Unique Games Conjecture
Two-Player One-Round Games

• $(x, y) \sim \mu$
• $V(x, y, a, b) \in \{0(\text{lose}), 1(\text{win})\}$
• $\text{val}(G) := \text{the highest probability to win the game}$
Two-Player One-Round Games

Example: 3SAT
\[ \psi = \psi_1 \land \cdots \land \psi_m \]
\[ \psi_i = x_{i_1} \lor x_{i_2} \lor x_{i_3} \]

\((x, y) \sim (\psi_i, x_{i_j})\)

- \(a\): assignment to all vars. in \(\psi_i\)
- \(b\): assignment to \(x_{i_j}\)

\[ V(x, y, a, b) = 1 \iff a \text{ satisfies } \psi_i \text{ and } a, b \text{ consistent} \]

\(\psi\) satisfiable \(\Rightarrow\) \(\text{val}(G) = 1\)

\(\psi\) unsatisfiable \(\Rightarrow\) \(\text{val}(G) \leq 1 - \frac{1}{3m}\)
Two-Player One-Round Games

- It captures the complexity of many optimization problems.
- Computing $\text{val}(G)$ is NP-hard
Two-Player One-Round Games

- It captures the complexity of many optimization problems.

- **Computing** $\text{val}(G)$
  Approximating $\text{val}(G)$ to a 1/poly precision is NP-hard

**PCP theorem.**
For any constant $\delta$, $\exists G$ such that distinguishing the following two cases is NP-complete
- Yes. $\text{val}(G) \geq 1 - \delta$
- No. $\text{val}(G) \leq \delta$
Unique Games and UGC

Unique Games

∀x, y
∀a ∃ unique b s.t. V(x, y, a, b) = 1
and
∀b ∃ unique a s.t. V(x, y, a, b) = 1

Unique Game conjecture.
For any constant δ, ∃ G unique games G such that distinguishing the following two cases is NP-complete

• Yes. val(G) ≥ 1 − δ
• No. val(G) ≤ δ
Main Theorem

[Kho02] UGC ⇒
There is no polynomial time algorithm that approximate MAX-CUT to any constant better than

\[ \alpha = \min_{-1 \leq \rho \leq 1} \frac{2 \arccos \rho}{\pi (1 - \rho)} \approx 0.87856 \]
Graphical Representation

- \((x, y) \sim \mu\)
- \(V(x, y, a, b) \in \{0(\text{lose}), 1(\text{win})\}\)
- \(val(G) := \text{the highest probability to win the game}\)
Graphical Representation

- \((x, y) \sim \mu\)
- \(V(x, y, a, b) \in \{0(lose), 1(win)\}\)
- \(val(G) \) := the highest probability to win the game
Graphical Representation for Unique Games

- The answer sets $|A| = |B|$
- Assume that $A = B = \{1, ..., M\}$
- For any $(x, y)$ with $\mu(x, y) > 0$, there exists a permutation $\pi_{x,y}$ on $[M]$ s.t.
  $V(x, y, a, b) = 1$ iff. $a = \pi_{x,y}(b)$

- $\text{opt}(L) := \max \{ \sum_{(x,y) \text{is satisfied}} \mu(x, y) \}$
- $(x, y) \sim \mu$
- $V(x, y, a, b) \in \{0(\text{lose}), 1(\text{win})\}$
- $\text{val}(G) := \text{the highest probability to win the game}$

- Unique label cover problem $ULC(\delta)$: given a unique game $L(V, W, E, [M], \{\pi_v, w\})$, whether $\text{opt}(L) \geq 1 - \delta$ or $\text{opt}(L) \leq \delta$
**Graphical Representation**

- **Unique label cover problem** $ULC(\delta)$: given a unique game $L(V, W, E, [M], \{\pi_{v,w}\})$, whether $\text{opt}(L) \geq 1 - \delta$ or $\text{opt}(L) \leq \delta$

- **Unique Games conjecture**: For any $\delta > 0$, there exists a constant $M$ s.t. it is NP-hard to decide $ULC(\delta)$ with a label set of size $M$. 
Prover and Verifier

