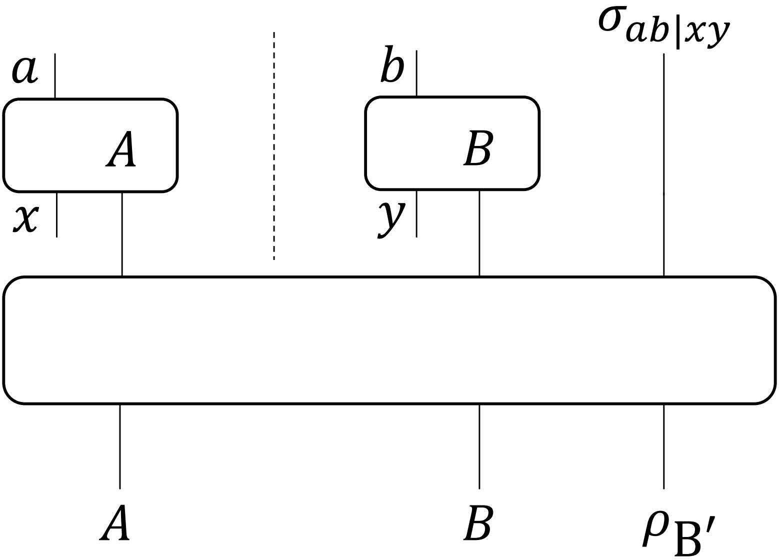
$$\Lambda_{\mathbf{a}_n|\mathbf{x}_n}(\cdot) = \mathrm{Tr}_{A_1,\ldots,A_n}(M^{(1)}_{a_1|x_1} \otimes \ldots \otimes M^{(n)}_{a_n|x_n} \otimes \mathbb{1}(\mathcal{E}(\rho_{A_1,\ldots,A_n} \otimes \cdot))).$$

Possible description on the level of assemblages of Choi matrices

$$\mathcal{J}(\Lambda) = \Lambda \otimes \mathrm{id}(|\phi^+_{BB}\rangle\langle\phi^+_{BB}|).$$

Analogous result: Existence of quantum yet non-local extreme points.

Asymmetric channel steering



Asymmetric channel assemblages

The family $\mathcal{L} = \{\Lambda_{ab|xy}\}_{a,b,x,y}$ of CP maps $\Lambda_{ab|xy} : B(H_{B'}) \to B(H_{\tilde{B}})$ defines an *asymmetric channel assemblage* if

$$\sum_a \Lambda_{ab|xy} = \sum_a \Lambda_{ab|x'y},$$

$$\sum_b \mathrm{Tr}(\Lambda_{ab|xy}) = \sum_b \mathrm{Tr}(\Lambda_{ab|xy'})$$

$$\sum_{a,b} \Lambda_{ab|xy} = \Lambda_{|y},\ \Lambda_{|y} - \mathrm{CPTP}$$

Proposition ([BRH22])

Family $\mathcal{L} = \{\Lambda_{ab|xy}\}_{a,b,x,y}$ given by $\Lambda_{ab|xy} : B(H_{B'}) \to B(H_{\tilde{B}})$ defines an asymmetric channel assemblage if and only if a family of positive Choi matrices $\Sigma = \{\sigma_{ab|xy} = \mathcal{J}(\Lambda_{ab|xy})\}_{ab|xy}$ fulfills the following conditions i) $\sum_a \sigma_{ab|xy} = \sum_a \sigma_{ab|x'y}$, ii) $\sum_b \mathrm{Tr}_{\tilde{B}}(\sigma_{ab|xy}) = \sum_b \mathrm{Tr}_{\tilde{B}}(\sigma_{ab|xy'})$, and iii) $\sum_{a,b} \sigma_{ab|xy} = \sigma_{|y}$ where $\sigma_{|y} \in B(H_{\tilde{B}}) \otimes B(H_{B'})$ such that $\mathrm{Tr}_{\tilde{B}}(\sigma_{|y}) = \frac{\mathbb{1}}{d_{B'}}$.

