Dinur's Proof of the PCP Theorem

Tiernan Garsys, Lucas Peña, and Noam Zilberstein

November 29, 2014

The PCP Theorem

- The class NP is equivalent to the set of languages of problems that can be decided by a probabilistically checkable proof using $O(\log n)$ random bits and $O(1)$ query bits.

The PCP Theorem

- The class NP is equivalent to the set of languages of problems that can be decided by a probabilistically checkable proof using $O(\log n)$ random bits and $O(1)$ query bits.
- Let $\mathrm{PCP}_{\epsilon}[r, q, a]$ be the class of languages with a PCP using r random bits and q queries that each return a-bit responses. If $x \in L$, then the verifier will always accept, if $x \notin L$ then the verifier will accept with probability at most ϵ.

The PCP Theorem

- The class NP is equivalent to the set of languages of problems that can be decided by a probabilistically checkable proof using $O(\log n)$ random bits and $O(1)$ query bits.
- Let $\mathrm{PCP}_\epsilon[r, q, a]$ be the class of languages with a PCP using r random bits and q queries that each return a-bit responses. If $x \in L$, then the verifier will always accept, if $x \notin L$ then the verifier will accept with probability at most ϵ.
- Dinur presents a new proof that $\mathrm{NP} = \mathrm{PCP}_{\frac{1}{2}}[c \log n, q, 1]$ where c and q are constants.

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors
  - $\mathcal{C} = \{c_e : \Sigma^2 \mapsto \{0, 1\} \mid e \in E\}$ is a set of constraints

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors
  - $\mathcal{C} = \{c_e : \Sigma^2 \mapsto \{0, 1\} \mid e \in E\}$ is a set of constraints
- G is a YES instance of CG iff:

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors
  - $\mathcal{C} = \{c_e : \Sigma^2 \mapsto \{0,1\} \mid e \in E\}$ is a set of constraints
- G is a YES instance of CG iff:
  - $\exists\sigma : V \mapsto \Sigma$ such that $\forall(u, v) \in E,\ c_{(u,v)}(\sigma(u), \sigma(v)) = 1$

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors
  - $\mathcal{C} = \{c_e : \Sigma^2 \mapsto \{0, 1\} \mid e \in E\}$ is a set of constraints
- G is a YES instance of CG iff:
  - $\exists\sigma : V \mapsto \Sigma$ such that $\forall(u, v) \in E,\ c_{(u,v)}(\sigma(u), \sigma(v)) = 1$
- **Example:** 3-Coloring:

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors
  - $\mathcal{C} = \{c_e : \Sigma^2 \mapsto \{0, 1\} \mid e \in E\}$ is a set of constraints
- G is a YES instance of CG iff:
  - $\exists\sigma : V \mapsto \Sigma$ such that $\forall(u, v) \in E,\ c_{(u,v)}(\sigma(u), \sigma(v)) = 1$
- **Example:** 3-Coloring:
  - $\Sigma = \{\text{RED, GREEN, BLUE}\}$

Constraint Graph Definition

- Let $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ be a constraint graph (CG) where:
  - $\langle V, E\rangle$ is a directed graph
  - Σ is a constant size set of colors
  - $\mathcal{C} = \{c_e : \Sigma^2 \mapsto \{0, 1\} \mid e \in E\}$ is a set of constraints
- G is a YES instance of CG iff:
  - $\exists\sigma : V \mapsto \Sigma$ such that $\forall(u, v) \in E,\ c_{(u,v)}(\sigma(u), \sigma(v)) = 1$
- **Example:** 3-Coloring:
  - $\Sigma = \{\text{RED, GREEN, BLUE}\}$
  - $\forall(u, v) \in E$,

$$c_{(u,v)}(\sigma(u), \sigma(v)) = \begin{cases} 1, & \sigma(u) \neq \sigma(v) \\ 0, & \text{otherwise} \end{cases}$$

Hardness of Constraint Graphs

- Determining if a constraint graph is satisfiable is NP-complete

Hardness of Constraint Graphs

- Determining if a constraint graph is satisfiable is NP-complete
  - Reduction from k-Coloring

Hardness of Constraint Graphs

- Determining if a constraint graph is satisfiable is NP-complete
  - Reduction from k-Coloring
  - CG $\in$ NP. Coloring is the proof, verification complexity is linear in number of edges

