Modern Complexity Theory (CS1.405)

Quiz 1 (Monsoon 2024)

International Institute of Information Technology, Hyderabad

Time: 1 hour and 15 minutes　　　　　　　　Total Marks: 20

Instructions: Answer *ALL* questions.

This is a CLOSED book and only OPEN class notes examination.

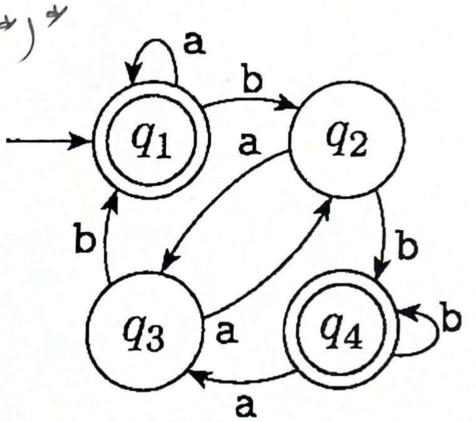
NO query in examination hall is allowed.

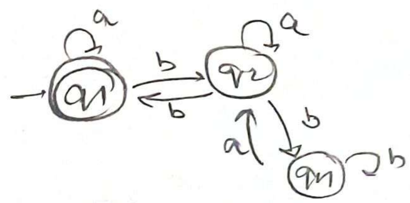
27 August 2024

1. Consider the deterministic finite automaton (DFA) M as shown in Figure 1. Write the formal description of M. Note that the alphabet is $\{a, b\}$. Also, find the language of M.

$(a^* (b^i a^j b^k)^*)^*$

i odd $k \neq 2$





$a^* b a^* b b^* a a^*$

$a^i b^j a^k b^l$　$i \geq 0$, $j \geq 1$, $k \geq 1$, $l \geq 1$

Figure 1: State diagram of the four-state finite automaton M

[5]

2. Design a finite automaton to recognize the regular language of all strings that contain the string 001 as a substring.

[5]

$a^* b a b a^*$

$a^* b b b^*$, $a^* b b b^* a a b b^*$

$a^* b aaabb^*$.

Modern Complexity Theory (CS1.405)

Mid Semester Examination (Monsoon 2024)

International Institute of Information Technology, Hyderabad

Time: 1 hour and 30 minutes Total Marks: 40

Instructions: Answer ANY FOUR questions from the following FIVE questions.

This is a closed book and notes examination.

Regular calculator is allowed.

NO query in examination hall is permitted.

1. **(a)** Give an algorithm to convert a k-tape Turing machine to a single-tape Turing machine. Also, define formally the computation of a k-tape Turing machine.

   (b) Let G be a connected undirected graph and define CONNECTED $:= \{\langle G\rangle | G$ is a connected undirected graph$\}$. Note that an undirected graph G is *connected* if every node (vertex) can be reached from every other node by traveling along the edges of the graph G. Prove that this language is in the class P.

   [(3+2) + 5 = 10]

2. **(a)** Define an enumerator. Prove that a language is Turing-recognizable if and only if some enumerator enumerates it.

   (b) Consider the Boolean satisfiability problem SAT $:= \{\langle\phi\rangle | \phi$ is a satisfiable Boolean formula$\}$. In proving SAT is NP-complete, the 2×3 windows are used to formulate ϕ_{move} in the Boolean formula $\phi = \phi_{start} \wedge \phi_{cell} \wedge \phi_{accept} \wedge \phi_{move}$. Discuss the role of legal 2×3 windows and then derive ϕ_{move} using those 2×3 windows.

   [(1 + 4) + 5 = 10]

3. **(a)** Let CLIQUE $:= \{\langle G, k\rangle | G$ is an undirected graph with a k-clique$\}$. Prove that CLIQUE is NP-hard. Also, show the construction of the undirected graph G with the 3cnf-Boolean formula $\phi = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_1 \vee \bar{x}_2) \wedge (x_2 \vee x_3 \vee \bar{x}_3)$.

   (b) Show that the class of regular languages is closed under the star operation.

   [(3 + 2) + 5 = 10]

4. **(a)** Define decidable, undecidable, tractable and intractable problems. Give examples of an undecidable problem and an intractable problem.