Asymmetric channel assemblages

The family $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ of CP maps $\Lambda_{ab|xy} : B(H_{B'}) \to B(H_{\tilde{B}})$ defines an *asymmetric channel assemblage* if

$$\sum_a \Lambda_{ab|xy} = \sum_a \Lambda_{ab|x'y},$$

$$\sum_b \mathrm{Tr}(\Lambda_{ab|xy}) = \sum_b \mathrm{Tr}(\Lambda_{ab|xy'})$$

$$\sum_{a,b} \Lambda_{ab|xy} = \Lambda_{|y},\ \Lambda_{|y} - \mathrm{CPTP}$$

Proposition ([BRH22])

Family $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ given by $\Lambda_{ab|xy} : B(H_{B'}) \to B(H_{\tilde{B}})$ defines an asymmetric channel assemblage if and only if a family of positive Choi matrices $\Sigma = \left\{\sigma_{ab|xy} = \mathcal{J}(\Lambda_{ab|xy})\right\}_{ab|xy}$ fulfills the following conditions i) $\sum_a \sigma_{ab|xy} = \sum_a \sigma_{ab|x'y}$, ii) $\sum_b \mathrm{Tr}_{\tilde{B}}(\sigma_{ab|xy}) = \sum_b \mathrm{Tr}_{\tilde{B}}(\sigma_{ab|xy'})$, and iii) $\sum_{a,b} \sigma_{ab|xy} = \sigma_{|y}$ where $\sigma_{|y} \in B(H_{\tilde{B}}) \otimes B(H_{B'})$ such that $\mathrm{Tr}_{\tilde{B}}(\sigma_{|y}) = \frac{\mathbb{1}}{d_{B'}}$.

Security from asymmetric channel assemblages

Consider a channel assemblage $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ for $a, b, x, y \in \{0, 1\}$ where $\Lambda_{ab|xy} : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ admits quantum realization

$$\Lambda_{ab|xy}(\cdot) = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}_{\tilde{B}}(\mathbb{1}_A \otimes \mathcal{E}_{CNOT}(|\phi^+_{AB}\rangle\langle\phi^+_{AB}| \otimes \cdot)))$$

with $P_{0|0} = Q_{0|0} = |0\rangle\langle 0|$ and $P_{0|1} = Q_{0|1} = |+\rangle\langle +|$.

Observe that

$$p(iii|000) = \mathrm{Tr}(|i\rangle\langle i|\Lambda_{ii|00}(|0\rangle\langle 0|)) = \frac{1}{2}, \ i = 0, 1$$

provides a perfectly random one bit.

Possible eavesdropper attack: $\Lambda_{ab|xy} = \sum_e q_e \Lambda^{(e)}_{ab|xy}$ with some asymmetric channel assemblages $\mathcal{L}^{(e)}$.

Analysis of the assemblage of Choi matrices $\Longrightarrow \Lambda_{ab|00} = \Lambda^{(e)}_{ab|00}$ for all a, b.

Security from asymmetric channel assemblages

Consider a channel assemblage $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ for $a, b, x, y \in \{0, 1\}$ where $\Lambda_{ab|xy} : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ admits quantum realization

$$\Lambda_{ab|xy}(\cdot) = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}_{\tilde{B}}(\mathbb{1}_A \otimes \mathcal{E}_{CNOT}(|\phi^+_{AB}\rangle\langle\phi^+_{AB}| \otimes \cdot)))$$

with $P_{0|0} = Q_{0|0} = |0\rangle\langle 0|$ and $P_{0|1} = Q_{0|1} = |+\rangle\langle +|$.

Observe that

$$p(iii|000) = \mathrm{Tr}(|i\rangle\langle i|\Lambda_{ii|00}(|0\rangle\langle 0|)) = \frac{1}{2},\ i = 0, 1$$

provides a perfectly random one bit.

Possible eavesdropper attack: $\Lambda_{ab|xy} = \sum_e q_e \Lambda^{(e)}_{ab|xy}$ with some asymmetric channel assemblages $\mathcal{L}^{(e)}$.

Analysis of the assemblage of Choi matrices $\Longrightarrow \Lambda_{ab|00} = \Lambda^{(e)}_{ab|00}$ for all a, b.

Security from asymmetric channel assemblages

Consider a channel assemblage $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ for $a, b, x, y \in \{0, 1\}$ where $\Lambda_{ab|xy} : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ admits quantum realization

$$\Lambda_{ab|xy}(\cdot) = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}_{\tilde{B}}(\mathbb{1}_A \otimes \mathcal{E}_{CNOT}(|\phi^+_{AB}\rangle\langle\phi^+_{AB}| \otimes \cdot)))$$

with $P_{0|0} = Q_{0|0} = |0\rangle\langle 0|$ and $P_{0|1} = Q_{0|1} = |+\rangle\langle +|$.