**Definition** (The class \( \text{NP} \))

A language \( L \subseteq \{0, 1\}^* \) is in \( \text{NP} \) if there exists a polynomial \( p : \mathbb{N} \to \mathbb{N} \) and a polynomial-time TM \( M \) such that for every \( x \in \{0, 1\}^* \),

\[
x \in L \text{ if and only if } \exists u \in \{0, 1\}^{p(|x|)} \text{ s.t. } M(x, u) = 1.
\]

**Proof/certificate**

Input \( x \)

Q: \( x \in L? \)

\[
\begin{array}{cccccccc}
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{array}
\]

Output \( M(x, u) \)

\[
\begin{cases}
\quad x \in L \text{ if } M(x, u) = 1 \\
\quad x \notin L \text{ otherwise.}
\end{cases}
\]

Verifier (polynomial-time verifiable)
Examples in NP

- **Maximum independent set.** \( \text{INDSET} = \{\langle G, k \rangle : \exists S \subseteq V(G) \text{ s.t. } |S| \geq k \text{ and } \forall u, v \in S, (u, v) \notin E(G) \} \). The certificate is the set of \( k \) vertices that are not adjacent to each other. **NP-complete.**

- **Traveling salesman.** Given a set of \( n \) nodes, \( \binom{n}{2} \) numbers \( d_{i,j} \) denoting the distances between all pairs of nodes, and a number \( k \), decide if there is a closed circuit (i.e., a salesperson tour) that visits every node exactly once and has total length at most \( k \). The certificate is the sequence of nodes in such a tour. **NP-complete.**

- **Subset sum.** Given a list of \( n \) numbers \( A_1, \ldots, A_n \) and a number \( T \), decide if there is a subset of the numbers that sums up to \( T \). The certificate is the list of members in such a subset. **NP-complete.**

- **Linear programming.** Given a list of \( m \) linear inequalities with rational coefficients over \( n \) variables \( u_1, \ldots, u_n \), decide if there is an assignment of rational numbers to the variables \( u_1, \ldots, u_n \) that satisfies all the inequalities. The certificate is the assignment. **P.**
Examples in NP

- **0/1 integer programming.** Given a list of \( m \) linear inequalities with rational coefficients over \( n \) variables \( u_1, \ldots, u_m \), find out if there is an assignment of zeroes and ones to \( u_1, \ldots, u_n \) satisfying all the inequalities. The certificate is the assignment. \textbf{NP}-complete.

- **Graph isomorphism.** Given two \( n \times n \) adjacency matrices \( M_1, M_2 \), decide if \( M_1 \) and \( M_2 \) define the same graph, up to renaming of vertices. The certificate is the permutation \( \pi : [n] \rightarrow [n] \) such that \( M_2 \) is equal to \( M_1 \) after reordering \( M_1 \)'s indices according to \( \pi \). Not known.

- **Composite numbers.** Given a number \( N \) decide if \( N \) is a composite (i.e., non-prime) number. The certificate is the factorization of \( N \). \textbf{P}

- **Factoring.** Given three numbers \( N, L, U \) decide if \( N \) has a prime factor \( p \) in the interval \([L, U] \). The certificate is the factor \( p \). Not known

- **Connectivity.** Given a graph \( G \) and two vertices \( s, t \) in \( G \), decide if \( s \) is connected to \( t \) in \( G \). The certificate is a path from \( s \) to \( t \). \textbf{P}
Main Theorem

For every \( \rho \in (-1,0) \) and \( \epsilon > 0 \) there exists \( \delta > 0 \) s.t. there exists a proof for \( ULC(\delta) \) in which the verifier reads two bits from the proof and accepts iff. They are unequal, and which has completeness

\[
c \geq \frac{1 - \rho}{2} - \epsilon
\]

and soundness

\[
s \leq \frac{1}{\pi} \arccos \rho + \epsilon
\]
Reduction from UGC to MAX-CUT

**Theorem**

For every $\rho \in (-1,0)$ and $\epsilon > 0$ there exists $\delta > 0$ and a polynomial-time reduction from an instance $L$ of $ULC(\delta)$ to an instance $G = (V, E, w)$ of MAX-CUT s.t.

