Limitations of monogamy, Tsirelson-type bounds, and other SDPs in quantum information

Aram W. Harrow\(^1\), Anand Natarajan\(^1\), Xiaodi Wu\(^2\)

\(^1\)MIT Center for Theoretical Physics

\(^2\)University of Oregon

IQI Seminar, Caltech
Semidefinite Programminings (SDPs) admit *polynomial time* solvers and plays an important role in quantum information.

- Consistency of reduced states, Quantum conditional min-entropy, local Hamiltonians
- QIP=PSPACE, QRG=EXP, .......

This talk is, however, about its *limitation* in

- Separability or entanglement detection,
- Approximation of Bell-violation (non-local game values).

Result: unconditional limitations of SDPs comparing to existing computational hardness.

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
SDPs in Quantum Information

Semidefinite Programmings (SDPs) admit *polynomial time* solvers and plays an important role in quantum information.

- Consistency of reduced states, Quantum conditional min-entropy, local Hamiltonians
- QIP=PSPACE, QRG=EXP, .......

This talk is, however, about its *limitation* in

- Separability or entanglement detection,
- Approximation of Bell-violation (non-local game values).

Result: unconditional limitations of SDPs comparing to existing computational hardness.
Semidefinite Programmings (SDPs) admit *polynomial time* solvers and plays an important role in quantum information.

- Consistency of reduced states, Quantum conditional min-entropy, local Hamiltonians
- QIP=PSPACE, QRG=EXP, .......

This talk is, however, about its **limitation** in

- Separability or entanglement detection,
- Approximation of Bell-violation (non-local game values).

**Result:** unconditional limitations of SDPs comparing to existing computational hardness.
**Problem 1: Separability**

**Definition (Separable and Entangled States)**

A bi-partitie state $\rho \in D(\mathcal{X} \otimes \mathcal{Y})$ is **separable** if $\exists$ dist. $\{\rho_i\}$,

$$\rho = \sum p_i \sigma^i_X \otimes \sigma^i_Y, \text{ s.t. } \sigma^i_X \in D(\mathcal{X}), \sigma^i_Y \in D(\mathcal{Y}).$$

Otherwise, $\rho$ is **entangled**. Let $\text{Sep} \overset{\text{def}}{=} \{ \text{separable states} \}$.

**Definition (Entanglement Detection)**

A **KEY** problem: given the description of $\rho \in D(\mathcal{X} \otimes \mathcal{Y})$, decide

Either $\rho \in \text{Sep}$, or $\rho$ is far away from $\text{Sep}$. 

---

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Problem 1: Separability

Definition (Separable and Entangled States)
A bi-partite state $\rho \in D (\mathcal{X} \otimes \mathcal{Y})$ is \textit{separable} if $\exists$ dist. $\{p_i\}$,

$$\rho = \sum p_i \sigma_i^X \otimes \sigma_i^Y, \text{ s.t. } \sigma_i^X \in D (\mathcal{X}), \sigma_i^Y \in D (\mathcal{Y}).$$

Otherwise, $\rho$ is \textit{entangled}. Let $\text{Sep} \overset{\text{def}}{=} \{ \text{separable states} \}$.

Definition (Entanglement Detection)
A \textit{KEY} problem: given the description of $\rho \in D (\mathcal{X} \otimes \mathcal{Y})$, decide

Either $\rho \in \text{Sep}$, or $\rho$ is far away from $\text{Sep}$.
Definition (Weak Membership)

\[ \text{WMem}(\epsilon, \| \cdot \|) : \text{for any } \rho \in D(\mathcal{X} \otimes \mathcal{Y}), \text{ decide either } \rho \in \text{Sep} \text{ or } \| \rho - \text{Sep} \| \geq \epsilon. \]

Via standard techniques in convex optimization, equivalent to

Definition (Weak Optimization)

\[ \text{WOpt}(M, \epsilon) : \text{for any } M \in \text{Herm}(\mathcal{X} \otimes \mathcal{Y}), \text{ estimate the value of} \]

\[ h_{\text{Sep}(d,d)}(M) := \max_{\rho \in \text{Sep}} \langle M, \rho \rangle, \]

with additive error \( \epsilon \).
Definition (Weak Membership)

WMem(\(\epsilon, \| \cdot \| \)) : for any \( \rho \in D(\mathcal{X} \otimes \mathcal{Y}) \), decide either \( \rho \in \text{Sep} \) or \( \| \rho - \text{Sep} \| \geq \epsilon \).

Via standard techniques in convex optimization, equivalent to

Definition (Weak Optimization)

WOpt(\(M, \epsilon\)) : for any \( M \in \text{Herm}(\mathcal{X} \otimes \mathcal{Y}) \), estimate the value of

\[
    h_{\text{Sep}(d,d)}(M) := \max_{\rho \in \text{Sep}} \langle M, \rho \rangle,
\]

with additive error \( \epsilon \).
$h_{\text{Sep}}(d,d)(M) := \max_{x,y \in \mathbb{C}^d} \sum_{i,j,k,l \in [d]} M_{ij,kl} x_i^* x_j y_k^* y_l.$  \hspace{1cm} (1)

REMARK: this is an instance of polynomial optimization problems with a homogenous degree 4 objective polynomial and a degree 2 constraint polynomial.
Connections

Quantum Information:
- **Mean-field** approximation in statistical quantum mechanics.
- **Positivity** test of quantum channels.
- Data hiding, Channel capacities, Privacy, ......
- 17 more examples in quantum information in [HM10].

Quantum Complexity:
- Quantum Merlin-Arthur Game with Two-Provers (QMA(2)).

Classical Complexity:
- Unique Game Conjecture and Small-set Expansion.
  \((\ell_2 \rightarrow \ell_4 \text{ norm})\)
Connections

Quantum Information:
- *Mean-field* approximation in statistical quantum mechanics.
- *Positivity* test of quantum channels.
- Data hiding, Channel capacities, Privacy, .......
- 17 more examples in quantum information in [HM10].

Quantum Complexity:
- Quantum Merlin-Arthur Game with Two-Provers (QMA(2)).

Classical Complexity:
- Unique Game Conjecture and Small-set Expansion.
  \((\ell_2 \rightarrow \ell_4 \text{ norm})\)
Connections

Quantum Information:
- *Mean-field* approximation in statistical quantum mechanics.
- *Positivity* test of quantum channels.
- Data hiding, Channel capacities, Privacy, ......
- 17 more examples in quantum information in [HM10].

Quantum Complexity:
- Quantum Merlin-Arthur Game with Two-Provers (QMA(2)).

Classical Complexity:
- Unique Game Conjecture and Small-set Expansion. ($\ell_2 \rightarrow \ell_4$ norm)
Connections

Quantum Information:
- Mean-field approximation in statistical quantum mechanics.
- Positivity test of quantum channels.
- Data hiding, Channel capacities, Privacy, .......
- 17 more examples in quantum information in [HM10].

Quantum Complexity:
- Quantum Merlin-Arthur Game with Two-Provers (QMA(2)).

Classical Complexity:
- Unique Game Conjecture and Small-set Expansion. ($\ell_2 \rightarrow \ell_4$ norm)
Connections

Quantum Information:
- *Mean-field* approximation in statistical quantum mechanics.
- *Positivity* test of quantum channels.
- Data hiding, Channel capacities, Privacy, ......
- 17 more examples in quantum information in [HM10].

Quantum Complexity:
- Quantum Merlin-Arthur Game with Two-Provers (QMA(2)).

Classical Complexity:
- Unique Game Conjecture and Small-set Expansion.
  ($\ell_2 \rightarrow \ell_4$ norm)
Connections

Quantum Information:
- *Mean-field* approximation in statistical quantum mechanics.
- *Positivity* test of quantum channels.
- Data hiding, Channel capacities, Privacy, ......
- *17 more examples in* quantum information in [HM10].

Quantum Complexity:
- Quantum Merlin-Arthur Game with Two-Provers (QMA(2)).

Classical Complexity:
- Unique Game Conjecture and Small-set Expansion.
  \((\ell_2 \rightarrow \ell_4\) norm\)
Heuristics

Separability Criteria:

- Positive Partial Transpose (PPT): $\rho^T = \rho$? [PH]
- Reduction Criteria: $I_X \otimes \rho_Y \geq \rho$? [HH]
- **FAILURE**: any such test has arbitrarily large error. [BS]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

- $\rho$ is $k$-extendible if $\exists$ symmetric $\sigma \in D(X \otimes Y_1 \otimes \cdots \otimes Y_k)$, $\forall i, \rho = \sigma_{XY_i}$.
- $\rho \in \text{Sep}$ if and only if $\rho$ is $k$-extendible for any $k \geq 0$.
- Semidefinite program (SDP): size exponential in $k$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
**Heuristics**

**Separability Criterions:**

- Positive Partial Transpose (PPT): $\rho^{T_Y} = \rho$? [PH]
- Reduction Criterions: $I_X \otimes \rho_Y \geq \rho$? [HH]
- **FAILURE**: any such test has arbitrarily large error. [BS]

**Doherty-Parrilo-Spedalieri (DPS) hierarchy:**

- $\rho$ is $k$-extendible if $\exists$ symmetric $\sigma \in D (X \otimes Y_1 \otimes \cdots \otimes Y_k)$, $\forall i, \rho = \sigma_{XY_i}$.
- $\rho \in \text{Sep}$ if and only if $\rho$ is $k$-extendible for any $k \geq 0$.
- Semidefinite program (SDP) size exponential in $k$.
Heuristics

Separability Criteria:

- Positive Partial Transpose (PPT): $\rho^T_Y = \rho$? [PH]
- Reduction Criteria: $I_X \otimes \rho_Y \geq \rho$? [HH]
- **FAILURE**: any such test has arbitrarily large error. [BS]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

- $\rho$ is $k$-extendible if $\exists$ symmetric $\sigma \in D (X \otimes Y_1 \otimes \cdots \otimes Y_k)$, $\forall i, \rho = \sigma_{XY_i}$.

