Håstad's 3-Bit PCP

Theorem NP has PCP verifier that

- uses $O(\log n)$ random bits
- 3 queries, linear predicate (over $\mathbb{F}_2$)
- $x \in L \Rightarrow \exists\, \pi \quad Pr[\text{Accept}] \geq 1-\varepsilon$

  $x \notin L \Rightarrow \forall\, \pi \quad Pr[\text{Accept}] \leq \frac{1}{2}+\varepsilon$

$\equiv$

Theorem Given 3-Lin instance S

$$\vdots$$
$$x \oplus y \oplus z = 0$$
$$x \oplus w \oplus u = 1$$
$$\vdots$$

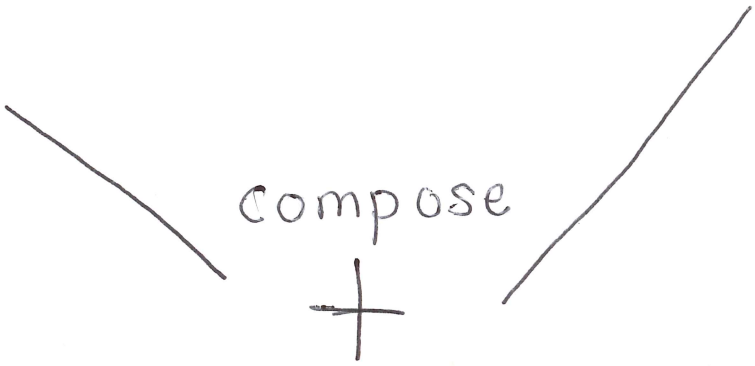
It is NP-hard to distinguish bet^n

(YES) $OPT(S') \geq 1-\varepsilon$

(NO) $OPT(S') \leq \frac{1}{2}+\varepsilon.$

- PCP Theorem (Gap3SAT)
- Label Cover
- Parallel Repetition Theorem

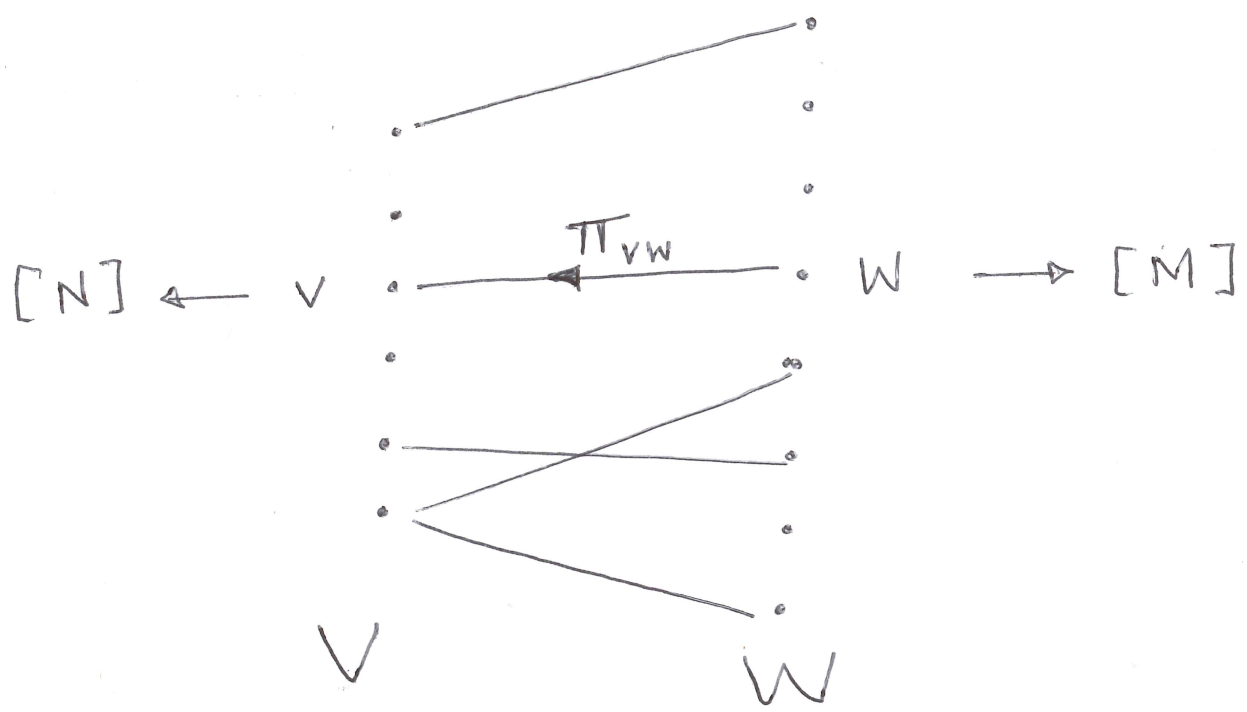
- $A: \{-1,1\}^n \to \{-1,1\}$
- Linearity Testing
- Dictatorship Testing



