MIP* = RE

Isaac Goldbring

University of California, Irvine

ASL North American Annual Meeting
Cornell University
April 7, 2022

Alice and Bob against the world

- Alice and Bob are two cooperating but *noncommunicating* players playing a game against a "referee."
- They are each asked a question $x, y \in [k] := \{1, \ldots, k\}$ randomly according to some probability distribution π on $[k] \times [k]$.
- Somehow they return answers $a, b \in [n]$ respectively.
- There is a function $D : [k]^2 \times [n]^2 \to \{0, 1\}$, called the **decision predicate**, which determines if they win this round of the game, that is, they win if and only if $D(x, y, a, b) = 1$.
- This describes a **nonlocal game** $\mathfrak{G} := (\pi, D)$ with k questions and n answers.

Alice and Bob against the world

- Alice and Bob are two cooperating but *noncommunicating* players playing a game against a "referee."
- They are each asked a question $x, y \in [k] := \{1, \ldots, k\}$ randomly according to some probability distribution π on $[k] \times [k]$.
- Somehow they return answers $a, b \in [n]$ respectively.
- There is a function $D : [k]^2 \times [n]^2 \to \{0, 1\}$, called the **decision predicate**, which determines if they win this round of the game, that is, they win if and only if $D(x, y, a, b) = 1$.
- This describes a **nonlocal game** $\mathfrak{G} := (\pi, D)$ with k questions and n answers.

Alice and Bob against the world

- Alice and Bob are two cooperating but *noncommunicating* players playing a game against a "referee."
- They are each asked a question $x, y \in [k] := \{1, \ldots, k\}$ randomly according to some probability distribution π on $[k] \times [k]$.
- Somehow they return answers $a, b \in [n]$ respectively.
- There is a function $D : [k]^2 \times [n]^2 \to \{0, 1\}$, called the **decision predicate**, which determines if they win this round of the game, that is, they win if and only if $D(x, y, a, b) = 1$.
- This describes a **nonlocal game** $\mathfrak{G} := (\pi, D)$ with k questions and n answers.

Alice and Bob against the world

- Alice and Bob are two cooperating but *noncommunicating* players playing a game against a “referee.”
- They are each asked a question $x, y \in [k] := \{1, \ldots, k\}$ randomly according to some probability distribution π on $[k] \times [k]$.
- Somehow they return answers $a, b \in [n]$ respectively.
- There is a function $D : [k]^2 \times [n]^2 \to \{0, 1\}$, called the **decision predicate**, which determines if they win this round of the game, that is, they win if and only if $D(x, y, a, b) = 1$.
- This describes a **nonlocal game** $\mathfrak{G} := (\pi, D)$ with k questions and n answers.

Alice and Bob against the world

- Alice and Bob are two cooperating but *noncommunicating* players playing a game against a "referee."
- They are each asked a question $x, y \in [k] := \{1, \ldots, k\}$ randomly according to some probability distribution π on $[k] \times [k]$.
- Somehow they return answers $a, b \in [n]$ respectively.
- There is a function $D : [k]^2 \times [n]^2 \to \{0, 1\}$, called the **decision predicate**, which determines if they win this round of the game, that is, they win if and only if $D(x, y, a, b) = 1$.
- This describes a **nonlocal game** $\mathfrak{G} := (\pi, D)$ with k questions and n answers.

Strategies for nonlocal games

- Alice and Bob can meet before the game to decide on a **strategy** for playing $\mathfrak{G}$ that they will use before the game.
- For us, a strategy will simply be a matrix $p(a, b|x, y) \in [0, 1]^{k^2 n^2}$ describing the conditional probability they respond with answers $(a, b) \in [n]^2$ given that they are asked questions $(x, y) \in [k]^2$.
- Given a strategy p, the **value of the game $\mathfrak{G}$ with respect to p** is the quantity

$$\operatorname{val}(\mathfrak{G}, p) := \sum_{(x,y)\in[k]^2} \pi(x, y) \sum_{(a,b)\in[n]^2} p(a, b|x, y) D(a, b, x, y).$$

- $\operatorname{val}(\mathfrak{G}, p)$ measures the expected probability of winning the game if they play according to the strategy p.

Strategies for nonlocal games

- Alice and Bob can meet before the game to decide on a **strategy** for playing $\mathfrak{G}$ that they will use before the game.
- For us, a strategy will simply be a matrix $p(a,b|x,y) \in [0,1]^{k^2n^2}$ describing the conditional probability they respond with answers $(a,b) \in [n]^2$ given that they are asked questions $(x,y) \in [k]^2$.
- Given a strategy p, the **value of the game $\mathfrak{G}$ with respect to p** is the quantity

$$\mathrm{val}(\mathfrak{G},p) := \sum_{(x,y)\in[k]^2} \pi(x,y) \sum_{(a,b)\in[n]^2} p(a,b|x,y)D(a,b,x,y).$$

- $\mathrm{val}(\mathfrak{G},p)$ measures the expected probability of winning the game if they play according to the strategy p.

Strategies for nonlocal games

- Alice and Bob can meet before the game to decide on a **strategy** for playing $\mathfrak{G}$ that they will use before the game.
- For us, a strategy will simply be a matrix $p(a,b|x,y) \in [0,1]^{k^2n^2}$ describing the conditional probability they respond with answers $(a,b) \in [n]^2$ given that they are asked questions $(x,y) \in [k]^2$.
- Given a strategy p, the **value of the game $\mathfrak{G}$ with respect to p** is the quantity

$$\mathrm{val}(\mathfrak{G},p) := \sum_{(x,y)\in[k]^2} \pi(x,y) \sum_{(a,b)\in[n]^2} p(a,b|x,y)D(a,b,x,y).$$

- $\mathrm{val}(\mathfrak{G},p)$ measures the expected probability of winning the game if they play according to the strategy p.

Strategies for nonlocal games

- Alice and Bob can meet before the game to decide on a **strategy** for playing $\mathfrak{G}$ that they will use before the game.
- For us, a strategy will simply be a matrix $p(a, b|x, y) \in [0, 1]^{k^2 n^2}$ describing the conditional probability they respond with answers $(a, b) \in [n]^2$ given that they are asked questions $(x, y) \in [k]^2$.
- Given a strategy p, the **value of the game $\mathfrak{G}$ with respect to p** is the quantity

$$\mathrm{val}(\mathfrak{G}, p) := \sum_{(x,y)\in[k]^2} \pi(x, y) \sum_{(a,b)\in[n]^2} p(a, b|x, y) D(a, b, x, y).$$

- $\mathrm{val}(\mathfrak{G}, p)$ measures the expected probability of winning the game if they play according to the strategy p.

Classical strategies for nonlocal games

- A **deterministic** strategy is given by a pair of functions $A, B : [k] \to [n]$ such that

$$p(A(x), B(y)|x, y) = 1 \text{ for all } (x, y) \in [k]^2.$$

- A **classical** (or **local**) strategy is given by a probability space (Ω, μ) together with pairs of functions $A_\omega, B_\omega : [k] \to [n]$ such that

$$p(a, b|x, y) = \mu(\{\omega \in \Omega \ : \ A_\omega(x) = a \text{ and } B_\omega(y) = b\}).$$

- $C_{\mathrm{loc}}(k, n) \subseteq [0, 1]^{k^2 n^2}$ denotes the set of classical strategies. It is the convex hull of the set $C_{\mathrm{det}}(k, n)$ of determinstic strategies.
- The **classical value** of $\mathfrak{G}$ is the quantity

$$\mathrm{val}(\mathfrak{G}) := \sup_{p \in C_{\mathrm{loc}}(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{\mathrm{det}}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

Classical strategies for nonlocal games

- A **deterministic** strategy is given by a pair of functions $A, B : [k] \to [n]$ such that

$$p(A(x), B(y)|x, y) = 1 \text{ for all } (x, y) \in [k]^2.$$

- A **classical** (or **local**) strategy is given by a probability space (Ω, μ) together with pairs of functions $A_\omega, B_\omega : [k] \to [n]$ such that

$$p(a, b|x, y) = \mu(\{\omega \in \Omega \ : \ A_\omega(x) = a \text{ and } B_\omega(y) = b\}).$$

