

CSL853: Complexity Theory

Ragesh Jaiswal, CSE, IIT Delhi

PCP Theorem and Hardness of Approximation

PCP Theorem and Hardness of Approximation

MAX-CUT

Definition (MAX-CUT)

Given a graph $G = (V, E)$ and a weight function $w : E \rightarrow \mathbb{R}^+$ such that for each edge (u, v) has a weight w_{uv} . Find a cut $S \subset V$ that maximises

$$\sum_{u \in S, v \in \bar{S}, (u,v) \in E} w_{uv}.$$

- Let us consider the following gap version $\text{GapMAXCUT}_{c,s}$ of the MAX-CUT problem:

Definition ($\text{GapMAXCUT}_{c,s}$)

Yes instance: The given graph has a cut containing at least c fraction of the edges.

No instance: The given graph does not have any cut with more than s fraction of the edges.

- Given that a conjecture known as the **Unique Games Conjecture (UGC)** holds, we will show that $\text{GapMAXCUT}_{\frac{1-\rho}{2}-\epsilon, \frac{\cos^{-1}\rho}{\pi}+\epsilon}$ is NP-hard.
- This shows that conditioned on UGC it is not possible to have an efficient approximation algorithm that gives approximation factor better than $\alpha = 0.87856$.

PCP Theorem and Hardness of Approximation

MAX-CUT

- To understand UGC and the reduction for the MAX-CUT problem, we will need the following **Unique Label Cover Problem**.

Definition (Unique Label Cover Problem (ULC))

The ULC problem is the same as the Label Cover problem with the addition restriction that for all edges $e \in E$, the function $\Pi_e : \Sigma \rightarrow \Sigma$ is a permutation.

- We will also need the following gap version of the ULC problem.

Definition (ULC_δ)

Yes instance: There is a labelling that satisfies at least $(1 - \delta)$ fraction of edges.

No instance: No labeling satisfies more than δ fraction of the edges.

Conjecture (Unique Games Conjecture (UGC))

For any $\delta > 0$, there is an M such that it is NP-hard to decide ULC_δ on instances with label set of size M .

PCP Theorem and Hardness of Approximation

MAX-CUT

Conjecture (Unique Games Conjecture (UGC))

For any $\delta > 0$, there is an M such that it is NP-hard to decide ULC_δ on instances with label set of size M .

- We will also need the following theorem for showing inapproximability for MAX-CUT.

Theorem

For every $\rho \in (-1, 0)$ and any $\epsilon > 0$, there is a some $\delta > 0$ such that there is a PCP for ULC_δ in which the verifier reads two bits of the proof and accepts if they are unequal and moreover the following holds:

- *If L is a yes instance of ULC_δ , then the verifier accepts with probability at least $c \geq \frac{(1-\rho)}{2} - \epsilon$.*
- *If L is a no instance of ULC_δ , then the verifier accepts with probability at most $s < \frac{\cos^{-1}(\rho)}{\pi} + \epsilon$.*

- Claim: The above theorem along with UGC implies that it is NP-hard to approximate MAX-CUT within a factor better than $\alpha = 0.87856$.

PCP Theorem and Hardness of Approximation

MAX-CUT

Theorem

For every $\rho \in (-1, 0)$ and any $\epsilon > 0$, there is a some $\delta > 0$ such that there is a PCP for ULC_δ in which the verifier reads two bits of the proof and accepts if they are unequal and moreover the following holds:

- If L is a yes instance of ULC_δ , then the verifier accepts with probability at least $c \geq \frac{(1-\rho)}{2} - \epsilon$.*
 - If L is a no instance of ULC_δ , then the verifier accepts with probability at most $s < \frac{\cos^{-1}(\rho)}{\pi} + \epsilon$.*
- Recall, while proving $\text{NP} \subseteq \text{PCP}(\text{poly}(n), 1)$ we used linearity testing crucially. For the above PCP statement, we will use a similar test known as the **long code test**.
 - Let $\{1, \dots, m\}$ be the message space. The long code for a message $i \in [m]$ is the truth table of the following function $f_i : \{-1, +1\}^m \rightarrow \{-1, +1\}$ defined as $f_i(x_1, \dots, x_m) = x_i$.

