A Survey on the Complexity of Entangled Provers

Zhengfeng Ji, IQC, U. Waterloo

What we will NOT cover

- Quantum verifier and messages
- Non-signalling provers
- Bell violations
- Parallel repetition theorems
- Unentangled provers
- \bullet … … …

Background

- Interactive proof systems and the PCP theorem [GMR '89] [Bab '85] [BOGKW '88] [BFL '91] randomness [FGL+ '96] [AS '98] [ALM+ '96]
- Entanglement and non-locality [EPR '35] [Bell '64]
- Two origins combined [CHTW'04]
	- All powerful provers
	- A CS approach to non-locality

interaction +

Problem setting and notions

• Strategy $(\rho, \{A_s^a\}, \{B_t^b\})$ $p(a,b|s,t) = \text{Tr}_{\rho}(A_s^a \otimes B_t^b)$ $\stackrel{\rm def}{=} \text{Tr}(A^a_s \otimes B^b_t \rho)$ Question in subscript, answer in superscript

Game values

$$
\omega^* = \sup_{\rho, A_s^a, B_t^b} \mathbb{E}_{s,t} \sum_{a,b} V(a,b|s,t) \text{Tr}_{\rho}(A_s^a \otimes B_t^b)
$$

$$
\omega^f = \sup_{\rho, A_s^a, B_t^b} \mathbb{E}_{s,t} \sum_{a,b} V(a,b|s,t) \text{Tr}_{\rho}(A_s^a B_t^b)
$$

$$
[A_s^a, B_t^b] = 0
$$

Problem setting and notions

• Strategy $(\rho, \{A_s^a\}, \{B_t^b\})$ $p(a,b|s,t) = \text{Tr}_{\rho}(A_s^a \otimes B_t^b)$ $\stackrel{\rm def}{=} \text{Tr}(A^a_s \otimes B^b_t \rho)$ Question in subscript, answer in superscript

- Symmetry assumption
- ρ -norm $||A||_\rho =$ $\overline{}$ $\text{Tr}_\rho(AA^\ast)$
- Measurement strategy replacement

Example I: Mermin-Peres magic square game

- Sample and send constraint-variable pair
- Check
	- Constraint
	- Consistency
- Magic: $1 = \omega^* > \omega$, 2 EPR pairs
- Binary constraint system games [CM '12]
- An instance of 3-SAT with 24 clauses

Example 2: Quantum 3-coloring game

- Sample and send vertices u, v to A and B respectively
- Check
	- $a = b$ if $u = v$, and
	- $a \neq b$ if *u*, *v* are adjacent
- \exists graph *G*, $1 = \omega^*(G) > \omega(G)$
- 3-COLORING*
- Entanglement undermines soundness
- A bug or a feature?

Entanglement undermines soundness

• Two-player XOR games

 \oplus MIP*(2,1) \subseteq EXP Tsirelson's theorem: $\langle \phi | X_s \otimes Y_t | \phi \rangle = x_s \cdot y_t$ ⊕MIP*(2,1) ⊆ QIP(2) ⊆ PSPACE [CHTW '04] [Weh '06] [JUW '09] $\oplus \text{MIP}$ (2, 1) = NEXP [Hås '01]

- Unique Games with Entangled Provers are Easy [KRT '08] "Quantum rounding" of SDP from UGC
- Unfixable bug…

Entanglement resistant techniques

- Consistency check
- Confusion check
- A third player
	- Bob'
	- 2-out-of-3
- PIR, $NP \subseteq \bigoplus MP^*(2)$ [CGJ'09]

Consistency check

- Send each player the same question *q* and expect the same answers
- 2-player consistency check
	- Quantum 3-coloring game
- 3-player consistency check
	- Linearity test and multilinearity test [IV '12]
	- PCP simulation test [IKP+ '08]

Consistency as a measure of "closeness"

