Anchoring games for parallel repetition

Henry Yuen

MIT

Mohammad Bavarian

MIT

Thomas Vidick

CalTech

Roadmap

Games and parallel repetition

Feige's Counterexample

The anchoring transformation and our results

Proof ideas

Roadmap

Games and parallel repetition

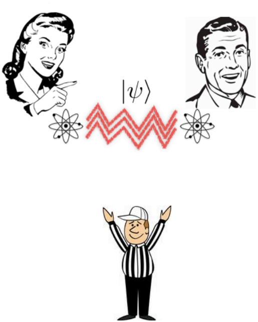
Feige's Counterexample

The anchoring transformation and our results

Proof ideas

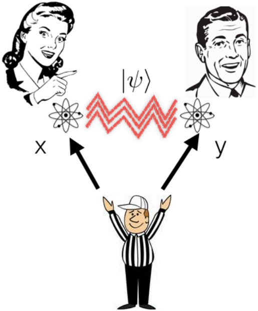
Two player games

Game G: distribution $\mu(x, y)$, predicate $V(x, y, a, b)$



Two player games

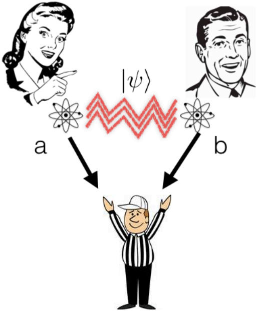
Game G: distribution $\mu(x, y)$, predicate $V(x, y, a, b)$



- Referee samples questions $(x, y) \sim \mu$
- Alice gets x, Bob gets y

Two player games

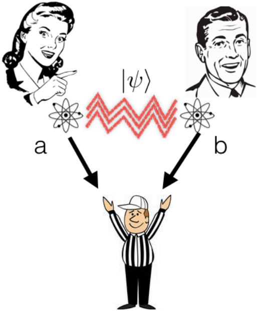
Game G: distribution $\mu(x, y)$, predicate $V(x, y, a, b)$



- Referee samples questions $(x, y) \sim \mu$
- Alice gets x, Bob gets y
- Alice answers with a, Bob answers with b

Two player games

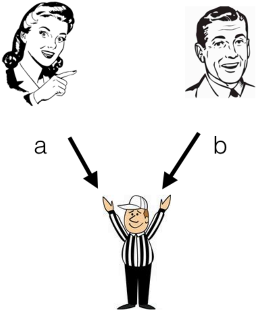
Game G: distribution $\mu(x,y)$, predicate $V(x,y,a,b)$



- Referee samples questions $(x,y) \sim \mu$
- Alice gets x, Bob gets y
- Alice answers with a, Bob answers with b
- Players **win** iff $V(x,y,a,b) = 1$

Two player games

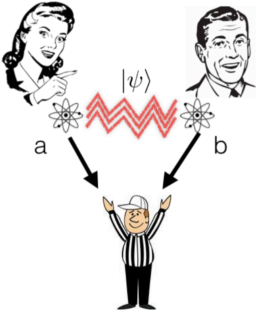
Game G: distribution $\mu(x, y)$, predicate $V(x, y, a, b)$



- **Classical value**: $\mathrm{val}(G) =$ maximum winning probability when Alice and Bob's strategies are *local* (i.e. no entanglement).
  - Can assume strategies are **deterministic**.

Two player games

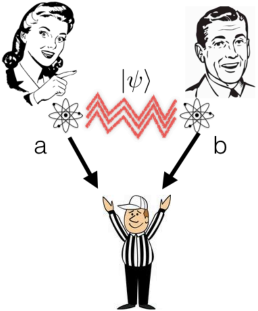
Game G: distribution $\mu(x, y)$, predicate $V(x, y, a, b)$



- **Classical value**: $\mathrm{val}(G) =$ maximum winning probability when Alice and Bob's strategies are *local* (i.e. no entanglement).
  - Can assume strategies are **deterministic**.
- **Entangled value**: $\mathrm{val}^{\star}(G) =$ maximum winning probability when Alice and Bob are *quantumly entangled*.

Two player games

Game G: distribution $\mu(x, y)$, predicate $V(x, y, a, b)$



- **Classical value**: $\mathrm{val}(G)$ = maximum winning probability when Alice and Bob's strategies are *local* (i.e. no entanglement).
  - Can assume strategies are **deterministic**.
- **Entangled value**: $\mathrm{val}^\star(G)$ = maximum winning probability when Alice and Bob are *quantumly entangled*.
- **Entanglement can help**: There exist G with $\mathrm{val}(G) < \mathrm{val}^\star(G)$ (e.g. CHSH).

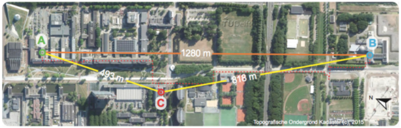
Why games?

Theoretical Computer Science

- Local checking of proofs (classical and quantum), hardness of constraint satisfaction problems, cryptography,...

Testing non-locality in quantum mechanics

- Bell inequality *violations* correspond to $\mathrm{val}^{\star}(G) > \mathrm{val}(G)$
- The recent Loophole-Free Bell Test by [Hensen, et al.] is a two player game in action



Device independent information processing

- Certified random number generation, QKD, delegated quantum computation,...

Testing non-locality in one round

- Consider the Greenberger-Horne-Zeilinger (GHZ) game
  - Three players
  - $\mathrm{val}(GHZ) = 3/4$
  - $\mathrm{val}^{\star}(GHZ) = 1$
- GHZ game was used in one of the earliest tests of quantum non-locality.