Semidefinite program (SDP): Size exponential in $k$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Heuristics

Separability Criterions:

- Positive Partial Transpose (PPT): $\rho^{T_Y} = \rho$? [PH]
- Reduction Criterions: $I_X \otimes \rho_Y \geq \rho$? [HH]
- FAILURE: any such test has arbitrarily large error. [BS]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

- $\rho$ is $k$-extendible if $\exists$ symmetric $\sigma \in D (X \otimes Y_1 \otimes \cdots \otimes Y_k)$, $\forall i, \rho = \sigma_{XY_i}$.
- $\rho \in \text{Sep}$ if and only if $\rho$ is $k$-extendible for any $k \geq 0$.
- Semidefinite program (SDP) size exponential in $k$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Heuristics

Separability Criterions:

- Positive Partial Transpose (PPT): \( \rho^T = \rho \) \[PH\]
- Reduction Criterions: \( I_X \otimes \rho_Y \geq \rho \) \[HH\]
- **FAILURE**: any such test has arbitrarily large error. \[BS\]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

- \( \rho \) is \( k \)-extendible if \( \exists \) symmetric \( \sigma \in D(\mathcal{X} \otimes \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k) \), \( \forall i, \rho = \sigma_{XY_i} \).
- \( \rho \in \text{Sep} \) if and only if \( \rho \) is \( k \)-extendible for any \( k \geq 0 \).
- Semidefinite program (SDP): size exponential in \( k \).
Heuristics

Separability Criterions:

- Positive Partial Transpose (PPT): $\rho^T = \rho$? [PH]
- Reduction Criterions: $I_X \otimes \rho_Y \geq \rho$? [HH]
- **FAILURE**: any such test has arbitrarily large error. [BS]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

- $\rho$ is $k$-extendible if $\exists$ symmetric $\sigma \in D(\mathcal{X} \otimes \mathcal{V}_1 \otimes \cdots \otimes \mathcal{V}_k)$, $\forall i, \rho = \sigma_{XY_i}$.
- $\rho \in \text{Sep}$ if and only if $\rho$ is $k$-extendible for any $k \geq 0$.
- Semidefinite program (SDP): size exponential in $k$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Heuristics

Separability Criterions:
- Positive Partial Transpose (PPT): $\rho^T_{\mathcal{Y}} = \rho?$ [PH]
- Reduction Criterions: $I_{\mathcal{X}} \otimes \rho_{\mathcal{Y}} \geq \rho?$ [HH]
- **FAILURE:** any such test has arbitrarily large error. [BS]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:
- $\rho$ is $k$-extendible if $\exists$ symmetric $\sigma \in D(\mathcal{X} \otimes \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k)$, $\forall i, \rho = \sigma_{\mathcal{X} \mathcal{Y}_i}$.
- $\rho \in \text{Sep}$ if and only if $\rho$ is $k$-extendible for any $k \geq 0$.
- **Semidefinite program (SDP):** size exponential in $k$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
### Computational Hardness

<table>
<thead>
<tr>
<th>reference</th>
<th>$k$</th>
<th>$c$</th>
<th>$s$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>GNN12</td>
<td>2</td>
<td>1</td>
<td>$1 - \frac{1}{d \cdot \text{poly log}(d)}$</td>
<td>$O(d)$</td>
</tr>
<tr>
<td>Per12</td>
<td>2</td>
<td>1</td>
<td>$1 - \frac{1}{\text{poly}(d)}$</td>
<td>$O(d)$</td>
</tr>
<tr>
<td>AB+08</td>
<td>$\sqrt{d} \cdot \text{poly log}(d)$</td>
<td>1</td>
<td>0.99</td>
<td>$O(d)$</td>
</tr>
<tr>
<td>CD10</td>
<td>$\sqrt{d} \cdot \text{poly log}(d)$</td>
<td>$1 - 2^{-d}$</td>
<td>0.99</td>
<td>$O(d)$</td>
</tr>
<tr>
<td>HM13</td>
<td>2</td>
<td>1</td>
<td>0.01</td>
<td>$\frac{\log^2(d)}{\text{poly log}(d)}$</td>
</tr>
</tbody>
</table>

**Table:** Hardness results for $h_{\text{Sep}}^k(d)$ (extension of $h_{\text{Sep}}(d,d)$ to $k$ parties.)

**Hardness in the following sense:** determining satisfiability of 3-SAT instances with $n$ variables and $O(n)$ clauses can be reduced to distinguishing between $h_{\text{Sep}}^k(d) \geq c$ and $\leq s$ as above.
Exponential Time Hypothesis (ETH)

The 3-SAT problem with \( n \) variables requires \( 2^{\Omega(n)} \) time to solve.

- Combine with [HM13] hardness result ⇒ approximation of \( h_{\text{sep}}(d) \) with constant precision requires \( d^{\Omega(\log(d))} \) time.
- A matching upper bound: DPS to \( O(\log(d)/\epsilon^2) \) level for 1-LOCC \( M \): time \( d^{O(\log(d)/\epsilon^2)} \rightarrow d^{O(\log(d))} \). [BYC, BH]

Question: any unconditional lower bounds for DPS or any SDPs? any matching upper bounds?

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Introduction

Proof Technique

Conclusions

Motivations

Problems

Main Results & Implications

Computational Hardness

Exponential Time Hypothesis (ETH)

The 3-SAT problem with $n$ variables requires $2^{\Omega(n)}$ time to solve.

- Combine with [HM13] hardness result $\Rightarrow$ approximation of $h_{\text{Sep}}(d)$ with constant precision requires $d^{\Omega(\log(d))}$ time.
- A matching upper bound: DPS to $O(\log(d)/\epsilon^2)$ level for 1-LOCC $M$: time $d^{O(\log(d)/\epsilon^2)} \rightarrow d^{O(\log(d))}$. [BYC, BH]

Question: any unconditional lower bounds for DPS or any SDPs? any matching upper bounds?

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Exponential Time Hypothesis (ETH)

The 3-SAT problem with \( n \) variables requires \( 2^{\Omega(n)} \) time to solve.

- Combine with [HM13] hardness result \( \Rightarrow \) approximation of \( h_{\text{Sep}}(d) \) with constant precision requires \( d^{\Omega(\log(d))} \) time.

- A matching upper bound: DPS to \( O(\log(d)/\epsilon^2) \) level for 1-LOCC \( M \): time \( d^{O(\log(d)/\epsilon^2)} \rightarrow d^{O(\log(d))} \). [BYC, BH]

Question: any unconditional lower bounds for DPS or any SDPs? any matching upper bounds?
**Computational Hardness**

**Exponential Time Hypothesis (ETH)**

The 3-SAT problem with $n$ variables requires $2^{\Omega(n)}$ time to solve.

- Combine with [HM13] hardness result $\Rightarrow$ approximation of $h_{\text{Sep}}(d)$ with constant precision requires $d^{\Omega(\log(d))}$ time.
- A matching upper bound: DPS to $O(\log(d)/\epsilon^2)$ level for 1-LOCC $M$: time $d^{O(\log(d)/\epsilon^2)} \rightarrow d^{O(\log(d))}$. [BYC, BH]

**Question:** any unconditional lower bounds for DPS or any SDPs? any matching upper bounds?
Problem 2: Non-local Games

Non-local Game (denoted $G$):

- Two physically separated players Alice and Bob. **No** communication once the game starts.
- Sets of questions $S$, $T$ and answers $A$, $B$ and a distribution $\pi : S \times T \rightarrow [0, 1]$.
- Sample $(s, t) \in S \times T \sim \pi$ and ask Alice and Bob respectively. Obtain answers $a \in A$, $b \in B$.
- Determine **win** or **lose** by a predicate $V(a, b|s, t) \in \{0, 1\}$.

Motivation: Bell-violation (quantum **non-locality**) in a game language. Also related to quantum multi-prover interactive proofs with shared entanglement.
Problem 2: Non-local Games

Non-local Game (denoted $G$):

- Two physically **separated** players Alice and Bob. **No** communication once the game starts.
- Sets of questions $S$, $T$ and answers $A$, $B$ and a distribution $\pi : S \times T \rightarrow [0, 1]$.
- Sample $(s, t) \in S \times T \sim \pi$ and ask Alice and Bob respectively. Obtain answers $a \in A$, $b \in B$.
- Determine **win** or **lose** by a predicate $V(a, b|s, t) \in \{0, 1\}$.

**Motivation:** Bell-violation (quantum **non-locality**) in a game language. Also related to quantum multi-prover interactive proofs with shared entanglement.
Problem 2: Non-local Games

Non-local Game (denoted $G$):

- Two physically **separated** players Alice and Bob. **No** communication once the game starts.
- Sets of questions $S$, $T$ and answers $A$, $B$ and a distribution
  $\pi : S \times T \rightarrow [0, 1]$.
- Sample $(s, t) \in S \times T \sim \pi$ and ask Alice and Bob respectively. Obtain answers $a \in A, b \in B$.
- Determine **win** or **lose** by a predicate $V(a, b|s, t) \in \{0, 1\}$.

**Motivation:** Bell-violation (quantum **non-locality**) in a game language. Also related to quantum multi-prover interactive proofs with shared entanglement.
Problem 2: Non-local Games

Non-local Game (denoted $G$):

- Two physically **separated** players Alice and Bob. **No** communication once the game starts.
- Sets of questions $S$, $T$ and answers $A$, $B$ and a distribution $\pi : S \times T \rightarrow [0, 1]$.
- Sample $(s, t) \in S \times T \sim \pi$ and ask Alice and Bob respectively. Obtain answers $a \in A$, $b \in B$.
- Determine **win** or **lose** by a predicate $V(a, b|s, t) \in \{0, 1\}$.

**Motivation:** Bell-violation (quantum **non-locality**) in a game language. Also related to quantum multi-prover interactive proofs with shared entanglement.
Problem 2: Non-local Games

Non-local Game (denoted $G$):

- Two physically separated players Alice and Bob. No communication once the game starts.
- Sets of questions $S$, $T$ and answers $A$, $B$ and a distribution $\pi : S \times T \rightarrow [0, 1]$.
- Sample $(s, t) \in S \times T \sim \pi$ and ask Alice and Bob respectively. Obtain answers $a \in A$, $b \in B$.
- Determine **win** or **lose** by a predicate $V(a, b|s, t) \in \{0, 1\}$.

**Motivation:** Bell-violation (quantum non-locality) in a game language. Also related to quantum multi-prover interactive proofs with shared entanglement.
Problem 2: Non-local Games (cont’d)

Strategies:

- Denote by \( P[a, b|s, t] \) the probability of answering \((a, b)\) upon receiving \((s, t)\).
- Quantum strategies: share a quantum state \( |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \) and answer w.r.t measurements \( \{A^a_s\} \) and \( \{B^b_t\} \),

\[
P[a, b|s, t] = \langle \psi | A^a_s \otimes B^b_t | \psi \rangle.
\]
Problem 2: Non-local Games (cont’d)

Strategies:

- Denote by $P[a, b|s, t]$ the probability of answering $(a, b)$ upon receiving $(s, t)$.

