Extended nonlocal games

Ph.D. Defense

Vincent Russo

University of Waterloo

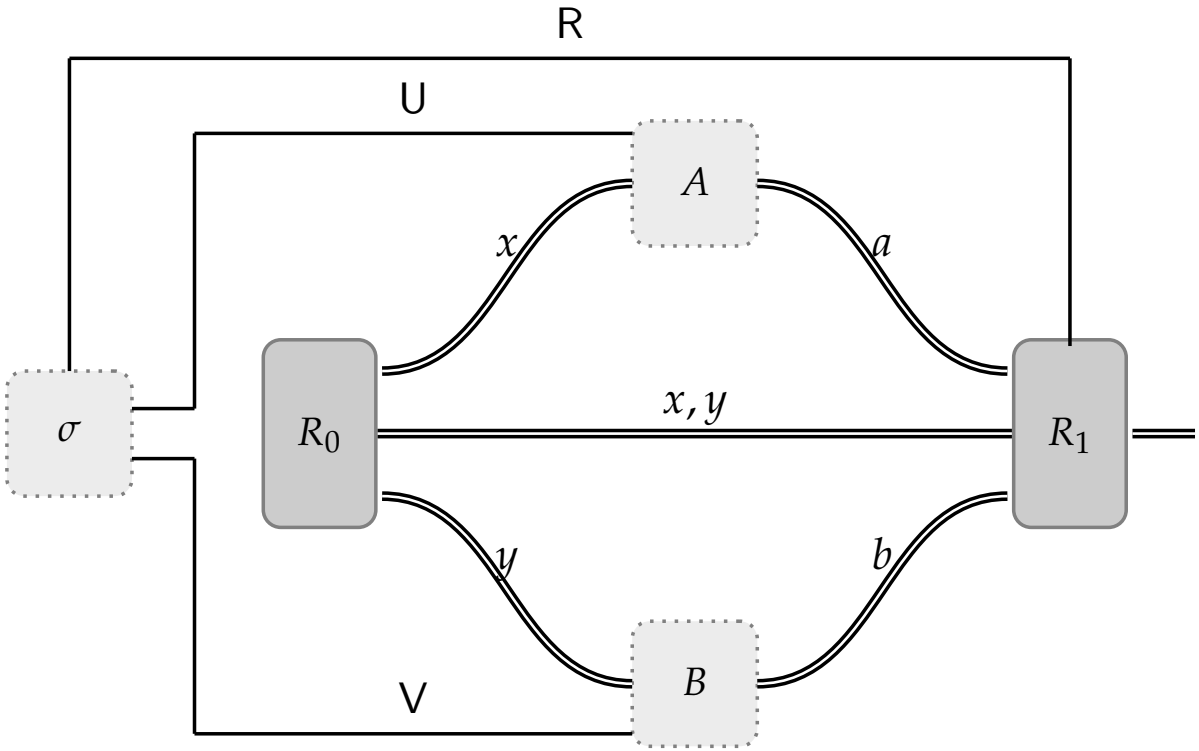
February 1, 2017

Outline

Extended nonlocal games

Extended nonlocal games

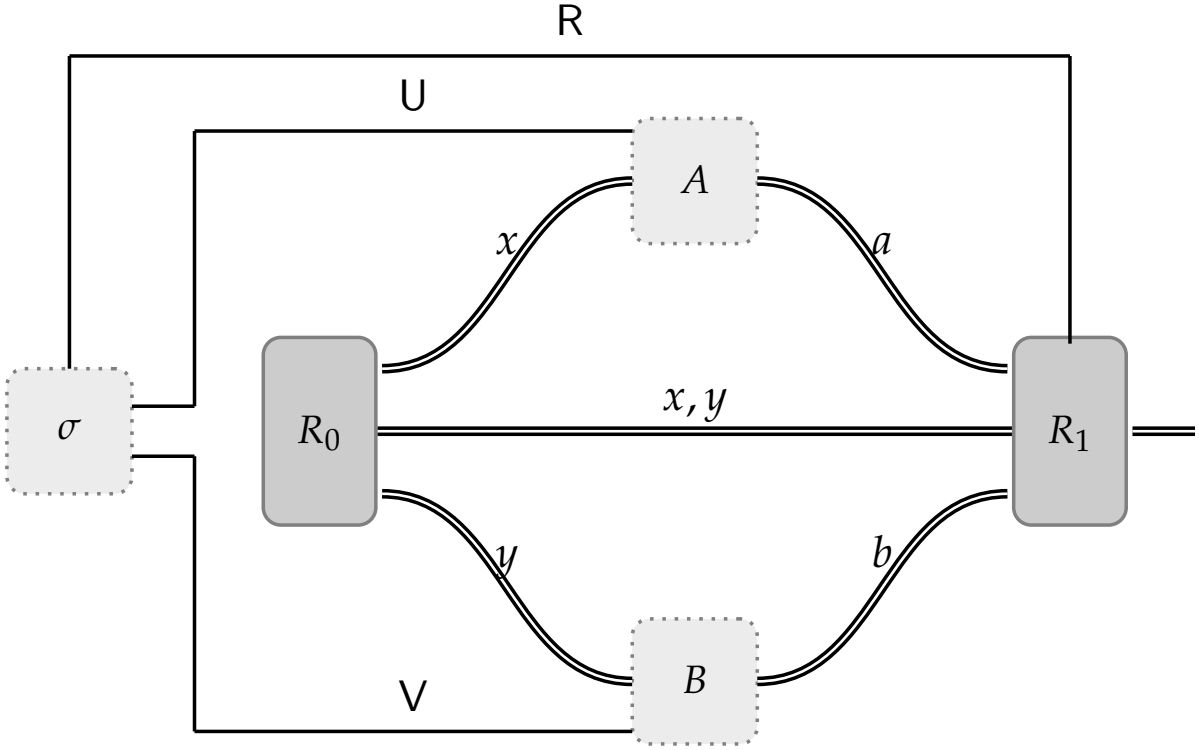
An *extended nonlocal game* (ENLG) is specified by:



- A probability distribution $\pi : X \times Y \to [0,1]$ for alphabets X and Y.
- A collection of measurement operators $\{P_{a,b,x,y} : a \in A,\ b \in B,\ x \in X,\ y \in Y\} \subset \mathrm{Pos}(\mathcal{R})$ where $\mathcal{R}$ is the space corresponding to R and A, B are alphabets.

Extended nonlocal games

An (ENLG) is played in the following manner:



1. Alice and Bob present referee with register R.
2. Referee generates $(x, y) \in X \times Y$ according to π and sends x to Alice and y to Bob. Alice responds with a and Bob with b.
3. Referee measures R w.r.t. measurement $\{P_{a,b,x,y}, \mathbb{1} - P_{a,b,x,y}\}$. Outcome is either *loss* or *win*.

Strategies for extended nonlocal games

One may consider *strategies* for Alice and Bob in an ENLG[1]:

- *Standard quantum strategies*:
  - $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$.
  - $\{A_a^x : a \in A\} \subset \mathrm{Pos}(\mathcal{U})$ and $\{B_b^y : b \in B\} \subset \mathrm{Pos}(\mathcal{V})$.
- *Unentangled strategies*: Standard quantum strategy where:
  - σ is separable.
- *Commuting measurement strategies*: Standard quantum strategy where:
  - $\sigma \in \mathrm{D}(\mathcal{R} \otimes \mathcal{H})$,
  - $[A_a^x, B_b^y] = 0$ for all x, y, a, b.
- *Non-signaling strategies*:
  - Satisfies non-signaling constraints.

[1] Chapter 3: "Extended nonlocal games".

Values of extended nonlocal games

The *value* of an ENLG, G, is the maximal winning probability for the players to win over all strategies of a specified type:[2]

- *Unentangled*: $\omega(G)$,
- *Standard quantum*: $\omega^*(G)$,
- *Commuting measurement*: $\omega_{\mathsf{c}}(G)$,
- *Non-signaling*: $\omega_{\mathsf{ns}}(G)$.

The values obey the following relationship:

$$0 \leq \omega(G) \leq \omega^*(G) \leq \omega_{\mathsf{c}}(G) \leq \omega_{\mathsf{ns}}(G) \leq 1.$$

[2] Chapter 3: "Extended nonlocal games".

Finite-dimensional standard quantum strategies

Finite-dimensional standard quantum strategies

$\omega_N^*(G)$: The standard quantum value of G when Alice and Bob use a state σ such that $\dim(\mathcal{U} \otimes \mathcal{V}) = N$:

[3] Chapter 4: "On the properties of the extended nonlocal game model".

[4] Regev, Vidick: "Quantum XOR games".

Finite-dimensional standard quantum strategies

$\omega_N^*(G)$: The standard quantum value of G when Alice and Bob use a state σ such that $\dim(\mathcal{U} \otimes \mathcal{V}) = N$:

Since $\omega^*(G)$ is over *all* standard quantum strategies (irrespective of dimension on σ):

$$\omega^*(G) = \lim_{N \to \infty} \omega_N^*(G).$$

[3] Chapter 4: "On the properties of the extended nonlocal game model".

[4] Regev, Vidick: "Quantum XOR games".

Finite-dimensional standard quantum strategies

$\omega_N^*(G)$: The standard quantum value of G when Alice and Bob use a state σ such that $\dim(\mathcal{U} \otimes \mathcal{V}) = N$:

Since $\omega^*(G)$ is over *all* standard quantum strategies (irrespective of dimension on σ):

$$\omega^*(G) = \lim_{N \to \infty} \omega_N^*(G).$$

Result:[3] There exists an ENLG, G, such that $\omega^*(G) = 1$ and $\omega_N^*(G) < 1$ when N is finite.

- Proof is inspired by the class of "quantum XOR games" as introduced by Regev and Vidick.[4]
- Implies the existence of a tripartite steering inequality for which an infinite-dimensional state is required to achieve maximal violation.

[3] Chapter 4: "On the properties of the extended nonlocal game model".

[4] Regev, Vidick: "Quantum XOR games".

Bounding the values of extended nonlocal games

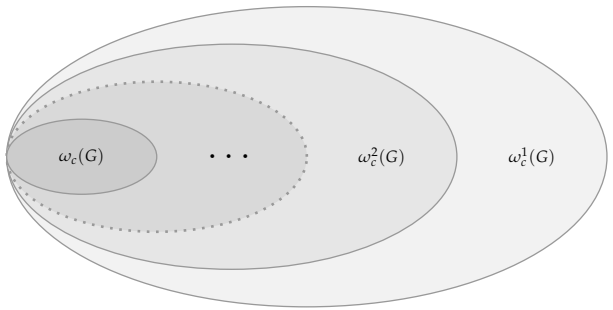
Calculating values of extended nonlocal games

One may either directly calculate or bound the value of extended nonlocal games:

- $\omega(G)$: A closed form expression exists that allows one to directly calculate this value.
- $\omega_{\mathsf{ns}}(G)$: May be phrased as an semidefinite program.

Calculating the standard quantum values of extended nonlocal games

- The *extended QC hierarchy*: extension of the QC hierarchy[5,6] that may be used to upper bound the standard quantum value for ENLGs.[7]



- $\omega^*(G)$: Extended QC hierarchy to upper bound. May also adapt "see-saw" method[8] for lower bounds.
- $\omega_c(G)$: Extended QC hierarchy.

[5] Doherty, Liang, Toner, Wehner: "The quantum moment problem and bounds on entangled multi-prover games", (2008).

[6] Navascues, Pironio, Acin: "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations", (2008).

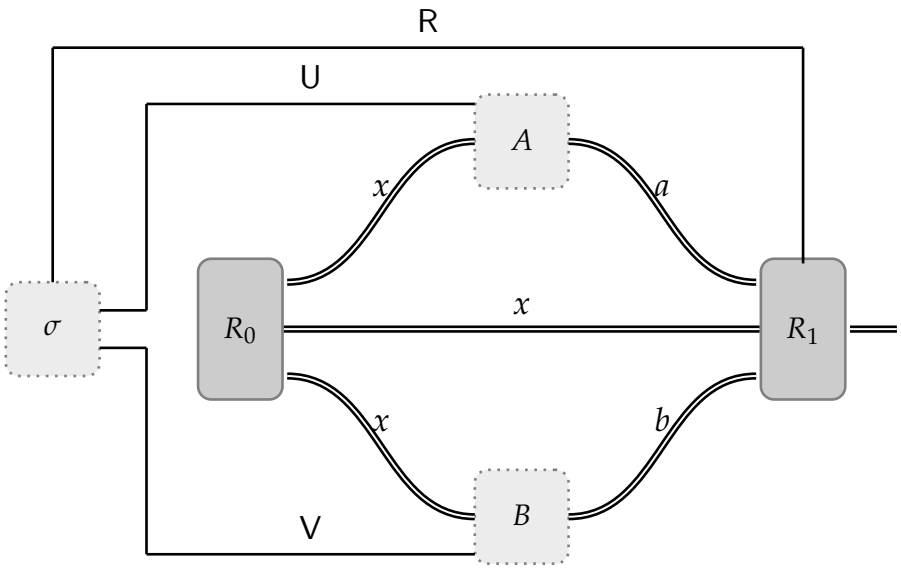
[7] Chapter 5: "Bounding the standard quantum value of extended nonlocal games."

[8] Liang, Doherty: "Bounds on Quantum Correlations in Bell Inequality Experiments", (2007).

Monogamy-of-Entanglement games

Monogamy-of-entanglement games

Monogamy-of-entanglement games[9], are a special type of extended nonlocal game.



1. Same question and answer sets: X and A.
2. Alice and Bob get the same question: $\pi(x, y) = 0$ for $x \neq y$.
3. Referee's measurement operator: $P : A \times X \to \mathrm{Pos}(\mathcal{R})$.
4. Winning condition: Iff Alice's output, Bob's output, and the referee's output are all the *equal*.

[9] Tomamichel, Fehr, Kaniewski, Wehner : "A Monogamy-of-Entanglement Game With Applications to Device-Independent Quantum Cryptography", (2013).

Parallel repetition of monogamy-of-entanglement games

- The following statements were proved in:[10]

$$\omega(G_{\mathrm{BB84}}) = \omega^*(G_{\mathrm{BB84}}) = \cos^2(\pi/8) \approx 0.8536.$$

- G_{BB84} obeys strong parallel repetition:

$$\omega^*(G_{\mathrm{BB84}}^n) = \omega^*(G_{\mathrm{BB84}})^n = \left(\cos^2(\pi/8)\right)^n.$$

[10] Tomamichel, Fehr, Kaniewski, Wehner : "A Monogamy-of-Entanglement Game With Applications to Device-Independent Quantum Cryptography", (2013).

Further properties of monogamy-of-entanglement games

General properties about monogamy-of-entanglement games:[11]

- For any monogamy-of-entanglement game, G, for which $|X| = 2$:

$$\omega(G) = \omega^*(G).$$

[11] Johnston, Mittal, R., Watrous: "Extended nonlocal games and monogamy-of-entanglement games", (2015).

Further properties of monogamy-of-entanglement games

General properties about monogamy-of-entanglement games:[11]

- For any monogamy-of-entanglement game, G, for which $|X| = 2$:

$$\omega(G) = \omega^*(G).$$

- There exists a monogamy-of-entanglement game, G, with $|X| = 4$ and $|A| = 3$ such that:

$$\omega(G) < \omega^*(G).$$

[11] Johnston, Mittal, R., Watrous: "Extended nonlocal games and monogamy-of-entanglement games", (2015).

Parallel repetition of monogamy-of-entanglement games

Parallel repetition of monogamy-of-entanglement games:[12]

- Let $G = (\pi, P)$ be a monogamy game where $|X| = 2$, π is uniform over X, and $P_{a,x}$ are projective operators. It holds that for all n:

$$\omega^*(G^n) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n,$$

where $c(G)$ is the maximal overlap of the referee's measurements:

$$c(G) = \max_{\substack{x,y \in X \\ x \neq y}} \max_{a,b \in A} \left\| \sqrt{P_{a,x}} \sqrt{P_{b,y}} \right\|^2.$$

[12] Johnston, Mittal, R., Watrous: "Extended nonlocal games and monogamy-of-entanglement games", (2015).

Parallel repetition of monogamy-of-entanglement games

Parallel repetition of monogamy-of-entanglement games:[12]

- Let $G = (\pi, P)$ be a monogamy game where $|X| = 2$, π is uniform over X, and $P_{a,x}$ are projective operators. It holds that for all n:

$$\omega^*(G^n) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n,$$

where $c(G)$ is the maximal overlap of the referee's measurements:

$$c(G) = \max_{\substack{x,y \in X \\ x \neq y}} \max_{a,b \in A} \left\| \sqrt{P_{a,x}} \sqrt{P_{b,y}} \right\|^2.$$

- There exists a monogamy-of-entanglement game, G, such that

$$\omega_{\mathrm{ns}}(G^2) \neq \omega_{\mathrm{ns}}(G)^2.$$

[12] Johnston, Mittal, R., Watrous: "Extended nonlocal games and monogamy-of-entanglement games", (2015).

Thanks!

Thank you for your attention!

Acknowledgments

Supervisors	Michele Mosca, John Watrous
Committee members	Richard Cleve Michele Mosca Vern Paulsen John Watrous
Co-authors	Nathaniel Johnston Rajat Mittal John Watrous
Funded by	NSERC US Army Research Office David R. Cheriton Scholarship

Publications

Directly related to the content in this presentation:

- V. R., J. Watrous. **Extended nonlocal games from quantum-classical games**. *In progress...*, 2017.
- N. Johnston, R. Mittal, V. R., J. Watrous. **Extended nonlocal games and monogamy-of-entanglement games**. *Proc. R. Soc. A 472:20160003*, 2016.

Completed during my Ph.D., but not directly related to my thesis work:

- S. Bandyopadhyay, A. Cosentino, N. Johnston, V. R., J. Watrous, and N. Yu. **Limitations on separable measurements by convex optimization**. *IEEE Transactions on Information Theory*, 2015.
- S. Arunachalam, N. Johnston, V. R. **Is absolute separability determined by the partial transpose?**. *Quantum Information & Computation*, 2015.
- D. Gosset, V. Kliuchinikov, M. Mosca, V. R. **An algorithm for the T-count**. *Quantum Information & Computation*, 2014.
- A. Cosentino and V. R. **Small sets of locally indistinguishable orthogonal maximally entangled states**. *Quantum Information & Computation*, 2014.
- S. Arunachalam, A. Molina, V. R. **Quantum hedging in two-round prover-verifier interactions**. *arXiv:1310.7954*, 2013.

Supplementary material

Supplementary material: Extended nonlocal games

Extended nonlocal games: Winning and losing probabilities

At the end of the protocol, the referee has:

1. The state at the end of the protocol:

$$\sigma_{a,b}^{x,y} \in \mathrm{D}(\mathcal{R}).$$

2. A measurement the referee makes on its part of the state σ:

$$P_{a,b,x,y} \in \mathrm{Pos}(\mathcal{R}).$$

The respective winning and losing probabilities are given by:

$$\left\langle P_{a,b,x,y}, \sigma_{a,b}^{x,y} \right\rangle \quad \text{and} \quad \left\langle \mathbb{1} - P_{a,b,x,y}, \sigma_{a,b}^{x,y} \right\rangle.$$

Assemblages

When analyzing a strategy for Alice and Bob, it may be convenient to define a function:

$$K : A \times B \times X \times Y \to \mathrm{Pos}(\mathcal{R}).$$

We refer to K as an *assemblage*.

Assemblages

When analyzing a strategy for Alice and Bob, it may be convenient to define a function:

$$K : A \times B \times X \times Y \to \mathrm{Pos}(\mathcal{R}).$$

We refer to K as an *assemblage*.

The assemblage K represents unnormalized states of the referee's system. We can normalize to obtain:

$$\sigma_{a,b}^{x,y} = \frac{K(a,b|x,y)}{\mathrm{Tr}(K(a,b|x,y)}.$$

Assemblages

When analyzing a strategy for Alice and Bob, it may be convenient to define a function:

$$K : A \times B \times X \times Y \to \mathrm{Pos}(\mathcal{R}).$$

We refer to K as an *assemblage*.

The assemblage K represents unnormalized states of the referee's system. We can normalize to obtain:

$$\sigma_{a,b}^{x,y} = \frac{K(a,b|x,y)}{\mathrm{Tr}(K(a,b|x,y)}.$$

The function K encodes the probability that Alice and Bob obtain answers a and b given questions x and y. The winning probability can then be represented as

$$\sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle P_{a,b,x,y}, K(a,b|x,y)) \right\rangle.$$

Standard quantum strategies for ENLGs

A *standard quantum strategy* consists of complex Euclidean spaces $\mathcal{R}$,$\mathcal{U}$, and $\mathcal{V}$ as well as

- Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$,
- Measurements: $\{A_a^x\} \subset \mathrm{Pos}(\mathcal{U}),\ \{B_b^y\} \subset \mathrm{Pos}(\mathcal{V})$.