$$opt(L) \geq 1 - \delta \Rightarrow mc(G) \geq \frac{1 - \rho}{2} - \epsilon$$

$$opt(L) \leq \delta \Rightarrow mc(G) \leq \frac{1}{\pi} \arccos \rho + \epsilon$$

- Every pair $(u_i, u_j)$ is connected with the weight = probability that it is picked by the verifier

$\Rightarrow$ It is NP-hard to approximate MAX-CUT to within

$$\frac{\arccos \rho}{\pi} + \epsilon > \frac{\arccos \rho / \pi}{(1 - \rho) / 2}$$
Theorem
For every $\rho \in (-1,0)$ and $\epsilon > 0$ there exists $\delta > 0$ and a polynomial-time reduction from an instance $L$ of $ULC(\delta)$ to an instance $G = (V,E,w)$ of MAX-CUT s.t.

\[
\text{opt}(L) \geq 1 - \delta \Rightarrow \text{mc}(G) \geq \frac{1 - \rho}{2} - \epsilon \\
\text{opt}(L) \leq \delta \Rightarrow \text{mc}(G) \leq \frac{1}{\pi} \arccos \rho + \epsilon
\]

- Every pair $(u_i, u_j)$ is connected with the weight = probability that it is picked by the verifier

⇒ It is NP-hard to approximate MAX-CUT to within

\[
\max_{-1 \leq \rho \leq 0} \frac{\arccos \rho / \pi}{(1 - \rho)/2} = \alpha
\]
Main Theorem

For every $\rho \in (-1,0)$ and $\epsilon > 0$ there exists $\delta > 0$ s.t. there exists a proof for $ULC(\delta)$ in which the verifier reads two bits from the proof and accepts iff. They are unequal, and which has completeness

$$c \geq \frac{1 - \rho}{2} - \epsilon$$

and soundness

$$s \leq \frac{1}{\pi} \arccos \rho + \epsilon$$
Long code

For any $x$, $f_x: \{-1\}^M \rightarrow \{-1\}$ s.t. $f_x(u) = u_a$ (dictator function)

For any $y$, $f_y: \{-1\}^M \rightarrow \{-1\}$ s.t. $f_y(v) = v_b$
2-Bit Test

Certificate: Long codes of the labels of all vertices.

1. Given \( L(V, W, E, [M], \{\pi_{v,w}\}) \) and a proof, sample \( v \in V \) uniformly, and sample two of its neighbors \( w, w' \in W \) uniformly and independently.
2. Let \( \pi = \pi_{v,w} \) and \( \pi' = \pi_{v,w'} \).
3. Sample \( x \in \{\pm 1\}^M \) uniformly and \( y \sim \rho \) \( x \). Namely
   \[
   \Pr[y_i = x_i] = \frac{1 + \rho}{2} \\
   \Pr[y_i = -x_i] = \frac{1 - \rho}{2}
   \]
4. Accept if \( f_w(x \circ \pi) = f_{w'}(y \circ \pi') \)
   where \( x \circ \pi = (x_{\pi(1)}, \ldots, x_{\pi(n)}) \)

Completeness \( \text{opt}(L) \geq 1 - \delta \)

\( f_w \) be the long code of the label of \( w \)

Let \( i, j, j' \) be the labels of \( v, w, w' \)

\[
\begin{align*}
\Pr[LMM] &= \Pr[x_i \neq y_i](1 - 2\delta) = \frac{1 - \rho}{2} - \epsilon
\end{align*}
\]
2-Bit Test

Certificate: Long codes of the labels of all vertices.

1. Given \( L(V, W, E, [M], \{\pi_{v,w}\}) \) and a proof, sample \( v \in V \) uniformly, and sample two of its neighbors \( w, w' \in W \) uniformly and independently.