- **Quantum strategies**: share a quantum state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and answer w.r.t measurements $\{A^a_s\}$ and $\{B^b_t\}$,

\[
P[a, b|s, t] = \langle \psi | A^a_s \otimes B^b_t | \psi \rangle.
\]
Non-local Games (cont’d)

Definition (Game Value)

\[ \omega(G) = \max_P \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) P(a,b|s,t). \]

Example: CHSH game:
- \( A = B = S = T = \{0, 1\} \) and \( \pi(s,t) = 1/4, \forall (s,t) \in S \times T \).
- \( V(a,b|s,t) = 1 \) iff \( a \oplus b = s \land t \).
- Classical strategies: \( \omega(CHSH) = 3/4 \).
- Quantum strategies: \( \omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85 \).
- Quantum strategies are strictly more powerful.

Question: calculate \( \omega^*(G) \) for any given \( G \). How hard is that?
Definition (Game Value)

\[ \omega(G) = \max_{\pi} \sum_{a,b,s,t} \pi(s,t) V(a, b|s, t) P(a, b|s, t). \]

Example: CHSH game:

- \( A = B = S = T = \{0, 1\} \) and \( \pi(s, t) = 1/4, \forall (s, t) \in S \times T \).
- \( V(a, b|s, t) = 1 \) iff \( a \oplus b = s \land t \).
- Classical strategies: \( \omega(CHSH) = 3/4 \). Quantum strategies: \( \omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85 \).
- Quantum strategies are strictly more powerful.

Question: calculate \( \omega^*(G) \) for any given \( G \). How hard is that?
Definition (Game Value)

\[ \omega(G) = \max \sum_{a,b,s,t} \pi(s, t) V(a, b|s, t) P(a, b|s, t). \]

Example: CHSH game:

- \( A = B = S = T = \{0, 1\} \) and \( \pi(s, t) = 1/4, \forall (s, t) \in S \times T \).
- \( V(a, b|s, t) = 1 \) iff \( a \oplus b = s \wedge t \).

Classical strategies: \( \omega(CHSH) = 3/4 \). Quantum strategies: \( \omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85 \).

Quantum strategies are strictly more powerful.

Question: calculate \( \omega^*(G) \) for any given \( G \). How hard is that?
Non-local Games (cont’d)

**Definition (Game Value)**

\[ \omega(G) = \max \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) P(a,b|s,t). \]

**Example: CHSH game:**

- \( A = B = S = T = \{0, 1\} \) and \( \pi(s,t) = 1/4, \forall (s,t) \in S \times T. \)
- \( V(a,b|s,t) = 1 \) iff \( a \oplus b = s \land t. \)
- **Classical strategies:** \( \omega(CHSH) = 3/4. \) **Quantum strategies:** \( \omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85. \)

- Quantum strategies are strictly more powerful.

**Question:** calculate \( \omega^*(G) \) for any given \( G. \) How hard is that?
Non-local Games (cont’d)

Definition (Game Value)

\[ \omega(G) = \max_P \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) P(a,b|s,t). \]

Example: CHSH game:

- \( A = B = S = T = \{0, 1\} \) and \( \pi(s,t) = 1/4, \forall (s,t) \in S \times T. \)
- \( V(a,b|s,t) = 1 \) iff \( a \oplus b = s \land t. \)
- Classical strategies: \( \omega(CHSH) = 3/4. \) Quantum strategies: \( \omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85. \)
- Quantum strategies are strictly more powerful.

Question: calculate \( \omega^*(G) \) for any given \( G. \) How hard is that?
Non-local Games (cont’d)

Definition (Game Value)

\[
\omega(G) = \max_P \sum_{a,b,s,t} \pi(s, t) V(a, b|s, t) P(a, b|s, t).
\]

Example: CHSH game:

- \(A = B = S = T = \{0, 1\}\) and \(\pi(s, t) = 1/4, \forall(s, t) \in S \times T\).
- \(V(a, b|s, t) = 1\) iff \(a \oplus b = s \land t\).
- Classical strategies: \(\omega(CHSH) = 3/4\). Quantum strategies: \(\omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85\).
- Quantum strategies are strictly more powerful.

Question: calculate \(\omega^*(G)\) for any given \(G\). How hard is that?
Calculating $\omega^*(G)$ for quantum strategies

**$\omega^*(G)$ for quantum strategies**: an optimization problem!

\[
\omega^*(G) = \lim_{d \to \infty} \max_{|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d} \max_{A^a_s, B^b_t} \sum_{a,b,s,t} \pi(s, t) V(a, b|s, t) \langle \psi | A^a_s \otimes B^b_t | \psi \rangle.
\]

- $\omega^*(G)$ is not known to be computable.
- A SDP hierarchy proposed by Navascues-Pironio-Acin (NPA) approximates $\omega^*(G)$ from above and converges at infinity.
- Converging rate only known for special cases: XOR, Unique games. No general upper or lower bounds known about the NPA hierarchy.
Calculating \( \omega^*(G) \) for quantum strategies

\( \omega^*(G) \) for quantum strategies: an optimization problem!

\[
\omega^*(G) = \lim_{d \to \infty} \max_{|\psi\rangle \in \mathbb{C}^d \times d} \max_{A_s^a, B_t^b} \sum_{a,b,s,t} \pi(s, t) V(a, b | s, t) \langle \psi | A_s^a \otimes B_t^b | \psi \rangle.
\]

- \( \omega^*(G) \) is not known to be computable.
- A SDP hierarchy proposed by Navascues-Pironio-Acin (NPA) approximates \( \omega^*(G) \) from above and converges at infinity.
- Converging rate only known for special cases: XOR, Unique games. No general upper or lower bounds known about the NPA hierarchy.
Calculating $\omega^*(G)$ for quantum strategies

$\omega^*(G)$ for quantum strategies: an optimization problem!

$$\omega^*(G) = \lim_{d \to \infty} \max_{|\psi\rangle \in \mathbb{C}^{d \times d}} \max_{A_s^a, B_t^b} \sum_{a,b,s,t} \pi(s, t) V(a, b|s, t) \langle \psi | A_s^a \otimes B_t^b | \psi \rangle.$$ 

- $\omega^*(G)$ is not known to be computable.
- A SDP hierarchy proposed by Navascues-Pironio-Acin (NPA) approximates $\omega^*(G)$ from above and converges at infinity.
- Converging rate only known for special cases: XOR, Unique games. No general upper or lower bounds known about the NPA hierarchy.
Calculating $\omega^*(G)$ for quantum strategies

$\omega^*(G)$ for quantum strategies: an optimization problem!

$$
\omega^*(G) = \lim_{d \to \infty} \max_{|\psi\rangle \in \mathbb{C}^{d \times d}} \max_{A^a_s, B^b_t} \sum_{a,b,s,t} \pi(s, t) V(a, b|s, t) \langle \psi | A^a_s \otimes B^b_t | \psi \rangle.
$$

- $\omega^*(G)$ is not known to be computable.
- A SDP hierarchy proposed by Navascues-Pironio-Acin (NPA) approximates $\omega^*(G)$ from above and converges at infinity.
- Converging rate only known for special cases: XOR, Unique games. No general upper or lower bounds known about the NPA hierarchy.
Computational Hardness

<table>
<thead>
<tr>
<th>reference</th>
<th>$k$</th>
<th>$c$</th>
<th>$s$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>KK+11</td>
<td>3</td>
<td>1</td>
<td>$1 - \frac{1}{\text{poly}(Q)}$</td>
<td>$O(Q)$</td>
</tr>
<tr>
<td>IKM09</td>
<td>2</td>
<td>1</td>
<td>$1 - \frac{1}{\text{poly}(Q)}$</td>
<td>$O(Q)$</td>
</tr>
<tr>
<td>IV12</td>
<td>4</td>
<td>1</td>
<td>$2^{-Q^{\Omega(1)}}$</td>
<td>$Q^{\Omega(1)}$</td>
</tr>
<tr>
<td>Vid13</td>
<td>3</td>
<td>1</td>
<td>$2^{-Q^{\Omega(1)}}$</td>
<td>$Q^{\Omega(1)}$</td>
</tr>
</tbody>
</table>

**Table:** Hardness results for $\omega^*(G)$ where $G$ is a one-round $k$-prover interactive proof protocol with question alphabet size $Q$.

**Hardness in the following sense:** determining satisfiability of 3-SAT instances with $n$ variables and $O(n)$ clauses can be reduced to distinguishing between $\omega^*(G) \geq c$ and $\leq s$ as above.
Result I: Unconditional Hardness for $h_{\text{Sep}}$?

Will the hardness of $h_{\text{Sep}(d)}$ for const $\epsilon$ hold w/o ETH?

**Theorem (Main I.1)**

The DPS hierarchy (or general Sum-of-Squares SDP) requires $\Omega(\log(d))$ levels to solve $h_{\text{Sep}(d)}$ with constant precision.

**Theorem (Main I.2)**

Any SDP relaxation that estimate $h_{\text{Sep}(d)}(M)$ with constant errors requires size $d^{\Omega(\log(d))}$.

**Remark:** Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.
Result I: Unconditional Hardness for $h_{\text{Sep}}$?

**Will the hardness of $h_{\text{Sep}(d)}$ for const $\epsilon$ hold w/o ETH?**

**Theorem (Main I.1)**

The DPS hierarchy (or general Sum-of-Squares SDP) requires $\Omega(\log(d))$ levels to solve $h_{\text{Sep}(d)}$ with constant precision.

**Theorem (Main I.2)**

Any SDP relaxation that estimate $h_{\text{Sep}(d)}(M)$ with constant errors requires size $d^{\Omega(\log(d))}$.

**Remark:** Match $d^\Omega(\log(d))$ time bound when assuming ETH.
Result I: Unconditional Hardness for $h_{\text{Sep}}$?

Will the hardness of $h_{\text{Sep}(d)}$ for $\text{const } \epsilon$ hold w/o ETH?

Theorem (Main I.1)

*The DPS hierarchy (or general Sum-of-Squares SDP) requires $\Omega(\log(d))$ levels to solve $h_{\text{Sep}(d)}$ with constant precision.*

Theorem (Main I.2)

*Any SDP relaxation that estimate $h_{\text{Sep}(d)}(M)$ with constant errors requires size $d^{\Omega(\log(d))}$.*

Remark: Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.
Result I: Unconditional Hardness for $h_{\text{Sep}}$?

Will the hardness of $h_{\text{Sep}(d)}$ for const $\epsilon$ hold w/o ETH?

**Theorem (Main I.1)**

The DPS hierarchy (or general Sum-of-Squares SDP) requires $\Omega(\log(d))$ levels to solve $h_{\text{Sep}(d)}$ with constant precision.