Technical Overview

- Show that the following are equivalent:

Technical Overview

- Show that the following are equivalent:
  - Property 1: $\mathsf{NP} \subseteq \mathsf{PCP}_{1-\epsilon}[O(\log n), 2, 4]$

Technical Overview

- Show that the following are equivalent:
  - Property 1: NP $\subseteq$ $\mathrm{PCP}_{1-\epsilon}[O(\log n), 2, 4]$
  - Property 2: For any language $L \in$ NP there is a polynomial time transformation T from instances of L to a constraint graphs on 16 colors $\mathcal{G}_{16}$ such that if $x \in L$ then $\mathcal{G}_{16}$ is satisfiable and if $x \notin L$ then at most $(1-\epsilon)|E|$ of the constraints are simultaneously satisfiable

Technical Overview

- Show that the following are equivalent:
  - Property 1: $\mathrm{NP} \subseteq \mathrm{PCP}_{1-\epsilon}[O(\log n), 2, 4]$
  - Property 2: For any language $L \in \mathrm{NP}$ there is a polynomial time transformation T from instances of L to a constraint graphs on 16 colors $\mathcal{G}_{16}$ such that if $x \in L$ then $\mathcal{G}_{16}$ is satisfiable and if $x \notin L$ then at most $(1-\epsilon)|E|$ of the constraints are simultaneously satisfiable
- It will suffice to prove Property 2

Technical Overview

- Show that the following are equivalent:
  - Property 1: NP $\subseteq$ $\mathrm{PCP}_{1-\epsilon}[O(\log n), 2, 4]$
  - Property 2: For any language $L \in$ NP there is a polynomial time transformation T from instances of L to a constraint graphs on 16 colors $\mathcal{G}_{16}$ such that if $x \in L$ then $\mathcal{G}_{16}$ is satisfiable and if $x \notin L$ then at most $(1-\epsilon)|E|$ of the constraints are simultaneously satisfiable
- It will suffice to prove Property 2
- Boost the accuracy of the solution to show that NP$\subseteq$ $\mathrm{PCP}_{(1-\epsilon)^c}[O(\log n), 8c, 1]$

Regarding Expanders

- Edge expansion property for a graph $G = \langle V, E \rangle$:
  $\varphi(G) = \min_{|S| \leq \frac{n}{2}} \left\{ \frac{E(S, \bar{s})}{|S|} \right\}$ such that $S \subseteq V$.

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

- $|G'|$ is $\Theta(|G|)$

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

- $|G'|$ is $\Theta(|G|)$
- $\Sigma' = \Sigma$

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

- $|G'|$ is $\Theta(|G|)$
- $\Sigma' = \Sigma$
- If $\text{UNSAT}(G) = 0$ then $\text{UNSAT}(G') = 0$

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

- $|G'|$ is $\Theta(|G|)$
- $\Sigma' = \Sigma$
- If $\mathrm{UNSAT}(G) = 0$ then $\mathrm{UNSAT}(G') = 0$
- $\mathrm{UNSAT}(G') \geq 2 \min\{\mathrm{UNSAT}(G), \alpha\}$

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

- $|G'|$ is $\Theta(|G|)$
- $\Sigma' = \Sigma$
- If $\mathrm{UNSAT}(G) = 0$ then $\mathrm{UNSAT}(G') = 0$
- $\mathrm{UNSAT}(G') \geq 2\min\{\mathrm{UNSAT}(G), \alpha\}$

Step 1: Preprocessing

Convert G to a constant degree expander. Worsens $\mathrm{UNSAT}(G)$ by a constant factor, blows up $|G|$ by a constant factor

The Gap Amplification Lemma

Lemma: Gap Amplification

There exists a constant $0 < \alpha < 1$, an alphabet Σ, and a polynomial time reduction mapping the CG $G = \langle\langle V, E\rangle, \Sigma, \mathcal{C}\rangle$ to $G = \langle\langle V', E'\rangle, \Sigma', \mathcal{C}'\rangle$ such that:

- $|G'|$ is $\Theta(|G|)$
- $\Sigma' = \Sigma$
- If $\text{UNSAT}(G) = 0$ then $\text{UNSAT}(G') = 0$
- $\text{UNSAT}(G') \geq 2\min\{\text{UNSAT}(G), \alpha\}$

Step 1: Preprocessing

Convert G to a constant degree expander. Worsens $\text{UNSAT}(G)$ by a constant factor, blows up $|G|$ by a constant factor

Step 2: Power Step

Assuming that the degree of G is constant, we amplify $\text{UNSAT}(G)$ while blowing up $|G|$ and $|\Sigma|$ by a constant factor.