Testing non-locality in one round

- Consider the Greenberger-Horne-Zeilinger (GHZ) game
  - Three players
  - $\mathrm{val}(GHZ) = 3/4$
  - $\mathrm{val}^{\star}(GHZ) = 1$
- GHZ game was used in one of the earliest tests of quantum non-locality.
- Testing non-locality using the GHZ game:
  - **Lose**: Players are not using optimal quantum strategy.
  - **Win**: Maybe players are using a quantum strategy.

Testing non-locality in one round

- Consider the Greenberger-Horne-Zeilinger (GHZ) game
  - Three players
  - $\mathrm{val}(GHZ) = 3/4$
  - $\mathrm{val}^{\star}(GHZ) = 1$
- GHZ game was used in one of the earliest tests of quantum non-locality.
- Testing non-locality using the GHZ game:
  - **Lose**: Players are not using optimal quantum strategy.
  - **Win**: Maybe players are using a quantum strategy.
- **Want**: Transform GHZ into a game G where
  - $\mathrm{val}^{\star}(G) = 1$
  - $\mathrm{val}(G) \leq 0.01$

Testing non-locality in one round

- Consider the Greenberger-Horne-Zeilinger (GHZ) game
  - Three players
  - $\mathrm{val}(GHZ) = 3/4$
  - $\mathrm{val}^{\star}(GHZ) = 1$
- GHZ game was used in one of the earliest tests of quantum non-locality.
- Testing non-locality using the GHZ game:
  - **Lose**: Players are not using optimal quantum strategy.
  - **Win**: Maybe players are using a quantum strategy.
- **Want**: Transform GHZ into a game G where
  - $\mathrm{val}^{\star}(G) = 1$
  - $\mathrm{val}(G) \leq 0.01$
- This is called **gap amplification**.

Testing non-locality in one round

Idea: Play many instances of the GHZ game in parallel.

GHZ^n: Alice, Bob and Charlie receive inputs for n GHZ games simultaneously and have to win all of them.

Testing non-locality in one round

Idea: Play many instances of the GHZ game in parallel.

GHZ^n: Alice, Bob and Charlie receive inputs for n GHZ games simultaneously and have to win all of them.

- $\mathrm{val}^\star(\mathrm{GHZ}^n) = 1$.
  - Play each GHZ game independently using entangled strategy.

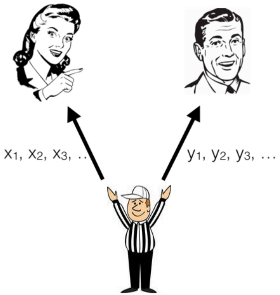
Testing non-locality in one round

Idea: Play many instances of the GHZ game in parallel.

GHZ^n: Alice, Bob and Charlie receive inputs for n GHZ games simultaneously and have to win all of them.

- $\mathrm{val}^\star(\mathrm{GHZ}^n) = 1$.
  - Play each GHZ game independently using entangled strategy.
- $\mathrm{val}(\mathrm{GHZ}^n) \overset{?}{\leq} (3/4)^n$

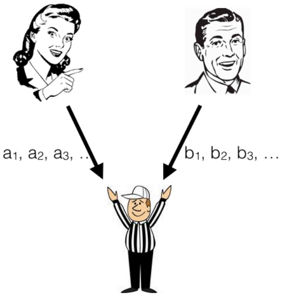
Parallel repetition of games



In G^n, the referee plays n independent instances of G **simultaneously** with Alice and Bob.

- Referee samples i.i.d. $(x_1, y_1), \ldots, (x_n, y_n) \sim \mu$
- Alice gets $(x_1, \ldots, x_n)$, Bob gets $(y_1, \ldots, y_n)$

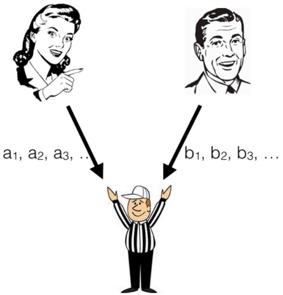
Parallel repetition of games



In G^n, the referee plays n independent instances of G **simultaneously** with Alice and Bob.

- Referee samples i.i.d. $(x_1, y_1), \ldots, (x_n, y_n) \sim \mu$
- Alice gets $(x_1, \ldots, x_n)$, Bob gets $(y_1, \ldots, y_n)$
- Alice and Bob win G^n if they win **all** n instances of G.

Parallel repetition of games



In G^n, the referee plays n independent instances of G **simultaneously** with Alice and Bob.

- Referee samples i.i.d. $(x_1, y_1), \ldots, (x_n, y_n) \sim \mu$
- Alice gets $(x_1, \ldots, x_n)$, Bob gets $(y_1, \ldots, y_n)$
- Alice and Bob win G^n if they win **all** n instances of G.

The Parallel Repetition Question: How does $\mathrm{val}(G^n)$ relate to $\mathrm{val}(G)$ and n?

Parallel repetition of games

- In 1995, Ran Raz proved the **Parallel Repetition Theorem**
  - For two player games G with $\mathrm{val}(G) < 1$, $\mathrm{val}(G^n)$ decays *exponentially fast* in n.

Parallel repetition of games

- In 1995, Ran Raz proved the **Parallel Repetition Theorem**
  - For two player games G with $\mathrm{val}(G) < 1$, $\mathrm{val}(G^n)$ decays *exponentially fast* in n.
  - Proof was highly non-trivial; one of the first applications of information theory to complexity theory.