- $C_{\mathrm{loc}}(k, n) \subseteq [0, 1]^{k^2 n^2}$ denotes the set of classical strategies. It is the convex hull of the set $C_{\mathrm{det}}(k, n)$ of determinstic strategies.
- The **classical value** of $\mathfrak{G}$ is the quantity

$$\mathrm{val}(\mathfrak{G}) := \sup_{p \in C_{\mathrm{loc}}(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{\mathrm{det}}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

Classical strategies for nonlocal games

- A **deterministic** strategy is given by a pair of functions $A, B : [k] \to [n]$ such that

$$p(A(x), B(y)|x, y) = 1 \text{ for all } (x, y) \in [k]^2.$$

- A **classical** (or **local**) strategy is given by a probability space (Ω, μ) together with pairs of functions $A_\omega, B_\omega : [k] \to [n]$ such that

$$p(a, b|x, y) = \mu(\{\omega \in \Omega \ : \ A_\omega(x) = a \text{ and } B_\omega(y) = b\}).$$

- $C_{\text{loc}}(k, n) \subseteq [0, 1]^{k^2 n^2}$ denotes the set of classical strategies. It is the convex hull of the set $C_{\text{det}}(k, n)$ of determinstic strategies.
- The **classical value** of $\mathfrak{G}$ is the quantity

$$\text{val}(\mathfrak{G}) := \sup_{p \in C_{\text{loc}}(k,n)} \text{val}(\mathfrak{G}, p) = \sup_{p \in C_{\text{det}}(k,n)} \text{val}(\mathfrak{G}, p).$$

Classical strategies for nonlocal games

- A **deterministic** strategy is given by a pair of functions $A, B : [k] \to [n]$ such that
$$p(A(x), B(y)|x, y) = 1 \text{ for all } (x, y) \in [k]^2.$$
- A **classical** (or **local**) strategy is given by a probability space (Ω, μ) together with pairs of functions $A_\omega, B_\omega : [k] \to [n]$ such that
$$p(a, b|x, y) = \mu(\{\omega \in \Omega \ : \ A_\omega(x) = a \text{ and } B_\omega(y) = b\}).$$
- $C_{\mathrm{loc}}(k, n) \subseteq [0, 1]^{k^2n^2}$ denotes the set of classical strategies. It is the convex hull of the set $C_{\mathrm{det}}(k, n)$ of determinstic strategies.
- The **classical value** of $\mathfrak{G}$ is the quantity
$$\mathrm{val}(\mathfrak{G}) := \sup_{p \in C_{\mathrm{loc}}(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{\mathrm{det}}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

The CHSH game

Example

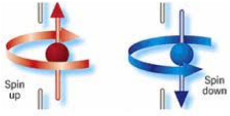
The CHSH game (named after Clauser, Horne, Shimony, and Holt) is the game $\mathfrak{G}_{\mathrm{CHSH}}$ with $k = n = 2$ and such that:

- If $x = 1$ or $y = 1$, then Alice and Bob win if and only if their answers agree.
- If $x = y = 2$, then Alice and Bob win if and only if their answers disagree.

By inspecting all deterministic strategies, one sees that

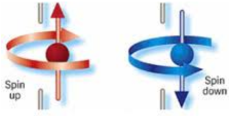
$$\mathrm{val}(\mathfrak{G}_{\mathrm{CHSH}}) = \frac{3}{4}.$$

The spin of an electron



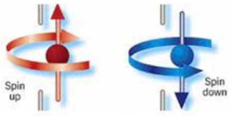
- An electron can have one of two spins: "up" or "down."
- At any given moment, however, it does not have a definite spin and instead is in a **superposition** of the two spins, as represented by the linear combination $\alpha|\text{up}\rangle + \beta|\text{down}\rangle \in \mathbb{C}^2$, where $|\text{up}\rangle$ and $|\text{down}\rangle$ are two orthogonal vectors in $\mathbb{C}^2$ and $\alpha, \beta \in \mathbb{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$.
- If it is not disturbed, its state evolves linearly according to the **Shrödinger equation.**
- However, when it is measured, its state randomly and discontinuously jumps to one of the two definite spin states $|\text{up}\rangle$ or $|\text{down}\rangle$ with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively.

The spin of an electron



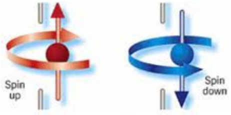
- An electron can have one of two spins: “up” or “down.”
- At any given moment, however, it does not have a definite spin and instead is in a **superposition** of the two spins, as represented by the linear combination $\alpha|\,\text{up}\rangle + \beta|\,\text{down}\rangle \in \mathbb{C}^2$, where $|\,\text{up}\rangle$ and $|\,\text{down}\rangle$ are two orthogonal vectors in $\mathbb{C}^2$ and $\alpha, \beta \in \mathbb{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$.
- If it is not disturbed, its state evolves linearly according to the **Shrödinger equation.**
- However, when it is measured, its state randomly and discontinuously jumps to one of the two definite spin states $|\,\text{up}\rangle$ or $|\,\text{down}\rangle$ with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively.

The spin of an electron



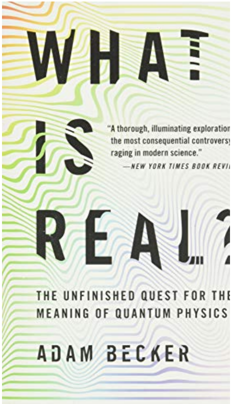
- An electron can have one of two spins: “up” or “down.”
- At any given moment, however, it does not have a definite spin and instead is in a **superposition** of the two spins, as represented by the linear combination $\alpha|\,\text{up}\rangle + \beta|\,\text{down}\rangle \in \mathbb{C}^2$, where $|\,\text{up}\rangle$ and $|\,\text{down}\rangle$ are two orthogonal vectors in $\mathbb{C}^2$ and $\alpha, \beta \in \mathbb{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$.
- If it is not disturbed, its state evolves linearly according to the **Shrödinger equation.**
- However, when it is measured, its state randomly and discontinuously jumps to one of the two definite spin states $|\,\text{up}\rangle$ or $|\,\text{down}\rangle$ with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively.

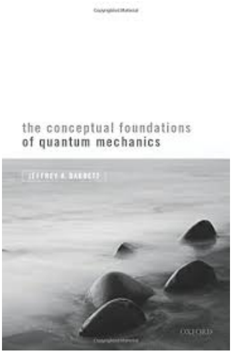
The spin of an electron

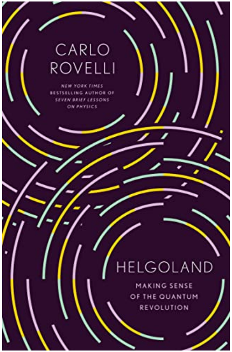


- An electron can have one of two spins: “up” or “down.”
- At any given moment, however, it does not have a definite spin and instead is in a **superposition** of the two spins, as represented by the linear combination $\alpha|\,\text{up}\rangle + \beta|\,\text{down}\rangle \in \mathbb{C}^2$, where $|\,\text{up}\rangle$ and $|\,\text{down}\rangle$ are two orthogonal vectors in $\mathbb{C}^2$ and $\alpha, \beta \in \mathbb{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$.
- If it is not disturbed, its state evolves linearly according to the **Shrödinger equation**.
- However, when it is measured, its state randomly and discontinuously jumps to one of the two definite spin states $|\,\text{up}\rangle$ or $|\,\text{down}\rangle$ with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively.