Håstad's 3-Bit PCP

Label Cover

$\mathcal{L}\left(G(V,W,E), [N], [M], \{\pi_{vw}\}_{(v,w)\in E}\right)$



- $\pi_{vw} : [M] \to [N]$. (projection).
- Labeling: $\ell : W \to [M]$, $\ell : V \to [N]$.
- Labeling ℓ "satisfies" edge (v,w) if

$$\pi_{vw}(\ell(w)) = \ell(v).$$

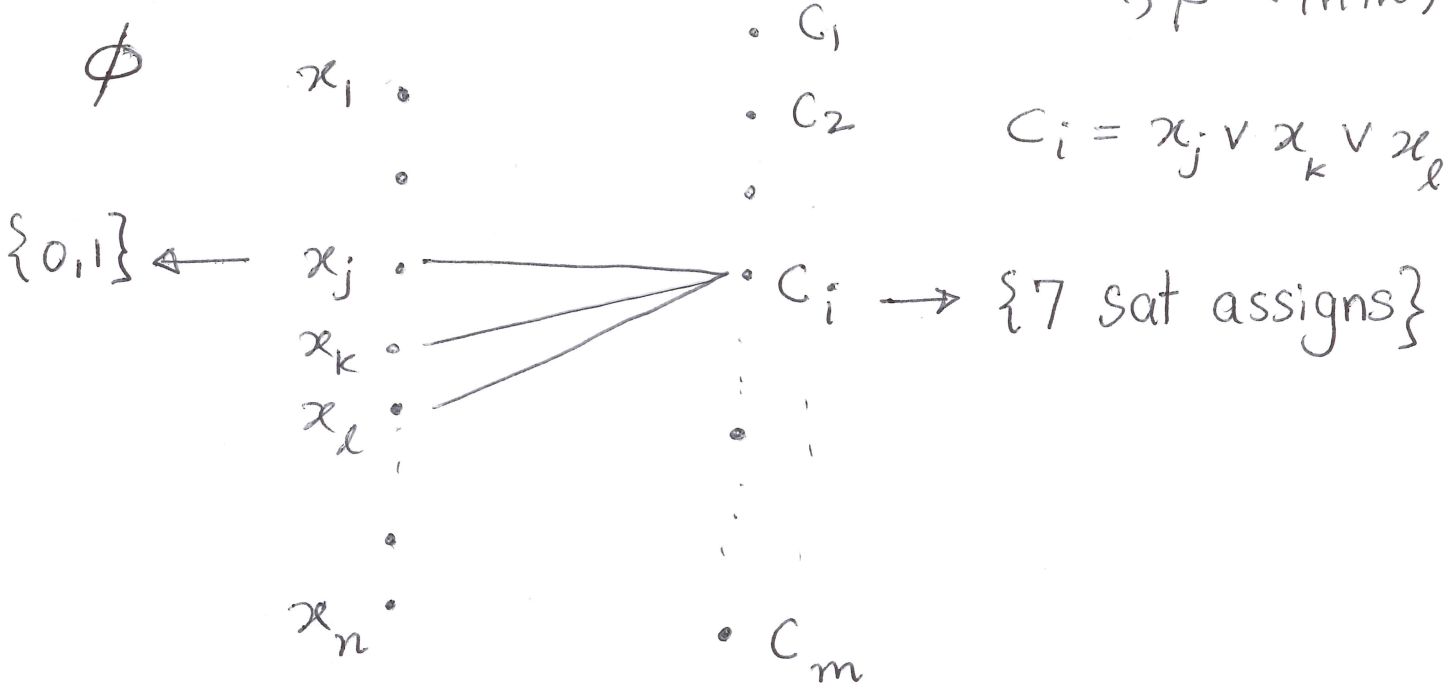
- Goal: Find a labeling that satisfies max fraction of edges. $\text{OPT}(\mathcal{L})$.