**Theorem (Main I.2)**

Any SDP relaxation that estimate $h_{\text{Sep}(d)}(M)$ with constant errors requires size $d^{\Omega(\log(d))}$.

**Remark:** Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.
Result II: Unconditional Hardness for $\omega^*(G)$?

Will the hardness of $\omega^*(G)$ hold w/o ETH?

**Theorem (Main II.1)**

There exists a family of games $\{G_n\}$ s.t. the NPA hierarchy requires $\Omega(n)$ levels to distinguish $\omega^*(G) = 1$ from $\omega^*(G) = 1 - \Omega(1/n^2)$.

**Theorem (Main II.2)**

Any SDP relaxation that estimates $\omega^*(G)$ with precision $O(1/n^2)$ requires size $(n/\log(n))^{\Omega(n)}$.

**Remark:** Match the computational hardness of [IKM]. Open for [IV12, Vid13].
Result II: Unconditional Hardness for $\omega^*(G)$?

Will the hardness of $\omega^*(G)$ hold w/o ETH?

Theorem (Main II.1)

There exists a family of games $\{G_n\}$ s.t. the NPA hierarchy requires $\Omega(n)$ levels to distinguish $\omega^*(G) = 1$ from $\omega^*(G) = 1 - \Omega(1/n^2)$.

Theorem (Main II.2)

Any SDP relaxation that estimates $\omega^*(G)$ with precision $O(1/n^2)$ requires size $(n/\log(n))^{\Omega(n)}$.

Remark: Match the computational hardness of [IKM]. Open for [IV12, Vid13].
Result II: Unconditional Hardness for $\omega^*(G)$?

Will the hardness of $\omega^*(G)$ hold w/o ETH?

Theorem (Main II.1)

*There exists a family of games $\{G_n\}$ s.t. the NPA hierarchy requires $\Omega(n)$ levels to distinguish $\omega^*(G) = 1$ from $\omega^*(G) = 1 - \Omega(1/n^2)$.*

Theorem (Main II.2)

*Any SDP relaxation that estimates $\omega^*(G)$ with precision $O(1/n^2)$ requires size $(n/\log(n))\Omega(n)$.*

Remark: Match the computational hardness of [IKM].
Open for [IV12, Vid13].
Result II: Unconditional Hardness for $\omega^*(G)$?

Will the hardness of $\omega^*(G)$ hold w/o ETH?

**Theorem (Main II.1)**

There exists a family of games $\{G_n\}$ s.t. the NPA hierarchy requires $\Omega(n)$ levels to distinguish $\omega^*(G) = 1$ from $\omega^*(G) = 1 - \Omega(1/n^2)$.

**Theorem (Main II.2)**

Any SDP relaxation that estimates $\omega^*(G)$ with precision $O(1/n^2)$ requires size $(n/\log(n))\Omega(n)$.

**Remark:** Match the computational hardness of [IKM]. Open for [IV12, Vid13].
Unconditional SoS & SDP lower bounds

- First unconditional lower bounds (SoS or SDP) for both $h_{\text{Sep}}$ and $\omega^*(G)$ problems.
- Match all bounds from computational hardness for $h_{\text{Sep}}$, especially the DPS hierarchy.
- Improve lower bounds from level $k \leq 5$ to $k = \Omega(n)$ for the NPA hierarchy.

**Consequences**

- Implication to any resolution of the complexity of QMA(2). Discussed later.
- Hardness extends to the 2→4 norm, and thus small-set expansions (SSE), and potentially the unique game conjecture (UGC).

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Unconditional SoS & SDP lower bounds

- First unconditional lower bounds (SoS or SDP) for both $h_{Sep}$ and $\omega^*(G)$ problems.
- Match all bounds from computational hardness for $h_{Sep}$, especially the DPS hierarchy.
- Improve lower bounds from level $k \leq 5$ to $k = \Omega(n)$ for the NPA hierarchy.

Consequences

- Implication to any resolution of the complexity of QMA(2). Discussed later.
- Hardness extends to the $2 \rightarrow 4$ norm and three small-set expansions (SSE), and potentially the unique game conjecture (UGC).
Unconditional SoS & SDP lower bounds

- First unconditional lower bounds (SoS or SDP) for both $h_{\text{Sep}}$ and $\omega^*(G)$ problems.
- Match all bounds from computational hardness for $h_{\text{Sep}}$, especially the DPS hierarchy.
- Improve lower bounds from level $k \leq 5$ to $k = \Omega(n)$ for the NPA hierarchy.

Consequences

- Implication to any resolution of the complexity of QMA(2). Discussed later.
- Hardness extends to the $2 \rightarrow 4$ norm, and thus small-set expansions (SSE), and potentially the unique game conjecture (UGC).
Unconditional SoS & SDP lower bounds

- First unconditional lower bounds (SoS or SDP) for both $h_{\text{Sep}}$ and $\omega^*(G)$ problems.
- Match all bounds from computational hardness for $h_{\text{Sep}}$, especially the DPS hierarchy.
- Improve lower bounds from level $k \leq 5$ to $k = \Omega(n)$ for the NPA hierarchy.

Consequences

- Implication to any resolution of the complexity of QMA(2). Discussed later.
- Hardness extends to the $2 \rightarrow 4$ norm, and thus small-set expansions (SSE), and potentially the unique game conjecture (UGC).
Unconditional SoS & SDP lower bounds

- First unconditional lower bounds (SoS or SDP) for both $h_{\text{Sep}}$ and $\omega^*(G)$ problems.
- Match all bounds from computational hardness for $h_{\text{Sep}}$, especially the DPS hierarchy.
- Improve lower bounds from level $k \leq 5$ to $k = \Omega(n)$ for the NPA hierarchy.

Consequences

- Implication to any resolution of the complexity of QMA(2). Discussed later.
- Hardness extends to the $2 \rightarrow 4$ norm, and thus small-set expansions (SSE), and potentially the unique game conjecture (UGC).
QMA(2) vs QMA

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
QMA(2) vs QMA

Q-Prover \rightarrow \text{quantum message } |\psi\rangle \rightarrow \text{Q-Verifier}

C-Prover \rightarrow \text{C-Verifier}

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
QMA(2) vs QMA

C-Prover \rightarrow \text{classical message } m_1 \rightarrow \text{C-Verifier}

Q-Prover \rightarrow \text{quantum message } |\psi\rangle \rightarrow \text{Q-Verifier}

NP

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
QMA(2) vs QMA

C-Prover \( \text{classical message } m_1 \) C-Verifier

Q-Prover \( \text{quantum message } |\psi\rangle \) Q-Verifier

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
QMA(2) vs QMA

C-Verifier

C-P₁

C-P₂

Q-Prover

quantum message |ψ⟩

Q-Verifier

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
QMA(2) vs QMA

C-P_1 \rightarrow \text{C-Verifier} \rightarrow NP(2)

C-P_2 \rightarrow \text{C-Verifier} \rightarrow NP(2)

Q-Prover \rightarrow \text{Q-Verifier} \rightarrow Q-Verifier

Classical messages: m_1, m_2

Quantum message: |\psi\rangle

Motivations
Problems
Main Results & Implications
QMA(2) vs QMA

C-P₁ \text{ classical message } m₁ \rightarrow \text{ C-Verifier} \rightarrow \text{ NP(2)}

C-P₂ \text{ classical message } m₂ \rightarrow \text{ C-Verifier} \rightarrow \text{ NP(2)}

Q-P₁ \text{ quantum message } |ψ₁⟩ \rightarrow \text{ Q-Verifier} \rightarrow \text{ QMA(2)}

Q-P₂ \text{ quantum message } |ψ₂⟩ \rightarrow \text{ Q-Verifier} \rightarrow \text{ QMA(2)}
QMA(2) vs QMA

**C-P_1 \circ P_2**

- Classical message $m_1$
- Classical message $m_2$

- C-Verifier

**Q-P_1**

- Quantum message $|\psi_1\rangle$

- Q-Verifier

**Q-P_2**

- Quantum message $|\psi_2\rangle$

**NP(2)**

**QMA(2)**

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
**QMA(2) vs QMA**

\[ \text{QC-P}_1 \circ \text{P}_2 \rightarrow m_1 + m_2 \rightarrow \text{QC-Verifier} \]

\[ \text{Q-P}_1, \text{Q-P}_2 \rightarrow \text{Q-Verifier} \]

| Quantum message | | Quantum message |
|-----------------|-----------------|
| \( | \psi_1 \rangle \) | \( | \psi_2 \rangle \) |
QMA(2) vs QMA

\[ \text{C-} P_1 \circ P_2 \rightarrow m_1 + m_2 \rightarrow \text{C-Verifier} \]

\[ \text{Q-} Q_1 \otimes Q_2 \rightarrow \text{Q-Verifier} \]

Quantum message \( |\psi_1\rangle \)

Quantum message \( |\psi_2\rangle \)

\[ \text{NP(2)} = \text{NP} \]

\[ \text{QMA(2)} = \text{QMA} \]

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
First study in [KMY01, KMY03]. Surprising: NP ⊆ QMA(2)_log [BT09] v.s. QMA_log = BQP [MW05].

Main open question is to improve the trivial upper bound NEXP.

Variants of QMA(2) have been studied, such as BellQMA, LOCC-QMA, which collapse to QMA [Bra, ABD+, BCY].

QMA(2) = QMA(poly) [HM10].

A recently claimed result QMA(2) ⊆ EXP with questionable correctness [Sch15].

It suffices to solve $h_{\text{Sep}(d)}(M_{\text{acc}})$ with $M_{\text{acc}}$ the POVM from QMA(2) protocols.
History about QMA(2)

- First study in [KMY01, KMY03]. **Surprising:** \( \text{NP} \subseteq \text{QMA}(2)_{\text{log}} \) [BT09] v.s. \( \text{QMA}_{\text{log}} = \text{BQP} \) [MW05].

Main open question is to improve the trivial upper bound NEXP.

- Variants of QMA(2) have been studied, such as BellQMA, LOCC-QMA, which collapse to QMA [Bra, ABD+, BCY].
- QMA(2) = QMA(poly) [HM10].
- A recently claimed result QMA(2) ⊆ EXP with questionable correctness [Sch15].

It suffices to solve \( h_{\text{Sep}}(d)(M_{\text{acc}}) \) with \( M_{\text{acc}} \) the POVM from QMA(2) protocols.
History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA(2)$_{\log}$ [BT09] v.s. QMA$_{\log} = $ BQP [MW05].

  Main open question is to improve the trivial upper bound NEXP.

- Variants of QMA(2) have been studied, such as BellQMA, LOCC-QMA, which collapse to QMA [Bra, ABD+, BCY].