• For two measurements A and B, define

$$
CONS(A, B) = \sum_{a} \text{Tr}_{\rho}(A^{a} \otimes B^{a})
$$

$$
INC(A, B) = 1 - CONS(A, B)
$$

• Inconsistency as a "distance" of measurements

$$
\sum_{a} \|A^a - B^a\|_{\rho}^2 \le O(\sqrt{\text{INC}(A, B)})
$$

Confusion check

- Sample two questions *q*, *q'*. Send the unordered pair *q*, *q'* to *A* and *q* to *B*
- Used to prove NP-hardness of computing ω^* to inverse polynomial precision [IKM '09]
- Lemma $CONF(A, B) = \sum \text{Tr}_{\rho}(A_{q,q'}^{a,a'} \otimes B_q^a)$ a,a'

$$
\text{CONF}(A, B) \ge 1 - \epsilon \implies \mathbb{E}_{q, q'} \sum_{a, a'} \left\| [B_q^a, B_{q'}^{a'}] \right\|_{\rho}^2 \le O(\epsilon)
$$

A third player

- Monogamy of entanglement
- Bob' construction

- NP-hardness of 3-player games [KKM+ '08]
- Effect on the magic square game
- 2-out-of-3
	- Used with low degree test in [Vid '13]

NP-hardness of exact computation of ω^*

- It is NP-hard to distinguish
	- $\omega^* = 1$ and

- $ω^*$ ≤ 1 $O(1/n^c)$ [KKM+ '08] [IKM '09]
- State invariant lemma with Bob'

$$
\left\| \sum_{a} \sqrt{B_q^a} \rho_{AB} \sqrt{B_q^a} - \rho_{AB} \right\|_1 = O(\sqrt{\text{INC}(B_q)})
$$

- Sequential measurement rounding
- Bad soundness

$MIP = NEXP \subseteq MIP^*$ [IV '12]

- Entangled provers are at least as expressive as their classical counterpart
- Any MIP protocol can be modified immune to entanglement
- Bug fixed for once and for all
- The best one can hope for using the entanglement resistant techniques

What to prove?

- Follows the proof of NEXP ⊆ MIP of [BFL'91]
- Multilinearity test is sound against entangled provers
	- Consistency test
	- Multilinearity test (axis aligned linearity test)
- Classically: provers act according to a common multilinear function

What to prove?

• What is the right thing to prove in the quantum setting?

 $1 - \epsilon$, then there exists POVM $\{V^g\}$ such that Theorem. Suppose that the strategy passes both the consistency test and multilinearity test with probability

$$
\mathbb{E}_{\boldsymbol{x}}\Big[\text{INC}(A_{\boldsymbol{x}},V_{\boldsymbol{x}})\Big] = O(\epsilon^c),
$$

where $V_x^a = \sum V^g$. $\overline{g:g}(\overline{\boldsymbol{x}})=a$

Proof outline

- Remove the dependence on *xi* one by one by induction
- Error (in terms of inconsistency) grows exponentially. Need an (active) consolidation step using SDPs
- Pasting lemma + consolidation (self-improvement) lemma
- The base step of the induction

The base step

• The statement $\boldsymbol{x} \in \mathbb{F}^n \quad \boldsymbol{x}' = x'_i, \boldsymbol{x}_{\neg i}$

$$
\begin{aligned}\n\exists \quad & \{B_{\boldsymbol{x}_{-i}}^l\} \quad B_{\boldsymbol{x}}^a = \sum_{l:l(x_i)=a} B_{\boldsymbol{x}_{-i}}^l \\
\mathbb{E}_{\boldsymbol{x}}\left[\text{INC}(A_{\boldsymbol{x}}, B_{\boldsymbol{x}})\right] & \leq O(\sqrt{\epsilon})\n\end{aligned}
$$

