

# Monogamy-of-entanglement games

## Theory Seminar

Vincent Russo

University of Waterloo

August 11, 2016

UNIVERSITY OF  
WATERLOO



# Outline

Nonlocal games

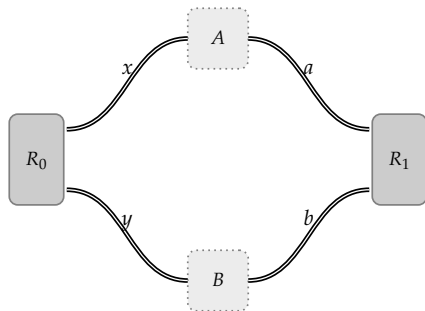
Extended nonlocal games

Monogamy-of-entanglement games

## Nonlocal games

## Nonlocal games

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



1. Question and answer sets:  $(\Sigma_A, \Sigma_B)$  and  $(\Gamma_A, \Gamma_B)$ ,
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  $f : \Sigma_A \rightarrow \Gamma_A$  and  $g : \Sigma_B \rightarrow \Gamma_B$ .
- ▶ *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  $f : \Sigma_A \rightarrow \Gamma_A$  and  $g : \Sigma_B \rightarrow \Gamma_B$ .
- ▶ *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

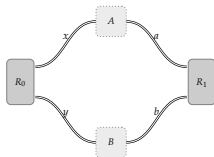
The CHSH game ( $G_{\text{CHSH}}$ ). Question and answer sets over  $\{0, 1\}$ .

Question pairs  $\{00, 01, 10, 11\}$  selected with equal probability.

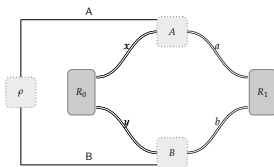
Winning condition iff  $a \oplus b = x \wedge y$ .

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

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



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



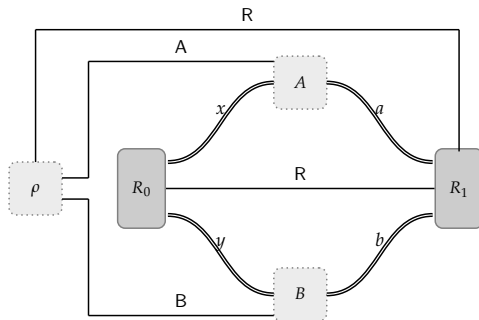
Demo Time: CHSH Game in QETLAB  
CHSH\_GAME.M



## 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  $(\Sigma_A, \Sigma_B)$  and  $(\Gamma_A, \Gamma_B)$ .
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  $\rho$ :

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

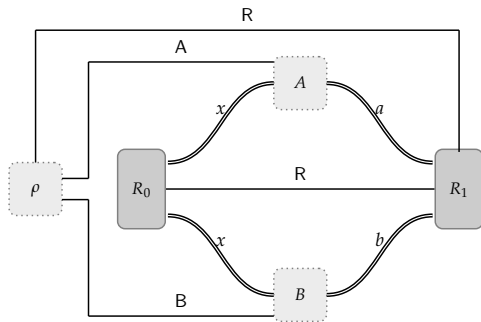
The respective winning and losing probabilities are given by

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

## Monogamy-of-entanglement games

# Monogamy-of-entanglement games

Monogamy-of-entanglement games<sup>¶</sup>, 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 output are all the equal.