Parallel repetition of games

- In 1995, Ran Raz proved the **Parallel Repetition Theorem**
  - For two player games G with $\mathrm{val}(G) < 1$, $\mathrm{val}(G^n)$ decays *exponentially fast* in n.
  - Proof was highly non-trivial; one of the first applications of information theory to complexity theory.
- **Open questions**: Does the Parallel Repetition Theorem hold for:
  - Entangled games?
  - Multiplayer games?

Parallel repetition of games

- In 1995, Ran Raz proved the **Parallel Repetition Theorem**
  - For two player games G with $\mathrm{val}(G) < 1$, $\mathrm{val}(G^n)$ decays *exponentially fast* in n.
  - Proof was highly non-trivial; one of the first applications of information theory to complexity theory.
- **Open questions**: Does the Parallel Repetition Theorem hold for:
  - Entangled games?
  - Multiplayer games?
- **Our result**: We change the problem by solving the **gap amplification** problem for entangled games and multiplayer games by introducing a technique called **anchored parallel repetition**.

Roadmap

Games and parallel repetition

Feige's Counterexample

The anchoring transformation and our results

Proof ideas

Parallel repetition of games

- How does $\mathrm{val}(G^n)$ compare to $\mathrm{val}(G)$?

Parallel repetition of games

- How does $\mathrm{val}(G^n)$ compare to $\mathrm{val}(G)$?
  - **Trivial bound**: $\mathrm{val}(G)^n \leq \mathrm{val}(G^n)$.

Parallel repetition of games

- How does $\mathrm{val}(G^n)$ compare to $\mathrm{val}(G)$?
  - **Trivial bound**: $\mathrm{val}(G)^n \leq \mathrm{val}(G^n)$.

- **"Theorem"**: $\mathrm{val}(G^n) = \mathrm{val}(G)^n$.
  - "**Proof**": The instances of G are independent of each other, and each instance cannot be won with probability greater than $\mathrm{val}(G)$, so the maximum success probability is at most $\mathrm{val}(G)^n$.

Parallel repetition of games

- How does $\mathrm{val}(G^n)$ compare to $\mathrm{val}(G)$?
  - **Trivial bound**: $\mathrm{val}(G)^n \leq \mathrm{val}(G^n)$.

- **“Theorem”**: $\mathrm{val}(G^n) = \mathrm{val}(G)^n$.
  - “**Proof**”: The instances of G are independent of each other, and each instance cannot be won with probability greater than $\mathrm{val}(G)$, so the maximum success probability is at most $\mathrm{val}(G)^n$.

$\mathrm{val}(G^n) \neq \mathrm{val}(G)^n$ **in general!**

Parallel repetition of games

- How does $\mathrm{val}(G^n)$ compare to $\mathrm{val}(G)$?
  - **Trivial bound**: $\mathrm{val}(G)^n \leq \mathrm{val}(G^n)$.

- **"Theorem"**: $\mathrm{val}(G^n) = \mathrm{val}(G)^n$.
  - "**Proof**": The instances of G are independent of each other, and each instance cannot be won with probability greater than $\mathrm{val}(G)$, so the maximum success probability is at most $\mathrm{val}(G)^n$.

$\mathrm{val}(G^n) \neq \mathrm{val}(G)^n$ **in general!**

Next: Feige's Counterexample G where $\frac{1}{2} = \mathrm{val}(G) = \mathrm{val}(G^2)$.

Feige's Counterexample

- Alice and Bob get uniform and independent bits $x, y \in \{0, 1\}$.
- Alice and Bob both output a statement of the form

"**[Alice/Bob]'s input bit is [$0/1$]**"

- Players win iff their statements agree and are true.

Feige's Counterexample

- Alice and Bob get uniform and independent bits $x, y \in \{0, 1\}$.
- Alice and Bob both output a statement of the form

"[Alice/Bob]'s input bit is [$0/1$]"

- Players win iff their statements agree and are true.

Examples

Alice gets $x = 0$, Bob gets $y = 1$.

- Alice says "Alice's input bit is 0", Bob says "Alice's input bit is 0". ✓
- Alice says "Alice's input bit is 0", Bob says "Bob's input bit is 1". ✗

Feige's Counterexample

- Alice and Bob get uniform and independent bits $x, y \in \{0, 1\}$.
- Alice and Bob both output a statement of the form

"[Alice/Bob]'s input bit is [$0/1$]"

- Players win iff their statements agree and are true.

Examples

Alice gets $x = 0$, Bob gets $y = 1$.

- Alice says "Alice's input bit is 0", Bob says "Alice's input bit is 0". ✓
- Alice says "Alice's input bit is 0", Bob says "Bob's input bit is 1". ✗

$$\mathrm{val}(G) = 1/2$$

Feige's Counterexample

The repeated game G^2

- Alice gets $(x_1, x_2) \in \{0,1\}^2$
- Bob gets $(y_1, y_2) \in \{0,1\}^2$
- Alice and Bob have to output two statements of the form:

"[Alice/Bob]'s input bit in G_1 is [$0/1$]"

"[Alice/Bob]'s input bit in G_2 is [$0/1$]"

Feige's Counterexample

The repeated game G^2

- Alice gets $(x_1, x_2) \in \{0,1\}^2$
- Bob gets $(y_1, y_2) \in \{0,1\}^2$
- Alice and Bob have to output two statements of the form:

"**[Alice/Bob]'s input bit in G_1 is [$0/1$]**"

"**[Alice/Bob]'s input bit in G_2 is [$0/1$]**"

- Would expect $\mathrm{val}(G^2) = \mathrm{val}(G)^2 = \frac{1}{4}$.

