CS221 LECTURE 19 4/3/2018

TODAY: PCP Theorem; Proof by Dinur

- Generalized Graph k-colorability
- Equivalence to PCP
- Main Lemma:
- Main "Sub-Lemmas" (2 of them)
- Proof of 2^{nd} Sub-Lemma

Recall $PCP_\epsilon[r, q] \ni L$ if $\exists V$ s.t.

V tosses $r(n)$ coins, queries $q(n)$ bit

$x \in L \Rightarrow \exists y$ s.t. $V^y(x)$ accepts w.p. 1

$x \notin L \Rightarrow \forall y$ $V^y(x)$ accepts w.p. $\leq 1-\epsilon$.

Gap_ϵ Generalized Graph k-Colorability:

Input: $G = (V, E)$ with functions $f_{uv} : [k] \times [k] \to \{0,1\}$ on edges

Goal: Distinguish • G s.t. G k colorable with $\forall (u,v) \in E$ $f_{uv}(X(u), X(v)) = 1$

• from "ϵ-unsat G" i.e., $\forall X$, $> \epsilon$-fraction of edges satisfy $f_{uv}(X(u), X(v)) = 0$.

Proposition: $PCP_{\epsilon}[O(\log n), q] \cong \epsilon$-Gen. Graph k-colorabitity

Proof: $\Rightarrow$ ϵ-Gen Graph $k$colorabity $\in PCP_{\epsilon}[O(\log n), 2\log k]$

PCP Proof: Write k-Coloring in bits

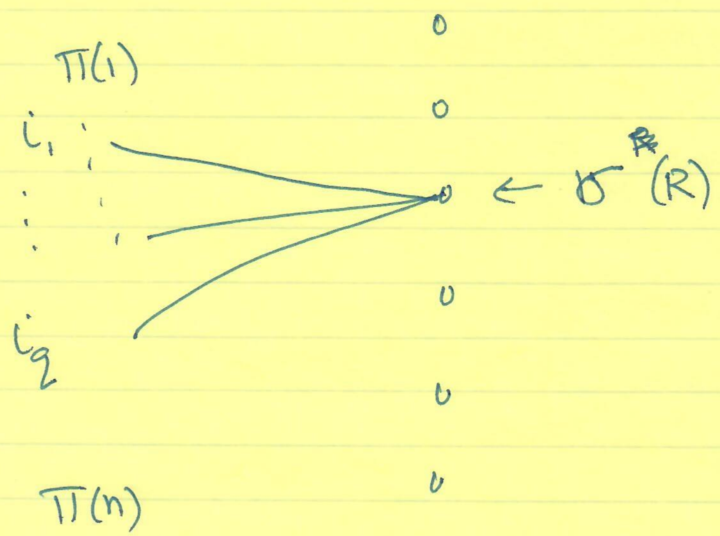
Verifier: Pick random edge $(u,v) \in E$ & Verify

$$f_{uv}(\underbrace{\chi(u)}_{k}, \underbrace{\chi(v)}_{q}) = 1$$

$2\log k$ queries

$\Leftarrow$ $PCP_{\epsilon}[O(\log n), q] \leq \Omega\left(\frac{\epsilon}{q}\right)$- Gen-graph-$2^q$-color...

Given Proof length n & # random string R, Graph is bipartite



- $\sigma(R) \longleftrightarrow i_j$ if on random string R, π_{i_j} is queried
- $f_{\sigma(R), i_j}(a, b) = 1$ if $a \in \{0,1\}^q$, $V^a(R)$ accepts, $b \in \{0,1\}$, & $a_j = b$.

Soundness analysis: Exercise

- Roughly coloring to left is a PCP proof.
- rejected w.p. ϵ
- if R is rejecting string, ~~Π~~ either $V^{a}(R)=0$ reject always
  or $\underbrace{a_j \neq \Pi_{i_j} \text{ for some } j}_{\text{reject w.p. } \frac{1}{2}}$.