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0
- G is transformed as follows:

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0
- G is transformed as follows:
  - Each vertex $v \in V$ (with degree d_v) is replaced with expander graph G_{d_v} and each edge incident on v is assigned to a vertex in G_{d_v}.

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0
- G is transformed as follows:
  - Each vertex $v \in V$ (with degree d_v) is replaced with expander graph G_{d_v} and each edge incident on v is assigned to a vertex in G_{d_v}.
  - All edges in G_{d_v} have equality constraints. All other edges retain original constraints

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0
- G is transformed as follows:
  - Each vertex $v \in V$ (with degree d_v) is replaced with expander graph G_{d_v} and each edge incident on v is assigned to a vertex in G_{d_v}.
  - All edges in G_{d_v} have equality constraints. All other edges retain original constraints
  - Now, we have that $|V'| = \sum_{v \in V} d_v = 2|E|$ and $|E'| = frac(d+1)|V'|2 = (d+1)|E|$, so $|G'|$ is $\Theta(|G|)$.

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0
- G is transformed as follows:
  - Each vertex $v \in V$ (with degree d_v) is replaced with expander graph G_{d_v} and each edge incident on v is assigned to a vertex in G_{d_v}.
  - All edges in G_{d_v} have equality constraints. All other edges retain original constraints
  - Now, we have that $|V'| = \sum_{v \in V} d_v = 2|E|$ and $|E'| = frac(d+1)|V'|2 = (d+1)|E|$, so $|G'|$ is $\Theta(|G|)$.
  - If UNSAT$(G) = 0$, then $UNSAT(G') = 0$ by assigning each vertex in G_{d_v} to the color of v

The Gap Amplification Lemma

Step 1A

Convert G in to a constant degree graph

- Let G_n be a family of expander graphs of degree d and edge expansion at least φ_0
- G is transformed as follows:
  - Each vertex $v \in V$ (with degree d_v) is replaced with expander graph G_{d_v} and each edge incident on v is assigned to a vertex in G_{d_v}.
  - All edges in G_{d_v} have equality constraints. All other edges retain original constraints
  - Now, we have that $|V'| = \sum_{v \in V} d_v = 2|E|$ and $|E'| = frac(d+1)|V'|2 = (d+1)|E|$, so $|G'|$ is $\Theta(|G|)$.
  - If $\mathrm{UNSAT}(G) = 0$, then $UNSAT(G') = 0$ by assigning each vertex in G_{d_v} to the color of v
  - Now, we need to show that if $\mathrm{UNSAT}(G) \neq 0$, then $\mathrm{UNSAT}(G')$ is not much smaller

The Gap Amplification Lemma

Step 1A

If $\mathrm{UNSAT}(G) \neq 0$, then $\mathrm{UNSAT}(G')$ is not much smaller

The Gap Amplification Lemma

Step 1A

If UNSAT$(G) \neq 0$, then UNSAT(G') is not much smaller

- Let $\sigma' : V' \mapsto \Sigma$ be the best coloring for G'

The Gap Amplification Lemma

Step 1A

If $\text{UNSAT}(G) \neq 0$, then $\text{UNSAT}(G')$ is not much smaller

- Let $\sigma' : V' \mapsto \Sigma$ be the best coloring for G'
- We now obtain $\sigma : V \mapsto \Sigma$ where $\sigma(v)$ is the most popular color in $\{\sigma'(u) \mid u \in G_{d_v}\}$

The Gap Amplification Lemma

Step 1A

If UNSAT$(G) \neq 0$, then UNSAT(G') is not much smaller

- Let $\sigma' : V' \mapsto \Sigma$ be the best coloring for G'
- We now obtain $\sigma : V \mapsto \Sigma$ where $\sigma(v)$ is the most popular color in $\{\sigma'(u) \mid u \in G_{d_v}\}$
- Let $\mu =$UNSAT(G)