Standard quantum strategies for ENLGs

A *standard quantum strategy* consists of complex Euclidean spaces $\mathcal{R}$,$\mathcal{U}$, and $\mathcal{V}$ as well as

- Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$,
- Measurements: $\{A_a^x\} \subset \mathrm{Pos}(\mathcal{U}),\ \{B_b^y\} \subset \mathrm{Pos}(\mathcal{V})$.

Winning probability for a standard quantum strategy is given by:

$$\sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \pi(x,y)\left\langle A_a^x \otimes P_{a,b,x,y} \otimes B_b^y, \sigma \right\rangle.$$

Standard quantum strategies for ENLGs

A *standard quantum strategy* consists of complex Euclidean spaces $\mathcal{R}, \mathcal{U}$, and $\mathcal{V}$ as well as

- Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$,
- Measurements: $\{A_a^x\} \subset \mathrm{Pos}(\mathcal{U}),\ \{B_b^y\} \subset \mathrm{Pos}(\mathcal{V})$.

Winning probability for a standard quantum strategy is given by:

$$\sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \pi(x,y) \left\langle A_a^x \otimes P_{a,b,x,y} \otimes B_b^y, \sigma \right\rangle.$$

Equivalently, the winning probability for such a strategy is given by

$$\sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle P_{a,b,x,y}, K(a,b|x,y) \right\rangle,$$

where

$$K(a,b|x,y) = \mathrm{Tr}_{\mathcal{U}\otimes\mathcal{V}} \left((A_a^x \otimes \mathbb{1}_{\mathcal{R}} \otimes B_b^y)\sigma \right).$$

Standard quantum values for ENLGs

$\omega^*(G)$: Standard quantum value of an ENLG, G:

- Supremum winning probability of G over *all* standard quantum strategies.

[13] R., Watrous : Extended nonlocal games from quantum-classical games (2017).

Standard quantum values for ENLGs

$\omega^*(G)$: Standard quantum value of an ENLG, G:

- Supremum winning probability of G over *all* standard quantum strategies.

Note: Supremum is *not* always achieved for $\omega^*(G)$ since the $\dim(\mathcal{U})$ and $\dim(\mathcal{V})$ is not a priori bounded.

- There exists a sequence of strategies where as the dimension increases, the probabilities converge to, but never reach, its standard quantum value.[13]

[13] R., Watrous : Extended nonlocal games from quantum-classical games (2017).

Standard quantum values for ENLGs

$\omega^*(G)$: Standard quantum value of an ENLG, G:

- Supremum winning probability of G over *all* standard quantum strategies.

Note: Supremum is *not* always achieved for $\omega^*(G)$ since the $\dim(\mathcal{U})$ and $\dim(\mathcal{V})$ is not a priori bounded.

- There exists a sequence of strategies where as the dimension increases, the probabilities converge to, but never reach, its standard quantum value.[13]

Note: Not known if supremum is always achieved for $\omega^*(G)$ where G is a nonlocal game.

[13] R., Watrous : Extended nonlocal games from quantum-classical games (2017).

Unentangled strategies

In an *unentangled strategy*, the state σ prepared by Alice and Bob is *fully separable*, that is,

$$\{\sigma_j^{\mathsf{U}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{U}), \quad \{\sigma_j^{\mathsf{R}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{R}), \quad \{\sigma_j^{\mathsf{V}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{V}),$$

such that

$$\sigma = \sum_{j \in \Delta} p(j) \sigma_j^{\mathsf{U}} \otimes \sigma_j^{\mathsf{R}} \otimes \sigma_j^{\mathsf{V}}.$$

Unentangled strategies

In an *unentangled strategy*, the state σ prepared by Alice and Bob is *fully separable*, that is,

$$\{\sigma_j^{\mathsf{U}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{U}), \quad \{\sigma_j^{\mathsf{R}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{R}), \quad \{\sigma_j^{\mathsf{V}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{V}),$$

such that

$$\sigma = \sum_{j \in \Delta} p(j) \sigma_j^{\mathsf{U}} \otimes \sigma_j^{\mathsf{R}} \otimes \sigma_j^{\mathsf{V}}.$$

Winning probability for an unentangled strategy is given by:

$$\sum_{(x,y) \in X \times Y} \pi(x,y) \sum_{(a,b) \in A \times B} \left\langle A_a^x \otimes P_{a,b,x,y} \otimes B_b^y, \sigma \right\rangle$$

where σ is separable.

Unentangled value

The *unentangled value*, denoted as $\omega(G)$, is the supremum of the winning probability over all unentangled strategies.

Unentangled value

The *unentangled value*, denoted as $\omega(G)$, is the supremum of the winning probability over all unentangled strategies.

For an unentangled strategy, we have that the referee, Alice, and Bob share

$$\sigma = \sum_{j \in \Delta} p(j) \sigma_j^{\mathsf{U}} \otimes \sigma_j^{\mathsf{R}} \otimes \sigma_j^{\mathsf{V}}.$$

- For $\omega(G)$, we want the *best* Alice and Bob can do.
- Since σ is separable (no quantum correlations) pick *best* j:

$$\sigma = \sigma^{\mathsf{U}} \otimes \sigma^{\mathsf{R}} \otimes \sigma^{\mathsf{V}}.$$

Unentangled value

In an unentangled strategy, Alice and Bob provide the referee with a pure state $\sigma \in \mathrm{D}(\mathcal{R})$ and Alice responds to question x with $a = f(x)$ and Bob responds to y with $b = f(y)$ for some deterministic functions mapping from the input to output sets.

The *unentangled value*, denoted as $\omega(G)$, is written as

$$\omega(G) = \max_{f,g} \left\| \sum_{x,y} \pi(x,y) P_{f(x),g(y),x,y} \right\|,$$

where the maximum is over all functions

$$f : X \to A \quad \text{and} \quad g : Y \to B.$$

Commuting measurement strategies

A *commuting measurement strategy* consists of a complex Euclidean space $\mathcal{R}$ and a (possibly) infinite-dimensional Hilbert space $\mathcal{H}$ as well as

- Shared state: $\sigma \in \mathrm{D}(\mathcal{R} \otimes \mathcal{H})$,
- Measurements $\{A_a^x\} \subset \mathrm{Pos}(\mathcal{H})$, $\{B_b^y\} \subset \mathrm{Pos}(\mathcal{H})$ such that

$$\left[A_a^x, B_b^y\right] = 0$$

  for all $x \in X$, $y \in Y$, $a \in A$, and $b \in B$.

Commuting measurement strategies

Winning probability for a commuting measurement strategy is given by

$$\sum_{\substack{(x,y)\in X\times Y\\(a,b)\in A\times B}} \left\langle P_{a,b,x,y} \otimes A_a^x B_b^y, \sigma \right\rangle.$$

Equivalently, the winning probability for such a strategy is given by

$$\sum_{\substack{(x,y)\in X\times Y\\(a,b)\in A\times B}} \left\langle P_{a,b,x,y}, K(a,b|x,y) \right\rangle,$$

where

$$K(a,b|x,y) = \mathrm{Tr}_{\mathcal{H}}\left(\mathbb{1}_{\mathcal{R}} \otimes (A_a^x B_b^y)\sigma\right),$$

is a commuting measurement assemblage.

Commuting measurement values for ENLGs

$\omega_c(G)$: Commuting measurement value of an ENLG, G:

- Supremum winning probability of G over *all* commuting measurement strategies.

Commuting measurement values for ENLGs

$\omega_c(G)$: Commuting measurement value of an ENLG, G:

- Supremum winning probability of G over *all* commuting measurement strategies.

Note: Supremum is achieved.

Non-signaling strategies

A *non-signaling strategy* consists of a non-signaling assemblage

$$K : A \times B \times X \times Y \to \mathrm{Pos}(R)$$

such that

$$\sum_{a \in A} K(a, b|x, y) = \xi_b^y \quad \text{and} \quad \sum_{b \in B} K(a, b|x, y) = \rho_a^x,$$

for all $x \in X$ and $y \in Y$ where

$$\sum_{a \in A} \rho_a^x = \tau = \sum_{b \in B} \xi_b^y,$$

where $\tau \in \mathrm{D}(\mathcal{R})$.

Non-signaling strategies

A *non-signaling strategy* consists of a non-signaling assemblage

$$K : A \times B \times X \times Y \to \mathrm{Pos}(R)$$

such that

$$\sum_{a \in A} K(a, b|x, y) = \xi_b^y \quad \text{and} \quad \sum_{b \in B} K(a, b|x, y) = \rho_a^x,$$

for all $x \in X$ and $y \in Y$ where

$$\sum_{a \in A} \rho_a^x = \tau = \sum_{b \in B} \xi_b^y,$$

where $\tau \in \mathrm{D}(\mathcal{R})$.

The winning probability for a non-signaling strategy is given by

$$\sum_{\substack{(x,y) \in X \times Y \\ (a,b) \in A \times B}} \left\langle P_{a,b,x,y}, K(a, b|x, y) \right\rangle,$$

where K is a non-signaling assemblage.

Non-signaling values for ENLGs

$\omega_{\mathsf{ns}}(G)$: Non-signaling value of an ENLG, G:

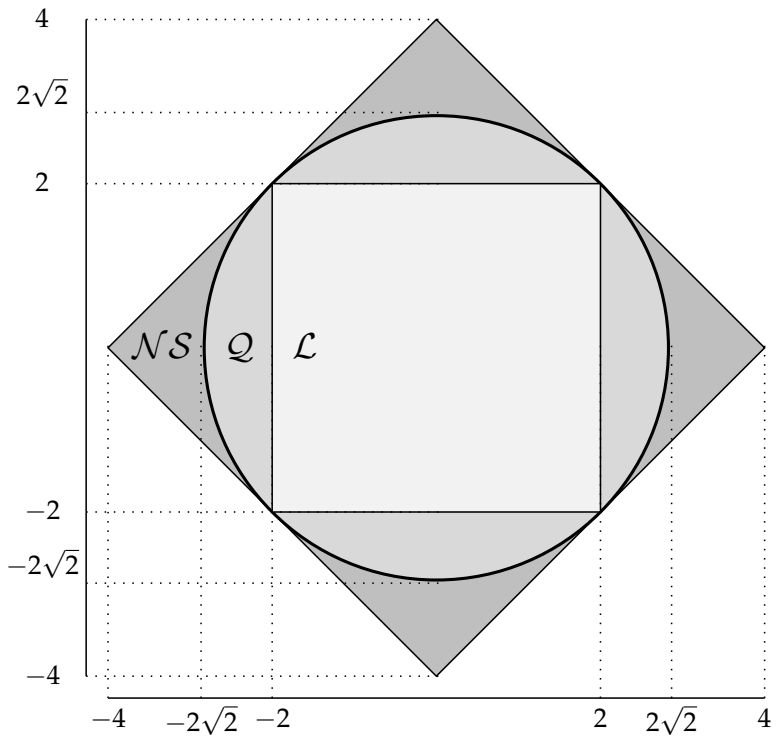
- Supremum winning probability of G over *all* non-signaling strategies.

Non-signaling values for ENLGs

$\omega_{\mathsf{ns}}(G)$: Non-signaling value of an ENLG, G:

- Supremum winning probability of G over *all* non-signaling strategies.

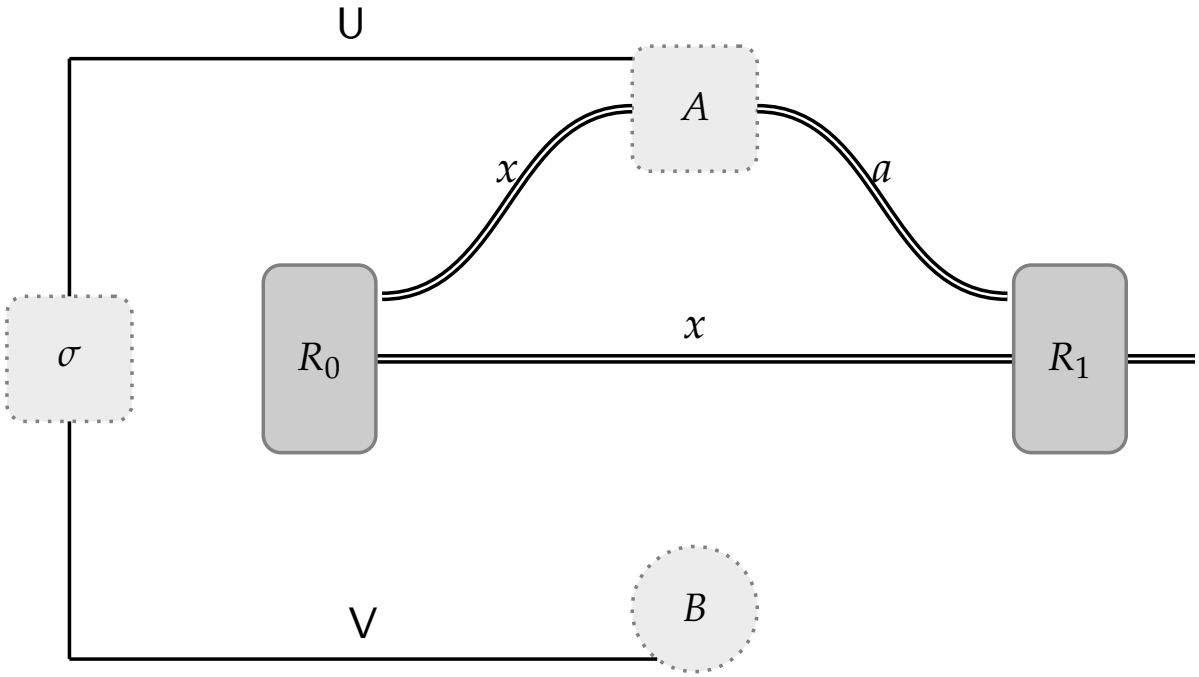
Note: Supremum is achieved since the set of non-signaling assemblages is compact and therefore closed and bounded, which implies that the supremum is achieved.



Supplementary material:
Steering and extended nonlocal games

Bipartite steering

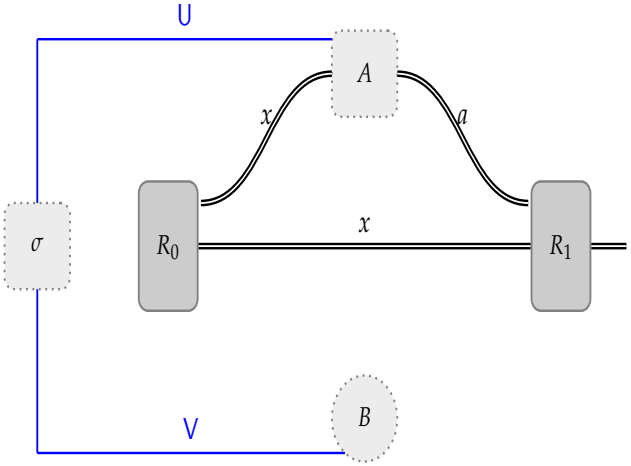
Alice and Bob each receive part of a quantum state (sent by the referee). Their goal is to determine whether this state is entangled.



- Bob's measurement device is "trusted", whereas Alice's is not:
  - Outcome of Alice's measurements are only ± 1 (a conclusive outcome) or 0 (a non-conclusive outcome).
- To demonstrate entanglement, Alice needs to "steer" Bob's state by her choice of measurement.

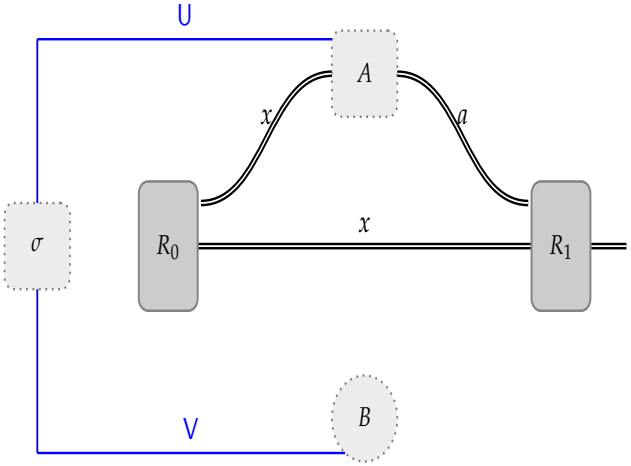
NLGs, ENLGs, and steering

Bipartite steering with one untrusted party:

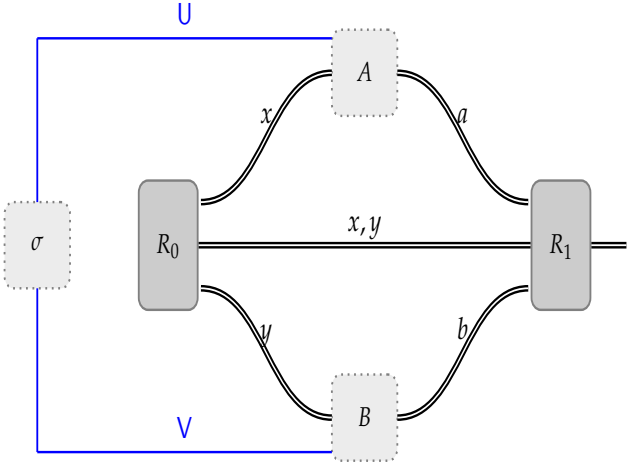


NLGs, ENLGs, and steering

Bipartite steering with one untrusted party:

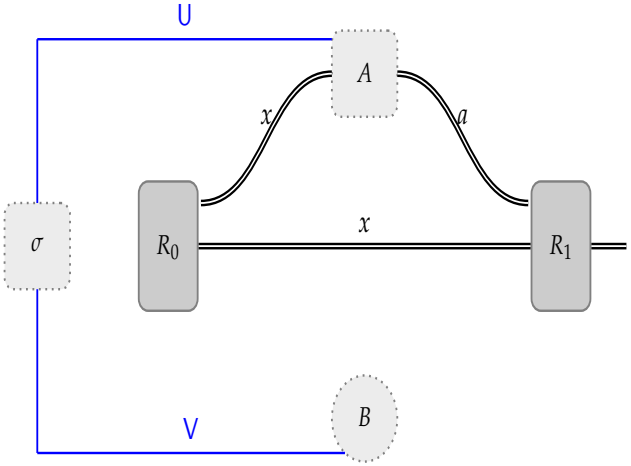


Bipartite steering with two untrusted parties (NLG):

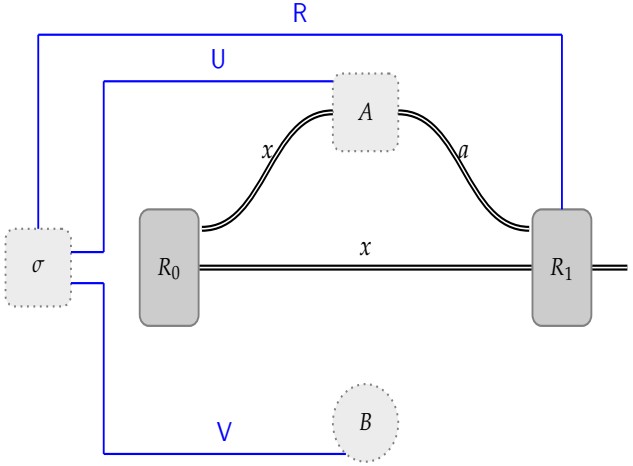


NLGs, ENLGs, and steering

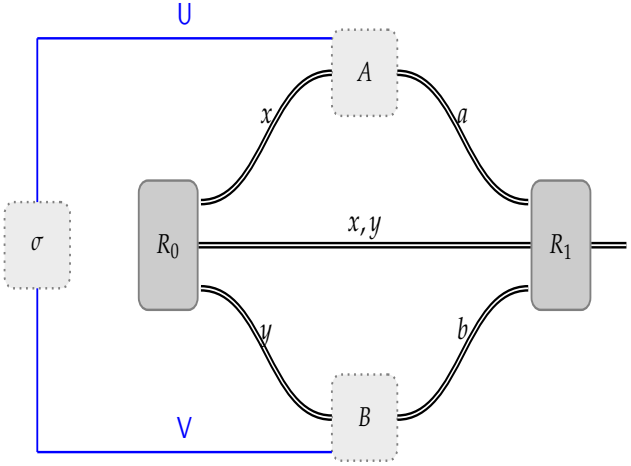
Bipartite steering with one untrusted party:



Tripartite steering with one untrusted party:

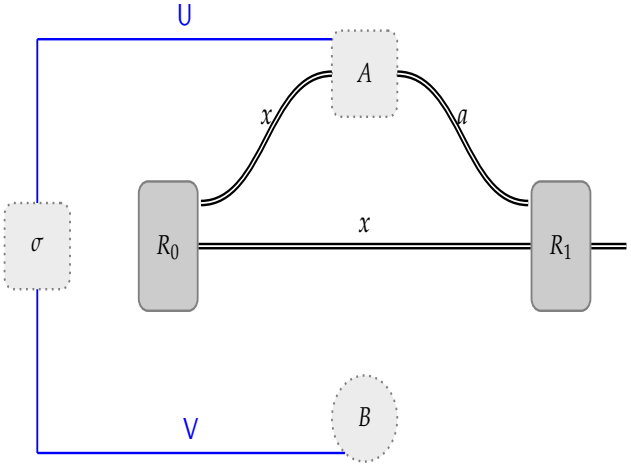


Bipartite steering with two untrusted parties (NLG):

