CMPUT 675: Approximation Algorithms **Winter 2005**

Lecture 25: Apr. 13

Lecturer: Mohammad R. Salavatipour *Scribe: Eddie Rafols*

25.1 2P1R Proof Systems

Raz's verifier is a 2 Prover 1-round proof system for a language L with parameters c and s (where c is usually 1 and s is usually 1-ϵ) is a probabilistic verifier V with access to two proofs Π_1 and Π_2 such that an input y for L, V sends one query to each of Π_1 and Π_2 and:

- if $y \in L \rightarrow \exists \Pi_1$ and Π_2 such that $Pr[V \text{ accepts}] = c$
- if $y \notin L \rightarrow \forall \Pi_1$ and Π_2 such that $Pr[V \text{ accepts}] \leq s$

The PCP Theorem shows that for every $L \in$ NP, there is a 2P1R with $c = 1$,$s = 1 - \delta$ for some $\delta > 0$.

Every problem in NP can be reduced to MAX-3SAT. We construct a 2P1R proof system with the above parameters for MAX-3SAT. Given a formula ϕ, the proofs Π_1 and Π_2 are supposed to encode a truth assignment to ϕ. For every variable $x_i \in \phi$, the value of $\Pi_1[i] \in \{0,1\}$ is the value of x_i. For every $C_j \in \phi$, $\Pi_2[j] \in \{1,\ldots,7\}$ is one of seven satisfying assignments for C_j. V picks a random clause C_j and a random variable, say x_i, from that clause accepts if and only if $\Pi_1[i]$ is consistent with $\Pi_2[j]$.

- if ϕ is a "yes" instance $\rightarrow$ proofs Π_1 and Π_2 form a satisfying truth assignment $\rightarrow$ V accepts with probability 1
- if ϕ is a "no" instance $\rightarrow$ at most $(1-\epsilon)m$ clauses can be satisfied $\rightarrow$ there is a probability of at least $\frac{\epsilon}{3}$ that the answers from Π_1 and Π_2 are inconsistent $\rightarrow$ V accepts with probability $< 1 - \frac{\epsilon}{3}$ (where $\frac{\epsilon}{3} = \delta$)

Can we amplify this probability by repetition?

A k-repetition for this 2P1R proof system is as follows: verifier V^k chooses k clauses (randomly) and a variable (randomly) from each. We have proof entries $\Pi_1[i_1 \ldots i_k] \in \{0,1\}^k$ (representing assignments to k-tuples of variables $i_1 \ldots i_k$) and $\Pi_2[j_i \ldots j_k] \in \{1,\ldots,7\}^k$ (representing satisfying assignments to k clauses $C_{j_1} \ldots C_{j_k}$). V^k accepts if and only if all answers are consistent.

This corresponds to the following repetition of label cover: from an instance $\mathcal{L}(\mathcal{G}(\mathcal{V},\mathcal{W},\mathcal{E}),[\mathcal{M}],[\mathcal{N}],\{\Pi_{vw}\})$, we build $\mathcal{L}^k(G'(V',W',E'),[M'],[N'],\{\Pi'_{vw}\})$ where:

- $V' = V^k$ (k-tuples of V)
- $W' = W^k$
- $[M]' = [M]^k$
- $[N]' = [N]^k$
- $(V',W') \in E' \Leftrightarrow (v_{i_j}, w_{i_j}) \in E,\ \forall i,j\ 1 \leq j \leq k\ (V' = (v_{i_1},\ldots,v_{i_k}), W' = (w_{i_1},\ldots,w_{i_k}))$

- $\Pi'_{vw}(b_1, \ldots, b_k) = \Pi_{v_{i_1}, w_{i_1}}(b_1), \Pi_{v_{i_2}, w_{i_2}}(b_2), \ldots, \Pi_{v_{i_k}, w_{i_k}}(b_k)$
- if $\mathrm{OPT}(\mathcal{L}) = 1 \rightarrow \mathrm{OPT}(\mathcal{L}^k) = 1$

We expect that if $\mathrm{OPT}(\mathcal{L}) \leq 1 - \delta$ then $\mathrm{OPT}(\mathcal{L}^k) \leq (1-\delta)^k$, but this is not true.