Theorem It is NP-hard to distinguish if $\mathcal{L}(G(V, W, E), [2], [7], \{\pi_{vw}\})$ has

(YES) $OPT(\mathcal{L}) = 1$ or

(NO) $OPT(\mathcal{L}) \leq \alpha$ $(\alpha < 1$, constant).

Proof Reduction from $Gap3SAT_{1,\beta}$ (PCP Thm).



- π_{x_j, C_i} maps assign to C_i to that to x_j.

- $OPT(\phi) = 1 \Rightarrow OPT(\mathcal{L}) = 1$.

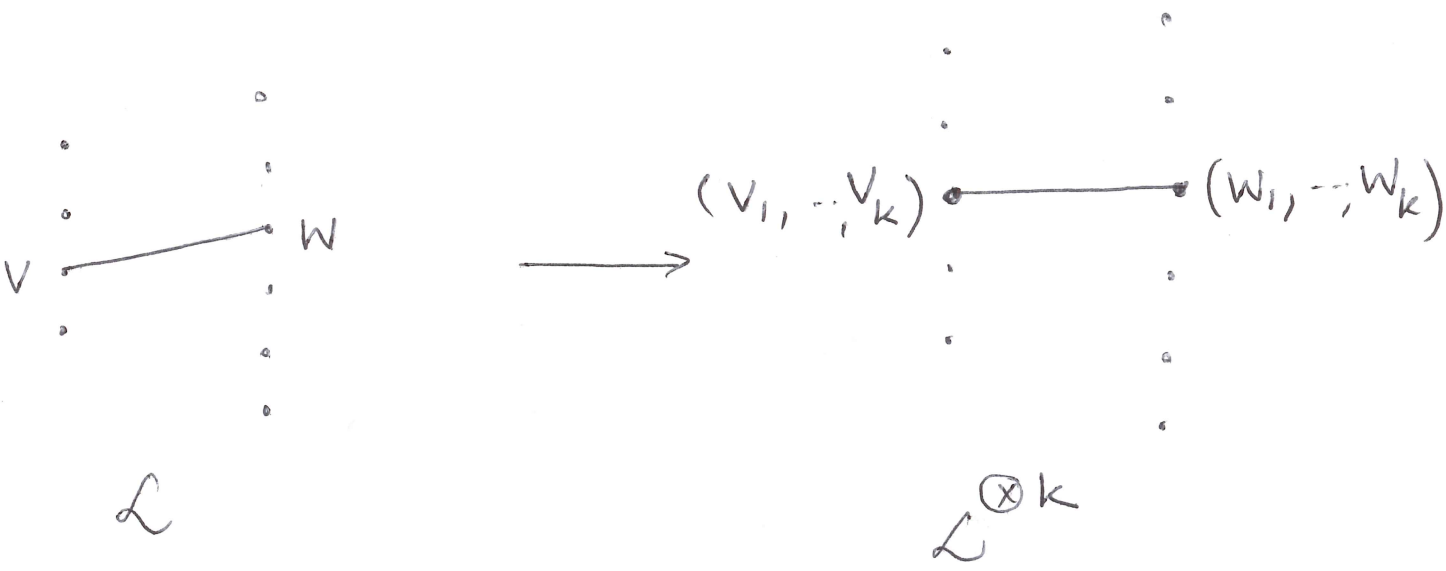
  $OPT(\phi) \leq \beta \Rightarrow OPT(\mathcal{L}) \leq 1 - \frac{1-\beta}{3} = \alpha$.

Parallel Repetition

$$\mathcal{L}\left(G(V,W,E),\ [N],\ [M],\ \{\pi_{vw}\}\right)$$

$$\downarrow$$

$$\mathcal{L}^{\otimes k} = \mathcal{L}'\left(G'(V',W',E'),\ [N'],\ [M'],\ \{\pi_{v'w'}\}\right)$$



- $OPT(\mathcal{L}) = 1 \Rightarrow OPT(\mathcal{L}^{\otimes k}) = 1$.
- [Raz]

  $OPT(\mathcal{L}) \leq \alpha \Rightarrow OPT(\mathcal{L}^{\otimes k}) \leq \tilde{\alpha}^k$.

