

Monogamy-of-entanglement games

Nonlocal Games Seminar

Vincent Russo

University of Waterloo

June 22, 2016

UNIVERSITY OF
WATERLOO



Outline

Nonlocal games

Extended nonlocal games

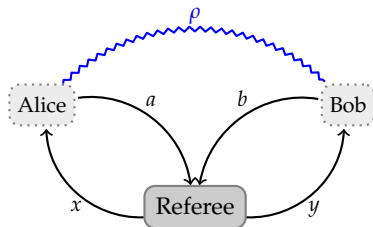
Monogamy-of-entanglement games

Supplementary material

Nonlocal games

Nonlocal games

A *nonlocal game* is a cooperative game played between *Alice* and *Bob* against a *referee*.



1. Question and answer sets: (Σ_A, Σ_B) and (Γ_A, Γ_B)
2. Distributions on question pairs: $\pi : \Sigma_A \times \Sigma_B \rightarrow [0, 1]$
3. A predicate $V : \Gamma_A \times \Gamma_B \times \Sigma_A \times \Sigma_B \rightarrow \{0, 1\}$, where

$$V(a, b|x, y) = \begin{cases} 1 & \text{if Alice and Bob win} \\ 0 & \text{if Alice and Bob lose} \end{cases},$$

Strategies and values for nonlocal games

Alice and Bob could use different types of *strategies*:

- ▶ *Classical strategies*: Alice and Bob answer deterministically, determined by functions of $x \in \Sigma_A$ and $y \in \Sigma_B$.
- ▶ *Quantum strategies*: Alice and Bob share a joint quantum system $\rho \in \mathcal{D}(\mathcal{A} \otimes \mathcal{B})$ and allow their answers to be outcomes of measurements on this shared system.

Strategies and values for nonlocal games

Alice and Bob could use different types of *strategies*:

- ▶ *Classical strategies*: Alice and Bob answer deterministically, determined by functions of $x \in \Sigma_A$ and $y \in \Sigma_B$.
- ▶ *Quantum strategies*: Alice and Bob share a joint quantum system $\rho \in \mathcal{D}(\mathcal{A} \otimes \mathcal{B})$ and allow their answers to be outcomes of measurements on this shared system.

The *value* of a nonlocal game is the maximal winning probability for the players to win over all strategies of a specified type.

For a nonlocal game, G , we denote the classical and quantum values as

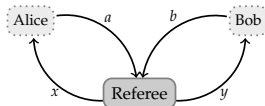
- ▶ Classical value: $\omega(G)$,
- ▶ Quantum value: $\omega^*(G)$.

Example: The CHSH game

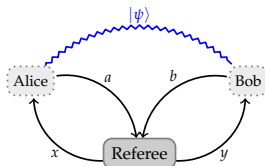
The CHSH game (G_{CHSH}). Winning condition iff $a \oplus b = x \wedge y$.

$$\omega(G_{\text{CHSH}}) < \omega^*(G_{\text{CHSH}})$$

► $\omega(G_{\text{CHSH}}) = \frac{3}{4} = 0.75$:



► $\omega^*(G_{\text{CHSH}}) = \cos^2(\frac{\pi}{8}) \approx 0.8536$:

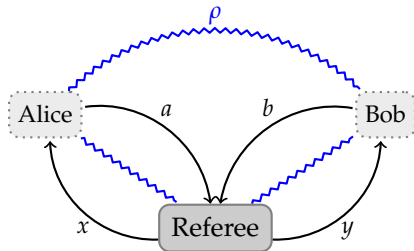


Demo Time: CHSH Game in QETLAB
CHSH_GAME.M

Extended nonlocal games

Extended nonlocal games

An *extended nonlocal game* is a nonlocal game where the *referee* also holds a quantum system that he measures provided by Alice and Bob.



1. Question and answer sets (Σ_A, Σ_B) and (Γ_A, Γ_B) .
2. Distribution on question pairs: $\pi : \Sigma_A \times \Sigma_B \rightarrow [0, 1]$.
3. A measurement operator $V : \Gamma_A \times \Gamma_B \times \Sigma_A \times \Sigma_B \rightarrow \text{Pos}(\mathcal{R})$.

