Advanced Algorithmics

Strategies for Tackling Hard Problems

Sebastian Wild

Markus Nebel

Lecture 22

2017-07-06

Gap Reduction: Example 1

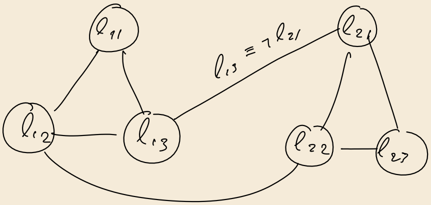
Lemma 5.46 (Max-3SAT $\leq_{GP}$ Independent-Set)

MAX-3SAT $\leq_{GP}$ INDEPENDENT-SET with parameters (c, s) and $(\frac{c}{3}, \frac{s}{3})$ for any $0 \leq s \leq c \leq 1$.

We use the number of clauses resp. number of vertices as $|x|$.

Proof: W.l.o.g. every clause has exactly 3 literals (just duplicate)

Construct graph as for vertex cover reduction



assignment in φ that satisfies k clauses

$\cong$ selection of one vertex per $\triangle$ with k-subset with indep. nodes

$$\frac{k}{m} \begin{cases} \geq c \\ < s \end{cases} \iff \frac{k}{3m} \begin{cases} \geq \frac{c}{3} \\ < \frac{c}{3} \end{cases}$$

Gap Reduction: Example 2

Lemma 5.47 (Gap-Amplification for Independent-Set)

INDEPENDENT-SET $\le_{GP}$ INDEPENDENT-SET with parameters (c, s) and (c^2, s^2) for any $0 \le s \le c \le 1$.

We use the number of vertices as $|x|$.

$\nexists\ \frac{c}{s}$-approx

Since $\left(\frac{c}{s}\right)^2 > \frac{c}{s}$, we find by Lemma 5.44:

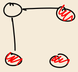
$\rightsquigarrow \nexists\ \left(\frac{c}{s}\right)^2$-approx

Corollary 5.48 (PTAS or nothing)

INDEPENDENT-SET $\in \mathcal{PTAS} \iff$ INDEPENDENT-SET $\in \mathcal{APX}$.

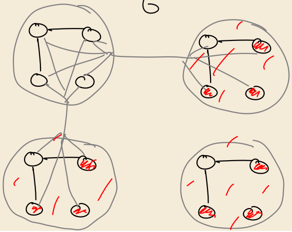
Proof: Construct square graph $G = (V, E)$ $\quad V^2 = V \times V$

$E = \{\{(x,y), (x',y')\} : \{x,x'\} \in E \wedge y = y' \vee \{y,y'\} \in E\}$



G

G^2



$\frac{k}{n} \begin{cases} \ge c \\ < s \end{cases}$

$\frac{k^2}{n^2} \begin{cases} \ge c^2 \\ < s^2 \end{cases}$

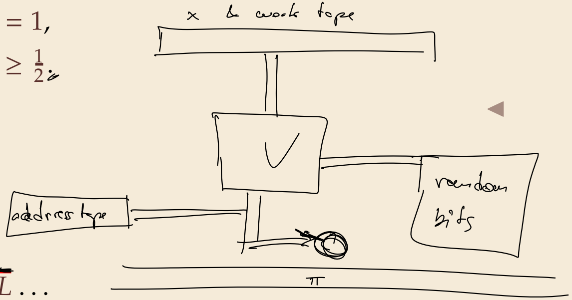
5.10 Probabilistically-Checkable-Proof Systems

Definition 5.49 (Probabilistic Verifier)

Let L be a language. A randomized algorithm V with read-only *random access* to a *proof string* $\pi \in \{0,1\}^\star$ is a *probabilistic verifier* for L if

1. $V(x,\pi)$ runs in poly-time in $|x|$ assuming constant-time random access to π,
2. $\forall x \in L \quad \exists \pi \in \{0,1\}^{\ell(|x|)} \;:\; \Pr[V(x,\pi) = 1] = 1$,
3. $\forall x \notin L \quad \forall \pi \in \{0,1\}^{\ell(|x|)} \;:\; \Pr[V(x,\pi) = 0] \geq \frac{1}{2}$.

where $\ell(n) = q(n)2^{r(n)}$



proof string π for PCP $\widehat{=}$ certificate c for $\mathcal{VP}$

Beware: Acceptance Criterion

probabilistic verifier for L $\iff$ OSE-MC for $\overline{L}$ ...

Definition 5.50 (PCP(r,q))

Let $r, q : \mathbb{N}_0 \to \mathbb{N}_0$ be two functions.

The class $\mathrm{PCP}(r, q)$ consists of all languages $L \subseteq \Sigma^\star$ for which there is a probabilistic verifier V for L with

1. $Random_V(n) = \mathcal{O}(r(n))$, ($r$ random bits)
   i.e., V uses $\mathcal{O}(r(n))$ random bits on inputs x with $|x| = n$,
2. V inspects $\mathcal{O}(q(n))$ bits from π on inputs x with $|x| = n$, and (q proof queries)
3. the positions/indices accessed in π do not depend on previously read values of π (non-adaptive).

Trivial Examples:

- $\mathcal{P} = \mathrm{PCP}(0, 0)$
- $\mathcal{NP} = \mathcal{VP} = \bigcup_{c \in \mathbb{N}} \mathrm{PCP}(0, n^c)$
- $\text{co-}\mathcal{RP} = \bigcup_{c \in \mathbb{N}} \mathrm{PCP}(n^c, 0)$

A more interesting PCP system?

