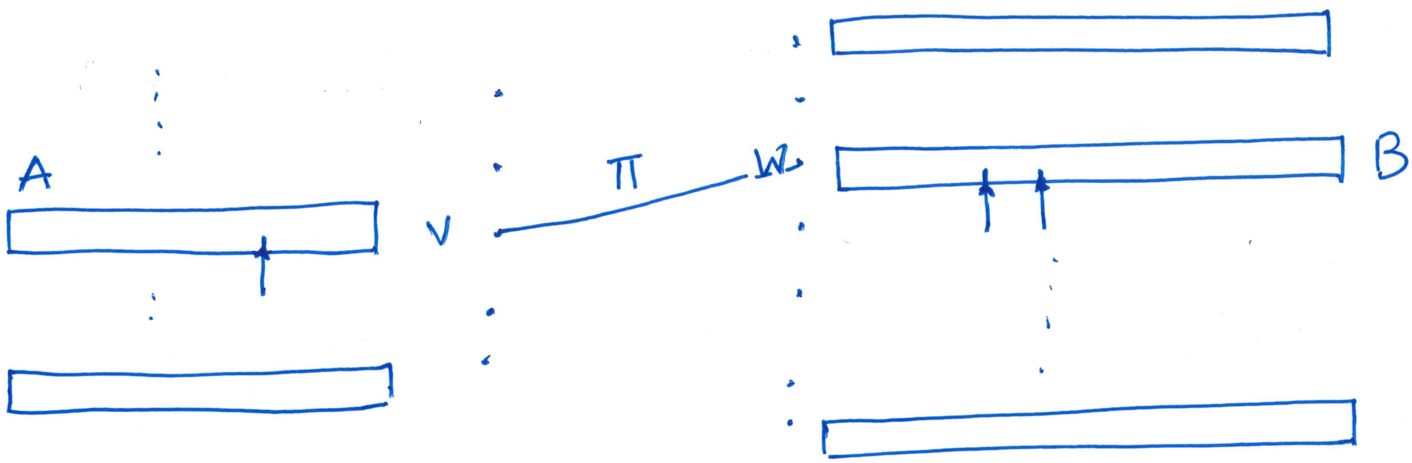
Håstad's 3-Bit PCP : Final Construction

$\text{Gap}_{1,\delta}$ $\mathcal{L}(G(V,W,E), [n], [m], \{\pi_{vw}\})$



$\pi : [m] \to [n]$.

→ Expect as a proof, $\forall\, v, w$

Long Code of $\ell(v)$ $\quad 1 \le \ell(v) \le n$

Long Code of $\ell(w)$ $\quad 1 \le \ell(w) \le m$.

- Test

  - Pick edge (v, w) at random. $\pi = \pi_{vw}$.
  - Let A = Supposed Long code of $\ell(v)$.
    B = Supposed Long Code of $\ell(w)$.
  - Run Consistency Test (A, B, π).
    (with noise ε).

Completeness
- $OPT(\mathcal{L}) = 1$.
- $l : V \to [n]$, $l : W \to [m]$ labeling.

- $\forall (v,w) \in E$,
  - $\pi(l(w)) = l(v)$
  - A, B be correct long codes.
  - $\Pr[\text{consistency test acc}] \geq 1-\varepsilon$.

Soundness If $\Pr[\text{verifier acc}] \geq \frac{1}{2} + \eta$ then we show that $\mathcal{L}$ has a labeling that satisfies $\Omega(\varepsilon^{1} \eta^{3} \log^{-1}(1/\eta))$ fraction of its edges. If $OPT(\mathcal{L}) \leq \delta \ll$, contradiction. (and hence $\Pr[\text{verifier accepts}] \leq \frac{1}{2} + \eta$.

Proof
- Suppose $\Pr[\text{verifier acc}] \geq \frac{1}{2} + \eta$
- By "averaging argument," for $\geq \frac{\eta}{2}$ fraction of edges (v,w),
  Consistency Test (A, B, π) accepts w.p. $\geq \frac{1}{2} + \frac{\eta}{2}$.

$\therefore$ For every such "good" edge

$$\sum_{\substack{\alpha \subseteq \pi(\beta) \\ |\beta| \leq \frac{1}{\varepsilon} \cdot \log(1/\eta)}} \hat{A}_\alpha^2 \hat{B}_\beta^2 \geqslant \frac{\eta^2}{4}. \quad \text{--- } (\#1)$$

consider the following labeling. (probabilistic).

For v: - Consider table A.

- Pick $\alpha \subseteq [n]$ w.p. $\hat{A}_\alpha^2$ $\left(\because \sum_\alpha \hat{A}_\alpha^2 = 1\right)$.

- Pick a random $i \in \alpha$.

For w:

- Consider table B.

- Pick $\beta \subseteq [m]$ w.p. $\hat{B}_\beta^2$ $\left(\because \sum_\beta \hat{B}_\beta^2 = 1\right)$.

- Pick a random $j \in \beta$.

Note: For a probabilistic labeling, there exists a deterministic one, as good as its expectation.

#1 implies that

- w.p. $\geq \frac{\eta^2}{4}$, $\alpha \subseteq \pi(\beta)$.

  $|\beta| \leq 1/\varepsilon \log(1/\eta)$.

- After picking $i_0 \in \alpha$ (as label), $\exists\, j_0 \in \beta$ s.t. $\pi(j_0) = i_0$

and $j_0 \in \beta$ (as label) is picked w.p. $\geq \varepsilon \log^{-1}(1/\eta)$.

$\therefore$ overall fraction of label cover edges satisfied is at least (in expectation)

$$\underbrace{\frac{\eta}{2}}_{(v,w)\text{ "good"}} \cdot \underbrace{\frac{\eta^2}{4}}_{\#1} \cdot \underbrace{\varepsilon \log^{-1}(1/\eta)}_{j_0 \in \beta \text{ picked.}},$$

i.e. at least $\Omega(\varepsilon\, \eta^3 \log^{-1}(1/\eta))$.

$\blacksquare$

Folding

- Note that we assumed that $\hat{A}_\alpha \neq 0$ only if $\alpha \neq \phi$.

- We can enforce the condition that

$$A(-x) = -A(x) \quad \forall\, x \in \{-1,1\}^n.$$

Such A is called "folded".

Effectively the bits / variables $A(-x)$, $A(x)$ are declared as negations of each other.

Exercise If A is folded (i.e. $A(-x) = -A(x)$)

then $\hat{A}_\alpha \neq 0 \implies |\alpha|$ is odd

(in particular $\alpha \neq \phi$).

Effectively some equations of form

$a \oplus b \oplus c = 0$ are turned into

$a \oplus b \oplus c = 1$. $\blacksquare$

To conclude

$\forall\ \varepsilon, \eta > 0$, (constant)

Given instance of 3 Lin

S :

$$\vdots$$
$$a \oplus b \oplus c = 1$$
$$b \oplus d \oplus e = 0$$
$$\vdots$$

it is NP-hard to distinguish if

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

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

Note: Imperfect completeness is necessary.

Corollary Gap $3SAT_{1-\varepsilon,\ \frac{7}{8}+\eta}$ is NP-hard.