INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

	Stamp / Signature of the Invigilator

EXAMINATION (Mid Semester)	SEMESTER (Autumn)

Roll Number										Section		Name	
Subject Number	C	S	2	1	0	0	1	Subject Name	*Discrete Structures*				
Department / Center of the Student		Additional sheets											

Important Instructions and Guidelines for Students

1. You must occupy your seat as per the Examination Schedule/Sitting Plan.
2. Do not keep mobile phones or any similar electronic gadgets with you even in the switched off mode.
3. Loose papers, class notes, books or any such materials must not be in your possession, even if they are irrelevant to the subject you are taking examination.
4. Data book, codes, graph papers, relevant standard tables/charts or any other materials are allowed only when instructed by the paper-setter.
5. Use of instrument box, pencil box and non-programmable calculator is allowed during the examination. However, exchange of these items or any other papers (including question papers) is not permitted.
6. Write on both sides of the answer script and do not tear off any page. **Use last page(s) of the answer script for rough work.** Report to the invigilator if the answer script has torn or distorted page(s).
7. It is your responsibility to ensure that you have signed the Attendance Sheet. Keep your Admit Card/Identity Card on the desk for checking by the invigilator.
8. You may leave the examination hall for wash room or for drinking water for a very short period. Record your absence from the Examination Hall in the register provided. Smoking and the consumption of any kind of beverages are strictly prohibited inside the Examination Hall.
9. Do not leave the Examination Hall without submitting your answer script to the invigilator. **In any case, you are not allowed to take away the answer script with you.** After the completion of the examination, do not leave the seat until the invigilators collect all the answer scripts.
10. During the examination, either inside or outside the Examination Hall, gathering information from any kind of sources or exchanging information with others or any such attempt will be treated as **'unfair means'**. Do not adopt unfair means and do not indulge in unseemly behavior.

Violation of any of the above instructions may lead to severe punishment.

Signature of the Student

To be filled in by the examiner

Question Number	1	2	3	4	5	6	7	8	9	10	Total
Marks Obtained											

Marks obtained (in words)	Signature of the Examiner	Signature of the Scrutineer

CS21001 Discrete Structures, Autumn 2019–2020

Mid-Semester Test

24–September–2019 NR 221/222/321/322, 02:00pm–04:00pm Maximum marks: 60

Instructions

- Write your answers in the question paper itself. Be brief and precise. Answer all questions.
- Write the answers only in the respective spaces provided. The last two blank pages may be used for additional rough work.
- If you use any theorem/result/formula covered in the class, just mention it, do not elaborate.
- Write all the proofs in mathematically precise language. Unclear and/or dubious statements would be severely penalized.
- Common notations:

$$
\begin{array}{rcl}
\mathbb{N} & = & \text{The set of natural numbers } = \{1,2,3,\ldots\} \\
\mathbb{N}_0 & = & \text{The set of non-negative integers } = \{0,1,2,3,\ldots\} \\
\mathbb{Z} & = & \text{The set of integers } = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\} \\
\mathbb{Q} & = & \text{The set of rational numbers } = \left\{\frac{a}{b} \mid a \in \mathbb{Z},\, b \in \mathbb{N}\right\} \\
\mathbb{R} & = & \text{The set of real numbers} \\
\mathbb{C} & = & \text{The set of complex numbers} \\
\mathscr{P}(A) & = & \text{The power set of } A \text{ (also denoted as } 2^A) \\
(a,b) & = & \text{The open interval } \{x \in \mathbb{R} \mid a < x < b\} \\
[a,b] & = & \text{The closed interval } \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\} \\
\lfloor x \rfloor & = & \text{The floor of } x \\
\lceil x \rceil & = & \text{The ceiling of } x
\end{array}
$$

Do not write anything on this page.

Questions start from the next page.

1. While walking in a labyrinth, you find yourself in front of three possible roads. The road on your left is paved with gold, the road in front of you is paved with marble, while the road on your right is made of small stones. Each road is protected by a guard. You talk to the guards, and this is what they tell you.

- The guard of the gold road: "This road will bring you straight to the center. Moreover, if the stones take you to the center, then also the marble takes you to the center."
- The guard of the marble road: "Neither the gold nor the stones will take you to the center."
- The guard of the stone road: "Follow the gold, and you will reach the center. Follow the marble, and you will be lost."

You know that all the guards are liars. Your goal is to choose the correct road that will lead you to the center of the labyrinth. Solve your problem using a propositional-logic formulation and deduction. **(10)**

Solution Introduce the following propositions.