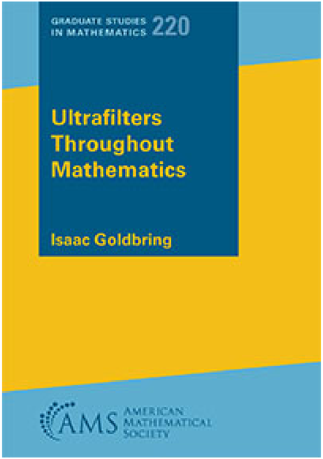
Recommended summer reading







More summer reading (shameless plug)



General quantum systems

- Associated to a quantum system is its **state space**, which is a complex Hilbert space H.
- The **state** of the system at any given moment is described by a unit vector $\xi \in H$, which evolves linearly until it is measured.
- A **measurement** with n outcomes is a tuple $M_1, \ldots, M_n \in B(H)$ such that, upon measurement, the probability of outcome i occurring is given by $\|M_i\xi\|^2$, in which case the state of the system jumps to $\frac{M_i\xi}{\|M_i\xi\|}$. (**Born rule**)
- For these to determine legitimate probabilities, for all unit vectors $\xi \in H$, one must have

$$1 = \sum_{i=1}^{n} \|M_i\xi\|^2 = \sum_{i=1}^{n} \langle M_i^* M_i \xi, \xi \rangle$$

and thus $\sum_{i=1}^{n} M_i^* M_i = I_H$.

General quantum systems

- Associated to a quantum system is its **state space**, which is a complex Hilbert space H.
- The **state** of the system at any given moment is described by a unit vector $\xi \in H$, which evolves linearly until it is measured.
- A **measurement** with n outcomes is a tuple $M_1, \ldots, M_n \in B(H)$ such that, upon measurement, the probability of outcome i occurring is given by $\|M_i\xi\|^2$, in which case the state of the system jumps to $\frac{M_i\xi}{\|M_i\xi\|}$. (**Born rule**)
- For these to determine legitimate probabilities, for all unit vectors $\xi \in H$, one must have

$$1 = \sum_{i=1}^{n} \|M_i\xi\|^2 = \sum_{i=1}^{n} \langle M_i^* M_i\xi, \xi\rangle$$

and thus $\sum_{i=1}^{n} M_i^* M_i = I_H$.

General quantum systems

- Associated to a quantum system is its **state space**, which is a complex Hilbert space H.
- The **state** of the system at any given moment is described by a unit vector $\xi \in H$, which evolves linearly until it is measured.
- A **measurement** with n outcomes is a tuple $M_1, \ldots, M_n \in B(H)$ such that, upon measurement, the probability of outcome i occurring is given by $\|M_i\xi\|^2$, in which case the state of the system jumps to $\frac{M_i\xi}{\|M_i\xi\|}$. (**Born rule**)
- For these to determine legitimate probabilities, for all unit vectors $\xi \in H$, one must have

$$1 = \sum_{i=1}^{n} \|M_i\xi\|^2 = \sum_{i=1}^{n} \langle M_i^* M_i \xi, \xi\rangle$$

and thus $\sum_{i=1}^{n} M_i^* M_i = I_H$.

General quantum systems

- Associated to a quantum system is its **state space**, which is a complex Hilbert space H.
- The **state** of the system at any given moment is described by a unit vector $\xi \in H$, which evolves linearly until it is measured.
- A **measurement** with n outcomes is a tuple $M_1, \ldots, M_n \in B(H)$ such that, upon measurement, the probability of outcome i occurring is given by $\|M_i\xi\|^2$, in which case the state of the system jumps to $\frac{M_i\xi}{\|M_i\xi\|}$. (**Born rule**)
- For these to determine legitimate probabilities, for all unit vectors $\xi \in H$, one must have

$$1 = \sum_{i=1}^{n} \|M_i\xi\|^2 = \sum_{i=1}^{n} \langle M_i^* M_i \xi, \xi \rangle$$

and thus $\sum_{i=1}^{n} M_i^* M_i = I_H$.

POVMs and PVMs

- If one only cares about the statistics of the outcomes of a measurement (like us!), then we can simplify matters by assuming that each measurement operator is **positive.**
- A **POVM** (positive operator-valued measure) of length n is a collection $A_1, \ldots, A_n$ of positive operators on H such that $\sum_{i=1}^n A_i = I_H$.
- On state ξ, the probability outcome i occurs is given by $\langle A_i \xi, \xi \rangle$.
- If each A_i is actually a **projection**, we speak of **PVMs** (projection-valued measures). This is the same as an orthogonal decomposition of H into n orthogonal subspaces.
- The case of the spin of an electron was a PVM corresponding to the one-dimensional subspaces spanned by $|\mathrm{up}\rangle$ and $|\mathrm{down}\rangle$.

POVMs and PVMs

- If one only cares about the statistics of the outcomes of a measurement (like us!), then we can simplify matters by assuming that each measurement operator is **positive.**
- A **POVM** (positive operator-valued measure) of length n is a collection $A_1, \ldots, A_n$ of positive operators on H such that $\sum_{i=1}^{n} A_i = I_H$.
- On state ξ, the probability outcome i occurs is given by $\langle A_i\xi, \xi\rangle$.
- If each A_i is actually a **projection**, we speak of **PVMs** (projection-valued measures). This is the same as an orthogonal decomposition of H into n orthogonal subspaces.
- The case of the spin of an electron was a PVM corresponding to the one-dimensional subspaces spanned by $|\,\mathrm{up}\rangle$ and $|\,\mathrm{down}\rangle$.

POVMs and PVMs

- If one only cares about the statistics of the outcomes of a measurement (like us!), then we can simplify matters by assuming that each measurement operator is **positive.**
- A **POVM** (positive operator-valued measure) of length n is a collection $A_1, \ldots, A_n$ of positive operators on H such that $\sum_{i=1}^n A_i = I_H$.
- On state ξ, the probability outcome i occurs is given by $\langle A_i\xi, \xi\rangle$.
- If each A_i is actually a **projection**, we speak of **PVMs** (projection-valued measures). This is the same as an orthogonal decomposition of H into n orthogonal subspaces.
- The case of the spin of an electron was a PVM corresponding to the one-dimensional subspaces spanned by $|\mathrm{up}\rangle$ and $|\mathrm{down}\rangle$.

POVMs and PVMs

- If one only cares about the statistics of the outcomes of a measurement (like us!), then we can simplify matters by assuming that each measurement operator is **positive**.
- A **POVM** (positive operator-valued measure) of length n is a collection $A_1, \ldots, A_n$ of positive operators on H such that $\sum_{i=1}^n A_i = I_H$.
- On state ξ, the probability outcome i occurs is given by $\langle A_i\xi, \xi\rangle$.
- If each A_i is actually a **projection**, we speak of **PVMs** (projection-valued measures). This is the same as an orthogonal decomposition of H into n orthogonal subspaces.
- The case of the spin of an electron was a PVM corresponding to the one-dimensional subspaces spanned by $|\,\mathrm{up}\rangle$ and $|\,\mathrm{down}\rangle$.

POVMs and PVMs

- If one only cares about the statistics of the outcomes of a measurement (like us!), then we can simplify matters by assuming that each measurement operator is **positive**.
- A **POVM** (positive operator-valued measure) of length n is a collection $A_1, \ldots, A_n$ of positive operators on H such that $\sum_{i=1}^n A_i = I_H$.
- On state ξ, the probability outcome i occurs is given by $\langle A_i\xi, \xi\rangle$.
- If each A_i is actually a **projection**, we speak of **PVMs** (projection-valued measures). This is the same as an orthogonal decomposition of H into n orthogonal subspaces.
- The case of the spin of an electron was a PVM corresponding to the one-dimensional subspaces spanned by $|\mathrm{up}\rangle$ and $|\mathrm{down}\rangle$.

