

Btech 2015 Mid- Sem Examination 2016

(2)

HS 102 Culture and Human Values

Note: All the questions are compulsory

Time: 2 hrs

Marks: 30

**Q.1.** Expand on any one of the following. (200 words) **5 marks**

1. Look before you leap

2. Beauty lies in the eye of the beholder.

**Q.2.** Use the following words in your own sentence. Do any Six. **3 marks**

1. Affectation 2. Effulgent 3. Posterity 4. Diligence 5. Immanent, 6. Assimilate,

7. contemporary.

**Q.3.** Short answers questions. Do any four. (100 words) **12 marks**

1. What Shakespeare has to say about 'thought and action'?

2. What does Tagore mean by Deliverance?

3. Why is it difficult to be poor and not grumble?

4. Who is the person who finds Happiness in Truth?

5. What standard does a great man set, which is followed by the entire world?

**Q.4.** Explain the following passages in your own words.

200 words.  $5*2=10$  marks

1. Reading maketh a full man; conference a ready man; and writing an exact man; and therefore , if a man write little, he had need have a great memory; if he conferred little, he had need have a present wit; and if he read little, he had need have much cunning, to seem to know that he doth not.

2. Whenever walking in a company of three, I can always find my teacher among them. I select a good person and follow his example or I see a bad person and correct it in myself.

health  
health



**Roll No:**.....

Name:.....

**Signature:**.....

22

## Quiz-II (07 April 2017)

B. Tech (Computer Science & Engineering) IV Semester, 2017

Course Name: Computer System Architecture and Organization

Maximum Marks - 20

## **Course Code: CS202**

Total Time: 00:50 Hours

**Note:** Attempt all questions.

- Q.1. a) What is addressing modes, explain the relative and base with index addressing modes in detail with example. (05 marks)

Q.2. a) Show how the multiplication  $A \times B$  would be performed on the 6-bit unsigned numbers  $A = 111011$  and  $B = 100101$  by the Sequential Circuit Multiplier, by constructing charts similar to those discussed in class. (05 marks)

b) Multiply the following pairs of signed 2's-complement numbers using the Bit pair recoding algorithm. Assume that A is the multiplicand and B is the multiplier. (05 marks)

$$A = 110001 \text{ and } B = 101101$$

- Q.3. a) How does the excess-x representation for exponents of the scale factor in the floating-point number representation facilitate the comparison of the relative sizes of two floating-point numbers? (05 marks)

$$\begin{array}{r}
 \begin{array}{c} 8 \\ 000101 \\ 011011 \end{array} & \begin{array}{c} 5 \\ \underline{27} \\ \underline{135} \end{array} & \begin{array}{c} 1111 \\ 010011 \\ \hline 19 \end{array} & \begin{array}{c} 15 \\ 285 \\ \hline 13 \end{array}
 \end{array}$$

$$\begin{array}{r}
 011101 \quad 111001 \\
 \times 4 \quad 32 \quad 16 \quad 8 \quad 4 \quad 2 \\
 \hline
 100010 \quad 000111 \\
 \times 128 \quad \times 42 \\
 \hline
 1285 \quad 256 \\
 \hline
 285 \\
 \hline
 \end{array}$$

$$\begin{array}{r}
 1.2 \times 2 \\
 1.11 \times 2 \\
 \hline
 1.11 \times 2 \\
 \hline
 256 \\
 21 \\
 \hline
 285 \\
 \hline
 8427 \\
 100 \\
 \hline
 64 \\
 11 \\
 \hline
 75
 \end{array}$$

PDDM IIITDM JABALPUR  
CS203 DATABASE DESIGN AND MANAGEMENT  
QUIZ 2 April 06, 2017

MaxMarks 30

(23)

Roll No: 2015196

Name: Rahul Gupta

Time 1 hour

1. [1] Schema normalization is not for

- (a). reducing the number of tables in the schema.
- (b). eliminating uncontrolled redundancy of data.
- (c). eliminating anomalies that could otherwise occur with inserts.
- (d). eliminating anomalies that could otherwise occur with deletes.
- (e). ensuring that functional dependencies are enforced.

✓ 2. [1] Complete this statement: 'WHERE' and 'HAVING' are equivalent \_\_\_\_\_

✓ 3. [2] Assume a schema of Employee (Id, Name, DeptId), Deptt (Id, Name).

If there are 20 records in the Employee table and 5 records in the Deptt table, how many rows will be displayed in the result of the following SQL query:

Select \* From Employee, Deptt

Explain your answer.

✓ 4. [2] In the instance of the relation R(A,B,C,D,E) shown below, which of the following functional dependencies (FD's) hold? Justify your choice.

A	B	C	D	E
1	2	3	4	5
1	4	3	4	5
1	2	4	4	1

I. AB->C

II. B->D

III. DE->A

✓ 5. [2] Which of the following is not a relational schema and why? (The underlined attributes are to indicate the key.)

(A). marriage(wife: name of the wife,

husband: name of the husband,

when: the date when they were married)

(B). personal(name: name of the individual,

birthdate: when he or she was born,

from: where the individual lives,

hobbies: a list of that person's hobbies (references hobby))

(C). procedure(name: a unique name for this piece of code,

language: computer language it is written in (references language),

code: the code itself,

description: a description of what the code does)

(D). book(title: the title of the book,

year: the year it was published,

author: who wrote it,

publisher: who published the book,

text: the entire text of the book)

(E). disease(name: medical name of the disease,  
symptom1: boolean, whether the disease has symptom #1,

symptom1219: boolean, whether the disease has symptom #1219)

6. [2] Consider the relation R with attributes A, B, C, D, E, F, and G and with the following functional dependencies (FDs):

$$AD \rightarrow E; BE \rightarrow F; B \rightarrow C; AF \rightarrow G$$

Find the key of R.