   (b) An oracle is a language $L \subseteq \{0,1\}^*$. An oracle Turing machine is the same as a normal Turing machine, only with the addition of a second tape, called the oracle tape. The cells on the oracle tape can contain either blanks, 0's, or 1's. Cook Reduction is a reduction computed by a deterministic polynomial time oracle Turing machine. Karp-reduction is a polynomial-time many-one reduction. Show that, if $NP \neq P$, there exists an infinite sequence of sets $\{S_1, S_2, \ldots\}$ in $NP \setminus P$ such that S_{i+1} is Karp-reducible to S_i, but S_i is not Cook-reducible to S_{i+1}.

   Prove that if every set in NP can be Cook-reduced to some set in NP $\cap$ CoNP, then NP = CoNP.

   [(2 + 2) + 6 = 10]

5. **(a)** Define NP-hard and NP-complete complexity classes. If a language B is NP-complete and $B \leq_p C$ for some language C in NP, then show that C is also NP-complete.

(b) Let G be an undirected graph, and define the following problem:

LPATH $:= \{\langle G, a, b, k\rangle | G$ contains a simple path of length at least k from vertex a to vertex $b\}$.

Show that LPATH is NP-complete.

[(2+2) + 6 = 10]

****************** End of Question Paper **********************

Modern Complexity Theory (CS1.405)

Quiz 2 (Monsoon 2024)

International Institute of Information Technology, Hyderabad

Time: 1 hour and 15 minutes Total Marks: 20

Instructions: Answer *ALL* questions.

This is a CLOSED book and only OPEN class notes examination.

NO query in examination hall is allowed.

18 October 2024 (Friday)

1. Define the following problem:

$$\text{2SAT} := \{\langle\phi\rangle | \phi \text{ is a 2cnf satisfiable Boolean formula}\}.$$

(a) Prove that 2SAT is in NL.

(b) Prove that 2SAT is also NL-complete.
[Hint: Use the log-space reduction: $\overline{PATH}$ to 2SAT.]

[4 + 6 = 10]

2. Let $f : N \to N$ be a function such that $f(n) \geq n$, where N be the set of natural numbers. Show that for any such function $f : N \to N$, the space complexity class $SPACE(f(n))$ remains the same whether we define the class by using the single-tap Turing machine (TM) model or the two-tape read-only input TM model.

[5 + 5 = 10]

***************** **End of Question Paper** *********************

Modern Complexity Theory (CS1.405)

End Semester Examination (Monsoon 2024)

International Institute of Information Technology, Hyderabad

Time: 3 hours Total Marks: 70

Instructions: Q1 is COMPULSORY, and answer *ANY FIVE* questions from the remaining questions Q2–Q8.

This is a closed book and notes examination.

Regular calculator is allowed.

NO query is allowed in the examination hall.

Q1. Answer all the questions in this part.

(a) Which is the following is TRUE?

A) $TIME(2^n) \subseteq TIME(2^{2n+1})$

B) $TIME(2^n) \neq TIME(2^{n+1})$

C) $TIME(2^n) \subset TIME(2^{2n})$

D) $NTIME(n) \subseteq PSPACE$

(b) Let us consider an elliptic curve $E_p(a,b)$ over Z_p, where p is prime and $p > 3$. Let $\#E$ denote the number of points on $E_p(a,b)$. Then, which one of the following is TRUE?

A) $p+1 \leq \#E \leq p+1+2\sqrt{p}$

B) $p+1-2\sqrt{p} \leq \#E \leq p+2\sqrt{p}$

C) $p \leq \#E \leq p+1+2\sqrt{p}$

D) $p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$

(c) In RSA public key cryptosystem, we know that $\gcd(e, \phi(n)) = 1$. Then, the encryption exponent e must be

A) Even

B) Odd

C) Any number

D) None of these

(d) If $A \in P$, then $P^A =$ P____.

(e) Which of the following statement(s) is/are TRUE? NP $\subseteq$ P^{SAT} SAT

A) If $NP = P^{SAT}$, then NP = coNP. ?

B) An oracle A exists whereby $P^A \neq NP^A$.

C) An oracle B exists whereby $P^B = NP^B$.

D) $TQBF \in SPACE(n^{1/3})$.

(f) If $A \in TIME(t(n))$, then A has circuit complexity $NC^{t(n)}$____.