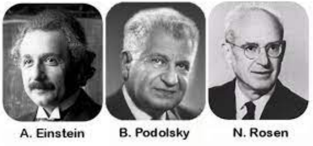
The EPR state

- Another axiom of quantum mechanics is that if H_A and H_B are the state spaces for two quantum systems, then the state space for their composite system is given by $H_A \otimes H_B$.
- Thus, the state space for two electrons is given by $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.
- The **EPR state** is given by $\psi_{\mathrm{EPR}} = \frac{1}{\sqrt{2}}|\mathrm{up}\rangle|\mathrm{up}\rangle + \frac{1}{\sqrt{2}}|\mathrm{down}\rangle|\mathrm{down}\rangle$.
- It was used by Einstein, Podolsky, and Rosen in their famous paper arguing that quantum mechanics was incomplete!
- The spookiness of entanglement!

The EPR state

- Another axiom of quantum mechanics is that if H_A and H_B are the state spaces for two quantum systems, then the state space for their composite system is given by $H_A \otimes H_B$.
- Thus, the state space for two electrons is given by $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.
- The **EPR state** is given by $\psi_{\mathrm{EPR}} = \frac{1}{\sqrt{2}}|\mathrm{up}\rangle|\mathrm{up}\rangle + \frac{1}{\sqrt{2}}|\mathrm{down}\rangle|\mathrm{down}\rangle$.
- It was used by Einstein, Podolsky, and Rosen in their famous paper arguing that quantum mechanics was incomplete!
- The spookiness of entanglement!

The EPR state

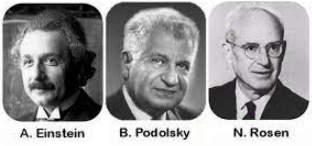


- Another axiom of quantum mechanics is that if H_A and H_B are the state spaces for two quantum systems, then the state space for their composite system is given by $H_A \otimes H_B$.
- Thus, the state space for two electrons is given by $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.
- The **EPR state** is given by $\psi_{\text{EPR}} = \frac{1}{\sqrt{2}}|\text{up}\rangle|\text{up}\rangle + \frac{1}{\sqrt{2}}|\text{down}\rangle|\text{down}\rangle$.
- It was used by Einstein, Podolsky, and Rosen in their famous paper arguing that quantum mechanics was incomplete!
- The spookiness of entanglement!

The EPR state

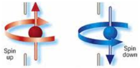
- Another axiom of quantum mechanics is that if H_A and H_B are the state spaces for two quantum systems, then the state space for their composite system is given by $H_A \otimes H_B$.
- Thus, the state space for two electrons is given by $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.
- The **EPR state** is given by $\psi_{\text{EPR}} = \frac{1}{\sqrt{2}}|\,\text{up}\rangle|\,\text{up}\rangle + \frac{1}{\sqrt{2}}|\,\text{down}\rangle|\,\text{down}\rangle$.
- It was used by Einstein, Podolsky, and Rosen in their famous paper arguing that quantum mechanics was incomplete!
- The spookiness of entanglement!

The EPR state



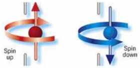
- Another axiom of quantum mechanics is that if H_A and H_B are the state spaces for two quantum systems, then the state space for their composite system is given by $H_A \otimes H_B$.
- Thus, the state space for two electrons is given by $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.
- The **EPR state** is given by $\psi_{\text{EPR}} = \frac{1}{\sqrt{2}} |\text{ up}\rangle |\text{ up}\rangle + \frac{1}{\sqrt{2}} |\text{ down}\rangle |\text{ down}\rangle$.
- It was used by Einstein, Podolsky, and Rosen in their famous paper arguing that quantum mechanics was incomplete!
- The spookiness of entanglement!

Quantum strategies for nonlocal games



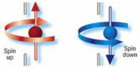
- Consider a game $\mathfrak{G}$ with k questions and n answers.
- This time, when playing the game, Alice and Bob have quantum systems H_A and H_B and share a state $\xi \in H_A \otimes H_B$.
- Upon receiving question $x \in [k]$, Alice will perform a POVM $A^x = (A_1^x, \ldots, A_n^x)$ on her part of ξ to decide which answer to give.
- Bob similarly has a POVM $B^y = (B_1^y, \ldots, B_n^y)$ for measuring on his part of ξ.
- We then have $p(a, b|x, y) = \langle (A_a^x \otimes B_b^y)\xi, \xi \rangle$.

Quantum strategies for nonlocal games



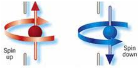
- Consider a game $\mathfrak{G}$ with k questions and n answers.
- This time, when playing the game, Alice and Bob have quantum systems H_A and H_B and share a state $\xi \in H_A \otimes H_B$.
- Upon receiving question $x \in [k]$, Alice will perform a POVM $A^x = (A_1^x, \ldots, A_n^x)$ on her part of ξ to decide which answer to give.
- Bob similarly has a POVM $B^y = (B_1^y, \ldots, B_n^y)$ for measuring on his part of ξ.
- We then have $p(a, b|x, y) = \langle (A_a^x \otimes B_b^y)\xi, \xi \rangle$.

Quantum strategies for nonlocal games



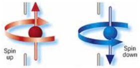
- Consider a game $\mathfrak{G}$ with k questions and n answers.
- This time, when playing the game, Alice and Bob have quantum systems H_A and H_B and share a state $\xi \in H_A \otimes H_B$.
- Upon receiving question $x \in [k]$, Alice will perform a POVM $A^x = (A^x_1, \ldots, A^x_n)$ on her part of ξ to decide which answer to give.
- Bob similarly has a POVM $B^y = (B^y_1, \ldots, B^y_n)$ for measuring on his part of ξ.
- We then have $p(a, b|x, y) = \langle (A^x_a \otimes B^y_b)\xi, \xi \rangle$.

Quantum strategies for nonlocal games



- Consider a game $\mathfrak{G}$ with k questions and n answers.
- This time, when playing the game, Alice and Bob have quantum systems H_A and H_B and share a state $\xi \in H_A \otimes H_B$.
- Upon receiving question $x \in [k]$, Alice will perform a POVM $A^x = (A^x_1, \ldots, A^x_n)$ on her part of ξ to decide which answer to give.
- Bob similarly has a POVM $B^y = (B^y_1, \ldots, B^y_n)$ for measuring on his part of ξ.
- We then have $p(a, b|x, y) = \langle (A^x_a \otimes B^y_b)\xi, \xi \rangle$.

Quantum strategies for nonlocal games

- Consider a game $\mathfrak{G}$ with k questions and n answers.
- This time, when playing the game, Alice and Bob have quantum systems H_A and H_B and share a state $\xi \in H_A \otimes H_B$.
- Upon receiving question $x \in [k]$, Alice will perform a POVM $A^x = (A_1^x, \ldots, A_n^x)$ on her part of ξ to decide which answer to give.
- Bob similarly has a POVM $B^y = (B_1^y, \ldots, B_n^y)$ for measuring on his part of ξ.
- We then have $p(a, b|x, y) = \langle (A_a^x \otimes B_b^y)\xi, \xi \rangle$.

The entangled value of a nonlocal game

- $C_q(k,n)$ denotes the set of strategies for which there are:
  - **finite-dimensional** Hilbert spaces H_A and H_B,
  - POVMs A^x and B^y on H_A and H_B respectively (one for each $x, y \in [k]$), and
  - a unit vector $\xi \in H_A \otimes H_B$

  for which $p(a,b|x,y) = \langle (A^x_a \otimes B^y_b)\xi, \xi\rangle$.
- We also consider $C_{qa}(k,n) := \overline{C_q(k,n)}$.
- If $\mathfrak{G}$ is a nonlocal game with k questions and n answers, the **entangled value** of $\mathfrak{G}$ is

$$\mathrm{val}^*(\mathfrak{G}) := \sup_{p \in C_q(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{qa}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

- $C_{\mathrm{loc}}(k,n) \subseteq C_q(k,n)$ so $\mathrm{val}(\mathfrak{G}) \leq \mathrm{val}^*(\mathfrak{G})$.

