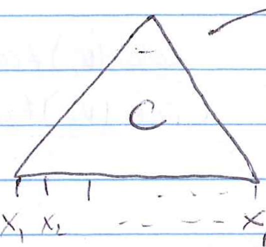
Lecture 25 - The PCP Theorem

[[Scribe]] (A proof sketch)

[[A gem in TCS. Orig. FGLSS/AS/ALMSS early '90s
Dinur '05: A new proof which is very short if you already have a lot of TCS tools in your back pocket. And we do! Didn't plan this for the course, but it recently occurred to me.]]

PCP Thm: $\exists\, \varepsilon_0 > 0$ s.t. $(1-\varepsilon_0, 1)$-approxing Max-3Sat is NP-hard.
[[Håstad: ε_0 can be any $\# < 1/8$. Needs many more tools. Our $\varepsilon_0 \approx 10^{-20}$ or something]]

[[more prec.]] [[De-Morgan]] [[canonical Cook-Levin NP-hard prob]]
CIRCUIT-SAT $\xrightarrow{\text{poly(n)-time alg } R}$ Max-3Sat.



size n [[#bits to write]], $n' \le n$

$\mathcal{C} = R(C)$

$y_1 \vee y_3 \vee y_{10}$
$\bar{y}_2 \vee \bar{y}_{18} \vee y_N$ (*)
$\vdots$

$m = \text{poly}(n)$ constrs

thm: • $\exists$ asgn to x's sating C $\Rightarrow$ $\exists$ asgn to y's sating all clauses of $\mathcal{C}$

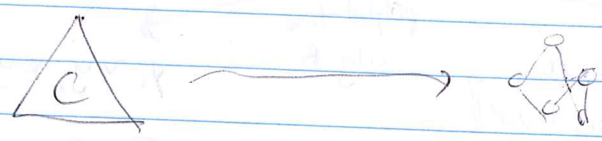
• $\nexists$ ~~~~~~ $\Rightarrow$ every asgn to y's falsifies $> \varepsilon_0$ frac. of clauses.

[[Why cool?]] "Proofs viewpoint": Can verify NP statements w.h.p. while only looking at $O(1)$ bits of a proof.

[[Merlin: "Hey Arthur, check out this ckt C. It's satisfiable!"
Arthur: "Oh yeah? Prove it." Merlin: "Sure, here's a sat. asgn for x's."
Arthur: "I'm feeling lazy today. Give me a sat asgn for y's instead."
Merlin: "Okay. Here, I wrote it on this piece of paper."
Arthur: *Picks one of the m constrs of $\mathcal{C}$ at random*, say (*).
"Hmm, I'll read your asgn just to y_2, y_{18}, y_N.
Hmm, $\bar{y}_2 \vee \bar{y}_{18} \vee y_N$ checks out. I guess C was sat'ble."
"Wait, maybe I was cheated. Well I'll just do $O(1/\varepsilon_0)$ more spot-checks"

rem: The $\varepsilon_0 = 0$ (or $\varepsilon_0 = \frac{1}{2m} = \frac{1}{\mathrm{poly}(n)}$) case is just NP-hardness of 3-Sat
↳ its proof: • Some of the y's can be x's. ⟶ [[ℓ contains the usual "proof"]]
• Rest ("auxiliary vbls") can be C's gate values
• Encode gate consist., "output = 1" as 3Sat constrs.

rem: Nothing special abt. 3Sat in PCP Thm. Any NP-hard CSP w/ $\boxed{\text{const. arity / domain}}$ is OK. [[ε_0 changes.]]
[[3 / 2 for 3Sat]]
Say [[2 / 3]] PCP Thm. proved with 3-Coloring [[3-Col]].



= color(v_1) ≠ color(v_5)
color(v_3) ≠ color(v_4)
⋮

"gadget"
encode v_i with 2 y's
R ⟶ 00
G ⟶ 01
B ⟶ 10.
encode constrs w/ ~~8~~ 4CNFs.
3 aux vbls, some 8 3CNFs.