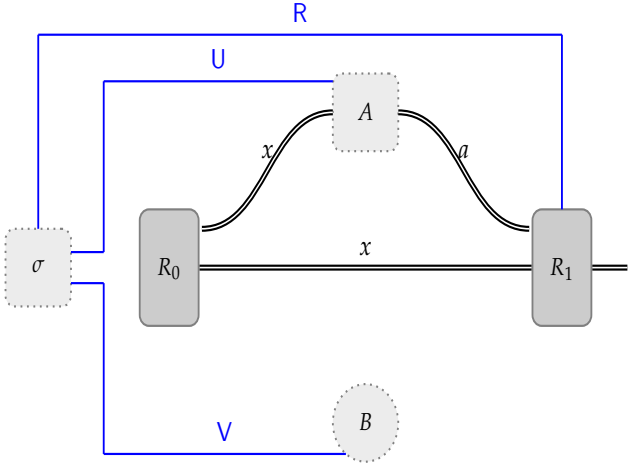


NLGs, ENLGs, and steering

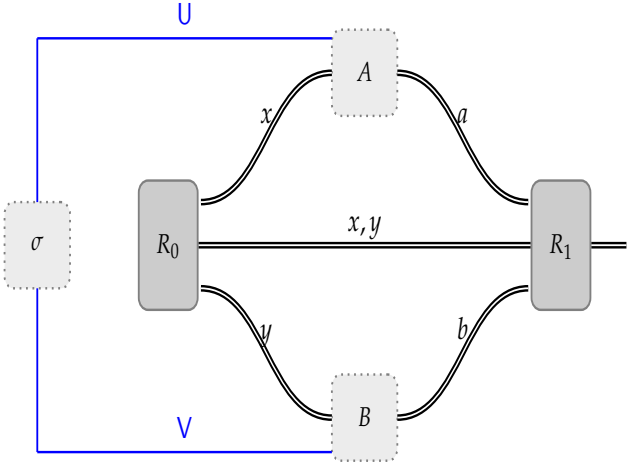
Bipartite steering with one untrusted party:



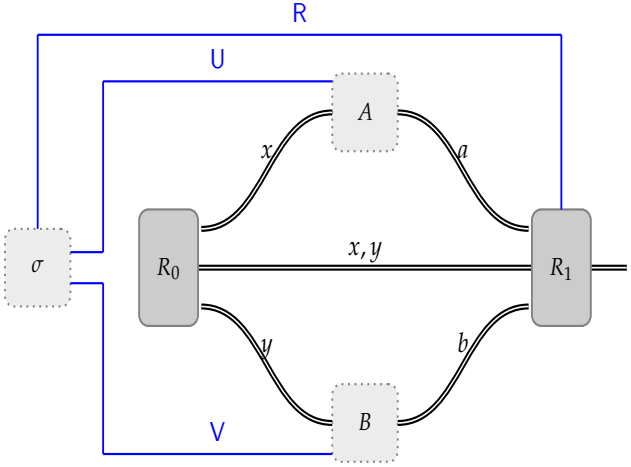
Tripartite steering with one untrusted party:



Bipartite steering with two untrusted parties (NLG):



Tripartite steering with two untrusted parties (ENLG):



ENLG and steering

Tripartite steering: same thing as before, only now we have three parties where two members are untrusted and one member is trusted.

ENLG and steering

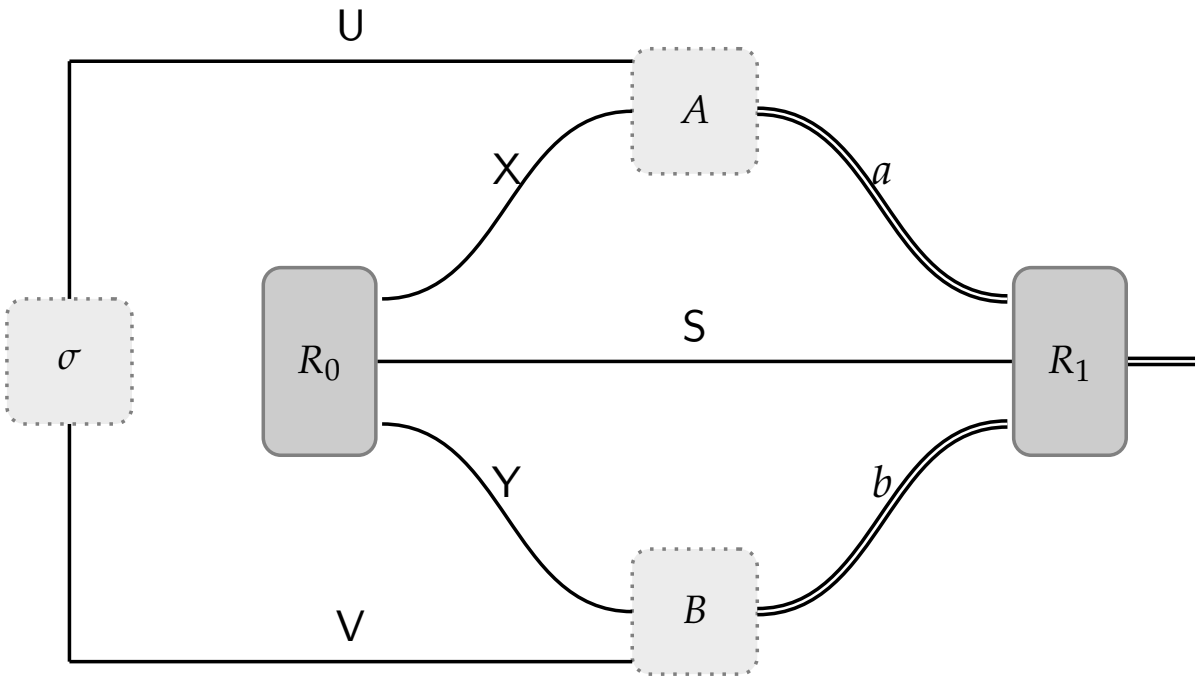
Tripartite steering: same thing as before, only now we have three parties where two members are untrusted and one member is trusted.

In tripartite steering, Alice and Bob are the untrusted parties, and the referee is the trusted party.

Supplementary material:
Finite-dimensional standard quantum strategies

Quantum-classical games

A *quantum-classical game* (QCG) is a cooperative game played between *Alice* and *Bob* against a *referee*.

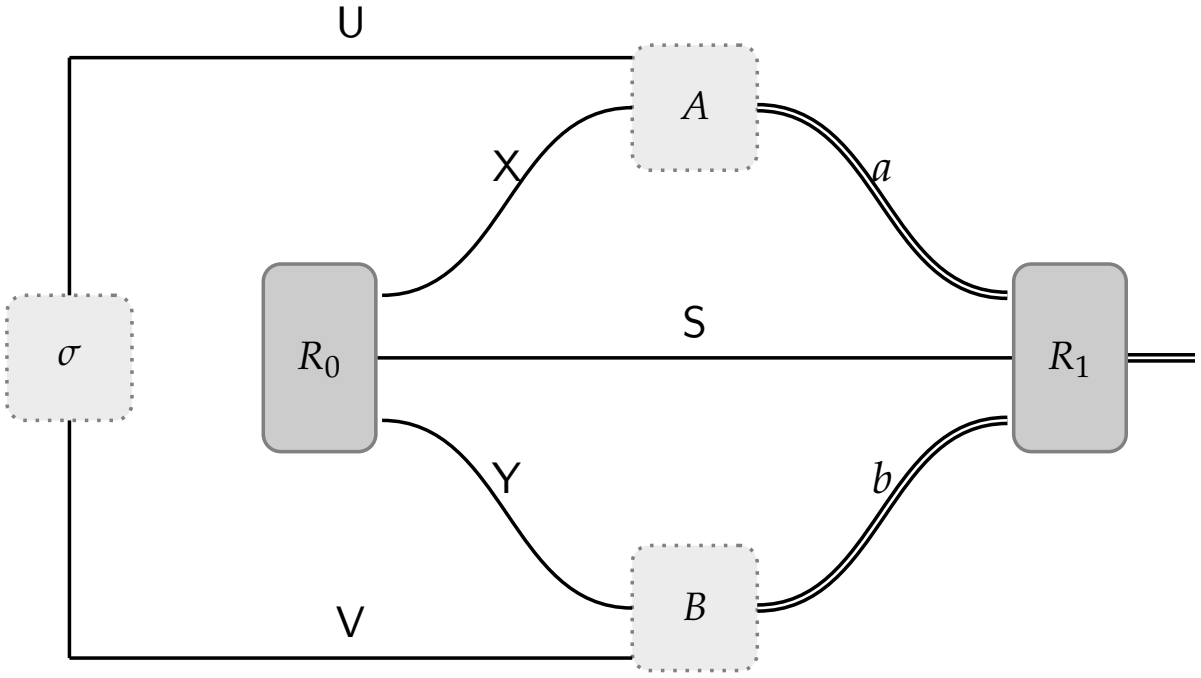


Specified by:

- A *state* $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{S} \otimes \mathcal{Y})$ in registers $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$.
- Collection of *measurement operators* $\{Q_{a,b} : a \in A,\ b \in B\} \subset \mathrm{Pos}(\mathcal{S})$ for alphabets A and B.

Quantum-classical games

A (QCG) is played in the following manner.



1. Referee prepares $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$ in state ρ and sends X to Alice and Y to Bob.
2. Alice responds with $a \in A$ and Bob with $b \in B$.
3. Referee measures S w.r.t. measurement $\{Q_{a,b}, \mathbb{1} - Q_{a,b}\}$. The outcome of this measurement results in "0" or "1", indicating a *loss* or a *win*.

Entangled strategies for QCGs

For a QCG, an *entangled strategy* consists of complex Euclidean spaces $\mathcal{U}$ and $\mathcal{V}$ as well as

- Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{V})$,
- Measurements: $\{A_a : a \in A\} \subset \mathrm{Pos}(\mathcal{U} \otimes \mathcal{X}), \{B_b : b \in B\} \subset \mathrm{Pos}(\mathcal{V} \otimes \mathcal{Y})$.

Entangled strategies for QCGs

For a QCG, an *entangled strategy* consists of complex Euclidean spaces $\mathcal{U}$ and $\mathcal{V}$ as well as

- Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{V})$,
- Measurements: $\{A_a : a \in A\} \subset \mathrm{Pos}(\mathcal{U} \otimes \mathcal{X}), \{B_b : b \in B\} \subset \mathrm{Pos}(\mathcal{V} \otimes \mathcal{Y})$.

Winning probability for a entangled strategy is given by:

$$\sum_{(a,b) \in A \times B} \left\langle A_a \otimes Q_{a,b} \otimes B_b, W\left(\sigma \otimes \rho\right) W^* \right\rangle,$$

where W is the unitary operator that corresponds to the natural re-ordering of registers consistent with the tensor product operators.

Entangled values for QCGs

For any QCG denoted as G, the *entangled value* of G, denoted as $\omega^*(G)$, represents the supremum of the winning probabilities taken over all entangled strategies.

We may also write $\omega_N^*(G)$ to denote the *maximum* winning probability taken over all entangled strategies for which $\dim(\mathcal{U} \otimes \mathcal{V}) = N$, so that the entangled value of G is

$$\omega^*(G) = \lim_{N \to \infty} \omega_N^*(G).$$

Values and the dimension of shared entanglement

Question: Does the dimensionality of the state that Alice and Bob share determine how well Alice and Bob perform?

[14] Regev, Vidick, (2012): "Quantum XOR games".

Values and the dimension of shared entanglement

Question: Does the dimensionality of the state that Alice and Bob share determine how well Alice and Bob perform?

Partial answer: Regev and Vidick showed that there exists a specific class of QCG such that if the dimension of Alice and Bob's quantum system, N, is finite then $\omega_N^*(G) < 1$, but $\omega^*(G) = 1$.[14]

[14] Regev, Vidick, (2012): "Quantum XOR games".

Values and the dimension of shared entanglement

Question: Does the dimensionality of the state that Alice and Bob share determine how well Alice and Bob perform?

Partial answer: Regev and Vidick showed that there exists a specific class of QCG such that if the dimension of Alice and Bob's quantum system, N, is finite then $\omega_N^*(G) < 1$, but $\omega^*(G) = 1$.[14]

What about ENLG?

[14] Regev, Vidick, (2012): "Quantum XOR games".

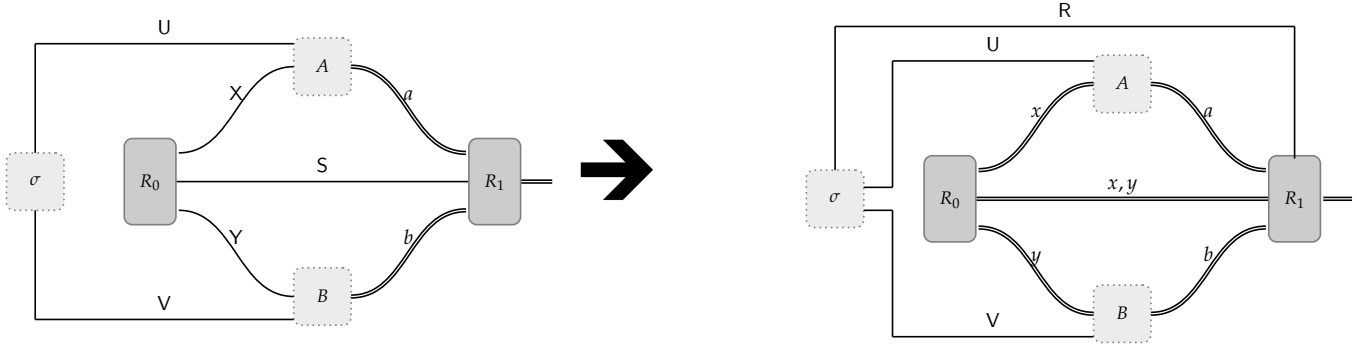
Relationship between ENLGs and QCGs

Main question: Does there also exist an ENLG, H, such that $\omega^*(H) = 1$ and $\omega^*_N(H) < 1$ when N is finite?

Relationship between ENLGs and QCGs

Main question: Does there also exist an ENLG, H, such that $\omega^*(H) = 1$ and $\omega^*_N(H) < 1$ when N is finite?

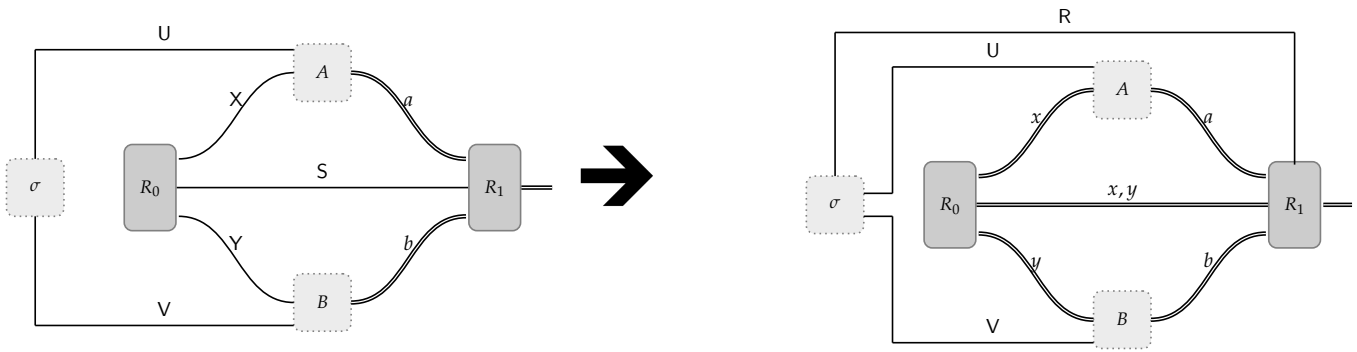
- It is possible to construct an ENLG from any QCG (not obvious).



Relationship between ENLGs and QCGs

Main question: Does there also exist an ENLG, H, such that $\omega^*(H) = 1$ and $\omega^*_N(H) < 1$ when N is finite?

- It is possible to construct an ENLG from any QCG (not obvious).



- From this construction, it turns out that this property also holds for ENLG, that is, there does exist an ENLG such that Alice and Bob can only win with certainty iff they share an infinite-dimensional state.

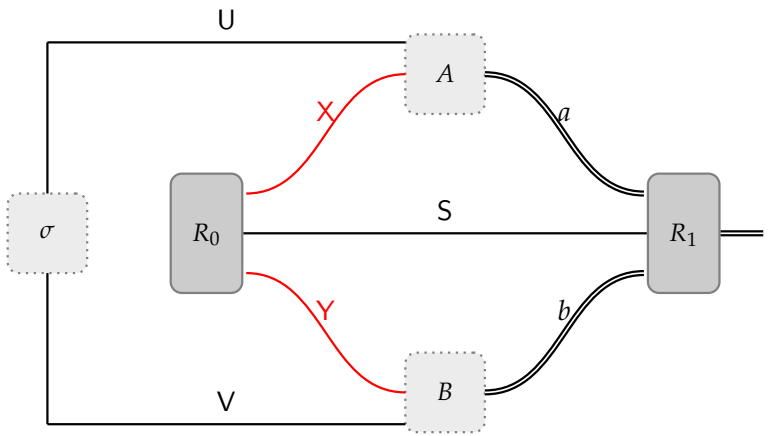
Main restriction

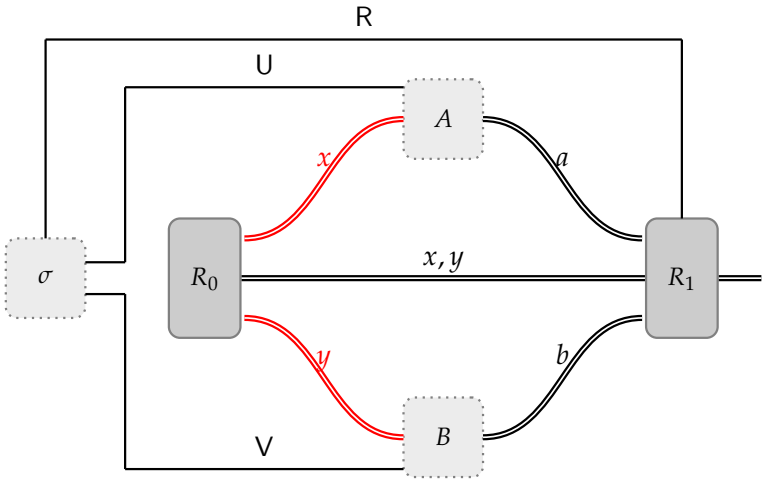
Show that for an arbitrary and fixed strategy for G, that it's possible to adapt this strategy for H.

Main restriction

Show that for an arbitrary and fixed strategy for G, that it's possible to adapt this strategy for H.

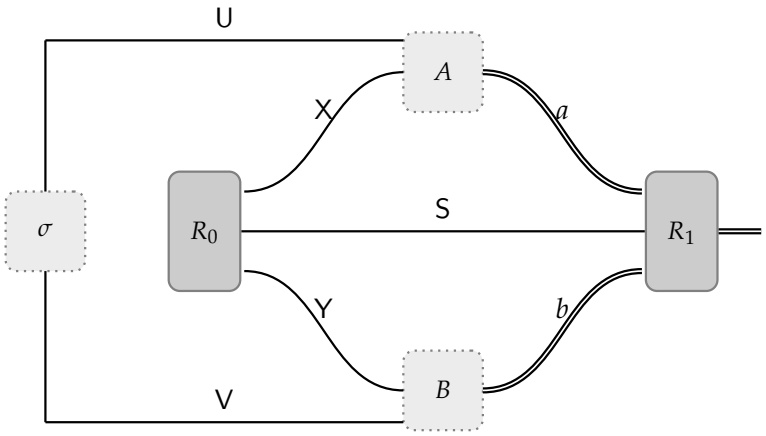
Main restriction: In G, the referee is sending quantum registers, but in H, the referee is restricted to sending classical questions.