The entangled value of a nonlocal game

- $C_q(k, n)$ denotes the set of strategies for which there are:
  - **finite-dimensional** Hilbert spaces H_A and H_B,
  - POVMs A^x and B^y on H_A and H_B respectively (one for each $x, y \in [k]$), and
  - a unit vector $\xi \in H_A \otimes H_B$

  for which $p(a, b|x, y) = \langle (A^x_a \otimes B^y_b)\xi, \xi\rangle$.
- We also consider $C_{qa}(k, n) := \overline{C_q(k, n)}$.
- If $\mathfrak{G}$ is a nonlocal game with k questions and n answers, the **entangled value** of $\mathfrak{G}$ is

$$\mathrm{val}^*(\mathfrak{G}) := \sup_{p \in C_q(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{qa}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

- $C_{\mathrm{loc}}(k, n) \subseteq C_q(k, n)$ so $\mathrm{val}(\mathfrak{G}) \leq \mathrm{val}^*(\mathfrak{G})$.

The entangled value of a nonlocal game

- $C_q(k,n)$ denotes the set of strategies for which there are:
  - **finite-dimensional** Hilbert spaces H_A and H_B,
  - POVMs A^x and B^y on H_A and H_B respectively (one for each $x, y \in [k]$), and
  - a unit vector $\xi \in H_A \otimes H_B$

  for which $p(a,b|x,y) = \langle (A^x_a \otimes B^y_b)\xi, \xi\rangle$.
- We also consider $C_{qa}(k,n) := \overline{C_q(k,n)}$.
- If $\mathfrak{G}$ is a nonlocal game with k questions and n answers, the **entangled value** of $\mathfrak{G}$ is

$$\mathrm{val}^*(\mathfrak{G}) := \sup_{p \in C_q(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{qa}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

- $C_{\mathrm{loc}}(k,n) \subseteq C_q(k,n)$ so $\mathrm{val}(\mathfrak{G}) \leq \mathrm{val}^*(\mathfrak{G})$.

The entangled value of a nonlocal game

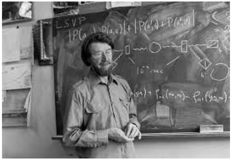
- $C_q(k,n)$ denotes the set of strategies for which there are:
  - **finite-dimensional** Hilbert spaces H_A and H_B,
  - POVMs A^x and B^y on H_A and H_B respectively (one for each $x, y \in [k]$), and
  - a unit vector $\xi \in H_A \otimes H_B$

  for which $p(a,b|x,y) = \langle (A_a^x \otimes B_b^y)\xi, \xi\rangle$.
- We also consider $C_{qa}(k,n) := \overline{C_q(k,n)}$.
- If $\mathfrak{G}$ is a nonlocal game with k questions and n answers, the **entangled value** of $\mathfrak{G}$ is

$$\mathrm{val}^*(\mathfrak{G}) := \sup_{p \in C_q(k,n)} \mathrm{val}(\mathfrak{G}, p) = \sup_{p \in C_{qa}(k,n)} \mathrm{val}(\mathfrak{G}, p).$$

- $C_{\mathrm{loc}}(k,n) \subseteq C_q(k,n)$ so $\mathrm{val}(\mathfrak{G}) \leq \mathrm{val}^*(\mathfrak{G})$.

CHSH, EPR, and Bell's Theorem



Theorem (Bell's Theorem)

$\mathrm{val}^*(\mathfrak{G}_{\mathrm{CHSH}}) > \mathrm{val}(\mathfrak{G}_{\mathrm{CHSH}})$.

- Recall $\mathrm{val}(\mathfrak{G}_{\mathrm{CHSH}}) = \frac{3}{4}$.
- However, there is an entangled strategy p, based on the EPR state ψ_{EPR}, such that $\mathrm{val}(\mathfrak{G}, p) = \cos^2(\frac{\pi}{8}) \approx 0.85$ (which equals $\mathrm{val}^*(\mathfrak{G}_{\mathrm{CHSH}})$ by a result of Tsirelson).
- This inequality showed that EPR were wrong!

How hard is it to compute $\mathrm{val}^*(\mathfrak{G})$?

- One can effectively compute *lower bounds* for $\mathrm{val}^*(\mathfrak{G})$ uniformly in $\mathfrak{G}$:
- Given some dimension d, you can enumerate a computable sequence of finite nets $N_1^d \subseteq N_2^d \subseteq \cdots$ over all states and POVMs in dimension d with $|N_m^d| = m^{O(d^2)}$ such that for any $p \in C_q(k, n)$ based on a d-dimensional strategy and any m, there is $q \in N_m^d$ with $|\mathrm{val}(\mathfrak{G}, p) - \mathrm{val}(\mathfrak{G}, q)| < \frac{1}{m}$.
- Set

$$\mathrm{val}^n(\mathfrak{G}, p) = \max_{d,m \leq n} \max_{p \in N_m^d} \mathrm{val}(\mathfrak{G}, p).$$

- Then $\mathrm{val}^n(\mathfrak{G}, p)$ is computable and $\mathrm{val}^n(\mathfrak{G}, p) \nearrow \mathrm{val}(\mathfrak{G})$.
- Could it be that $\mathrm{val}^*(\mathfrak{G})$ is actually uniformly computable in $\mathfrak{G}$?

How hard is it to compute $\mathrm{val}^*(\mathfrak{G})$?

- One can effectively compute *lower bounds* for $\mathrm{val}^*(\mathfrak{G})$ uniformly in $\mathfrak{G}$:
- Given some dimension d, you can enumerate a computable sequence of finite nets $N_1^d \subseteq N_2^d \subseteq \cdots$ over all states and POVMs in dimension d with $|N_m^d| = m^{O(d^2)}$ such that for any $p \in C_q(k,n)$ based on a d-dimensional strategy and any m, there is $q \in N_m^d$ with $|\mathrm{val}(\mathfrak{G},p) - \mathrm{val}(\mathfrak{G},q)| < \frac{1}{m}$.
- Set

$$\mathrm{val}^n(\mathfrak{G},p) = \max_{d,m\leq n} \max_{p\in N_m^d} \mathrm{val}(\mathfrak{G},p).$$

- Then $\mathrm{val}^n(\mathfrak{G},p)$ is computable and $\mathrm{val}^n(\mathfrak{G},p) \nearrow \mathrm{val}(\mathfrak{G})$.
- Could it be that $\mathrm{val}^*(\mathfrak{G})$ is actually uniformly computable in $\mathfrak{G}$?

How hard is it to compute $\mathrm{val}^*(\mathfrak{G})$?

- One can effectively compute *lower bounds* for $\mathrm{val}^*(\mathfrak{G})$ uniformly in $\mathfrak{G}$:
- Given some dimension d, you can enumerate a computable sequence of finite nets $N_1^d \subseteq N_2^d \subseteq \cdots$ over all states and POVMs in dimension d with $|N_m^d| = m^{O(d^2)}$ such that for any $p \in C_q(k,n)$ based on a d-dimensional strategy and any m, there is $q \in N_m^d$ with $|\mathrm{val}(\mathfrak{G},p) - \mathrm{val}(\mathfrak{G},q)| < \frac{1}{m}$.
- Set

$$\mathrm{val}^n(\mathfrak{G},p) = \max_{d,m\leq n} \max_{p\in N_m^d} \mathrm{val}(\mathfrak{G},p).$$

- Then $\mathrm{val}^n(\mathfrak{G},p)$ is computable and $\mathrm{val}^n(\mathfrak{G},p) \nearrow \mathrm{val}(\mathfrak{G})$.
- Could it be that $\mathrm{val}^*(\mathfrak{G})$ is actually uniformly computable in $\mathfrak{G}$?

How hard is it to compute $\mathrm{val}^*(\mathfrak{G})$?