Feige's Counterexample

Strategy for G^2

Alice says:

"**Alice's input in G_1 is x_1**"

"**Bob's input in G_2 is x_1**"

Bob says:

"**Alice's input in G_1 is y_2**"

"**Bob's input in G_2 is y_2**"

Feige's Counterexample

Strategy for G^2

Alice says:

"Alice's input in G_1 is x_1"

"Bob's input in G_2 is x_1"

Bob says:

"Alice's input in G_1 is y_2"

"Bob's input in G_2 is y_2"

Analyzing $\mathrm{val}(G^2)$

- $\Pr[\text{Win } G_1] = \Pr[x_1 = y_2] = 1/2$.

Feige's Counterexample

Strategy for G^2

Alice says:

"Alice's input in G_1 is x_1"

"Bob's input in G_2 is x_1"

Bob says:

"Alice's input in G_1 is y_2"

"Bob's input in G_2 is y_2"

Analyzing $\mathrm{val}(G^2)$

- $\Pr[\text{Win } G_1] = \Pr[x_1 = y_2] = 1/2$.
- $\Pr[\text{Win } G_2 \mid \text{Win } G_1] = \Pr[\text{Win } G_2 \mid x_1 = y_2] = 1$.

Feige's Counterexample

Strategy for G^2

Alice says:

"Alice's input in G_1 is x_1"

"Bob's input in G_2 is x_1"

Bob says:

"Alice's input in G_1 is y_2"

"Bob's input in G_2 is y_2"

Analyzing $\mathrm{val}(G^2)$

- $\Pr[\text{Win } G_1] = \Pr[x_1 = y_2] = 1/2$.
- $\Pr[\text{Win } G_2 \mid \text{Win } G_1] = \Pr[\text{Win } G_2 \mid x_1 = y_2] = 1$.
- $\Pr[\text{Win } G^2] = \Pr[\text{Win } G_2 | \text{Win } G_1] \times \Pr[\text{Win } G_1] = \frac{1}{2}$.

Feige's Counterexample

Strategy for G^2

Alice says:

"Alice's input in G_1 is x_1"

"Bob's input in G_2 is x_1"

Bob says:

"Alice's input in G_1 is y_2"

"Bob's input in G_2 is y_2"

Analyzing $\mathrm{val}(G^2)$

- $\Pr[\text{Win } G_1] = \Pr[x_1 = y_2] = 1/2.$
- $\Pr[\text{Win } G_2 \mid \text{Win } G_1] = \Pr[\text{Win } G_2 \mid x_1 = y_2] = 1.$
- $\Pr[\text{Win } G^2] = \Pr[\text{Win } G_2 | \text{Win } G_1] \times \Pr[\text{Win } G_1] = \frac{1}{2}.$
- **Winning G_2 is correlated with winning G_1!**

$$\mathrm{val}(G^2) = \mathrm{val}(G)$$

Parallel repetition of games

Non-product strategies makes the parallel repetition of games non-trivial!

- The difficulty of non-product strategies is pervasive
  - Additivity conjectures in quantum information
  - Hardness amplification of proof systems
  - Direct sum/product theorems in complexity theory

Parallel repetition of games

Parallel Repetition Theorem [Raz '95, Holenstein '07]

For a two-player game G with $\mathrm{val}(G) = 1 - \varepsilon \geq 1/2$,

$$\mathrm{val}(G^n) = (1 - \varepsilon^3)^{\Omega(n/s)}.$$

where s is length of players' answers.

Parallel repetition of games

Parallel Repetition Theorem [Raz '95, Holenstein '07]

For a two-player game G with $\mathrm{val}(G) = 1 - \varepsilon \geq 1/2$,

$$\mathrm{val}(G^n) = (1 - \varepsilon^3)^{\Omega(n/s)}.$$

where s is length of players' answers.

Two major open questions since then:

Does Raz's parallel repetition theorem extend to

1. More than two players?
2. Entangled players?

Answers known for special classes of games.

- **Quantum parallel repetition**
  - XOR games [Cleve, et al. ’08]
  - Unique games [Kempe-Regev-Toner ’08]
  - Free games [Chailloux-Scarpa ’14, Jain-Pereszlényi-Yao ’14, Chung-Wu-Y. ’15]
  - Projection games [Dinur-Steurer-Vidick ’14]
- **Multiplayer parallel repetition**
  - Free games [Chung-Wu-Y. ’15]

Answers known for special classes of games.

- **Quantum parallel repetition**
  - XOR games [Cleve, et al. ’08]
  - Unique games [Kempe-Regev-Toner ’08]
  - Free games [Chailloux-Scarpa ’14, Jain-Pereszlényi-Yao ’14, Chung-Wu-Y. ’15]
  - Projection games [Dinur-Steurer-Vidick ’14]
- **Multiplayer parallel repetition**
  - Free games [Chung-Wu-Y. ’15]

General case is still wide open!

Changing the problem

For the purposes of gap amplification, a completely general parallel repetition theorem is **unnecessary**.

Changing the problem

For the purposes of gap amplification, a completely general parallel repetition theorem is **unnecessary**.

- Raz's Parallel Repetition Theorem: $G \to G^n$ performs gap amplification for 2-player classical games.