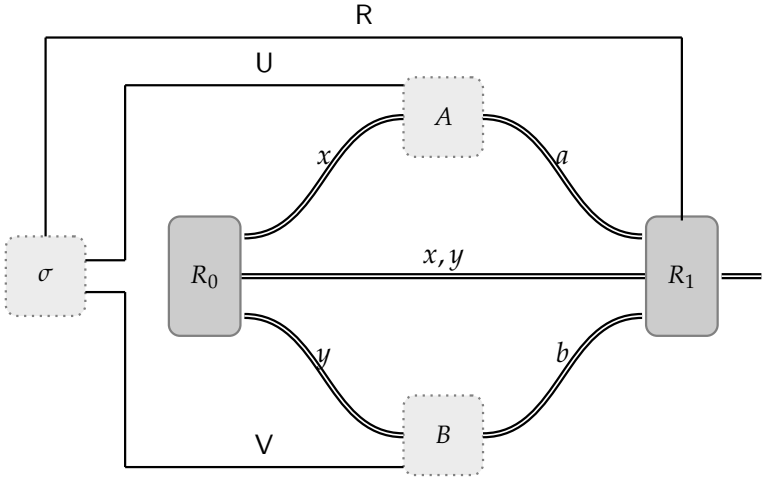




Relationship between ENLGs and QCGs

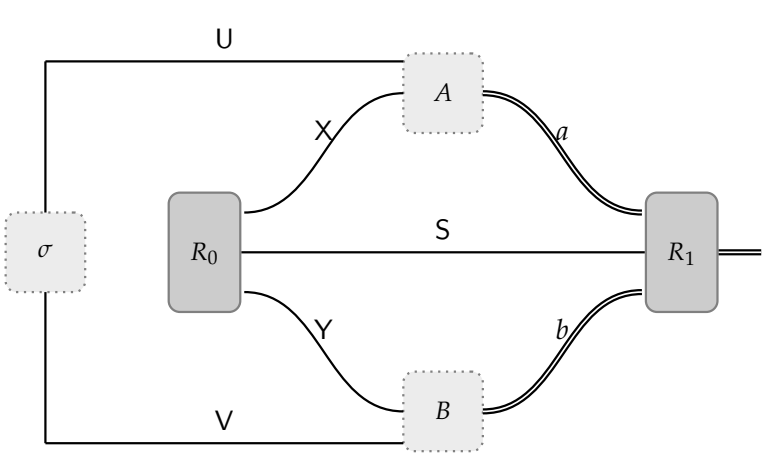
We want to establish a relationship between QCGs and ENLGs.

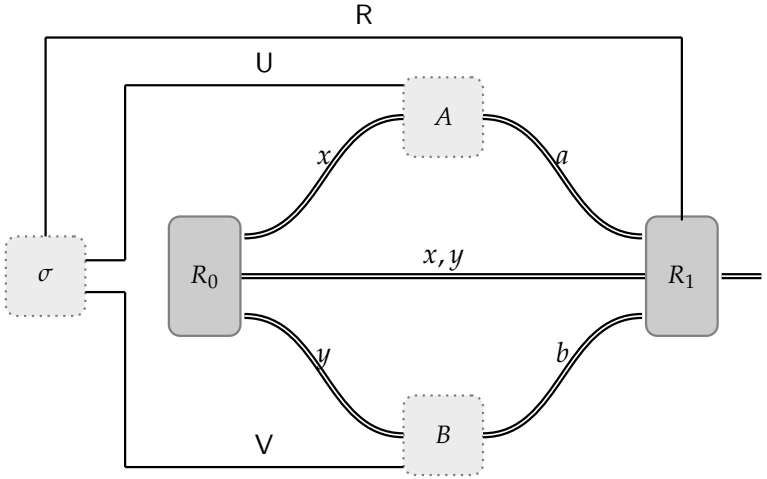




Relationship between ENLGs and QCGs

We want to establish a relationship between QCGs and ENLGs.



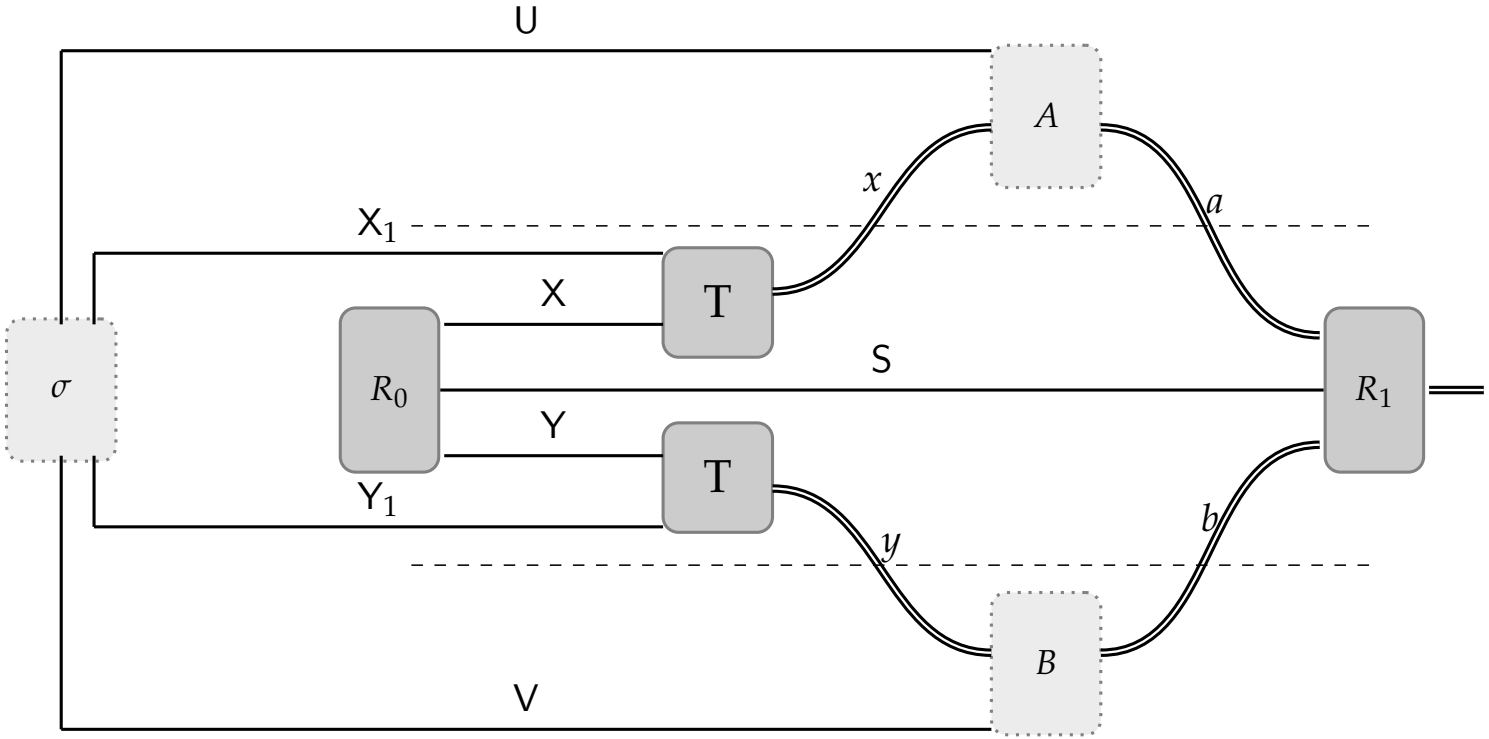


Approach:

- Show relationship between QCG and something called a "teleportation game".
- Show relationship between teleportation game and ENLG.

Teleportation games

A *teleportation game* is specified by



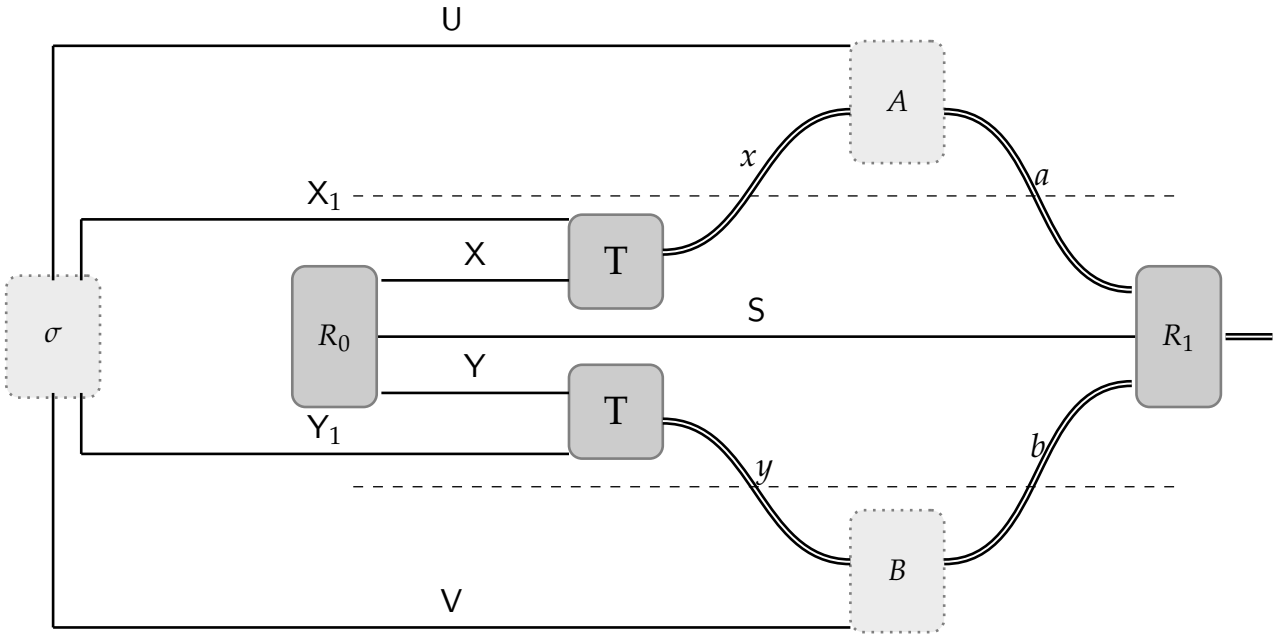
- A state $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{S} \otimes \mathcal{Y})$ in $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$.
- A collection of measurement operators

$$\{Q_{a,b} : a \in A,\ b \in B\} \subset \mathrm{Pos}(\mathcal{S}),$$

where A and B are alphabets.

Teleportation games

A teleportation game is played in the following way:



- Referee is presented with $\mathsf{R} = (\mathsf{X}_1, \mathsf{Y}_1)$ (where X_1 and Y_1 are copies of X and Y).
- Referee prepares $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$ in state ρ and performs Bell measurements on $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$.
- Alice and Bob respond with a and b.
- Referee measures S w.r.t. $\{Q_{a,b}, \mathbb{1} - Q_{a,b}\}$.

Teleportation games and QCGs

Lemma

Given any QCG, G_{qc} with registers (X, Y), there exists a teleportation game, G_t, s.t.

$$\omega_N^*(G_{qc}) \leq \omega_{N|\mathsf{X}||\mathsf{Y}|}^*(G_t) \quad \text{and} \quad \omega_N^*(G_t) \leq \omega_{N|\mathsf{X}||\mathsf{Y}|}^*(G_{qc}),$$

for all $N \geq 1$.

Teleportation games and QCGs

Lemma

Given any QCG, G_{qc} with registers (X, Y), there exists a teleportation game, G_t, s.t.

$$\omega_N^*(G_{qc}) \leq \omega_{N|\mathsf{X}||\mathsf{Y}|}^*(G_t) \quad \text{and} \quad \omega_N^*(G_t) \leq \omega_{N|\mathsf{X}||\mathsf{Y}|}^*(G_{qc}),$$

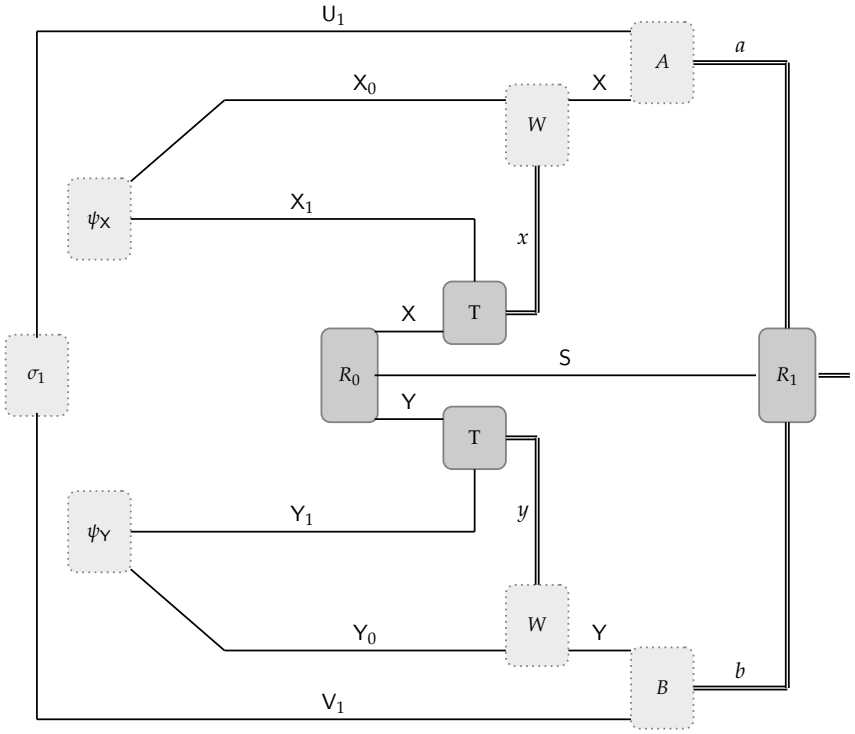
for all $N \geq 1$.

Main approach:

- First inequality:
  - Alice and Bob play honestly, i.e. they play along and perform teleportation as expected.
- Second inequality:
  - Alice and Bob play dishonestly. Alice and Bob perform a teleportation protocol "to themselves".

Teleportation games and QCGs

$\omega^*_N(G_{qc}) \leq \omega^*_{N|\mathsf{X}||\mathsf{Y}|}(G_t)$:



- Halves of MES in registers X_1 and Y_1 are sent to referee.
- Referee prepares state in $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$, measures $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$ in Bell basis.
- Alice and Bob apply Pauli corrections on $(\mathsf{U}_1, \mathsf{X}_0)$ and $(\mathsf{V}_1, \mathsf{Y}_0)$, thereby transmitting X and Y.

Teleportation games and QCGs

$\omega^*_N(G_t) \leq \omega^*_{N|X||Y|}(G_{qc})$:

1. States:
   - σ in (U, X_1, Y_1, V),
   - ρ prepared by referee in (X, S, Y).

Teleportation games and QCGs

$\omega^*_N(G_t) \leq \omega^*_{N|\mathsf{X}||\mathsf{Y}|}(G_{qc})$:

1. States:
   - σ in $(\mathsf{U}, \mathsf{X}_1, \mathsf{Y}_1, \mathsf{V})$,
   - ρ prepared by referee in $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$.
2. Alice and Bob measure $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$ in Bell basis yielding outcomes x and y.

Teleportation games and QCGs

$\omega^*_N(G_t) \leq \omega^*_{N|\mathsf{X}||\mathsf{Y}|}(G_{qc})$:

1. States:
   - σ in $(\mathsf{U}, \mathsf{X}_1, \mathsf{Y}_1, \mathsf{V})$,
   - ρ prepared by referee in $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$.
2. Alice and Bob measure $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$ in Bell basis yielding outcomes x and y.
3. Alice and Bob perform measurements

$$\{A^x_a : a \in A\} \subset \mathrm{Pos}(\mathcal{U}) \quad \text{and} \quad \{B^y_b : b \in B\} \subset \mathrm{Pos}(\mathcal{V})$$

   and obtain outcomes a and b.

Teleportation games and QCGs

$\omega^*_N(G_t) \leq \omega^*_{N|\mathsf{X}||\mathsf{Y}|}(G_{qc})$:

1. States:
   - σ in $(\mathsf{U}, \mathsf{X}_1, \mathsf{Y}_1, \mathsf{V})$,
   - ρ prepared by referee in $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$.
2. Alice and Bob measure $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$ in Bell basis yielding outcomes x and y.
3. Alice and Bob perform measurements

$$\{A^x_a : a \in A\} \subset \mathrm{Pos}(\mathcal{U}) \quad \text{and} \quad \{B^y_b : b \in B\} \subset \mathrm{Pos}(\mathcal{V})$$

   and obtain outcomes a and b.
   - Steps 2 and 3 may be described by measurement operators

$$\sum_{x \in X} A^x_a \otimes \phi_x^{|\mathsf{X}|} \quad \text{and} \quad \sum_{y \in Y} B^y_b \otimes \phi_y^{|\mathsf{Y}|}$$

     in registers $(\mathsf{U}, \mathsf{X}_1, \mathsf{X})$ and $(\mathsf{V}, \mathsf{Y}_1, \mathsf{Y})$.

Teleportation games and QCGs

$\omega^*_N(G_t) \leq \omega^*_{N|\mathsf{X}||\mathsf{Y}|}(G_{qc})$:

1. States:
   - σ in $(\mathsf{U}, \mathsf{X}_1, \mathsf{Y}_1, \mathsf{V})$,
   - ρ prepared by referee in $(\mathsf{X}, \mathsf{S}, \mathsf{Y})$.
2. Alice and Bob measure $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$ in Bell basis yielding outcomes x and y.
3. Alice and Bob perform measurements

$$\{A^x_a : a \in A\} \subset \mathrm{Pos}(\mathcal{U}) \quad \text{and} \quad \{B^y_b : b \in B\} \subset \mathrm{Pos}(\mathcal{V})$$

   and obtain outcomes a and b.
   - Steps 2 and 3 may be described by measurement operators

$$\sum_{x \in X} A^x_a \otimes \phi_x^{|\mathsf{X}|} \quad \text{and} \quad \sum_{y \in Y} B^y_b \otimes \phi_y^{|\mathsf{Y}|}$$

     in registers $(\mathsf{U}, \mathsf{X}_1, \mathsf{X})$ and $(\mathsf{V}, \mathsf{Y}_1, \mathsf{Y})$.
4. Finally referee measures on S.

ENLGs and teleportation games

Lemma

For any teleportation game G_t with registers (X, Y), there exists an ENLG H_t such that

$$\omega_N^*(H_t) = 1 - \frac{1 - \omega_N^*(G_t)}{|\mathsf{X}|^2 |\mathsf{Y}|^2}$$

for all N.

ENLGs and teleportation games

Lemma

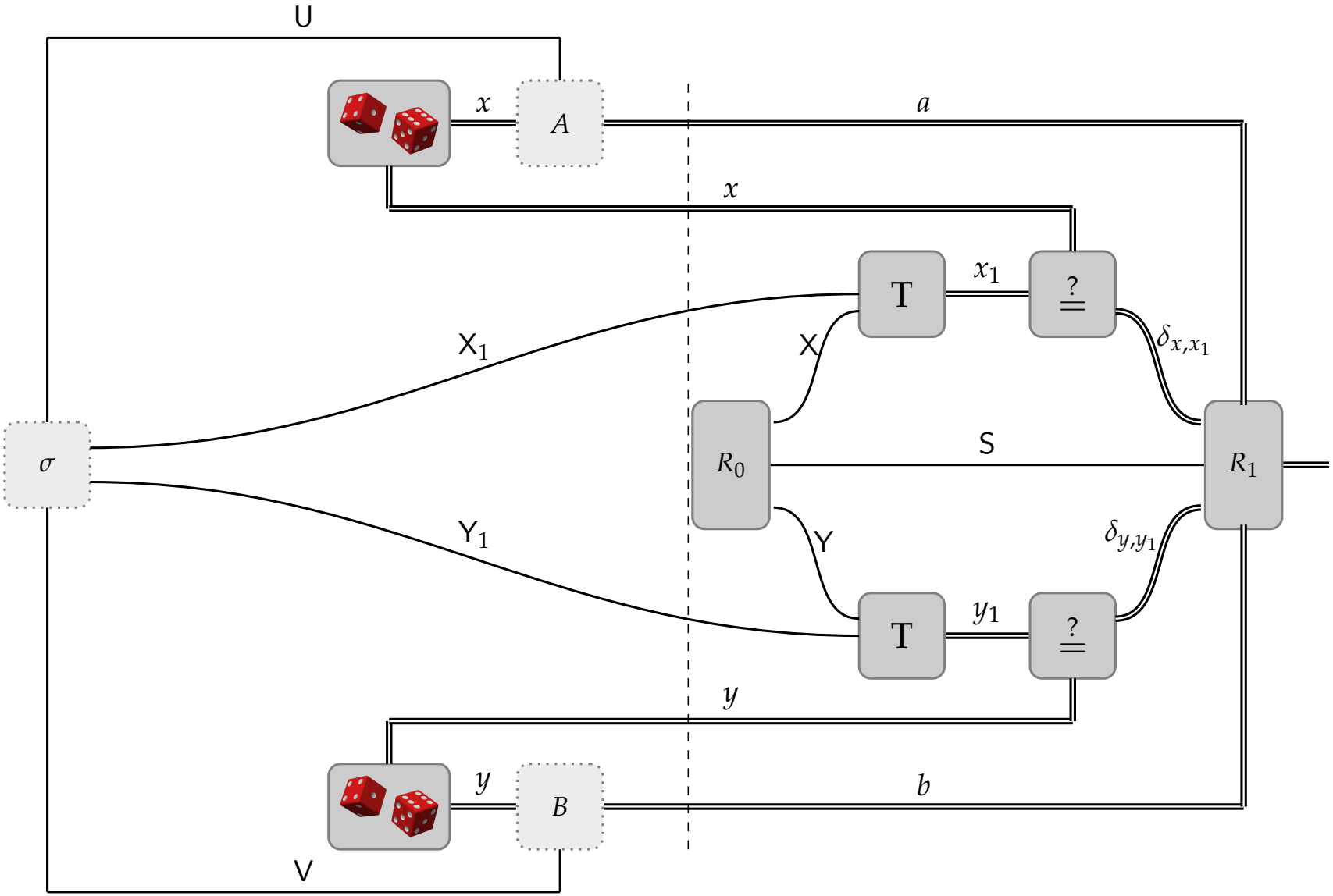
For any teleportation game G_t with registers (X, Y), there exists an ENLG H_t such that

$$\omega_N^*(H_t) = 1 - \frac{1 - \omega_N^*(G_t)}{|\mathsf{X}|^2 |\mathsf{Y}|^2}$$

for all N.

