CMSC 39600 – Lec#1 (Sep 25)

Today

- Administrivia
- PCPs Introduction – 2 views
  - Hardness of Approximation
  - Proof Verification

Administrivia

Lecturer: Prahladh Harsha (prahladh@tti-c.org)

Course Web page:

ttic.uchicago.edu/~prahladh/teaching/07autumn

To do

- Sign up for mailing list
- Sign up for scribes
- Problem Sets/Exercises

Grading:

- 2 Problem Sets (Oct 23 – Nov 8, Nov 15 – Dec 6)
- 2 scribes

Scribes:

Volunteer for scribing

PCPs - Introduction

2 views

Hardness of Approximation

Optimization Problems

$\left\{ \begin{array}{l} \text{Computation Problems} \\ \text{Decision Problems} \end{array} \right\}$ - Polynomially Equivalent

eg:-

SATISFIABILITY ~~SAT~~

CLIQUE - Find largest clique in graph

CLIQUE $= \{\langle G, k\rangle \mid G$ has a clique of size $\geq k\}$

Sufft to work with Decision problems to understand hardness of comp (upto polynomial factors)

~~Approximation problems?~~

MAX-E3SAT: Given 3CNF φ, find assign that satisfies most clauses

MAX-CLIQUE: Given G, find the largest clique

SET-COVER: Given sets $S_1 \ldots S_m \subseteq \{1 \ldots n\}$ find the smallest number that covers $\{1 \ldots n\}$

Approximation Alg:

α-approx - A ~~($0 \le \alpha \le 1$)~~

$\forall$ instances, x

$OPT(x) \ge A(x) \ge \alpha \cdot OPT(x)$ (Maximization $0 \le \alpha \le 1$)

$OPT(x) \le A(x) \le \alpha \cdot OPT(x)$ (Minimization $\alpha \ge 1$

How does one understand of hardness of approx problems?

- Model as gap problems. ($YES \cap NO = \phi$, $YES \cup NO \subsetneq \Sigma^*$)

Eg: Gap-E3SAT$_g$

$YES = \{\langle \varphi, k\rangle \mid \exists$ assig satisfying $\ge k$ clauses$\}$

$NO = \{\langle \varphi, k\rangle \mid \forall$ assig $\le k/g$ clauses are satisfied$\}$

Equivalence of Gap-E3SAT$_g$ & g-approx MAX-E3SAT

($\Rightarrow$) g-approx $(\varphi) \ge k/g \Rightarrow YES$, else NO

($\Leftarrow$) Run Gap-E3SAT$_g$ on $\langle \varphi, 1\rangle, \ldots \langle \varphi, m-1\rangle$

Output $k'=k/g$ largest k s.t. $\langle \varphi, k\rangle \in YES$

$\langle \varphi, k\rangle \notin NO \Rightarrow \exists$ assig that satisfies $\ge k/g$

$\langle \varphi, k+1\rangle \notin YES \Rightarrow opt(\varphi) < k+1$

~~Similarity for Clique?~~

Suff! to work w/ gap-problems.

Theorem (*)

$\exists g$, There exists a poly time redn from ~~SAT~~ 3-color to gap-E3SAT$_g$

$\cancel{\varphi \in L \Rightarrow opt(R(\varphi)) \geq k}$

$$G \longmapsto \langle \psi, k \rangle$$

- $G \in$ 3-COLOR $\Rightarrow$ $OPT(\psi) \geq k$
- $G \notin$ 3-COLOR $\Rightarrow$ $OPT(\psi) \leq k/g$.

ie., gap-E3SAT$_g$ is NP-hard.

Proof Verification:

Proof System

statement

"φ is satisfiable"

"G is 3-colorable"

"G has clique $\geq \frac{n}{100}$"

V

π

Polynomial Verifiers

Defn:

$L \in NP$, iff $\exists$ det polytime verifier V s.t

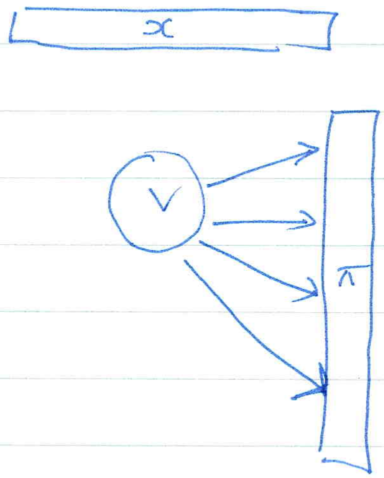
Comp: $\forall x \in L$, $\exists \pi$, $|\pi| \leq poly$ $V(x,\pi) = accept$

Sound. $\forall x \notin L$, $\forall \pi$ $V(x,\pi) = reject$

- Randomized Verifiers.
  - IP, ~~MA~~, AM, MIP, ... PCP.

Theorem (**) [PCP Theorem]
Every lang $L \in NP$ has a prob-checkable pf (PCP)

ie.,



$|\pi| \le \text{poly}\,|x|$

$L \in PCP_{1,1/2}[c_L \log n, q_L]$

$NP \subseteq \bigcup_{c \ge 0} PCP_{1,1/2}[c \log n, q]$

- Proof $|\pi| \le \text{poly}\,|x|$
- Verifier ~~tosse~~ - randomized
  - tosses $c_L(\log n)$ coins
  - probes q_L locations of proof

Comp: $\forall x \in L$, $\exists \pi$
$$\Pr[V^{\pi}(x) = \text{accept}] = 1$$

Sound: $\forall x \notin L$ $\forall \pi$
$$\Pr[V^{\pi}(x) = \text{acc}] \le 1/2$$

Remark: (a) Sequential Repetition
(b) Suffices to look at specific NP-complete lang.

Theorem (*) equivalent Theorem (**)

(a) NP-hardness of Gap-E3SAT $\Rightarrow$ PCP Theorem

Assignment is proof.

(b) PCP Theorem $\Rightarrow$ NP-hardness

Encode Verifiers action by a formula φ

Random string R — Verifier's action q-ary function.

Prop: $\forall q$, $\exists\ \ell(q), k(q)$, s.t any binary fn h over q variables can be encoded by a 3CNF formula $\varphi(h)$ w $k(q)$-clauses over $q+\ell(q)$ variables $\{x_1 .. x_q, \cancel{y_1 .. y_\ell}\ z_1 .. z_{\ell(q)}\}$ s.t

$h(x)=1 \Rightarrow \exists z,\ g(x,z)=1$

$h(x)=0 \Rightarrow \forall z,\ g(x,z)=0.$

$R \longrightarrow h_R \longrightarrow \varphi(h_R)$

$\varphi = \bigwedge_R \varphi(h_R)$ (# clauses in $\varphi = 2^R \cdot k(q) = M$

Comp: $G \in$ 3-COLOR $\Rightarrow$ φ is satisfiable

$G \notin$ 3-COLOR $\Rightarrow$ # clauses satisfied $\leq \frac{M}{2} + \frac{M}{2}\left(1-\frac{1}{k}\right) = \underline{M\left(1-\frac{1}{2k}\right)}$