Changing the problem

For the purposes of gap amplification, a completely general parallel repetition theorem is **unnecessary**.

- Raz's Parallel Repetition Theorem: $G \to G^n$ performs gap amplification for 2-player classical games.

We present the **anchoring transformation**:

$$G \to G_\perp \to G_\perp^n$$

For all G, $G_\perp$ is an equivalent game that obeys quantum and multiplayer parallel repetition theorems.

Changing the problem

For the purposes of gap amplification, a completely general parallel repetition theorem is **unnecessary**.

- Raz's Parallel Repetition Theorem: $G \to G^n$ performs gap amplification for 2-player classical games.

We present the **anchoring transformation**:

$$G \to G_\perp \to G_\perp^n$$

For all G, $G_\perp$ is an equivalent game that obeys quantum and multiplayer parallel repetition theorems.

- Technique of *changing the game* for gap amplification is inspired by [Feige-Kilian '94].

Roadmap

Games and parallel repetition

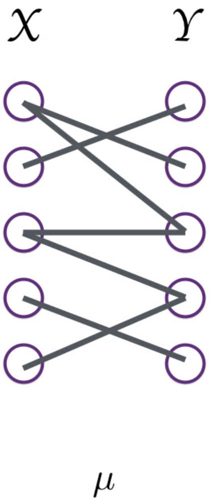
Feige's Counterexample

The anchoring transformation and our results

Proof ideas

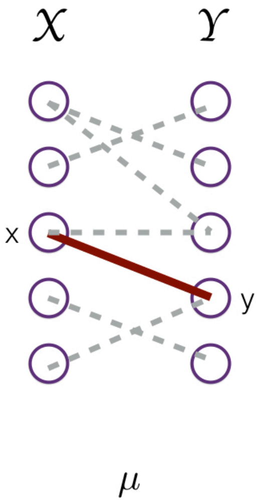
Anchoring transformation

- A two player game G can be viewed as a **graph game**.
- $(x, y) \sim \mu$ is a uniformly random edge from a bipartite graph.



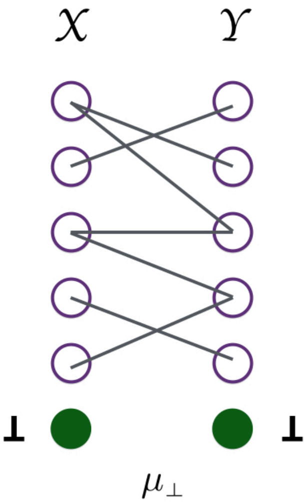
Anchoring transformation

- A two player game G can be viewed as a **graph game**.
- $(x, y) \sim \mu$ is a uniformly random edge from a bipartite graph.



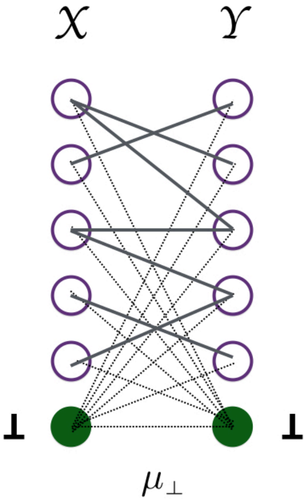
Anchoring transformation

- $G \to G_\perp$: Add **anchor questions**, and connect all other questions to them.



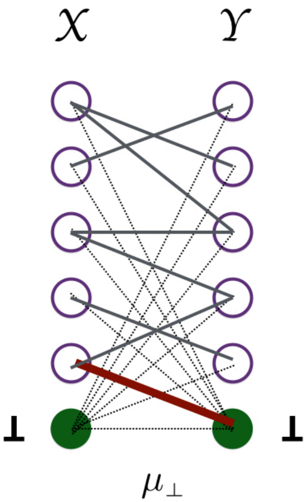
Anchoring transformation

- $G \to G_\perp$: Add **anchor questions**, and connect all other questions to them.
  - Add enough **anchor edges** so that they form a (small) constant fraction of the total number of edges (say $1/100$).



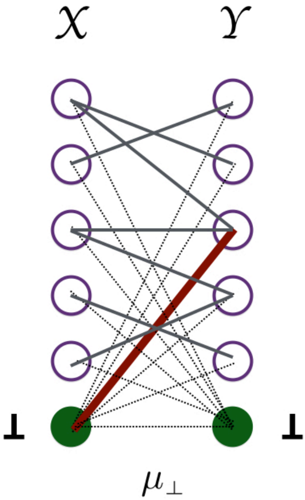
Anchoring transformation

- $G \rightarrow G_\perp$: Add **anchor questions**, and connect all other questions to them.
  - Add enough **anchor edges** so that they form a (small) constant fraction of the total number of edges (say $1/100$).



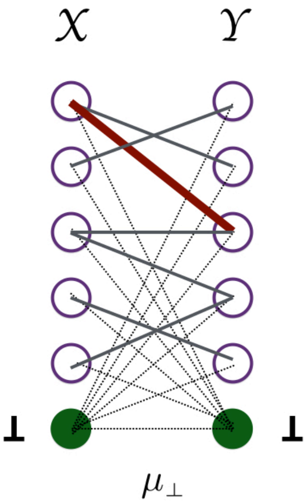
Anchoring transformation

- $G \to G_\perp$: Add **anchor questions**, and connect all other questions to them.
    - Add enough **anchor edges** so that they form a (small) constant fraction of the total number of edges (say $1/100$).



