LECTURE 20

Note Title

TODAY:

The PCP Landscape

- Basic Equivalences
- Structure of
  - Dinur's PCP
  - Raz PCP
  - Håstad PCP

Incomplete

Use with care!

Recall Defn.

PCP - adaptive queries $q(n)$ bits

tosses $r(n)$ coins

$x \in L \Rightarrow \exists \pi$ Accepts w.p. $\geq c(n)$

$x \notin L \Rightarrow \forall \pi$ Accepts w.p. $\leq s(n)$

$\Rightarrow L \in PCP_{c,s}[r, q]$

EQUIVALENCE 1

Non-adaptive vs. Adaptive

- $PCP_{c,s}[r,q] \subseteq$ non-adaptive $PCP_{c,s}[r, 2^q]$

  Easy: Just read all 2^q variables in decision tree.

- Gap (q vs. 2^q) Necessary?

  - No ... many strong PCPs non-adaptive
  - Difference is at most 1 or 2 addit. query bits!
  - Gap does exist (assuming $P \neq NP$)

    E.g. n.a. $PCP_{1,\frac{5}{8}}[O(\log n), 3] \subseteq P$

    while $NP \subseteq PCP_{1,\frac{1}{2}+\epsilon}[O(\log n), 3]$

Non-adaptive PCP ≡ Gen. Hypergraph Coloring

Gen. Hypergraph Coloring (t, k):

- Input = t-uniform hypergraph $G = (V, E)$

  + functions $\left\{ \Pi_e : [1 .. k]^t \to \{0,1\} \right\}_{e \in E}$

- Gap Gen. Hyp. Color $(t, k)_{c,s}$:

  Distinguish G s.t. $\text{UNSAT}(G) \leq 1 - c$

  from $\text{UNSAT}(G) \geq 1 - s$

Syntactically:

- Gap Gen. Hyp. Color $(t, k)_{c,s}$

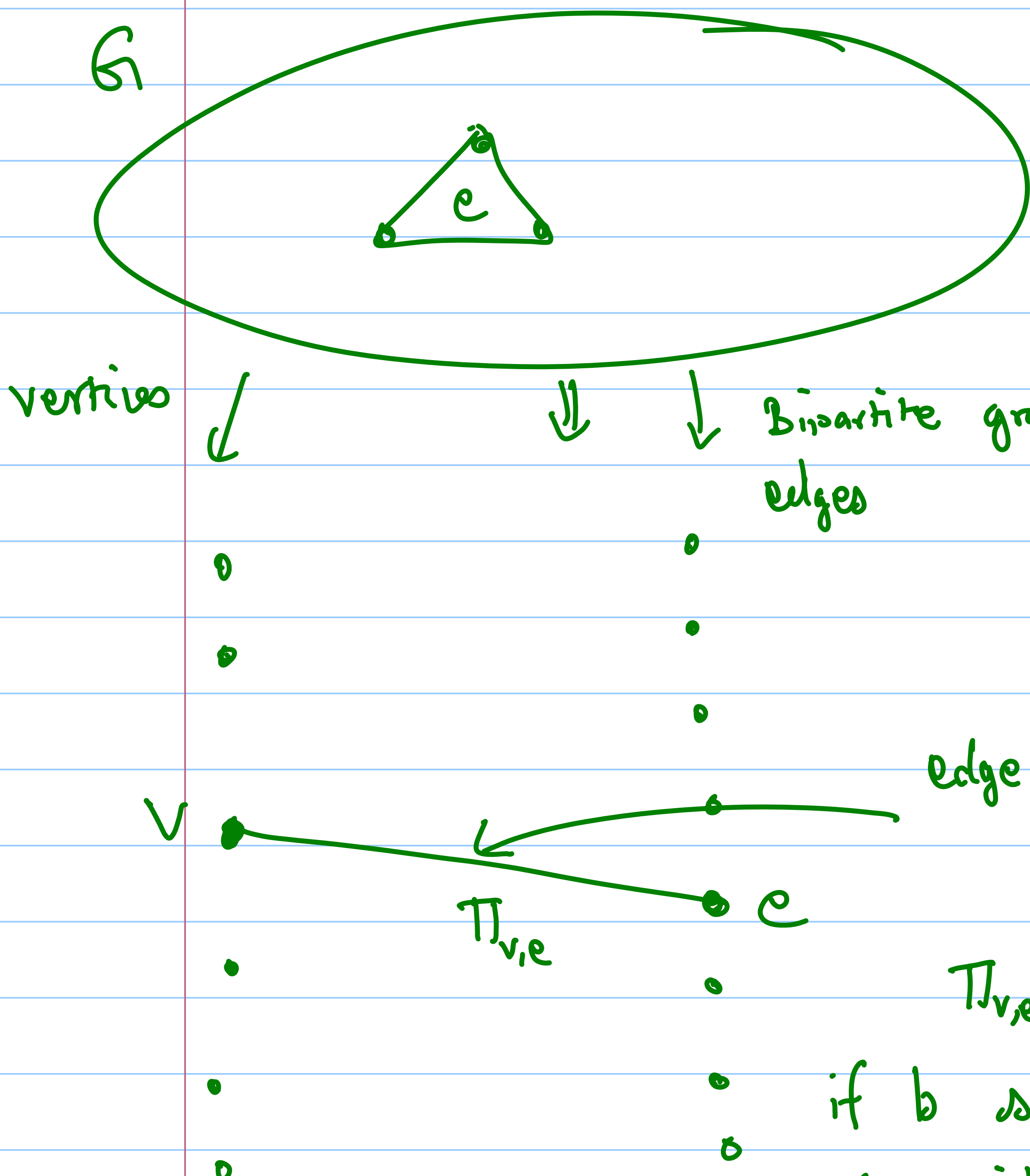
$$\in \text{PCP}_{c,s}\left[O(\log n),\ t \log k \right]$$

