Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

Foundations of Computing Science (CS60005) **Autumn Semester, 2022-2023**

Mid-Semester Examination **22-Sep-2022 (Thursday), 09:00–11:00** **Maximum Marks: 60**

Instructions:

- Write your answers in the answer booklet provided to you in the examination hall.
- There are a total of SIX questions, each having 10 marks.
- Answer ALL the questions (or as many as you can) mentioning the question numbers clearly.
- Be brief and precise. Write the answers for all parts of a question together.
- If you use any theorem/result/formula covered in the class, just mention it, do not elaborate.
- Write all the proofs/deductions in mathematically/logically precise language.
  Unclear and/or dubious statements would be severely penalized.

– The question paper starts from the next page –

Q1. Your task is to (logically) solve a murder-mystery on behalf of Sherlock Holmes which appeared in the novel “A Study in Scarlet” by Sir Arthur Conan Doyle. The arguments (simplified from the novel) go as follows.

F_1 : There was a murder. If it was not done for robbery, then either it was a political assassination, or it might be for a woman.

F_2 : In case of robbery, usually something is taken.

F_3 : However, nothing was taken from the murderer’s place.

F_4 : Political assassins leave the place immediately after their assassination work gets completed.

F_5 : On the contrary, the assassin left his/her tracks all over the murderer’s place.

F_6 : For an assassin, to leave tracks all over the murderer’s place indicates that (s)he was there all the time (for long duration).

Your goal is to (logically) find the reason for the murder. Please frame the above arguments logically (using propositional logic) and formally derive the solution. *Present your answer as asked in the following parts.*

(a) Write all propositions with English meaning (statements) that you have used. **(2)**

(b) Build suitable propositional logic formula to encode each of the *six* statements above. **(3)**

(c) Show all deduction steps (with the name of the rules you apply) to derive the goal (mystery). **(4)**

(d) Conclude what was the reason for the murder. **(1)**

Solution:

(a) We may use the following propositions.

rob: Murder was done for robbery.

pol: Murder was a political assassination.

wom: Murder was for a woman.

tak: Something was taken from murderer’s place.

imm: Assassin left immediately after work done.

trc: Assassin left tracks all over the room.

(b) The propositional formula corresponding to the given arguments are as follows.

F_1: $\neg\,\texttt{rob} \rightarrow \texttt{pol} \vee \texttt{wom}$

F_2: $\texttt{rob} \rightarrow \texttt{tak}$

F_3: $\neg\,\texttt{tak}$

F_4: $\texttt{pol} \rightarrow \texttt{imm}$

F_5: $\texttt{trc}$

F_6: $\texttt{trc} \rightarrow \neg\,\texttt{imm}$

(c) The logical deduction steps are given as follows.

$$\begin{array}{rl} F_2 : & \texttt{rob} \rightarrow \texttt{tak} \\ F_3 : & \neg\texttt{tak} \\ \hline \therefore\ G_1 : & \neg\texttt{rob} \\ & \text{(Modus Tollens)} \end{array} \qquad \begin{array}{rl} F_1 : & \neg\texttt{rob} \rightarrow \texttt{pol} \vee \texttt{wom} \\ G_1 : & \neg\texttt{rob} \\ \hline \therefore\ G_2 : & \texttt{pol} \vee \texttt{wom} \\ & \text{(Modus Ponens)} \end{array} \qquad \begin{array}{rl} F_5 : & \texttt{trc} \\ F_6 : & \texttt{trc} \rightarrow \neg\texttt{imm} \\ \hline \therefore\ G_3 : & \neg\texttt{imm} \\ & \text{(Podus Ponens)} \end{array}$$

$$\begin{array}{rl} F_4 : & \texttt{pol} \rightarrow \texttt{imm} \\ G_3 : & \neg\texttt{imm} \\ \hline \therefore\ G_4 : & \neg\texttt{pol} \\ & \text{(Modus Tollens)} \end{array} \qquad \begin{array}{rl} G_2 : & \texttt{pol} \vee \texttt{wom} \\ G_4 : & \neg\texttt{pol} \\ \hline \therefore\ G : & \texttt{wom} \\ & \text{(Disjunctive Syllogism)} \end{array}$$

(d) The murder was done for a woman.