Exercise 2: Reduce to GenGraph 3-coloring
~~In future will ans~~

Dinur's Theorem

$\exists$ reduction from ~~Gap Graph~~ Gap_0 Gen Graph 3-coloring (ϵ_0 & polytime)
to Gap_{ϵ_0} - Gen Grap 3-coloring

Dinur's Main Lemma

$\exists\ \epsilon_0, c$ & tranformation T, with $|T(G)| \leq c \cdot |G|$

s.t. G 3-colorable $\Longrightarrow$ $T(G)$ 3-colorable

G ϵ-unsat $\Longrightarrow$ $T(G)$ $\min\{2\epsilon, \epsilon_0\}$ unsat

Easy: Lemma $\Rightarrow$ Theorem

Given G with $|G| = n$, let $H = T^{(\log n)}(G)$

① G 3col $\Rightarrow T(G)$ 3col $\Rightarrow \ldots$ $T^{(\log n)}(G)$ 3col.

② G $\frac{1}{n}$-uncol $\Rightarrow T(G)$ $\frac{2}{n}$-uncol $\Rightarrow \ldots$ $T^{(\log n)}(G)$ - ϵ_0 uncol

③ $|T^{(\log n)}(G)| \leq C^{\log n} \cdot n \leq poly(n)$ $\boxtimes$

"Sub-Lemma's"

"Zig-Zag" Philosophy: Want to drive two parameters down simultaneously

Design 2 operations:

Op 1: Parameter 1 $\uparrow$, Parameter 2 $\downarrow$

Op 2: Parameter 2 $\downarrow$; Parameter 1 $\uparrow$

when is composition going to reduce both?

Ideal Setting

① $\exists f(c)$ s.t. $\forall c$ $OP1_c \rightarrow \left(f(c) \cdot P_1, \frac{P_2}{c}\right)$] OP1:

② $\exists D$ $\forall$ ~~c~~ f $OP2_f \rightarrow \left(\frac{P_1}{f}, D \cdot P_2\right)$] OP2:

[Compose ~~Op~~ right $OP2_{f(2D)/2} \circ OP_{1\,2D} \Rightarrow \left(\frac{P_1}{2}, \frac{P_2}{2}\right)$

In our case parameters : $P1 = \#$ colors

$P2 = $ "ϵ" (uncolorability)

<u>SubLemma 1</u> : [Amplification Theorem]

$\exists \epsilon_1 \; \forall c \; \exists f(c), C_1$ & tranformation T'_c s.t.

~~Gap Gen~~ ① $|T'_c(G)| \leq C_1 |G|$

② G 3-color $\Rightarrow$ $T'_c(G)$ $f(c)$- colorable

③ G ϵ-uncol $\Rightarrow$ $T'_c(G)$ $\min\{\epsilon_1, (c \cdot \epsilon)\}$- uncolor.

<u>SubLemma 2</u> : [Alphabet/Color Reduction]

$\exists \epsilon_2 \; \forall K \; \exists$ Transformation $T^2_{\epsilon_2, K}$ & const C_2 s.t.

① $|T^2_{\epsilon_2,K}(G)| \leq C_2 |G|$

② G K-color $\Rightarrow$ $T(G)$ 3-color

③ G ϵ-uncolor $\Rightarrow$ $T(G)$ $(\epsilon \cdot \epsilon_2)$- uncolor.