7. [3] Consider a relation R(A, B, C, D, E) with the following functional dependencies:

$$A \rightarrow C; B \rightarrow D; \text{ and } AB \rightarrow E$$

Find the highest normal form this table is in.

8. [4+4] Consider the following database:

MOVIE(id,title,yr)

ACTOR(id,name)

CASTING(movieid,actorid)

Using this database, write the SQL commands for the following queries:

(a) Titles of all films of actress Madhubala in 1970.

(b) Movies released with the same title in a year. Display their titles and year of release.

9. [4] Is anything wrong with the following SQL query? If yes, then correct it so that it may execute properly.

```
SELECT Id, YEAR(BillingDate) AS BillingYear  
FROM Invoices  
WHERE BillingYear >= 2010;
```

10. [5] Consider the relation Student\_Performance(rollNo, name, courseNo, grade) with the following functional dependencies: A      B      C      D

name, courseNo  $\rightarrow$  grade;

rollNo, courseNo  $\rightarrow$  grade;

name  $\rightarrow$  rollNo; and rollNo  $\rightarrow$  name

[while answering consider this relation as R(A, B, C, D) and solve it in terms of A, B, C, D only.]

*keep it in the highest Normal form.*

PDPM Indian Institute of Information Technology, Design &  
Manufacturing, Jabalpur

(24)

Mid Semester Examination

**Subject Name: Management Concepts & Techniques**

**Marks: 50**

**Subject Code: MS301 (Section B)**

**Time: 2 Hrs.**

**Instruction:** Attempt any five questions and all questions carry Equal marks.  
(question number 4 is mandatory)

**Assume if any data is missing**

---

**Question 1:** Describe Short notes on (Any four)

**(10)**

- a) Capital Budgeting,
- b) Agglomeration
- c) Price Elasticity of Demand
- d) Reorder point and Lead time
- e) Bullwhip effect

**Question 2:** Suppose a regional medical warehouse is to be established to serve several Veterans Administration hospitals throughout the country. The supplies originate at  $S_1$  and  $S_2$  and are destined for hospitals at  $H_1$  through  $H_4$ . The relative locations are shown on the map grid. Other data are:

Point $i$	Products	Location	Annual Volume (Cwt.)	Rate (\$/Cwt/mi.)	$X_i$	$Y_i$
$S_1$	A	Seattle	8000	0.02	0.6	7.3
$S_2$	B	Atlanta	9500	0.02	8.6	3.0
$H_1$	A & B	New York	5500	0.05	10.6	5.2
$H_2$	A & B	Chicago	4000	0.05	7.9	5.5
$H_3$	A & B	Dallas	3000	0.05	5.5	2.4
$H_4$	A & B	Los Angeles	5000	0.05	2.0	3.0

Determine the location of new distribution centre by COG method and total cost of the location. (scaling factor 1=500 miles).

**(10)**

**Question 3:** (a) Describe the economic order quantity and mathematically determine the basic model of EOQ.

**(7)**

(24)

- (b) (a) A manufacturing company supplies vending machines and sell of soft drink by vending machine is \$ 1.80 per bottle. At that price, customer purchase 1960 bottles per week. In order to increase sell, company's management decide to decrease the price to \$ 0.8, and sales increases to 3000 bottles. so, determine the price elasticity of demand for soft drinks and write the conclusion of result. (3)

**Question 4.** Faced with court order to desegregate its school, a country school board decides to redistribute its minority students through bussing. The Plan calls for bussing 50 students from each of three cities white, black, brown to the four schools East, West, North and South. For perfect desegregation, the school need 20, 40, 30, and 60 minority students respectively. The dollar cost of bussing each student is given as follows:

City	School				50
	East	West	North	South	
White	7	6	5	4	50
Black	9	7	3	6	50
Brown	8	8	7	3	50

The school board wishes to meet the court with least cost.

- (a) Setup the transportation table/matrix for above problem.
- (b) Find an initial basic feasible solution by North West corner rule.
- (c) Determine the optimal bussing plan using u-v method.
- (d) Because of "detour" near East school for road construction, the bussing cost from every city to that school increase by \$1. Explain how this will affect your optimal solution found in (c). (11)

**Question 5:** A local distributor for a national tire company expects to sell approximately 8600 steel belt radial tires of certain size and tread design next year. The ordering cost of items \$ 65 and carrying cost is \$1.2 per tire per month. The distributor operates 280 days a year.

- \* Determine EOQ?
- \* How many times per year does the store re-order?
- \* What is the length of an order cycle?
- \* What is Total annual cost if EOQ quantity is ordered? (10)

**Question 6:** (a) Describe the types of supply chain and classification logistic decision method. (6)

- (b) Is it possible to have negative inventory level? If so, explain why? (4)



पी.डी.पी.एम.

भारतीय सूचना प्रौद्योगिकी, अभिकल्पन  
एवं विनिर्माण संस्थान जबलपुर

(25)

PDPM

Indian Institute of Information Technology,  
Design & Manufacturing Jabalpur

Dumna Airport Road, PO: Khamaria, Jabalpur 482005, INDIA

Operating System (CS306)  
Mid Semester Exam (18-09-2017)

Time: 02 hours

Max. Marks: 20

Note: Attempt all questions.

- Q.1. Write a C program using the *fork()* system call that generates the Fibonacci sequence in the child process. The number of the sequence will be provided in the command line. For example, if 5 is provided, the first five numbers in the Fibonacci sequence will be output by the child process. Because the parent and child processes have their own copies of the data, it will be necessary for the child to output the sequence. Have the parent invoke the *wait()* call to wait for the child process to complete before exiting the program. 5
- Q.2. Write a C program to create 3 new threads for Linux operating system. These threads will perform the factorial calculation of given number n, Addition of two matrices a and b and Subtraction of two matrices a and b, respectively. You can take the elements of these matrices in master thread itself. 3+2+3+2
- Q.3. Write a C program to implement First-Cum-First-Serve CPU Scheduling algorithm. 5



पी.डी.पी.एम.