Q2. Let the relation σ on $\mathbb{N}$ (the set of natural numbers) consist only of the following tuples:

$$\sigma = \Big\{(n, n) \mid n \in \mathbb{N}\Big\} \bigcup \Big\{(2n, 2n-1) \mid n \in \mathbb{N}\Big\} \bigcup \Big\{(2n, 2n+1) \mid n \in \mathbb{N}\Big\}.$$

(a) Prove that σ is a partial order. **(6)**

(b) Is σ a total (that is, linear) order? **(2)**

(c) Is $\mathbb{N}$ a lattice under σ? **(2)**

Solution:

(a) Let $a \in \mathbb{N}$. The crucial observations are as follows.

Observation-1: If a is even, it is related only to $a, a-1, a+1$.

Observation-2: If a is odd, it is related only to a.

Now, we proceed to prove the partial-order properties of σ.

[Reflexive] All the tuples $(a, a) \in \sigma$.

[Antisymmetric] Let $(a, b), (b, a) \in \sigma$. Consider the two cases.

(i) If a is even, $b \in \{a, a-1, a+1\}$ (by Observation-1). If $b \neq a$, then $b = a \pm 1$ is odd, and $a \neq b$ cannot be related to b (by Observation-2). Therefore, we must have $b = a$.

(ii) if a is odd, the hypothesis $(a, b) \in \sigma$ and Observation (2) imply $a = b$.

[Transitive] Let $(a, b), (b, c) \in \sigma$. Again consider the two cases.

(i) If a is even, then $b \in \{a, a-1, a+1\}$. If $b = a$, then $(a, c) = (b, c) \in \sigma$. If $b = a \pm 1$, then b is odd, and so $c = b$, that is, $(a, c) = (a, b) \in \sigma$.

(ii) If a is odd, then $b = a$, so $(a, c) = (b, c) \in \sigma$.

(b) *False.*

For example, neither $(1, 3)$ nor $(3, 1)$ is in σ.

(c) *False.*

1 is related only to 1, and 3 only to 3. That is, we cannot find an $a \in \mathbb{N}$ such that $(1, a) \in \sigma$ and $(3, a) \in \sigma$. This implies that 1 and 3 does not have any common upper bound. In particular, $\texttt{lub}(1, 3)$ does not exist. Moreover, $\texttt{lub}(2, 6)$, $\texttt{glb}(1, 5)$, and $\texttt{glb}(2, 4)$ also do not exist.

Q3. Let S be the set of all infinite bit sequences. In the class, S has been proven to be uncountable (using diagonization argument). The n-th element of a sequence $\alpha \in S$ is denoted by $\alpha(n)$ for $n \geq 0$.

Prove the countability / uncountability of each of the following subsets of S.

(a) $T_1 = \Big\{\alpha \in S \;\Big|\; \alpha(n) = 1 \text{ and } \alpha(n+1) = 0,\ \text{for } \underline{\text{some}}\ n \geq 0\Big\}$. **(5)**

(b) $T_2 = \Big\{\alpha \in S \;\Big|\; \alpha(n) = 1 \text{ and } \alpha(n+1) = 0,\ \text{for } \underline{\text{no}}\ n \geq 0\Big\}$. **(5)**

Note: Solve the above parts independently, that is, do not use the result of any part in the other.

Solution:

(a) *Uncountable.*

Consider the set,

$$T_3 = \{\alpha \in S \mid \alpha(0) = 1 \text{ and } \alpha(1) = 0\}.$$

We have $T_3 \subseteq T_1$, and so $|T_3| \leq |T_1| \leq |S|$ (use the canonical inclusion maps which are injective).

On the other hand, take any $\alpha = (1, 0, a_2, a_3, a_4, \ldots, a_n, \ldots) \in T_3$.