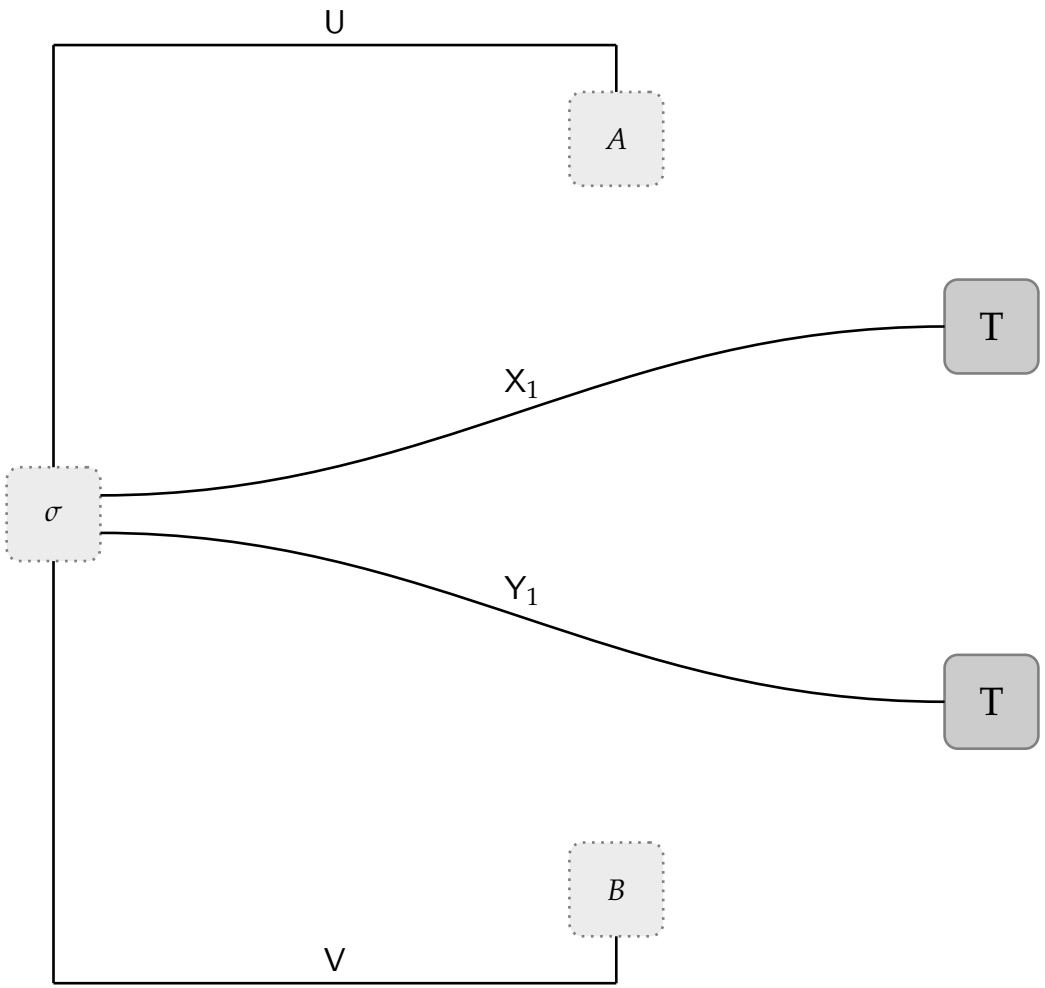
1. Describe how H_t is played.
2. Proceed to show the above Lemma.

Post-selected teleportation protocol for H_t



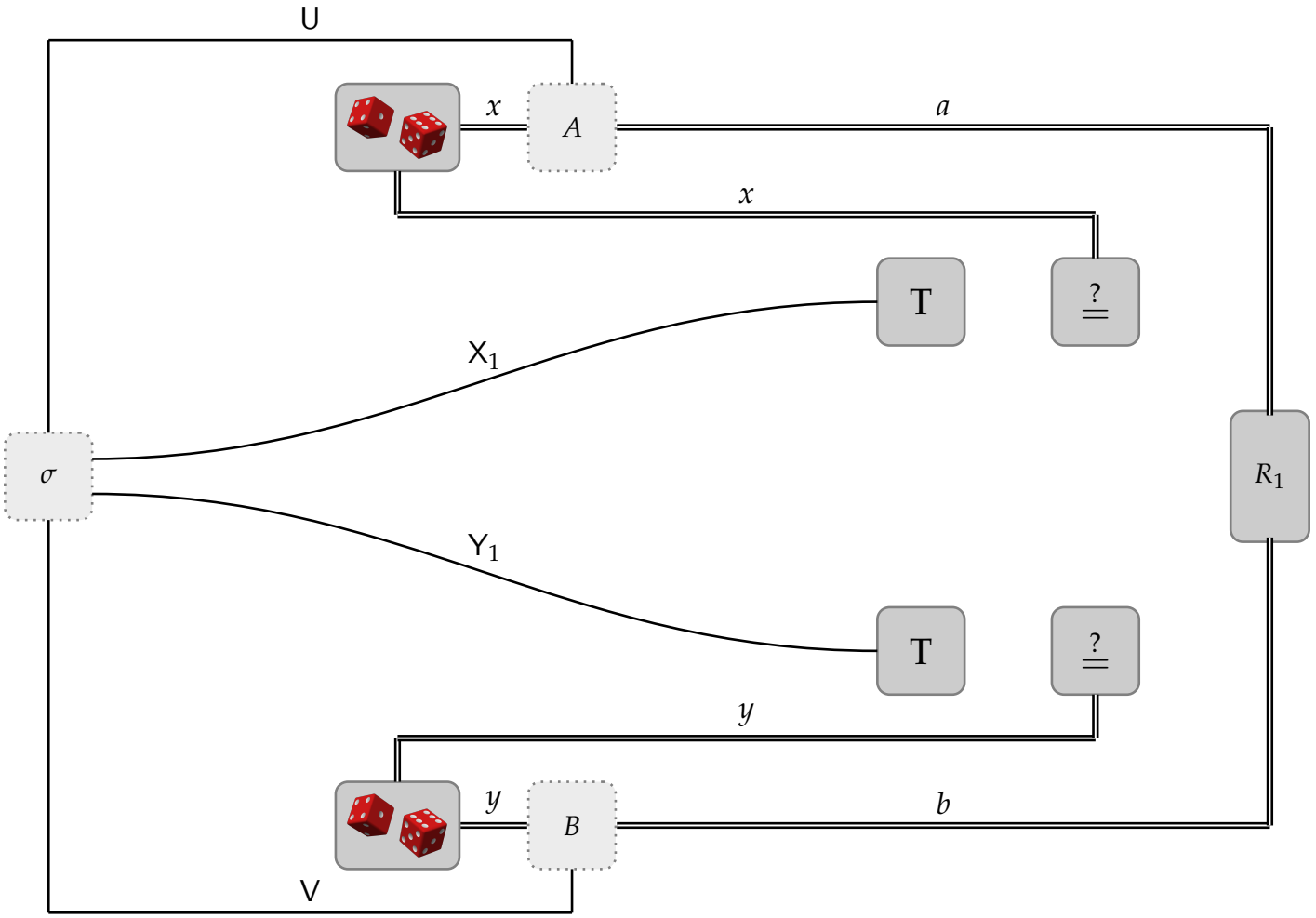
Step 1: Post-selected teleportation protocol for H_t

The state $\sigma \in \mathrm{D}(\mathcal{U} \otimes (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes \mathcal{V})$ is prepared.



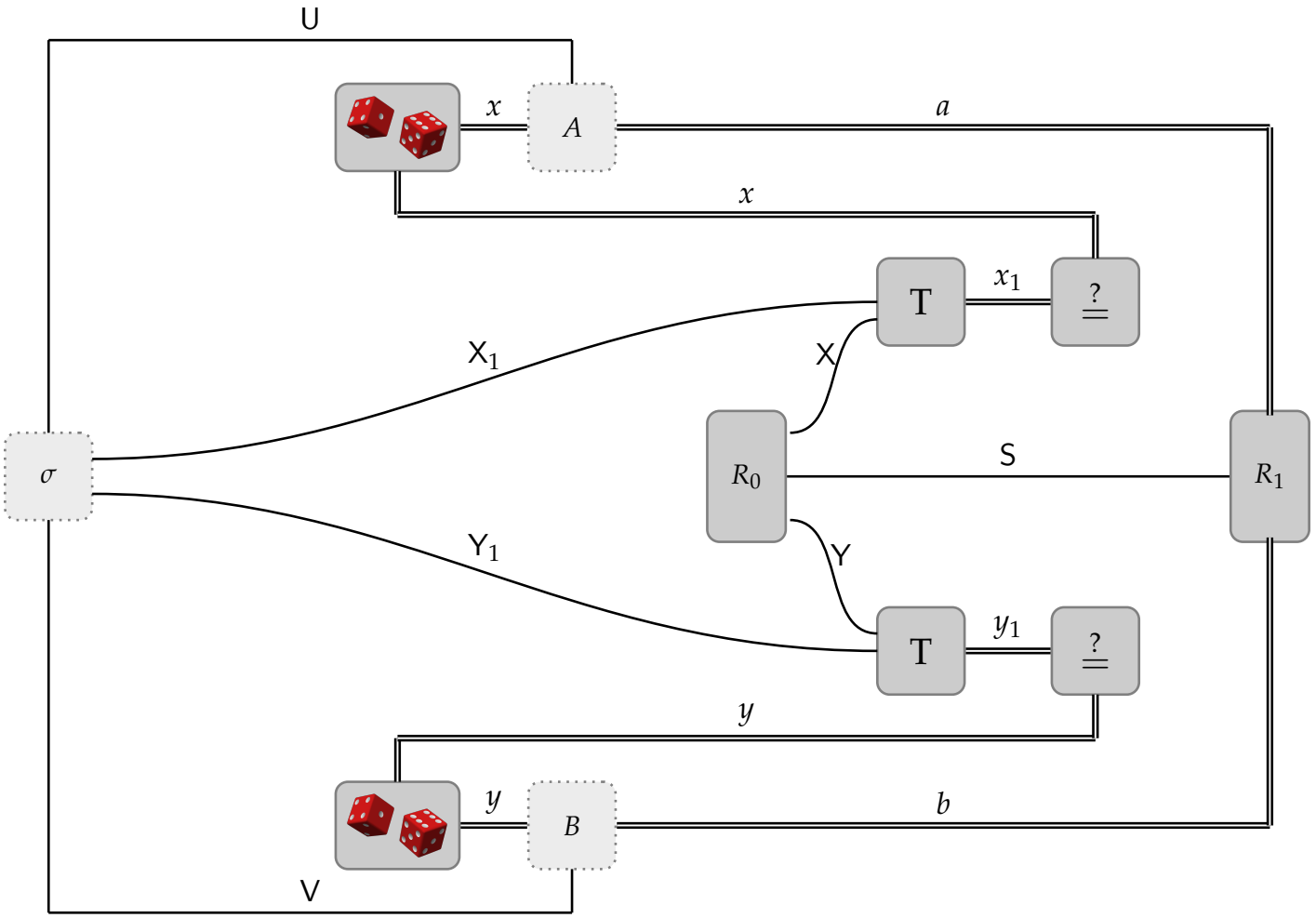
Step 2: Post-selected teleportation protocol for H_t

Referee randomly selects and sends (x, y); keeps a local copy. Alice and Bob respond with (a, b).



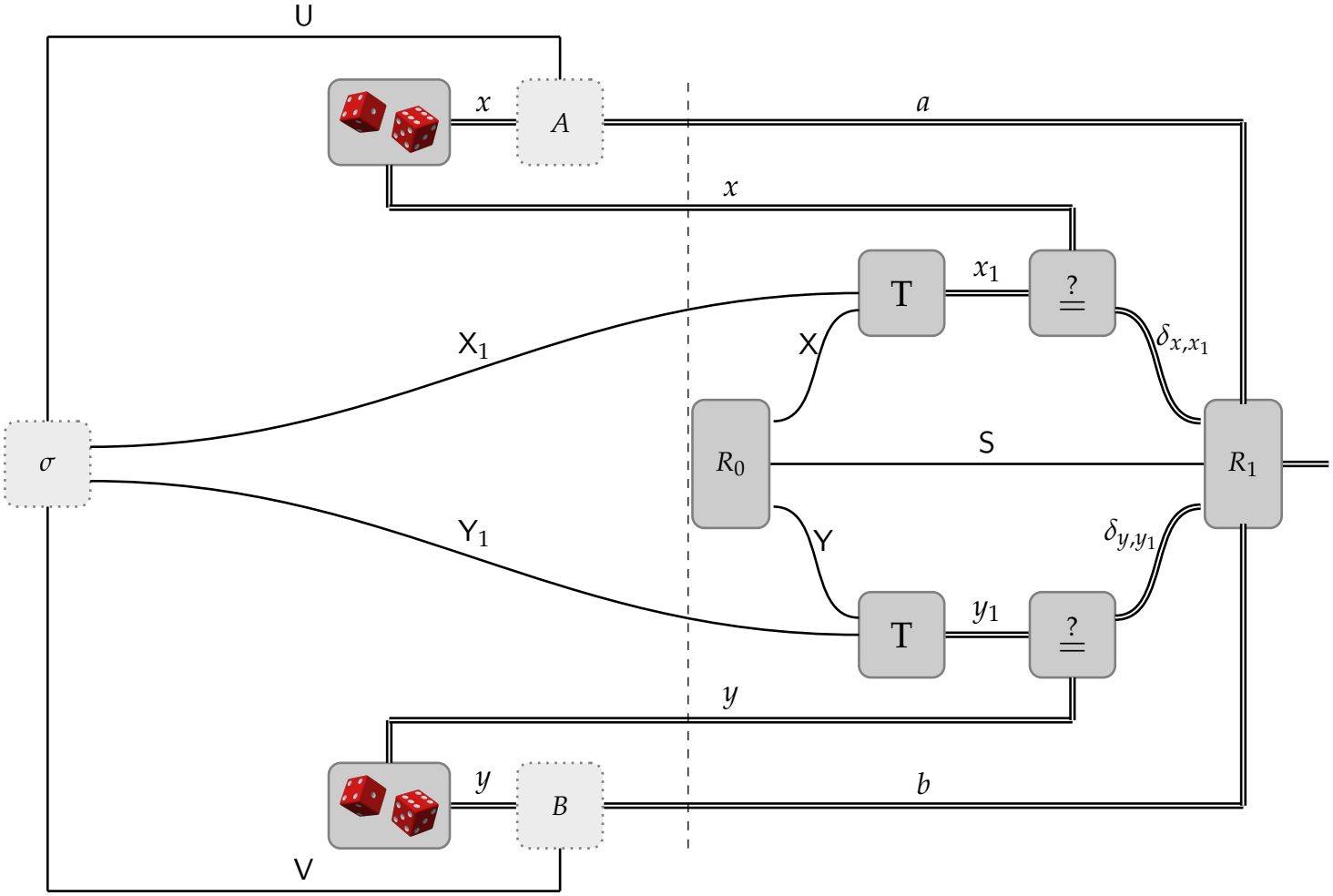
Step 3: Post-selected teleportation protocol for H_t

Referee prepares $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{S} \otimes \mathcal{Y})$. Performs teleportation using $(\mathsf{X}, \mathsf{X}_1)$ and $(\mathsf{Y}, \mathsf{Y}_1)$ resulting in outcomes (x_1, y_1).



Step 4: Post-selected teleportation protocol for H_t

1. If $x \neq x_1$ or $y \neq y_1$: teleportation fails; Alice and Bob win.
2. If $x = x_1$ and $y = y_1$: teleportation succeeds; referee measures.



ENLGs and teleportation games: Main proof idea

Main approach:

1. Consider a G_t and H_t, which are defined by the same objects:

$$\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{S} \otimes \mathcal{Y}) \quad \text{and} \quad \{Q_{a,b}\} \subset \mathrm{Pos}(\mathcal{S}).$$

2. In both games, a strategy is defined by:

$$\sigma \in \mathrm{D}(\mathcal{U} \otimes (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes \mathcal{V}), \quad \{A_a^x\} \subset \mathrm{Pos}(\mathcal{U}), \quad \text{and} \quad \{B_b^y\} \subset \mathrm{Pos}(\mathcal{V}).$$

ENLGs and teleportation games: Main proof idea

Main approach:

1. Consider a G_t and H_t, which are defined by the same objects:

$$\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{S} \otimes \mathcal{Y}) \quad \text{and} \quad \{Q_{a,b}\} \subset \mathrm{Pos}(\mathcal{S}).$$

2. In both games, a strategy is defined by:

$$\sigma \in \mathrm{D}(\mathcal{U} \otimes (\mathcal{X}_1 \otimes \mathcal{Y}_1) \otimes \mathcal{V}), \quad \{A_a^x\} \subset \mathrm{Pos}(\mathcal{U}), \quad \text{and} \quad \{B_b^y\} \subset \mathrm{Pos}(\mathcal{V}).$$

We will consider the winning and losing probabilities for this strategy for G_t and H_t.

ENLGs and teleportation games: G_t

For G_t, the winning probability, denoted by p, is given by:

$$p = \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes \phi_x^{|\mathsf{X}|} \otimes Q_{a,b} \otimes \phi_y^{|\mathsf{Y}|} \otimes B_b^y, W(\rho\otimes\sigma)W^* \right\rangle,$$

where $\phi_x^{|\mathsf{X}|}$ and $\phi_y^{|\mathsf{Y}|}$ are Bell measurements.

ENLGs and teleportation games: G_t

For G_t, the winning probability, denoted by p, is given by:

$$p = \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes \phi_x^{|\mathsf{X}|} \otimes Q_{a,b} \otimes \phi_y^{|\mathsf{Y}|} \otimes B_b^y, W(\rho\otimes\sigma)W^* \right\rangle,$$

where $\phi_x^{|\mathsf{X}|}$ and $\phi_y^{|\mathsf{Y}|}$ are Bell measurements.

Likewise, the losing probability for G_t is given by:

$$1 - p = \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes \phi_x^{|\mathsf{X}|} \otimes (\mathbb{1} - Q_{a,b}) \otimes \phi_y^{|\mathsf{Y}|} \otimes B_b^y, W(\rho\otimes\sigma)W^* \right\rangle.$$

ENLGs and teleportation games: H_t

For H_t the winning probability, denoted by q, is given by:

$$q = \frac{1}{|\mathrm{X}|^2|\mathrm{Y}|^2} \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes P_{x,y,a,b} \otimes B_b^y, W\left(\rho \otimes \sigma\right) W^* \right\rangle.$$

ENLGs and teleportation games: H_t

For H_t the winning probability, denoted by q, is given by:

$$q = \frac{1}{|\mathrm{X}|^2|\mathrm{Y}|^2} \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes P_{x,y,a,b} \otimes B_b^y, W\left(\rho\otimes\sigma\right)W^* \right\rangle.$$

Likewise, the losing probability for H_t is given by:

$$\begin{aligned} 1-q &= \frac{1}{|\mathrm{X}|^2|\mathrm{Y}|^2} \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes \left(\mathbb{1} - P_{x,y,a,b}\right) \otimes B_b^y, W\left(\rho\otimes\sigma\right)W^* \right\rangle \\ &= \frac{1}{|\mathrm{X}|^2|\mathrm{Y}|^2} \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle A_a^x \otimes \phi_x^{|\mathrm{X}|} \otimes \left(\mathbb{1} - Q_{a,b}\right) \otimes \phi_y^{|\mathrm{Y}|} \otimes B_b^y, W\left(\rho\otimes\sigma\right)W^* \right\rangle \\ &= \frac{1}{|\mathrm{X}|^2|\mathrm{Y}|^2}(1-p), \end{aligned}$$

where again p is the winning probability for G_t.