- One can effectively compute *lower bounds* for $\mathrm{val}^*(\mathfrak{G})$ uniformly in $\mathfrak{G}$:
- Given some dimension d, you can enumerate a computable sequence of finite nets $N_1^d \subseteq N_2^d \subseteq \cdots$ over all states and POVMs in dimension d with $|N_m^d| = m^{O(d^2)}$ such that for any $p \in C_q(k,n)$ based on a d-dimensional strategy and any m, there is $q \in N_m^d$ with $|\mathrm{val}(\mathfrak{G},p) - \mathrm{val}(\mathfrak{G},q)| < \frac{1}{m}$.
- Set

$$\mathrm{val}^n(\mathfrak{G},p) = \max_{d,m\leq n} \max_{p\in N_m^d} \mathrm{val}(\mathfrak{G},p).$$

- Then $\mathrm{val}^n(\mathfrak{G},p)$ is computable and $\mathrm{val}^n(\mathfrak{G},p) \nearrow \mathrm{val}(\mathfrak{G})$.
- Could it be that $\mathrm{val}^*(\mathfrak{G})$ is actually uniformly computable in $\mathfrak{G}$?

How hard is it to compute $\mathrm{val}^*(\mathfrak{G})$?

- One can effectively compute *lower bounds* for $\mathrm{val}^*(\mathfrak{G})$ uniformly in $\mathfrak{G}$:
- Given some dimension d, you can enumerate a computable sequence of finite nets $N_1^d \subseteq N_2^d \subseteq \cdots$ over all states and POVMs in dimension d with $|N_m^d| = m^{O(d^2)}$ such that for any $p \in C_q(k,n)$ based on a d-dimensional strategy and any m, there is $q \in N_m^d$ with $|\mathrm{val}(\mathfrak{G},p) - \mathrm{val}(\mathfrak{G},q)| < \frac{1}{m}$.
- Set

$$\mathrm{val}^n(\mathfrak{G},p) = \max_{d,m\leq n} \max_{p\in N_m^d} \mathrm{val}(\mathfrak{G},p).$$

- Then $\mathrm{val}^n(\mathfrak{G},p)$ is computable and $\mathrm{val}^n(\mathfrak{G},p) \nearrow \mathrm{val}(\mathfrak{G})$.
- Could it be that $\mathrm{val}^*(\mathfrak{G})$ is actually uniformly computable in $\mathfrak{G}$?

$\mathrm{MIP}^* = \mathrm{RE}$





Theorem (Ji, Natarajan, Vidick, Wright, Yuen (2020))

There is an effective mapping $\mathcal{M} \mapsto \mathfrak{G}_{\mathcal{M}}$ from Turing machines to nonlocal games such that:

- *If $\mathcal{M}$ halts, then* $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = 1$.
- *If $\mathcal{M}$ does not halt, then* $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) \leq \frac{1}{2}$.

Uniform game sequences

Definition

A **uniform game sequence** (UGS) is an infinite sequence $\bar{\mathfrak{G}} := (\mathfrak{G}_1, \mathfrak{G}_2, \ldots,)$ of nonlocal games for which there is a single Turing machine V which computes in time $\mathrm{poly}(\log n)$:

- The number of questions and answers in $\mathfrak{G}_n$.
- A Turing machine which specifies the probability distribution for $\mathfrak{G}_n$.
- A Turing machine which specifies the decision predicate for $\mathfrak{G}_n$.

Entanglement lower bound for nonlocal games

Definition

Given a nonlocal game $\mathfrak{G}$ and $r \in [0,1]$, we set $\mathcal{E}(\mathfrak{G}, r)$ to be the minimum dimension d for which there exists a strategy $p \in C_q$ based on d-dimensional Hilbert spaces so that $\mathrm{val}(\mathfrak{G}, p) \geq r$.

Example

1. $\mathcal{E}(\mathfrak{G}_{\mathrm{CHSH}}, \frac{3}{4}) = 0$
2. $\mathcal{E}(\mathfrak{G}_{\mathrm{CHSH}}, \cos^2(\frac{\pi}{8})) = 2$
3. $\mathcal{E}(\mathfrak{G}_{\mathrm{CHSH}}, 1) = \infty$

Entanglement lower bound for nonlocal games

Definition

Given a nonlocal game $\mathfrak{G}$ and $r \in [0,1]$, we set $\mathcal{E}(\mathfrak{G}, r)$ to be the minimum dimension d for which there exists a strategy $p \in C_q$ based on d-dimensional Hilbert spaces so that $\mathrm{val}(\mathfrak{G}, p) \geq r$.

Example

1. $\mathcal{E}(\mathfrak{G}_{\mathrm{CHSH}}, \frac{3}{4}) = 0$
2. $\mathcal{E}(\mathfrak{G}_{\mathrm{CHSH}}, \cos^2(\frac{\pi}{8})) = 2$
3. $\mathcal{E}(\mathfrak{G}_{\mathrm{CHSH}}, 1) = \infty$

Compression theorem for nonlocal games

Theorem

There exists an algorithm C such that upon input a Turing machine V describing a UGS $\bar{\mathfrak{G}}$ with each $\mathfrak{G}_n$ of "complexity" at most $O(n^2)$ outputs a Turing machine V' describing a UGS $\bar{\mathfrak{G}}'$ of polynomial-time computable games such that:

- *If* $\mathrm{val}^*(\mathfrak{G}_n) = 1$, *then* $\mathrm{val}^*(\mathfrak{G}'_n) = 1$.
- $\mathcal{E}(\mathfrak{G}'_n, \frac{1}{2}) \geq \max\{\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}), n\}$.
- *The time complexity of* $\mathfrak{G}'_n$ *is* $\mathrm{poly}(\log n)$.

Compression theorem for nonlocal games

Theorem

There exists an algorithm C such that upon input a Turing machine V describing a UGS $\bar{\mathfrak{G}}$ with each $\mathfrak{G}_n$ of "complexity" at most $O(n^2)$ outputs a Turing machine V' describing a UGS $\bar{\mathfrak{G}}'$ of polynomial-time computable games such that:

- *If* $\mathrm{val}^*(\mathfrak{G}_n) = 1$, *then* $\mathrm{val}^*(\mathfrak{G}'_n) = 1$.
- $\mathcal{E}(\mathfrak{G}'_n, \frac{1}{2}) \geq \max\{\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}), n\}$.
- *The time complexity of* $\mathfrak{G}'_n$ *is* $\mathrm{poly}(\log n)$.

Compression theorem for nonlocal games

Theorem

There exists an algorithm C such that upon input a Turing machine V describing a UGS $\bar{\mathfrak{G}}$ with each $\mathfrak{G}_n$ of "complexity" at most $O(n^2)$ outputs a Turing machine V' describing a UGS $\bar{\mathfrak{G}}'$ of polynomial-time computable games such that:

- *If* $\mathrm{val}^*(\mathfrak{G}_n) = 1$, *then* $\mathrm{val}^*(\mathfrak{G}'_n) = 1$.
- $\mathcal{E}(\mathfrak{G}'_n, \frac{1}{2}) \geq \max\{\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}), n\}$.
- *The time complexity of* $\mathfrak{G}'_n$ *is* $\mathrm{poly}(\log n)$.

Compression theorem for nonlocal games

Theorem

There exists an algorithm C such that upon input a Turing machine V describing a UGS $\bar{\mathfrak{G}}$ with each $\mathfrak{G}_n$ of "complexity" at most $O(n^2)$ outputs a Turing machine V' describing a UGS $\bar{\mathfrak{G}}'$ of polynomial-time computable games such that:

- *If* $\mathrm{val}^*(\mathfrak{G}_n) = 1$, *then* $\mathrm{val}^*(\mathfrak{G}'_n) = 1$.
- $\mathcal{E}(\mathfrak{G}'_n, \frac{1}{2}) \geq \max\{\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}), n\}$.
- *The time complexity of* $\mathfrak{G}'_n$ *is* $\mathrm{poly}(\log n)$.