GG : The guard of the gold road is telling the truth
GM : The guard of the marble road is telling the truth
GS : The guard of the stone road is telling the truth
G : The gold road leads to the center
M : The marble road leads to the center
S : The stone road leads to the center

The statements of the three guards can be logically encoded as follows.

$$\begin{aligned} GG &\leftrightarrow \left[G \wedge (S \to M)\right] \\ GM &\leftrightarrow \left[\neg G \wedge \neg S\right] \\ GS &\leftrightarrow \left[G \wedge \neg M\right] \end{aligned}$$

You also know that the following statement is true.

$$\begin{aligned} Z &\equiv \neg GG \wedge \neg GM \wedge \neg GS \\ &\equiv \neg\left[G \wedge (S \to M)\right] \wedge \neg\left[\neg G \wedge \neg S\right] \wedge \neg\left[G \wedge \neg M\right] \\ &\equiv \left[\neg G \vee (S \wedge \neg M)\right] \wedge \left[G \vee S\right] \wedge \left[\neg G \vee M\right]. \end{aligned}$$

The truth table of Z is given below.

G	M	S	$\neg G \vee (S \wedge \neg M)$	$G \vee S$	$\neg G \vee M$	Z
0	0	0	1	0	1	0
0	**0**	**1**	**1**	**1**	**1**	**1**
0	1	0	1	0	1	0
0	**1**	**1**	**1**	**1**	**1**	**1**
1	0	0	0	1	0	0
1	0	1	1	1	0	0
1	1	0	0	1	1	0
1	1	1	0	1	1	0

This truth table implies that $Z \equiv \left[\neg G \wedge S\right]$, that is, the stone road will surely lead you to the center. (This also implies that the gold road will surely not lead you to the center, and the marble road may or may not lead you to the center, but these conclusions are not part of the solution to your problem.)

ROUGH WORK

2. Prove using the theory of loop invariance that the following function prints d, u, v, where $d = \gcd(x, y) = ux + vy$ with $d \in \mathbb{N}$ and $u, v \in \mathbb{Z}$. Assume that both the arguments x and y are supplied *positive* values. **(10)**

```
void egcd ( unsigned int x, unsigned int y )
{
   int a1, a2, u1, u2;

   a1 = x; a2 = y; u1 = 1; u2 = 0;
   while (a1 != a2) {
      if (a1 > a2) { a1 = a1 - a2; u1 = u1 - u2; }
      else         { a2 = a2 - a1; u2 = u2 - u1; }
   }
   printf("%d, %d, %d\n", a1, u1, (a1 - u1 * x) / y);
}
```

Solution The loop of the given function maintains two invariance properties.

(1) $\gcd(a_1, a_2) = \gcd(x, y)$.

(2) There exist *integers* v_1, v_2 such that $a_1 = u_1 x + v_1 y$ and $a_2 = u_2 x + v_2 y$.

Initially, $a_1 = x$ and $a_2 = y$, so Invariance (1) is true. It is maintained because $\gcd(a_1, a_2) = \gcd(a_1 - a_2, a_2) = \gcd(a_1, a_2 - a_1)$.

Invariance (2) is trickier. Given $a_1, a_2, u_1, u_2 \in \mathbb{Z}$, we can always find *unique* values for $v_1 = (a_1 - u_1 x)/y$ and $v_2 = (a_2 - u_2 x)/y$. What is important to establish in this context is that the way a_1, a_2, u_1, u_2 are updated will ensure that v_1, v_2 will always have integer values.

Initially, $v_1 = (a_1 - u_1 x)/y = (x - x)/y = 0$ and $v_2 = (a_2 - u_2 x)/y = (y - 0)/y = 1$ are integers. Assume that $a_1 > a_2$ in some iteration (the other case can be symmetrically handled). At the beginning of the loop, we have integer values for v_1, v_2 such that Invariance (2) holds, that is,

$$\begin{aligned} a_1 &= u_1 x + v_1 y, \\ a_2 &= u_2 x + v_2 y. \end{aligned}$$

But then,

$$a_1 - a_2 = (u_1 - u_2)x + (v_1 - v_2)y.$$

We update a_1 to $a_1 - a_2$, and u_1 to $u_1 - u_2$ in this case ($a_1 > a_2$). If we also update v_1 to $v_1 - v_2$ (and keep v_2 unchanged), then v_1, v_2 will continue to remain integers, and Invariance (2) will continue to hold.

The loop must terminate, because $\max(a_1, a_2)$ strictly decreases in each iteration. At the end of the loop, we have $a_1 = a_2$, so by Invariance (1), $\gcd(x, y) = \gcd(a_1, a_2) = a_1 = a_2$. Moreover, by Invariance (2), we have $\gcd(x, y) = a_1 = u_1 x + v_1 y$ for some integer v_1. This v_1 is computed as $(a_1 - u_1 x)/y$.

ROUGH WORK

3. Consider the real intervals $(0,1)$ and $[0,1]$. A function $f:(0,1)\to[0,1]$ is defined as follows. Take $x\in(0,1)$. Find (the unique) $n\in\mathbb{N}$ such that $\frac{1}{2^n}\leqslant x<\frac{1}{2^{n-1}}$. Define $f(x)=\frac{3-2^n x}{2^n}$.