Anchoring transformation

- $G \to G_{\perp}$: Add **anchor questions**, and connect all other questions to them.
  - Add enough **anchor edges** so that they form a (small) constant fraction of the total number of edges (say $1/100$).
- If either player receives "$\perp$", then players **automatically win**. Otherwise, the referee checks according to G.



Anchored games

G: k-player game with question distribution μ.

In $G_\perp$:

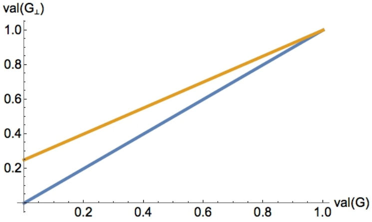
- Referee samples question according to μ.
- With probability α, each player's question independently replaced with anchor question "$\perp$" (α is called the **probability of anchoring**).
- If any player receives "$\perp$", players win automatically.
- Otherwise, referee checks answers according to G.

Anchored games

G: k-player game with question distribution μ.

In $G_\perp$:

- Referee samples question according to μ.
- With probability α, each player's question independently replaced with anchor question "$\perp$" (α is called the **probability of anchoring**).
- If any player receives "$\perp$", players win automatically.
- Otherwise, referee checks answers according to G.



$$\mathrm{val}(G_\perp) = p_\alpha \cdot \mathrm{val}(G) + (1 - p_\alpha)$$

$$\mathrm{val}^\star(G_\perp) = p_\alpha \cdot \mathrm{val}^\star(G) + (1 - p_\alpha)$$

$$p_\alpha = (1-\alpha)^k$$

Our results

Theorem: Multiplayer parallel repetition

If G is a k-player game with $\mathrm{val}(G) = 1 - \varepsilon$, then

$$\mathrm{val}(G_{\perp}^{n}) = (1 - \varepsilon^{3})^{\Omega(n/s)}.$$

Our results

Theorem: Multiplayer parallel repetition

If G is a k-player game with $\mathrm{val}(G) = 1 - \varepsilon$, then

$$\mathrm{val}(G_{\perp}^{n}) = (1 - \varepsilon^{3})^{\Omega(n/s)}.$$

Theorem: Quantum parallel repetition

If G is a two-player game with $\mathrm{val}^{\star}(G) = 1 - \delta$, then

$$\mathrm{val}^{\star}(G_{\perp}^{n}) = (1 - \delta^{8})^{\Omega(n/s)}.$$

s denotes answer lengths of the players.

Applications: Testing non-locality

- Greenberger-Horne-Zeilinger (GHZ) game
  - Three players
  - $\mathrm{val}(GHZ) = 3/4$
  - $\mathrm{val}^{\star}(GHZ) = 1$

Applications: Testing non-locality

- Greenberger-Horne-Zeilinger (GHZ) game
  - Three players
  - $\mathrm{val}(GHZ) = 3/4$
  - $\mathrm{val}^\star(GHZ) = 1$
- **Using our multiplayer parallel repetition theorem**:
  - $\mathrm{val}^\star(\mathrm{GHZ}_\perp^n) = 1$
  - $\mathrm{val}(\mathrm{GHZ}_\perp^n) = e^{-\Omega(n)}$.

Applications: Complexity theory

- Suppose it is NP-hard (or QMA-hard) to distinguish between: given G,
  - $\mathrm{val}^\star(G) = 1$, or
  - $\mathrm{val}^\star(G) < 1 - \delta$.

Applications: Complexity theory

- Suppose it is NP-hard (or QMA-hard) to distinguish between: given G,
  - $\mathrm{val}^{\star}(G) = 1$, or
  - $\mathrm{val}^{\star}(G) < 1 - \delta$.
- **Using our quantum parallel repetition theorem**: Then for all $\varepsilon > 0$ it is NP-hard (or QMA-hard) to distinguish between: given G
  - $\mathrm{val}^{\star}(G) = 1$
  - $\mathrm{val}^{\star}(G) = \varepsilon$.

Roadmap

Games and parallel repetition

Feige's Counterexample

The anchoring transformation and our results

Proof ideas

Why does anchoring help?

An anchored game $G_\perp$ is *easier* than G. How could analyzing $G_\perp^n$ be helpful?

Why does anchoring help?

An anchored game $G_\perp$ is *easier* than G. How could analyzing $G_\perp^n$ be helpful?

Recall that the difficulty comes from non-product strategies.

- Strategies try to correlate winning in one round with winning in other rounds.
- E.g., Alice's answer for G_1 can depend on her question in G_2.

Why does anchoring help?

An anchored game $G_\perp$ is *easier* than G. How could analyzing $G_\perp^n$ be helpful?

Recall that the difficulty comes from non-product strategies.

- Strategies try to correlate winning in one round with winning in other rounds.
- E.g., Alice's answer for G_1 can depend on her question in G_2.

Intuition: Anchor questions randomly "disrupt" careful coordination of players!

- E.g., if Alice's question in G_2 is "$\perp$", she cannot use it to play G_1.
- But Bob doesn't know she received "$\perp$" in G_2!

Proof strategy

Proof by contradiction:

Proof strategy

Proof by contradiction: If $\mathrm{val}^\star(G^n)$ is too large (i.e. *supergood*),

Proof strategy

Proof by contradiction: If $\mathrm{val}^\star(G^n)$ is too large (i.e. *supergood*), then we get a strategy for G with success probability greater than $\mathrm{val}^\star(G)$.