MIP* = RE from Compression: Part I

- Given $\mathcal{M}$, we define a Turing machine $V^{\mathcal{M}}$ which computes a UGS $\bar{\mathfrak{G}}^{\mathcal{M}} = (\mathfrak{G}_1, \mathfrak{G}_2, \ldots)$.
- Here is how $\mathfrak{G}_n$ looks:
  - Run $\mathcal{M}$ on the empty input for n time steps. If $\mathcal{M}$ halts, then victory!
  - If not, run C on $V^{\mathcal{M}}$ to get $V' := (V^{\mathcal{M}})'$ which computes the UGS $\bar{\mathfrak{G}}'$.
  - Then play $\mathfrak{G}'_{n+1}$.
- This is self-referential, but we are used to that :)
- The compression algorithm is indeed applicable (check execution times of the various steps...)
- Define $\mathfrak{G}_{\mathcal{M}} := \mathfrak{G}_1$.
- Why does this work?

MIP* = RE from Compression: Part I

- Given $\mathcal{M}$, we define a Turing machine $V^{\mathcal{M}}$ which computes a UGS $\bar{\mathfrak{G}}^{\mathcal{M}} = (\mathfrak{G}_1, \mathfrak{G}_2, \ldots)$.
- Here is how $\mathfrak{G}_n$ looks:
  - Run $\mathcal{M}$ on the empty input for n time steps. If $\mathcal{M}$ halts, then victory!
  - If not, run C on $V^{\mathcal{M}}$ to get $V' := (V^{\mathcal{M}})'$ which computes the UGS $\bar{\mathfrak{G}}'$.
  - Then play $\mathfrak{G}'_{n+1}$.
- This is self-referential, but we are used to that :)
- The compression algorithm is indeed applicable (check execution times of the various steps...)
- Define $\mathfrak{G}_{\mathcal{M}} := \mathfrak{G}_1$.
- Why does this work?

MIP* = RE from Compression: Part I

- Given $\mathcal{M}$, we define a Turing machine $V^{\mathcal{M}}$ which computes a UGS $\bar{\mathfrak{G}}^{\mathcal{M}} = (\mathfrak{G}_1, \mathfrak{G}_2, \ldots)$.
- Here is how $\mathfrak{G}_n$ looks:
  - Run $\mathcal{M}$ on the empty input for n time steps. If $\mathcal{M}$ halts, then victory!
  - If not, run C on $V^{\mathcal{M}}$ to get $V' := (V^{\mathcal{M}})'$ which computes the UGS $\bar{\mathfrak{G}}'$.
  - Then play $\mathfrak{G}'_{n+1}$.
- This is self-referential, but we are used to that :)
- The compression algorithm is indeed applicable (check execution times of the various steps...)
- Define $\mathfrak{G}_{\mathcal{M}} := \mathfrak{G}_1$.
- Why does this work?

MIP* = RE from Compression: Part I

- Given $\mathcal{M}$, we define a Turing machine $V^{\mathcal{M}}$ which computes a UGS $\bar{\mathfrak{G}}^{\mathcal{M}} = (\mathfrak{G}_1, \mathfrak{G}_2, \ldots)$.
- Here is how $\mathfrak{G}_n$ looks:
  - Run $\mathcal{M}$ on the empty input for n time steps. If $\mathcal{M}$ halts, then victory!
  - If not, run C on $V^{\mathcal{M}}$ to get $V' := (V^{\mathcal{M}})'$ which computes the UGS $\bar{\mathfrak{G}}'$.
  - Then play $\mathfrak{G}'_{n+1}$.
- This is self-referential, but we are used to that :)
- The compression algorithm is indeed applicable (check execution times of the various steps...)
- Define $\mathfrak{G}_{\mathcal{M}} := \mathfrak{G}_1$.
- Why does this work?

MIP* = RE from Compression: Part I

- Given $\mathcal{M}$, we define a Turing machine $V^{\mathcal{M}}$ which computes a UGS $\bar{\mathfrak{G}}^{\mathcal{M}} = (\mathfrak{G}_1, \mathfrak{G}_2, \ldots)$.
- Here is how $\mathfrak{G}_n$ looks:
  - Run $\mathcal{M}$ on the empty input for n time steps. If $\mathcal{M}$ halts, then victory!
  - If not, run C on $V^{\mathcal{M}}$ to get $V' := (V^{\mathcal{M}})'$ which computes the UGS $\bar{\mathfrak{G}}'$.
  - Then play $\mathfrak{G}'_{n+1}$.
- This is self-referential, but we are used to that :)
- The compression algorithm is indeed applicable (check execution times of the various steps...)
- Define $\mathfrak{G}_{\mathcal{M}} := \mathfrak{G}_1$.
- Why does this work?

MIP* = RE from Compression: Part I

- Given $\mathcal{M}$, we define a Turing machine $V^{\mathcal{M}}$ which computes a UGS $\bar{\mathfrak{G}}^{\mathcal{M}} = (\mathfrak{G}_1, \mathfrak{G}_2, \ldots)$.
- Here is how $\mathfrak{G}_n$ looks:
  - Run $\mathcal{M}$ on the empty input for n time steps. If $\mathcal{M}$ halts, then victory!
  - If not, run C on $V^{\mathcal{M}}$ to get $V' := (V^{\mathcal{M}})'$ which computes the UGS $\bar{\mathfrak{G}}'$.
  - Then play $\mathfrak{G}'_{n+1}$.
- This is self-referential, but we are used to that :)
- The compression algorithm is indeed applicable (check execution times of the various steps...)
- Define $\mathfrak{G}_{\mathcal{M}} := \mathfrak{G}_1$.
- Why does this work?

MIP* = RE from Compression: Part II

- Case 1: $\mathcal{M}$ halts, say in T steps.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = 1$ for all $n \geq T$.
- What about $n < T$?
- For $n < T$, $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$.
- So $\mathrm{val}^*(\mathfrak{G}_{T-1}) = \mathrm{val}^*(\mathfrak{G}'_T) = 1$ since $\mathrm{val}^*(\mathfrak{G}_T) = 1$ (preservation of perfect completeness).
- By induction, we get that $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) = 1$.

MIP* = RE from Compression: Part II

- Case 1: $\mathcal{M}$ halts, say in T steps.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = 1$ for all $n \geq T$.
- What about $n < T$?
- For $n < T$, $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$.
- So $\mathrm{val}^*(\mathfrak{G}_{T-1}) = \mathrm{val}^*(\mathfrak{G}'_T) = 1$ since $\mathrm{val}^*(\mathfrak{G}_T) = 1$ (preservation of perfect completeness).
- By induction, we get that $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) = 1$.

MIP* = RE from Compression: Part II

- Case 1: $\mathcal{M}$ halts, say in T steps.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = 1$ for all $n \geq T$.
- What about $n < T$?
- For $n < T$, $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$.
- So $\mathrm{val}^*(\mathfrak{G}_{T-1}) = \mathrm{val}^*(\mathfrak{G}'_T) = 1$ since $\mathrm{val}^*(\mathfrak{G}_T) = 1$ (preservation of perfect completeness).
- By induction, we get that $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) = 1$.

MIP* = RE from Compression: Part II

- Case 1: $\mathcal{M}$ halts, say in T steps.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = 1$ for all $n \geq T$.
- What about $n < T$?
- For $n < T$, $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$.
- So $\mathrm{val}^*(\mathfrak{G}_{T-1}) = \mathrm{val}^*(\mathfrak{G}'_T) = 1$ since $\mathrm{val}^*(\mathfrak{G}_T) = 1$ (preservation of perfect completeness).
- By induction, we get that $\mathrm{val}^*(\mathfrak{G}_\mathcal{M}) = \mathrm{val}^*(\mathfrak{G}_1) = 1$.

MIP* = RE from Compression: Part II

- Case 1: $\mathcal{M}$ halts, say in T steps.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = 1$ for all $n \geq T$.
- What about $n < T$?
- For $n < T$, $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$.
- So $\mathrm{val}^*(\mathfrak{G}_{T-1}) = \mathrm{val}^*(\mathfrak{G}'_T) = 1$ since $\mathrm{val}^*(\mathfrak{G}_T) = 1$ (preservation of perfect completeness).
- By induction, we get that $\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) = 1$.

