# Unique games with entangled provers are easy

Presented By:-

Aman Sharma

Niraj Kumar

# Introduction

- We consider 2 prover-1 round games
- The game starts when the verifier sends two questions, one to each prover, chosen according to some joint distribution.
- Each prover then replies with an answer chosen from the alphabet $\{1, . . . , k\}$ for some $k \geq 1$.
- Finally, the verifier decides whether to accept or reject, based on the answers he received.
- The value of such a game is defined as the maximum success probability that the provers can achieve.

# Unique Games Conjecture [Kho02]

- For any e, $\delta > 0$ there exists a $k = k(e, \delta)$ such that it is NP-hard to determine whether, given a unique game with answers from a domain of size k, its value is at least $1 - e$ or at most $\delta$.

# Games with entangled provers

- In this paper we consider the model of two-prover one-round games in which the provers are allowed to share entanglement
- We define the entangled value of a game as the maximum success probability achievable by provers that share entanglement

# Main Result

- There exists an efficient algorithm that, given a unique game whose entangled value is $1 - \varepsilon$, outputs a value $\varepsilon/6 \leq \varepsilon' \leq \varepsilon$ and a description of an entangled strategy for the provers whose success probability is at least $1 - 6\varepsilon'$.
- This theorem shows that the analogue of the Unique Games Conjecture for entangled provers is false since , as long as, $6e + \delta < 1$, the algorithm can efficiently tell whether the entangled value of a game is at least $1 - e$ or at most $\delta$

# Game Description

- A one-round two-prover cooperative games $G = G(\pi, V)$ is specified by a set $Q$ and a number $k \geq 1$, a probability distribution $\pi : Q \times Q \rightarrow [0, 1]$, and a predicate $V : [k] \times [k] \times Q \times Q \rightarrow \{0, 1\}$.
- The referee samples $(s,t) \in Q \times Q$ according to $\pi$ and sends question $s$ to Alice and question $t$ to Bob. Alice replies with an answer $a \in [k]$, and Bob with an answer $b \in [k]$.
- The provers win if and only if $V(a, b \mid s, t) = 1$.
- A strategy for entangled provers is described by a shared quantum state, and a general measurement on Alice's part of the state for each of her questions, and a general measurement on Bob's part of the state for each of his question.

# Game Description

- Alice and Bob share an entangled state $|\psi\rangle \in C^{d*d}$ for some d ≥ 1, and they use projective measurements, i.e., for each s Alice's measurement is described by $\{A_a^s\}$ where the $A_a^s$ are orthogonal projectors and $\sum A_a^s = 1$. similarly Bob uses measurements $\{B_b^t\}$.
- By definition, the probability that on questions s, t Alice answers a and Bob answers b is given by $\langle\psi|A_a^s \otimes B_b^t|\psi\rangle$
- $$\omega^*(G) = \lim_{d\to\infty} \max_{|\psi\rangle\in\mathbb{C}^d\otimes\mathbb{C}^d} \max_{A_a^s, B_b^t} \sum_{abst} \pi(s,t) V(a,b\,|\,s,t) \langle\psi|A_a^s \otimes B_b^t|\psi\rangle$$

# Game Description

- A game is unique if we can associate a permutation $\sigma_{st}$ on [k] with each pair of questions (s, t) such that V(a, b |s, t) = 1 if and only if b = $\sigma_{st}$(a).
- A game is uniform if there exists an optimal strategy for entangled provers in which for each prover and each question, the marginal distribution of his answers is uniform over [k].

# SDP Relaxation

- The SDP maximizes over the real vectors $\{u_a^s\}, \{v_b^t\}$ $and$ $z$.