[[Every coloring blows $\geq \varepsilon_0$ frac of edges
⟹ in each, at least 1/8 3CNFs violated]]

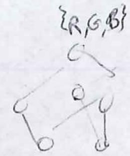
$\boxed{\varepsilon_0 \to \frac{\varepsilon_0}{8}}$

[[rem: And v.v.: 3Sat → 3col]]

[[On to proof.]]

def: Let $\mathcal{G}$ be an arity-2 CSP. $\underline{\mathrm{unsat}}(\mathcal{G})$:= frac. of constrs. violated by $\underline{\text{best}}$ asgn to $\mathcal{G}$.

[[only kind we'll consider, hence "$\mathcal{G}$" b/c like graph]]



$\exists\, \varepsilon_0 > 0,\ K < \infty$

Dinur thm: $\exists$ poly-time alg R mapping $\mathcal{G} \longrightarrow \mathcal{G}'$

$\mathcal{G}$: arity 2, domain $|\Omega| = 3$

s.t.: • $\text{size}(\mathcal{G}') \le K \cdot \text{size}(\mathcal{G})$ [[size = # bits]]

• if $\text{unsat}(\mathcal{G}) \le \varepsilon_0$ then $\text{unsat}(\mathcal{G}') \ge 2\,\text{unsat}(\mathcal{G})$

PCP Thm cor:

$$\underset{\text{size } n}{\overset{\text{Ckt-Sat}}{C}} \longrightarrow \overset{\text{3 Coloring}}{G_0} \xrightarrow[\log N \text{ times}]{\text{apply } R} \mathcal{H}$$

size n		size $N = \text{poly}(n)$		size $K^{\log N} \cdot N = \text{poly}(n)$
sat'ble	$\Rightarrow$	$\text{unsat}(G_0) = 0$	$\longrightarrow$	$\text{unsat}(\mathcal{H}) = 0$
un ~	$\Rightarrow$	$\text{unsat}(G_0) \ge \frac{1}{N}$	$\longrightarrow$	$\text{unsat}(\mathcal{H}) > \varepsilon_0$.

$\downarrow$ gadget to 3Sat if you wish.

[[Remark: R does not "know" unsat vals
But "spreads out the difficulty".]]

Dinur pf: R:
1. Degree Reduce } trivial
2. Expanderize } trivial
3. Power_t $\leftarrow$ innovative
4. Mini-PCP $\leftarrow$ " but prev. known.

Skipping: use a PCP(P) ~~[illegible]~~ But OK to have doubly expon cxty!: applied to const size constrs.
Tools: codes + Fourier analysis (Arrow's Thm!)

$\mathcal{G} \to \mathcal{G}'$

① Makes underlying graph of $\mathcal{G}'$ deg. 4.

side effects: • $\text{size}' \le K_1 \cdot \text{size}$.
• $|\Omega'| = 3$ [[but intros eq constraint]]
• $\text{unsat}(\mathcal{G}) = 0 \Rightarrow \text{unsat}(\mathcal{G}') = 0$: (all steps have this ppty)
• $\text{unsat}(\mathcal{G}') \ge \dfrac{\text{unsat}(\mathcal{G})}{C_1}$ $\leftarrow$ const. [[uh-oh, wrong way...]]

② Makes underlying graph a good 8-regular expander.
side effects: same

3 Increases unsat:

For any fixed t: • $\text{size}' \le 2^{O(t)}\ \text{size}$

• $|\Omega'| \approx 3^{8^t}$ [[!] [enormous domain, weird constrs]]

(weird 2-vbl constrs on huge domain)

• $\text{unsat}' \geq \frac{t}{c_2}\ \text{unsat}$ if $\text{unsat} \le \varepsilon_0$. ☺

$c_2 \leftarrow$ const.

