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

QMA(2) Workshop, UMD

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 SOS/SDPs comparable to existing computational hardness.

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 SOS/SDPs comparable to existing computational hardness.

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 SOS/SDPs comparable to existing computational hardness.

Problem 1: Separability

Definition (Separable and Entangled States)

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

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

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

Definition (Entanglement Detection)

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

Either $\rho \in$ Sep, or ρ is far away from Sep.

Problem 1: Separability

Definition (Separable and Entangled States)

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

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

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

Definition (Entanglement Detection)

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

Either $\rho \in$ Sep, or ρ is far away from Sep.

Alternative Formulation

Definition (Weak Membership)

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

Via standard techniques in convex optimization, equivalent to

Definition (Weak Optimization)

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

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

with additive error ϵ.

$h_{\mathrm{Sep}(d,d)}(M)$

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

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. ($\ell_2 \to \ell_4$ 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. ($\ell_2 \to \ell_4$ 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. ($\ell_2 \to \ell_4$ 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. ($\ell_2 \to \ell_4$ 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. ($\ell_2 \to \ell_4$ norm)

Heuristics

Separability Criterions:

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

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

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

Heuristics

Separability Criterions:

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

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

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

Heuristics

Separability Criterions:

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

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

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

Heuristics

Separability Criterions:

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

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

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

Heuristics

Separability Criterions:

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

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

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

Heuristics

Separability Criterions:

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

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

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

Heuristics

Separability Criterions:

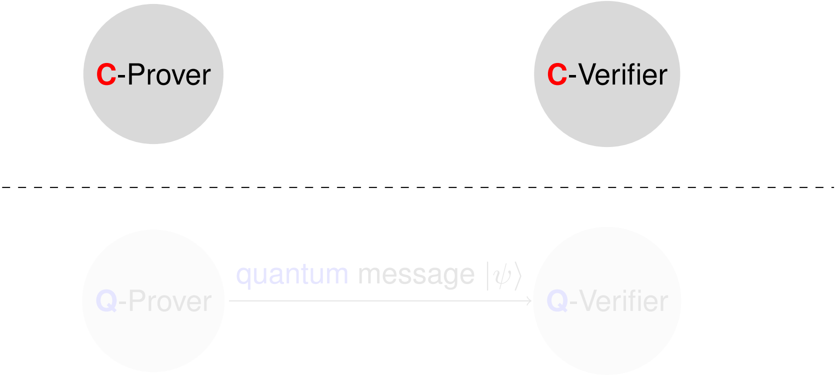
- Positive Partial Transpose (PPT) : $\rho^{T_{\mathcal{Y}}} = \rho$? [PH]
- Reduction Criterions: $I_{\mathcal{X}} \otimes \rho_Y \geq \rho$? [HH]
- **FAILURE**: any such test has arbitrarily large error. [BS]

Doherty-Parrilo-Spedalieri (DPS) hierarchy:

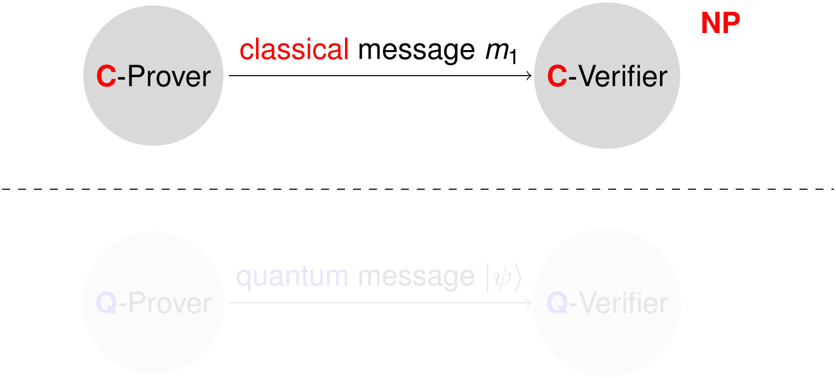
- ρ is k-extendible if $\exists$ *symmetric* $\sigma \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k)$, $\forall i, \rho = \sigma_{XY_i}$.
- $\rho \in$ Sep **if and only if** ρ is k-extendible for any $k \geq 0$.
- **Semidefinite program (SDP)**: size exponential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

QMA(2) vs QMA

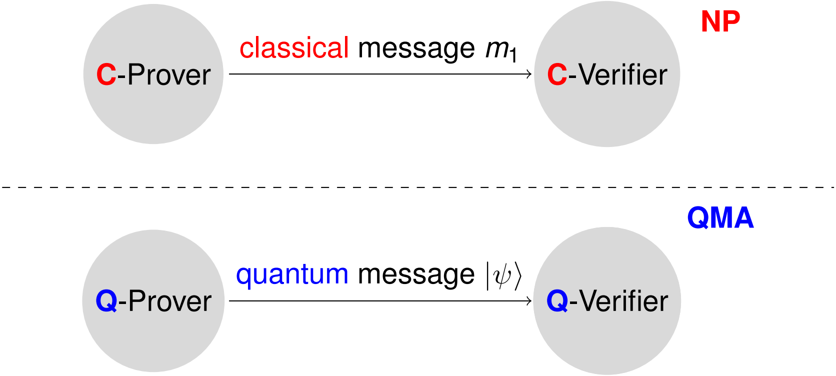
QMA(2) vs QMA


C-Prover
C-Verifier
Q-Prover
quantum message $|\psi\rangle$
Q-Verifier

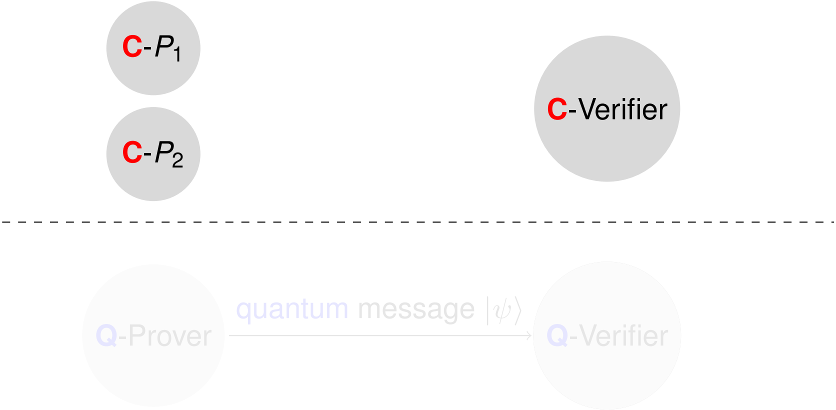
QMA(2) vs QMA


C-Prover
classical message m_1
C-Verifier
NP
Q-Prover
quantum message $|\psi\rangle$
Q-Verifier