• Construction of the *B* measurement

$$
B_{\boldsymbol{x}_{\neg i}}^{l} \stackrel{\text{def}}{=} \mathbb{E}_{x_i \neq x'_i} A_{\boldsymbol{x}}^{l(x_i)} A_{\boldsymbol{x}'}^{l(x'_i)} A_{\boldsymbol{x}}^{l(x_i)}
$$

$$
\mathbb{E}_{\boldsymbol{x}}\Big[\text{CONS}(A_{\boldsymbol{x}},B_{\boldsymbol{x}})\Big] \n= \mathbb{E}_{\boldsymbol{x},x'_{i}\neq x''_{i}} \sum_{a,l:l(x_{i})=a} \sum_{a'} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^{a} \otimes A_{\boldsymbol{x}'}^{l(x'_{i})} A_{\boldsymbol{x}''}^{l(x''_{i})} A_{\boldsymbol{x}'}^{l(x'_{i})} \otimes A_{\boldsymbol{x}'}^{a'}) \n\approx \mathbb{E}_{x,x'_{i}\neq x''_{i}} \sum_{a,l:l(x_{i})=a} \text{Tr}_{\rho}(A_{x}^{a} \otimes A_{x'}^{l(x'_{i})} A_{x''}^{l(x'_{i})} A_{x'}^{l(x'_{i})} \otimes A_{x'}^{l(x'_{i})}) \n\approx \sqrt{\epsilon} \mathbb{E}_{x,x'_{i}\neq x''_{i}} \sum_{a,l:l(x_{i})=a} \text{Tr}_{\rho}(A_{x}^{a} \otimes A_{x''}^{l(x''_{i})} \otimes A_{x'}^{l(x'_{i})}) \n\approx \epsilon \mathbb{E}_{x,x'_{i},x''_{i}} \sum_{l} \text{Tr}_{\rho}(A_{x}^{l(x_{i})} \otimes A_{x''}^{l(x''_{i})} \otimes A_{x'}^{l(x'_{i})}) \n= 1 - O(\sqrt{\epsilon})
$$

$$
\mathbb{E}_{\boldsymbol{x}}\Big[\text{CONS}(A_{\boldsymbol{x}},B_{\boldsymbol{x}})\Big] \n= \mathbb{E}_{\boldsymbol{x},x'_i \neq x''_i} \sum_{a,l:l(x_i)=a} \sum_{a'} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^a \otimes A_{\boldsymbol{x}'}^{l(x'_i)} A_{\boldsymbol{x}''}^{l(x''_i)} A_{\boldsymbol{x}'}^{l(x'_i)} \otimes A_{\boldsymbol{x}'}^{a'}) \n\approx_{\epsilon} \mathbb{E}_{\boldsymbol{x},x'_i \neq x''_i} \sum_{a,l:l(x_i)=a} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^a \otimes A_{\boldsymbol{x}'}^{l(x'_i)} A_{\boldsymbol{x}''}^{l(x'_i)} A_{\boldsymbol{x}'}^{l(x'_i)} \otimes A_{\boldsymbol{x}'}^{l(x'_i)}) \n\approx_{\sqrt{\epsilon}} \mathbb{E}_{\boldsymbol{x},x'_i \neq x''_i} \sum_{a,l:l(x_i)=a} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^a \otimes A_{\boldsymbol{x}''}^{l(x''_i)} \otimes A_{\boldsymbol{x}'}^{l(x'_i)}) \n\approx_{\epsilon} \mathbb{E}_{\boldsymbol{x},x'_i,x''_i} \sum_{l} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^{l(x_i)} \otimes A_{\boldsymbol{x}''}^{l(x''_i)} \otimes A_{\boldsymbol{x}'}^{l(x'_i)}) \n= 1 - O(\sqrt{\epsilon})
$$