4 Reduces domain size.

~~side effects~~

$|\Omega'| = 3$. $\text{size}' \le 2^{2^{2^{O(t)}}} \cdot \text{size}$

$\text{unsat}' \geq \frac{\text{unsat}}{c_3}$.

Put together: $\text{size}'''' \le 2^{2^{2^{O(t)}}}\ \text{size}$

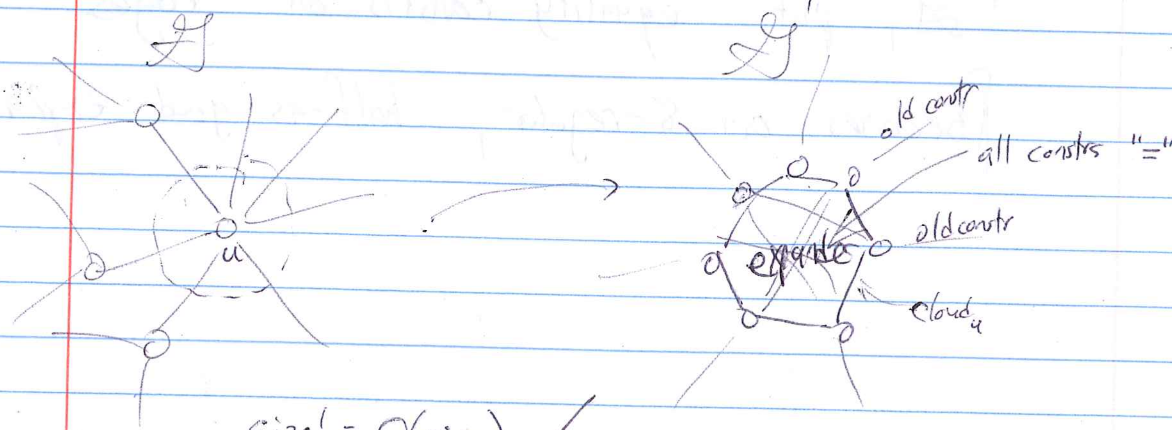
$|\Omega''''| = 3$

$\text{unsat}'''' \geq \frac{t}{c_1^2 c_2 c_3}\ \text{unsat}$ if $\text{unsat} \le \varepsilon_0$.

Take $t = 2c_1^2 c_2 c_3 = O(1)$. ☺

$\square$

1 (Sketch) [[Replacement of each vtx by 3-reg. expander]]



size$'$ = O(size) ✓

unsat = 0 ⇒ unsat$'$ = 0 ✓ [[label everything in cloud by "correct" label]]

$\text{unsat}' \geq \frac{\text{unsat}}{O(1)}$?

Let A' be best asgn for $\mathcal{G}'$: gets $\varepsilon := \text{unsat}'$ frac. of constrs wrong. Define A for $\mathcal{G}$ by letting $A(u) = \text{plur}(A'(\text{cloud}_u))$

~~[illegible]~~

A must violate $\geq \text{unsat}(\mathcal{G})$ frac of constrs in $\mathcal{G}$.
For each constr (u', v') in $\mathcal{G}'$ either it's viol'd by A' or u' or v' gets a minority label for its cloud.
⇒ $\Omega(\text{unsat})$ viol'd intercloud edges in $\mathcal{G}'$
or $\Omega(\text{unsat})$ frac. of vertices in $\mathcal{G}'$ have A'-minority labels

$\underset{\text{expansion}}{\Longrightarrow}$ $\Omega(\text{unsat})$ frac. of intra-cloud equal. constrs violated by A'!

[[Remark: only reason to use an expander here and not a random graph is so that the overall NP-hardness reduction is det'ic.
But not a huge deal to me to use a randomized reduction. Implies $(1-\varepsilon_0, 1)$-approx Max-3Sat $\in$ P ⇒ NP ⊆ RP. Good enough for me, Clay.]]

② Expanderize: Slap a ~~constant degree~~ ~~4~~ 3-regular expander on $\mathcal{G}$, put equality constrs on edges.