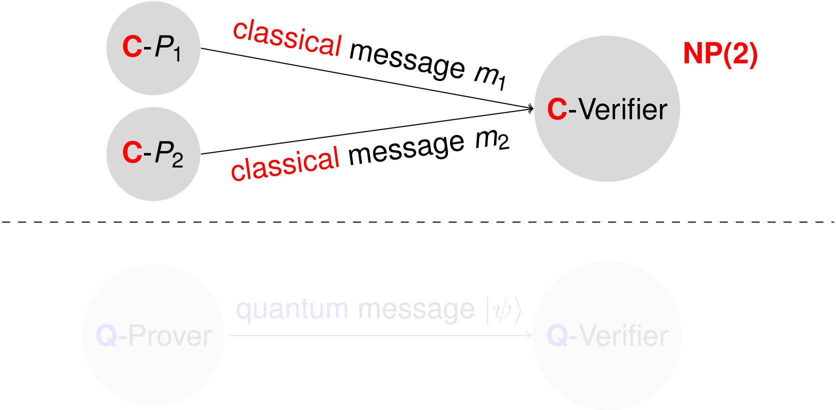
QMA(2) vs QMA


NP
C-Prover
classical message m_1
C-Verifier
QMA
Q-Prover
quantum message $|\psi\rangle$
Q-Verifier

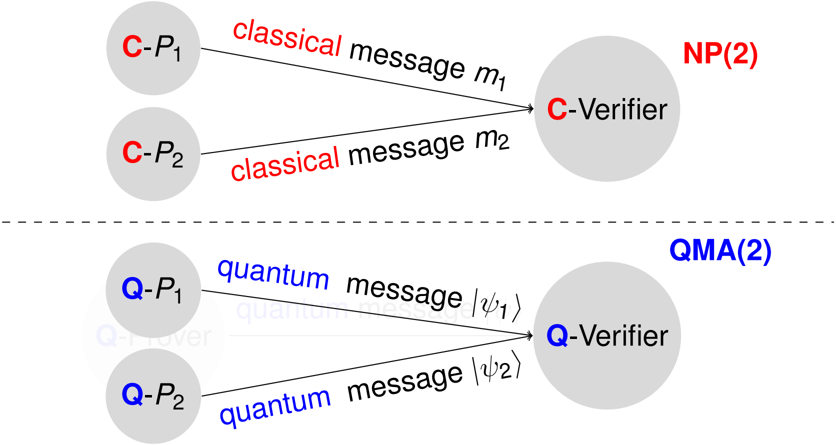
QMA(2) vs QMA


C-P_1
C-P_2
C-Verifier
Q-Prover
quantum message $|\psi\rangle$
Q-Verifier

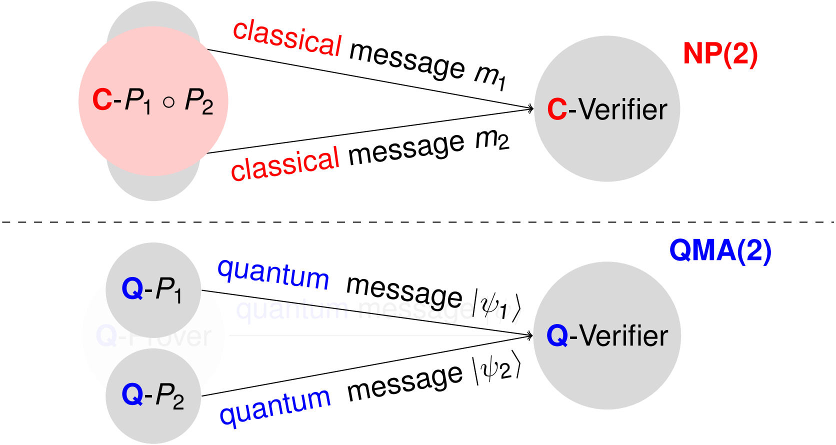
QMA(2) vs QMA


C-P_1
classical message m_1
C-P_2
classical message m_2
C-Verifier
NP(2)
Q-Prover
quantum message $|\psi\rangle$
Q-Verifier

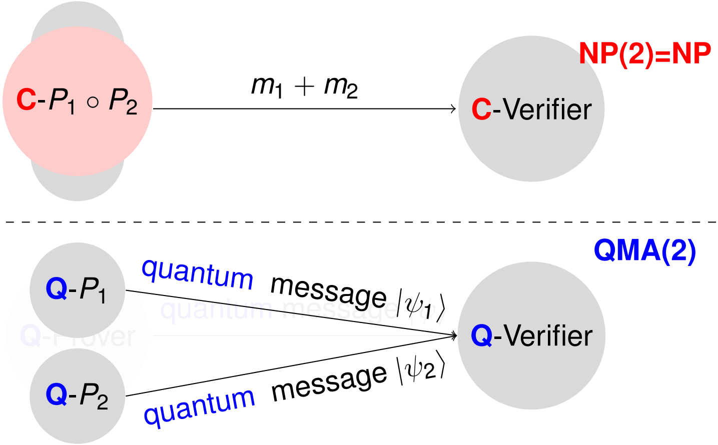
QMA(2) vs QMA


C-P_1
classical message m_1
C-P_2
classical message m_2
C-Verifier
NP(2)
QMA(2)
Q-P_1
quantum message $|\psi_1\rangle$
Q-P_2
quantum message $|\psi_2\rangle$
Q-Verifier