- $\text{PCP}_{c,s}\left[O(\log n), q \right] \leq \text{G.G.H.C}(q, 2)_{c,s}$

Gen. Hypergraph Coloring $\equiv$ Gen. Graph Coloring

$$\mathrm{GGHC}(t,k)_{1,s} \le \mathrm{GGGC}(k^t)_{1,\,1-\left(\frac{1-s}{t}\right)}$$

[Fortnow, Rompel, Sipser]



edge if e incident on v.

$\Pi_{v,e}(a,b) = 1$

if b satisfies Π_e, & consistent with a.

Analysis : Exercise !

Notes: Actually final graph is <u>bipartite</u> ; constraints are "<u>projections</u>".

(function from right side to left side)

<u>Aka</u>

MIP (2-prover 1-round Interactive Proofs)

Label Cover

Dinur's PCP

Linear-time (size) Reductions

1. $GGC(k) \longrightarrow GGC(K)$

$C \cdot UNSAT(G) \leq UNSAT(\tilde{G})$

$\forall C \; \exists K \; \ldots$

2. $GGC(K) \longrightarrow GGC(k)$

$\epsilon \cdot UNSAT(G) \leq UNSAT(\tilde{G})$

$\exists \epsilon$ s.t. $\forall K \; \ldots$

1. Won't see here ... "Amplification"
2. Based on Exp. PCP from last lecture ... will try one more today.

Parallel Repetition Theorem [Raz]

Bipartite $\text{GGC}_{c,s}(k) \leq$ Bipartite $\text{GGGC}_{c^t,(s')^t}(k^t)$

Quantifiers ? $\boxed{\forall k,\ s<1\ \exists\ s'<1 \text{ s.t. } \forall t}$

Reduction

$G \longrightarrow G^{\otimes t}$

- Vertices = t-tuples of $V(G)$
- $(u_1 \dots u_t) \longleftrightarrow (v_1 \dots v_t)$ if $u_i \leftrightarrow v_i$ in G $\forall i$,
- Constraints

$$\bigwedge_i \Pi_{(u_i,v_i)}$$

Analysis: Omitted.

Not an **exercise** !

Difference w.r.t Dinur's ①

① Dinur : Reduction is <u>linear-time</u>

Raz : Reduced instance is n^t-sized.

Dinur : s goes down to $1-\epsilon$ for some fixed $\epsilon = \epsilon(K)$

Raz : s goes down as $(s')^t$!

as small as we may want!

Getting {STRONG} PCPs [Håstad]

- Start with Weak PCP (say DINUR's)
- By equivalence : $GGGC_{1,1-\epsilon}(k)$
  Bipartite
- Apply [Raz]'s Parallel Repetition

  $\Leftrightarrow$ suffices to consider

$$GGGC_{1,\delta}(K)$$

bipartite, projection.

$$\Downarrow$$

- [Håstad]

$$GGHC_{1-\epsilon,\frac{1}{2}+\delta'}(\overset{t_1}{\overset{\shortparallel}{3}},\overset{k}{\overset{\shortparallel}{2}})$$

THE PCP THEOREM

(BY GAP AMPLIFICATION [DINUR '05])

Recall: PCP THEOREM (VIEW 2)

Generalized r-Graph k-coloring

Given: $G = (V, E, \text{valid} : E \times [k]^r \to \{0,1\})$

$$E \subseteq \underbrace{V \times V \times \dots V}_{r\text{-times}}$$

Goal: - accept G if G "k-colorable".