2. Let \( \pi = \pi_{v,w} \) and \( \pi' = \pi_{v,w'} \).

3. Sample \( x \in \{\pm 1\}^M \) uniformly and \( y \sim \rho \ x \). Namely
   \[
   \Pr[y_i = x_i] = \frac{1 + \rho}{2} \\
   \Pr[y_i = -x_i] = \frac{1 - \rho}{2}
   \]

4. Accept if \( f_w(x \circ \pi) = f_{w'}(y \circ \pi') \)
   where \( x \circ \pi = (x_{\pi(1)}, \ldots, x_{\pi(n)}) \)

Soundness \( \text{opt}(L) \leq \delta \)

\( p_v \): prob. test accepts if choosing \( v \in V \)

\[
\begin{align*}
p_v &= E_{w,w',x,y \sim \rho} x \left[ 1 - f_w(x \circ \pi)f_{w'}(y \circ \pi') \right] \\
&= \frac{1}{2} - \frac{1}{2} E_{x,y \sim \rho} x [g_v(x)g_v(y)] \\
&= \frac{1}{2} - \frac{1}{2} \text{Stab}_\rho(g_v) \text{ (noise stability)}
\end{align*}
\]

where \( g_v(x) = E_{w \sim v}[f_w(x \circ \pi_{v,w})] \)
2-Bit Test

Certificate: Long codes of the labels of all vertices.

Soundness \( \text{opt}(L) \leq \delta \)

\( p_v: \) prob. test accepts if choosing \( v \in V \)

\[
p_v = E_{w,w',x,y \sim \rho x} \left[ \frac{1 - f_w(x \circ \pi)f_w'(y \circ \pi')}{2} \right]
\]

\[
= \frac{1}{2} - \frac{1}{2} E_{x,y \sim \rho x} [g_v(x)g_v(y)]
\]

\[
= \frac{1}{2} - \frac{1}{2} Stab_\rho (g_v) \text{ (noise stability)}
\]

where \( g_v(x) = E_{w \sim v} [f_w(x \circ \pi_{v,w})] \)

Completeness \( \Rightarrow \)

If \( f_w \) and \( f_{w'} \) are both dictator functions. Then \( p_v \geq 1 - \rho \)

\( f_w \) and \( f_{w'} \) are “close”-to dictator function

\( \Rightarrow p_v \) is large

“close”: there exists a coordinate \( i \) which has high influence to the function of the value
Noise Stability

Certificate: Long codes of the labels of all vertices.

Soundness \( \text{opt}(L) \leq \delta \)

\( p_v: \) prob. test accepts if choosing \( v \in V \)

\[
p_v = \frac{1}{2} - \frac{1}{2} E_{x,y \sim x} [g_v(x)g_v(y)] = \frac{1}{2} - \frac{1}{2} \text{Stab}_\rho(g_v)
\]

Given \(-1 < \rho < 0\), \( \min g \text{Stab}_\rho(g) \)

Let \( f(x) = \frac{g(x) - g(-x)}{2} \)

\[
\text{Stab}_{-\rho}(f) = -\text{Stab}_\rho(g)
\]

Theorem (Majority is Stablest [MOO05]) The max is at most \( 1 - \frac{2}{\pi} \arccos \rho + \epsilon \)

\[
\Rightarrow p_v \geq \frac{1}{\pi} \arccos \rho - \epsilon
\]
Majority is the stablest

Given $0 < \rho < 1$

$$\min \text{Stab}_\rho(g) = E_{x,y \sim \rho x}[g(x)g(y)]$$

$$\text{s.t.} \ E[g] = 0$$

Every coordinate $i$ is low influential

Q: What is the stablest voting scheme?