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:

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

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

$$V(a, b|x, y) \in \text{Pos}(\mathcal{R}).$$

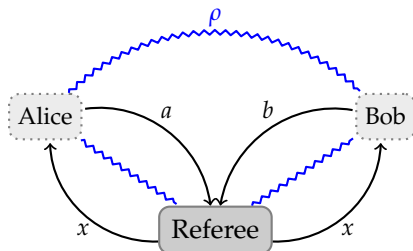
The respective winning and losing probabilities are given by

$$\left\langle V(a, b|x, y), \rho_{a,b}^{x,y} \right\rangle \quad \text{and} \quad \left\langle \mathbb{1} - V(a, b|x, y), \rho_{a,b}^{x,y} \right\rangle.$$

Monogamy-of-entanglement games

Monogamy-of-entanglement games

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



1. Same question and answer sets: $\Sigma = \Sigma_A = \Sigma_B$ and $\Gamma = \Gamma_A = \Gamma_B$.
2. Alice and Bob get the same question: $\pi(x, y) = 0$ for $x \neq y$.
3. Referee's measurement operator: $R : \Sigma \times \Gamma \rightarrow \text{Pos}(\mathcal{R})$.
4. Winning condition: Iff Alice's output, Bob's output, and the referee's measurement output are the *same*.

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

Standard quantum strategies for monogamy-of-entanglement games

- ▶ The expected *pay-off* for a monogamy-of-entanglement game, G using a standard quantum strategy is:

$$\sum_{x \in \Sigma} \pi(x) \sum_{a \in \Gamma} \left\langle R(a|x) \otimes A_a^x \otimes B_a^x, \rho \right\rangle.$$

- ▶ Since ρ just needs to be a valid density matrix, we use convexity to assume that ρ is pure (rank-one):

$$\omega^*(G) = \left\| \sum_{x \in \Sigma} \pi(x) \sum_{a \in \Gamma} R(a|x) \otimes A_a^x \otimes B_a^x \right\|$$

Unentangled strategies for monogamy-of-entanglement games

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:

$$\omega(G) = \max_{f: \Sigma \rightarrow \Gamma} \left\| \sum_{x \in \Sigma} \pi(x) R(f(x)|x) \right\|.$$

for choice of measurements $\{A_a^x\}$ for Alice and $\{B_b^y\}$ for Bob.

The BB84 monogamy-of-entanglement game

The BB84 game (G_{BB84} for short)[¶] is defined by:

1. Question and answer sets:

$$\Sigma = \Gamma = \{0, 1\},$$

2. Uniform probability for questions:

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

3. Measurements defined by the BB84 bases:

$$\text{For } x = 0: \quad R(0|0) = |0\rangle\langle 0|, \quad R(1|0) = |1\rangle\langle 1|$$

$$\text{For } x = 1: \quad R(0|1) = |+\rangle\langle +|, \quad R(1|1) = |-\rangle\langle -|$$

The *unentangled* and *standard quantum* values for G_{BB84} coincide:

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

[¶] G_{BB84} was introduced in [Tomamichel, Fehr, Kaniewski, Wehner, (2013)].

Demo Time: BB84 Game
BB84_GAME.M

Exhaustive search over unentangled strategies

Consider the following SDP:

Primal Problem: (γ)

$$\begin{aligned} \max: \quad & \sum_{x \in \Sigma} \pi(x) \left\langle R(f(x)|x), \rho \right\rangle \\ \text{s.t.:} \quad & \text{Tr}(\rho) = 1, \quad (\rho \text{ is pure}). \\ & \rho \geq 0, \quad (\rho \text{ is PSD}). \end{aligned}$$

We cycle over all possible choices of $f(x) \rightarrow a$ and run the above SDP. The best we can do is represented by $\max(\gamma)$ over all such choices.

- Calculating $\max(\gamma)$ is now not an SDP, but for small values of $|\Sigma|$ and $|\Gamma|$, we can brute force over every possible combination to obtain the maximum.

Demo Time: Calculating the unentangled value
UNENTANGLED_MOE_2IN_2OUT.M

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 ?

Demo Time: Random Monogamy Games

RANDOM_MOE_GAMES.M

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 $|\Sigma| = 4$ and $|\Gamma| = 3$ such that

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

1. Question and answer sets:

$$\Sigma = \{0, 1, 2, 3\}, \quad \Gamma = \{0, 1, 2\}.$$

2. Uniform probability for questions:

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

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

$$\{R(0|x), R(1|x), R(2|x)\}.$$

[¶] $|u_x(a)^* u_{x'}(a)|^2 = 1/|\Gamma|$ for $R(a|x) = u_x(a)u_x(a)^*$, $R(a|x') = u_{x'}(a)u_{x'}(a)^*$

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 *NPA hierarchy*.