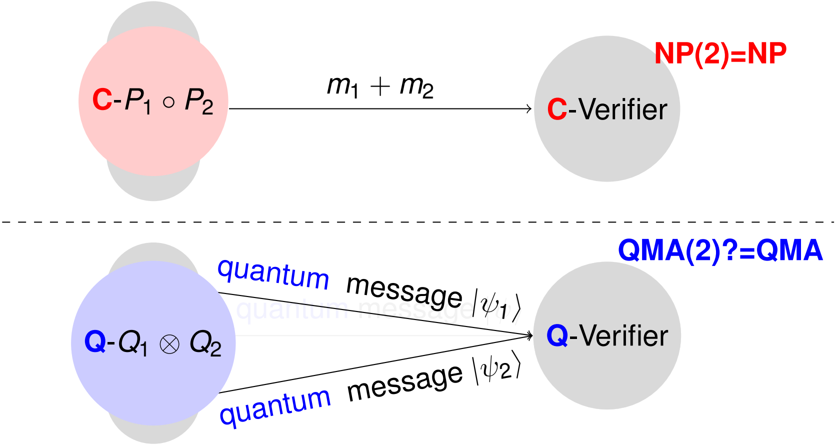
QMA(2) vs QMA


C-$P_1 \circ P_2$
classical message m_1
classical message m_2
C-Verifier
NP(2)
QMA(2)
Q-P_1
Q-P_2
quantum message $|\psi_1\rangle$
quantum message $|\psi_2\rangle$
Q-Verifier

QMA(2) vs QMA


C-$P_1 \circ P_2$
$m_1 + m_2$
C-Verifier
NP(2)=NP
QMA(2)
Q-P_1
Q-P_2
quantum message $|\psi_1\rangle$
quantum message $|\psi_2\rangle$
Q-Verifier

QMA(2) vs QMA


C-$P_1 \circ P_2$
$m_1 + m_2$
C-Verifier
NP(2)=NP
QMA(2)?=QMA
quantum message $|\psi_1\rangle$
Q-$Q_1 \otimes Q_2$
Q-Verifier
quantum message $|\psi_2\rangle$

History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA(2)$_{\log}$ [BT09, GNN] v.s. QMA$_{\log}$ = BQP [MW05].
- QMA(2) solves 3SAT (constant gaps) with $\tilde{O}(\sqrt{n})$-qubit proofs [ABD+, CD].
- QMA(2)=QMA(poly) [HM10].
- "Separable Hamiltonian Problem" (QMA(2)-complete) [CS12]. Tuesday
- Attacking QMA(2) by the perturbation method [Sch15]. Tuesday

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

History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA$(2)_{\log}$ [BT09, GNN] v.s. QMA$_{\log}$ $=$ BQP [MW05].
- QMA(2) solves 3SAT (constant gaps) with $\tilde{O}(\sqrt{n})$-qubit proofs [ABD+, CD].
- QMA(2)=QMA(poly) [HM10].
- "Separable Hamiltonian Problem" (QMA(2)-complete) [CS12]. Tuesday
- Attacking QMA(2) by the perturbation method [Sch15]. Tuesday

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

History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA(2)$_{\log}$ [BT09, GNN] v.s. QMA$_{\log}$ $=$ BQP [MW05].
- QMA(2) solves 3SAT (constant gaps) with $\tilde{O}(\sqrt{n})$-qubit proofs [ABD+, CD].
- QMA(2)=QMA(poly) [HM10].
- "Separable Hamiltonian Problem" (QMA(2)-complete) [CS12]. Tuesday
- Attacking QMA(2) by the perturbation method [Sch15]. Tuesday

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

History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA(2)$_{\log}$ [BT09, GNN] v.s. QMA$_{\log}$ $=$ BQP [MW05].
- QMA(2) solves 3SAT (constant gaps) with $\tilde{O}(\sqrt{n})$-qubit proofs [ABD+, CD].
- QMA(2)=QMA(poly) [HM10].
- "Separable Hamiltonian Problem" (QMA(2)-complete) [CS12]. Tuesday
- Attacking QMA(2) by the perturbation method [Sch15]. Tuesday

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

History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA(2)$_{\log}$ [BT09, GNN] v.s. QMA$_{\log}$ $=$ BQP [MW05].
- QMA(2) solves 3SAT (constant gaps) with $\tilde{O}(\sqrt{n})$-qubit proofs [ABD+, CD].
- QMA(2)=QMA(poly) [HM10].
- "Separable Hamiltonian Problem" (QMA(2)-complete) [CS12]. Tuesday
- Attacking QMA(2) by the perturbation method [Sch15]. Tuesday

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

History about QMA(2)

- First study in [KMY01, KMY03]. Surprising: NP $\subseteq$ QMA(2)$_{\log}$ [BT09, GNN] v.s. QMA$_{\log}$ $=$ BQP [MW05].
- QMA(2) solves 3SAT (constant gaps) with $\tilde{O}(\sqrt{n})$-qubit proofs [ABD+, CD].
- QMA(2)=QMA(poly) [HM10].
- ”Separable Hamiltonian Problem” (QMA(2)-complete) [CS12]. Tuesday
- Attacking QMA(2) by the perturbation method [Sch15]. Tuesday

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

Computational Hardness

reference	k	c	s	n
GNN12	2	1	$1 - \frac{1}{d \cdot \text{poly}\log(d)}$	$O(d)$
Per12	2	1	$1 - \frac{1}{\text{poly}(d)}$	$O(d)$
AB+08	$\sqrt{d} \cdot \text{poly}\log(d)$	1	0.99	$O(d)$
CD10	$\sqrt{d} \cdot \text{poly}\log(d)$	$1 - 2^{-d}$	0.99	$O(d)$
HM13	2	1	0.01	$\frac{\log^2(d)}{\text{poly}\log(d)}$

Table: Hardness results for $h_{\text{Sep}^k(d)}$ (k-partitie $h_{\text{Sep}(d,d)}$).

Hardness: 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.

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 $d^{O(\log(d)/\epsilon^2)} \to d^{O(\log(d))}$. [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?

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 $h_{\mathrm{Sep}(d)}$ 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 $d^{O(log(d)/\epsilon^2)} \to d^{O(log(d))}$. [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 $h_{\mathrm{Sep}(d)}$ 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 $d^{O(log(d)/\epsilon^2)} \to d^{O(log(d))}$. [BYC, BH]

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

Result I: Unconditional Hardness for h_{Sep}?

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

Theorem (Main I.1)

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

Theorem (Main I.2)

Any SDP relaxation that estimates $h_{\mathrm{Sep}(d)}(M)$ with $O(1/d^2)$ errors requires size $d^{\tilde{\Omega}(\log(d))}$.