भारतीय सूचना प्रौद्योगिकी, अभिकल्पन  
एवं विनिर्माण संस्थान जबलपुर

Dumna Airport Road, PO: Khamaria, Jabalpur 482005, INDIA

PDPM

Indian Institute of Information Technology,  
Design & Manufacturing Jabalpur

26

## Operating System (CS306)

### Quiz 1 (07-09-2017)

Time: 01 hours

Max. Marks: 10

Note: Attempt all questions.

- Q.1. Consider an environment in which there is a one-to-one mapping between user-level threads and kernel level threads that allows one or more threads within a process to issue blocking system calls while other threads continue to run. Explain why this model can make multithreaded programs run faster than their single threaded counterparts on a uniprocessor computer. 2
- Q.2. Measurements of a certain system have shown that the average process runs for a time  $T$  before blocking on I/O. Within  $T$ , process switch overhead is  $S$ . In other words, assume  $T$  includes the overhead for switching processes on the CPU and  $S < T$ . For the round robin scheduling policy with time quantum  $Q$ , give a formula for the CPU efficiency for each of the following. CPU efficiency is defined as the fraction of time the CPU is executing user code (not process switch time) over total time. 5
- I.  $Q > T$
  - II.  $Q = S$
  - III.  $Q$  nearly zero
- Q.3. Multiple jobs can run in parallel and finish faster than if they had run sequentially. Suppose that two jobs, each of which needs 10 minutes of CPU time, start simultaneously. How long will the last one take to complete if they run sequentially? How long if they run in parallel? Assume 50% I/O wait. 3

(28)

MM 75

Time – 02 Hours

- Q.1** Consider the following scenario of the 'Mess Management System' in IIITDM Jabalpur.

The messing facilities for the students of IIITDM Jabalpur are provided through two different, centralized messes. At the beginning of a semester, a student can opt for any mess, but after that, he/she has to dine in the same mess. There is a mess manager, who is responsible for ensuring proper functioning of the mess which includes arranging food, cleanliness, preparing mess menu (i.e. the weekly food schedule). He is also responsible for responding the queries/feedback received from the mess users.

*No days for leave.*

There is an attendance system, which records the daily attendance of the registered students in both of the messes. Based on this data, the monthly bill of the registered students is generated by the system on the first day of the next month, which each user can view through their user accounts. A registered user can pay this bill online through a hired payment gateway. A user can also see the mess menu, can provide his/her feedback on the quality of the food served or on the cleanliness in the mess. A registered user who goes out of the city on a short leave or does not wish to eat in the mess for a short duration can apply for the rebate by giving the duration and a proper reason(s), which has to be approved by the mess warden. Once approved, the mess bill will be reflecting the same.

There is a mess committee, which is responsible for ensuring the food quality as well as approving the mess menu. The convener of the mess committee is supposed to carry out regular meetings of the mess committee, and the agenda of these meetings as well as the decisions taken in the meeting have to be conveyed to all concern. Occasionally, some opinion polls can be carried out by the mess committee for which a user can participate in it and provide his/her response. All concern can see the results of such opinion polls.

Now answer the following. Please restrict your efforts to the scope of the problem as specified above unless you are told to do otherwise:

- (i) Develop a use case diagram of the problem specified as above. [10]
- (ii) Give the documentation of a use case "apply for the rebate." [10]
- (iii) The text given above represents, in some sense, the requirements of the 'Mess Management System' which we need in our institute. Identify point-wise (a) Incompleteness in the requirements given above (b) Ambiguity in the requirements given above (c) Incorrectness in the requirements given above [15]
- (iv) Give the domain model (i.e., the class diagram) for the information given in the text above [20]

**Q.2**

What are 3 P's of Software Engineering? For each of the following roles involved in the software development process, list at least four responsibilities/tasks to be undertaken by them.

- (i) Product Manager (Business Analyst)
- (ii) Project Manager (Tech Lead)
- (iii) Product Designer (Technical Architect)
- (iv) QA Person (Tester)

[20]

*are not enough*

**3D**

Note – Attempt All Questions

Time – 3 Hour

Maximum Marks 100

**Q.1** (a) Explain with suitable examples, five typical design tradeoffs that may exists between various non-functional requirements. [10]

(b) Give a schematic diagram with all required details clearly highlighting the interactions between various elements of the code to implement **one use case** of your course project module based on MVC architecture. In case you did not worked on a specific module, you can use any of the modules of the course project [10]

**Q.2** (a) Explain the following design principles with suitable examples

(i) "Separate the parts of the application those vary with the parts those do not"

[5+5]