$$
\mathbb{E}_{\boldsymbol{x}}\Big[\text{CONS}(A_{\boldsymbol{x}}, B_{\boldsymbol{x}})\Big] \n= \mathbb{E}_{\boldsymbol{x}, x'_i \neq x''_i} \sum_{a, l: l(x_i) = a} \sum_{a'} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^a \otimes A_{\boldsymbol{x}'}^{l(x'_i)} A_{\boldsymbol{x}''}^{l(x'_i)} A_{\boldsymbol{x}'}^{l(x'_i)} \otimes A_{\boldsymbol{x}'}^{a'_i}) \n\approx_{\epsilon} \mathbb{E}_{\boldsymbol{x}, x'_i \neq x''_i} \sum_{a, l: l(x_i) = a} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^a \otimes A_{\boldsymbol{x}'}^{l(x'_i)} A_{\boldsymbol{x}''}^{l(x'_i)} A_{\boldsymbol{x}'}^{l(x'_i)} \otimes A_{\boldsymbol{x}'}^{l(x'_i)}) \n\approx_{\sqrt{\epsilon}} \mathbb{E}_{\boldsymbol{x}, x'_i \neq x''_i} \sum_{a, l: l(x_i) = a} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^a \otimes A_{\boldsymbol{x}''}^{l(x''_i)} \otimes A_{\boldsymbol{x}'}^{l(x'_i)}) \n\approx_{\epsilon} \mathbb{E}_{\boldsymbol{x}, x'_i, x''_i} \sum_{l} \text{Tr}_{\rho}(A_{\boldsymbol{x}}^{l(x_l)} \otimes A_{\boldsymbol{x}''}^{l(x''_l)} \otimes A_{\boldsymbol{x}''}^{l(x'_i)}) \n= 1 - \mathcal{O}(\sqrt{\epsilon})
$$

$$
\mathbb{E}_{\mathbf{x}}\left[\text{CONS}(A_{\mathbf{x}},B_{\mathbf{x}})\right]
$$
\n
$$
= \mathbb{E}_{\mathbf{x},x'_{i}\neq x''_{i}} \sum_{a,l:l(x_{i})=a} \sum_{a'} \text{Tr}_{\rho}(A_{\mathbf{x}}^{a} \otimes A_{\mathbf{x}'}^{l(x'_{i})} A_{\mathbf{x}''}^{l(x'_{i})} A_{\mathbf{x}'}^{l(x'_{i})} \otimes A_{\mathbf{x}'}^{a'_{i}})
$$
\n
$$
\approx_{\epsilon} \mathbb{E}_{\mathbf{x},x'_{i}\neq x''_{i}} \sum_{a,l:l(x_{i})=a} \text{Tr}_{\rho}(A_{\mathbf{x}}^{a} \otimes A_{\mathbf{x}'}^{l(x'_{i})} A_{\mathbf{x}''}^{l(x'_{i})} A_{\mathbf{x}'}^{l(x'_{i})} \otimes A_{\mathbf{x}'}^{l(x'_{i})})
$$
\n
$$
\approx_{\sqrt{\epsilon}} \mathbb{E}_{\mathbf{x},x'_{i}\neq x''_{i}} \sum_{a,l:l(x_{i})=a} \text{Tr}_{\rho}(A_{\mathbf{x}}^{a} \otimes A_{\mathbf{x}''}^{l(x''_{i})} \otimes A_{\mathbf{x}'}^{l(x'_{i})})
$$
\n
$$
\approx_{\epsilon} \mathbb{E}_{\mathbf{x},x'_{i},x''_{i}} \sum_{l} \text{Tr}_{\rho}(A_{\mathbf{x}}^{l(x_{i})} \otimes A_{\mathbf{x}''}^{l(x''_{i})} \otimes A_{\mathbf{x}'}^{l(x'_{i})})
$$
\n
$$
= 1 - O(\sqrt{\epsilon})
$$