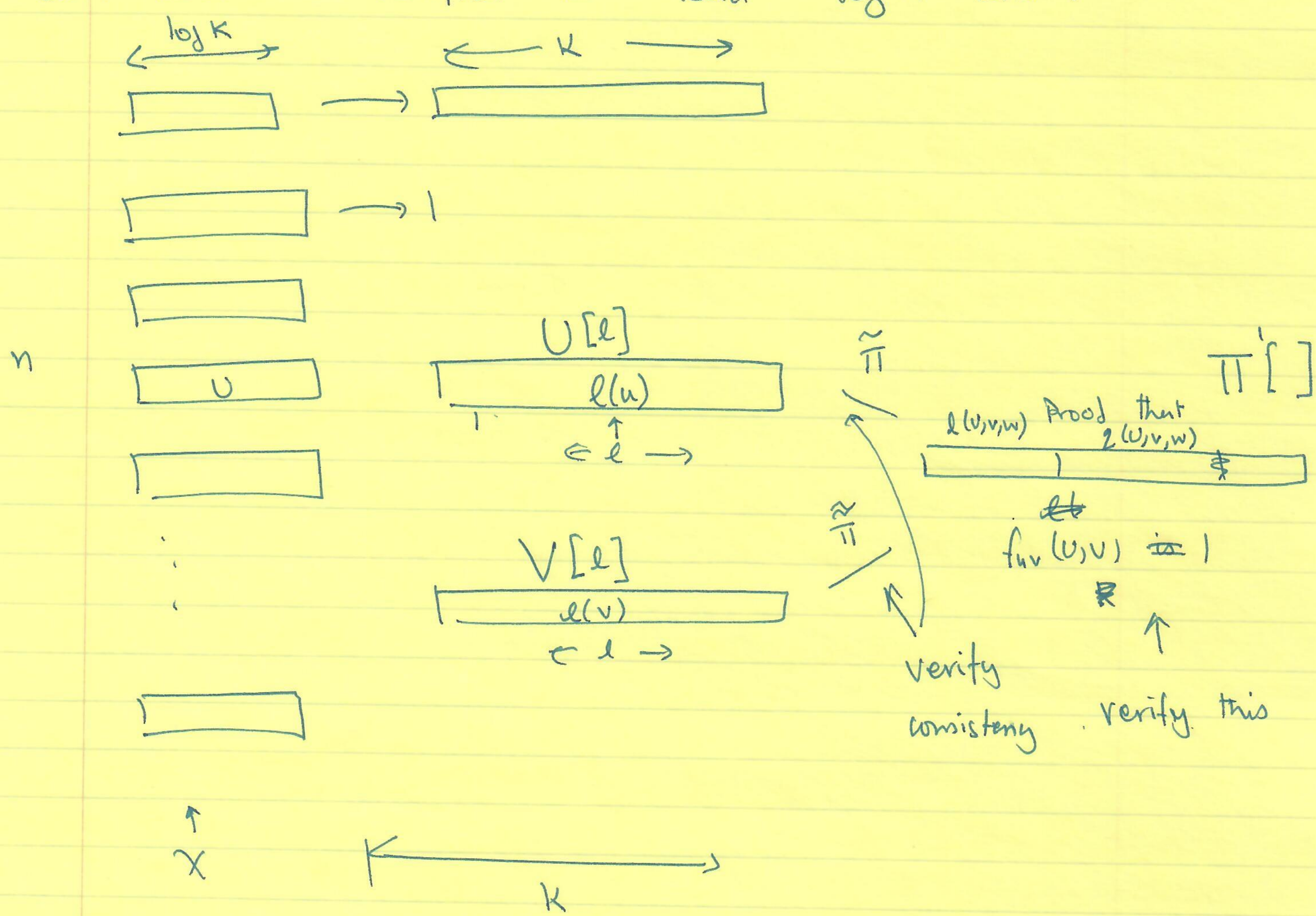
<u>Exercise</u> : Sub-lemmas $\Rightarrow$ Lemma

(sketch)

Proof of Sublemma 2

Uses PCP(poly(n), 8) from last lecture!

Idea: Want to prove G has K-coloring but Don't want ~~ver~~ verifier to read log K-bits.



all linear functions on X(v)
~~for~~ all v

Verify $U[\ell] = \Pi[R + \tilde{\ell}] - \Pi[R]$ etc.

$V[\ell] = \Pi[R + \tilde{\tilde{\ell}}] - \Pi[R]$.