The Gap Amplification Lemma

Step 1A

If UNSAT$(G) \neq 0$, then UNSAT(G') is not much smaller

- Let $\sigma' : V' \mapsto \Sigma$ be the best coloring for G'
- We now obtain $\sigma : V \mapsto \Sigma$ where $\sigma(v)$ is the most popular color in $\{\sigma'(u) \mid u \in G_{d_v}\}$
- Let $\mu =$UNSAT(G)
- B is the set of edges violated by σ and B' is the set of edges violated by σ'

The Gap Amplification Lemma

Step 1A

If UNSAT$(G) \neq 0$, then UNSAT(G') is not much smaller

- Let $\sigma' : V' \mapsto \Sigma$ be the best coloring for G'
- We now obtain $\sigma : V \mapsto \Sigma$ where $\sigma(v)$ is the most popular color in $\{\sigma'(u) \mid u \in G_{d_v}\}$
- Let $\mu =$UNSAT(G)
- B is the set of edges violated by σ and B' is the set of edges violated by σ'
- $S = \{v \in V' \mid \sigma'(v)$ is not the popular color$\}$

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\mathrm{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\mathrm{UNSAT}(G)}{2(d+1)}$$

In both cases, since $\mathrm{UNSAT}(G')$ is optimal, we have proven that $\mathrm{UNSAT}(G) \leq k \cdot \mathrm{UNSAT}(G')$ for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$\mathrm{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\mathrm{UNSAT}(G)}{2(d+1)}$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

In both cases, since $\mathrm{UNSAT}(G')$ is optimal, we have proven that $\mathrm{UNSAT}(G) \leq k \cdot \mathrm{UNSAT}(G')$ for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\text{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\text{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'

In both cases, since UNSAT(G') is optimal, we have proven that UNSAT(G) $\leq k \cdot$UNSAT(G') for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\text{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\text{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'
- S^v = vertices in G_{d_v} that did not get the popular color

In both cases, since UNSAT(G') is optimal, we have proven that UNSAT(G) $\leq k \cdot$UNSAT(G') for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\mathrm{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\mathrm{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'
- $S^v =$ vertices in G_{d_v} that did not get the popular color
- $\forall a \in \Sigma$, $\Sigma_a^v = \{v \in \Sigma^v \mid \sigma'(v) = a\}$

In both cases, since $\mathrm{UNSAT}(G')$ is optimal, we have proven that $\mathrm{UNSAT}(G) \leq k \cdot \mathrm{UNSAT}(G')$ for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\text{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\text{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'
- $S^v =$ vertices in G_{d_v} that did not get the popular color
- $\forall a \in \Sigma$, $\Sigma_a^v = \{v \in \Sigma^v \mid \sigma'(v) = a\}$
- $|S_a^v| < \frac{d_v}{2}$

In both cases, since UNSAT(G') is optimal, we have proven that UNSAT(G) $\leq k \cdot$UNSAT(G') for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\mathrm{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\mathrm{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'
- S^v = vertices in G_{d_v} that did not get the popular color
- $\forall a \in \Sigma$, $\Sigma_a^v = \{v \in \Sigma^v \mid \sigma'(v) = a\}$
- $|S_a^v| < \frac{d_v}{2}$
- From the expansion property, $|E(S_a^v, \bar{S}_a^v)| \geq \varphi_0 |S_a^v|$

In both cases, since $\mathrm{UNSAT}(G')$ is optimal, we have proven that $\mathrm{UNSAT}(G) \leq k \cdot \mathrm{UNSAT}(G')$ for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\mathrm{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\mathrm{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'
- S^v = vertices in G_{d_v} that did not get the popular color
- $\forall a \in \Sigma$, $\Sigma_a^v = \{v \in \Sigma^v \mid \sigma'(v) = a\}$
- $|S_a^v| < \frac{d_v}{2}$
- From the expansion property, $|E(S_a^v, \bar{S}_a^v)| \geq \varphi_0 |S_a^v|$
- All edge constraints in $E(S_a^v, \bar{S}_a^v)$ are violated!