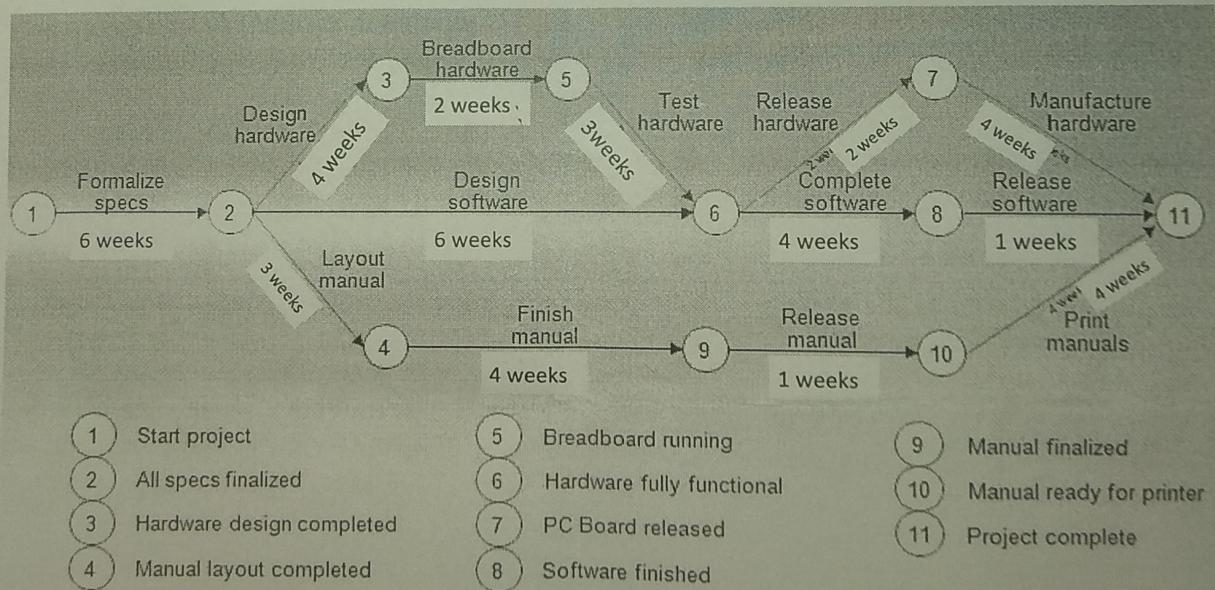
(ii) "Strive for loosely coupled designs for interacting objects"

(b) For the course project modules (any module(s)), workout at least two different problem scenarios each of which should allow to use a different design pattern to provide the solution. Sketch the design of the solution in each case. [5+5]

**Q.3** (a) (i) For the problem statement described in the SRS of your project module, give a functional (use case wise) decomposition of the module. Estimate the size of each use case in LOC. Assuming that your organization produces 300 LOC/pm with a burdened labor rate of \$8000 per person-month, estimate the effort and cost required to build the software using the LOC-based estimation technique. [5]

(ii) Use the COCOMO II model to estimate the effort and time required to build the module. Here you can assume moderate complexity and good developer/environment maturity (Hint – project in Semi-Detached Mode mode). [5]

(b) Consider the following activity graph. The number of an edge represents the number of weeks required to complete that activity



For the above activity graph, compute (Assume some date for the start of the project)

- Early start and early finish time for each task in the graph
- Late start and late finish time for each task in the graph
- slack time for each task
- Critical path of the graph

[4×2.5=10]

Q.4

32

Assume you are a test analyst working on a banking project to upgrade an existing automated teller machine system to allow customers to obtain cash advances from supported credit cards. The system should allow cash advances from 20 dollars to 500 dollars, inclusively, for all supported credit cards. The correct list of supported credit cards is American Express, Visa, Japan Credit Bank, Eurocard, and MasterCard. The user interface starts with a default amount of 100 dollars for advances, and the ATM keypad is used to increase or decrease that amount in 20-dollar increments.

Consider the following decision table that describes the handling of these transactions.

**Cash advance decision table**

Conditions	1	2	3	4	5
Supported card	N	Y	Y	Y	Y
User authenticated	-	N	Y	Y	Y
Allowed advance amount	-	-	N	Y	Y
Within available balance	-	-	-	N	Y
Actions					
Reject card	Y	Y	N	N	N
Prompt for new amount	N	N	Y	Y	N
Dispense cash	N	N	N	N	Y

Assume that you want to design a set of test cases where each of the following coverage is achieved:

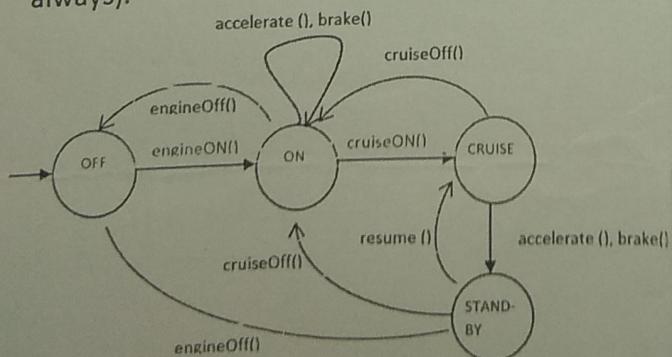
1. Decision table coverage (Cause and Effect Graphing)
2. Equivalence class partitioning (Strong Normal case)
3. Boundary values for allowed and disallowed advance amounts
4. All cases of Allowed advanced amount for each supported card and authenticated users

Design a set of test cases that achieves this level of coverage with the minimum possible number of test cases. Assume each test case consists of a single combination of conditions to create and a single combination of actions to check. How many test cases do you need in each case? Write them.

[5+10+10]

Q.5

Consider the following state model for a cruise controller where the functions indicated on the transitions represent possible action(s) when taken may cause the cruise controller to change its state (not necessarily always).



Using the state model, generate test sequences for

- (I) All-state coverage criteria
- (II) All-Transition (AT) coverage criteria
- (III) All-Transition-Pair (ATP) coverage criteria
- (IV) Transition-Tree coverage criteria [2+3+5+5]



पी.डी.पी.एम.

भारतीय सूचना प्रौद्योगिकी, अभिकल्पन  
एवं विनिर्माण संस्थान जबलपुर

Dumna Airport Road, PO: Khamaria, Jabalpur 482005, INDIA

(33)

PDPM

Indian Institute of Information Technology,  
Design & Manufacturing Jabalpur

### Operating System (CS306)

### End Semester Exam (24-11-2017)

Time: 03 hours

Max. Marks: 40

Note: Attempt all questions.