Observe that

$$p(iii|000) = \mathrm{Tr}(|i\rangle\langle i|\Lambda_{ii|00}(|0\rangle\langle 0|)) = \frac{1}{2}, \ i = 0, 1$$

provides a perfectly random one bit.

Possible eavesdropper attack: $\Lambda_{ab|xy} = \sum_e q_e \Lambda^{(e)}_{ab|xy}$ with some asymmetric channel assemblages $\mathcal{L}^{(e)}$.

Analysis of the assemblage of Choi matrices $\Longrightarrow \Lambda_{ab|00} = \Lambda^{(e)}_{ab|00}$ for all a, b.

Security from asymmetric channel assemblages

Consider a channel assemblage $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ for $a, b, x, y \in \{0, 1\}$ where $\Lambda_{ab|xy} : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ admits quantum realization

$$\Lambda_{ab|xy}(\cdot) = \mathrm{Tr}_{AB}(P_{a|x} \otimes Q_{b|y} \otimes \mathbb{1}_{\tilde{B}}(\mathbb{1}_A \otimes \mathcal{E}_{CNOT}(|\phi^+_{AB}\rangle\langle\phi^+_{AB}| \otimes \cdot)))$$

with $P_{0|0} = Q_{0|0} = |0\rangle\langle 0|$ and $P_{0|1} = Q_{0|1} = |+\rangle\langle +|$.

Observe that

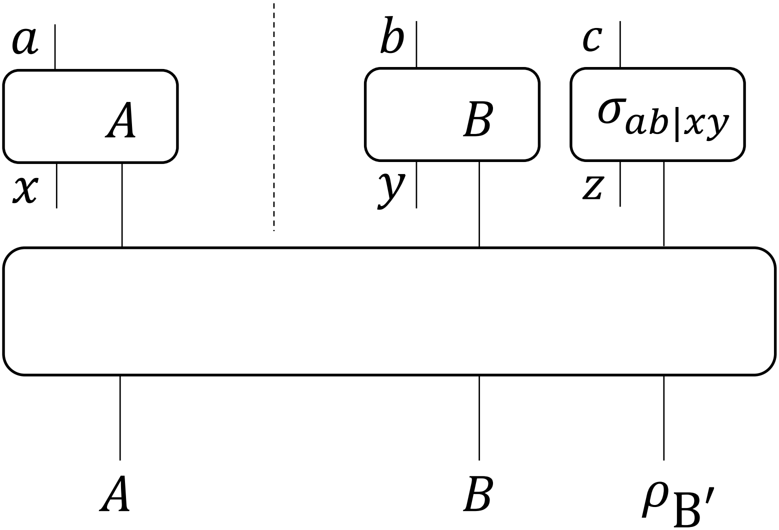
$$p(iii|000) = \mathrm{Tr}(|i\rangle\langle i|\Lambda_{ii|00}(|0\rangle\langle 0|)) = \frac{1}{2},\ i = 0, 1$$

provides a perfectly random one bit.

Possible eavesdropper attack: $\Lambda_{ab|xy} = \sum_e q_e \Lambda^{(e)}_{ab|xy}$ with some asymmetric channel assemblages $\mathcal{L}^{(e)}$.

Analysis of the assemblage of Choi matrices $\Longrightarrow \Lambda_{ab|00} = \Lambda^{(e)}_{ab|00}$ for all a, b.

Hybrid channel behaviors



Security from hybrid channel behaviors

The family $\mathcal{O} = \left\{\Omega_{abc|xyz}\right\}_{a,b,c,x,y,z}$ of CP maps $\Omega_{abc|xyz} : B(H_{B'}) \to \mathbb{C}$ defines a *hybrid channel behavior* if there exists an asymmetric channel assemblage $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ and POVMs elements $M_{c|z}$ such that

$$\Omega_{abc|xyz}(\cdot) = \mathrm{Tr}(M_{c|z}\Lambda_{ab|xy}(\cdot)).$$

Possible description on the level of assemblages of Choi matrices.

Analogous result: Perfectly secure one bit against adversary attack modeled by convex combinations of hybrid channel behaviors.