In both cases, since $\mathrm{UNSAT}(G')$ is optimal, we have proven that $\mathrm{UNSAT}(G) \leq k \cdot \mathrm{UNSAT}(G')$ for some constant k

The Gap Amplification Lemma

Case 1: $|B'| \geq \frac{\mu|E|}{2}$

$$\text{UNSAT}(G') = \frac{|B'|}{|E'|} \geq \frac{\mu|E|}{2|E'|} = \frac{\mu}{2(d+1)} = \frac{\text{UNSAT}(G)}{2(d+1)}$$

Case 2: $|S| \geq \frac{\mu|E|}{2}$

- Consider $v \in V$ and corresponding cloud G_{d_v} in G'
- S^v = vertices in G_{d_v} that did not get the popular color
- $\forall a \in \Sigma$, $\Sigma_a^v = \{v \in \Sigma^v \mid \sigma'(v) = a\}$
- $|S_a^v| < \frac{d_v}{2}$
- From the expansion property, $|E(S_a^v, \bar{S}_a^v)| \geq \varphi_0 |S_a^v|$
- All edge constraints in $E(S_a^v, \bar{S}_a^v)$ are violated!
- $|B'| \geq \frac{\sum |E(S_a^v, \bar{S}_a^v)|}{2} \geq \frac{\varphi_0 |S|}{2} \geq \frac{\mu\varphi_0}{4}|E| \geq \frac{\mu\varphi_0}{4(d+1)}|E'| = \text{UNSAT}(G)\frac{\varphi_0}{4(d=1)}$

In both cases, since UNSAT(G') is optimal, we have proven that UNSAT$(G) \leq k \cdot$UNSAT(G') for some constant k

The Gap Amplification Lemma

Step 1B

The Gap Amplification Lemma

Step 1B

- G' is $(d+1) - \textit{regular}$

The Gap Amplification Lemma

Step 1B

- G' is $(d+1)-$ *regular*
- Superimpose $\tilde{d}$-regular expander on $|V'|$ nodes

The Gap Amplification Lemma

Step 1B

- G' is $(d+1) - \textit{regular}$
- Superimpose $\tilde{d}$-regular expander on $|V'|$ nodes
- The new superimposed graph has the same vertex set as the original constraint graph, but its edges are the union of the 2 graphs (G' and the expander)

The Gap Amplification Lemma

Step 1B

- G' is $(d+1) - regular$
- Superimpose $\tilde{d}$-regular expander on $|V'|$ nodes
- The new superimposed graph has the same vertex set as the original constraint graph, but its edges are the union of the 2 graphs (G' and the expander)
- Add self-loops to each vertex to get G''

The Gap Amplification Lemma

Step 1B

- G' is $(d+1) - \textit{regular}$
- Superimpose $\tilde{d}$-regular expander on $|V'|$ nodes
- The new superimposed graph has the same vertex set as the original constraint graph, but its edges are the union of the 2 graphs (G' and the expander)
- Add self-loops to each vertex to get G''
- Impose dummy constraints on each new edge

The Gap Amplification Lemma

Step 1B

- G' is $(d+1) - regular$
- Superimpose $\tilde{d}$-regular expander on $|V'|$ nodes
- The new superimposed graph has the same vertex set as the original constraint graph, but its edges are the union of the 2 graphs (G' and the expander)
- Add self-loops to each vertex to get G''
- Impose dummy constraints on each new edge
- G'' is still an expander with constant degree $d + 2 + \tilde{d}$

The Gap Amplification Lemma

Step 1B

- G' is $(d+1) - \textit{regular}$
- Superimpose $\tilde{d}$-regular expander on $|V'|$ nodes
- The new superimposed graph has the same vertex set as the original constraint graph, but its edges are the union of the 2 graphs (G' and the expander)
- Add self-loops to each vertex to get G''
- Impose dummy constraints on each new edge
- G'' is still an expander with constant degree $d + 2 + \tilde{d}$
-

Main Lemma

Main Lemma

There exists as constant $\beta > 0$ such that if UNSAT$(G) \leq \frac{1}{t}$ then UNSAT$(G') \geq \beta\sqrt{t}UNSAT(G)$

Proof:

- Let $\sigma' : V \mapsto \Sigma'$ be the best coloring for G', hence $\alpha' =$UNSAT(G') is the fraction of walk constraints violated by σ'
- Let $\sigma : V \mapsto \Sigma$ be $\sigma(v) = \arg\max_{a \in \Sigma} \Pr[X_{v,t/2} = a]$ where $X_{v,i}$ is the opinion that a vertex has of v that is i random steps away from v
- If $\sigma(v) = a$ then $\Pr[X_{v,t/2} = a] \geq \frac{1}{\Sigma}$
- Let B be the set of edges that are violated by σ in G, then $\frac{|B|}{|E|} \geq$UNSAT$(G) = \alpha$