- Q.1. Consider a magnetic disk consisting of 16 heads and 400 cylinders. This disk is divided into four 100-cylinder zones with the cylinders in different zones containing 160, 200, 240 and 280 sectors, respectively. Assume that each sector contains 512 bytes, average seek time between adjacent cylinders is 1 msec and the disk rotates at 7200 RPM. Calculate the 6  
(a) disk capacity (b) maximum data transfer rate.

- Q.2. Consider a swapping system in which memory consists of the following hole sizes in 6  
memory order: 10 KB, 4 KB, 20 KB, 18 KB, 7 KB, 9 KB, 12 KB and 15 KB. Which hole  
is taken for successive segment requests of  
(a) 12 KB  
(b) 10 KB  
(c) 9 KB

For first fit? Now repeat the question for best fit, worst fit and next fit.

- Q.3. Suppose that a machine has 38-bit virtual addresses and 32-bit physical addresses. 6  
(a) What is the main advantage of a multilevel page table over a single -level one?  
(b) With a two-level page table, 16 KB pages and 4-byte entries, how many bits should be  
allocated for the top level page table field and how many for the next-level page table  
field? Explain.

- Q.4. Consider the following page reference string: 6  
1, 2, 3, 4, 2, 1, 5, 6, 2, 1, 2, 3, 7, 6, 3, 2, 1, 2, 3, 6.  
How many page faults would occur for the following replacement algorithms, assuming  
one, two, three, four, five, and six frames? Remember all frames are initially empty, so  
your first unique pages will all cost one fault each.

- LRU replacement
- FIFO replacement
- Second Chance

- Q.5. Apply the banker's algorithm for deadlock avoidance for following resource assignment  
request and calculate the order of the allocation of resources to different processes. Show  
all intermediate steps. 6



३३

पा.डी.पो.एम.

भारतीय सूचना प्रौद्योगिकी, अभिकल्पन  
एवं विनिर्माण संस्थान जबलपुर

५१

PDPM

Indian Institute of Information Technology,  
Design & Manufacturing Jabalpur

Dumna Airport Road, PO: Khamaria, Jabalpur 482005, INDIA

Process	Allocation			Max			Available		
	A	B	C	A	B	C	A	B	C
P <sub>0</sub>	0	1	0	7	5	3	3	3	2
P <sub>1</sub>	2	0	0	3	2	2			
P <sub>2</sub>	3	0	2	9	0	2			
P <sub>3</sub>	2	1	1	2	2	2			
P <sub>4</sub>	0	0	2	4	3	3			

Q.6. Explain different file operations in detail. Also explain how a file system can be 5 implemented.

Q.7. Explain the solution of Dinning Philosopher problem using Semaphores. 5

(34)

PDPM IIITDM  
B.TECH, Final-Sem EXAMINATION 2018  
HS 303  
Soft Skills and the Use of English Language

Time: 3 hours

M.M. 40

Note: - All questions are compulsory.

All Questions carry equal marks

**Q. 1.** What makes a Master Mind a Leader in every situation and never a servant? Can this notion become clearer in the light of the Upanishadic study on soft body. **(200 words, 10 marks)**

**Q.2.** Explain how better development of the soft body becomes the soft skills?

**(200 word, 10 marks)**

Or

How Purpose of life helps us form the Master Mind with the people and become a UNIT?

**✓ Q.3.** How can you study the character of a person through hand shake? Can we read the Mind of the people through the body language they display **(200 words, 10 marks)**

**Q.4.**

a. Write short notes on the following (Any Two, 150 words each, 4\*2)

**8 marks**

1. Inferential Model of communication and Logical Fallacy.
2. Prof. Ervin Laszlo and Love.
3. Upanishads and Soft Body

b. What is your impression of the course? What more could be done to enhance the Energy quotient through courses of this kind? **(100 words, 2 marks)**

*Best of Luck*



35

Mid-Semester 2018  
ES307a: Number Theory and Cryptography

Answer all the questions. Write all parts of any question at one place. Class room notations are freely used.

Max. Marks: 35

Duration: 2 Hour

- 
1. [6 marks] A small private club has only 100 members. Answer the following questions. Explain your answers briefly.
    - (a) How many secret keys are needed if all the members of the club need to send secret messages to each other?
    - (b) How many secret keys are needed if everyone trusts the president of the club? If a member needs to send a message to another member, she first sends it to the president; the president then sends the message to the other member.
    - (c) How many secret keys are needed if the president decides that the two members who need to communicate should contact him first? The president then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.
  2. [6 marks] Let  $E_k(m)$  and  $D_k(c)$  denote the encryption and decryption functions of a block cipher. Let a sequence of message blocks  $m_1, m_2, \dots$  be encrypted as ciphertext blocks  $c_1, c_2, \dots$  using the following method:  $c_i = m_{i-1} \oplus E_k(m_i \oplus c_{i-1})$ ;  $i \geq 1$  where  $m_0$  and  $c_0$  are fixed (public) initialization vectors.
    - (a) Describe how decryption is performed.
    - (b) Suppose ciphertext block  $c_i$  is damaged in transit. Which plaintext blocks become undecipherable as a result and why?
    - (c) Draw diagrams for both the encryption and decryption methods (say for  $c_i$  and  $p_i$ )
  3. [6 marks] (a) Suppose DESX was proposed to protect DES against exhaustive key search. DESX uses: one 64-bit secret key  $W$  to perform pre- and postwhitening of data and a 56-bit DES key  $K$  and it operates as follows:  $C = W \oplus DES_K(P \oplus W)$ . Show how the decryption is done?  
(b) Show that a similar construction,  $C = W \oplus DES_K(P)$  without prewhitening is insecure and can be broken using an attack of complexity  $2^{56}$ .  
(c) Devise a block cipher using DES 2 times. Explain the encryption and decryption processes of your cipher.
  4. [5 marks] For a 3 round Fiestel cipher, show that decryption of the ciphertext produces the original plaintext.