Remark: Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.

Result I: Unconditional Hardness for h_{Sep}?

Will the hardness of $h_{\text{Sep}(d)}$ for const ϵ 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 estimates $h_{\text{Sep}(d)}(M)$ with $O(1/d^2)$ errors requires size $d^{\tilde{\Omega}(\log(d))}$.

Remark: Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.

Result I: Unconditional Hardness for h_{Sep}?

Will the hardness of $h_{\text{Sep}(d)}$ for const ϵ 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 estimates $h_{\text{Sep}(d)}(M)$ with $O(1/d^2)$ errors requires size $d^{\tilde{\Omega}(\log(d))}$.

Remark: Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.

Result I: Unconditional Hardness for h_{Sep}?

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

Theorem (Main I.1)

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

Theorem (Main I.2)

Any SDP relaxation that estimates $h_{\mathrm{Sep}(d)}(M)$ with $O(1/d^2)$ errors requires size $d^{\tilde{\Omega}(\log(d))}$.

Remark: Match $d^{\Omega(\log(d))}$ time bound when assuming ETH.

Implication on QMA(2)

Hardness applies to QMA(2)

- Our explicit hard instance M_{acc} is from a QMA(2) instance.
- de Finetti theorem of 1-LOCC [BCY, BH]: best possible parameters.

Unconditional proof of Watrous's dis-entangler conjecture

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

Implication on QMA(2)

Hardness applies to QMA(2)

- Our explicit hard instance M_{acc} is from a QMA(2) instance.
- de Finetti theorem of 1-LOCC [BCY, BH]: best possible parameters.

Unconditional proof of Watrous's dis-entangler conjecture

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

Implication on QMA(2)

Hardness applies to QMA(2)

- Our explicit hard instance M_{acc} is from a QMA(2) instance.
- de Finetti theorem of 1-LOCC [BCY, BH]: best possible parameters.

Unconditional proof of Watrous's dis-entangler conjecture

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

Implication on QMA(2)

Hardness applies to QMA(2)

- Our explicit hard instance M_{acc} is from a QMA(2) instance.
- de Finetti theorem of 1-LOCC [BCY, BH]: best possible parameters.

Unconditional proof of Watrous's dis-entangler conjecture

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

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 $\pi : S \times T \to [0, 1]$.
- 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 $\pi : S \times T \to [0, 1]$.
- 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 $\pi : S \times T \to [0, 1]$.
- 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 $\pi : S \times T \to [0, 1]$.
- 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 $\{A_s^a\}$ and $\{B_t^b\}$,

$$P[a,b|s,t] = \langle\psi| A_s^a \otimes B_t^b |\psi\rangle .$$

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 $\{A_s^a\}$ and $\{B_t^b\}$,

$$P[a, b|s, t] = \langle\psi| A_s^a \otimes B_t^b |\psi\rangle .$$

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 $a \oplus b = s \wedge t$.
- **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)

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

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 $a \oplus b = s \wedge t$.
- **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)

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

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 $a \oplus b = s \wedge t$.
- **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)

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

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 $a \oplus b = s \wedge t$.
- **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)

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

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 $a \oplus b = s \wedge t$.
- **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)

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

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 $a \oplus b = s \wedge t$.
- **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?

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!

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

- $\omega^*(G)$ 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.

Computational Hardness

reference	k	c	s	n
KK+11	3	1	$1-\frac{1}{\text{poly}(Q)}$	$O(Q)$
IKM09	2	1	$1-\frac{1}{\text{poly}(Q)}$	$O(Q)$
IV12	4	1	$2^{-Q^{\Omega(1)}}$	$Q^{\Omega(1)}$
Vid13	3	1	$2^{-Q^{\Omega(1)}}$	$Q^{\Omega(1)}$

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 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].

Technical Outline & Contributions

Technical Target

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

Technical Contributions

- Formulate a framework of reductions for this purpose. Other applications, e.g., Nash's equilibria [HNW16].
- Design low-degree reductions in this 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, pattern matrices, and non-commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Other applications, e.g., Nash's equilibria [HNW16].
- Design low-degree reductions in this 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, pattern matrices, and non-commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Other applications, e.g., Nash's equilibria [HNW16].
- Design low-degree reductions in this 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, pattern matrices, and non-commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Other applications, e.g., Nash's equilibria [HNW16].
- Design low-degree reductions in this 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, pattern matrices, and non-commutative problems.

Technical Contributions

- Formulate a framework of reductions for this purpose. Other applications, e.g., Nash's equilibria [HNW16].
- Design low-degree reductions in this framework.
- Special techniques to handle general domains and non-commutative problems.

Principle of Sum-of-Squares

One way to show that a polynomial $f(x)$ is *nonnegative* could be

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

Example

$$\begin{aligned} f(x) &= 2x^2 - 6x + 5 \\ &= (x^2 - 2x + 1) + (x^2 - 4x + 4) \\ &= (x-1)^2 + (x-2)^2 \geq 0. \end{aligned}$$

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

Principle of SoS : constrained domain

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!

Principle of SoS : constrained domain

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!

Principle of SoS : constrained domain

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!

SoS in Optimization

$$\begin{aligned} \max \quad & f(x) \\ \text{subject to} \quad & g_i(x) = 0 \quad \forall i \end{aligned} \tag{2}$$

is equivalent to (justified by *Positivstellensatz*)

$$\begin{aligned} \min \quad & \nu \\ \text{such that} \quad & \nu - f(x) = \sigma(x) + \sum_i b_i(x) g_i(x), \end{aligned} \tag{3}$$

where $\sigma(x)$ is SOS and $b_i(x)$ is any polynomial.

Pseudo-distribution

Dual of the SOS cone

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

Pseudo-distributrion/expectation

- Moment $M_D(x)$ gives rise to *pseudo-distribution*. Expectation on it is *pseudo-expectation*.
- Behave similarly to expectation for low-degree polynomials.

Pseudo-distribution

Dual of the SOS cone

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

Pseudo-distributrion/expectation

- Moment $M_D(x)$ gives rise to *pseudo-distribution*. Expectation on it is *pseudo-expectation*.
- Behave similarly to expectation for low-degree polynomials.