Demo Time: MUB game
MUB_4_3_GAME.M

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

For certain classes, Yes.

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

Theorem

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

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

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

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

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

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

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

$$\omega^*(G) \leq \left\| \lambda \sum_{a \in \Gamma} R(a|0) \otimes A_a^0 \otimes \mathbb{1}_B + (1 - \lambda) \sum_{b \in \Gamma} R(b|1) \otimes \mathbb{1}_A \otimes B_b^1 \right\|$$

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

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

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

$$\omega^*(G) \leq \left\| \lambda \sum_{a \in \Gamma} R(a|0) \otimes A_a^0 \otimes \mathbb{1}_B + (1 - \lambda) \sum_{b \in \Gamma} R(b|1) \otimes \mathbb{1}_A \otimes B_b^1 \right\|$$

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

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

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

(Previous slide):

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

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

(Previous slide):

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

Since $\{A_a^0 \otimes B_b^1 : a, b \in \Gamma\}$ are pairwise orthogonal projections ($\langle A_a^0 \otimes B_b^1, A_{a'} \otimes B_{b'} \rangle = 0$ for $a \neq a'$ and $b \neq b'$) we have

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

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

(Previous slide):

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

Since $\{A_a^0 \otimes B_b^1 : a, b \in \Gamma\}$ are pairwise orthogonal projections ($\langle A_a^0 \otimes B_b^1, A_{a'} \otimes B_{b'} \rangle = 0$ for $a \neq a'$ and $b \neq b'$) we have

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

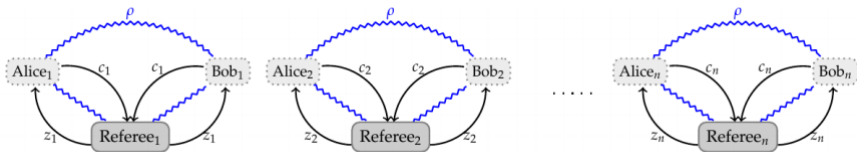
Every entangled strategy is equivalent to one where Alice and Bob use projective measurements so

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

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:

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

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

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

[¶][Tomamichel, Fehr, Kaniewski, Weher, (2013)]

Demo Time: Strong parallel repetition of BB84
BB84_PARALLEL_REP.M

Strong parallel repetition for certain monogamy-of-entanglement games

Theorem (Johnston, Mittal, R, Watrous)

Let $G = (\pi, R)$ be a monogamy-of-entanglement game for which $\Sigma_A = \{0, 1\}$, π is uniform over Σ_A , and $R(a|x)$ is a projection operator. It holds that

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

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

$$c(G) = \max_{\substack{x, y \in \Sigma_A \\ x \neq y}} \max_{a, b \in \Gamma_A} \left\| \sqrt{R(a|x)} \sqrt{R(b|y)} \right\|^2$$

A key proposition and lemma

Proposition

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

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

Lemma

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

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

Proof of proposition

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

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

The lower bound on $\omega(G)^*$ is obtained from [TFWK13][¶]. The upper bound follows from the fact that Alice and Bob can just play the optimal strategy for every n :

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

[¶][Tomamichel, Fehr, Kaniweski, Wehner (2013)]

Open questions

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

Inputs ($ \Sigma $)	Outputs ($ \Gamma $)	$\omega^*(G) = \omega(G)$	$\omega^*(G^n) = \omega^*(G)^n$	$\omega_{\text{ns}}(G^n) = \omega_{\text{ns}}(G)^n$
2	$ \Gamma \geq 1$	yes	yes [¶]	no
3	$ \Gamma \geq 1$?	?	no
4	3	no	?	no

Question: What about $|\Sigma| = 3$?

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

[¶]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

Supplementary material: Extended nonlocal games

Winning probability for standard quantum strategies

The winning probability is given by the following equation:

$$\sum_{x,y} \pi(x,y) \sum_{a,b} \frac{\langle V(a,b|x,y), \text{Tr}_{\mathcal{A} \otimes \mathcal{B}} (\mathbb{1}_{\mathcal{R}} \otimes A_a^x \otimes B_b^y) \rho \rangle}{\text{Tr}(\mathbb{1}_{\mathcal{R}} \otimes A_a^x \otimes B_b^y) \rho} \text{Tr}(\mathbb{1}_{\mathcal{R}} \otimes A_a^x \otimes B_b^y) \rho$$