Proof strategy

Proof by contradiction: If $\mathrm{val}^\star(G^n)$ is too large (i.e. *supergood*), then we get a strategy for G with success probability greater than $\mathrm{val}^\star(G)$.

Contradiction.

Proof strategy

Fix a *supergood* strategy for G^n.

- Entangled state: $|\psi\rangle$
- For all $\mathbf{x} = (x_1, \ldots, x_n)$, Alice uses POVM $\{A_{\mathbf{x}}(\mathbf{a})\}_{\mathbf{a}}$.
- For all $\mathbf{y} = (y_1, \ldots, y_n)$, Bob uses POVM $\{B_{\mathbf{y}}(\mathbf{b})\}_{\mathbf{b}}$.

Proof strategy

Fix a *supergood* strategy for G^n.

- Entangled state: $|\psi\rangle$
- For all $\mathbf{x} = (x_1, \ldots, x_n)$, Alice uses POVM $\{A_{\mathbf{x}}(\mathbf{a})\}_{\mathbf{a}}$.
- For all $\mathbf{y} = (y_1, \ldots, y_n)$, Bob uses POVM $\{B_{\mathbf{y}}(\mathbf{b})\}_{\mathbf{b}}$.

Claim: If $\mathrm{val}^\star(G^n) \gg \mathrm{val}^\star(G)^n$, there exist many i such that

$$\Pr[\text{Win } G_i \,|\, \text{Win } G_1, \ldots, G_{i-1}] > \mathrm{val}^\star(G) + \delta.$$

Proof strategy

Fix a *supergood* strategy for G^n.

- Entangled state: $|\psi\rangle$
- For all $\mathbf{x} = (x_1, \ldots, x_n)$, Alice uses POVM $\{A_{\mathbf{x}}(\mathbf{a})\}_{\mathbf{a}}$.
- For all $\mathbf{y} = (y_1, \ldots, y_n)$, Bob uses POVM $\{B_{\mathbf{y}}(\mathbf{b})\}_{\mathbf{b}}$.

Claim: If $\mathrm{val}^\star(G^n) \gg \mathrm{val}^\star(G)^n$, there exist many i such that

$$\Pr[\text{Win } G_i \mid \text{Win } G_1, \ldots, G_{i-1}] > \mathrm{val}^\star(G) + \delta.$$

Goal: Alice and Bob try to simulate playing G_i *conditioned* on winning games $G_1, \ldots, G_{i-1}$.

Proof strategy

Strategy for G_i:

1. Alice gets x_i, Bob gets y_i.
2. Using local operations Alice and Bob generate the entangled state $|\Phi_{x_i,y_i}\rangle$.
3. Alice and Bob measure the state to obtain answers a_i and b_i.

Proof strategy

Strategy for G_i:

1. Alice gets x_i, Bob gets y_i.
2. Using local operations Alice and Bob generate the entangled state $|\Phi_{x_i,y_i}\rangle$.
3. Alice and Bob measure the state to obtain answers a_i and b_i.

Intuition: The state $|\Phi_{x_i,y_i}\rangle$ represents the behavior of Alice and Bob in G^n conditioned on winning games $G_1,\ldots,G_{i-1}$ and inputs (x_i,y_i).

What is $|\Phi_{x_i,y_i}\rangle$?

Imagine the following experiment: Alice and Bob play G^n using the optimal entangled strategy, but their inputs $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are in **superposition**.

What is $|\Phi_{x_i,y_i}\rangle$?

Imagine the following experiment: Alice and Bob play G^n using the optimal entangled strategy, but their inputs $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are in **superposition**.

Initially, the state of Alice and Bob is

$$|\Phi\rangle = \sum_{\mathbf{x},\mathbf{y}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\ |\mathbf{x}\rangle \otimes |\psi\rangle \otimes |\mathbf{y}\rangle$$

Recall that $\mu(\mathbf{x},\mathbf{y}) = \mu(x_1, y_1) \times \cdots \times \mu(x_n, y_n)$.

What is $|\Phi_{x_i,y_i}\rangle$?

Imagine the following experiment: Alice and Bob play G^n using the optimal entangled strategy, but their inputs $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are in **superposition**.

Controlled by their question registers, they apply their measurements, and coherently store their answers.

$$|\Phi\rangle = \sum_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\ |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

$$|\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle = \left(\sqrt{A_{\mathbf{x}}(\mathbf{a})} \otimes \sqrt{B_{\mathbf{y}}(\mathbf{b})}\right)|\psi\rangle.$$

What is $|\Phi_{x_i,y_i}\rangle$?

Imagine the following experiment: Alice and Bob play G^n using the optimal entangled strategy, but their inputs $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ are in **superposition**.

After conditioning the state on winning $G_1, \dots, G_{i-1}$ and (x_i, y_i) we have

$$|\Phi_{x_i,y_i}\rangle \propto \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}: \\ V(x_j,y_j,a_j,b_j)=1\ \forall j<i \\ x_i,y_i}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\ |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

In other words: $|\Phi_{x_i,y_i}\rangle$ is the *post-measurement state* of Alice and Bob in the game G^n, conditioned on questions (x_i, y_i) and the having won games $G_1, \dots, G_{i-1}$.

Why is $|\Phi_{x_i,y_i}\rangle$ useful?

$$|\Phi_{x_i,y_i}\rangle \propto \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}: \\ V(x_j,y_j,a_j,b_j)=1\ \forall j<i \\ x_i,y_i}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\ |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

Suppose Alice and Bob can prepare $|\Phi_{x_i,y_i}\rangle$ when given questions (x_i, y_i).