**SDP 1**

| | |
|---|---|
| **Maximize:** | $\sum_{abst} \pi(s,t) V(a,b \mid s,t) \langle u_a^s, v_b^t \rangle$ |
| **Subject to:** | $\|z\| = 1$ |
| | $\forall s,t,\ \sum_a u_a^s = \sum_b v_b^t = z$ |
| | $\forall s,t,\ \forall a \neq b,\ \langle u_a^s, u_b^s \rangle = 0$ and $\langle v_a^t, v_b^t \rangle = 0$ |
| | $\forall s,t,a,b,\ \langle u_a^s, v_b^t \rangle \geq 0$ |

- In an equivalent formulation in SDP language, we can replace the first two constraints by $\sum_{\{a,b\}} \langle u_a^s, v_b^t \rangle = 1$ , $\sum_{\{a\}} \langle u_a^s, u_a^s \rangle = 1$ and $\sum_{\{b\}} \langle v_b^t, v_b^t \rangle = 1$.

# SDP Relaxation

- Lemma : Let G = G(π, V) be a (not necessarily unique) one-round two-prover game. Then $\omega^*(G) \leq \omega^{sdp1}$(G).

- For Uniform unique games:

**Additional constraint for SDP 2:** $\forall s, t, a, b,\ \|u_a^s\| = \|v_b^t\| = 1/\sqrt{k}.$

# Quantum Rounding

- The basic idea in quantum rounding is to use the solution of the SDP to define a measurement for Alice & Bob on the *maximally entangled state* $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i, i\rangle$.
- For Uniform Unique games:
  - Consider a solution of SDP2 and use this solution to define part of a basis.
  - Complete this basis to a basis of $R^n$ in an arbitrary way
  - When Alice(Bob) is asked question s(t), she measures her half of $|\psi\rangle$ and outputs $a$(b) if her measurement corresponds to the basis element $u_a^s(v_b^t)$ and outputs nothing if she obtains one of the extra basis elements
  - They keep repeating this procedure on fresh copies of $|\psi\rangle$ until they obtain an output.

# Quantum Rounding

- For General Unique Games:
  - The rounding algorithm is similar to the one used for unique uniform games
  - However, in our rounding algorithm, we have to account for the fact that the vectors $u_a^s, v_b^t$ might not be of the same length
  - To this end, we use a rejection sampling technique as follows:
    - Alice and Bob use a shared random variable $\lambda$ sampled uniformly from [0,1].
    - Alice outputs her outcome a iff $\lambda \leq \left||u_a^s|\right|^2$ and Bob outputs his outcome b iff $\lambda \leq \left||v_b^t|\right|^2$

# Quantum Rounding Algorithm

**Algorithm 1** Quantum rounding for unique games.

| | |
|---|---|
| **Setup:** | Alice and Bob share many copies of an $n$-dimensional maximally entangled state $\|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \|i,i\rangle$, for some fixed basis $\{\|i\rangle\}$ of $\mathbb{C}^n$, as well as a sequence $\Lambda = (\lambda_1, \lambda_2, \dots)$ of real numbers, where the $\lambda_i$ are independent and each is sampled uniformly from $[0,1]$. |
| **Alice:** | On input $s$, performs the measurement $\textsc{Measure}(u_1^s, u_2^s, \dots, u_k^s)$ on her share of the maximally entangled states and the sequence $\Lambda$. |
| **Bob:** | On input $t$, performs the measurement $\textsc{Measure}(v_1^t, v_2^t, \dots, v_k^t)$ on his share of the maximally entangled states and the sequence $\Lambda$. |

# Measurement Procedure

**Measurement 1** The measurement $\text{MEASURE}(x_1, x_2, \dots, x_k)$ used in Algorithm 1.

| | |
|---|---|
| **Input:** | A state on a Hilbert space $\mathcal{H} = \bigotimes_{r=1}^{\infty} \mathcal{H}_r$, where each $\mathcal{H}_r \cong \mathbb{C}^n$, and a sequence of real numbers $\Lambda = (\lambda_1, \lambda_2, \dots)$, where each $\lambda_r \in [0, 1]$. |
| **Parameters:** | $k$ orthogonal vectors $x_1, x_2, \dots, x_k \in \mathbb{R}^n$. |
| **Output:** | An integer $m \in \{1, 2, \dots, k\}$. |
| **Measurement:** | Define a POVM on $\mathbb{C}^n$ with elements |

$$P_i = \left| \frac{x_i}{\|x_i\|} \right\rangle \left\langle \frac{x_i}{\|x_i\|} \right| \text{ for } i = 1, 2, \dots, k \text{ and } P_0 = I - \sum_{i=1}^{k} P_i,$$

where for a vector $w \in \mathbb{R}^n$ we write $|w\rangle = \sum_i (w)_i |i\rangle$ for its embedding into $\mathbb{C}^n$.