The probabilities cancel giving

$$\sum_{x,y} \pi(x,y) \sum_{a,b} \text{Tr}(V(a,b|x,y) \text{Tr}_{\mathcal{A} \otimes \mathcal{B}} (\mathbb{1}_{\mathcal{R}} \otimes A_a^x \otimes B_b^y) \rho)$$

The trace operator slips past the $\mathbb{1}_{\mathcal{R}}$ giving

$$\sum_{x,y} \pi(x,y) \sum_{a,b} \text{Tr}(V(a,b|x,y) \otimes (A_a^x \otimes B_b^y) \rho)$$

Writing the trace in terms of the inner product, we have that

$$\sum_{x,y} \pi(x,y) \sum_{a,b} \left\langle V(a,b|x,y) \otimes A_a^x \otimes B_b^y, \rho \right\rangle.$$

Values of nonlocal games

The *value* of a game is the maximal winning probability of the players, where the winning probability for a choice of a, b, x, y is

- ▶ Classical:

$$\omega(G) = \max_{(a,b) \in \Gamma} \sum_{(x,y) \in \Sigma} V(f(x), g(y) | x, y),$$

where the max is over all functions $f : \Sigma_A \rightarrow \Gamma_A$ and $g : \Sigma_B \rightarrow \Gamma_B$.

- ▶ Quantum:

$$\omega^*(G) = \sup \sum_{(x,y) \in \Sigma} \pi(x, y) \sum_{(a,b) \in \Gamma} V(a, b | x, y)$$

Measurements may be assumed to be projective

WLOG, we may assume that Alice and Bob's measurements are projective since:

- ▶ Alice and Bob may extend the sizes of their Hilbert spaces,
- ▶ Naimark's theorem states that any strategy using non-projective measurements can be simulated by a strategy with projective measurements.

Supplementary material:
Monogamy-of-entanglement games

Pure strategies are sufficient

Recall that the pay-off for a standard quantum strategy is given by

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} \left\langle V(a,b|x,y) \otimes A_a^x \otimes B_b^y, \rho \right\rangle.$$

WLOG, ρ can be assumed to be pure and the measurement operators projective since one could increase the dimension of the Hilbert space, i.e.:

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} u^* (V(a,b|x,y) \otimes A_a^x \otimes B_b^y) u,$$

where $\rho = uu^*$ with $u \in \mathcal{R} \otimes \mathcal{A} \otimes \mathcal{B}$. This follows from Naimark's theorem (next slide).

Pure strategies are sufficient: Naimark's theorem

Let $u \in \mathcal{R} \otimes \mathcal{A} \otimes \mathcal{B}$, $w_0 \in \mathbb{C}^{\Gamma_A}$. Define

$$v = u \otimes w_0 \in \mathcal{R} \otimes \mathcal{A} \otimes \mathcal{B} \otimes \mathbb{C}^{\Gamma_A} \quad \text{and} \quad \tilde{A}_a^x = U^* (\mathbb{1}_{\mathcal{A}} \otimes E_{a,a}) U,$$

where $U \in \mathcal{U}(\mathcal{A} \otimes \mathbb{C}^{\Gamma_A})$ such that

$$U = w \otimes w_0 \rightarrow \sum_{a \in \Gamma_A} \sqrt{A_a^x} w \otimes e_a \quad (\forall w \in \mathcal{A}).$$

It holds that $\tilde{A}_a^x \in \text{Proj}(\mathcal{A})$ and hence

$$\tilde{A}_a^x v = U^* (\mathbb{1}_{\mathcal{A}} \otimes E_{a,a}) U (u \otimes w_0) = U^* \sqrt{A_a^x} u \otimes e_a,$$

and $\tilde{A}_a^x = \left(\tilde{A}_a^x \right)^* \left(\tilde{A}_a^x \right)$. Note ¶.

¶ A similar argument holds for Bob's measurements.

The BB84 game: Unentangled value

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

$$\omega(G) = \max_{f: \Sigma \rightarrow \Gamma} \left\| \sum_{x \in \Sigma} \pi(x) R(f(x)|x) \right\|$$

Recall, G_{BB84} has

$$\pi(0) = \pi(1) = 1/2 \quad \text{and} \quad \Sigma = \Gamma = \{0, 1\}.$$

So we have that:

$$\begin{aligned} \omega(G_{\text{BB84}}) &= \max_{f: \Sigma \rightarrow \Gamma} \left\| \frac{1}{2} R(f(x)|0) + \frac{1}{2} R(f(x)|1) \right\| \\ &= \frac{1}{2} \| |0\rangle\langle 0| + |+\rangle\langle +| \| + \frac{1}{2} \| |1\rangle\langle 1| + |-\rangle\langle -| \| \\ &= \frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^2(\pi/8). \end{aligned}$$