Pseudo-expectation

A degree-$2d$ pseudo-expectation $\tilde{\mathbb{E}}$ is an element of $\mathcal{R}[x]_{2d}^*$ (i.e. a linear map from $\mathcal{R}[x]_{2d}$ to $\mathcal{R}$) satisfying

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

$\tilde{\mathbb{E}}$ satisfies the constraints $g_1, \ldots, g_m$ if $\tilde{\mathbb{E}}[g_i q] = 0$ for all $i \in [n]$ and all $q \in \mathcal{R}[x]_{2d-\deg(g_i)}$.

$$f_{\mathrm{SoS}}^{2d} = \max\{\tilde{\mathbb{E}}[f] : \tilde{\mathbb{E}} \text{ of degree-}2d \text{ satisfying } g_1, \ldots, g_m\}. \quad (4)$$

Pseudo-expectation

A degree-$2d$ pseudo-expectation $\tilde{\mathbb{E}}$ is an element of $\mathcal{R}[x]^*_{2d}$ (i.e. a linear map from $\mathcal{R}[x]_{2d}$ to $\mathcal{R}$) satisfying

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

$\tilde{\mathbb{E}}$ satisfies the constraints $g_1, \dots, g_m$ if $\tilde{\mathbb{E}}[g_i q] = 0$ for all $i \in [n]$ and all $q \in \mathcal{R}[x]_{2d-\deg(g_i)}$.

$$f^{2d}_{\text{SoS}} = \max\{\tilde{\mathbb{E}}[f] : \tilde{\mathbb{E}} \text{ of degree-}2d \text{ satisfying } g_1, \dots, g_m\}. \quad (4)$$

Pseudo-expectation

A degree-$2d$ pseudo-expectation $\tilde{\mathbb{E}}$ is an element of $\mathcal{R}[x]_{2d}^*$ (i.e. a linear map from $\mathcal{R}[x]_{2d}$ to $\mathcal{R}$) satisfying

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

$\tilde{\mathbb{E}}$ satisfies the constraints $g_1, \ldots, g_m$ if $\tilde{\mathbb{E}}[g_i q] = 0$ for all $i \in [n]$ and all $q \in \mathcal{R}[x]_{2d-\deg(g_i)}$.

$$f_{\text{SoS}}^{2d} = \max\{\tilde{\mathbb{E}}[f] : \tilde{\mathbb{E}} \text{ of degree-}2d \text{ satisfying } g_1, \ldots, g_m\}. \quad (4)$$

SoS relaxation: (Dual) Lasserre/Parrilo Hierarchy

- By bounding the degrees in (4), we get the (dual) Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

$$\begin{aligned} \max \quad & \tilde{\mathbb{E}}[f] \\ \text{such that} \quad & \tilde{\mathbb{E}}[g_i q] = 0, \quad \forall i \in [n], q \in \mathcal{R}[x]_{2d-\deg(g_i)}, \end{aligned} \tag{5}$$

where $\tilde{\mathbb{E}}[f]$ is a degree $2d$ pseudo-distribution.

Remark: degree $2d$ pseudo-distributions $\tilde{\mathbb{E}}[f]$ can be efficiently searched by SDP of size of $O(n^d)$.

SoS relaxation: (Dual) Lasserre/Parrilo Hierarchy

- By bounding the degrees in (4), we get the (dual) Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

$$\begin{aligned} \max \quad & \tilde{\mathbb{E}}[f] \\ \text{such that} \quad & \tilde{\mathbb{E}}[g_i q] = 0, \quad \forall i \in [n], q \in \mathcal{R}[x]_{2d-\deg(g_i)}, \end{aligned} \tag{5}$$

where $\tilde{\mathbb{E}}[f]$ is a degree $2d$ pseudo-distribution.

Remark: degree $2d$ pseudo-distributions $\tilde{\mathbb{E}}[f]$ can be efficiently searched by SDP of size of $O(n^d)$.

SoS relaxation: (Dual) Lasserre/Parrilo Hierarchy

- By bounding the degrees in (4), we get the (dual) Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

$$\begin{aligned} \max \quad & \tilde{\mathbb{E}}[f] \\ \text{such that} \quad & \tilde{\mathbb{E}}[g_i q] = 0, \quad \forall i \in [n], q \in \mathcal{R}[x]_{2d-\deg(g_i)}, \end{aligned} \tag{5}$$

where $\tilde{\mathbb{E}}[f]$ is a degree $2d$ pseudo-distribution.

Remark: degree $2d$ pseudo-distributions $\tilde{\mathbb{E}}[f]$ can be efficiently searched by SDP of size of $O(n^d)$.

SoS relaxation: (Dual) Lasserre/Parrilo Hierarchy

- By bounding the degrees in (4), we get the (dual) Lasserre/Parrilo hierarchy, which is a SDP hierarchy.

$$\begin{aligned} \max \quad & \tilde{\mathbb{E}}[f] \\ \text{such that} \quad & \tilde{\mathbb{E}}[g_i q] = 0, \quad \forall i \in [n], q \in \mathcal{R}[x]_{2d-\deg(g_i)}, \end{aligned} \tag{5}$$

where $\tilde{\mathbb{E}}[f]$ is a degree $2d$ pseudo-distribution.

Remark: degree $2d$ pseudo-distributions $\tilde{\mathbb{E}}[f]$ can be efficiently searched by SDP of size of $O(n^d)$.

Recall $h_{\mathrm{Sep}(d,d)}(M)$

$$h_{\mathrm{Sep}(d,d)}(M) := \max_{\substack{x,y\in\mathbb{C}^d \\ \|x\|_2=\|y\|_2=1}} \sum_{i,j,k,l\in[d]} M_{ij,kl} x_i^* x_j y_k^* y_l. \tag{6}$$

Its SOS hierarchy is the DPS hierarchy with full symmetry.

$$\rho \propto \sum_{\substack{i_1 i_2 \ldots i_d \\ j_1 j_2 \ldots j_d}} \tilde{\mathbb{E}}_x[x_{i_1} \ldots x_{i_d} x_{j_1} \ldots x_{j_d}] \, |i_1 \ldots i_d\rangle \langle j_1 \ldots j_d| \, .$$

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^x, s.t. $f(x) = F(X^x)$. Embedding!
- Subtleties: $\{0,1\}^n$, embedding, problem structure.