$$
\mathbb{E}_{\mathbf{x}}\left[\text{CONS}(A_{\mathbf{x}}, B_{\mathbf{x}})\right]
$$
\n
$$
= \mathbb{E}_{\mathbf{x}, x'_i \neq x''_i} \sum_{a, l: l(x_i) = a} \sum_{a'} \text{Tr}_{\rho}(A_{\mathbf{x}}^a \otimes A_{\mathbf{x}'}^{l(x'_i)} A_{\mathbf{x}''}^{l(x'_i)} A_{\mathbf{x}'}^{l(x'_i)} \otimes A_{\mathbf{x}'}^{a'_i})
$$
\n
$$
\approx_{\epsilon} \mathbb{E}_{\mathbf{x}, x'_i \neq x''_i} \sum_{a, l: l(x_i) = a} \text{Tr}_{\rho}(A_{\mathbf{x}}^a \otimes A_{\mathbf{x}'}^{l(x'_i)} A_{\mathbf{x}''}^{l(x'_i)} A_{\mathbf{x}'}^{l(x'_i)} \otimes A_{\mathbf{x}'}^{l(x'_i)})
$$
\n
$$
\approx_{\sqrt{\epsilon}} \mathbb{E}_{\mathbf{x}, x'_i \neq x''_i} \sum_{a, l: l(x_i) = a} \text{Tr}_{\rho}(A_{\mathbf{x}}^a \otimes A_{\mathbf{x}'}^{l(x''_i)} \otimes A_{\mathbf{x}'}^{l(x'_i)})
$$
\n
$$
\approx_{\epsilon} \mathbb{E}_{\mathbf{x}, x'_i, x''_i} \sum_{l} \text{Tr}_{\rho}(A_{\mathbf{x}}^{l(x_i)} \otimes A_{\mathbf{x}'}^{l(x''_i)} \otimes A_{\mathbf{x}'}^{l(x'_i)})
$$
\n
$$
= 1 - O(\sqrt{\epsilon})
$$

Upper bounds?

- Nothing known
- Possible approaches
	- Random projections?
	- Non-commutative Positivestellensatz [DLTW '08]

 \longrightarrow $\omega^* \doteq \omega^f$ \longleftarrow SDP Hierarchy

• Connes' embedding problem and Tsirelson's problem [JNP+ '11] [Fri '12]

Binary Constraint System Games

- The bug vs. feature question
- Exact case characterization

A BCS game has a perfect quantum strategy the corresponding BCS has a quantum satisfying assignment if and only if

[CM '12, ARXIV:1209.2729]

• Rewrite constraints as polynomials over reals

• Rewrite constraints as polynomials over reals

$$
x_1 \oplus x_2 = 0,
$$

\n $x_1 \oplus x_2 = 1.$ $x_1 + x_2 - 2x_1x_2 = 0,$
\n $x_1 + x_2 - 1 = 0.$

• Rewrite constraints as polynomials over reals

$$
x_1 \oplus x_2 = 0,
$$

\n $x_1 \oplus x_2 = 1.$ $x_1 + x_2 - 2x_1x_2 = 0,$
\n $x_1 + x_2 - 1 = 0.$

Quantum Satisfying Assignment $x_j \mapsto X_j$

• Rewrite constraints as polynomials over reals

$$
x_1 \oplus x_2 = 0,
$$

\n $x_1 \oplus x_2 = 1.$ $x_1 + x_2 - 2x_1x_2 = 0,$
\n $x_1 + x_2 - 1 = 0.$

Quantum Satisfying Assignment $x_j \mapsto X_j$

- (a) Satisfy every polynomial constraints.
- (b) For all j , $X_j^2 = X_j$.
- (c) Each pair of operators *Xj*, *Xk* appearing in the same constraint commute.

• Rewrite constraints as polynomials over reals

$$
x_1 \oplus x_2 = 0,
$$

\n $x_1 \oplus x_2 = 1.$ $x_1 + x_2 - 2x_1x_2 = 0,$
\n $x_1 + x_2 - 1 = 0.$

Quantum Satisfying Assignment $x_j \mapsto X_j$

- (a) Satisfy every polynomial constraints.
- (b) For all j , $X_j^2 = X_j$.
- (c) Each pair of operators *Xj*, *Xk* appearing in the same constraint commute.