PCP Theorem and Hardness of Approximation

MAX-CUT

Theorem

For every $\rho \in (-1, 0)$ and any $\epsilon > 0$, there is a some $\delta > 0$ such that there is a PCP for ULC_δ in which the verifier reads two bits of the proof and accepts if they are unequal and moreover the following holds:

- If L is a yes instance of ULC_δ , then the verifier accepts with probability at least $c \geq \frac{(1-\rho)}{2} - \epsilon$.
- If L is a no instance of ULC_δ , then the verifier accepts with probability at most $s < \frac{\cos^{-1}(\rho)}{\pi} + \epsilon$.

- Recall, while proving $\text{NP} \subseteq \text{PCP}(\text{poly}(n), 1)$ we used linearity testing crucially. For the above PCP statement, we will use a similar test known as the **long code test**.
- Let $\{1, \dots, m\}$ be the message space. The long code for a message $i \in [m]$ is the truth table of the following function $f_i : \{-1, +1\}^m \rightarrow \{-1, +1\}$ defined as $f_i(x_1, \dots, x_m) = x_i$.
- Problem: Design a **two** query test with the following properties:
 - If a function f is a long code for some $i \in [m]$ (in other words f is a **dictator** function), then the function passes the test with high probability.
 - If the function is “far from being a dictator”, then it passes the test with low probability.

PCP Theorem and Hardness of Approximation

MAX-CUT

- Problem: Design a **two** query test with the following properties:
 - If a function f is a long code for some $i \in [m]$ (in other words f is a **dictator** function), then the function passes the test with high probability.
 - If the function is “far from being a dictator”, then it passes the test with low probability.
- Consider the following test: Pick $x \in_R \{-1, +1\}^m$ and let $y = -x$. Accept if $f(x) \neq f(y)$ else reject.
 - Completeness: If the function is a dictator, then it passes the test with probability 1.
 - Soundness: Functions that are far from being dictators also pass the test with good probability. For example, the majority function $MAJ(x_1, \dots, x_m) = \text{sgn} \sum_i x_i$ for odd m .

PCP Theorem and Hardness of Approximation

MAX-CUT

- Problem: Design a **two** query test with the following properties:
 - If a function f is a long code for some $i \in [m]$ (in other words f is a **dictator** function), then the function passes the test with high probability.
 - If the function is “far from being a dictator”, then it passes the test with low probability.
- Consider the following test:
 - Pick $x \in_R \{-1, +1\}^m$.
 - Pick μ as follows: for each $i \in [m]$ set μ_i to $+1$ with probability $(1 + \rho)/2$ and -1 with the remaining probability.
 - Let $y = x \cdot \mu$.
 - Accept if $f(x) \neq f(y)$, else reject.
- Let us analyze the above test:
 - Completeness: What is the probability that a dictator function passes the test?

PCP Theorem and Hardness of Approximation

MAX-CUT

- Problem: Design a **two** query test with the following properties:
 - If a function f is a long code for some $i \in [m]$ (in other words f is a **dictator** function), then the function passes the test with high probability.
 - If the function is “far from being a dictator”, then it passes the test with low probability.
- Consider the following test:
 - Pick $x \in_R \{-1, +1\}^m$.
 - Pick μ as follows: for each $i \in [m]$ set μ_i to $+1$ with probability $(1 + \rho)/2$ and -1 with the remaining probability.
 - Let $y = x \cdot \mu$.
 - Accept if $f(x) \neq f(y)$, else reject.
- Let us analyze the above test:
 - Completeness: What is the probability that a dictator function passes the test?
 - Soundness: We do some analysis. For any function f we have:

$$\begin{aligned}\Pr_{x,\mu}[f(x) \neq f(y)] &= \Pr_{x,\mu}[f(x) \neq f(\mu \cdot x)] \\ &= \mathbf{E}_{x,\mu} \left[\frac{1 - f(x)f(\mu \cdot x)}{2} \right] \\ &= \frac{1}{2} - \frac{1}{2} \cdot \mathbf{E}_{x,\mu} [f(x)f(\mu \cdot x)]\end{aligned}$$