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^x, s.t. $f(x) = F(X^x)$. Embedding!
- Subtleties: $\{0,1\}^n$, embedding, problem structure.

General SDPs

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

Lee-Raghavendra-Steurer

- Any $\deg_{\mathrm{sos}}$ 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!**
- Subtleties: $\{0,1\}^n$, embedding, problem structure.

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!**
- Subtleties: $\{0,1\}^n$, embedding, problem structure.

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!**
- Subtleties: $\{0,1\}^n$, embedding, problem structure.

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!**
- Subtleties: $\{0,1\}^n$, embedding, problem structure.

Integrality Gaps

What constitutes an integrality gap?

- An instance Φ that has $f_{\mathrm{opt}}(\Phi)$ is small.
- But $f^{d}_{\mathrm{SoS}}(\Phi)$ 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.

Integrality Gaps

What constitutes an integrality gap?

- An instance Φ that has $f_{\mathrm{opt}}(\Phi)$ is small.
- But $f^{d}_{\mathrm{SoS}}(\Phi)$ 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 $\Phi^A \to \Phi^B$.
- **Soundness**: $f^A_{\text{opt}}(\Phi^A)$ small $\Rightarrow f^B_{\text{opt}}(\Phi^B)$
- **Pseudo-completeness**: $f^{d_A}_{\text{SoS}}(\Phi^A)$ large $\Rightarrow f^{d_B}_{\text{SoS}}(\Phi^B)$ large, d_B is not too smaller than d_A.

Pseudo-completeness: low-degree reduction

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

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 $\mu_A(\tilde{\mathbb{E}}_A)$ be the pseudo-solution for Φ^A. One needs to construct a $\mu_B(\tilde{\mathbb{E}}_B)$ for Φ^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 $\Phi^A \to \Phi^B$.
- **Soundness**: $f^A_{\text{opt}}(\Phi^A)$ small $\Rightarrow$ $f^B_{\text{opt}}(\Phi^B)$
- **Pseudo-completeness**: $f^{d_A}_{\text{SoS}}(\Phi^A)$ large $\Rightarrow$ $f^{d_B}_{\text{SoS}}(\Phi^B)$ large, d_B is not too smaller than d_A.

Pseudo-completeness: low-degree reduction

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

Extend integrality gaps via reductions

Reduction from A to B

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

Pseudo-completeness: low-degree reduction

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

Extend integrality gaps via reductions

Reduction from A to B

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

Pseudo-completeness: low-degree reduction

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

Extend integrality gaps via reductions

Reduction from A to B

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

Pseudo-completeness: low-degree reduction

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

More on the low-degree reduction

Lemma

Let $A \subset \mathbb{R}^n, B \subset \mathbb{R}^m$ be algebraic varieties, meaning that

$$\begin{aligned} A &= \{x \in \mathbb{R}^n : g_1(x) = \cdots = g_{n'}(x) = 0\} \\ B &= \{x \in \mathbb{R}^m : h_1(x) = \cdots = h_{m'}(x) = 0\}, \end{aligned}$$

for some polynomials $\{g_i\}, \{h_i\}$.
Suppose that p is a degree-d polynomial map from $\mathcal{R}^n \to \mathcal{R}^m$ such that $p(A) \subseteq B$.
Let $\tilde{\mathbb{E}}_A \in \mathbb{R}[x_1, \ldots, x_n]_\ell^*$ be a degree-ℓ pseudo-expectation (compatible with the constraints $g_1, \ldots, g_{n'}$) $\Rightarrow$ a degree-ℓ/d pseudo-expectation $\tilde{\mathbb{E}}_B \in \mathbb{R}[y_1, \ldots, y_m]_{\ell/d}{}^*$ (compatible with the constraints $h_1, \ldots, h_{m'}$).

Extend integrality gaps via reductions:

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

SDP lower bounds (LRS)

- Only apply to $\{0, 1\}^n \Rightarrow$ no direct application on h_{Sep} or $\omega^*(G)$.
- Additional condition: embedding, "self-symmetry"

Extend integrality gaps via reductions:

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

SDP lower bounds (LRS)

- Only apply to $\{0,1\}^n \Rightarrow$ no direct application on h_{Sep} or $\omega^*(G)$.
- Additional condition: embedding, ”self-symmetry”
  - 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 tricky condition on the structure of the problem.

Extend integrality gaps via reductions:

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

SDP lower bounds (LRS)

- Only apply to $\{0,1\}^n \Rightarrow$ no direct application on h_{Sep} or $\omega^*(G)$.
- Additional condition: embedding, ”self-symmetry”
  - 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 tricky condition on the structure of the problem.

Extend integrality gaps via reductions:

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

SDP lower bounds (LRS)

- Only apply to $\{0,1\}^n \Rightarrow$ no direct application on h_{Sep} or $\omega^*(G)$.
- Additional condition: embedding, "self-symmetry"
  - 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 tricky condition on the structure of the problem.

Extend integrality gaps via reductions:

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

SDP lower bounds (LRS)

- Only apply to $\{0,1\}^n \Rightarrow$ no direct application on h_{Sep} or $\omega^*(G)$.
- Additional condition: embedding, ”self-symmetry”
  - 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 tricky condition on the structure of the problem.

Extend integrality gaps via reductions:

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

SDP lower bounds (LRS)

- Only apply to $\{0,1\}^n \Rightarrow$ no direct application on h_{Sep} or $\omega^*(G)$.
- Additional condition: embedding, ”self-symmetry”
  - 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 tricky condition on the structure of the problem.

A typical reduction

$$3\text{XOR} \underset{R_1}{\Longrightarrow} \cdots \underset{R_2}{\Longrightarrow} A \text{ over } \{0,1\}^n \underset{R_3}{\Longrightarrow} \cdots \underset{R_4}{\Longrightarrow} \text{Final Problem}$$

- 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

$$3\text{XOR} \underset{R_1}{\Longrightarrow} \cdots \underset{R_2}{\Longrightarrow} A \text{ over } \{0,1\}^n \underset{R_3}{\Longrightarrow} \cdots \underset{R_4}{\Longrightarrow} \text{Final Problem}$$

- 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

$$\text{3XOR} \underset{R_1}{\Longrightarrow} \cdots \underset{R_2}{\Longrightarrow} A \text{ over } \{0,1\}^n \underset{R_3}{\Longrightarrow} \cdots \underset{R_4}{\Longrightarrow} \text{Final Problem}$$

- 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

$$3\text{XOR} \underset{R_1}{\Longrightarrow} \cdots \underset{R_2}{\Longrightarrow} A \text{ over } \{0,1\}^n \underset{R_3}{\Longrightarrow} \cdots \underset{R_4}{\Longrightarrow} \text{Final Problem}$$

- 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.