The BB84 game: Standard quantum value

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

$$\omega^*(G) = \left\| \sum_{x \in \Sigma} \pi(x) \sum_{a \in \Gamma} R(a|x) \otimes A_a^x \otimes B_a^x \right\|.$$

1. Alice and Bob send the following state to the referee:

$$v_{\pm} = \cos(\pi/8)|0\rangle \pm \sin(\pi/8)|1\rangle.$$

2. Alice and Bob always output $a = 0$ and have measurements:

$$A_0^0 = v_+ v_+^*, \quad A_0^1 = v_- v_-^*, \quad B_0^0 = B_0^1 = \mathbb{1}$$

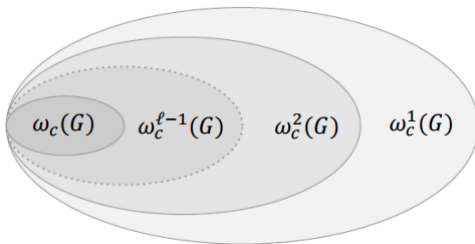
Plugging this into the standard quantum value formula:

$$\omega^*(G) = \left\| \frac{1}{2} (|0\rangle\langle 0| \otimes A_0^0 \otimes B_0^0 + |1\rangle\langle 1| \otimes A_0^0 \otimes B_0^0) + \right. \\ \left. \frac{1}{2} (|+\rangle\langle +| \otimes A_0^1 \otimes B_0^1 + |-\rangle\langle -| \otimes A_0^1 \otimes B_0^1) \right\| = \cos^2(\pi/8)$$

Supplementary material:
Upper bounds for extended nonlocal games

Upper bounds for nonlocal games

- ▶ The NPA 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, ℓ 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 .



[¶][Navascués, Pironio, and Acín, (2008)]

NPA hierarchy: Level 1

For a nonlocal game, the pay-off for a commuting measurement strategy is[¶]

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} V(a,b|x,y) \langle A_a^x B_b^y, \rho \rangle.$$

[¶]for $[A_a^x, B_b^y] = 0$, $\{A_a^x\}, \{B_b^y\} \subset \text{Pos}(\mathcal{H})$, and $\rho \in \mathcal{D}(\mathcal{H})$.

NPA hierarchy: Level 1

For a nonlocal game, the pay-off for a commuting measurement strategy is[¶]

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} V(a,b|x,y) \langle A_a^x B_b^y, \rho \rangle.$$

Define a Gram matrix with entries:

$$C((x,a),(y,b)) = \langle A_a^x B_b^y, \rho \rangle.$$

[¶]for $[A_a^x, B_b^y] = 0$, $\{A_a^x\}, \{B_b^y\} \subset \text{Pos}(\mathcal{H})$, and $\rho \in D(\mathcal{H})$.

NPA hierarchy: Level 1

For a nonlocal game, the pay-off for a commuting measurement strategy is[¶]

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} V(a,b|x,y) \langle A_a^x B_b^y, \rho \rangle.$$

Define a Gram matrix with entries:

$$C((x,a),(y,b)) = \langle A_a^x B_b^y, \rho \rangle.$$

The full block-matrix is

$$C = \left(\begin{array}{c|c} \langle A_a^x A_{a'}^{x'}, \rho \rangle & \langle A_a^x B_b^y, \rho \rangle \\ \hline \langle B_b^y A_a^x, \rho \rangle & \langle B_b^y B_{b'}^{y'}, \rho \rangle \end{array} \right)$$

- ▶ If the entries in C come from a commuting measurement strategy, C will satisfy *certain properties*.
- ▶ These properties are verifiable via an SDP.

[¶]for $[A_a^x, B_b^y] = 0$, $\{A_a^x\}, \{B_b^y\} \subset \text{Pos}(\mathcal{H})$, and $\rho \in \mathcal{D}(\mathcal{H})$.

Matrix constraints

As mentioned, the matrix C satisfies a number of constraints:

- ▶ It is positive semidefinite (by definition from the fact that it is a Gram matrix)
- ▶ Normalization: $C(1, 1) = 1$.
- ▶ Commutation:

$$C((x, a), (y, b)) = C((y, b), (x, a))$$

- ▶ Measurements sum to identity:

$$\sum_{(x,a)} C((x, a), (y, b)) = C(1, (y, b))$$

$$\sum_{(y,b)} C((x, a), (y, b)) = C((x, a), 1).$$

- ▶ Measurements are projective:

$$C(1, (y, b)) = C((y, b), (y, b))$$

$$C((x, a), 1) = C((x, a), (x, a))$$

Pseudo commuting measurement assemblages

If these properties are satisfied, we say that C is a 1-*st order pseudo commuting measurement assemblage*.