Theorem 25.1 (Raz 1998) *Parallel Repetition Theorem*
if $OPT(\mathcal{L}) \leq 1 - \delta \rightarrow OPT(\mathcal{L}^k) \leq (1-\delta)^{\Omega(k)}$
i.e. if ϕ *is a no instance of SAT,* V^k *accepts with probability* $2^{-\Omega(k)}$

Note: $[M'] = [7^k]$ and $[N'] = [2^k]$

Theorem 25.2 *There is a reduction from SAT to an instance* $\mathcal{L}(G(V, W, E), [7^k], [2^k], \{\Pi_{vw}\})$ *of label cover such that:*

- *if* ϕ *is a yes instance* $\rightarrow OPT(\mathcal{L}) = 1$
- *if* ϕ *is a no instance* $\rightarrow OPT(\mathcal{L}) = 2^{-ck}$ *for some constant* $c < 1$

and $\mathcal{L} = n^{O(k)}$

Corollary 25.3 *if NP is not a subset of* $O(n^{poly\ log(n)})$ *then there is no* $2^{log^{1-\epsilon} n}$*-approximation for label cover for any* $\epsilon > 0$.

25.2 Hardness of Set Cover

A set-system with parameters m and l consists of:

- U a universe (of elements)
- $C_1, \ldots, C_m, \bar{C_1}, \ldots, \bar{C_m}$ are subsets of U
- For any set of ℓ subsets from C_i's and $\bar{C_i}$'s that does not include a C_j's and $\bar{C_j}$ together, the union does not cover U.

Theorem 25.4 *Given* m, ℓ *there is a set system with* $|U| = O(\ell\ log\ m \cdot 2^\ell)$.

Consider a label cover instance $\mathcal{L}(G(V, W, E), [7^k], [2^k], \{\Pi_{vw}\})$ (where $k = \mathrm{loglog}\ n$ and $|\mathcal{L}| = n^{O(loglog\ n)}$). We can assume that $|V| = |W|$ (e.g. create copies of vertices in V with the same neighbors). We build an instance of set cover $\mathcal{S}$ such that:

- if $\mathrm{OPT}(\mathcal{L}) = 1 \rightarrow \mathrm{OPT}(\mathcal{S}) \leq |V| + |W|$
- if $\mathrm{OPT}(\mathcal{L}) \leq \frac{1}{log^3 |\mathcal{L}|} \rightarrow \mathrm{OPT}(\mathcal{S}) \geq \Omega(log\ |\mathcal{S}|)(|V| + |W|)$

25.2.1 Construction

Consider a set system with $m = N = 2^k$ and for ℓ (to be specified later). For every edge $e = (v, w) \in G$ we have a (disjoint) (m, ℓ)-set system with universe U_e. The union of all U_e's (for all the edges e) is the universe for the set cover instance. Let $\mathcal{U} = \bigcup_{e \in G} U_e$ and let $C_1^{vw}, \ldots, C_m^{vw}$ be the subsets of U_e. For every vertex $v \in V$ and every label $i \in [2^k]$ we have a set $S_{v,i}$. (similarly for every label $j \in [7^k]$ we have a set $S_{w,j}$.

i.e. $S_{v,i} = \bigcup_{w:(v,w)\in E} C_i^{vw}$ and $S_{w,j} = \bigcup_{v:(v,w)\in E} \bar{C}^{vw}_{\Pi_{vw} c_j}$

Lemma 25.5 *if* $OPT(\mathcal{L}) = 1$ *then* $OPT(\mathcal{S}) \leq |V| + |W|$.