  - QMA(2)=QMA(poly) [HM10].
  - A recently claimed result QMA(2) $\subseteq$ EXP with questionable correctness [Sch15].

  It suffices to solve $h_{\text{Sep}(d)}(M_{\text{acc}})$ with $M_{\text{acc}}$ the POVM from QMA(2) protocols.
History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP ⊆ QMA(2)_log [BT09] v.s. QMA_log = BQP [MW05].

Main open question is to improve the trivial upper bound NEXP.

- Variants of QMA(2) have been studied, such as BellQMA, LOCC-QMA, which collapse to QMA [Bra, ABD+, BCY].

- QMA(2)=QMA(poly) [HM10].

- A recently claimed result QMA(2) ⊆ EXP with questionable correctness [Sch15].

It suffices to solve $h_{sep}(d)(M_{acc})$ with $M_{acc}$ the POVM from QMA(2) protocols.
History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP ⊆ QMA(2)_log [BT09] v.s. QMA_log = BQP [MW05].

Main open question is to improve the trivial upper bound NEXP.

- Variants of QMA(2) have been studied, such as BellQMA, LOCC-QMA, which collapse to QMA [Bra, ABD+, BCY].
- QMA(2)=QMA(poly) [HM10].
- A recently claimed result QMA(2) ⊆ EXP with questionable correctness [Sch15].

It suffices to solve \( h_{\text{Sep}(d)}(M_{\text{acc}}) \) with \( M_{\text{acc}} \) the POVM from QMA(2) protocols.
History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP ⊆ QMA(2)_{log} [BT09] v.s. QMA_{log} = BQP [MW05].

Main open question is to improve the trivial upper bound NEXP.

- Variants of QMA(2) have been studied, such as BellQMA, LOCC-QMA, which collapse to QMA [Bra, ABD+, BCY].
- QMA(2) = QMA(poly) [HM10].
- A recently claimed result QMA(2) ⊆ EXP with questionable correctness [Sch15].

It suffices to solve \( h_{\text{Sep}(d)}(M_{\text{acc}}) \) with \( M_{\text{acc}} \) the POVM from QMA(2) protocols.
Implication on QMA(2)

**Hardness applies to QMA(2)**
- Our explicit hard instance is a **valid** QMA(2) instance.
- Hardness implies that the de Finetti theorem of 1-LOCC [BCY, BH] is the best possible.

**Unconditional proof of Watrous’s dis-entangler conjecture**
- Dis-entangler: a hypothetical channel that a) its output is always \( \epsilon \)-close to a separable state, and b) its image is \( \delta \)-close to any separable state, both in trace distance.
- Input dimension \( \dim(H) = \infty \) for \( \epsilon = \delta = 0 \) [AB+09].
Implication on QMA(2)

Hardness applies to QMA(2)
- Our explicit hard instance is a valid QMA(2) instance.
- Hardness implies that the de Finetti theorem of 1-LOCC [BCY, BH] is the best possible.

Unconditional proof of Watrous’s dis-entangler conjecture
- Dis-entangler: a hypothetical channel that a) its output is always $\epsilon$-close to a separable state, and b) its image is $\delta$-close to any separable state, both in trace distance.
- Input dimension $\dim(\mathcal{H}) = \infty$ for $\epsilon = \delta = 0$ [AB+09].
- $\forall \epsilon + \delta < 1$, $\dim(\mathcal{H}) \geq \Omega(d^{\log(d)/\text{poly} \log \log(d')}).$
Implication on QMA(2)

**Hardness applies to QMA(2)**
- Our explicit hard instance is a **valid** QMA(2) instance.
- Hardness implies that the de Finetti theorem of 1-LOCC \[ \text{[BCY, BH]} \] is the best possible.

**Unconditional proof of Watrous’s dis-entangler conjecture**
- Dis-entangler: a hypothetical channel that a) its output is always \( \epsilon \)-close to a separable state, and b) its image is \( \delta \)-close to any separable state, both in trace distance.
- Input dimension \( \dim(H) = \infty \) for \( \epsilon = \delta = 0 \) \[ \text{[AB+09]} \].
- \( \forall \epsilon + \delta < 1, \dim(H) \geq \Omega(d^{\log(d) / \text{poly log log}(d')}) \).
Hardness applies to QMA(2)

- Our explicit hard instance is a **valid** QMA(2) instance.
- Hardness implies that the de Finetti theorem of 1-LOCC [BCY, BH] is the best possible.

Unconditional proof of Watrous’s dis-entangler conjecture

- Dis-entangler: a hypothetical channel that a) its output is always $\epsilon$-close to a separable state, and b) its image is $\delta$-close to any separable state, both in trace distance.
- Input dimension $\dim(H) = \infty$ for $\epsilon = \delta = 0$ [AB+09].
- $\forall \epsilon + \delta < 1$, $\dim(H) \geq \Omega(d^{\log(d) / \text{poly log log}(d)})$. 
Technical Outline & Contributions

Technical Target
- Introduce hardness of SDPs/SoS into quantum problems.
- Deal with their limitations, such as boolean domains and commutative problems.

Technical Contributions
- Formulate a framework of reductions for this purpose. Also applicable to other problems, e.g., Nash's equilibria.
- Design reductions following the guidelines of the framework.
- Special techniques to handle general domains and non-commutative problems.
Technical Target

- Introduce hardness of SDPs/SoS into quantum problems.
- Deal with their limitations, such as boolean domains and commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Also applicable to other problems, e.g., Nash’s equilibria.
- Design reductions following the guideline of the framework.
- Special techniques to handle general domains and non-commutative problems.
Technical Outline & Contributions

Technical Target

- Introduce hardness of SDPs/SoS into quantum problems.
- Deal with their limitations, such as boolean domains and commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Also applicable to other problems, e.g., Nash’s equilibria.
- Design reductions following the guideline of the framework.
- Special techniques to handle general domains and non-commutative problems.
Technical Outline & Contributions

Technical Target

- Introduce hardness of SDPs/SoS into quantum problems.
- Deal with their limitations, such as boolean domains and commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Also applicable to other problems, e.g., Nash’s equilibria.
- Design reductions following the guideline of the framework.
- Special techniques to handle general domains and non-commutative problems.
Technical Outline & Contributions

Technical Target

- Introduce hardness of SDPs/SoS into quantum problems.
- Deal with their limitations, such as boolean domains and commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Also applicable to other problems, e.g., Nash’s equilibria.
- Design reductions following the guideline of the framework.
- Special techniques to handle general domains and non-commutative problems.
One way to show that a polynomial $f(x)$ is nonnegative could be

$$f(x) = \sum a_i(x)^2 \geq 0.$$ 

**Example**

$$f(x) = 2x^2 - 6x + 5$$

$$= (x^2 - 2x + 1) + (x^2 - 4x + 4)$$

$$= (x - 1)^2 + (x - 2)^2 \geq 0.$$ 

Such a decomposition is called a sum of squares (SOS) certificate for the non-negativity of $f$. The min degree, $\deg_{sos}$. 

---

This example illustrates the principle of sum-of-squares (SoS) in showing the non-negativity of a polynomial. The sum-of-squares certificate, $f(x) = \sum a_i(x)^2 \geq 0$, provides a way to demonstrate that a polynomial is nonnegative by expressing it as a sum of squares of other polynomials.

---

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
**Definition (Variety)**

A set \( V \subseteq \mathbb{C}^n \) is called an *algebraic variety* if

\[
V = \{ x \in \mathbb{C}^n : g_1(x) = \cdots = g_k(x) = 0 \}.
\]

Non-negativity of \( f(x) \) on \( V \) could be shown by

\[
f(x) = \sum a_i(x)^2 + \sum b_j(x)g_j(x) \geq 0.
\]

**Question:** whether all nonnegative polynomials on certain variety have a *SOS certificate*? Hilbert 17th problem!
**Definition (Variety)**

A set $V \subseteq \mathbb{C}^n$ is called an *algebraic variety* if

$$V = \{ x \in \mathbb{C}^n : g_1(x) = \cdots = g_k(x) = 0 \}.$$

Non-negativity of $f(x)$ on $V$ could be shown by

$$f(x) = \sum a_i(x)^2 + \sum b_j(x)g_j(x) \geq 0.$$  

**Question:** whether all nonnegative polynomials on certain variety have a **SOS certificate**? Hilbert 17th problem!

A. Harrow, A. Natarajan, and X. Wu  
Limitations of monogamy, Tsirelson bounds & SDPs
A set $V \subseteq \mathbb{C}^n$ is called an \textit{algebraic variety} if $V = \{x \in \mathbb{C}^n : g_1(x) = \cdots = g_k(x) = 0\}$.

Non-negativity of $f(x)$ on $V$ could be shown by

$$f(x) = \sum a_i(x)^2 + \sum b_j(x)g_j(x) \geq 0.$$ 

\textbf{Question}: whether all nonnegative polynomials on certain variety have a \textbf{SOS} certificate? Hilbert 17th problem!
SoS in Optimization

\[
\begin{align*}
\max & \quad f(x) \\
\text{subject to} & \quad g_i(x) = 0 \quad \forall i
\end{align*}
\] (2)

is equivalent to (justified by Positivstellensatz)

\[
\begin{align*}
\min & \quad \nu \\
\text{such that} & \quad \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x),
\end{align*}
\] (3)

where \(\sigma(x)\) is SOS and \(b_i(x)\) is any polynomial.
If $\sigma(x), b_i(x)$ have any degrees (or $\deg_{\text{sos}}(\nu - f)$), then problem (3) is equivalent to problem (2).

By bounding the degrees, we get the Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

\[
\min \nu \quad \text{such that} \quad \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x), \quad (4)
\]

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\deg(\sigma(x)), \deg(b_i(x)g_i(x)) \leq 2D$. 

A. Harrow, A. Natarajan, and X. Wu  
Limitations of monogamy, Tsirelson bounds & SDPs
SoS relaxation: Lasserre/Parrilo Hierarchy

- If $\sigma(x), b_i(x)$ have any degrees (or $\deg_{\text{sos}}(\nu - f)$), then problem (3) is equivalent to problem (2).