Why is $|\Phi_{x_i,y_i}\rangle$ useful?

$$|\Phi_{x_i,y_i}\rangle \propto \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}: \\ V(x_j,y_j,a_j,b_j)=1\,\forall j<i \\ x_i,y_i}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\; |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

Suppose Alice and Bob can prepare $|\Phi_{x_i,y_i}\rangle$ when given questions (x_i, y_i). Then if Alice and Bob measure a_i and b_i, the answers will win with probability close to

$$\Pr[\text{Win } G_i \,|\, \text{Win } G_1, \ldots, G_{i-1}] > \mathrm{val}^\star(G) + \delta.$$

Why is $|\Phi_{x_i,y_i}\rangle$ useful?

$$|\Phi_{x_i,y_i}\rangle \propto \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}: \\ V(x_j,y_j,a_j,b_j)=1\,\forall j<i \\ x_i,y_i}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\; |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

Suppose Alice and Bob can prepare $|\Phi_{x_i,y_i}\rangle$ when given questions (x_i, y_i). Then if Alice and Bob measure a_i and b_i, the answers will win with probability close to

$$\Pr[\text{Win } G_i \mid \text{Win } G_1,\ldots,G_{i-1}] > \mathrm{val}^\star(G) + \delta.$$

Contradiction.

Why is $|\Phi_{x_i,y_i}\rangle$ useful?

$$|\Phi_{x_i,y_i}\rangle \propto \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}: \\ V(x_j,y_j,a_j,b_j)=1\ \forall j<i \\ x_i,y_i}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\ |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

- **It's not clear how to locally sample $|\Phi_{x_i,y_i}\rangle$!**

Why is $|\Phi_{x_i,y_i}\rangle$ useful?

$$|\Phi_{x_i,y_i}\rangle \propto \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}: \\ V(x_j,y_j,a_j,b_j)=1\ \forall j<i \\ x_i,y_i}} \sqrt{\mu(\mathbf{x},\mathbf{y})}\ |\mathbf{x}\rangle|\mathbf{a}\rangle \otimes |\psi_{\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b}}\rangle \otimes |\mathbf{y}\rangle|\mathbf{b}\rangle$$

- **It's not clear how to locally sample $|\Phi_{x_i,y_i}\rangle$!**
- This is the primary challenge of proving a quantum parallel repetition theorem.

Anchoring our way to parallel repetition

We carefully define $|\Phi_{x_i,y_i}\rangle$ so that

1. it allows Alice and Bob to win G_i with high probability, and
2. is jointly sampleable by the players with high fidelity.

Anchoring our way to parallel repetition

We carefully define $|\Phi_{x_i,y_i}\rangle$ so that

1. it allows Alice and Bob to win G_i with high probability, and
2. is jointly sampleable by the players with high fidelity.

Key Lemma

On average over $(x_i, y_i) \sim \mu$,

$$|\Phi_{x_i,y_i}\rangle \approx U_{x_i} \otimes V_{y_i} |\Phi_{\perp,\perp}\rangle$$

for some unitaries U_{x_i}, V_{y_i}.

Ingredients in our Key Lemma

- We bound

$$I(X_i;B)_\Phi \le \varepsilon \qquad \text{and} \qquad I(Y_i;A)_\Phi \le \varepsilon$$

- By Pinsker, this implies that Bob's side of entanglement in Φ is nearly independent of X_i, and Alice's side of Φ is nearly independent of Y_i.
- (**The Church of the Larger Hilbert Space**) Uhlmann's Theorem implies there exist unitaries U_{x_i} and V_{y_i} so that

$$|\Phi_{x_i,\perp}\rangle \approx U_{x_i} \otimes \mathbb{I}|\Phi_{\perp,\perp}\rangle \qquad \text{and} \qquad |\Phi_{\perp,y_i}\rangle \approx \mathbb{I} \otimes V_{y_i}|\Phi_{\perp,\perp}\rangle$$

- Using the fact that the "$\perp$" questions anchor all other questions, we can stitch together these two statements to get

$$|\Phi_{x_i,y_i}\rangle \approx U_{x_i} \otimes V_{y_i}|\Phi_{\perp,\perp}\rangle$$

Theorem: Quantum parallel repetition

If G is a two-player game with $\mathrm{val}^\star(G) = 1 - \delta$, then

$$\mathrm{val}^\star(G_\perp^n) = (1 - \delta^8)^{\Omega(n/s)}$$

Conclusion

What we showed: We give the first gap amplification results for general games in the quantum and multiplayer settings.

Future directions

- Other applications of anchoring?
  - Direct sums in communication complexity?
  - Additivity questions in quantum information
- Prove a general quantum parallel repetition theorem
  - First, prove that $\mathrm{val}^\star(G^n)$ **goes to 0 as $n \to \infty$** for all G when $\mathrm{val}^\star(G) < 1$.
- Prove a general multiplayer parallel repetition theorem

Conclusion

What we showed: We give the first gap amplification results for general games in the quantum and multiplayer settings.

Future directions

- Other applications of anchoring?
  - Direct sums in communication complexity?
  - Additivity questions in quantum information
- Prove a general quantum parallel repetition theorem
  - First, prove that $\mathrm{val}^\star(G^n)$ **goes to 0 as $n \to \infty$** for all G when $\mathrm{val}^\star(G) < 1$.
- Prove a general multiplayer parallel repetition theorem

Thank you! Any questions?