MIP* = RE from Compression: Part II

- Case 1: $\mathcal{M}$ halts, say in T steps.
- Then $\text{val}^*(\mathfrak{G}_n) = 1$ for all $n \geq T$.
- What about $n < T$?
- For $n < T$, $\text{val}^*(\mathfrak{G}_n) = \text{val}^*(\mathfrak{G}'_{n+1})$.
- So $\text{val}^*(\mathfrak{G}_{T-1}) = \text{val}^*(\mathfrak{G}'_T) = 1$ since $\text{val}^*(\mathfrak{G}_T) = 1$ (preservation of perfect completeness).
- By induction, we get that $\text{val}^*(\mathfrak{G}_{\mathcal{M}}) = \text{val}^*(\mathfrak{G}_1) = 1$.

MIP* = RE from Compression: Part III

- Now suppose that $\mathcal{M}$ does not halt.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$ and $\mathcal{E}(\mathfrak{G}_n, r) = \mathcal{E}(\mathfrak{G}'_{n+1}, r)$ for all $n \in \mathbb{N}$ and $r \in [0,1]$.
- $\mathcal{E}(\mathfrak{G}'_{n+1}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+1}, \frac{1}{2}) = \mathcal{E}(\mathfrak{G}'_{n+2}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+2}, \frac{1}{2}) \cdots$
- $\therefore \mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}'_m, \frac{1}{2})$ for all $m > n$.
- OTOH $\mathcal{E}(\mathfrak{G}'_m, \frac{1}{2}) \geq m$ for all $m \in \mathbb{N}$.
- Therefore $\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) = \infty$ for all $n \in \mathbb{N}$ and thus

$$\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) < \frac{1}{2}.$$

MIP* = RE from Compression: Part III

- Now suppose that $\mathcal{M}$ does not halt.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$ and $\mathcal{E}(\mathfrak{G}_n, r) = \mathcal{E}(\mathfrak{G}'_{n+1}, r)$ for all $n \in \mathbb{N}$ and $r \in [0, 1]$.
- $\mathcal{E}(\mathfrak{G}'_{n+1}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+1}, \frac{1}{2}) = \mathcal{E}(\mathfrak{G}'_{n+2}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+2}, \frac{1}{2}) \cdots$
- $\therefore \mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}'_m, \frac{1}{2})$ for all $m > n$.
- OTOH $\mathcal{E}(\mathfrak{G}'_m, \frac{1}{2}) \geq m$ for all $m \in \mathbb{N}$.
- Therefore $\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) = \infty$ for all $n \in \mathbb{N}$ and thus

$$\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) < \frac{1}{2}.$$

MIP* = RE from Compression: Part III

- Now suppose that $\mathcal{M}$ does not halt.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$ and $\mathcal{E}(\mathfrak{G}_n, r) = \mathcal{E}(\mathfrak{G}'_{n+1}, r)$ for all $n \in \mathbb{N}$ and $r \in [0, 1]$.
- $\mathcal{E}(\mathfrak{G}'_{n+1}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+1}, \frac{1}{2}) = \mathcal{E}(\mathfrak{G}'_{n+2}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+2}, \frac{1}{2}) \cdots$
- $\therefore \mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}'_m, \frac{1}{2})$ for all $m > n$.
- OTOH $\mathcal{E}(\mathfrak{G}'_m, \frac{1}{2}) \geq m$ for all $m \in \mathbb{N}$.
- Therefore $\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) = \infty$ for all $n \in \mathbb{N}$ and thus

$$\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) < \frac{1}{2}.$$

$\mathrm{MIP}^* = \mathrm{RE}$ from Compression: Part III

- Now suppose that $\mathcal{M}$ does not halt.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$ and $\mathcal{E}(\mathfrak{G}_n, r) = \mathcal{E}(\mathfrak{G}'_{n+1}, r)$ for all $n \in \mathbb{N}$ and $r \in [0, 1]$.
- $\mathcal{E}(\mathfrak{G}'_{n+1}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+1}, \frac{1}{2}) = \mathcal{E}(\mathfrak{G}'_{n+2}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+2}, \frac{1}{2}) \cdots$
- $\therefore \mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}'_m, \frac{1}{2})$ for all $m > n$.
- OTOH $\mathcal{E}(\mathfrak{G}'_m, \frac{1}{2}) \geq m$ for all $m \in \mathbb{N}$.
- Therefore $\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) = \infty$ for all $n \in \mathbb{N}$ and thus

$$\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) < \frac{1}{2}.$$

MIP* = RE from Compression: Part III

- Now suppose that $\mathcal{M}$ does not halt.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$ and $\mathcal{E}(\mathfrak{G}_n, r) = \mathcal{E}(\mathfrak{G}'_{n+1}, r)$ for all $n \in \mathbb{N}$ and $r \in [0, 1]$.
- $\mathcal{E}(\mathfrak{G}'_{n+1}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+1}, \frac{1}{2}) = \mathcal{E}(\mathfrak{G}'_{n+2}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+2}, \frac{1}{2}) \cdots$
- $\therefore \mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}'_m, \frac{1}{2})$ for all $m > n$.
- OTOH $\mathcal{E}(\mathfrak{G}'_m, \frac{1}{2}) \geq m$ for all $m \in \mathbb{N}$.
- Therefore $\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) = \infty$ for all $n \in \mathbb{N}$ and thus

$$\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) < \frac{1}{2}.$$

MIP* = RE from Compression: Part III

- Now suppose that $\mathcal{M}$ does not halt.
- Then $\mathrm{val}^*(\mathfrak{G}_n) = \mathrm{val}^*(\mathfrak{G}'_{n+1})$ and $\mathcal{E}(\mathfrak{G}_n, r) = \mathcal{E}(\mathfrak{G}'_{n+1}, r)$ for all $n \in \mathbb{N}$ and $r \in [0, 1]$.
- $\mathcal{E}(\mathfrak{G}'_{n+1}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+1}, \frac{1}{2}) = \mathcal{E}(\mathfrak{G}'_{n+2}, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}_{n+2}, \frac{1}{2}) \cdots$
- $\therefore \mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) \geq \mathcal{E}(\mathfrak{G}'_m, \frac{1}{2})$ for all $m > n$.
- OTOH $\mathcal{E}(\mathfrak{G}'_m, \frac{1}{2}) \geq m$ for all $m \in \mathbb{N}$.
- Therefore $\mathcal{E}(\mathfrak{G}_n, \frac{1}{2}) = \infty$ for all $n \in \mathbb{N}$ and thus

$$\mathrm{val}^*(\mathfrak{G}_{\mathcal{M}}) = \mathrm{val}^*(\mathfrak{G}_1) < \frac{1}{2}.$$

Hand-waving about the proof of the Compression Theorem

- Question reduction
  - Get the players to sample questions for themselves.
  - Uses *rigidity of nonlocal games* and the *Heisenberg uncertainty principle*.
  - Brings the sampler complexity down from $\mathrm{poly}(n)$ to $\mathrm{poly}(\log n)$.
- Answer reduction
  - The players must now also compute the decision predicate $D_n(x, y, a, b)$ for themselves
  - They must include a *succint proof* that they computed D_n correctly
  - Uses *probabilistically checkable proofs* (PCP)
  - Brings the decider complexity down to $\mathrm{poly}(\log n)$

Hand-waving about the proof of the Compression Theorem

- Question reduction
  - Get the players to sample questions for themselves.
  - Uses *rigidity of nonlocal games* and the *Heisenberg uncertainty principle*.
  - Brings the sampler complexity down from $\mathrm{poly}(n)$ to $\mathrm{poly}(\log n)$.
- Answer reduction
  - The players must now also compute the decision predicate $D_n(x, y, a, b)$ for themselves
  - They must include a *succint proof* that they computed D_n correctly
  - Uses *probabilistically checkable proofs* (PCP)
  - Brings the decider complexity down to $\mathrm{poly}(\log n)$