- ▶ By imposing more structure on this matrix, we get closer to the set of commuting measurement operators.
- ▶ Indexing correspondence between strings and operators:

$$A_a^x \leftrightarrow (x, a) \quad \text{and} \quad A_{a_1}^{x_1} \cdots A_{a_n}^{x_n} \leftrightarrow (x_1, a_1) \cdots (x_n, a_n)$$

Analogous for B_b^y operators.

Pseudo commuting measurement assemblages

If these properties are satisfied, we say that C is a *1-st order pseudo commuting measurement assemblage*.

- ▶ By imposing more structure on this matrix, we get closer to the set of commuting measurement operators.
- ▶ Indexing correspondence between strings and operators:

$$A_a^x \leftrightarrow (x, a) \quad \text{and} \quad A_{a_1}^{x_1} \cdots A_{a_n}^{x_n} \leftrightarrow (x_1, a_1) \cdots (x_n, a_n)$$

Analogous for B_b^y operators.

Define the alphabets

$$\Delta_A^{\leq \ell} = \{\epsilon\} \cup (\Sigma_A \times \Gamma_A)^{\leq \ell} \quad \text{and} \quad \Delta_B^{\leq \ell} = \{\epsilon\} \cup (\Sigma_B \times \Gamma_B)^{\leq \ell}.$$

The ℓ -th order pseudo commuting measurement assemblage is

$$C^{(\ell)} = \left(\frac{\Delta_A^{\leq \ell} \cup \Delta_{\bar{A}}^{\leq \ell}}{\Delta_{\bar{B}}^{\leq \ell} \cup \Delta_{\bar{A}}^{\leq \ell}} \middle| \frac{\Delta_{\bar{A}}^{\leq \ell} \cup \Delta_B^{\leq \ell}}{\Delta_{\bar{B}}^{\leq \ell} \cup \Delta_{\bar{B}}^{\leq \ell}} \right)$$

NPA hierarchy theorem

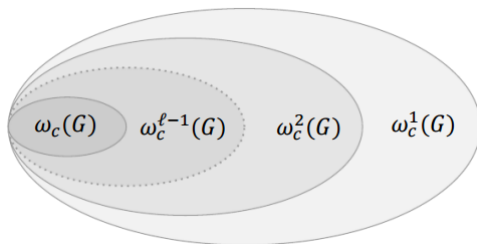
For some finite level ℓ , the pay-off for a commuting measurement strategy for a nonlocal game can be defined by

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} V(a,b|x,y) C^{(\ell)}.$$

Upper bounds for extended nonlocal games

Extended NPA hierarchy:

- ▶ Uses the same idea as the NPA hierarchy. (For $\dim(\mathcal{R}) = 1$, the NPA hierarchy is a special case.)
- ▶ Enables one to compute *upper bounds* on the *standard quantum value* for *extended nonlocal games*.
- ▶ Same idea as before, only now we need to take into account the actions of the referee.



Commuting measurement strategies

A *commuting measurement strategy* consists of a finite-dimensional complex Euclidean space \mathcal{H} as well as the following:

- ▶ Shared state: $\rho \in \mathcal{R} \otimes \mathcal{H}$.
- ▶ Measurements: $\{A_a^x\} \subset \text{Pos}(\mathcal{H})$, $\{B_b^y\} \subset \text{Pos}(\mathcal{H})$,
where $[A_a^x, B_b^y] = 0$ for all x, y, a, b .

Commuting measurement strategies

A *commuting measurement strategy* consists of a finite-dimensional complex Euclidean space \mathcal{H} as well as the following:

- ▶ Shared state: $\rho \in \mathcal{R} \otimes \mathcal{H}$.
- ▶ Measurements: $\{A_a^x\} \subset \text{Pos}(\mathcal{H})$, $\{B_b^y\} \subset \text{Pos}(\mathcal{H})$,
where $[A_a^x, B_b^y] = 0$ for all x, y, a, b .

The expected *pay-off* for a commuting measurement strategy is given by:

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} \left\langle V(a,b|x,y) \otimes A_a^x B_b^y, \rho \right\rangle$$

The *commuting measurement value*, denoted as $\omega_c(G)$, is the supremum of the pay-off over all commuting measurement strategies.