5. [7 marks] Suppose  $GF(2^8)$  modulo prime polynomial  $x^8 + x^4 + x^3 + x + 1$  over  $GF(2)$  is a Galois field. Multiply the following matrices where elements are defined over the above mentioned finite field and compute only the first two rows of the product matrix.

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

6. [5 marks] Consider the following hash function  $H$  design. The hash output is just one number between 0 and 25. The initialization vector  $h_0$  is set to 0. Let the message be split character wise, i.e.,  $M = x_0||x_1||x_2 \dots ||x_{t-1}$  (each character having value between 0 and 25, e.g., A=0, B=1, C=2, ..., Z=25). The hash output is produced as follows:

$$\begin{aligned} h_0 &= 0 \\ h_{i+1} &= f(h_i, x_i), \quad (0 \leq i \leq t-1) \\ H(M) &= h_t \end{aligned}$$

Here, the compression function  $f$  is defined as:  $f(a, b) = (a + b) \bmod 26$ .

- (a) What is the hash output for the message M=HELLO ?  
 (b) Find a valid second pre-image on the Hash value of part (a)

27/7/2025

2025

2025

(36)

PDPM IITDM

B.TECH, Mid-Sem EXAMINATION 2018

HS 303

Soft Skills and Use of English Language

M.M. 20

Time: 2 hours

Note: - All questions are compulsory.

Q. 1. Why EQ matters more than IQ? Explain, giving any three reasons as discussed by Dr. Travis Bradberry.

(150 words, 5marks)

Q.2. Elucidate on the statement of Albert Einstein, as quoted by Dr. Amen, "The intuitive mind is a sacred gift and the rational mind is a faithful servant. We have created a society that honors the servant and has forgotten the gift".

How does Dr. Amen talk about the intuitive power and logical thinking with reference to the two hemispheres of the brain in his article on PFC.

(150 words, 5marks)

Q. 3. How does Mr. Tarek Fatah in his talk emphasize on the need to cultivate EQ for a better society in India and how does he see women can help in making it such.

(150 words, 5 marks)

Q.4. a. Write a short note on **any one** of the following

✓ 1. Mirror Neurons from video of Dr. Ramchandran.

Or

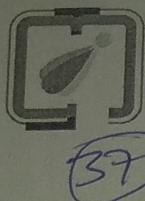
Protecting the Brain as studied by Dr. Amen.

(150 words, 3 marks)

b. What is your experience of attending classes of Soft Skills? Recommend changes, if any.

(2 marks)

Best of Luck



पी.डी.पी.एम.

भारतीय सूचना प्रौद्योगिकी, अभिकल्पन  
एवं विनिर्माण संस्थान जबलपुर

Dumna Airport Road, PO: Khamaria, Jabalpur 482005, INDIA

PDPM

Indian Institute of Information Technology,  
Design & Manufacturing Jabalpur

(37)

### Parallel Algorithms (CS631)

#### Quiz 1 (06-02-2018)

Time: 01 hours

Max. Marks: 10

Note: Attempt any ONE Section.

#### Section 1 (MPI)

- Q.1. Let us assume that 5 processors are arranged in a TORUS in ascending order of their processor ID. Let us also assume that processor with ID 0 is working as master node and I/O has to be performed from this processor only. Write a program using MPI and C which can calculate ADDITION, SUBTRACTION, MULTIPLICATION, DIVISION and MODULUS operation on two given input numbers on different processors. One processor has to perform only one operation. 5

- Q.2. Let us assume that processors are connected in HYPERCUBE model. Write a program using MPI and C to send the same data to all the nodes of the model. You also have to receive the data from all the nodes to the sending node.

*B. Gaitonde  
Result  
Gaitonde*

#### Section 2(CUDA)

- Q.1. Let us assume that two vectors A and B of the size  $N$  are there in the memory of the HOST machine. Write a program using CUDA and C to perform the addition of these two vectors on DEVICE. You have to invoke only as many threads as there are number of elements in each vector. Result has to be displayed by HOST. 5

- Q.1. Let us assume that there is a system of HOST and DEVICE. A thread of DEVICE has produces a result of the addition of TWO numbers i.e.  $c = a+b$ . Now another thread has to perform a operation  $e = d*c$ . Write a program using CUDA and C to perform these operations. I/O will be performed by HOST. 5

(3B)

**CS621 Image Processing**  
End semester Exam (Part B) - April 23, 2018

MM: 65

Time: 2 hours 10 mins

Note: All questions are compulsory. Be precise in writing answers.

- Q1. [5] Compute Laplacian of Gaussian (LOG), where  $G(x, y)$  is the Guassian function  $e^{-\frac{1}{2\sigma^2}(x^2+y^2)}$ .
- Q2. [5] Consider a  $3 \times 3$  filter that averages the two closest top and bottom neighbours of  $f(x, y)$ , but excludes the point itself from the average.
- Show the filter
  - Compute the frequency response of the filter
  - Check if it is a low pass filter

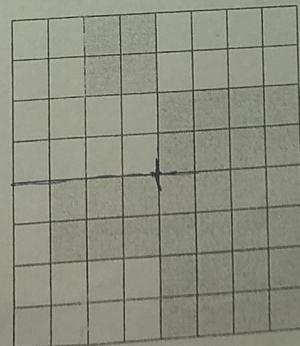
Use the following transformation property of Fourier transform:

$$f(x - x_0, y - y_0) \leftrightarrow F(u, v)e^{-i2\pi(\frac{ux_0}{M} + \frac{vy_0}{N})}$$

- Q3. [5] Generate the runlength representation of the following small image (each square represent a binary pixel). Use "EOL" symbol to show the end of each line.