The map taking $\alpha \mapsto (a_2, a_3, a_4, \ldots, a_{n+2}, \ldots) \in S$ is clearly a bijection $T_3 \to S$, implying that $|T_3| = |S|$. We therefore conclude that $|T_1| = |T_3| = |S|$.

(b) *Countable.*

Each sequence of T_2 either starts with a finite (may be empty) sequence of 0's followed by an infinite sequence of 1's, or consists only of 0's.

Consider the function $T_2 \to \mathbb{N}$ that maps $(0, 0, 0, \ldots)$ to 1, and $(0, 0, \ldots, 0, 1, 1, 1, \ldots, 1, \ldots)$ with $n \geq 0$ number of initial 0's to $n + 2 \in \mathbb{N}$.

This function is clearly bijective.

Q4. Let $R = \mathbb{Z} \times \mathbb{Z}$ (Cartesian product between set of integers). Define addition and multiplication on R as:

$$\begin{aligned} a, b) + (c, d) &= (a + c,\ b + d), \text{ and} \\ (a, b) \cdot (c, d) &= (ac + ad + bc,\ 2ac + bd). \end{aligned}$$

(a) Verify that R is a ring under these two operations. **(7)**

(b) Prove that R is a commutative ring with unity. **(3)**

Solution:

(a) All ring axioms are now verified one by one.

[Closure under $+$] For $a, b, c, d \in \mathbb{Z}$, we have $a + c, b + d \in \mathbb{Z}$.

[Associativity of $+$] $(a + c) + e = a + (c + e)$ and $(b + d) + f = b + (d + f)$.

[Commutativity of $+$] $a + c = c + a$ and $b + d = d + b$.

[Additive identity] $(0, 0)$ is the additive identity.

[Additive inverse] $-(a, b) = (-a, -b)$.

[Closure under $\cdot$] $ac + ad + bc,\ 2ac + bd \in \mathbb{Z}$.

[Associativity of $\cdot$] On the one hand, we have,

$$\begin{aligned} & ((a, b) \cdot (c, d)) \cdot (e, f) \\ = \ & (ac + ad + bc,\ 2ac + bd) \cdot (e, f) \\ = \ & ((ac + ad + bc)e + (ac + ad + bc)f + (2ac + bd)e,\ 2(ac + ad + bc)e + (2ac + bd)f) \\ = \ & (3ace + acf + ade + adf + bce + bcf + bde,\ 2ace + 2acf + 2ade + 2bce + bdf). \end{aligned}$$

On the other hand, we have,

$$\begin{aligned} & (a, b) \cdot ((c, d) \cdot (e, f)) \\ = \ & (a, b) \cdot (ce + cf + de,\ 2ce + df) \\ = \ & (a(ce + cf + de) + a(2ce + df) + b(ce + cf + de),\ 2a(ce + cf + de) + b(2ce + df)) \\ = \ & (3ace + acf + ade + adf + bce + bcf + bde,\ 2ace + 2acf + 2ade + 2bce + bdf). \end{aligned}$$

[Distributivity of $\cdot$ over $+$] We have,

$$\begin{aligned} & (a, b) \cdot ((c, d) + (c', d')) \\ = \ & (a, b) \cdot (c + c', d + d') \\ = \ & (a(c + c') + a(d + d') + b(c + c'),\ 2a(c + c') + b(d + d')) \\ = \ & (ac + ad + bc,\ 2ac + bd) + (ac' + ad' + bc',\ 2ac' + bd') \\ = \ & (a, b) \cdot (c, d) + (a, b) \cdot (c', d'). \end{aligned}$$

Likewise, show that $((a, b) + (a', b')) \cdot (c, d) = (a, b) \cdot (c, d) + (a', b') \cdot (c, d)$.

(b) We have $(a, b) \cdot (c, d) = (ac + ad + bc, 2ac + bd)$ and $(c, d) \cdot (a, b) = (ca + cb + da, 2ca + db)$. Next, use the commutativity of integer addition and multiplication.