Extended NPA hierarchy

Same idea, but now we're taking into account the referee, and therefore have a larger matrix.

For each ℓ , now consider block matrices

$$M^{(\ell)} = \begin{pmatrix} M_{1,1}^{(\ell)} & \cdots & M_{1,m}^{(\ell)} \\ \vdots & \ddots & \vdots \\ M_{m,1}^{(\ell)} & \cdots & M_{m,m}^{(\ell)} \end{pmatrix}$$

where each block takes the form $M_{i,j}^{(\ell)} : \Sigma^{\leq \ell} \times \Sigma^{\leq \ell} \rightarrow \mathbb{C}$.

- ▶ Each submatrix has similar properties to what we saw for the NPA hierarchy.
- ▶ The overall matrix also has some structure, which is unique to this case.

Assemblages

- ▶ Another natural way to think about the commuting measurement value is in terms of *assemblages*:

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

- ▶ For a particular choice of x, y, a, b , an assemblage corresponds to the *unnormalized state* in the referee's hands at the end of the game.
- ▶ The function K completely determines the performance of Alice and Bob's strategy:

$$\sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x, y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} \left\langle V(a, b|x, y), K(a, b|x, y) \right\rangle.$$

Extended NPA hierarchy theorem

Let $\dim(\mathcal{R}) = m$. Then

$$\left\langle V(a, b|x, y), K(a, b|x, y) \right\rangle = \left\langle V(a, b|x, y), M^{(\ell)}((x, a), (y, b)) \right\rangle$$

for all $m, \ell \geq 1$, $(x, y) \in \Sigma_A \times \Sigma_B$ and $(a, b) \in \Gamma_A \times \Gamma_B$.

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¶

¶[Liang and Doherty (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¶

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.

¶[Liang and Doherty (2007)]

Lower bounds for extended nonlocal games

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

$$f = \sum_{(x,y) \in \Sigma_A \times \Sigma_B} \pi(x,y) \sum_{(a,b) \in \Gamma_A \times \Gamma_B} \left\langle V(a,b|x,y) \otimes B_b^y, \rho_a^x \right\rangle$$

Lower bound (SDP-1)

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

Lower bound (SDP-2)

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

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

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

A key lemma (proof)

By definition

$$\|\Pi_0 + \Pi_1\| = \max\{v^*(\Pi_0 + \Pi_1)v : v \in \mathcal{S}\}.$$

A key lemma (proof)

By definition

$$\|\Pi_0 + \Pi_1\| = \max\{v^*(\Pi_0 + \Pi_1)v : v \in \mathcal{S}\}.$$

Since $v \in \mathcal{S}$ are unit vectors,

$$v^*(\Pi_0 + \Pi_1)v = v^*\Pi_0v + v^*\Pi_1v = \|\Pi_0\|^2 + \|\Pi_1\|^2.$$

A key lemma (proof)

By definition

$$\|\Pi_0 + \Pi_1\| = \max\{v^*(\Pi_0 + \Pi_1)v : v \in \mathcal{S}\}.$$

Since $v \in \mathcal{S}$ are unit vectors,

$$v^*(\Pi_0 + \Pi_1)v = v^*\Pi_0v + v^*\Pi_1v = \|\Pi_0\|^2 + \|\Pi_1\|^2.$$

Recall the definition of the ∞ -norm for some operator $A \in L(\mathcal{X}, \mathcal{Y})$:

$$\|A\| = \max\{\|Av\| : v \in \mathcal{S}(\mathcal{X})\}.$$

We can then rewrite our expression as

$$\max\{\|\Pi_0v\|^2 + \|\Pi_1v\|^2 : v \in \mathcal{S}\}.$$

A key lemma (proof)

Define unit vectors $u_0, u_1 \in \mathcal{S}(\mathbb{C}^n)$, we can write

$$\Pi_0 = u_0 u_0^* \quad \text{and} \quad \Pi_1 = u_1 u_1^*.$$

A key lemma (proof)

Define unit vectors $u_0, u_1 \in \mathcal{S}(\mathbb{C}^n)$, we can write

$$\Pi_0 = u_0 u_0^* \quad \text{and} \quad \Pi_1 = u_1 u_1^*.$$

Therefore

$$\Pi_0 v = u_0 u_0^* v = \langle u_0, v \rangle u_0$$

and that

$$\|\Pi_0 v\|^2 = |\langle u_0, v \rangle|^2 \|u_0\|^2 = |\langle u_0, v \rangle|^2$$

(and similarly for Π_1 and u_1).

