

Introduction to Computational Complexity

Lance Fortnow

Notes(27-2-2008) by Ramanathan Narayanan

- Lemma : Given $b, k, l > 0, l \geq \max(b, 8), C \subseteq \Sigma^k$
 $H = \{h_1, h_2, \dots, h_l\}$ (l linear functions), and l^2 strings z_1, z_2, \dots, z_{l^2}
 1. If $|C| = \frac{2^b}{4}$, then $\Pr(H(C) \cap Z \neq \phi) \geq 1 - 2^{-\frac{l}{8}}$
 2. If $|C| \leq \frac{2^b}{d}$ then $\Pr(H(C) \cap Z \neq \phi) \leq \frac{l^3}{d}$
- Proof of #2
 $|H(C)| \leq l|C| \leq l \frac{2^b}{d}$ (happens when all the l functions map members of C to unique values)
Pick z_i at random, then
 $\Pr(z_i \in H(C)) \leq \frac{l 2^b}{2^b} \leq \frac{l}{d}$
Since z_i are independent for all i ,
 $\Pr(\exists z_i \in H(C)) \leq l^2 \frac{l}{d} \leq \frac{l^3}{d}$
- Public coin AM protocol for GNI
- $\pi \in S_n$ is an automorphism of G if $\forall u, v (u, v) \in E$ iff $(\pi(u), \pi(v)) \in E$
Let $\text{Aut}(G)$ = number of automorphisms of G
If $G_1 \not\cong G_2$, then $\text{Aut}(G_1 \cup G_2) = \text{Aut}(G_1) * \text{Aut}(G_2)$
If $G_1 \cong G_2$, then $\text{Aut}(G_1 \cup G_2) = 2 * \text{Aut}(G_1) * \text{Aut}(G_2)$
- $\text{Diff}(G)$ = number of different graphs isomorphic to G
 $\text{Diff}(G) * \text{Aut}(G) = |V|!$
 $\text{Aut}(G_1 \cup G_2) * \text{Diff}(G_1 \cup G_2) = (2n)!$
- If $G_1 \not\cong G_2$, then $\text{Diff}(G_1 \cup G_2) * \text{Aut}(G_1) * \text{Aut}(G_2) = (2n)!$
If $G_1 \cong G_2$, then $\text{Diff}(G_1 \cup G_2) * \text{Aut}(G_1) * \text{Aut}(G_2) = \frac{(2n)!}{2}$
- Let $C = \{(\sigma_1, \pi_1, H_1)(\sigma_2, \pi_2, H_2) \dots (\sigma_r, \pi_r, H_r)\}$, where
 σ_i is an automorphism of G_1
 π_i is an automorphism of G_2
 H_i is an automorphism of $G_1 \cup G_2$
- If $G_1 \not\cong G_2$, then $|C| = (2n!)^r$
If $G_1 \cong G_2$, then $|C| = \frac{1}{2}^r (2n!)^r$

- If $G_1 \not\cong G_2$, then $\Pr(H(C) \cap Z \neq \phi) \geq 1 - 2^{-\frac{l}{8}} \geq 1 - 2^{-\frac{b}{8}} \geq \frac{2}{3}$
- If $G_1 \cong G_2$, then $\Pr(H(C) \cap Z \neq \phi) \leq \frac{l^3}{rd} \leq \frac{b^3}{d} \leq \frac{r^3(\log(2n!))+2}{2^{r+2}} \leq \frac{1}{3}$, for sufficiently large r
- Public coin AM Protocol for GNI
 Arthur: picks $h_1, h_2, \dots, h_l, z_1, z_2, \dots, z_{l^2}$ at random and sends them to Merlin
 Merlin: computes $((\sigma_i, \pi_i, H_i), \dots, (\sigma_r, \pi_r, H_r))$ such that
 for some i, j $h_i(\sigma_1, \dots, H_n) = 2 * j$
 Arthur: then checks if σ_i is an automorphism of G_1 , π_i is an automorphism of G_2 , and H_i
 is an automorphism of $G_1 \cup G_2$
- Every AM protocol has an equivalent one with a “public coin”
- If $\text{DTIME}(2^n) \not\subseteq \text{DTIME}(2^{\epsilon n})$, for some $\epsilon > 0$, then
 $P = BPP$, $MA = AM = NP$, $GNI \in NP$, $GI \in \text{co-NP}$