The multiplicative identity is $(0, 1)$ since $(0, 1) \cdot (a, b) = (0 \times a + 1 \times a + 0 \times b, 2 \times 0 \times a + 1 \times b) = (a, b)$ and $(a, b) \cdot (0, 1) = (a \times 0 + a \times 1 + b \times 0, 2a \times 0 + b \times 1) = (a, b)$.

Q5. Let L be a language over an alphabet Σ. Recall that a string x is called a prefix of a string y if $y = xz$ for some string z. For example, all the prefixes of $abbab$ are $\varepsilon, a, ab, abb, abba, abbab$. From L, we generate the language $\texttt{dupPrefix}(L)$ by duplicating prefixes of strings in L. More precisely, we define,

$$\texttt{dupPrefix}(L) = \Big\{ xy \;\Big|\; y \in L, \text{ and } x \text{ is a prefix of } y \Big\}.$$

Prove / Disprove:

(a) If L is regular, then $\texttt{dupPrefix}(L)$ must also be regular. **(5)**

(b) If L is not regular, then $\texttt{dupPrefix}(L)$ must also be non-regular. **(5)**

Solution:

(a) *False.*

Take $\Sigma = \{a, b\}$, and $L = \mathscr{L}(a^*b) = \{a^n b \mid n \geq 0\}$. Suppose that, $\texttt{dupPrefix}(L)$ is regular. Let k be a pumping lemma constant for $\texttt{dupPrefix}(L)$. Supply the string $a^k b a^k b \in \texttt{dupPrefix}(L)$ to the pumping lemma with $u = a^k b$, $v = a^k$, and $w = b$. The lemma returns a decomposition $v = xyz$ with $y = a^l$ for some $l > 0$. Pumping out y, we get the string $uxzw = a^k b a^{k-l} b \in L$. But since $l > 0$, $a^k b$ cannot be a prefix of $a^{k-l} b$, leading to a contradiction!

(b) *False.*

Take $\Sigma = \{a\}$, and $L = \{a^{n^2} \mid n \geq 0\}$ (a language already proven to be non-regular using pumping lemma argument!).

We have,

$$\texttt{dupPrefix}(L) = \Big\{ a^m \;\Big|\; m \geq 0, m \neq 3 \Big\}$$

which is regular (because its complement is a finite set).

Q6. Consider the following language L_1 over the alphabet $\{a, b, \#\}$.

$$L_1 = \Big\{x\#y \mid x, y \in \{a, b\}^*,\ x \neq y,\ |x| = |y|\Big\}.$$

Here, $|w|$ denotes the length of the string w. Prove / Disprove: L_1 is context-free. **(10)**

Solution:

False.

Consider the language,

$$L_1 = \Big\{x\#y \mid x, y \in \{a, b\}^*,\ x \neq y,\ |x| = |y|\Big\}.$$

Here, x, y are in $\{a, b\}^*$. This language is not context-free. We prove this by the pumping lemma. Suppose that L_1 is context-free, and let k be a pumping-lemma constant for L_1. Consider the string,

$$z = a^{k+k!}b^k\#a^kb^{k+k!} \in L_1.$$

The pumping lemma gives a decomposition of this string of the form $z = uvwxy$ such that $vx \neq \varepsilon$, $|vwx| \leq k$, and $z_i = uv^iwx^iy \in L_1$ for all $i \geq 0$. We consider the following (several) cases.

Case-1: vx contains $\#$. Then, z_0 does not contain any $\#$.

Case-2: v and x are both to the left of $\#$, or both to the right of $\#$. Then, for all $i \neq 1$, the two sides of $\#$ in z_i are of unequal lengths.

Case-3: v is to the left of $\#$ and x is to the right of $\#$. If $|v| \neq |x|$, then again for $i \neq 1$, the two sides of $\#$ in z_i are of unequal lengths. So, we must have $|v| = |x| \neq 0$. Since $|vwx| \leq k$, we must have v in the left block of b's, and x in the right block of a's. Since $1 \leq l = |v| = |x| \leq k$, we conclude that l is a divisor of $k!$. But then, $z_{1+k!/l} = a^{k+k!}b^{k+k!}\#a^{k+k!}b^{k+k!} \notin L_1$.