# Standard quantum strategies for monogamy-of-entanglement games

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

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

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

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  $\rho$  prepared by Alice and Bob is fully separable, that is

$$\{\rho_j^{\mathcal{R}} : j \in \Delta\} \subseteq \mathcal{D}(\mathcal{R}), \quad \{\rho_j^{\mathcal{A}} : j \in \Delta\} \subseteq \mathcal{D}(\mathcal{A}), \quad \{\rho_j^{\mathcal{B}} : j \in \Delta\} \subseteq \mathcal{D}(\mathcal{B}),$$

such that

$$\rho = \sum_{j \in \Delta} p(j) \rho_j^{\mathcal{R}} \otimes \rho_j^{\mathcal{A}} \otimes \rho_j^{\mathcal{B}}.$$

## Unentangled strategies for monogamy-of-entanglement games

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

$$\{\rho_j^R : j \in \Delta\} \subseteq D(\mathcal{R}), \quad \{\rho_j^A : j \in \Delta\} \subseteq D(\mathcal{A}), \quad \{\rho_j^B : j \in \Delta\} \subseteq D(\mathcal{B}),$$

such that

$$\rho = \sum_{j \in \Delta} p(j) \rho_j^R \otimes \rho_j^A \otimes \rho_j^B.$$

Winning probability for an unentangled strategy is given by:

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

where  $\rho$  is separable.

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



# Unentangled value of monogamy-of-entanglement games

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

$$\rho = \sum_{j \in \Delta} p(j) \rho_j^R \otimes \rho_j^A \otimes \rho_j^B.$$

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

$$\rho = \rho^R \otimes \rho^A \otimes \rho^B.$$

# 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:

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

where the maximum is over all functions  $f : \Sigma \rightarrow \Gamma$ .

# The BB84 monogamy-of-entanglement game

The BB84 game ( $G_{\text{BB84}}$  for short)<sup>¶</sup> 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  $G_{\text{BB84}}$  coincide:

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

---

<sup>¶</sup> $G_{\text{BB84}}$  was introduced in [Tomamichel, Fehr, Kaniewski, Wehner, (2013)].

Demo Time: BB84 Game  
BB84\_GAME.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<sup>¶</sup>:

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

---

<sup>¶</sup>  $|u_x(a)^* u_{x'}(a)|^2 = 1/|\Gamma|$  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 (Johnston, Mittal, R, Watrous)

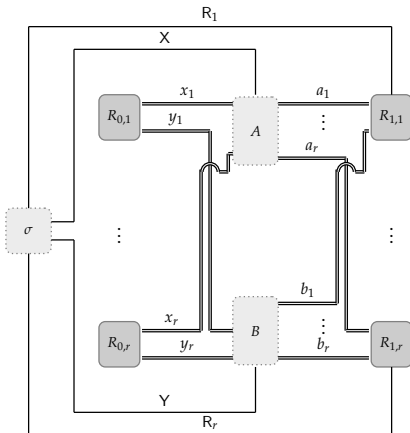
*For any monogamy-of-entanglement game,  $G$ , for which  $|\Sigma| = 2$ :*

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

## 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:

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

- $G_{\text{BB84}}$  obeys strong parallel repetition<sup>¶</sup>:

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

---

<sup>¶</sup>[Tomamichel, Fehr, Kaniewski, Wehner, (2013)]



Demo Time: Strong parallel repetition of BB84  
BB84\_PARALLEL\_REP.M

# Upper bounds on strong parallel repetition for monogamy games

Theorem (Tomamichel, Fehr, Kaniewski, Wehner)

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

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

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

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

# Strong parallel repetition for certain monogamy games

## Theorem (Johnston, Mittal, R, Watrous)

*Let  $G = (\pi, R)$  be a monogamy game where  $|\Sigma| = 2$ ,  $\pi$  is uniform over  $\Sigma$ , and  $R(a|x)$  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

## Proposition

*Let  $G = (\pi, R)$  be a monogamy-of-entanglement game for which  $\Sigma = \{0, 1\}$ ,  $\pi$  is uniform over  $\Sigma$ , 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  $\Pi_0$  and  $\Pi_1$  be nonzero projection operators on  $\mathbb{C}^n$ . It holds that*

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

## Proof of proposition

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

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

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

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

## 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,

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

## 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 <sup>¶</sup>	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.

---

<sup>¶</sup>So long as the measurements used by the referee are projective and the probability distribution,  $\pi$ , from which the questions are asked is uniform.