Proof of Main Lemma

We want to show that bad walks do not overlap very much

- Let w be a random t-walk in G', we now define the following random variable:

$$N = \begin{cases} \text{number of bad edges in } I & C_w \text{ is violated by } \sigma' \\ 0 & \text{otherwise} \end{cases}$$

- $\mathrm{UNSAT}(G') \geq \Pr[N > 0]$, we wish to lower bound $\Pr[N > 0]$
- Claim 1: $\exists \mu > 0$ such that $E[N] \geq \frac{2\mu\sqrt{t}|B|}{|E|}$
- Claim 2: $\exists C > 0$ such that $E[N^2] \leq \frac{C\sqrt{t}|B|}{|E|}$
- Chosing $\beta = \frac{4\mu^2}{C}$ completes the proof:

$$\begin{aligned} \Pr[N > 0] &\geq \frac{E[N]^2}{E[N^2]} \text{ (By the second moments inequality)} \\ &= \frac{\frac{4\mu^2 t|B|^2}{|E|^2}}{\frac{C\sqrt{t}|B|}{|E|}} = \frac{4\mu^2\sqrt{t}}{C}\frac{|B|}{|E|} \geq \beta \mathrm{UNSAT}(G)\sqrt{t} \end{aligned}$$

Proof of Claim 1

- For a random walk w, define 2 random variables:

$$Z_i = \begin{cases} 1, & i^{\text{th}} \text{ edge of } w \text{ is in } B \\ 0, & \text{otherwise} \end{cases}$$

$$Y_i = \begin{cases} 1, & w \text{ is a rejecting } t\text{-walk and } Z_i = 1 \\ 0, & \text{otherwise} \end{cases}$$

- Note: $\forall i, Y_i \leq Z_i$

Proof of Claim 1

- Let $N = \sum_{i \in I} Y_i$, then we have:

$$
\begin{aligned}
E[N] &= \sum_{i \in I} E[Y_i] \\
&= \sum_{i \in I} \Pr[Y_i = 1] \\
&= \sum_{i \in I} \Pr[Y_i = 1 \mid Z_i = 1] \Pr[Z_i = 1]
\end{aligned}
$$

We know that $\Pr[Z_i = 1] = \frac{|B|}{|E|}$ and $\Pr[Y_i = 1 \mid Z_i = 1] \geq \frac{\tau^2}{|\Sigma|^2} = \mu$, so we get:

$$
\begin{aligned}
&\geq \sum_{i \in I} \mu \frac{|B|}{|E|} \\
&= \frac{2\mu\sqrt{t}|B|}{|E|}
\end{aligned}
$$

Proof of Claim 2

- Since $Y_i \leq Z_i$, we know that $N \leq \sum_{i \in I} Z_i$, therefore:

$$
\begin{aligned}
E[N^2] &\leq E[(\sum_{i \in I} Z_i)^2] \\
&\leq 2 \sum_{i \in I} \sum_{j \geq i} E[Z_i Z_j] \\
&= 2 \sum_{i \in I} \Pr[Z_i = 1] \sum_{j \geq i} \Pr[Z_j = 1 \mid Z_i = 1] \\
&= 2 \frac{|B|}{|E|} \sum_{i \in I} \sum_{j \geq i} \underbrace{\Pr[Z_j = 1 \mid Z_i = 1]}_{\downarrow}
\end{aligned}
$$

Probability that a random walk has its $(j - i + 1)^{\text{th}}$ edge in B given that the first edge in the walk is in B

Proof of Claim 2

$$
\begin{aligned}
E[N^2] &\leq 2\frac{|B|}{|E|}\sum_{i\in I}\sum_{j\geq i}\Pr[Z_j = 1 \mid Z_i = 1] \\
&\leq 2\frac{|B|}{|E|}\sum_{i\in I}\sum_{j\geq i}\left(\frac{|B|}{|E|} + \lambda^{j-i}\right) \\
&\leq C\frac{|B|}{|E|}2\sqrt{t}\sqrt{t}\left(\frac{1}{\sqrt{t}}\right) \\
&\leq \frac{C\sqrt{t}|B|}{|E|}
\end{aligned}
$$