  (if $\alpha < 1$ then $\tilde{\alpha} < 1$).

Label Cover Hardness

It is NP-hard to distinguish if

$\mathcal{L}(G(V, W, E), [N], [M], \{\pi_{vw}\})$ has

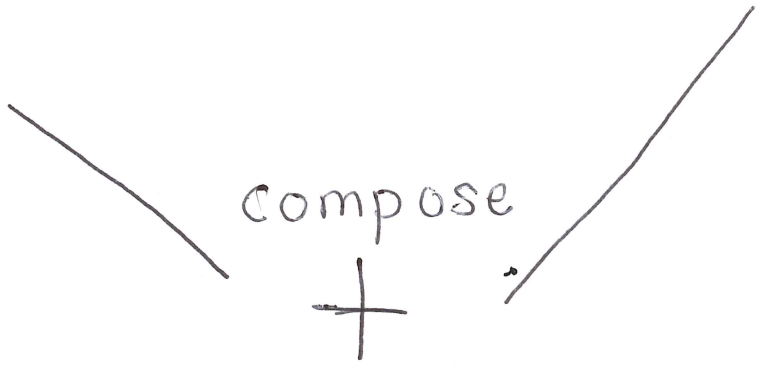
(YES) $\quad OPT(\mathcal{L}) = 1 \quad$ or

(NO) $\quad OPT(\mathcal{L}) \leq \varepsilon := 2^{-k}$.

Here, $|G| = n^{O(k)}$, N, M are $2^{O(k)}$.

- PCP Theorem (Gap3SAT)
- Label Cover
- Parallel Repetition Theorem

- $A: \{-1,1\}^n \to \{-1,1\}$
- Linearity Testing
- Dictatorship Testing



Håstad's 3-Bit PCP

Basics of Fourier Analysis

- 2^n-dim space of $A: \{-1,1\}^n \to \mathbb{R}$
- Mainly interested in Boolean, $A: \{-1,1\}^n \to \{-1,1\}$
- $A(x_1, x_2, \ldots, x_n)$, $x_i \in \{-1,1\}$, $x = (x_1, \ldots, x_n)$.

Def For $\alpha \subseteq [n]$, character $\chi_\alpha : \{-1,1\}^n \to \{-1,1\}$

$$\chi_\alpha(x) = \prod_{i \in \alpha} x_i .$$

$$\chi_\phi \equiv 1 .$$

Def $A, B : \{-1,1\}^n \to \mathbb{R}$.

$$\langle A, B \rangle = \mathop{\mathbb{E}}_{x} [A(x) B(x)] .$$

Def w.r.t. $\langle , \rangle$, $\{\chi_\alpha \mid \alpha \subseteq [n]\}$ forms an orthonormal basis.

Fact Every $A: \{-1,1\}^n \to \mathbb{R}$ can be written as

$$A(x) = \sum_{\alpha \subseteq [n]} \hat{A}_\alpha \chi_\alpha(x).$$

($\hat{A}_\alpha$: Fourier coefficients)

Fact $\hat{A}_\alpha = \langle A, \chi_\alpha \rangle$.

Fact $\sum_{\alpha \subseteq [n]} \hat{A}_\alpha^2 = 1$ if A is Boolean.

Def A, B Boolean. $\Delta(A,B) = \Pr_x [A(x) \neq B(x)]$.

Fact $\Delta(A, \chi_\alpha) = \frac{1}{2} - \frac{1}{2}\hat{A}_\alpha$.

Proof Next page.

$$\hat{A}_\alpha = \langle A, \chi_\alpha \rangle$$

$$= \mathop{\mathbb{E}}_{x} [A(x)\ \chi_\alpha(x)]$$

$$= \Pr_x [A(x) = \chi_\alpha(x)] - \Pr_x [A(x) \neq \chi_\alpha(x)]$$

$$= 1 - 2 \Pr_x [A(x) \neq \chi_\alpha(x)]$$

$$= 1 - 2\ \Delta(A, \chi_\alpha).$$

$$\therefore \quad \Delta(A, \chi_\alpha) = \frac{1}{2} - \frac{1}{2} \hat{A}_\alpha.$$

In particular,

$$\hat{A}_\alpha \to 1 \iff \Delta(A, \chi_\alpha) \to 0.$$