[Becomes an 8-regular, half-as-good expander]

(3) **Powering$_t$** [Sketch]

Input: $\mathcal{G}$ ← arity-2, domain $|\Omega| = 3$, 8-regular expander.

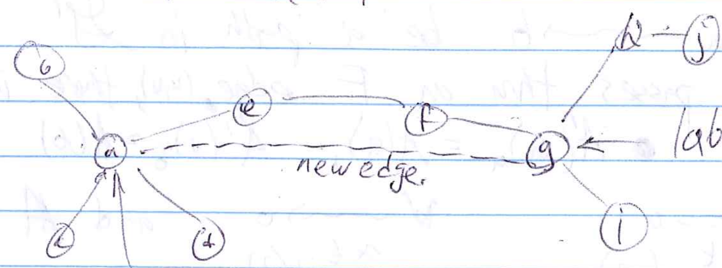
$\mathcal{G}'$: variable/vtx set: same as $\mathcal{G}$.

: edges/constrs in $\mathcal{G}'$ ≡ (lazy) paths of length ≈ t in $\mathcal{G}$.

↳ new degree $\approx 8^t$

: new domain: $\Omega' = \Omega^{1+8+8^2+\dots+8^t}$ (size 3^{8^t})

We think of a label to $u' \in \mathcal{G}'$ as giving an "opinion" label (R, G, B color) to its old dist ≤ t nbrs



labeled by "g ↦ R
h ↦ B
f ↦ G
e ↦ R
j ↦ B
i ↦ G
a ↦ B" ∈ Ω'

($t=3$)

labeled by "a ↦ R
b ↦ G
c ↦ G
d ↦ R
e ↦ B
f ↦ B
g ↦ B" ∈ Ω'

Constraints: between path endpts:

"test everything".

In partic, for each edge (u,v) on a path (a,g) (edge in $\mathcal{G}'$) test that "a's color opinion for u, together with g's color opinion for v satisfies the old (u,v) constr in $\mathcal{G}$"

- $\text{size}' \le 2^{O(t)}\ \text{size}$ ✓

unsat' ?? Sketch...

Let A' be best asgnment for $\mathcal{G}'$. Write $\underbrace{A'(w)_v}_{\text{of } v\text{'s color}}$ $\in \Omega$ for w's "opinion"
Define asgn A for $\mathcal{G}$ as follows:

$$A(v) = \underset{w:\ \text{dist}(w) \approx t}{\text{plurality}} \{A'(w)_v\}.$$

A violates $\geq \varepsilon := \min(\text{unsat}, \varepsilon_0 := \frac{1}{t})$ frac. of $\mathcal{G}$ constrs.
Let F be the edges of $\mathcal{G}$ it violates.
Goal: A' viols about $\Omega(t)$ frac. of ~~edg~~ path constrs in $\mathcal{G}'$.

Let $a \rightsquigarrow b$ be a path in $\mathcal{G}'$.
If it passes thru an F edge, (u,v), there is $\overset{\approx \frac{1}{q}}{(\text{"const."})}$ chance that $A'(u)_a = A(a)$, $A'(v)_b = A(b)$ because

$a \xleftarrow[\approx t\ (/2)]{} u \qquad v \xrightarrow[\approx t\ (/2)]{} b$ and A does plurality vote.

This $\Rightarrow$ A' violates the path constr. on $a \rightsquigarrow b$.

"$\therefore$" $\text{unsat}' \gtrsim \frac{1}{q} \cdot \underbrace{\{\text{Frac of paths passing thru } F\}}$

- F is an unsat frac. of G's edges
- path of len $\approx t$
- $\mathcal{G}$ is an expander so edges are $\approx$ "randomly" distrib.
- Prob path misses F $\approx (1-\text{unsat})^t \approx 1 - \text{unsat}\, t$

$\Rightarrow$ Frac of paths hitting F $\approx t \cdot \text{unsat}$.

$\square$