Real reductions for h_{Sep} and $\omega^*(G)$

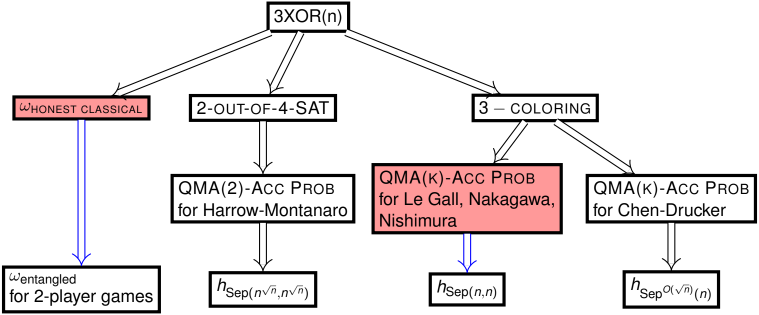


Figure: All our results are derived from the integrality gaps of 3XOR. **Red nodes**: problems over the boolean cube and LRS is applied. **Blue arrows** are "embedding reductions".

Reduction for h_{Sep} : Inspired by Aaronson et al.

$$3SAT \underset{R_1}{\Longrightarrow} \text{2-OUT-OF-4-SAT} \underset{R_2}{\Longrightarrow} \text{QMA(2)-ACC PROB} \underset{R_3}{\Longrightarrow} h_{\text{Sep}}$$

- R_1: a classical step done by PCP. Not a low-degree reduction :(!
- R_2: a quantum step. Tests in the QMA(2) protocol refer to low-degree polynomials of entries of quantum proofs. Soundness inhered from the above protocol.
- R_3: embedding by construction. Not always satisfy the "self-symmetry" condition.

Reduction for h_{Sep} : Inspired by Aaronson et al.

$$3SAT \underset{R_1}{\Longrightarrow} \text{2-OUT-OF-4-SAT} \underset{R_2}{\Longrightarrow} \text{QMA(2)-ACC PROB} \underset{R_3}{\Longrightarrow} h_{\text{Sep}}$$

- R_1: a classical step done by PCP. Not a low-degree reduction :(!
- R_2: a quantum step. Tests in the QMA(2) protocol refer to low-degree polynomials of entries of quantum proofs. Soundness inhered from the above protocol.
- R_3: embedding by construction. Not always satisfy the "self-symmetry" condition.

Reduction for h_{Sep} : Inspired by Aaronson et al.

$$3SAT \underset{R_1}{\Longrightarrow} \text{2-OUT-OF-4-SAT} \underset{R_2}{\Longrightarrow} \text{QMA(2)-ACC PROB} \underset{R_3}{\Longrightarrow} h_{\mathrm{Sep}}$$

- R_1: a classical step done by PCP. Not a low-degree reduction :(!
- R_2: a quantum step. Tests in the QMA(2) protocol refer to low-degree polynomials of entries of quantum proofs. Soundness inhered from the above protocol.
- R_3: embedding by construction. Not always satisfy the "self-symmetry" condition.

Reduction for h_{Sep}: SOS lower bounds

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

- Start with the 3XOR integrity gap (true value $\frac{1}{2} + \epsilon$, fools $\Omega(n)$-degree).
- R_1: a classical step. Replacing 3SAT by 3XOR. Achieve PCP's effect by using some steps in Dinur's PCP proof.
- R_2: a quantum step. 2-OUT-OF-4-SAT-EQ replaces 2-OUT-OF-4-SAT. Slightly change QMA(2) protocol.
- A constant integrity gap: $\Omega(\sqrt{n})$-degree pseudo-distribution over proofs of dimension $d = n^{\sqrt{n}}$. That is $\tilde{\Omega}(\log(d))$.

Reduction for h_{Sep}: SOS lower bounds

3XOR $\underset{R_1}{\Longrightarrow}$ 2-OUT-OF-4-SAT-EQ $\underset{R_2}{\Longrightarrow}$ QMA(2)-ACC PROB $\underset{R_3}{\Longrightarrow}$ h_{Sep}

- Start with the 3XOR integrity gap (true value $\frac{1}{2} + \epsilon$, fools $\Omega(n)$-degree).
- R_1: a classical step. Replacing 3SAT by 3XOR. Achieve PCP's effect by using some steps in Dinur's PCP proof.
- R_2: a quantum step. 2-OUT-OF-4-SAT-EQ replaces 2-OUT-OF-4-SAT. Slightly change QMA(2) protocol.
- A constant integrity gap: $\Omega(\sqrt{n})$-degree pseudo-distribution over proofs of dimension $d = n^{\sqrt{n}}$. That is $\tilde{\Omega}(\log(d))$.

Reduction for h_{Sep}: SOS lower bounds

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

- Start with the 3XOR integrity gap (true value $\frac{1}{2} + \epsilon$, fools $\Omega(n)$-degree).
- R_1: a classical step. Replacing 3SAT by 3XOR. Achieve PCP's effect by using some steps in Dinur's PCP proof.
- R_2: a quantum step. 2-OUT-OF-4-SAT-EQ replaces 2-OUT-OF-4-SAT. Slightly change QMA(2) protocol.
- A constant integrity gap: $\Omega(\sqrt{n})$-degree pseudo-distribution over proofs of dimension $d = n^{\sqrt{n}}$. That is $\tilde{\Omega}(\log(d))$.