ENLGs and teleportation games

In both cases, the cost of the strategy is the same

$$N = \dim(\mathcal{U} \otimes \mathcal{V}).$$

Optimizing over strategies of cost N gives

$$\omega_N^*(H_t) = 1 - \frac{1 - \omega_N^*(G_t)}{|\mathrm{X}|^2 |\mathrm{Y}|^2}.$$

Proving relationship between ENLGs and QCGs

By recalling the correspondence between:

1. QCG $\leftrightarrow$ teleportation game,
2. Teleportation game $\leftrightarrow$ ENLG,

we obtain a direct correspondence between QCGs and ENLGs.

Proving relationship between ENLGs and QCGs

By recalling the correspondence between:

1. QCG $\leftrightarrow$ teleportation game,
2. Teleportation game $\leftrightarrow$ ENLG,

we obtain a direct correspondence between QCGs and ENLGs.

1. From QCG $\leftrightarrow$ teleportation game:

$$\omega_N^*(G_{qc}) \leq \omega_{N|X||Y|}^*(G_t) \quad \text{and} \quad \omega_N^*(G_t) \leq \omega_{N|X||Y|}^*(G_{qc}).$$

Proving relationship between ENLGs and QCGs

By recalling the correspondence between:

1. QCG $\leftrightarrow$ teleportation game,
2. Teleportation game $\leftrightarrow$ ENLG,

we obtain a direct correspondence between QCGs and ENLGs.

1. From QCG $\leftrightarrow$ teleportation game:

$$\omega_N^*(G_{qc}) \leq \omega_{N|X||Y|}^*(G_t) \quad \text{and} \quad \omega_N^*(G_t) \leq \omega_{N|X||Y|}^*(G_{qc}).$$

2. From Teleportation game $\leftrightarrow$ ENLG:

$$\omega_N^*(H_t) = 1 - \frac{1 - \omega_N^*(G_t)}{|X|^2|Y|^2}.$$

Proving relationship between ENLGs and QCGs

By recalling the correspondence between:

1. QCG $\leftrightarrow$ teleportation game,
2. Teleportation game $\leftrightarrow$ ENLG,

we obtain a direct correspondence between QCGs and ENLGs.

1. From QCG $\leftrightarrow$ teleportation game:

$$\omega_N^*(G_{qc}) \leq \omega_{N|X||Y|}^*(G_t) \quad \text{and} \quad \omega_N^*(G_t) \leq \omega_{N|X||Y|}^*(G_{qc}).$$

2. From Teleportation game $\leftrightarrow$ ENLG:

$$\omega_N^*(H_t) = 1 - \frac{1 - \omega_N^*(G_t)}{|X|^2|Y|^2}.$$

3. Rewriting the above, we obtain:

$$\omega_N^*(G_t) = 1 - |\mathrm{X}|^2|\mathrm{Y}|^2 \left(1 - \omega_N^*(H_t)\right).$$

Proving relationship between ENLGs and QCGs

By recalling the correspondence between:

1. QCG $\leftrightarrow$ teleportation game,
2. Teleportation game $\leftrightarrow$ ENLG,

we obtain a direct correspondence between QCGs and ENLGs.

1. From QCG $\leftrightarrow$ teleportation game:

$$\omega_N^*(G_{qc}) \leq \omega_{N|X||Y|}^*(G_t) \quad \text{and} \quad \omega_N^*(G_t) \leq \omega_{N|X||Y|}^*(G_{qc}).$$

2. From Teleportation game $\leftrightarrow$ ENLG:

$$\omega_N^*(H_t) = 1 - \frac{1 - \omega_N^*(G_t)}{|X|^2|Y|^2}.$$

3. Rewriting the above, we obtain:

$$\omega_N^*(G_t) = 1 - |\mathrm{X}|^2|\mathrm{Y}|^2 \left(1 - \omega_N^*(H_t)\right).$$

4. Using (1) and applying to (2) we have that

$$1 - \frac{1 - \omega_N^*(G_{qc})}{|\mathrm{X}|^2|\mathrm{Y}|^2} \leq \omega_{N|\mathrm{X}||\mathrm{Y}|}^*(H_t) \quad \text{and} \quad \omega_N^*(H_t) \leq 1 - \frac{1 - \omega_{N|\mathrm{X}||\mathrm{Y}|}^*(G_{qc})}{|\mathrm{X}|^2|\mathrm{Y}|^2}$$

Supplementary material:
Variations on extended nonlocal games

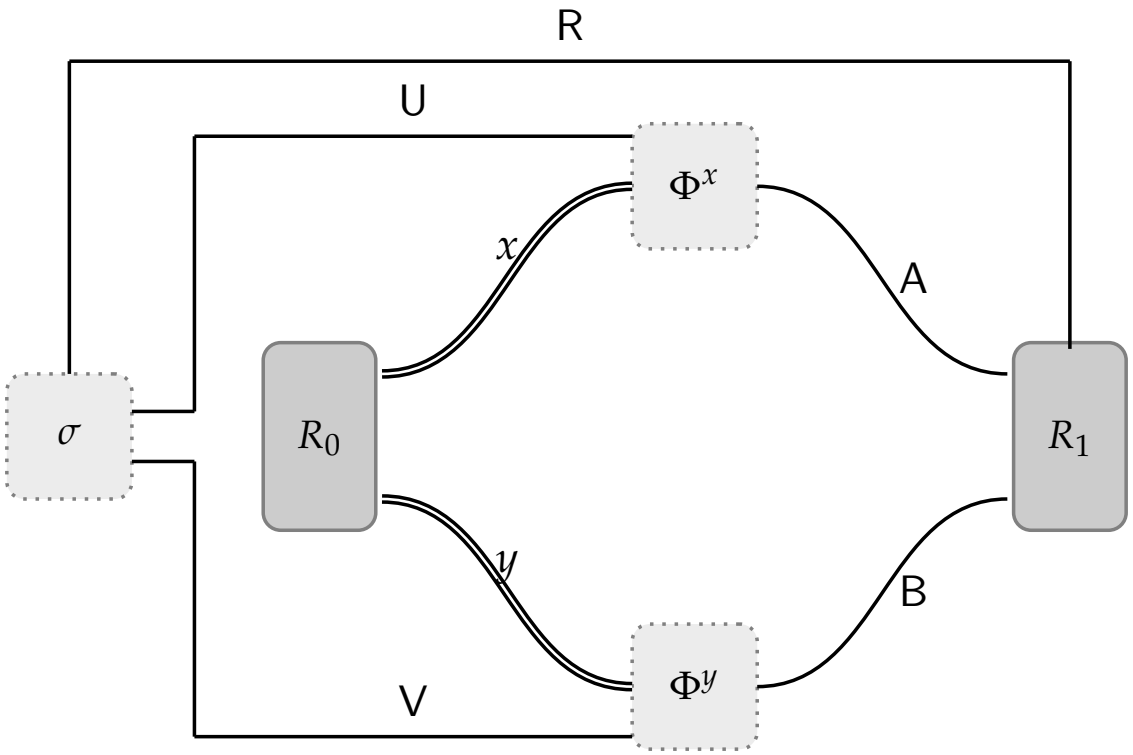
Quantum-classical-quantum extended nonlocal games

One may also investigate other models of extended nonlocal games where the variance is with respect to the type of communication.

Quantum-classical-quantum extended nonlocal games

One may also investigate other models of extended nonlocal games where the variance is with respect to the type of communication.

A *quantum-classical-quantum extended nonlocal game* (QCQ ENLG) is an ENLG where the answers are quantum registers instead of classical strings.



Quantum-classical-quantum extended nonlocal games

One may define various strategies for a QCQ ENLG. A standard quantum strategy consists of

1. Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$.
2. Collection of channels: $\{\Phi^x\} \subset \mathrm{C}(\mathcal{U}, \mathcal{A})$ and $\{\Phi^y\} \subset \mathrm{C}(\mathcal{V}, \mathcal{B})$.

Quantum-classical-quantum extended nonlocal games

One may define various strategies for a QCQ ENLG. A standard quantum strategy consists of

1. Shared state: $\sigma \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$.
2. Collection of channels: $\{\Phi^x\} \subset \mathrm{C}(\mathcal{U}, \mathcal{A})$ and $\{\Phi^y\} \subset \mathrm{C}(\mathcal{V}, \mathcal{B})$.

The winning probability for such a strategy is given by:

$$\sum_{(x,y)\in X\times Y} \left\langle P_{x,y}, \left(\Phi^x \otimes \mathbb{1}_{\mathrm{L}(\mathcal{R})} \otimes \Phi^y\right)(\sigma) \right\rangle.$$

Supplementary material: Determining the value of extended nonlocal games

Calculating the unentangled value of ENLGs

Recall that

$$\omega(G) = \max_{f,g} \left\| \sum_{x,y} \pi(x,y) P_{f(x),g(y),x,y} \right\|,$$

where the maximum is over all functions

$$f : X \to A \quad \text{and} \quad g : Y \to B.$$

This may be easily calculated in MATLAB (for instance), and is implemented along with other ENLG functionality on Github.[15]

[15] github.com/vprusso/phd_thesis

Calculating the non-signaling value of ENLGs

The non-signaling value can be calculated by a semidefinite program where the non-signaling constraints are the "subject to" conditions:

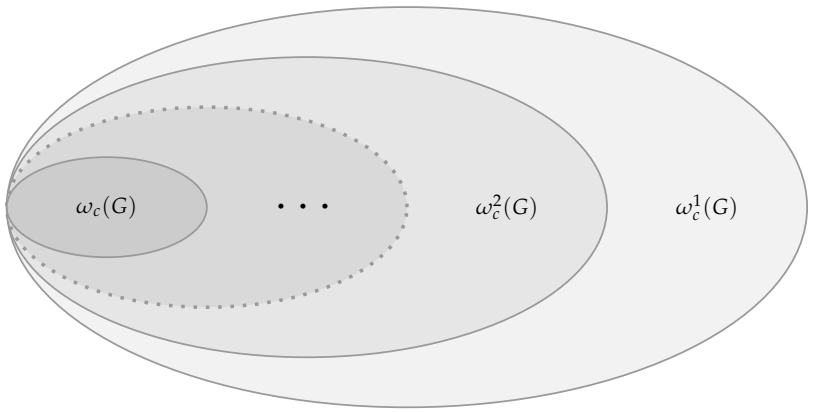
$$\underline{\text{Primal problem}}$$

$$\begin{aligned}
\text{maximize:} \quad & \frac{1}{|\mathrm{X}||\mathrm{Y}|} \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \left\langle P_{a,b,x,y}, K(a,b|x,y) \right\rangle \\
\text{subject to:} \quad & \sum_{a\in A} K(a,b|x,y) = \xi_b^y, \qquad \forall x \in X, \\
& \sum_{b\in B} K(a,b|x,y) = \rho_a^x, \qquad \forall y \in Y, \\
& \sum_{a\in A} \rho_a^x = \tau = \sum_{b\in B} \xi_b^y, \qquad \forall x \in X,\ y \in Y, \\
& \tau \in \mathrm{Pos}(\mathcal{R}).
\end{aligned}$$

Supplementary material:
Upper bounds for extended nonlocal games

The QC hierarchy: Upper bounds for nonlocal games

- The QC hierarchy is a method of placing *upper bounds* on the *quantum value* of nonlocal games.
- Hierarchy of semidefinite programs is *guaranteed* to converge to the commuting measurement value for some finite level, k of the hierarchy.
- The commuting measurement value is an upper bound on the quantum value, $\omega^*(G) \leq \omega_c(G)$, for all nonlocal games, G.



The QC hierarchy: Main idea

- Finding a quantum state and measurements for a quantum strategy is a computationally difficult task.

The QC hierarchy: Main idea

- Finding a quantum state and measurements for a quantum strategy is a computationally difficult task.
- Instead then, let's think about a set of *weaker* conditions that correspond to a commuting measurement strategy.

The QC hierarchy: Main idea

- Finding a quantum state and measurements for a quantum strategy is a computationally difficult task.
- Instead then, let's think about a set of *weaker* conditions that correspond to a commuting measurement strategy.
- In the QC hierarchy, each condition amounts to verifying the existence of a positive semidefinite matrix with structure that depends on algebraic properties satisfied by a commuting measurement strategy.

The QC hierarchy: Main idea

- Finding a quantum state and measurements for a quantum strategy is a computationally difficult task.
- Instead then, let's think about a set of *weaker* conditions that correspond to a commuting measurement strategy.
- In the QC hierarchy, each condition amounts to verifying the existence of a positive semidefinite matrix with structure that depends on algebraic properties satisfied by a commuting measurement strategy.
- If any of these conditions are violated, we may conclude that there does not exist an adequate state and sets of measurements.

The extended QC hierarchy

Recall the commuting measurement value of an ENLG may be obtained by maximizing

$$\sum_{(x,y)\in X\times Y} \pi(x,y) \sum_{(a,b)\in A\times B} \left\langle P_{a,b,x,y}, K(a,b|x,y) \right\rangle,$$

where K is a commuting measurement assemblage operator.

The extended QC hierarchy

Recall the commuting measurement value of an ENLG may be obtained by maximizing

$$\sum_{(x,y)\in X\times Y} \pi(x,y) \sum_{(a,b)\in A\times B} \left\langle P_{a,b,x,y}, K(a,b|x,y) \right\rangle,$$

where K is a commuting measurement assemblage operator.

The extended QC hierarchy allows us to phrase the above as

$$\sum_{(x,y)\in X\times Y} \pi(x,y) \sum_{(a,b)\in A\times B} \left\langle P_{a,b,x,y}, M^{(k)}((x,a),(y,b)) \right\rangle,$$

where $M^{(k)}$ is some matrix parametrized by some integer k with entries indexed by a, b, x, y satisfying *certain constraints*.

Primal problem

$$
\begin{aligned}
\text{maximize:} \quad & \left\langle P_{a,b,x,y}, M^{(k)} \right\rangle \\
\text{subject to:} \quad & \underbrace{\sum_i M^{(k)}_{i,i}(\epsilon,\epsilon) = 1,}_{\text{normalization}} \\
& \underbrace{\begin{aligned} \sum_a M^{(k)}_{i,j}\left((x,a),(y,b)\right) &= M^{(k)}_{i,j}\left(1,(y,b)\right), \\ \sum_b M^{(k)}_{i,j}\left((x,a),(y,b)\right) &= M^{(k)}_{i,j}\left((x,a),1\right), \end{aligned}}_{\text{measurements sum to } \mathbb{1}} \\
& \underbrace{\begin{aligned} M^{(k)}_{i,j}\left(1,(y,b)\right) &= M^{(k)}_{i,j}\left((y,b),(y,b)\right), \\ M^{(k)}_{i,j}\left((x,a),1\right) &= M^{(k)}_{i,j}\left((x,a),(x,a)\right), \end{aligned}}_{\text{projective measurements}} \\
& \underbrace{M^{(k)}_{i,j}\left((x,a),(y,b)\right) = M^{(k)}_{i,j}\left((y,b),(x,a)\right),}_{\text{commutation}} \\
& M^{(k)} \in \mathrm{Pos}(\mathcal{R}).
\end{aligned}
$$

Strings

In order to index into $M^{(k)}((x, a), (y, b))$, we will consider strings.

Define

$$\Delta = (X \times A) \mathbin{\dot\cup} (Y \times B),$$

define Δ^* to denote the set of all strings (of finite length) over Δ.

Strings

In order to index into $M^{(k)}((x,a),(y,b))$, we will consider strings.

Define

$$\Delta = (X \times A) \mathbin{\dot\cup} (Y \times B)\,,$$

define Δ^* to denote the set of all strings (of finite length) over Δ.

We may also want to refer to the set of all strings of some length. For instance for $k = 1$, we have that

$$\Delta^{\leq 1} = \{\epsilon\} \cup \{(x,a)\} \cup \{(y,b)\}.$$

Strings

In order to index into $M^{(k)}((x,a),(y,b))$, we will consider strings.

Define

$$\Delta = (X \times A) \uplus (Y \times B),$$

define Δ^* to denote the set of all strings (of finite length) over Δ.

We may also want to refer to the set of all strings of some length. For instance for $k = 1$, we have that

$$\Delta^{\leq 1} = \{\epsilon\} \cup \{(x,a)\} \cup \{(y,b)\}.$$

For example, we can refer to operators (or products of operators) as tuples of concatenated strings. For example:

$$A_a^x \to (x,a), \quad \text{and}$$
$$A_{a_1}^{x_1} \dots A_{a_k}^{x_k} \to (x_1,a_1) \dots (x_k,a_k).$$

Similarly for Bob.

Equivalence relations for strings

The measurements in a commuting measurement strategy are *projective* and they *commute*. This property can be conveyed in terms of a string relation:

For all strings $s, t \in \Delta^*$,

1. Projective: $s\sigma t \sim s\sigma\sigma t$ for all $\sigma \in \Delta$
2. Commute: $s\sigma\tau t \sim s\tau\sigma t$ for all $\sigma \in X \times A$ and $\tau \in Y \times B$.

Admissible functions

The function

$$\phi : \Delta^* \to \mathbb{C}$$

is *admissible* iff it satisfies the following conditions:

1. Measurements sum to identity:

$$\sum_{a \in A} \phi(s(x,a)t) = \sum_{b \in B} \phi(s(y,b)t) = \phi(st),$$

   for all $x, y \in X \times Y$.

2. For every string $s, t \in \Delta^*$:

$$\phi(s(x,a)(x,a')t) = 0 \quad \text{and} \quad \phi(s(y,b)(y,b')t) = 0$$

   for all $x \in X$ and $a, a' \in A$ s.t. $a \neq a'$ and $b, b' \in B$ s.t. $b \neq b'$.

3. For all $s, t \in \Sigma^*$ where $s \sim t$:

$$\phi(s) = \phi(t).$$

k-th order admissible matrices

We call the matrix $M^{(k)}$ an *k-th order admissible matrix* if

1. There exists an admissible function

$$\phi : \Delta^{\leq k} \to \mathbb{C},$$

   such that

$$M^{(k)}(s,t) = \phi(s^R t) \quad \forall s,t \in \Delta^{\leq k},$$

2. Normalization: $M^{(k)}(\epsilon,\epsilon) = 1$,
3. $M^{(k)}$ is positive semidefinite.

k-th order pseudo commuting measurement assemblages

Define an *k-th order pseudo commuting measurement assemblage*

$$K : A \times B \times X \times Y \to \mathrm{L}(\mathbb{C}^m),$$

for which there exists an k-th order admissible matrix $M^{(k)}$ such that

$$K(a, b|x, y) = M^{(k)}((x, a), (y, b)) \quad \forall x, y, a, b.$$

The extended QC hierarchy

Theorem

Let X, Y, A, and B be alphabets, let m be a positive integer, let $\mathcal{R} = \mathbb{C}^m$ be a complex Euclidean space, and let

$$K : A \times B \times X \times Y \to \mathrm{L}(\mathcal{R})$$

be a function. The following statements are equivalent:

1. *The function K is a commuting measurement assemblage.*
2. *The function K is a k-th order pseudo commuting measurement assemblage for every positive integer k.*

The extended QC hierarchy

Theorem

Let X, Y, A, and B be alphabets, let m be a positive integer, let $\mathcal{R} = \mathbb{C}^m$ be a complex Euclidean space, and let

$$K : A \times B \times X \times Y \to \mathrm{L}(\mathcal{R})$$

be a function. The following statements are equivalent:

1. *The function K is a commuting measurement assemblage.*
2. *The function K is a k-th order pseudo commuting measurement assemblage for every positive integer k.*

Note: For $m = 1$, this is precisely the original QC hierarchy theorem.

The extended QC hierarchy: 1 $\implies$ 2

Let K be a commuting measurement assemblage. Then K is also a k-th order pseudo commuting measurement assemblage for every k (easier direction):

- Since K is a commuting measurement assemblage, we have:

$$\{A_a^x : a \in A\} \subset \mathrm{Pos}(\mathcal{H}) \quad \text{and} \quad \{B_b^y : b \in B\} \subset \mathrm{Pos}(\mathcal{H}),$$

  along with a pure state $u \in \mathcal{R} \otimes \mathcal{H}$ where

$$u = \sum_{j=1}^{m} e_j \otimes u_j,$$

  where $u_1, \ldots, u_m \in \mathcal{H}$.

The extended QC hierarchy: 1 $\implies$ 2

Since we have a state and measurements, we just need to show that those can be used to define a k-th order pseudo commuting measurement assemblage. This just follows more or less from the definition:

- Shorthand Π_c^z to be either measurement for Alice or Bob.
- The matrix $M^{(k)}$ has entries

$$M_{i,j}^{(k)}(s,t) = \phi_{i,j}(s^R t)$$

where

$$\phi_{i,j}\left((z_1, c_1)\dots(z_\ell, c_\ell)\right) = u_i \Pi_{c_1}^{z_1} \cdots \Pi_{c_\ell}^{z_\ell} u_j$$

The extended QC hierarchy: 2 $\implies$ 1

Assuming we are given K as a k-th order pseudo commuting measurement assemblage for every k, show that this is equivalent to K being a commuting measurement assemblage (harder direction).

