Note Title 11/30/2015

Lecture Notes on PCP

Today

PCP & Inapproximability

"Inapproximability Result"

Thm: [Håstad '97]:
MAX 3SAT is hard to approximate to within $\frac{7}{8}+\epsilon$.

$$\Uparrow$$

Lemma: $\exists$ polytime reduction T s.t.

G 3-colorable $\Rightarrow T(G) = C_1, C_2 \ldots C_m$
all C_i satisfiable

G not 3-colorable $\Rightarrow T(G) = C_1 \ldots C_m$
any assgnt sat.
$\leq \left(\frac{7}{8}+\epsilon\right) m$ clauses.

T = "gap-creating reduction"

Most Inapprox. Results use "gap-preserving" reduction

$$\text{3coloring} \xrightarrow[\text{creating}]{\text{gap}} \boxed{\text{PCP}} \xrightarrow[\text{preserving}]{\text{gap}} \boxed{\text{3SAT}} \xrightarrow[\text{preserving}]{\text{gap}} \boxed{\text{Clique}}$$

Gap-Preserving Reduction (by example)

3SAT $\longrightarrow$ Clique

m clauses $\longrightarrow$ $7m$ vertices

$OPT = t$ $\longrightarrow$ clique size $= t$

$\shortparallel$

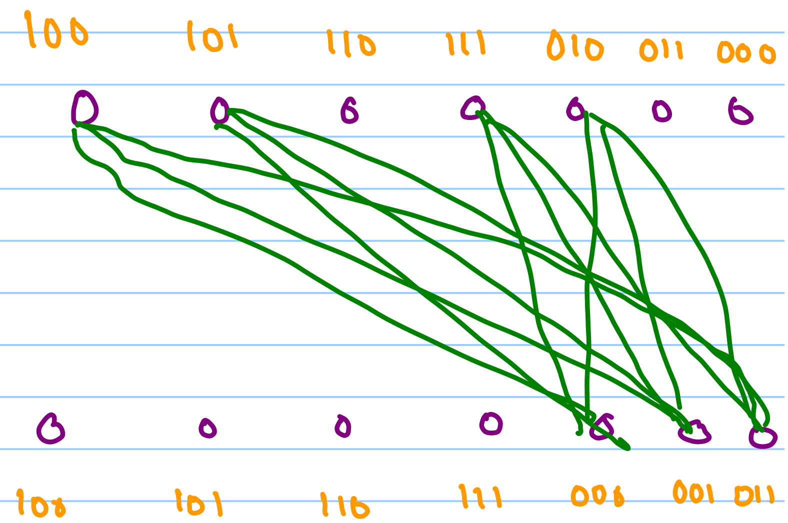
max # sat. clauses

Reduction

$X_1 \vee X_2 \vee \overline{X_3} \longrightarrow$

clause $\longrightarrow$

$X_2 \vee \overline{X_4} \vee X_5 \longrightarrow$



Edges $\equiv$ Consistency

Claim:

Assignment $\Rightarrow$ Clique

Clique $\Rightarrow$ Partial Assignment

Clique has $\leq$ one vertex from each row

$\Rightarrow$ # rows = # satisfying clauses !

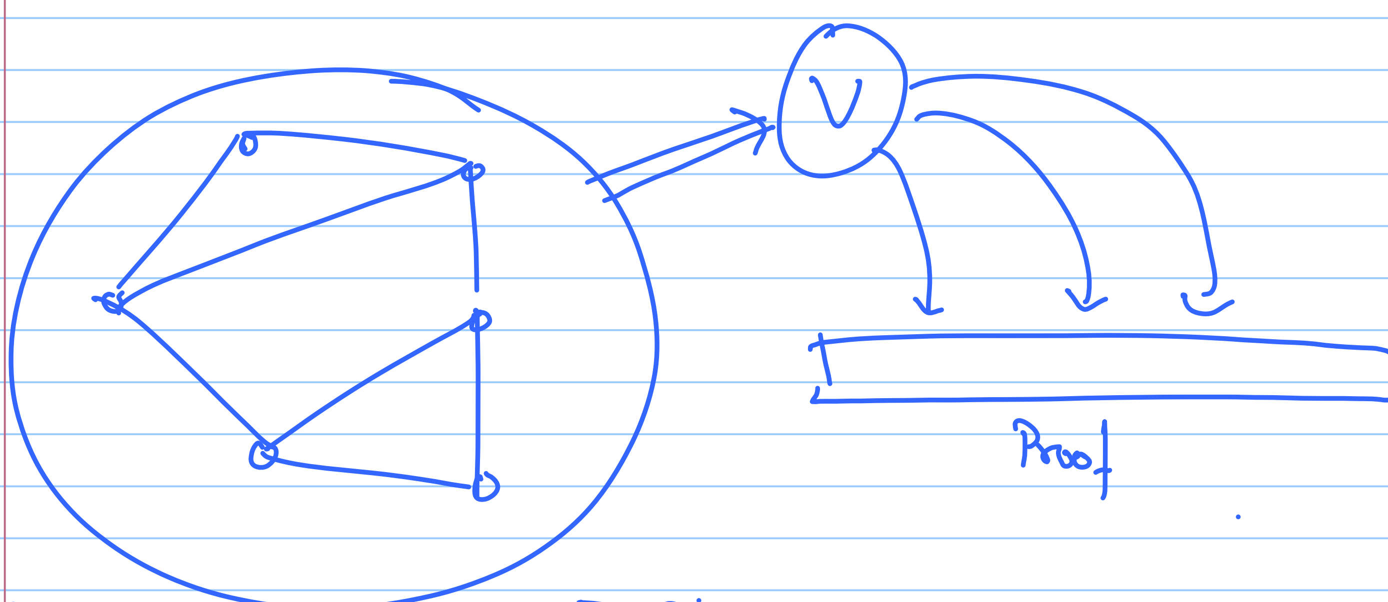
PCP = ?