(a) Prove that f is injective (one-one). **(6)**

Solution Break the domain of f into mutually disjoint intervals $I_n=\left[\frac{1}{2^n},\frac{1}{2^{n-1}}\right)$ for all $n\in\mathbb{N}$. We have $(0,1)=\bigcup_{n\in\mathbb{N}} I_n$. The codomain, on the other hand, can be decomposed as $[0,1]=\{0\}\bigcup\left(\bigcup_{n\in\mathbb{N}} J_n\right)$, where $\{0\}$ and the intervals $J_n=\left(\frac{1}{2^n},\frac{1}{2^{n-1}}\right]$ for $n\in\mathbb{N}$ are again mutually disjoint. For each $n\in\mathbb{N}$, the function f maps I_n to J_n, because

$$\begin{aligned}
x\in I_n \quad &\iff \quad \frac{1}{2^n}\leqslant x<\frac{1}{2^{n-1}}\\
&\iff \quad -\frac{1}{2^{n-1}}<-x\leqslant-\frac{1}{2^n}\\
&\iff \quad \frac{3}{2^n}-\frac{1}{2^{n-1}}<\frac{3}{2^n}-x\leqslant\frac{3}{2^n}-\frac{1}{2^n}\\
&\iff \quad \frac{1}{2^n}<\frac{3-2^n x}{2^n}\leqslant\frac{1}{2^{n-1}}\\
&\iff \quad f(x)\in J_n.
\end{aligned}$$

Moreover, the restriction of f to $I_n\to J_n$ is bijective, because (1) $f(x)=f(y)$ for $x,y\in I_n$ implies $x=y$, and (2) for each $y\in J_n$, we have $x=\frac{3-2^n y}{2^n}\in I_n$ such that $f(x)=y$. It follows that f is injective.

(b) Prove/Disprove: f is surjective (onto). **(4)**

Solution *False*. We have

$$f((0,1)) = f\left(\bigcup_{n\in\mathbb{N}} I_n\right) = \bigcup_{n\in\mathbb{N}} J_n = [0,1]\setminus\{0\},$$

that is, 0 is not in the range of f.

ROUGH WORK

4. Let the relation σ on $\mathbb{N}$ consist only of the following tuples:

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

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

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

(1) If a is even, it is related only to $a, a-1, a+1$.

(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.

- 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 $b = a$.
- 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.

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

ROUGH WORK

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

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

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

Solution *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, $lub(1,3)$ does not exist. Moreover, $lub(2,6)$, $glb(1,5)$, and $glb(2,4)$ also do not exist.

ROUGH WORK

5. Let S be the set of all infinite bit sequences. In the class, S is proved to be uncountable. The n-th element of a sequence $\alpha \in S$ is denoted by $\alpha(n)$ for $n \geqslant 0$. Prove the countability/uncountability of each of the following two subsets of S. Solve the parts independently, that is, do not use the result of any part in the other.

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

Solution 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 $|T_3| \leqslant |T_1| \leqslant |S|$ (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 $|T_1| = |T_3| = |S|$.

ROUGH WORK

(b) $T_2 = \left\{\alpha \in S \mid \alpha(n) = 1 \text{ and } \alpha(n+1) = 0 \text{ for } \underline{\text{no}}\ n \geqslant 0\right\}$. **(5)**

Solution 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 $n \geqslant 0$ number of initial 0's to $n+2 \in \mathbb{N}$. This function is clearly bijective.

ROUGH WORK

6. Let $a_0, a_1, a_2, a_3, \ldots, a_n, \ldots$ be the sequence generated by $\sum_{r \in \mathbb{N}} \frac{x^r}{1-x^r}$. Denote by p_n the parity of a_n, that is, $p_n = a_n \pmod 2$, that is, $p_n = \begin{cases} 0 & \text{if } a_n \text{ is even,} \\ 1 & \text{if } a_n \text{ is odd.} \end{cases}$ Determine all $n \in \mathbb{N}$, for which $p_n = 1$. Justify. **(10)**

Solution We have

$$\sum_{r\in\mathbb{N}} \frac{x^r}{1-x^r} = \sum_{r\in\mathbb{N}} x^r(1+x^r+x^{2r}+x^{3r}+\cdots) = \sum_{r\in\mathbb{N}} (x^r+x^{2r}+x^{3r}+x^{4r}+\cdots) = \sum_{n\in\mathbb{N}} \left(\sum_{\substack{r\in\mathbb{N} \\ r|n}} 1 \right) x^n.$$

So a_n is the number of positive (integral) divisors of n (for $n \geqslant 1$).

Claim: a_n is odd if and only if n is a perfect square.

Proof Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be the prime factorization of n. Every positive divisor of n is of the form $p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$ for integers $0 \leqslant f_i \leqslant e_i$, $i = 1, 2, 3, \ldots, t$. It follows that

$$a_n = (e_1+1)(e_2+1)\cdots(e_t+1).$$

Consequently, a_n is odd if and only if all the factors $e_i + 1$ are odd, that is, if and only if all e_i are even. ◀

Therefore $p_n = 1$ if and only if $n \in \{1^2, 2^2, 3^2, 4^2, \ldots\}$.

ROUGH WORK