The extended QC hierarchy: 2 $\implies$ 1

Assuming we are given K as a k-th order pseudo commuting measurement assemblage for every k, show that this is equivalent to K being a commuting measurement assemblage (harder direction).

The proof approach for this direction is summarized below:

1. Show that the matrices $M^{(k)}$ admit a proper limit:

$$\lim_{k\to\infty} M^{(k)} \to M.$$

2. Construct a quantum state and sets of measurements from M that satisfy properties of a commuting measurement strategy:
   - 2.1 Construct $\rho \in \mathrm{D}(\mathcal{R} \otimes \mathcal{H})$ from M.
   - 2.2 Construct measurements

$$\{A_a^x : a \in A\} \subset \mathrm{Pos}(\mathcal{H}) \quad \text{and} \quad \{B_b^y : b \in B\} \subset \mathrm{Pos}(\mathcal{H})$$

   from M.

The extended QC hierarchy: 2 $\implies$ 1

In order to define the limit, we must show the entries of $M^{(k)}$ are bounded:

Lemma

Let $m, k \geq 1$ be positive integers. Then a k-th order admissible matrix, $M^{(k)}$, satisfies

$$|M^{(k)}_{i,j}(s,t)| \leq 1,$$

for every $i, j \in \{1, \ldots, m\}$ and all $s, t \in \Delta^{\leq k}$.

The extended QC hierarchy: 2 $\implies$ 1

Proof: We know $M^{(k)}$ is PSD. By definition, any 2×2 submatrix is also PSD:

$$\begin{pmatrix} M_{i,i}^{(k)}(s,s) & M_{i,j}^{(k)}(s,t) \\ M_{j,i}^{(k)}(t,s) & M_{j,j}^{(k)}(t,t) \end{pmatrix}.$$

1. Off-diagonal (follows from PSD property):

$$|M_{i,j}^{(k)}(s,t)| \leq \sqrt{M_{i,i}^{(k)}(s,s)}\sqrt{M_{j,j}^{(k)}(t,t)}$$

2. Diagonal (follows from routine calculation on admissible function def.):

$$M_{i,i}^{(k)}((z,c)t,(z,c)t) \leq M_{i,i}^{(k)}(t,t).$$

The extended QC hierarchy: 2 $\implies$ 1

Matrix is bounded. Now let's show a proper limit exists:

- Create $\hat{M}^{(k)}$: a matrix we obtain by padding the blocks of $M^{(k)}$ in a way to make them infinite.
  - By Banach-Alaoglu theorem, we have that:

$$\lim_{l\to\infty} \hat{M}^{(k_l)} \to M,$$

where M is an infinite matrix s.t.

$$M = \begin{pmatrix} M_{1,1} & \dots & M_{1,m} \\ \vdots & \ddots & \vdots \\ M_{m,1} & \dots & M_{m,m} \end{pmatrix}$$

where

$$M_{i,j} : \Delta^* \times \Delta^* \to \mathbb{C}$$

for each $i, j \in \{1, \dots, m\}$.

- This M matrix satisfies the same constraints that the $M^{(k)}$ matrix does (that is, it is a k-th admissible matrix).

The extended QC hierarchy: 2 $\implies$ 1

Each block of M may be written as

$$M_{i,j}(s,t) = \left\langle u_{i,s}, u_{j,t} \right\rangle,$$

for all $i, j \in \{1, \ldots, m\}$ and $s, t \in \Delta^*$ where the vectors

$$\{u_{i,s} : i \in \{1, \ldots, m\}, s \in \Delta^*\} \subset \mathcal{H}.$$

The extended QC hierarchy: 2 $\implies$ 1

Now that we have the infinite matrix, M, we need to show how a state and sets of measurements arise that satisfy the constraints for a commuting measurement assemblage. Specifically:

1. Define a state from M satisfying the specifications of a commuting measurement assemblage.
2. Define sets of measurements for Alice and Bob satisfying the specifications of a commuting measurement assemblage:
   - 2.1 Measurements are projective.
   - 2.2 Measurements commute.

The extended QC hierarchy: 2 $\implies$ 1 (constructing quantum state)

Create state from commuting assemblage:

1. Define a pure state that corresponds to the vector

$$u = \sum_{j=1}^{m} e_j \otimes u_{j,\epsilon} \in \mathcal{R} \otimes \mathcal{H}.$$

2. The vector u is a unit vector (verified by calculation).

The extended QC hierarchy: 2 $\implies$ 1 (constructing measurements)

Create measurements from commuting assemblage:

1. Define Π_c^z to represent the projection operator onto the span of the set:

$$\{u_{j,(z,c)s} : j \in \{1, \ldots, m\}, s \in \Delta^*\}.$$

Need to prove that these projections, Π_c^z, are *projections* and also *commute*.

The extended QC hierarchy: 2 $\implies$ 1 (constructing measurements)

Some helpful properties:

1. Vectors $u_{j,s}$ and $u_{j,(z,c)s}$ have the same inner product with every vector in image of Π_c^z:

$$\left\langle u_{i,(z,c)t}, u_{j,s} \right\rangle = \left\langle u_{i,(z,c)t}, u_{j,(z,c)s} \right\rangle.$$

2. From the above it follows that

$$\Pi_c^z u_{j,s} = u_{j,(z,c)s}.$$

The extended QC hierarchy: 2 $\implies$ 1 (constructing measurements)

Measurements Π_c^z are projections ($\Pi_a^x \Pi_b^y = 0$).

- Measurements are orthogonal projections:

$$\begin{aligned}\left\langle u_{i,(z,c)t}, u_{j,(z,d)s} \right\rangle &= M_{i,j}((z,c)t,(z,d)s) \\ &= \phi_{i,j}(t^R(z,c)(z,d)s) \\ &= 0.\end{aligned}$$

The extended QC hierarchy: 2 $\implies$ 1 (constructing measurements)

Measurements Π_c^z obey $\sum_{a\in A}\Pi_a^x = \mathbb{1}$ and $\sum_{b\in B}\Pi_b^y = \mathbb{1}$.

- Measurements sum to $\mathbb{1}$:

$$\begin{aligned}\sum_{a\in A}\left\langle u_{i,s}, \Pi_a^x u_{j,t}\right\rangle &= \sum_{a\in A}\left\langle u_{i,s}, u_{j,(x,a)t}\right\rangle \\ &= \sum_{a\in A}\phi_{i,j}((s^R(x,a)t)) \\ &= \phi_{i,j}(s^R t) \\ &= \left\langle u_{i,s}, u_{j,t}\right\rangle.\end{aligned}$$

The extended QC hierarchy: 2 $\implies$ 1 (constructing measurements)

Measurements Π_c^z pairwise commute, $[\Pi_a^x, \Pi_b^y] = 0$.

- Measurements commute:

$$\begin{aligned}
\left\langle u_{i,s}, \Pi_a^x \Pi_b^y u_{j,t} \right\rangle &= \left\langle u_{i,(x,a)s}, u_{j,(y,b)t} \right\rangle \\
&= \phi_{i,j}(s^R(x,a)(y,b)t) \\
&= \phi_{i,j}(s^R(y,b)(x,a)t) \\
&= \left\langle u_{i,(y,b)s}, u_{j,(x,a)t} \right\rangle \\
&= \left\langle u_{i,s}, \Pi_b^y \Pi_a^x u_{j,t} \right\rangle.
\end{aligned}$$

The extended QC hierarchy: 2 $\implies$ 1 (constructing measurements)

Strategy represented by state u and projective measurements $\{\Pi_a^x\}$ and $\{\Pi_b^y\}$ yields a commuting measurement assemblage:

- Recall $\Pi_c^z u_{j,s} = u_{j,(z,c)s}$:

$$M_{i,j}((x,a),(y,b)) = \left\langle u_{i,(x,a)}, u_{j,(y,b)} \right\rangle = \left\langle \Pi_a^x \Pi_b^y, u_{j,\epsilon} u_{i,\epsilon}^* \right\rangle,$$

  and therefore

$$K(a,b|x,y) = \mathrm{Tr}_{\mathcal{H}}\left((\mathbb{1} \otimes \Pi_a^x \Pi_b^y) uu^*\right)$$

  for all x, y, a, b.

Supplementary material:
Lower bounds for extended nonlocal games

Lower bounds for extended nonlocal games

Key idea: Fixing measurements on one system yields the optimal measurements of the other system via an SDP.[16]

[16] Liang, Doherty: "Bounds on Quantum Correlations in Bell Inequality Experiments", (2007).

Lower bounds for extended nonlocal games

Key idea: Fixing measurements on one system yields the optimal measurements of the other system via an SDP.[16]

Iterative "see-saw" algorithm between two SDPs:

- SDP-1: Fix Bob's measurements. Optimize over Alice's measurements.
- SDP-2: Fix Alice's measurements (from SDP-1). Optimize over Bob's measurements.
- Repeat.

Not guaranteed to give optimal value, as the algorithm can get stuck in a local minimum.

[16] Liang, Doherty: "Bounds on Quantum Correlations in Bell Inequality Experiments", (2007).

Lower bounds for extended nonlocal games

Define $\{\rho_a^x : x \in X,\ a \in A\} \subset \mathrm{Pos}(\mathcal{R} \otimes \mathcal{B})$ as the residual states acting on the referee and Bob's systems and let

$$f = \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \pi(x,y)\big\langle P_{a,b,x,y} \otimes B_b^y, \rho_a^x \big\rangle,$$

$$g = \sum_{\substack{(x,y)\in X\times Y \\ (a,b)\in A\times B}} \pi(x,y)\big\langle B_b^y, \Phi^*(\rho_a^x) \big\rangle.$$

Lower bound: (SDP-1)

$$\begin{aligned} \text{max:} \quad & f \\ \text{s.t.:} \quad & \sum_{a\in A} \rho_a^x = \tau, \\ & \rho_a^x \in \mathrm{Pos}(\mathcal{R} \otimes \mathcal{B}), \\ & \tau \in \mathrm{D}(\mathcal{R} \otimes \mathcal{B}). \end{aligned}$$

Lower bound: (SDP-2)

$$\begin{aligned} \text{max:} \quad & g \\ \text{s.t.:} \quad & \sum_{b\in B} B_b^y = \mathbb{1}_{\mathcal{B}}, \\ & B_b^y \in \mathrm{Pos}(\mathcal{B}). \end{aligned}$$

- Iterate between SDP-1 and SDP-2 until desired numerical precision is reached.

Supplementary material: Monogamy-of-Entanglement games

Supplementary material: Motivation for monogamy-of-entanglement games

Motivation for monogamy-of-entanglement games

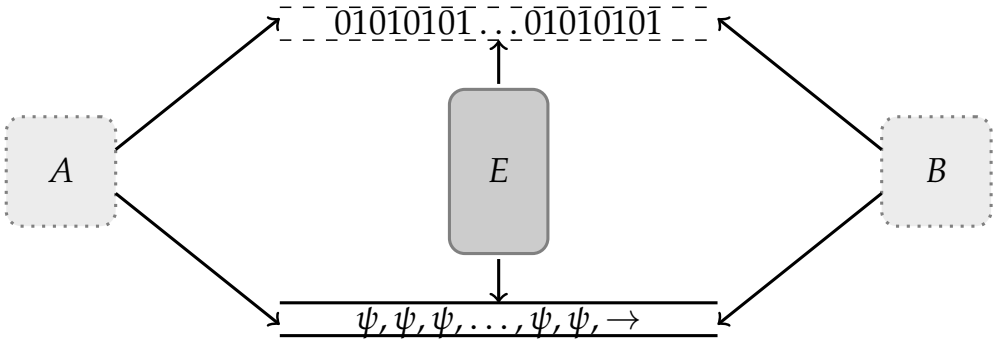
Monogamy-of-entanglement games were introduced to study *quantum cryptography*.

Motivation for monogamy-of-entanglement games

Monogamy-of-entanglement games were introduced to study *quantum cryptography*.

The BB84 protocol is the first quantum cryptographic protocol and is referred to as a *quantum key distribution* (QKD) scheme.

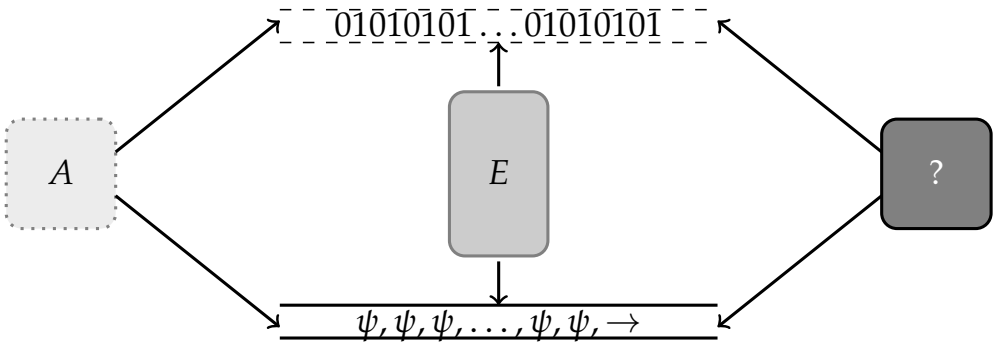
- Alice wants to send private key to Bob. Eve may eavesdrop and compromise security. BB84 relies on fundamental principles of quantum mechanics to determine if Eve eavesdropped.



Motivation for monogamy-of-entanglement games

Monogamy-of-entanglement games were introduced to study *quantum cryptography*.
The BB84 protocol is the first quantum cryptographic protocol and is referred to as a *quantum key distribution* (QKD) scheme.

- Alice wants to send private key to Bob. Eve may eavesdrop and compromise security. BB84 relies on fundamental principles of quantum mechanics to determine if Eve eavesdropped.



The authors showed that the above protocol is secure even if Bob's device is untrusted[17].

[17] [Tomamichel, Fehr, Kaniewski, Wehner, (2013)]

The monogamy-of-entanglement property

Monogamy-of-entanglement games embody a fundamental monogamous property exhibited by entangled states:

The monogamy-of-entanglement property

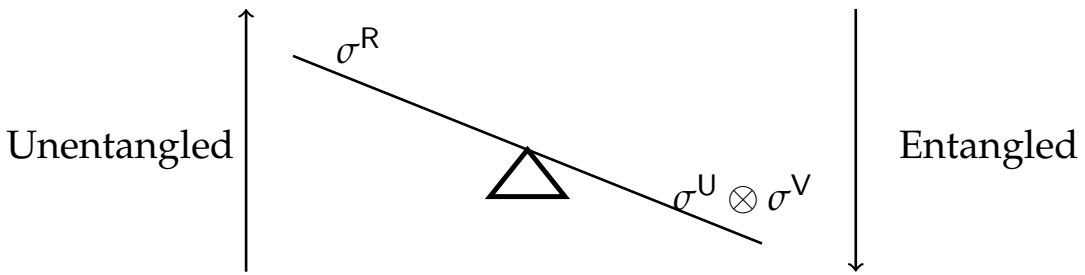
Monogamy-of-entanglement games embody a fundamental monogamous property exhibited by entangled states:

Consider $\sigma = \sigma^{\mathsf{U}} \otimes \sigma^{\mathsf{R}} \otimes \sigma^{\mathsf{V}}$.

- If $\sigma^{\mathsf{U}} \otimes \sigma^{\mathsf{V}}$ are *maximally entangled* (that is):

$$\sigma^{\mathsf{U}} = \begin{pmatrix} \frac{1}{n} & & \\ & \ddots & \\ & & \frac{1}{n} \end{pmatrix},$$

then σ^{R} is completely unentangled with σ^{U} and σ^{V}.



Similar to a "see-saw": When $\sigma^{\mathsf{U}} \otimes \sigma^{\mathsf{V}}$ cannot be more entangled, the state σ^{R} has *no* entanglement with $\sigma^{\mathsf{U}} \otimes \sigma^{\mathsf{V}}$.

Standard quantum strategies for monogamy-of-entanglement games

A *standard quantum strategy* consists of a tripartite state $\rho \in \mathrm{D}(\mathcal{U} \otimes \mathcal{R} \otimes \mathcal{V})$ and sets of local measurements for Alice and Bob.

- The winning probability for a monogamy-of-entanglement game using a standard quantum strategy is:

$$\sum_{\substack{x \in X \\ a \in A}} \pi(x) \left\langle A_a^x \otimes P_{a,x} \otimes B_a^x, \sigma \right\rangle.$$

The standard quantum value of a monogamy-of-entanglement game, G, denoted as $\omega^*(G)$, is the maximal winning probability for Alice and Bob over all standard quantum strategies.

Unentangled strategies for monogamy-of-entanglement games

In an *unentangled strategy*, the state σ prepared by Alice and Bob is fully separable, that is

$$\{\sigma_j^{\mathsf{R}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{R}), \quad \{\sigma_j^{\mathsf{U}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{U}), \quad \{\sigma_j^{\mathsf{V}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{V}),$$

such that

$$\sigma = \sum_{j \in \Delta} p(j) \sigma_j^{\mathsf{U}} \otimes \sigma_j^{\mathsf{R}} \otimes \sigma_j^{\mathsf{V}}.$$

Unentangled strategies for monogamy-of-entanglement games

In an *unentangled strategy*, the state σ prepared by Alice and Bob is fully separable, that is

$$\{\sigma_j^{\mathsf{R}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{R}), \quad \{\sigma_j^{\mathsf{U}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{U}), \quad \{\sigma_j^{\mathsf{V}} : j \in \Delta\} \subseteq \mathrm{D}(\mathcal{V}),$$

such that

$$\sigma = \sum_{j \in \Delta} p(j) \sigma_j^{\mathsf{U}} \otimes \sigma_j^{\mathsf{R}} \otimes \sigma_j^{\mathsf{V}}.$$

Winning probability for an unentangled strategy is given by:

$$\sum_{\substack{x \in X \\ a \in A}} \pi(x) \left\langle A_a^x \otimes P_{a,x} \otimes B_a^x, \sigma \right\rangle,$$

where σ is separable.
The *unentangled value*, denoted as $\omega(G)$, is the supremum of the winning probability over all unentangled strategies.

Unentangled value for monogamy-of-entanglement games

- For $\omega(G)$, we want the *best* Alice and Bob can do.
- Since σ is separable (no quantum correlations) we can imagine Alice and Bob optimizing functions $f : X \to A$ locally.

Unentangled value for monogamy-of-entanglement games

- For $\omega(G)$, we want the *best* Alice and Bob can do.
- Since σ is separable (no quantum correlations) we can imagine Alice and Bob optimizing functions $f : X \to A$ locally.

Alice and Bob only win when their outputs agree, and we assume that the measurements of the referee are positive semidefinite (from the definition for monogamy-of-entanglement games).

- For any monogamy-of-entanglement game, G, the unentangled value is:

$$\omega(G) = \max_{f:X\to A} \left\| \sum_{x\in X} \pi(x) P_{f(x),x} \right\|,$$

where the maximum is over all functions $f : X \to A$.

Supplementary material: Standard quantum and unentangled values of monogamy-of-entanglement games

A natural question for monogamy-of-entanglement games

- *Question:* For any monogamy-of-entanglement game, G, is it true that the *unentangled* and *standard quantum* values always coincide? In other words is it true that:

$$\omega(G) = \omega^*(G)$$

for all monogamy-of-entanglement games G?

A natural question for monogamy-of-entanglement games

- *Question:* For any monogamy-of-entanglement game, G, is it true that the *unentangled* and *standard quantum* values always coincide? In other words is it true that:

$$\omega(G) = \omega^*(G)$$

  for all monogamy-of-entanglement games G?

- *Answer:*
  - For certain cases: Yes.
  - In general: No.

$$\omega(G) = \omega^*(G)$$

In general: No.

Monogamy-of-entanglement games where $\omega(G) \neq \omega^*(G)$

There exists a monogamy-of-entanglement game, G, with $|X| = 4$ and $|A| = 3$ such that

$$\omega(G) < \omega^*(G).$$

1. Question and answer sets:

$$X = \{0, 1, 2, 3\}, \quad A = \{0, 1, 2\}.$$

2. Uniform probability for questions:

$$\pi(0) = \pi(1) = \pi(2) = \pi(3) = \frac{1}{4}.$$

3. Measurements defined by a mutually unbiased basis[18]:

$$\{P_{0,x}, P_{1,x}, P_{2,x}\}.$$

[18] $|u_x(a)^* u_{x'}(a)|^2 = 1/|A|$ for $P_{a,x} = u_x(a)u_x(a)^*, P_{a,x'} = u_{x'}(a)u_{x'}(a)^*$

Monogamy-of-entanglement games where $\omega(G) \neq \omega^*(G)$

- An exhaustive search over all unentangled strategies reveals an optimal unentangled value:

$$\omega(G) = \frac{3+\sqrt{5}}{8} \approx 0.6545.$$

- Alternatively, a computer search over standard quantum strategies and a heuristic approximation for the upper bound of $\omega^*(G)$ reveals that:

$$2/3 \geq \omega^*(G) \geq 0.6609.$$

This ability to compute upper bounds for extended nonlocal games is obtained from an adaptation of a technique known as the *QC hierarchy.*

$$\omega(G) = \omega^*(G)$$

For certain classes: Yes.