Lemma 5.51 (PCP for 3SAT)

3SAT $\in$ PCP$(n \log n, n)$ We actually showed PCP$(1, n) \ni$ 3SAT

Proof: Input φ with m clauses and n variables

π contains satisfying assignment if one exists

otherwise any string

$\pi_1 \cdots \pi_n$ $\pi_i = \alpha(x_i)$

A: Random clause $C = \ell_1 \vee \ell_2 \vee \ell_3$

Access π_{ℓ_1} π_{ℓ_2} π_{ℓ_3}

Return whether C is satisfied

$\Rightarrow$

- φ satis. $\leadsto \Pr[A(\varphi,\pi) = 1] = 1$
- φ unsat. $\leadsto \Pr\{A(\varphi,\pi) = 0\} \geq \frac{1}{m}$

B: Repeat A k times

Return 0 if any runs returned 0

- φ satis. $\leadsto \Pr[B(\varphi,\pi)=1] = 1$
- φ unsat. $\leadsto \Pr[B(\varphi,\pi)=0] = 1 - \left(\Pr[A(\varphi,\pi)=1]\right)^k$

$$\geq 1 - \left(1-\frac{1}{m}\right)^k$$

$$\overset{!}{\geq} \frac{1}{2} \qquad <$$

$$k \geq \log_{\frac{m-1}{m}}\left(\frac{1}{2}\right) = \frac{-\ln(2)}{\underbrace{\ln(m-1)}_{H_{m-1}} - \underbrace{\ln m}_{H_m}} \sim \ln 2 \cdot m$$

$k = \ln 2 \cdot m$

$\Rightarrow \quad q(|\varphi|) = \Theta(|\varphi|)$

$r(|\varphi|) = \Theta(|\varphi| \log |\varphi|)$

$\square$

An even more interesting PCP system?

Lemma 5.52 (Better PCP for 3SAT)

3SAT $\in$ PCP$(n \log n, 1)$

Proof: π contains values for <u>all</u> formulas with m clauses over n variables

$$\varphi = (x_1 \vee x_2 \vee \neg x_3)$$

1 001 010 111

$$\leadsto \quad m \cdot \left(3\left(\lceil \mathrm{ld}(n+1)\rceil + 1\right)\right) = O(m \log m)$$

$$\pi \qquad \ell(m) = 2^{O(m \log m)}$$

What to do with PCP systems?

Theorem 5.53 (Nondeterministic simulation)
If L has a PCP verifier V that uses $r(n)$ random bits, uses $q(n)$ proof queries and runs in time $p(n)$, then there is a nondeterministic TM that decides L in running time

$$O\left(2^{r(n)}\left(q(n)+p(n)\right)\right).$$

In particular: $\mathrm{PCP}(\log n, 1) \subseteq \mathcal{NP}$.

Proof: Non-determ. guess $\pi \in \{0,1\}^{\ell}$ $\ell = 2^{r(n)} \cdot q(n)$

then de-randomize V, i.e. run all 2^r runs sequentially,

each with running time $p(n)$

Accept if all accept.

What to do with PCP systems?

Theorem 5.54 (Translation to formula)

Given a PCP verifier V for $L \in \Sigma^\star$ using $r(n)$ random bits and $q(n)$ proof queries, we can construct for each $x \in \Sigma^\star$ a CNF-formula $\varphi(x)$ of size $\mathcal{O}\left(2^{r(n)}2^{q(n)} \cdot q(n)\right)$ so that:

1. If $x \in L$ the $\varphi(x)$ is satisfiable.
2. If $x \notin L$, only a $(1 - \varepsilon)$-fraction of the clauses is satisfied. $\longrightarrow$ $1-\varepsilon$ 1

same ε for all x

Proof: $\pi_1, \ldots, \pi_\ell \rightsquigarrow$ variables in φ

for each random bit string $\rho \in \{0,1\}^r$

we read $\pi_{Q(\rho)_1}, \ldots, \pi_{Q(\rho)_q} \Rightarrow x, \rho$ fixed, V is a Boolean function of q variables

For pattern B where $\pi_{Q(\rho)} = B \rightsquigarrow V$ rejects on x, ρ

add clause "$\pi_{Q(\rho)} \neq B$" to $\varphi(x)$

$$\bigwedge_{\rho, B} \left(\bigvee_{\substack{i \\ B_i = 0}} \pi_{Q(\rho)_i} \vee \bigvee_{\substack{i \\ B_i = 1}} \neg \pi_{Q(\rho)_i} \right) = \varphi(x)$$

at most $2^r \cdot 2^q$ clauses, each of size q

- $x \in L$ $\quad \varphi(x)$ satisfiable since $V(x, \rho)$ never rejects.
- $x \notin L$ $\quad \forall \pi$ at least $\frac{1}{2}$ of ρ-values reject

$\frac{1}{2} \cdot 2^r$ clauses not fulfilled

$(1-\varepsilon)$-fraction not fulfilled

for $\varepsilon = \dfrac{2^{r-1}}{2^{r+q}} = 2^{-q-1}$

Theorem 5.55 (PCP-Theorem)

$\mathcal{NP} = \mathrm{PCP}(\log(n), 1)$.

Proof of $\subseteq$ well beyond scope of this course . . .

Theorem 5.56 (Max-Sat has no PTAS)

$\mathcal{P} \neq \mathcal{NP} \rightsquigarrow \underline{\textsc{Max}\text{-SAT} \notin \mathcal{PTAS}}$.

Using PCP-Theorem with $q = 3$ $\rightsquigarrow$ Max-3SAT has no poly-time $\dfrac{1}{\frac{7}{8} - \varepsilon}$-approx