**For** $r = 1, 2, \dots$ do:

Measure $\mathcal{H}_r$ using POVM $(P_0, \dots, P_k)$, obtaining outcome $m$.

**If** ($m \neq 0$ and $\lambda_r \leq \|x_m\|^2$) **then** output $m$ and exit.

# Analysis of Measurement Procedure

- Lemma : Let $x_1, . . . , x_k$ and $y_1, . . . , y_k$ be two sequences of orthogonal vectors in $\boldsymbol{R}^n$ such that $\sum_{i=1}^{k}||x_i||^2 = \sum_{i=1}^{k}||y_i||^2 = 1$. Assume Alice and Bob apply Measurement 1, Alice using $(x_i)$ and Bob using $(y_i)$. For any i, j ∈ {1, . . . , k} define:

$$q_{i,j} := \left\langle \frac{x_i}{\|x_i\|}, \frac{y_j}{\|y_j\|} \right\rangle^2 \min(\|x_i\|^2, \|y_j\|^2)$$

- Let $q_{total} = \sum_{i=1}^{k} q_{i,j}$. Then for any i, j ∈ {1, . . . , k}, the probability that Alice outputs i and Bob outputs j is at least

$$\frac{q_{i,j}}{2 - q_{\text{total}}}.$$

# Corollary:

- Let V be a subset of $\{1, \ldots, k\}^2$. Then, in the setting of previous Lemma , the probability that Alice's output i and Bob's output j are such that (i, j) ∈ V is at least:

$$\frac{p_V}{2 - p_V} \geq 1 - 2(1 - p_V),$$

$$p_V := \sum_{i,j \in V} \left\langle \frac{x_i}{\|x_i\|}, \frac{y_j}{\|y_j\|} \right\rangle^2 \min(\|x_i\|^2, \|y_j\|^2).$$

# Analysis of Quantum Rounding

- Theorem 1: (Uniform unique games). Let G be a uniform unique game. Suppose that $\omega_{sdp2}(G) = 1 - \varepsilon$. Then $\omega^*(G) \geq 1 - 4\varepsilon$.

- Theorem 2: (General unique games). Let G be a unique game. Suppose that $\omega_{sdp1}(G) = 1 - \varepsilon$. Then $\omega^*(G) \geq 1 - 6\varepsilon$.

# Final Results:

- For a Uniform Unique Game:

$$1 - 4\varepsilon \leq \omega^* \, (G) \leq 1 - \varepsilon$$

- For a general Unique Game:

$$1 - 6\varepsilon \leq \omega^* \, (G) \leq 1 - \varepsilon$$

# Parallel Repetition Results

- Theorem 1[Rao08]:
  - Let G be a unique game with value $\omega(G) = 1 - \epsilon$. Then $\forall m \geq 1$ $(1-\epsilon)^m \leq \omega(G^m) \leq (1 - c\epsilon^2)^m$ where $c > 0$ is a universal constant
- Theorem 2:
  - Let G be a unique game with entangled value $\omega^*(G) = 1 - \epsilon$. Then, $(1-\epsilon)^m \leq \omega^*(G^m) \leq \left(1 - \frac{\epsilon^2}{16}\right)^m$
- Theorem 3:
  - Let G be a uniform unique game with value $\omega(G) = 1 - \epsilon$ such that $G^m$ is also uniform. Then$(1-\epsilon)^m \leq \omega^*(G^m) \leq \left(1 - \frac{\epsilon}{4}\right)^m$