- By bounding the degrees, we get the Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

\[
\begin{align*}
\min \quad & \nu \\
\text{such that} \quad & \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x), \\
\end{align*}
\]

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\deg(\sigma(x)), \deg(b_i(x)g_i(x)) \leq 2D$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
SoS relaxation: Lasserre/Parrilo Hierarchy

- If \( \sigma(x), b_i(x) \) have any degrees (or \( \text{deg}_{\text{sos}}(\nu - f) \)), then problem (3) is equivalent to problem (2).
- By bounding the degrees, we get the Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

\[
\begin{align*}
\min \quad & \nu \\
\text{such that} \quad & \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x), \\
\text{where} \quad & \sigma(x) \text{ is SOS and } b_i(x) \text{ is any polynomial and } \text{deg}(\sigma(x)), \\
& \text{deg}(b_i(x)g_i(x)) \leq 2D.
\end{align*}
\]
SoS relaxation: Lasserre/Parrilo Hierarchy

- If $\sigma(x), b_i(x)$ have any degrees (or $\text{deg}_{\text{sos}}(\nu - f)$), then problem (3) is equivalent to problem (2).
- By bounding the degrees, we get the Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

\[
\begin{align*}
\min & \quad \nu \\
\text{such that} & \quad \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x),
\end{align*}
\]

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\text{deg}(\sigma(x)), \text{deg}(b_i(x)g_i(x)) \leq 2D$. 

A. Harrow, A. Natarajan, and X. Wu  
Limitations of monogamy, Tsirelson bounds & SDPs
Recall $h_{\text{Sep}(d,d)}(M)$:

$$h_{\text{Sep}(d,d)}(M) := \max_{x,y \in \mathbb{C}^d, \|x\|_2 = \|y\|_2 = 1} \sum_{i,j,k,l \in [d]} M_{ij,kl} x_i^* x_j y_k^* y_l. \quad (5)$$

**Recall**: this is an instance of *polynomial optimization* problems with a homogenous degree 4 objective polynomial and a degree 2 constraint polynomial.

Its Lasserre’s hierarchy is the DPS hierarchy with full symmetry.
Non-commutative (nc) SoS

Given $F, G_1, \ldots, G_m \in \mathcal{R}\langle X \rangle$, define

$$F_{\text{max}} := \sup_{\rho, X=(X_1, \ldots, X_n)} \text{Tr}[\rho F(X)]$$

subject to $\rho \geq 0$, $\text{Tr} \rho = 1$, $G_1(X) = \cdots = G_m(X) = 0$. \hspace{1cm} (6)

Note that the supremum here is over density operators $\rho$ and Hermitian operators $X_1, \ldots, X_n$ that may be infinite dimensional;
A non-commutative SoS proof can be expressed similarly as

\[ c - F = \sum_{i=1}^{k} P_i^+ P_i + \sum_{i=1}^{m} Q_i G_i R_i, \quad (7) \]

for \( \{ P_i \}, \{ Q_i \}, \{ R_i \} \subset \mathcal{R}(X) \). Likewise the best degree-\( d \) ncSoS proof can be found in time \( n^{O(d)} m^{O(1)} \) by SDPs.

The NPA hierarchy for approximating \( \omega^*(G) \) is an ncSoS SDP hierarchy.
A non-commutative SoS proof can be expressed similarly as

$$c - F = \sum_{i=1}^{k} P_i^\dagger P_i + \sum_{i=1}^{m} Q_i G_i R_i,$$

(7)

for \(\{P_i\}, \{Q_i\}, \{R_i\} \subset \mathcal{R}\langle X\rangle\). Likewise the best degree-\(d\) ncSoS proof can be found in time \(n^{O(d)} m^{O(1)}\) by SDPs.

The NPA hierarchy for approximating \(\omega^*(G)\) is an ncSoS SDP hierarchy.
General SDPs

- The DPS and NPA hierarchies are just SoS and ncSoS SDP hierarchies.
- Thus, lower bounds for $\deg_{\text{SOS}} \Rightarrow$ lower bounds for DPS and NPA.
- How about general SDPs?

Lee-Raghavendra-Steurer

- Any $\deg_{\text{SOS}}$ lower bound on $\{0, 1\}^n$ $\Rightarrow$ a lower bound on SDP relaxations
- Optimization over $x \in \{0, 1\}^n$ relaxed $X'$ is $f(X') = f(x)$. Embedding!
- LRS's analysis crucially relies on $\{0, 1\}^n$
General SDPs

- The DPS and NPA hierarchies are just SoS and ncSoS SDP hierarchies.
- Thus, lower bounds for \( \text{deg}_{\text{SoS}} \) \( \Rightarrow \) lower bounds for DPS and NPA.
- How about general SDPs?

Lee-Raghavendra-Steurer

- Any \( \text{deg}_{\text{SoS}} \) lower bound on \( \{0, 1\}^n \) \( \Rightarrow \) a lower bound on SDP relaxations.
- Embedding! LRS's analysis crucially relies on \( \{0, 1\}^n \).

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
The DPS and NPA hierarchies are just SoS and ncSoS SDP hierarchies.

Thus, lower bounds for $\deg_{\text{SoS}} \Rightarrow$ lower bounds for DPS and NPA.

How about general SDPs?

Lee-Raghavendra-Steurer

- Any $\deg_{\text{SoS}}$ lower bound on $\{0,1\}^n \Rightarrow$ a lower bound on SDP relaxations.
- SDP relaxation: $\forall x \in \{0,1\}^n$, $\exists$ relaxed $X'$, s.t., $f(x) = F(X')$. Embedding!
- LRS's analysis crucially relies on $\{0,1\}^n$. 

A. Harrow, A. Natarajan, and X. Wu  Limitations of monogamy, Tsirelson bounds & SDPs
General SDPs

- The DPS and NPA hierarchies are just SoS and ncSoS SDP hierarchies.
- Thus, lower bounds for $\deg_{\text{sos}} \Rightarrow$ lower bounds for DPS and NPA.
- How about general SDPs?

Lee-Raghavendra-Steurer

- Any $\deg_{\text{sos}}$ lower bound on $\{0, 1\}^n \Rightarrow$ a lower bound on SDP relaxations.
  - SDP relaxation: $\forall x \in \{0, 1\}^n$, $\exists$ relaxed $X'$, s.t., $f(x) = F(X')$. Embedding!
  - LRS’s analysis crucially relies on $\{0, 1\}^n$. 
General SDPs

- The DPS and NPA hierarchies are just SoS and ncSoS SDP hierarchies.
- Thus, lower bounds for $\deg_{\text{sos}} \Rightarrow$ lower bounds for DPS and NPA.
- How about general SDPs?

Lee-Raghavendranda-Steurer

- Any $\deg_{\text{sos}}$ lower bound on $\{0, 1\}^n \Rightarrow$ a lower bound on SDP relaxations.
- SDP relaxation: $\forall x \in \{0, 1\}^n$, $\exists$ relaxed $X'$, s.t., $f(x) = F(X')$. Embedding!
- LRS's analysis crucially relies on $\{0, 1\}^n$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
General SDPs

- The DPS and NPA hierarchies are just SoS and ncSoS SDP hierarchies.
- Thus, lower bounds for $\deg_{\text{sos}} \Rightarrow$ lower bounds for DPS and NPA.
- How about general SDPs?

Lee-Raghavendra-Steurer

- Any $\deg_{\text{sos}}$ lower bound on $\{0, 1\}^n \Rightarrow$ a lower bound on SDP relaxations.
- SDP relaxation: $\forall x \in \{0, 1\}^n$, $\exists$ relaxed $X'$, s.t., $f(x) = F(X')$. Embedding!
- LRS’s analysis crucially relies on $\{0, 1\}^n$. 
Pseudo-distribution

Dual of the SOS cone

- Let $\Sigma_{d,2D}$ be the cone of all PSD matrices representing SOS polynomials with degree up to $2D$.
- The dual cone $\Sigma^*_{d,2D}$ is moment $M_D(x) \geq 0$, where entry $(\alpha, \beta)$ of $M_d(x)$ is $\int x^{\alpha+\beta} \mu(dx)$, $|\alpha|, |\beta| \leq d$.

Pseudo-distribution/expectation

- Moment $M_D(x)$ gives rise to pseudo-distribution.
- Expectation on it is pseudo-expectation.
- Behave similar to expectation for low-degree polynomials.
Dual of the SOS cone

- Let $\Sigma_{d,2D}$ be the cone of all PSD matrices representing SOS polynomials with degree up to $2D$.
- The dual cone $\Sigma^*_{d,2D}$ is moment $M_D(x) \geq 0$, where entry $(\alpha, \beta)$ of $M_d(x)$ is $\int x^{\alpha+\beta} \mu(dx)$, $|\alpha|, |\beta| \leq d$.

Pseudo-distribution/expectation

- Moment $M_D(x)$ gives rise to pseudo-distribution. Expectation on it is pseudo-expectation.
- Behave similar to expectation for low-degree polynomials.
A degree-\(d\) pseudo-expectation \(\tilde{E}\) is an element of \(\mathcal{R}[x]^*_d\) (i.e. a linear map from \(\mathcal{R}[x]_d\) to \(\mathcal{R}\)) satisfying

- **Normalization.** \(\tilde{E}[1] = 1\).
- **Positivity.** \(\tilde{E}[p^2] \geq 0\) for any \(p \in \mathcal{R}[x]_{d/2}\).

\(\tilde{E}\) satisfies the constraints \(g_1, \ldots, g_m\) if \(\tilde{E}[g_iq] = 0\) for all \(i \in [n]\) and all \(q \in \mathcal{R}[x]_{d-\deg(g_i)}\).

\[ f^d_{\text{SoS}} = \max\{\tilde{E}[f] : \tilde{E} \text{ of degree-}d \text{ satisfying } g_1, \ldots, g_m\}. \quad (8) \]
A degree-$d$ pseudo-expectation $\tilde{E}$ is an element of $\mathcal{R}[x]_d^*$ (i.e. a linear map from $\mathcal{R}[x]_d$ to $\mathcal{R}$) satisfying

- **Normalization.** $\tilde{E}[1] = 1$.
- **Positivity.** $\tilde{E}[p^2] \geq 0$ for any $p \in \mathcal{R}[x]_{d/2}$.

$\tilde{E}$ satisfies the constraints $g_1, \ldots, g_m$ if $\tilde{E}[g_i q] = 0$ for all $i \in [n]$ and all $q \in \mathcal{R}[x]_{d-\deg(g_i)}$.

$$f_{\text{SoS}}^d = \max\{\tilde{E}[f] : \tilde{E} \text{ of degree-}d \text{ satisfying } g_1, \ldots, g_m\}. \quad (8)$$
A degree-\(d\) pseudo-expectation \(\tilde{E}\) is an element of \(\mathcal{R}[x]^{\ast}_d\) (i.e. a linear map from \(\mathcal{R}[x]_d\) to \(\mathcal{R}\)) satisfying

- **Normalization.** \(\tilde{E}[1] = 1\).
- **Positivity.** \(\tilde{E}[p^2] \geq 0\) for any \(p \in \mathcal{R}[x]_{d/2}\).