Defined for language L by verifier V

V: - prob. algorithm ;

- reads "Theorem" fully
- queries "Proof" briefly
- Accepts valid Proofs
- Rejects invalid theorems w.h.p.

E.g. PCP for graph coloring



G 3 colorable $\Rightarrow$ $\exists$ Proof accepted whp

G not 3colorable $\Rightarrow$ $\forall$ Proof, accept w. low. prob.

[Håstad '97]: $\exists$ verifier V running in polytime, makes 3 queries to proof, accepts valid proofs w.p. $.999 \sim 1$

rejects invalid theorems w.p. $.499 \sim \frac{1}{2}$

- furthermore every "check" of the form "is $\Pi_{i_1} \oplus \Pi_{i_2} \oplus \Pi_{i_3} = 0/1$?"
- Proof is of poly size $S = n^{O(1)}$

PCP $\Longrightarrow$ Max 3SAT

One variable for every bit of proof.

One "constraint" for every check

$\equiv$ 4 clauses for every check

Example

$$\Pi_i \oplus \Pi_j \oplus \Pi_k = 0 \Rightarrow \begin{array}{l} (x_i \vee x_j \vee \bar{x}_k) \\ \wedge (x_i \vee \bar{x}_j \vee x_k) \\ \wedge (\bar{x}_i \vee x_j \vee x_k) \\ \wedge (\bar{x}_i \vee \bar{x}_j \vee \bar{x}_k) \end{array}$$

Analysis

- G 3colorable $\Rightarrow$ $\exists$ proof s.t. V accepts w.p. ≈ 1

  $\Rightarrow$ $\exists$ assignment $a_1 \dots a_s$ to $X_1 \dots X_s$ sat. almost all clauses

- G not 3 colorable $\Rightarrow$ $\forall$ proofs V accepts w.p. $\approx \frac{1}{2}$

  $\Rightarrow$ $\forall$ assignments $a_1 \dots a_s$ to $X_1 \dots X_s$, for about $\frac{1}{2}$ the checks only 3/4 clauses sat.

  $\Rightarrow$ any assignment sat. at most $\approx \frac{7}{8}$ fraction of clauses

PCP for Graph Coloring = Proof ?

Recall : Cook-Levin Thm, NP-Completeness of 3-Coloring

+ Short Proof $\in$ NP !

$\Rightarrow$ Given any "theorem" T, system of logic L & length n of proof size .

$\Downarrow$

Can construct in time $\mathrm{Poly}(n)$, graph $G = G(T, L, n)$ s.t.

G is 3colorable $\Leftrightarrow$ T has a proof of length $\leq n$

Moral : 3 coloring PCP suffices

PCP Constructions

(too long to fit this margin)

Main Idea: "Speak in Polynomials"

—— x ——

To say: $a_1 \ldots a_n$,

write instead

$A(1) \ldots A(n^2)$, where

$A(x)$ has degree $\leq n$

& $A(i) = a_i \quad \forall\ i \in \{1 \ldots n\}$

—— x ——

- Graph 3 coloring "logically"

given $E : [n] \times [n] \to \{0,1\}$

$\exists\ X : [n] \to \{0,1,2\}$

s.t. $\forall (i,j) \quad E(i,j) = 0$ or $X(i) \neq X(j)$

- Graph 3 coloring "algebraically"

Given : $E(y,z)$ poly of deg $\leq n$

$\exists\ X(z)$

s.t. $\forall\ z \in [n]$

$X(z) \cdot (X(z)-1) \cdot (X(z)-2) = 0$?

& $\forall\ y,z \in [n]$

$$E(y,z) \cdot \prod_{l \in \{-2,-1,1,2\}} (X(y) - X(z) - l) = 0 \ ?$$

"Polynomial Relation" ~ "Easy to check" (easier)

~ Details Omitted ~

Approx. today

Strong Optimization (extensions of LP)

\+ Strong "PCP" techniques suggest nearly optimal analysis of many many many optimization problems

modulo one conjecture

is the following problem hard?

$$\left\{ \begin{array}{l} x_i + x_j = a_{ij} \pmod p \\ \text{for } (i,j) \in E \end{array} \right\}$$

Can you distinguish most being satisfiable from most being unsatisfiable?

"Unique Games Conjecture": NO!