# Bipartite SDPs

- These SDPs have two sets of variables, $u_1, u_2 \ldots u_{n_1}$ and $v_1, v_2 \ldots v_{n_2}$.
- *Optimization* Function only involves inner products between u variables and v variables; and the *constraints* are all equality constraints and involve either only u variables or only v variables.
- The SDP specified by the $n_1 \times n_2$ matrix $J$, $n_1 \times n_1$ symmetric matrix $A^1 \cdots A^L$, $n_2 \times n_2$ symmetric matrix $B^1 \cdots B^L$ and the real numbers $a_1 \cdots a_L$ and $b_1 \cdots b_L$ :

**Maximize:** $\sum_{i=1,j=1}^{n_1,n_2} J_{ij} \langle u_i, v_j \rangle$

**Subject to:** $\sum_{i,j=1}^{n_1} A_{ij}^l \langle u_i, u_j \rangle = a_l$ for $l = 1, \ldots, L_1$

$\sum_{i,j=1}^{n_2} B_{ij}^l \langle v_i, v_j \rangle = b_l$ for $l = 1, \ldots, L_2$.

# Bipartite Product SDPs

- Assume S has $n_1 + n_2$ variables and $L_1 + L_2$ constraints, and is specified by $J, A^l, B^l, a^l$ and $b^l$, and similarly for $S'$
- Then $S \otimes_b S'$ is the bipartite SDP over $n_1 n_1' + n_2 n_2'$ variables and $L_1 L_1' + L_2 L_2'$ given by $J \otimes J'$,the matrices $A^l \otimes A'^{l'}$ and $B^l \otimes B'^{l'}$ and the numbers $a_l a_{l'}'$ and $b_l b_{l'}'$.

**Maximize:** $\sum_{i=1,j=1,i'=1,j'=1}^{n_1,n_2,n_1',n_2'} J_{ij} J'_{i'j'} \langle u_{ii'}, v_{jj'} \rangle$

**Subject to:** $\sum_{i,j=1,i',j'=1}^{n_1,n_1'} A^l_{ij} A'^{l'}_{i'j'} \langle u_{ii'}, u_{jj'} \rangle = a_l a'_{l'}$ for $l = 1, \ldots, L_1$, $l' = 1, \ldots, L_1'$

$\sum_{i,j=1,i',j'=1}^{n_2,n_2'} B^l_{ij} B'^{l'}_{i'j'} \langle v_{ii'}, v_{jj'} \rangle = b_l b'_{l'}$ for $l = 1, \ldots, L_2$, $l' = 1, \ldots, L_2'$.

# $SDP_3$ and $SDP_4$ Construction

- For General Unique Games:

| **SDP 3** | |
|---|---|
| **Maximize:** | $\sum_{abst} \pi(s,t) V(a,b \mid s,t) \langle u_a^s, v_b^t \rangle$ |
| **Subject to:** | $\forall s,\ \forall a \neq b,\ \langle u_a^s, u_b^s \rangle = 0$ and $\forall t,\ \forall a \neq b,\ \langle v_a^t, v_b^t \rangle = 0$ |
| | $\forall s,\ \sum_a \langle u_a^s, u_a^s \rangle = 1$ and $\forall t,\ \sum_b \langle v_b^t, v_b^t \rangle = 1$ |

- $SDP_3$ is a relaxation of SDP 1, and hence for any game G its value satisfies $\omega_{sdp3}(G) \geq \omega_{sdp1}(G) \geq \omega^*(G)$.
- For Uniform Unique Games:

| **SDP 4** | |
|---|---|
| **Maximize:** | $\sum_{abst} \pi(s,t) V(a,b \mid s,t) \langle u_a^s, v_b^t \rangle$ |
| **Subject to:** | $\forall s,a,b,\ \langle u_a^s, u_b^s \rangle = \frac{1}{k}\delta_{a,b}$ and $\forall t,a,b,\ \langle v_a^t, v_b^t \rangle = \frac{1}{k}\delta_{a,b}$ |

THANK YOU!!