\(\tilde{E}\) satisfies the constraints \(g_1, \ldots, g_m\) if \(\tilde{E}[g_i q] = 0\) for all \(i \in [n]\) and all \(q \in \mathcal{R}[x]_{d-\deg(g_i)}\).

\[
f_{\text{SoS}}^d = \max\{\tilde{E}[f] : \tilde{E} \text{ of degree-}d \text{ satisfying } g_1, \ldots, g_m\}. \quad (8)
\]
What constitutes an integrality gap?

- An instance $\Phi$ that has $f_{\text{opt}}(\Phi)$ is small.
- But $f_{\text{SoS}}^d(\Phi)$ is large for some $d \Rightarrow$ lower bound at level $d$.

Example

- 3XOR: $O(n)$ clauses on $n$ boolean variables:
  $$x_i \oplus x_j \oplus x_k = C_{ijk}.$$
- A random instance satisfies $1/2 + \epsilon$ of clauses while an $\Omega(n)$ pseudo-solution believes it satisfies all clauses.
What constitutes an integrality gap?

- An instance $\Phi$ that has $f_{\text{opt}}(\Phi)$ is small.
- But $f^d_{\text{SoS}}(\Phi)$ is large for some $d \Rightarrow$ lower bound at level $d$.

Example

- 3XOR: $O(n)$ clauses on $n$ boolean variables:
  \[ x_i \oplus x_j \oplus x_k = C_{ijk}. \]
- A random instance satisfies $1/2 + \epsilon$ of clauses while an $\Omega(n)$ pseudo-solution believes it satisfies all clauses.
Extend integrality gaps via reductions

Reduction from $A$ to $B$

- **Reduction** is an instance-mapping $\Phi^A \rightarrow \Phi^B$.
- **Soundness**: $f^A_{\text{opt}}(\Phi^A)$ small $\Rightarrow f^B_{\text{opt}}(\Phi^B)$
- **Pseudo-completeness**: $f^d_{\text{SoS}}(\Phi^A)$ large $\Rightarrow f^d_{\text{SoS}}(\Phi^B)$ large, $d_B$ is not too smaller than $d_A$.

Pseudo-completeness: low-degree reduction

- Let $\mu^A(\tilde{E}^A)$ be the pseudo-solution for $\Phi^A$. One needs to construct a $\mu^B(\tilde{E}^B)$ for $\Phi^B$.
- Sufficient condition: a low-degree polynomial that maps $\mu^A \rightarrow \mu^B$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Extend integrality gaps via reductions

**Reduction from A to B**

- Reduction is an instance-mapping $\Phi^A \rightarrow \Phi^B$.
- **Soundness**: $f_{\text{opt}}^A(\Phi^A)$ small $\Rightarrow f_{\text{opt}}^B(\Phi^B)$
- **Pseudo-completeness**: $f_{\text{SoS}}^{d_A}(\Phi^A)$ large $\Rightarrow f_{\text{SoS}}^{d_B}(\Phi^B)$ large, $d_B$ is not too smaller than $d_A$.

**Pseudo-completeness: low-degree reduction**

- Let $\mu^A_{\text{SoS}}(\tilde{E}^A)$ be the pseudo-solution for $\Phi^A$. One needs to construct a mapping for $\Phi^B$.
- Sufficient conditions: a low-degree polynomial that maps $\mu^A$ to $\mu^B$.

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Extend integrality gaps via reductions

Reduction from A to B

- Reduction is an instance-mapping $\Phi^A \rightarrow \Phi^B$.
- **Soundness**: $f_{\text{opt}}^A(\Phi^A)$ small $\Rightarrow f_{\text{opt}}^B(\Phi^B)$
- **Pseudo-completeness**: $f_{\text{SoS}}^{d_A}(\Phi^A)$ large $\Rightarrow f_{\text{SoS}}^{d_B}(\Phi^B)$ large, $d_B$ is not too smaller than $d_A$.

Pseudo-completeness: low-degree reduction

- Let $\mu_A(\tilde{E}_A)$ be the pseudo-solution for $\Phi^A$. One needs to construct a $\mu_B(\tilde{E}_B)$ for $\Phi^B$.
- Sufficient condition: a low-degree polynomial that maps $\mu_A(\tilde{E}_A)$ to $\mu_B(\tilde{E}_B)$.
Extend integrality gaps via reductions

**Reduction from A to B**

- Reduction is an instance-mapping $\Phi^A \rightarrow \Phi^B$.
- **Soundness**: $f_{opt}^A(\Phi^A)$ small $\Rightarrow f_{opt}^B(\Phi^B)$
- **Pseudo-completeness**: $f_{SoS}^{d_A}(\Phi^A)$ large $\Rightarrow f_{SoS}^{d_B}(\Phi^B)$ large, $d_B$ is not too smaller than $d_A$.

**Pseudo-completeness: low-degree reduction**

- Let $\mu_A(\tilde{E}_A)$ be the pseudo-solution for $\Phi^A$. One needs to construct a $\mu_B(\tilde{E}_B)$ for $\Phi^B$.
- Sufficient condition: a low-degree polynomial that maps $\mu_A \rightarrow \mu_B$.
Extend integrality gaps via reductions

Reduction from A to B
- Reduction is an instance-mapping $\Phi^A \rightarrow \Phi^B$.
- **Soundness**: $f_{\text{opt}}^A(\Phi^A)$ small $\Rightarrow f_{\text{opt}}^B(\Phi^B)$
- **Pseudo-completeness**: $f_{\text{SoS}}^{d_A}(\Phi^A)$ large $\Rightarrow f_{\text{SoS}}^{d_B}(\Phi^B)$ large, $d_B$ is not too smaller than $d_A$.

Pseudo-completeness: low-degree reduction
- Let $\mu_A(\tilde{E}_A)$ be the pseudo-solution for $\Phi^A$. One needs to construct a $\mu_B(\tilde{E}_B)$ for $\Phi^B$.
- **Sufficient condition**: a low-degree polynomial that maps $\mu_A \rightarrow \mu_B$. 

---

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Extend integrality gaps via reductions

Reduction from A to B

- Reduction is an instance-mapping $\Phi^A \rightarrow \Phi^B$.
- **Soundness**: $f_{\text{opt}}^A(\Phi^A)$ small $\Rightarrow f_{\text{opt}}^B(\Phi^B)$
- **Pseudo-completeness**: $f_{\text{SoS}}^{d_A}(\Phi^A)$ large $\Rightarrow f_{\text{SoS}}^{d_B}(\Phi^B)$ large, $d_B$ is not too smaller than $d_A$.

Pseudo-completeness: low-degree reduction

- Let $\mu_A(\tilde{E}_A)$ be the pseudo-solution for $\Phi^A$. One needs to construct a $\mu_B(\tilde{E}_B)$ for $\Phi^B$.
- **Sufficient condition**: a low-degree polynomial that maps $\mu_A \rightarrow \mu_B$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Extend integrality gaps via reductions:

A reduction with *pseudo-completeness* and *soundness* leads to an integrality gap of degree $d_B$ for $\Phi^B$.

SDP lower bounds (LRS)

- Only apply to $\{0, 1\}^n \Rightarrow$ no direct application on $h_{\text{Sep}}$ or $\omega^*(G)$.
- Additional condition: embedding (replacing pseudo-completeness)
Extend integrality gaps via reductions:

A reduction with *pseudo-completeness* and *soundness* leads to an integrality gap of degree $d_B$ for $\Phi^B$.

**SDP lower bounds (LRS)**

- Only apply to $\{0, 1\}^n \Rightarrow$ no direct application on $h_{\text{Sep}}$ or $\omega^*(G)$.
- Additional condition: embedding (replacing pseudo-completeness)
  - Assume $A \Rightarrow B$ and apply LRS on $A$ that is on $\{0, 1\}^n$.
  - Then $\Rightarrow$ needs to be embedded as well as its composition with SDP relaxations.
A reduction with *pseudo-completeness* and *soundness* leads to an integrality gap of degree \( d_B \) for \( \Phi_B \).

**SDP lower bounds (LRS)**

- Only apply to \( \{0, 1\}^n \) \( \Rightarrow \) no direct application on \( h_{\text{Sep}} \) or \( \omega^*(G) \).
- Additional condition: embedding (replacing pseudo-completeness)
  - Assume \( A \Rightarrow B \) and apply LRS on \( A \) that is on \( \{0, 1\}^n \).
  - Then \( \Rightarrow \) needs to be embedded as well as its composition with SDP relaxations.
Extend integrality gaps via reductions:

A reduction with *pseudo-completeness* and *soundness* leads to an integrality gap of degree $d_B$ for $\Phi^B$.

**SDP lower bounds (LRS)**

- Only apply to $\{0, 1\}^n \Rightarrow$ no direct application on $h_{\text{Sep}}$ or $\omega^*(G)$.
- Additional condition: embedding (replacing pseudo-completeness)
  - Assume $A \Rightarrow B$ and apply LRS on $A$ that is on $\{0, 1\}^n$.
  - Then $\Rightarrow$ needs to be embedded as well as its composition with SDP relaxations.
Extend integrality gaps via reductions:

A reduction with *pseudo-completeness* and *soundness* leads to an integrality gap of degree $d_B$ for $\Phi^B$.