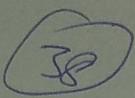
1	1	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	0	1
0	0	0	0	0
1	0	0	0	1
1	0	0	0	1
1	0	1	1	0
1	1	1	1	0

- Q4. [5] Represent the following image by a quadtree, where each square represent a binary pixel. Show the partitioning and merging process separately. For partitioning use notation  $R_{ij}$  to represent region, where  $i$  denotes the level number of partitioning and  $j$  denotes the region (1-4: top left, top right, bottom left, and bottom right). For merging use the notation as:  $R_{i134}$  shows merging of regions  $R_{i1}$ ,  $R_{i3}$ , and  $R_{i4}$ .



- Q5. [5] Consider the following  $4 \times 4$  image with 4-gray-levels present. Calculate GLCM by taking offset distance as 1 and offset direction as North. Use this GLCM to find the contrast of this image.

$$I_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 2 & 3 & 3 & 3 \end{bmatrix}$$



Q6. [6] Histogram equalize the following  $8 \times 8$  image where the pixels take on values  $\{0, 1, \dots, 7\}$ .

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
1	1	1	2	2	2	3	4
1	1	1	2	2	2	3	4
1	1	1	2	2	2	3	4
1	1	1	2	2	2	3	5
2	2	2	2	2	5	5	5
6	6	6	6	7	7	5	5

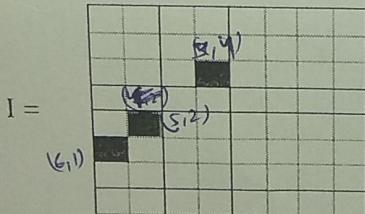
Q7. [6] Consider the chain code for digit '8' as 00012231234445675667 for font size  $8 \times 6$ . Find its formfactor  $\left(\frac{4\pi \cdot \text{Area}}{\text{Perimeter}^2}\right)$ .

Q8. [7] The colors (in symbol) and their probabilities for an image are given as:

Color symbol	C1	C2	C3	C4	C5	C6	C7	C8
Probability	0.19	0.25	0.21	0.16	0.08	0.06	0.03	0.02

Find out the Huffman code (form the code by keeping lesser probability symbol on the left side of the tree). Based on this code, decode a scan line of the image given as 111011111000111110110.

Q9. [7] Consider the following binary image I. Complete the table to express the Hough transform in the corresponding polar coordinates.



$\theta/\rho$	0	1	$\sqrt{2}$	2	$2\sqrt{2}$	3	$4\sqrt{2}$	5
0								
$\pi/4$								
$\pi/2$								
$3\pi/4$								

Identify the item receiving the most votes and deduce the equation of the line in polar coordinates, which connects three points of the image

Q10. [4+4+3+3] Perform dilation, erosion, opening and closing operations on the image given below with the given structuring element. Origin of the structuring element is its center.

$$I = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad SE = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

(39)

**CS621 Image Processing**

Mid semester Exam – February 22, 2018

Time: 2 hours

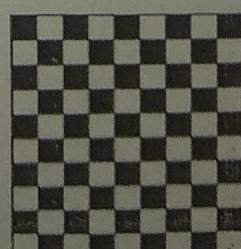
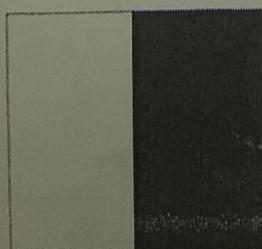
MM: 40

1. [1] Digitizing the coordinate values is \_\_\_\_\_ and digitizing the amplitude values is \_\_\_\_\_.
- ✓ 2. [1] Choose the best answer. Let  $G(\omega)$  be the Fourier transform of a signal  $g(x)$ . As you vary  $\omega$ , a plot of  $|G(\omega)|^2$  reveals:
  - How the energy of a periodic signal is concentrated at continuous frequencies.
  - How the energy of the signal is distributed as a function of frequency.
  - How two different signals can have the same energy and phase distribution.
  - None of these is true.
3. [1] Read the following statements and mention the correct ones.
  - $g(x)$  and  $g(x - a)$  have the same energy distribution as a function of time.
  - The respective Fourier transforms of  $g(x)$  and  $g(x - a)$  differ only by a linear phase term.
  - $g(x)$  and  $g(x - a)$  have the same energy distribution as a function of frequency.
- ✓ 4. [1] Which arithmetic operation can be used to detect motion?
- ✓ 5. [2] Consider the following  $4 \times 4$  image represented by 8-bit integers:

$$I = \begin{bmatrix} 157 & 165 & 141 & 93 \\ 205 & 50 & 88 & 130 \\ 250 & 147 & 157 & 100 \\ 101 & 193 & 155 & 100 \end{bmatrix}$$

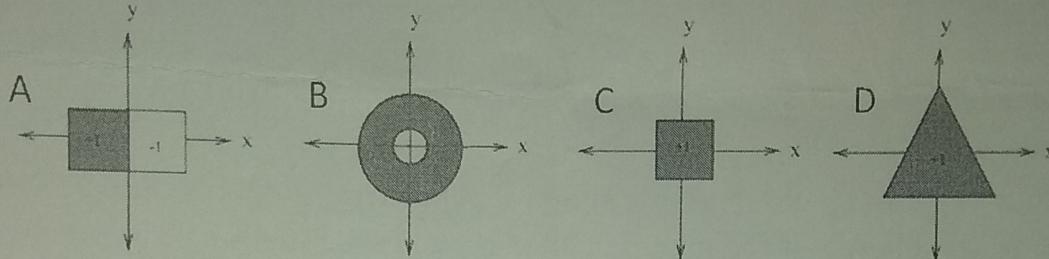
Use an arithmetic operation to get this image defined with 5-bit integers.

6. [3] Establish a grey scale transformation that maps the darkest 5% of the image pixels to black, the brightest 10% of pixels to white (255) and linearly transforms the grey values of all remaining pixels between black and white.
- ✓ 7. [3] Consider the following images of size  $256 \times 256$ . How their histogram will look before and after smoothing operation. (Calculations are not required, only logical answer is required.)