- reject G if "$\text{unsat}(G) \geq \epsilon$"

Definitions

- **Coloring** : $\mathcal{X} : V \to \{1 \dots k\}$
- $e = (v_1 \dots v_r)$ **Satisfied** by $\mathcal{X}$ if $\mathrm{valid}(e, \mathcal{X}(v_1), \dots, \mathcal{X}(v_r)) = 1$.
- G is **k-colorable** if $\exists\, \mathcal{X}$ s.t. $\forall e \in E$, e is satisfied by $\mathcal{X}$.
- $$\mathrm{Unsat}_{\mathcal{X}}(G) = \frac{|\{e \in E \mid e \text{ not satisfied by } \mathcal{X}\}|}{|E|}$$
- $$\mathrm{Unsat}(G) = \min_{\mathcal{X}} \{ \mathrm{unsat}_{\mathcal{X}}(G) \}$$

Reductions: $(k, r, \epsilon) \to (k', r', \epsilon')$

means $\exists$ linear time reduction T

r-graph $G \longrightarrow r'$-Graph G'

G k colorable $\Longrightarrow$ G' k'-colorable

$\text{unsat}(G) \geq \epsilon \Longrightarrow \text{unsat}(G') \geq \epsilon'$.

Easy Reductions (Complexity TQE):

(i) $(k, r, \epsilon) \longrightarrow (2, r\log k, \epsilon)$

(ii) $(k, r, \epsilon) \longrightarrow \left(k^r, 2, \frac{\epsilon}{r}\right)$ [FRS]

(iii) $(k, 2, \epsilon) \longrightarrow \left(3, 2, \frac{\epsilon}{f(k)}\right)$ [PY] [Petrank]

(iv) $(2, r, \epsilon) \to \left(2, 3, \frac{\epsilon}{r}\right)$ [Cook]

Problem with easy reductions

Gap always reduces.

One neo-classical reduction

(based on expander walks)

$$(V)\quad (k, r, \epsilon) \longrightarrow (k,\ c\cdot r,\ \sim \underset{\substack{\| \\ 1-(1-\epsilon)^c}}{\epsilon\cdot c})$$

Still:

$$\frac{\log k \times r}{\epsilon}$$ usually gets worse.

[DINUR]'s KEY INSIGHT

I. $(k, 2, \epsilon) \longrightarrow (K, 2, c \cdot \epsilon)$

Quantifiers are important! So ....

$\forall c, k, \exists K$ s.t. $\forall \epsilon(\cdot)$

$$(k, 2, \epsilon(\cdot)) \rightarrow (K, 2, c \cdot \epsilon(\cdot))$$

What? Why is this interesting?

"Observation"

II (Monday's lecture $\Longrightarrow$)

$\exists \delta \;\; \forall K$

$$(K, 2, \epsilon) \longrightarrow (2, 4, \epsilon \cdot \delta)$$

$\mathrm{I} + \mathrm{II} + (\mathrm{ii}) =$

III. $(16, 2, \epsilon) \longrightarrow (16, 2, 2\cdot\epsilon)$

Proof: Let δ be from II.

Set $C = \dfrac{8}{\delta}$,

Let K be as in I. $(R = 16)$

Then

$$(16, 2, \epsilon) \xrightarrow{\mathrm{I}} (K, 2, \epsilon\cdot C)$$

$$\xrightarrow{\mathrm{II}} (2, 4, \epsilon\cdot C\cdot\delta)$$

$$\xrightarrow{(\mathrm{ii})} (16, 2, 2\epsilon)$$

$\boxtimes$

Why does Monday's Lecture $\Rightarrow$ II ?