Majority!
Majority is the stablest

**Theorem** (Majority is Stablest [MOO05]) For every $0 \leq \rho < 1$, $\epsilon > 0$, if $f: \{-1,1\}^n \rightarrow [-1,1]$ with $E[f] = 0$ and the influence of every coordinate to $f(x)$ is sufficiently low, then

$$Stab_{\rho}(f) \leq Stab_{\rho}(\text{Maj}) + \epsilon = 1 - \frac{2}{\pi} \arccos \rho + \epsilon$$

**Proof**

- Analysis of Boolean functions
- Invariance principle
- Hypercontractive inequality
Central Limit Theorem

Theorem. Let \( X_1, ..., X_n \sim_u \{-1,1\} \) be i.i.d. Then for any \( a \)

\[
\lim_{n \to \infty} \Pr \left[ \frac{X_1 + \cdots + X_n}{\sqrt{n}} \leq a \right] = \Pr_{g \sim N(0,1)} [g \leq a]
\]

Let \( \Psi(x) = \begin{cases} 
1 & \text{if } x \leq a \\
0 & \text{otherwise}
\end{cases} \) and \( p(x_1, ..., x_n) = \frac{x_1 + \cdots + x_n}{\sqrt{n}} \)

\[
E[\Psi \circ p(x_1, ..., x_n)] = E_{(g_1, ..., g_n) \sim N(0,1)^n} [\Psi \circ p(g_1, ..., g_n)]
\]

Note that \( \frac{g_1 + \cdots + g_n}{\sqrt{n}} \sim N(0,1) \)
Central Limit Theorem

Theorem. Let $X_1, \ldots, X_n \sim u \{−1, 1\}$ be i.i.d. Then for any $a$

$$\left| \Pr \left[ \frac{X_1 + \cdots + X_n}{\sqrt{n}} \leq a \right] - \Pr_{g \sim N(0,1)} [g \leq a] \right| \leq \frac{C}{\sqrt{n}}$$

for some constant $C$.

Let $\Psi(x) = \begin{cases} 1 & \text{if } x \leq a \\ 0 & \text{otherwise} \end{cases}$ and $p(x_1, \ldots, x_n) = \frac{x_1 + \cdots + x_n}{\sqrt{n}}$

$$\left| E[\Psi \circ p(x_1, \ldots, x_n)] - E_{(g_1, \ldots, g_n) \sim N(0,1)^n} [\Psi \circ p(g_1, \ldots, g_n)] \right| \leq \frac{C}{\sqrt{n}}$$

for some constant $C$. 
Invariance Principle

Let \( \Psi(x) = \begin{cases} 1 & \text{if } x \leq a \\ 0 & \text{otherwise} \end{cases} \) and \( p(x_1, ..., x_n) = \frac{x_1 + \ldots + x_n}{\sqrt{n}} \)

\[
\left| E[\Psi \circ p(x_1, ..., x_n)] - E_{(g_1, ..., g_n) \sim N(0,1)^n} [\Psi \circ p(g_1, ..., g_n)] \right| \leq \frac{C}{\sqrt{n}}
\]

for some constant \( C \).

Q: Can we replace \( \Psi \) and \( p \) by other functions?

A: Invariance Principle \( \Rightarrow \) it still holds if

\( \Psi \) is “flat” and continuous function.
\( p \) is a low degree polynomial and each variable is “low influential”
Invariance Principle

Q: Can we replace $\Psi$ and $p$ by other functions?

A: Invariance Principle $\Rightarrow$ it still holds if

$\Psi$ is “flat” and continuous function.
$p$ is a low degree polynomial and each variable is “low influential”

Q: But $\Psi$ in Berry-Esseen Theorem is not continuous

A: It can be approximated by a flat and continuous function
Majority is stablest

Given $0 < \rho < 1$

$$\min \text{Stab}_\rho(g) = E_{x,y \sim \rho x}[g(x)g(y)]$$

s.t. $E[g] = 0$

Every coordinate $i$ is low influential

Invariance Principle $\Rightarrow \text{Stab}_\rho(g) \approx E_{(u,v) \sim \sigma^n}[g(u)|_{[-1,1]} \cdot g(v)|_{[-1,1]}]$ 

$G_\rho$ is a two-dimensional normal distribution $(X,Y)$ with mean $(0,0)$ and covariance matrix

$$\begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}$$

Borell Theorem [Bor’85] The maximum is achieved when $g = \text{Maj}$.