PCP Theorem and Hardness of Approximation

MAX-CUT

- Problem: Design a **two** query test with the following properties:
 - If a function f is a long code for some $i \in [m]$ (in other words f is a **dictator** function), then the function passes the test with high probability.
 - If the function is “far from being a dictator”, then it passes the test with low probability.
- Consider the following test:
 - Pick $x \in_R \{-1, +1\}^m$.
 - Pick μ as follows: for each $i \in [m]$ set μ_i to $+1$ with probability $(1 + \rho)/2$ and -1 with the remaining probability.
 - Let $y = x \cdot \mu$.
 - Accept if $f(x) \neq f(y)$, else reject.
- Let us analyze the above test:
 - Completeness: What is the probability that a dictator function passes the test?
 $\frac{(1-\rho)}{2}$
 - Soundness: We do some analysis. For any function f we have:

$$\Pr_{x,\mu}[f(x) \neq f(y)] = \frac{1}{2} - \frac{1}{2} \cdot \mathbf{E}_{x,\mu}[f(x)f(\mu \cdot x)]$$

Definition (ρ -stability)

The ρ -stability of a function f , denoted by $\text{Stab}_\rho(f)$, is defined as $\mathbf{E}_{x,\mu}[f(x)f(\mu \cdot x)]$. Here μ is defined as in the test.

PCP Theorem and Hardness of Approximation

MAX-CUT

Definition (ρ -stability)

The ρ -stability of a function f , denoted by $Stab_\rho(f)$, is defined as $\mathbf{E}_{x,\mu}[f(x)f(\mu \cdot x)]$. Here μ is defined as in the test.

- Intuitively, it captures how stable the function is to change.
- Larger value of $Stab_\rho$ indicate more stable functions.
- For constant functions $Stab_\rho(f) = 1$.
- For dictator functions $Stab_\rho(f) = \rho$.
- Fact: For any function f , $Stab_\rho(f) = \sum_{S \subseteq [m]} \hat{f}(S)^2 \cdot \rho^{|S|}$.
- For majority function MAJ , $\frac{1}{2} - \frac{1}{2} \cdot Stab_\rho(MAJ)$ approaches $\frac{\cos^{-1}(\rho)}{\pi}$ as m approaches infinity.
- What we want to show is that if a function f passes the test with probability at least $\frac{\cos^{-1}(\rho)}{\pi}$ for some $\epsilon > 0$, then f must be **similar to a dictator function**.

Definition (Influence of a variable)

For any function $f : \{-1, +1\}^m \rightarrow \{-1, +1\}$, the influence of a variable x_i is defined to be $Inf_i(f) = \Pr_{x \in \{-1, +1\}^m} [f(x) \neq f(x_1, \dots, x_{i-1}, -x_i, x_{i+1}, \dots, x_m)]$

PCP Theorem and Hardness of Approximation

MAX-CUT

Definition (ρ -stability)

The ρ -stability of a function f , denoted by $Stab_\rho(f)$, is defined as $\mathbf{E}_{x,\mu}[f(x)f(\mu \cdot x)]$. Here μ is defined as in the test.

- What we want to show is that if a function f passes the test with probability at least $\frac{\cos^{-1}(\rho)}{\pi}$ for some $\epsilon > 0$, then f must be **similar to a dictator function**.

Definition (Influence of a variable)

For any function $f : \{-1, +1\}^m \rightarrow \{-1, +1\}$, the influence of a variable x_i is defined to be $Inf_i(f) = \mathbf{Pr}_{x \in \{-1, +1\}^m} [f(x) \neq f(x_1, \dots, x_{i-1}, -x_i, x_{i+1}, \dots, x_m)]$

- What is $Inf_i(\text{parity}) = ?$
- What is $Inf_i(\chi_S) = ?$
- What is $Inf_i(\text{Maj}) = ?$

PCP Theorem and Hardness of Approximation

MAX-CUT

Definition (ρ -stability)

The ρ -stability of a function f , denoted by $Stab_\rho(f)$, is defined as $\mathbf{E}_{x,\mu}[f(x)f(\mu \cdot x)]$. Here μ is defined as in the test.

- What we want to show is that if a function f passes the test with probability at least $\frac{\cos^{-1}(\rho)}{\pi}$ for some $\epsilon > 0$, then f must be **similar to a dictator function**.

Definition (Influence of a variable)

For any function $f : \{-1, +1\}^m \rightarrow \{-1, +1\}$, the influence of a variable x_i is defined to be $Inf_i(f) = \mathbf{Pr}_{x \in \{-1, +1\}^m} [f(x) \neq f(x_1, \dots, x_{i-1}, -x_i, x_{i+1}, \dots, x_m)]$

- What is $Inf_i(\text{parity}) = ?$ **1**
- What is $Inf_i(\chi_S) = ?$ **1 if $i \in S$ and 0 otherwise**
- What is $Inf_i(\text{Maj}) = ?$ **$\theta(1/\sqrt{m})$**
- Fact: For any function f , $Inf_i(f) = \sum_{S: i \in S} \hat{f}(S)^2$.