Informally:

- PCP more than just a proof.
- Commitment to a specific proof.
- i.e., not just "$\exists a$ s.t. $C(a)=1$"

  but "here's $\Pi(a) \approx \tilde{\Pi}$ s.t. $\tilde{\Pi}[Q] = Q(a)$

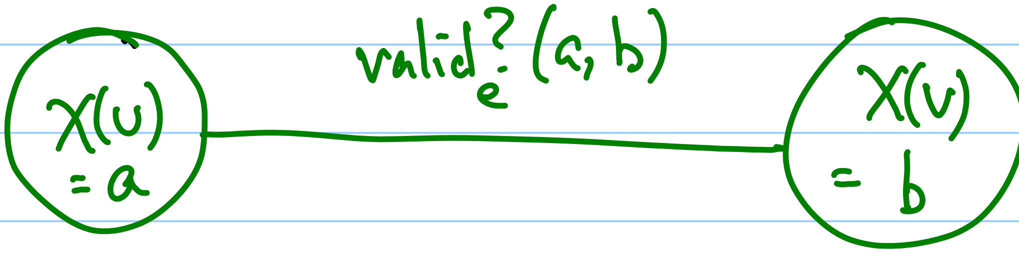
  s.t. $C(a) = 1$"

- Can extend to prove

  "here's $X(u)$, $X(v)$ s.t.

  $\text{valid}\left(X(u), X(v)\right) = 1$"

FORMALLY: PCP GADGET

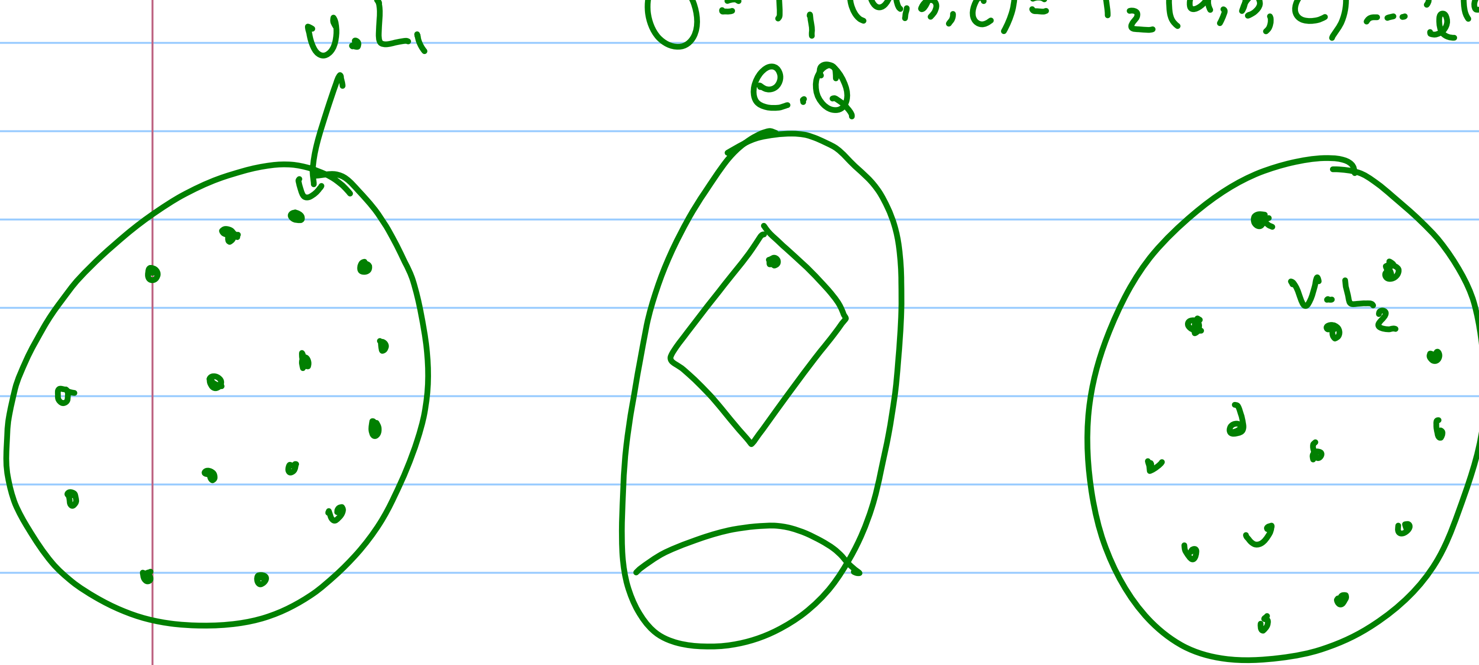


$$\exists \underbrace{P_1 \dots P_\ell}_{\text{degree } 2} (x_1 \dots x_k, y_1 \dots y_k, z_1 \dots z_t) \quad \text{s.t.}$$