Reduction for h_{Sep}: SOS lower bounds

$$3\text{XOR} \underset{R_1}{\Longrightarrow} 2\text{-OUT-OF-4-SAT-EQ} \underset{R_2}{\Longrightarrow} \text{QMA(2)-ACC PROB} \underset{R_3}{\Longrightarrow} h_{\mathrm{Sep}}$$

- Start with the 3XOR integrity gap (true value $\frac{1}{2} + \epsilon$, fools $\Omega(n)$-degree).
- R_1: a classical step. Replacing 3SAT by 3XOR. Achieve PCP's effect by using some steps in Dinur's PCP proof.
- R_2: a quantum step. 2-OUT-OF-4-SAT-EQ replaces 2-OUT-OF-4-SAT. Slightly change QMA(2) protocol.
- A constant integrity gap: $\Omega(\sqrt{n})$-degree pseudo-distribution over proofs of dimension $d = n^{\sqrt{n}}$. That is $\tilde{\Omega}(\log(d))$.

SDP lower bound: the tricky condition

LRS core technical object: the pattern matrix

$$M_f^n : [n]^m \times \{0,1\}^n \mapsto \mathbb{R}_{\geq 0}, M_f^n(S,x) = c - f(x_S).$$

Lemma (Theorem 3.8 of LRS)

Suppose Φ is an instance of an optimization problem over m variables, and $\deg_{\mathrm{SoS}}(c - f_\Phi(x)) \geq d$. Then for $n \geq m^{d/4}$, $\mathrm{rk}_{\mathrm{psd}}(M_f^n) \geq \Omega(m^{d^2/8})$.

Make M_f^n a sub-matrix of the slack-matrix of your optimization problem. The tricky condition.

Real reductions for h_{Sep} and $\omega^*(G)$

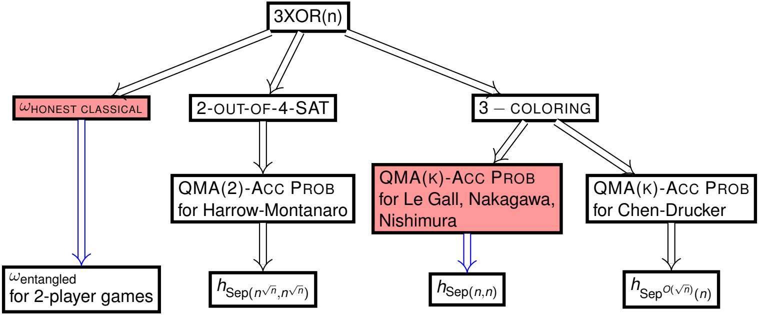


Figure: All our results are derived from the integrality gaps of 3XOR. **Red nodes**: problems over the boolean cube and LRS is applied. **Blue arrows** are "embedding reductions".

Summary

Results

- First unconditional SoS/SDP lower bounds for h_{Sep} and $\omega^*(G)$.
- Match ETH-based bounds for h_{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.

Summary

Results

- First unconditional SoS/SDP lower bounds for h_{Sep} and $\omega^*(G)$.
- Match ETH-based bounds for h_{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 general SDPs.
- Prove stronger SoS lower bounds than ETH bounds.
- Prove hardness for 1-LOCC instances or so.
- Consider general convex programming for h_{Sep}.
- Other applications of the techniques here.

Open Questions

- Prove stronger hardness for general SDPs.
- Prove stronger SoS lower bounds than ETH bounds.
- Prove hardness for 1-LOCC instances or so.
- Consider general convex programming for h_{Sep}.
- Other applications of the techniques here.

Open Questions

- Prove stronger hardness for general SDPs.
- Prove stronger SoS lower bounds than ETH bounds.
- Prove hardness for 1-LOCC instances or so.
- Consider general convex programming for h_{Sep}.
- Other applications of the techniques here.

Open Questions

- Prove stronger hardness for general SDPs.
- Prove stronger SoS lower bounds than ETH bounds.
- Prove hardness for 1-LOCC instances or so.
- Consider general convex programming for h_{Sep}.
- Other applications of the techniques here.

Open Questions

- Prove stronger hardness for general SDPs.
- Prove stronger SoS lower bounds than ETH bounds.
- Prove hardness for 1-LOCC instances or so.
- Consider general convex programming for h_{Sep}.
- Other applications of the techniques here.

Question And Answer

Thank you!

Q & A

SoS relaxation: Lasserre/Parrilo Hierarchy

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

$$\begin{aligned} \min \quad & \nu \\ \text{such that} \quad & \nu - f(x) = \sigma(x) + \sum_i b_i(x) g_i(x), \end{aligned} \tag{7}$$

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 $\deg_{\rm sos}(v - f)$), then problem (3) is equivalent to problem (2).
- By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

$$\begin{aligned} \min \quad & \nu \\ \text{such that} \quad & \nu - f(x) = \sigma(x) + \sum_i b_i(x) g_i(x), \end{aligned} \tag{7}$$

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 $\deg_{\text{sos}}(v - f)$), then problem (3) is equivalent to problem (2).
- By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

$$\begin{aligned} &\min && \nu \\ &\text{such that} && \nu - f(x) = \sigma(x) + \sum_i b_i(x) g_i(x), \end{aligned} \tag{7}$$

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 $\deg_{\text{sos}}(v - f)$), then problem (3) is equivalent to problem (2).
- By bounding the degrees, we get the Lasserre/Parrilo hierarchy.

$$\begin{aligned} \text{min} \quad & \nu \\ \text{such that} \quad & \nu - f(x) = \sigma(x) + \sum_i b_i(x) g_i(x), \end{aligned} \tag{7}$$

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

$$\begin{aligned} \min_{\nu, b_{i\alpha} \in \mathbb{R}} \quad & \nu \\ \text{such that} \quad & \nu A_0 - F - \sum_{i\alpha} b_{i\alpha} G_{i\alpha} \geq 0. \end{aligned} \tag{8}$$

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

Why it is a SDP?

Observation

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

$$\begin{aligned} \min_{\nu, b_{i\alpha} \in \mathbb{R}} \quad & \nu \\ \text{such that} \quad & \nu A_0 - F - \sum_{i\alpha} b_{i\alpha} G_{i\alpha} \geq 0. \end{aligned} \tag{8}$$

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

Why it is a SDP?

Observation

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

$$\begin{aligned} \min_{\nu, b_{i\alpha} \in \mathbb{R}} \quad & \nu \\ \text{such that} \quad & \nu A_0 - F - \sum_{i\alpha} b_{i\alpha} G_{i\alpha} \geq 0. \end{aligned} \tag{8}$$

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