Monogamy games that obey $\omega(G) = \omega^*(G)$

Theorem (Johnston, Mittal, R, Watrous)

For any monogamy-of-entanglement game, G, for which $|X| = 2$:

$$\omega(G) = \omega^*(G).$$

Proof: Monogamy games that obey $\omega(G) = \omega^*(G)$

Recall that for any monogamy-of-entanglement, G, the standard quantum value may be written as

$$\omega^*(G) = \left\| \lambda \sum_{a \in A} A_a^0 \otimes P_{a,0} \otimes B_a^0 + (1-\lambda) \sum_{b \in A} A_b^1 \otimes P_{b,1} \otimes B_b^1 \right\|$$

Proof: Monogamy games that obey $\omega(G) = \omega^*(G)$

Recall that for any monogamy-of-entanglement, G, the standard quantum value may be written as

$$\omega^*(G) = \left\| \lambda \sum_{a \in A} A_a^0 \otimes P_{a,0} \otimes B_a^0 + (1-\lambda) \sum_{b \in A} A_b^1 \otimes P_{b,1} \otimes B_b^1 \right\|$$

Since $\|P\| \leq \|Q\|$ if $P \leq Q$ for any $P, Q \geq 0$:

$$\omega^*(G) \leq \left\| \lambda \sum_{a \in A} A_a^0 \otimes P_{a,0} \otimes \mathbb{1}_{\mathcal{V}} + (1-\lambda) \sum_{b \in A} \mathbb{1}_{\mathcal{U}} \otimes P_{b,1} \otimes B_b^1 \right\|$$

Proof: Monogamy games that obey $\omega(G) = \omega^*(G)$

Recall that for any monogamy-of-entanglement, G, the standard quantum value may be written as

$$\omega^*(G) = \left\| \lambda \sum_{a \in A} A_a^0 \otimes P_{a,0} \otimes B_a^0 + (1-\lambda) \sum_{b \in A} A_b^1 \otimes P_{b,1} \otimes B_b^1 \right\|$$

Since $\|P\| \leq \|Q\|$ if $P \leq Q$ for any $P, Q \geq 0$:

$$\omega^*(G) \leq \left\| \lambda \sum_{a \in A} A_a^0 \otimes P_{a,0} \otimes \mathbb{1}_{\mathcal{V}} + (1-\lambda) \sum_{b \in A} \mathbb{1}_{\mathcal{U}} \otimes P_{b,1} \otimes B_b^1 \right\|$$

Since $\sum_{a \in A} A_a^x = \sum_{b \in A} B_b^y = \mathbb{1}$ the above quantity is equal to:

$$\omega^*(G) \leq \left\| \lambda \sum_{a,b \in A} A_a^0 \otimes P_{a,0} \otimes B_b^1 + (1-\lambda) \sum_{a,b \in A} A_a^0 \otimes P_{b,1} \otimes B_b^1 \right\|.$$

Monogamy games that obey $\omega(G) = \omega^*(G)$

(Previous slide):

$$\omega^*(G) \leq \left\| \lambda \sum_{a,b \in A} A_a^0 \otimes P_{a,0} \otimes B_b^1 + (1-\lambda) \sum_{a,b \in A} A_a^0 \otimes P_{b,1} \otimes B_b^1 \right\|.$$

Monogamy games that obey $\omega(G) = \omega^*(G)$

(Previous slide):

$$\omega^*(G) \leq \left\| \lambda \sum_{a,b \in A} A_a^0 \otimes P_{a,0} \otimes B_b^1 + (1-\lambda) \sum_{a,b \in A} A_a^0 \otimes P_{b,1} \otimes B_b^1 \right\|.$$

Since $\langle A_a^0 \otimes B_b^1, A_{a'}^0 \otimes B_{b'}^1 \rangle = 0$ for $a \neq a'$ and $b \neq b'$ and noting that

$$\left\| \sum_k A_k \otimes \Pi_k \right\| = \max_k \| A_k \|$$

for any projective measurement $\{\Pi_k\}$, we have that

$$\left\| \sum_{(a,b) \in A} A_a^0 \otimes (\lambda P_{a,0} + (1-\lambda) P_{b,1}) \otimes B_b^1 \right\| \leq \max_{a,b \in A} \left\| \lambda P_{a,0} + (1-\lambda) P_{b,1} \right\|.$$

Monogamy games that obey $\omega(G) = \omega^*(G)$

(Previous slide):

$$\omega^*(G) \leq \left\| \lambda \sum_{a,b \in A} A_a^0 \otimes P_{a,0} \otimes B_b^1 + (1-\lambda) \sum_{a,b \in A} A_a^0 \otimes P_{b,1} \otimes B_b^1 \right\|.$$

Since $\langle A_a^0 \otimes B_b^1, A_{a'}^0 \otimes B_{b'}^1 \rangle = 0$ for $a \neq a'$ and $b \neq b'$ and noting that

$$\left\| \sum_k A_k \otimes \Pi_k \right\| = \max_k \| A_k \|$$

for any projective measurement $\{\Pi_k\}$, we have that

$$\left\| \sum_{(a,b) \in A} A_a^0 \otimes (\lambda P_{a,0} + (1-\lambda) P_{b,1}) \otimes B_b^1 \right\| \leq \max_{a,b \in A} \left\| \lambda P_{a,0} + (1-\lambda) P_{b,1} \right\|.$$

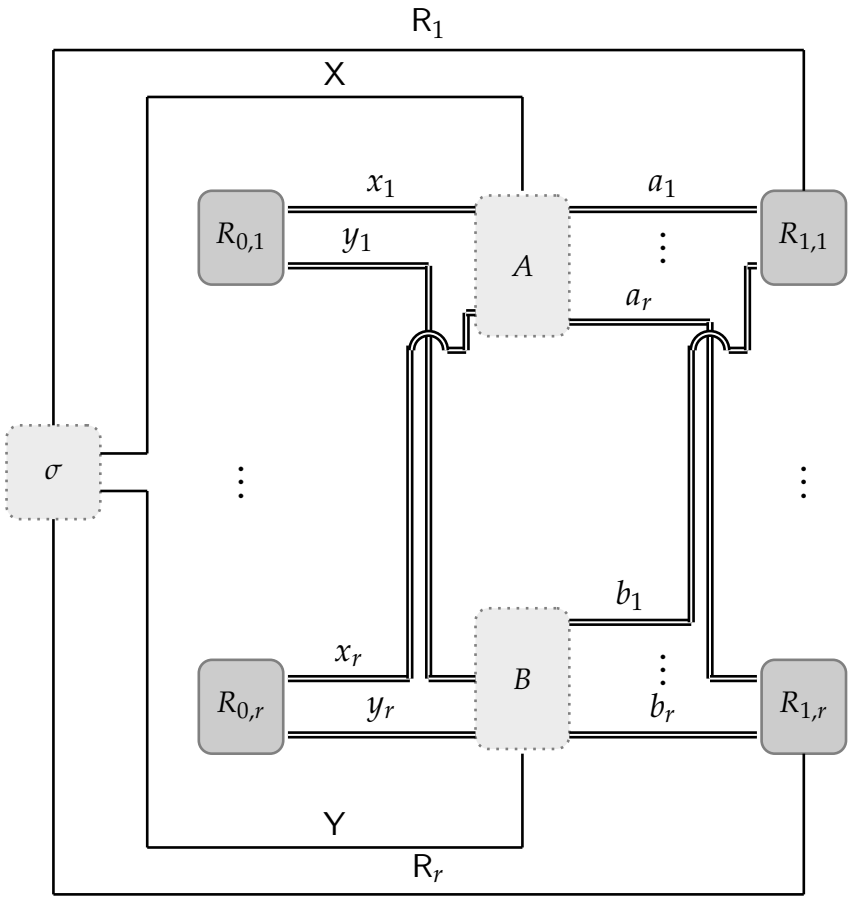
It follows by definition of the unentangled value that

$$\omega(G) = \max_{a,b \in A} \left\| \lambda P_{a,0} + (1-\lambda) P_{b,1} \right\|.$$

Supplementary material: Parallel repetition of monogamy-of-entanglement games

Parallel repetition of monogamy-of-entanglement games

- *Parallel repetition:* Run a monogamy-of-entanglement game, G, for n times in parallel, denoted as G^n.
- *Strong parallel repetition:* $\omega(G^n) = \omega(G)^n$



Question: Do all monogamy-of-entanglement games obey strong parallel repetition?

Parallel repetition of monogamy-of-entanglement games

- Recall:

$$\omega(G_{\mathrm{BB84}}) = \omega^*(G_{\mathrm{BB84}}) = \cos^2(\pi/8) \approx 0.8536.$$

- G_{BB84} obeys strong parallel repetition[19]:

$$\omega^*(G_{\mathrm{BB84}}^n) = \omega^*(G_{\mathrm{BB84}})^n = \left(\cos^2(\pi/8)\right)^n.$$

[19] Tomamichel, Fehr, Kaniewski, Wehner : "A Monogamy-of-Entanglement Game With Applications to Device-Independent Quantum Cryptography", (2013).

Upper bounds on strong parallel repetition for monogamy games

Theorem (Tomamichel, Fehr, Kaniewski, Wehner)

Let $G = (\pi, P)$ be a monogamy game where π is uniform over X. It holds that

$$\omega^*(G^n) \leq \left(\frac{1}{|X|} + \frac{|X|-1}{|X|} \sqrt{c(G)} \right)^n,$$

where $c(G)$ is the "maximal overlap of measurements" of the referee

$$c(G) = \max_{\substack{x,y \in X \\ x \neq y}} \max_{a,b \in A} \left\| \sqrt{P_{a,x}} \sqrt{P_{b,y}} \right\|^2.$$

Strong parallel repetition for certain monogamy games

Theorem (Johnston, Mittal, R, Watrous)

Let $G = (\pi, P)$ be a monogamy game where $|X| = 2$, π is uniform over X, and $P_{a,x}$ are projective operators. It holds that

$$\omega^*(G^n) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n.$$

A key proposition and lemma

Lemma

Let Π_0 and Π_1 be nonzero projection operators on $\mathbb{C}^n$. It holds that

$$\|\Pi_0 + \Pi_1\| = 1 + \|\Pi_0 \Pi_1\|.$$

Proposition

Let $G = (\pi, P)$ be a monogamy-of-entanglement game for which $X = \{0, 1\}$, π is uniform over X, and $P_{a,x}$ is a projection operator for each $x \in X$ and $a \in A$. It holds that

$$\omega(G) = \frac{1}{2} + \frac{1}{2} \max_{a,b \in A} \left\| P_{a,0} P_{b,1} \right\|.$$

Proof of proposition

Recall that the unentangled value for any monogamy game G is written as

$$\omega(G) = \max_{f:X\to A} \left\| \sum_{x\in X} \pi(x) P_{f(x),x} \right\|.$$

Assuming the lemma stating $\|\Pi_0 + \Pi_1\| = 1 + \|\Pi_0\Pi_1\|$, we have

$$\omega(G) = \max_{a,b\in A} \left\| \frac{P_{a,0} + P_{b,1}}{2} \right\| = \frac{1}{2} + \frac{1}{2} \max_{a,b\in A} \left\| P_{a,0} P_{b,1} \right\|.$$

Proof of theorem

From the proposition that

$$\omega(G) = \frac{1}{2} + \frac{1}{2}\sqrt{c(G)}.$$

Proof of theorem

From the proposition that

$$\omega(G) = \frac{1}{2} + \frac{1}{2}\sqrt{c(G)}.$$

Since this is an unentangled strategy, we can assume that Alice and Bob just play every instance optimally (since there is no quantum correlation). It follows then that

$$\omega(G^n) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n.$$

Proof of theorem

From the proposition that

$$\omega(G) = \frac{1}{2} + \frac{1}{2}\sqrt{c(G)}.$$

Since this is an unentangled strategy, we can assume that Alice and Bob just play every instance optimally (since there is no quantum correlation). It follows then that

$$\omega(G^n) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n.$$

Recall that the theorem from [Tomamichel, Fehr, Kaniewski, Wehner, (2013)] gives us

$$\omega^*(G^n) \leq \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n,$$

which gives us that $\omega^*(G^n) \leq \omega(G^n)$.

Proof of theorem

From the proposition that

$$\omega(G) = \frac{1}{2} + \frac{1}{2}\sqrt{c(G)}.$$

Since this is an unentangled strategy, we can assume that Alice and Bob just play every instance optimally (since there is no quantum correlation). It follows then that

$$\omega(G^n) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n.$$

Recall that the theorem from [Tomamichel, Fehr, Kaniewski, Wehner, (2013)] gives us

$$\omega^*(G^n) \leq \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n,$$

which gives us that $\omega^*(G^n) \leq \omega(G^n)$. Finally,

$$\omega^*(G^n) \geq \omega(G^n) \geq \left(\frac{1}{2} + \frac{1}{2}\max_{a,b\in A}\left\|P_{a,0}P_{b,1}\right\|\right)^n = \left(\frac{1}{2} + \frac{1}{2}\sqrt{c(G)}\right)^n.$$

Unentangled vs. standard quantum strategies for monogamy-of-entanglement games

Inputs ($\lvert X\rvert$)	Outputs ($\lvert A\rvert$)	$\omega^*(G) = \omega(G)$	$\omega^*(G^n) = \omega^*(G)^n$	$\omega_{\mathrm{ns}}(G^n) = \omega_{\mathrm{ns}}(G)^n$
2	≥ 1	yes	yes[20]	no
3	≥ 1	?	?	no
4	3	no	?	no

Question: What about $|X| = 3$?

- Proof technique fails for $|X| > 2$.
- Computational search:
  - Generate random monogamy-of-entanglement games where $|X| = 3$ and $|A| \geq 2$.
  - 10^8 random games generates, no counterexamples found.

[20] So long as the measurements used by the referee are projective and the probability distribution, π, from which the questions are asked is uniform.

Supplementary material: Misc. Questions

Supplementary material: Strategies of pure states and projective measurements

Strategies of pure states and projective measurements

Claim: For any strategy, there is an equivalent strategy where the state σ is pure and the sets of measurements for Alice and Bob are projective.

1. Either Alice or Bob may *purify* their state.
2. Non-projective measurements may be simulated by projective measurements as is done in *Naimark's theorem*.

Purifications of quantum states

Purification idea: Consider a state $\rho \in \mathrm{D}(\mathcal{X})$ in register X. We could, if we wish, view X as a subregister of some compound register (X, Y), and think of ρ as being obtained by

$$\rho = \mathrm{Tr}_{\mathcal{Y}}(uu^*)$$

for some pure state uu^* of (X, Y).

Purifications of quantum states

Purification idea: Consider a state $\rho \in \mathrm{D}(\mathcal{X})$ in register X. We could, if we wish, view X as a subregister of some compound register (X, Y), and think of ρ as being obtained by

$$\rho = \mathrm{Tr}_{\mathcal{Y}}(uu^*)$$

for some pure state uu^* of (X, Y).

Purification (formal): Let $P \in \mathrm{Pos}(\mathcal{X})$ and let $u \in \mathcal{X} \otimes \mathcal{Y}$. Then u is a purification of P iff

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = P.$$

Existence of purifications

We know that purifications must exist as a corollary to the following theorem:

Theorem

Let $\mathcal{X}$ and $\mathcal{Y}$ be cEs and let $P \in \mathrm{Pos}(\mathcal{X})$. There exists a vector $u \in \mathcal{X} \otimes \mathcal{Y}$ s.t.

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = P$$

iff $\dim(\mathcal{Y}) \geq \mathrm{rank}(P)$.

Existence of purifications

We know that purifications must exist as a corollary to the following theorem:

Theorem

Let $\mathcal{X}$ and $\mathcal{Y}$ be cEs and let $P \in \mathrm{Pos}(\mathcal{X})$. There exists a vector $u \in \mathcal{X} \otimes \mathcal{Y}$ s.t.

$$\mathrm{Tr}_{\mathcal{Y}}(uu^*) = P$$

iff $\dim(\mathcal{Y}) \geq \mathrm{rank}(P)$.

The corollary being:

Corollary

Let $\mathcal{X}$ and $\mathcal{Y}$ be cEs where $\dim(\mathcal{Y}) \geq \dim(\mathcal{X})$. For every $P \in \mathrm{Pos}(\mathcal{X})$, there exists a vector $u \in \mathcal{X} \otimes \mathcal{Y}$ s.t. $\mathrm{Tr}_{\mathcal{Y}}(uu^*) = P$.

Naimark's theorem

Idea: Relationship between arbitrary measurements and projective measurements. Any measurement may be viewed as a projective measurement on a compound register that includes the original register as a subregister.

Naimark's theorem

Idea: Relationship between arbitrary measurements and projective measurements. Any measurement may be viewed as a projective measurement on a compound register that includes the original register as a subregister.

Theorem

Let $\mathcal{X}$ be a cEs, let X be an alphabet, let $\Pi : \Sigma \to \mathrm{Pos}(\mathcal{X})$ be a measurement, and let $\mathcal{Y} = \mathbb{C}^{\Sigma}$. There exists an isometery $A \in \mathrm{U}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ s.t.

$$\Pi_a = A^* \left(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a,} \right) A$$

for every $a \in \Sigma$.

Naimark's theorem

Proof.

Let $A \in \mathrm{L}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ where

$$A = \sum_{a \in \Sigma} \sqrt{\Pi_a} \otimes e_a.$$

It can be checked that

$$A^* A = \sum_{a \in \Sigma} \Pi_a = \mathbb{1}_{\mathcal{X}},$$

which implies that A is an isometry. $\square$

Corollary of Naimark

As a corollary to Naimark's theorem, we have that

Corollary

Let $\mathcal{X}$ be a cEs, let Σ be an alphabet, and let $\{M_a : a \in \Sigma\} \subset \mathrm{Pos}(\mathcal{X})$ be a measurement. Take $\mathcal{Y} = \mathbb{C}^\Sigma$ and let $u \in \mathcal{Y}$ be a unit vector. There exists a projective measurement $\{\Pi_a : a \in \Sigma\} \subset \mathrm{Proj}(\mathcal{X} \otimes \mathcal{Y})$ s.t.

$$\left\langle \Pi_a, X \otimes uu^* \right\rangle = \left\langle M_a, X \right\rangle$$

for all $X \in \mathrm{L}(\mathcal{X})$.

Proof of corollary

Proof.

Let $A \in \mathrm{U}(\mathcal{X}, \mathcal{X} \otimes \mathcal{Y})$ be the isometry (that arises from Naimark's theorem). Let $U \in \mathrm{U}(\mathcal{X} \otimes Y)$ be a unitary operator where

$$U(\mathbb{1}_{\mathcal{X}} \otimes u) = A$$

is satisfied, and define $\{\Pi_a : a \in \Sigma\} \subset \mathrm{Pos}(\mathcal{X} \otimes \mathcal{Y})$ as

$$\Pi_a = U^* \left(\mathbb{1}_{\mathcal{X}} \otimes E_{a,a}\right) U$$

for each $a \in \Sigma$. It holds that:

$$\begin{aligned}
\left\langle \Pi_a, X \otimes uu^* \right\rangle &= \left\langle (\mathbb{1}_{\mathcal{X}} \otimes u^*) U^* (\mathbb{1}_{\mathcal{X}} \otimes E_{a,a} U (\mathbb{1}_{\mathcal{X}} \otimes u), X \right\rangle \\
&= \left\langle A^* (\mathbb{1}_{\mathcal{X}} \otimes E_{a,a}) A, X \right\rangle \\
&= \left\langle M_a, X \right\rangle,
\end{aligned}$$

for all $a \in \Sigma$. $\square$

Supplementary material:
The extended QC hierarchy and dimensionality

The extended QC hierarchy and dimensionality

Note: In the original QC hierarchy, there is no constraint on the dimension of the state σ shared by Alice and Bob.

[21] "Bounding the set of finite dimensional quantum correlations": Navascues, Vertesi

The extended QC hierarchy and dimensionality

Note: In the original QC hierarchy, there is no constraint on the dimension of the state σ shared by Alice and Bob.

Note: The same is true for the extended QC hierarchy.

[21] "Bounding the set of finite dimensional quantum correlations": Navascues, Vertesi

The extended QC hierarchy and dimensionality

Note: In the original QC hierarchy, there is no constraint on the dimension of the state σ shared by Alice and Bob.

Note: The same is true for the extended QC hierarchy.

Note: If, however, one wishes to place bounds on the dimension of σ, this was considered in[21] w.r.t. the original QC hierarchy.

[21] "Bounding the set of finite dimensional quantum correlations": Navascues, Vertesi

Supplementary material:
XX