(g) A language $L \subseteq \{0,1\}^*$ is in RP if and only if there is a probabilistic polynomial time Turing machine M such that

- $x \in L \implies Pr(M(x) = 1) \geq$ 1/2

12

- $x \notin L \implies Pr(M(x) = 0) =$ 1

(h) Let $CNF_{H1} = \{\langle\phi\rangle | \phi$ is a satisfiable cnf-formula where each clause contains any number of positive literals and at most one negated literal. Furthermore, each negated literal has at most one occurrence in $\phi\}$. Then,

A) CNF_{H1} is NP-complete
B) CNF_{H1} is L-complete
C) CNF_{H1} is P-complete
D) CNF_{H1} is NL-complete

(i) Let $ADD = \{\langle x, y, z\rangle | \ x, y, z > 0$ are binary integers and $x + y = z\}$. Then,

A) $ADD \in NL$
B) $ADD \in P$
C) $ADD \in L$
D) $ADD \in PP$

(j) For any space function $f : N \to N$, where $f(n) \geq n$, which one of the following is TRUE?

A) $NSPACE(f(n)) \subseteq SPACE(f^2(n))$
B) $NSPACE(f(n)) \subseteq SPACE(f^2(n \log n))$
C) $NSPACE(f(n)) \subseteq SPACE(f^3(n))$
D) $NSPACE(f(n)) \subseteq SPACE(f^3(n \log n))$

(k) Out of the following relationships, which one is valid?

A) $P \subseteq NP \subseteq PSPACE \subsetneq NPSPACE$
B) $P \subseteq NP \subseteq PSPACE = NPSPACE$
C) $P \subseteq NP \subsetneq PSPACE \subsetneq NPSPACE$
D) $P \subseteq NL \subseteq PSPACE \subsetneq NPSPACE$

(l) If a Turing machine M runs in $f(n)$-space and w is an input of length n, then the number of configurations of M on w is

$f(n) = 2^{g^{f(n)}}$

$2^{\log_2 5 f(n) g^{f(n)}}$

$= 2^{\log_2 5 + \log_2 f(n) + f(n) \log_2(g)}$

$2^{O(f(n))} = f(n)$

A) $2^{o(f(n))}$
B) $n^2 2^{o(f(n))}$
C) $n 2^{o(f(n))}$
D) $n 2^{o(f(n \log n))}$

(m) Out of the following relationships, which is/are TRUE?

A) If any NL-complete language is in L, then L = NL.
B) NL $\subseteq P$.
C) L $\subseteq$ coNL.
D) Any PSPACE-hard language is also NP-hard. NP $\subseteq$ PSPACE

(n) Let TRIPLE-SAT = $\{< \phi > | \phi$ has at least three satisfying assignments$\}$. Then, TRIPLE-SAT is in

A) P only
B) NP-complete
C) NP-hard only
D) NP only

(o) Recall that a directed graph is strongly connected if every two nodes are connected by a directed path in each direction. Let STRONGLY-CONNECTED = $\{\langle G\rangle | G$ is a strongly connected graph$\}$. Then,

A) STRONGLY-CONNECTED is in NL only

B) STRONGLY-CONNECTED is PSPACE-complete.

C) STRONGLY-CONNECTED is NL-complete.

D) STRONGLY-CONNECTED is L only.

(p) Which one is TRUE?

A) For any two real numbers ϵ_1 and ϵ_2 with $1 \leq \epsilon_1 < \epsilon_2$, $TIME(n^{\epsilon_1}) \subset TIME(n^{\epsilon_2})$.

B) For any two real numbers ϵ_1 and ϵ_2 with $0 \leq \epsilon_1 < \epsilon_2$, $TIME(n^{\epsilon_1}) \subseteq TIME(n^{\epsilon_2})$.

C) For any two real numbers ϵ_1 and ϵ_2 with $0 \leq \epsilon_1 < \epsilon_2$, $TIME(n^{\epsilon_1}) \subset TIME(n^{\epsilon_2})$.

D) For any two real numbers ϵ_1 and ϵ_2 with $1 \leq \epsilon_1 < \epsilon_2$, $TIME(n^{\epsilon_1}) \subseteq TIME(n^{\epsilon_2})$.

(q) With respect to the random oracle SAT, which one of the following is/are TRUE?

A) $NP \subset coNP^{SAT}$

B) $P = NP$

C) $NP \subseteq P^{SAT}$

D) $coNP \subseteq P^{SAT}$

CoNP $\rightarrow$ $\overline{SAT} \in$ CoNP i.e. SAT $\in$ NP so if P^{SAT} $\rightarrow$ not then we can solve coNP problems also.