$$\forall \; a = a_1 \dots a_k \;, \quad b = b_1 \dots b_k$$

$$\text{valid}_e(a,b) \iff \exists \; c_1 \dots c_t \quad \text{s.t.}$$

$$0 = P_1(a,b,c) = P_2(a,b,c) \dots P_\ell(a,b,c)$$



$L_1 = L_1(a)$ linear

$L_2 = L_2(b)$ linear

$Q = Q(a,b,c)$ quadratic

Constraints of type

I, II, III from last lecture

$$\begin{cases} \bullet\ \chi(e \cdot Q_1) + \chi(e \cdot Q_2) = \chi(e \cdot (Q_1 + Q_2)) \\ \bullet\ \quad \vdots \\ \bullet \\ \bullet \\ \bullet \end{cases}$$

Additionally

- $\chi(U \cdot L) = \chi(e \cdot Q) + \chi(e \cdot (Q + \tilde{L}))$

$[\tilde{L}(a,b,c) = L(a)]$

- All constraints on 4 Boolean colors.
- if 99% satisfied then
  - $\{X(v.L)\}_L$ uniquely close to $\{L(a)\}_L$
  - $\{X(v.L)\}_L$ uniquely close to $\{L(b)\}_L$
  - $\text{valid}_e(a,b) = 1$.

Yields II with

$$\boxed{\delta = \frac{1}{100}.}$$

Towards I

- How do you amplify errors?
- How do you amplify anything? (even (V))
- To get weak amplification with linear reduction [weak = increasing γ not k]:
  - Take random walk on G
  - Take conjunction of constraints on edges.
  - linear time if G is bounded degree.
  - [80's : AKS, CW, IZ]

    amplifies error if G expander.
  - ['88 : PY] can transform G into bounded degree (expander).

[Dinur]'s Construction

- Fix constant t
- Let $B_v = B_v^t = \{ u \mid \delta(u,v) \le t \text{ in } G \}$

length of shortest path.

- Reduces $G = (V, E, \text{valid})$

$$\Downarrow$$

$$G' = G'_t = (V', E', \text{valid}')$$

- $V' = V$
- $E' = \{ (u,v) \mid \exists\, \overset{u}{\overset{\shortparallel}{w_1}} \ldots \overset{v}{\overset{\shortparallel}{w_\ell}}$ s.t.

$(w_i, w_{i+1}) \in E$

$\frac{t}{2} \le \ell \le t \}$

multiset

- $\chi' : u \longmapsto \{ \chi_u : B_u \to \{1..k\} \}$

new coloring of u is a function giving old coloring to B_u (neighborhood of u).

- $\text{Valid}'(\chi_u, \chi_v)$

  if • $\forall\ w \in B_u \cap B_v$

  $\chi_u(w) = \chi_v(w)$ and

  • $\forall\ (w_1, w_2) \in E,\ w_1, w_2 \in B_u \cup B_v$

  $\text{Valid}_{w_1,w_2}\big(\chi_u(w_1), \chi_v(w_2)\big) = 1$.

- Analysis?
  - Technically simple variant of (V)
  - Conceptually brilliant!

III $\Rightarrow$ PCP Theorem ?

$$\underset{G_1}{\left(16, 2, \frac{1}{m}\right)} \Rightarrow \underset{G_2}{\left(16, 2, \frac{2}{m}\right)} \Rightarrow \vdots \quad G_3 \quad \Rightarrow \underset{G_{\log m}}{(16, 2, \epsilon)}$$

$\log m$ times

$$|G_i| = O(|G_{i-1}|) = c \cdot |G_{i-1}|$$

$$|G_{\log m}| = c^{\log m} |G| = m^{\log c} |G| .$$

$\boxtimes$

Conclusions

- Full proof of PCP Theorem
  - (i) BLR Theorem [.75 lectures]
  - (ii) Amplification Theorem [1.25 lectures]

- Remember consequences to Inapproximability
  - Given 3CNF formula, hard to find assgmt. satisfying $\left(\frac{7}{8}+\epsilon\right)$ fraction of clauses
    [PCP, ... , Håstad]

- Given n vertex graph with clique of size $n^{.99}$, can't find one of size $n^{.01}$.

- Given $n^{.01}$-colorable graph can't find $n^{.99}$-coloring.

- ... SET COVER

- MAX CUT

- VERTEX COVER

- Short vectors in lattices/codes

- TSP

⋮

(many important/hard questions)