Locally Commutative Condition

• Rewrite constraints as polynomials over reals

$$
x_1 \oplus x_2 = 0,
$$

\n
$$
x_1 \oplus x_2 = 1.
$$

\n
$$
x_1 + x_2 - 2x_1x_2 = 0,
$$

\n
$$
x_1 + x_2 - 1 = 0.
$$

\n
$$
x_1 + x_2 - 1 = 0.
$$

\n
$$
y
$$

\

- (a) Satisfy every polynomial constraints.
- (b) For all j , $X_j^2 = X_j$.
- (c) Each pair of operators *Xj*, *Xk* appearing in the same constraint commute.

Locally Commutative Condition

Magic square revisited

• Quantum satisfying assignment for magic square

$$
X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.
$$

- Anti-commutativity gadget
- Glue magic squares together
- Add a trivial constraint $f(x_2, x_4) \equiv 1$
- 3-SAT* with such trivial constraints

Theorem. 3-SAT* is Karp reducible to 3-COLORING*.

Theorem. 3-SAT* is Karp reducible to 3-COLORING*.

 $x_1,\overline{x_2},\overline{x_3},\ldots$

 $\bigwedge_{j=1}^m C_j$

 $x_1 \vee x_2 \vee \neg x_3$

Theorem. 3-SAT* is Karp reducible to 3-COLORING*.

 X_1, X_2, X_3, \ldots \longrightarrow Coloring measurements?

Theorem. 3-SAT* is Karp reducible to 3-COLORING*.

$$
\Lambda_{j=1}^{m} C_{j}
$$
\n
$$
x_{1}, x_{2}, x_{3}, \ldots
$$
\n
$$
(X_{1}, I - X_{1}, 0)
$$
\n
$$
x_{1} \vee x_{2} \vee \neg x_{3}
$$
\n
$$
T
$$

 X_1, X_2, X_3, \ldots **Coloring measurements?**

Theorem. 3-SAT* is Karp reducible to 3-COLORING*.

 X_1, X_2, X_3, \ldots Coloring measurements?

Triangular prism gadget

Lemma. The only constraint on the coloring operators of vertices *a* and *e* in the gadget is that they commute.

2. Extendibility 1. Commutativity

Commutativity gadget

Proof idea: Commutator is in the ideal generated by the constraints. Non-commutative Grobner basis.

Triangular prism gadget

Lemma. The only constraint on the coloring operators of vertices *a* and *e* in the gadget is that they commute.

Triangular prism gadget

Lemma. The only constraint on the coloring operators of vertices *a* and *e* in the gadget is that they commute.

The complexity of 3-SAT*

• NP-hardness of 3-SAT*

Commutativity gadget $x_1 \vee x_2 \vee y$

- Relation to the confusion check with *x*1 and *x*²
- 3-SAT* without confusion check is NP-hard (with inverse polynomial gap)
- Not known to be decidable

No dimension bound

• Relate it to approximate case?

• *k*-SAT*, 1-in-3-SAT*, KOCHEN-SPECKER*, 3-COLORING* and CLIQUE* are as hard as 3-SAT* A nonlocal NP theory

Schaefer's dichotomy theorem?

- 2-SAT^{*} and HORN-SAT^{*} are in P
- Affine-SAT^{*} or parity BCS games? [Ark '12]
- EPR pairs are optimal for perfect BCS games

Yet another quantum PCP theorem/conjecture?

- Hardness of approximation
	- Constant approximation of ω^* is NP-hard
	- Goal achieved with 3 players [Vid '13]
	- Constant approximation of ω^* is as hard as deciding ω^* =1?
- Nonlocal PCPs? (as non-signalling PCPs) $\mathop{{\rm Tr}}\nolimits_\rho (A^a_q \otimes A^{a'}_q \otimes A^{a''}_q) \qquad \qquad 24 - x_5 - x_6$
- Locally-commutative PCPs?

Open problems

- Upper bound of MIP*
- NEXP in MIP $*(2,1)$?
- 3-player vs. 2-player
- Power of 2-out-of-3 MIP*?
- BCS related problems

• …