A key lemma (proof)

Therefore, we have that

$$\max\{|\langle u_0, v \rangle| + |\langle u_1, v \rangle|^2 : v \in \mathcal{S}, u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\},$$

where \mathcal{S}_0 is unit sphere of $\text{im}(\Pi_0)$ (similarly for \mathcal{S}_1 and Π_1).

A key lemma (proof)

Therefore, we have that

$$\max\{|\langle u_0, v \rangle| + |\langle u_1, v \rangle|^2 : v \in \mathcal{S}, u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\},$$

where \mathcal{S}_0 is unit sphere of $\text{im}(\Pi_0)$ (similarly for \mathcal{S}_1 and Π_1). By Cauchy-Schwarz, we have that

$$|\langle u_0, v \rangle|^2 = \|u_0\| \|v\|$$

(similarly for u_1 and v). Equality is achieved since u_0 and v are linearly dependent.

A key lemma (proof)

Therefore, we have that

$$\max\{|\langle u_0, v \rangle| + |\langle u_1, v \rangle|^2 : v \in \mathcal{S}, u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\},$$

where \mathcal{S}_0 is unit sphere of $\text{im}(\Pi_0)$ (similarly for \mathcal{S}_1 and Π_1). By Cauchy-Schwarz, we have that

$$|\langle u_0, v \rangle|^2 = \|u_0\| \|v\|$$

(similarly for u_1 and v). Equality is achieved since u_0 and v are linearly dependent. Since v is a unit eigenvector of $u_0 u_0^* + u_1 u_1^*$ that corresponds to λ_{\max} we have that

$$v^*(u_0 u_0^* + u_1 u_1^*)v = \|u_0 u_0^* + u_1 u_1^*\|.$$

A key lemma (proof)

Therefore, we have that

$$\max\{|\langle u_0, v \rangle| + |\langle u_1, v \rangle|^2 : v \in \mathcal{S}, u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\},$$

where \mathcal{S}_0 is unit sphere of $\text{im}(\Pi_0)$ (similarly for \mathcal{S}_1 and Π_1). By Cauchy-Schwarz, we have that

$$|\langle u_0, v \rangle|^2 = \|u_0\| \|v\|$$

(similarly for u_1 and v). Equality is achieved since u_0 and v are linearly dependent. Since v is a unit eigenvector of $u_0 u_0^* + u_1 u_1^*$ that corresponds to λ_{\max} we have that

$$v^*(u_0 u_0^* + u_1 u_1^*)v = \|u_0 u_0^* + u_1 u_1^*\|.$$

Again using definition of norm

$$\max\{v^*(u_0 u_0^* + u_1 u_1^*)v : v \in \mathcal{S}, u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\}.$$

A key lemma (proof)

Therefore

$$\max\{\|u_0 u_0^* + u_1 u_1^*\| : u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\}.$$

A key lemma (proof)

Therefore

$$\max\{\|u_0 u_0^* + u_1 u_1^*\| : u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\}.$$

Note that for every unit vector $u_0, u_1 \in \mathbb{C}^n$ it holds that

$$\|u_0 u_0^* + u_1 u_1^*\| = 1 + |\langle u_0, u_1 \rangle|,$$

since $u_0 u_0^* + u_1 u_1^*$ has at most two nonzero eigenvalues of $1 \pm |\langle u_0, u_1 \rangle|$. Therefore

$$\max\{1 + |\langle u_0, u_1 \rangle| : u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\}.$$

A key lemma (proof)

Therefore

$$\max\{\|u_0 u_0^* + u_1 u_1^*\| : u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\}.$$

Note that for every unit vector $u_0, u_1 \in \mathbb{C}^n$ it holds that

$$\|u_0 u_0^* + u_1 u_1^*\| = 1 + |\langle u_0, u_1 \rangle|,$$

since $u_0 u_0^* + u_1 u_1^*$ has at most two nonzero eigenvalues of $1 \pm |\langle u_0, u_1 \rangle|$. Therefore

$$\max\{1 + |\langle u_0, u_1 \rangle| : u_0 \in \mathcal{S}_0, u_1 \in \mathcal{S}_1\}.$$

Finally, since

$$\|A\|_p = \max\{|\langle B, A \rangle| : B \in L(\mathcal{X}, \mathcal{Y}), \|B\|_{p^*} \leq 1\},$$

it holds that

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