**SDP lower bounds (LRS)**

- Only apply to $\{0, 1\}^n$ \implies no direct application on $h_{\text{Sep}}$ or $\omega^*(G)$.
- Additional condition: embedding (replacing pseudo-completeness)
  - Assume $A \Rightarrow B$ and apply LRS on $A$ that is on $\{0, 1\}^n$.
  - Then $\Rightarrow$ needs to be **embedded** as well as its composition with SDP relaxations.
A typical reduction

\[ \text{3XOR} \overset{R_1}{\longrightarrow} \cdots \overset{R_2}{\longrightarrow} A \text{ over } \{0, 1\}^n \overset{R_3}{\longrightarrow} \cdots \overset{R_4}{\longrightarrow} \text{Final Problem} \]

- Reductions \( R_1, \cdots, R_2 \) lead to an SoS integrality gap at the problem \( A \).
- Apply LRS on the problem \( A \) over boolean domains.
- Reductions \( R_3, \cdots, R_4 \) are embedding reductions.
- Extend LRS results without redoing their analysis.
A typical reduction

\[ 3\text{XOR} \underbrace{\Rightarrow \cdots \Rightarrow}_{R_1, R_2} A \text{ over } \{0, 1\}^n \underbrace{\Rightarrow \cdots \Rightarrow}_{R_3, R_4} \text{Final Problem} \]

- Reductions \( R_1, \cdots, R_2 \) lead to an SoS integrality gap at the problem \( A \).
- Apply LRS on the problem \( A \) over boolean domains.
- Reductions \( R_3, \cdots, R_4 \) are embedding reductions.
- Extend LRS results without redoing their analysis.
A typical reduction

\[ 3\text{XOR} \xrightarrow{R_1} \cdots \xrightarrow{R_3} A \text{ over } \{0, 1\}^n \xrightarrow{R_4} \cdots \xrightarrow{R_4} \text{Final Problem} \]

- Reductions \( R_1, \cdots, R_2 \) lead to an SoS integrality gap at the problem \( A \).
- Apply LRS on the problem \( A \) over boolean domains.
- Reductions \( R_3, \cdots, R_4 \) are embedding reductions.
- Extend LRS results without redoing their analysis.
A typical reduction

3XOR $\Rightarrow \cdots \Rightarrow A$ over $\{0, 1\}^n \Rightarrow \cdots \Rightarrow$ Final Problem

- Reductions $R_1, \cdots, R_2$ lead to an SoS integrality gap at the problem $A$.
- Apply LRS on the problem $A$ over boolean domains.
- Reductions $R_3, \cdots, R_4$ are embedding reductions.
- Extend LRS results without redoing their analysis.
Real reductions for $h_{\text{Sep}}$ and $\omega^*(G)$

Figure: All our results are derived from the integrality gaps of 3XOR. Red nodes: problems over the boolean cube and LRS is applied. Blue arrows are “embedding reductions”.

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Reduction for $h_{\text{Sep}}$

$3\text{XOR} \xrightarrow{R_1} 2\text{-OUT-OF-4-SAT-EQ} \xrightarrow{R_2} \text{QMA}(2)\text{-Acc PROB} \xrightarrow{R_3} h_{\text{Sep}}$

- $R_1$: a classical step. Low-degree & soundness similar to the degree reduction step in Dinur’s proof of the PCP theorem.
- $R_2$: a quantum step. Apply a modified QMA(2) protocol for 3-SAT [AB+09, HM13]. Low-degree due to the tests of the protocol. Soundness inhered from the protocol.
- $R_3$: embedding by construction. Soundness inhered from the above protocol.
Reduction for $h_{\text{Sep}}$

$3\text{XOR} \xrightarrow{R_1} 2\text{-OUT-OF-4-SAT-EQ} \xrightarrow{R_2} \text{QMA(2)-Acc Prob} \xrightarrow{R_3} h_{\text{Sep}}$

- $R_1$: a classical step. Low-degree & soundness similar to the degree reduction step in Dinur’s proof of the PCP theorem.

- $R_2$: a quantum step. Apply a modified QMA(2) protocol for 3-SAT [AB+09, HM13]. Low-degree due to the tests of the protocol. Soundness inhered from the protocol.

- $R_3$: embedding by construction. Soundness inhered from the above protocol.
Reduction for $h_{\text{Sep}}$

\[ 3\text{XOR} \xrightarrow{R_1} 2\text{-OUT-OF-4-SAT-EQ} \xrightarrow{R_2} \text{QMA}(2)\text{-Acc PROB} \xrightarrow{R_3} h_{\text{Sep}} \]

- $R_1$: a classical step. Low-degree & soundness similar to the degree reduction step in Dinur’s proof of the PCP theorem.

- $R_2$: a quantum step. Apply a modified QMA(2) protocol for 3-SAT [AB+09, HM13]. Low-degree due to the tests of the protocol. Soundness inhered from the protocol.

- $R_3$: embedding by construction. Soundness inhered from the above protocol.
Reduction for $\omega^*(G)$

- $R_1$: reduction by a multi-prover interactive proof protocol in [IKM]. Low-degree due to the tests of the protocol. Soundness inherited from the protocol.

- $R_2$: embedding by construction. Soundness inherited from the above protocol.

- Integrality gap for ncSOS: additional step to embed an SoS pseudo-solution into an ncSoS pseudo-solution.
Reduction for $\omega^*(G)$

\[
3\text{XOR} \xrightarrow{R_1} \omega_{\text{HONEST CLASSICAL}} \xrightarrow{R_2} \omega^*(G)
\]

- $R_1$: reduction by a multi-prover interactive proof protocol in [IKM]. Low-degree due to the tests of the protocol. Soundness inhered from the protocol.
- $R_2$: embedding by construction. Soundness inhered from the above protocol.
- Integrality gap for ncSOS: additional step to embed an SoS pseudo-solution into an ncSoS pseudo-solution.

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Reduction for $\omega^*(G)$

$3\text{XOR} \xrightarrow{R_1} \omega_{\text{HONEST CLASSICAL}} \xrightarrow{R_2} \omega^*(G)$

- $R_1$: reduction by a multi-prover interactive proof protocol in [IKM]. Low-degree due to the tests of the protocol. Soundness inhered from the protocol.
- $R_2$: embedding by construction. Soundness inhered from the above protocol.
- Integrality gap for ncSOS: additional step to embed an SoS pseudo-solution into an ncSoS pseudo-solution.
First unconditional SoS/SDP lower bounds for $h_{\text{Sep}}$ and $\omega^*(G)$.

Match ETH-based bounds for $h_{\text{Sep}}$.

Implication on QMA(2) and Watrous’s dis-entangler conjecture.

A reduction framework. Already find an application to the Nash equilibria.

Reductions for general domains and non-commutative problems.
Summary

**Results**
- First unconditional SoS/SDP lower bounds for $h_{\text{Sep}}$ and $\omega^*(G)$.
- Match ETH-based bounds for $h_{\text{Sep}}$.
- Implication on QMA(2) and Watrous’s dis-entangler conjecture.

**Technical Contribution**
- A reduction framework. Already find an application to the Nash equilibria.
- Reductions for general domains and non-commutative problems.
Open Questions

- Prove stronger hardness for $\omega^*(G)$ that matches computational hardness.
- Prover stronger SoS/SDP lower bounds than ETH bounds.
- Consider general convex programming for $h_{\text{Sep}}$.
- Other applications of the techniques here.
Open Questions

- Prove stronger hardness for $\omega^*(G)$ that matches computational hardness.
- Prover stronger SoS/SDP lower bounds than ETH bounds.
- Consider general convex programming for $h_{\text{Sep}}$.
- Other applications of the techniques here.
Open Questions

- Prove stronger hardness for $\omega^*(G)$ that matches computational hardness.
- Prover stronger SoS/SDP lower bounds than ETH bounds.
- Consider general convex programming for $h_{\text{Sep}}$.
- Other applications of the techniques here.
Open Questions

- Prove stronger hardness for $\omega^*(G)$ that matches computational hardness.
- Prover stronger SoS/SDP lower bounds than ETH bounds.
- Consider general convex programming for $h_{\text{Sep}}$.
- Other applications of the techniques here.
Thank you!
Q & A
If $\sigma(x), b_i(x)$ have any degrees (or $\deg_{\text{sos}}(\nu - f)$), then problem (3) is equivalent to problem (2).

By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

$$\min \nu$$

such that $\nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x)$, \hspace{1cm} (9)

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\deg(\sigma(x)), \deg(b_i(x)g_i(x)) \leq 2D$. 

---

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
If $\sigma(x), b_i(x)$ have any degrees (or $\deg_{sos}(\nu - f)$), then problem (3) is equivalent to problem (2).

By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

\[
\min \nu \\
\text{such that } \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x), \tag{9}
\]

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\deg(\sigma(x)), \deg(b_i(x)g_i(x)) \leq 2D$. 
If $\sigma(x), b_i(x)$ have any degrees (or $\deg_{\text{SOS}}(\nu - f)$), then problem (3) is equivalent to problem (2).

By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

\[
\min \nu \\
\text{such that} \quad \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x),
\]

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\deg(\sigma(x)), \deg(b_i(x)g_i(x)) \leq 2D.$
SoS relaxation: Lasserre/Parrilo Hierarchy

- If $\sigma(x), b_i(x)$ have any degrees (or $\deg_{\text{sos}}(\nu - f)$), then problem (3) is equivalent to problem (2).
- By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

$$\begin{align*}
\min & \quad \nu \\
\text{such that} & \quad \nu - f(x) = \sigma(x) + \sum_i b_i(x)g_i(x), \tag{9}
\end{align*}$$

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial and $\deg(\sigma(x)), \deg(b_i(x)g_i(x)) \leq 2D$. 
Why it is a SDP?

**Observation**

- Any \( p(x) \) (of degree \( 2D \)) = \( m^T Q m \), where \( m \) is the vector of monomials of degree up to \( 2D \) and \( Q \) is the coefficients.
- \( p(x) \) is a SOS iff \( Q \geq 0 \).

\[
\min_{\nu, b_{i\alpha} \in \mathbb{R}} \nu \text{ such that } \nu A_0 - F - \sum_{i\alpha} b_{i\alpha} G_{i\alpha} \geq 0. \tag{10}
\]

Complexity: \( \text{poly}(m) \text{ poly log}(1/\epsilon) \), where \( m = \left( \begin{array}{c} n+D \\ D \end{array} \right) \).
Why it is a SDP?

Observation

- Any $p(x)$ (of degree $2D$) $= m^T Q m$, where $m$ is the vector of monomials of degree up to $2D$ and $Q$ is the coefficients.
- $p(x)$ is a SOS iff $Q \geq 0$.

\[
\begin{align*}
\min_{\nu, b_{i\alpha} \in \mathbb{R}} & \quad \nu \\
\text{such that} & \quad \nu A_0 - F - \sum_{i\alpha} b_{i\alpha} G_{i\alpha} \geq 0. \\
\end{align*}
\]

(10)

Complexity: $\text{poly}(m) \text{poly log}(1/\epsilon)$, where $m = \binom{n+D}{D}$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs
Any $p(x)$ (of degree $2D$) $= m^T Q m$, where $m$ is the vector of monomials of degree up to $2D$ and $Q$ is the coefficients.

$p(x)$ is a SOS iff $Q \geq 0$.

\[
\min_{\nu, b_{i\alpha} \in \mathbb{R}} \nu \quad \text{such that} \quad \nu A_0 - F - \sum_{i\alpha} b_{i\alpha} G_{i\alpha} \geq 0. \tag{10}
\]

**Complexity:** $\text{poly}(m) \text{poly log}(1/\epsilon)$, where $m = (n+D^2)$. 

A. Harrow, A. Natarajan, and X. Wu

Limitations of monogamy, Tsirelson bounds & SDPs