(r) The complexity needed for the quantum Shor's algorithm to factor an large N to be factored is

A) $O((N \log N)^2)$

B) $O((N \log N)^3)$

C) $O((\log N)^2)$

D) $O((\log N)^3)$

(s) The *depth* of a circuit is $\log(n)$. n → no of gates

(t) The intersection of two NL-complete languages (over the same alphabet) is not. NL Complete

[$20 \times 1 = 20$]

Q2. **(a)** Define a bipartite graph. Let BIPARTITE := $\{\langle G \rangle |$ undirected graph G is bipartite$\}$. A coloring of a graph $G = (V, E)$ is a function $f : V \rightarrow \{1, 2, \cdots, k\}$ defined for all $i \in V$. If $(u, v) \in E$, then $f(u) \neq f(v)$. Thus, for a fixed k, define kCOLOR := $\{\langle G \rangle |$ undirected graph G is k-colorable, that is, no two adjucent nodes of G will be given the same color$\}$.

Prove that 2COLOR $\leq_p$ BIPARTITE.

(b) Prove that if P = NP and $L \in P - \{\emptyset, \Sigma^*\}$, then L is NP-complete.

[$5 + 5 = 10$]

Q3. **(a)** Let ALL$_{NFA}$:= $\{\langle A \rangle | A$ is a NFA and $L(A) = \Sigma^*\}$. Show that it can be decided by $O(n)$-space non-deterministic Turing machine (NTM), where n is the size of the input string.

(b) If f and g are log-space computable functions, show that the composition of f and g denoted by $f \circ g$, is also log-space computable function. Using this result, show that if $A \leq_L B$ and $B \leq_L C$, then $A \leq_L C$.

[$5 + 5 = 10$]

Q4. **(a)** Let TQBF = $\{ \langle \phi \rangle | \phi$ is a true fully quantified Boolean formula$\}$. Show that TQBF restricted to formulas where the part following the quantifies is in CNF (conjunctive normal form) is still PSPACE-complete.

(b) Let $EQ_{REX} = \{\langle R, S \rangle | R$ and S are equivalent regular expressions$\}$. Show that $EQ_{REX} \in$ PSPACE.

[$5 + 5 = 10$]

Q5. (a) State the Integer Factorization Problem (IFP). Prove that IFP $\in BQP$ using the Shor's algorithm.

(b) Let $\uparrow$ represent the exponentiation operation. If R is a regular expression and k is a non-negative integer, $R \uparrow$ is equivalent to the concatenation of R with itself k times. In other words, $R^k = R \uparrow k = R \circ R \circ \cdots R$ (k times).

Let $EQ_{REX\uparrow} = \{\langle Q, R\rangle | Q$ and R are equivalent regular expressions with exponentiation$\}$.

Prove that $EQ_{REX\uparrow}$ is EXPSPACE-complete.

[5 + 5 = 10]

Q6. (a) For a circuit C and input setting x, let $C(x)$ be the value of C on x. Define

$$\text{CIRCUIT-VALUE} := \{\langle C, x\rangle | C \text{ is a Boolean circuit and } C(x) = 1\}.$$

Prove that CIRCUIT-VALUE is P-complete.

(b) Define the unique-sat problem to be USAT = $\{\langle\phi\rangle|\phi$ is a Boolean formula that has a single satisfying assignment$\}$. Show that USAT $\in P^{SAT}$.

[5 + 5 = 10]

Q7. (a) Define the bounded-error quantum polynomial time (BQP) complexity class. Prove that $BPP \subseteq BQP$.

(b) Prove that the Diffie-Hellman key exchange protocol is secure against a passive adversary under the NP-hard problem, known as Discrete Logarithm Problem (DLP).

[5 + 5 = 10]

Q8. (a) Discuss the role of the blockchain technology in the blockchain-envisioned secure data delivery and collection Internet of Things (IoT)-enabled Internet of Drones (IoD) environment. What is the role of the NP-hard problem, known as the Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP) in the secure access control mechanism used in this scheme?

$Adv_A \geq \frac{q^2}{|Hash|} + 2\, Adv_A$

(b) State the "time hierarchy theorem". Using this theorem, prove that P $\subset$ EXPTIME.

Lemma no. lagta hai

[6 + 4 = 10]

**************** End of Question Paper ********************