Theory of Computation
Tutorial VI

Speaker: Yu-Han Lyu
December 26, 2006
Theory Matters

- http://theorymatters.org
- Recent TCS breakthroughs
  - Boosting
  - Random Graph
  - Quantum Computation
  - Hashing
  - Interactive Proof
  - Probabilistic Checkable Proof
  - Smoothed Analysis
Theory Research

• 2006年9月28日，微软亚洲研究院理论研究组正式成立，中科院外籍院士姚期智担任研究组首席顾问

• “Viewpoint: the real reason why software engineers need math”, Vol 44. No 10 CACM

• “Why computer science students need math”, Vol 34, Issue 4, ACM SIGCSE
Computer Science

- Taiwan CNET: New students avoid computer science
  - [http://taiwan.cnet.com/news/software/0,2000064574,20098521,00.htm](http://taiwan.cnet.com/news/software/0,2000064574,20098521,00.htm)

- Interview with Gates: Why computer science is not as popular
  - [http://taiwan.cnet.com/news/special/0,2000064597,20088003,00.htm](http://taiwan.cnet.com/news/special/0,2000064597,20088003,00.htm)

- University computer science programs lose student interest
  - [http://taiwan.cnet.com/news/hardware/0,2000064553,20091661,00.htm](http://taiwan.cnet.com/news/hardware/0,2000064553,20091661,00.htm)

- Impact factor
  - SIAM Journal on Computing
  - Journal of Complexity
Moderately Exponential

• $m(n)$ is of moderately exponential growth if
  \[ \forall k>0 \quad m(n) = \omega(n^k) \quad \text{and} \quad \forall \varepsilon > 0 \quad m(n) = o((1 + \varepsilon)^n) \]

• Example
  – $n^{\log n}$, $(\log n)!$

• If some NPC problem has moderately exponential lower bound, $\text{NP} \neq \text{P}$
NP-hard

- Given a language \( L \), if every NP language can polynomial time reduction to \( L \), then \( L \) is called NP-hard.
- If \( L \) is NP and NP-hard, then \( L \) is NP-complete.
- \( TM_{HALT} \) is NP-hard
  - Transform 3-SAT’s input to a TM \( M \), such that \( M \) tries all possible truth assignment.
  - If \( M \) finds one, accept. Otherwise, loop.
Closure Property

- Concatenation
  - P, NP
- Union
  - P, NP
- Star
  - P, NP
- Intersection
  - P, NP
- Complement
  - P, NP?
HAM-CIRCUIT $\leq_m$ HAM-PATH

• For any $(u,v) \in E$
  – Test whether exists a Ham-Path $(u,v)$
  – If one of $O(n^2)$ edge is accepted, accept.

• Is it a polynomial time many-one reduction?
• Why?
HW4 – Problem 1

• BB is not computable function
• Suppose f is any computable function
• We combine 3 TM
  – Write n 1s with n state
  – Double 1s on the tape with $c_1$ state
  – Write $f(2n)$ on the tape with $c_2$ state
• $BB(2n) > BB(n + c_1 + c_2) \geq f(2n)$
• $A_{\text{TM}}$?
HW4 – Problem 2

• AMBIG\textsubscript{CFG} is undecidable
• If P has a match $t_{i_1}t_{i_2}\ldots t_{i_l}=b_{i_1}b_{i_2}\ldots b_{i_l}$
  \hspace{1em} $t_{i_1}t_{i_2}\ldots t_{i_l}a_{i_l}\ldots a_{i_2}a_{i_1}$ has two derivation, one from T and one from B
• If CFG is ambiguous
  \hspace{1em} $s=w a_{i_l}\ldots a_{i_2}a_{i_1}$, where w contains only symbols from P, and s is ambiguous
  \hspace{1em} $s=t_{i_1}t_{i_2}\ldots t_{i_l}a_{i_l}\ldots a_{i_2}a_{i_1}$
  \hspace{1em} $s=b_{i_1}b_{i_2}\ldots b_{i_l}a_{i_l}\ldots a_{i_2}a_{i_1}$
HW4 – Problem 3

• $A_{2DFA}$ is decidable
  – A 2DFA which has $s$ states, on the input $x$ will has at most $s(|x|+2)^2$ possible configurations

• $E_{2DFA}$ is undecidable
  – $E_{2DFA}$ can decide $E_{TM}$
  – Construct a 2DFA can accept any accepting computation history for TM M.
    • Start configuration and accept configuration
    • Legally follow configuration
HW4 – Problem 4

- Let $J = \{ w | \text{either } w = 0x \text{ for some } x \in A_{TM}, \text{or } w = 1y \text{ for some } y \notin A_{TM} \}$. Show that neither $J$ nor complement of $J$ is Turing-recognizable.
- $A'_{TM} \leq_m J$
  - $f(x) = 1x$
- $A'_{TM} \leq_m J$’s complement
  - $f(x) = 0x$
HW4 – Problem 5

• Rice Theorem
• Refer to textbook
Homework 5

• Due
  – 3:20 pm, January 5, 2007 (before class)
• Easiest : Problem 1
• Normal : Problem 2, 4
• Harder : Problem 3
• Hardest : Problem 5
HW5 – Problem 1

• Show that HITSET is NP-complete.
HW5 - Problem 2

• Let $U = \{<M, x, #^t> \mid \text{TM } M \text{ accepts input } x \text{ within } t \text{ steps on at least one branch}\}$. Show that $U$ is NP-complete.

• You can not prove by reducing any NP-complete problem to $U$.

• By NP’s definition!!
HW5 – Problem 3

• Call a regular expression star-free if it does not contain any star operations.

• Let $\text{EQ}_{\text{SF-REX}} = \{ <R, S> | R \text{ and } S \text{ are equivalent star-free regular expressions} \}$. Show that $\text{EQ}_{\text{SF-REX}}$ is in coNP.

• Verifier is easier

• NP algorithm is also easy
HW5 – Problem 4

• You are given $Q = \{q_0, q_1, \ldots, q_l\}$ and a collection $\{(s_1, r_1), \ldots, (s_k, r_k)\}$. $s_i$ is string, $r_i$ is state. Determine whether a DFA $M$ exists where $\delta (q_0, s_i) = r_i$ for each $i$.

• 3-SAT
HW5 – Problem 5

- Minimize DFA’s algorithm
- Prove it is correct
- Prove it is minimum
  - Myhill-Nerode Theorem
- Prove it is in polynomial time.
HW5 – Self Learning

• Let $f: \mathbb{N} \rightarrow \mathbb{N}$ be any function where $f(n) = o(n \log n)$. Show that $\text{TIME}(f(n))$ contains only the regular languages.

• 1-tape TM

• HW3 Problem 1

• Myhill-Nerode Theorem