Security from hybrid channel behaviors

The family $\mathcal{O} = \left\{\Omega_{abc|xyz}\right\}_{a,b,c,x,y,z}$ of CP maps $\Omega_{abc|xyz} : B(H_{B'}) \to \mathbb{C}$ defines a *hybrid channel behavior* if there exists an asymmetric channel assemblage $\mathcal{L} = \left\{\Lambda_{ab|xy}\right\}_{a,b,x,y}$ and POVMs elements $M_{c|z}$ such that

$$\Omega_{abc|xyz}(\cdot) = \mathrm{Tr}(M_{c|z}\Lambda_{ab|xy}(\cdot)).$$

Possible description on the level of assemblages of Choi matrices.

Analogous result: Perfectly secure one bit against adversary attack modeled by convex combinations of hybrid channel behaviors.

Security from hybrid channel behaviors

The family $\mathcal{O} = \{\Omega_{abc|xyz}\}_{a,b,c,x,y,z}$ of CP maps $\Omega_{abc|xyz} : B(H_{B'}) \to \mathbb{C}$ defines a *hybrid channel behavior* if there exists an asymmetric channel assemblage $\mathcal{L} = \{\Lambda_{ab|xy}\}_{a,b,x,y}$ and POVMs elements $M_{c|z}$ such that

$$\Omega_{abc|xyz}(\cdot) = \mathrm{Tr}(M_{c|z}\Lambda_{ab|xy}(\cdot)).$$

Possible description on the level of assemblages of Choi matrices.

Analogous result: Perfectly secure one bit against adversary attack modeled by convex combinations of hybrid channel behaviors.

Thank you for your attention

Literature

- [B23] M. Banacki, *On steering in the C*-algebraic setting*, arXiv:2306.14344 (2023).
- [BRH22] M. Banacki, R. Ramanathan, P. Horodecki, *Multipartite channels assemblages*, arXiv:2205.05033 (2022).
- [G89] N. Gisin, *Stochastic quantum dynamics and relativity*, Helvetica Physica Acta **62**, 363 (1989).
- [HS18] M. J. Hoban, A. B. Sainz, *A channel-based framework for steering, non-locality and beyond*, New J. Phys. **20**, 053048 (2018).
- [HJW93] L. P. Hughston, R. Jozsa, K. Wooters, *A complete classification of quantum ensembles having a given density matrix*, Phys. Lett. A **183**, 14 (1993).
- [P15] M. Piani, *Channel steering*, Journal of the Optical Society of America B Vol. 32, **4**, A1-A7 (2015).

Literature

- [RBRH22] R. Ramanathan, M. Banacki, R. Ravell Rodríguez, P. Horodecki, *Single trusted qubit is necessary and sufficient for quantum realization of extremal no-signaling correlations*, npj Quantum Inf **8**, 119 (2022).
- [RTHH16] R. Ramanathan, J. Tuziemski, M. Horodecki and P. Horodecki, *No quantum realization of extremal no-signaling boxes*, Phys. Rev. Lett. **117**, 050401 (2016).
- [SAPHS18] A. B. Sainz, L. Aolita, M. Piani, M. J. Hoban, P. Skrzypczyk, *A formalism for steering with local quantum measurements*, New J. Phys. **20**, 083040 (2018).
- [SBCSV15] A. B. Sainz, N. Brunner, D. Cavalcanti, P. Skrzypczyk, T. Vértesi, *Postquantum Steering*, Phys. Rev. Lett. **115**, 190403 (2015).
- [ZSH22] B. Zjawin, D. Schmid, M. J. Hoban, A. B. Sainz, *The resource theory of nonclassicality of channel assemblages*, arXiv:2209.10177 (2022).

Acknowledgements

M.B., R. R. R and P.H. acknowledge support by the Foundation for Polish Science (IRAP project, ICTQT, contract no. MAB/2018/5, co-financed by EU within Smart Growth Operational Programme). M. B. acknowledges partial support from by DFG (Germany) and NCN (Poland) within the joint funding initiative Beethoven2 (Grant No. 2016/23/G/ST2/04273).

R.R. acknowledges support from the Start-up Fund 'Device-Independent Quantum Communication Networks' from The University of Hong Kong, the Seed Fund 'Security of Relativistic Quantum Cryptography' and the Early Career Scheme (ECS) grant 'Device-Independent Random Number Generation and Quantum Key Distribution with Weak Random Seeds'.

European Funds Smart Growth

Republic of Poland

FNP Foundation for Polish Science

European Union European Regional Development Fund