Definition (Low-degree influence)

$$Inf_i^{\leq d}(f) = \sum_{S: i \in S, |S| \leq d} \hat{f}(S)^2.$$

PCP Theorem and Hardness of Approximation

MAX-CUT

Definition (ρ -stability)

The ρ -stability of a function f , denoted by $\text{Stab}_\rho(f)$, is defined as $\mathbf{E}_{x,\mu}[f(x)f(\mu \cdot x)]$. Here μ is defined as in the test.

- What we want to show is that if a function f passes the test with probability at least $\frac{\cos^{-1}(\rho)}{\pi}$ for some $\epsilon > 0$, then f must be **similar to a dictator function**.

Definition (Influence of a variable)

For any function $f : \{-1, +1\}^m \rightarrow \{-1, +1\}$, the influence of a variable x_i is defined to be $\text{Inf}_i(f) = \mathbf{Pr}_{x \in \{-1, +1\}^m} [f(x) \neq f(x_1, \dots, x_{i-1}, -x_i, x_{i+1}, \dots, x_m)]$

Definition (Low-degree influence)

$$\text{Inf}_i^{\leq d}(f) = \sum_{S: i \in S, |S| \leq d} \hat{f}(S)^2.$$

Theorem (Generalized Majority is Stablest Theorem)

For any $\rho \in (-1, 0)$ and $\epsilon > 0$, there exists $\tau > 0$ and $d \in \mathbb{N}$, such that if some function has $\text{Inf}_i^{\leq d}(f) < \tau$ for all $i \in [m]$, then

$$\frac{1}{2} - \frac{1}{2} \cdot \text{Stab}_\rho(f) < \frac{\cos^{-1}(\rho)}{\pi} + \epsilon.$$

PCP Theorem and Hardness of Approximation

MAX-CUT

Theorem

For every $\rho \in (-1, 0)$ and any $\epsilon > 0$, there is a some $\delta > 0$ such that there is a PCP for ULC_δ in which the verifier reads two bits of the proof and accepts if they are unequal and moreover the following holds:

- If L is a yes instance of ULC_δ , then the verifier accepts with probability at least $c \geq \frac{(1-\rho)}{2} - \epsilon$.
- If L is a no instance of ULC_δ , then the verifier accepts with probability at most $s < \frac{\cos^{-1}(\rho)}{\pi} + \epsilon$.

Proof.

- Consider the following PCP proof system for a given instance $(G = (V_1, V_2, E), \Sigma, \Pi)$ with $|\Sigma| = m$.
 - The proof of size $|V_1 \cup V_2| \times 2^m$ is interpreted as the concatenation of long codes for a labeling of vertices.
 - The verifier does the following two query test on the proof:
 - Pick a vertex $v \in V_1$ uniformly at random. Let f denote the function corresponding to v .
 - Pick two random edges (v, w) and (v, w') .
 - Let π and π' be the permutations corresponding to edges (v, w) and (v, w') .
 - Pick x uniformly at random and μ according to ρ -biased distribution and let $y = \mu \cdot x$.
 - Accept if $f(x \circ \pi) \neq f(y \circ \pi')$ else reject.

PCP Theorem and Hardness of Approximation

MAX-CUT

Proof.

- Consider the following PCP proof system for a given instance $(G = (V_1, V_2, E), \Sigma, \Pi)$ with $|\Sigma| = m$.
 - The proof of size $|V_1 \cup V_2| \times 2^m$ is interpreted as the concatenation of long codes for a labeling of vertices.
 - The verifier does the following two query test on the proof:
 - Pick a vertex $v \in V_1$ uniformly at random. Let f denote the function corresponding to v .
 - Pick two random edges (v, w) and (v, w') .
 - Let π and π' be the permutations corresponding to edges (v, w) and (v, w') .
 - Pick x uniformly at random and μ according to ρ -biased distribution and let $y = \mu \cdot x$.
 - Accept if $f(x \circ \pi) \neq f(y \circ \pi')$ else reject.
- Completeness: $\frac{1-\rho}{2} - \epsilon$.
- Soundness: $\frac{\cos^{-1}\rho}{\pi} + \epsilon$.

End