(39)

8. [3] How separability property of DFT helps in reducing complexity of its calculation? Explain.
9. [4] Consider the images shown below (A to D). Using knowledge of the properties of Fourier transform (not exact calculation), explain which image(s) have Fourier transforms,  $F(u,v)$  with  $F(0,0) = 0$ . Assume that the shaded regions has value +1 and white region has value -1 in these images.



10. [5] Consider the image given on the right side. For  $V = \{1, 2\}$ , label the connected components using 4-connected components algorithm. While answering make use of labels a, b, c, d... In case of ambiguity consider labels in the alphabetic order.

0	0	0	1	1	1	0	0
0	0	0	1	1	0	1	0
0	2	1	0	1	0	1	1
0	1	1	1	2	0	1	1
0	0	2	1	2	0	2	1
1	2	0	2	0	0	1	0
0	0	1	0	0	0	1	0
0	0	0	0	0	1	1	1

11. [5] Suppose that an image with intensities (continuous) in the range  $[0, 1]$  has the PDF  $P_r(r) = -2r + 2, 0 \leq r \leq 1$ . Find the transformation function you would use for histogram equalization. Also verify that the PDF of the intensities in the new image is uniform.
12. [5] Show that subtracting the Laplacian from an image is proportional to the mask used in unsharp masking.
13. [6] Apply a  $3 \times 3$  median filter to the image  $I$  given below to produce an  $3 \times 3$  output image. Assume zeros outside of the image. Mention one general advantage and one general disadvantage of the median filter as compared to the mean filter as demonstrated by the result.

$$I = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 8 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

(10)

QUIZ 2Cryptography and Number TheoryTotal Marks: 15Duration: 1 hourQ1. If  $x \equiv a \pmod{m_1}$ 

$$x \equiv a \pmod{m_2},$$

Where,  $m_1$  and  $m_2$  are relatively prime. Then, show  $x \equiv a \pmod{(m_1 \times m_2)}$ **3 marks**Q2. Prove  $dlog_{a,p}(xy) \equiv [dlog_{a,p}(x) + dlog_{a,p}(y)] \pmod{\phi(p)}$  where,  $\phi(p)$  denotes Euler's Totient and p is a prime number**4 marks**Q3. Prove  $\phi(p^i) = p^i - p^{i-1}$  where,  $\phi(p)$  denotes Euler's Totient and p is a prime number**4 marks**HINT: Try to find numbers that are not relatively prime to  $p^i$ 

Q4. Using Fermat's theorem, find the solution of the linear congruence:

$$4x \equiv 11 \pmod{19}$$

**4 marks**HINT:  $x \equiv 11 \times (4^{-1}) \pmod{19}$ 

$$\begin{array}{r}
 15 \quad 45 \quad 45 \quad 4 \\
 \overline{+} \quad \overline{+} \quad \overline{+} \quad \overline{+} \\
 60 \quad 8 \times 16 \quad 128 \\
 \overline{-} \quad \overline{-} \quad \overline{-} \\
 14
 \end{array}$$



(41)

End-Semester 2018  
ES307a: Number Theory and Cryptography

Answer all the questions. Write all parts of any question at one place. Class room notations are freely used.

Max. Marks: 60

Duration: 3 Hour

1. [20 marks] Answer the following questions. Write precise answer (Preferably using no more than 3-4 sentences).
- ✓ (a) Is AES a Feistel cipher? Why/why not?
  - ✓ (b) Do you think RSA cryptosystem is secure? Justify your answer.
  - ✓ (c) Do you think ElGamal cryptosystem is secure? Justify your answer.
  - ✓ (d) What is the advantage of using primitive root in Diffie-Hellman key exchange protocol?
  - ✓ (e) What is the difference between digital signature and digital certificate?
  - ✓ (f) What is the main advantage of Elliptic curve cryptography?
  - ✓ (g) Describe an efficient way to calculate  $180P$ , where  $P$  is any point on the elliptic curve.
  - ✓ (h) What is the use of nonce in the key distribution?
  - ✓ (i) In what order should the signature function and the confidentiality function be applied to a message and why?
  - ✓ (j) How does a private key signature ensure non-repudiability?
2. [5 marks] Answer the questions below regarding key generation with Diffie-Hellman and RSA.
- ✓ (a) Suppose the Diffie-Hellman public values  $q$  and  $\alpha$  are 7, 4 respectively and private key  $x = 4$ . Compute a legitimate  $y$  value.
  - ✓ (b) Suppose your partner's  $y$  value is 3. What is your shared key?
  - ✓ (c) Suppose that you are computing an RSA key pair. What are  $p$  and  $q$  and  $\Phi(n)$  for an  $n = 51$ ?
  - ✓ (d) Find a legal RSA public key pair for this  $p$  and  $q$ .
  - ✓ (e) How many possible values for  $c$  are there?
3. [5 marks] A and B are communicating using the ElGamal cryptosystem with prime  $q = 23$  and primitive root of  $q$ ,  $\alpha = 7$ .
- ✓ (a) B creates her public key by choosing the private key  $a = 5$ . What is B's public key?
  - ✓ (b) A wants to send the message '3' to B. Demonstrate how A encrypts the message.

(Q1)

- (c) B receives the encrypted message  $(r, t) = (9, 6)$  from A. What is his plaintext message?

4. (a) [3 marks] Prove that  $\Phi(pq) = (p-1)(q-1)$  where p and q are primes and  $\Phi$  is Euler's totient function.

- (b) [2 marks] Using square and multiply method, calculate:  $5^{117} \bmod 19$

- (c) [3 marks] Solve for  $x$  using Chinese Remainder Theorem

$$2x \equiv 5 \bmod 7$$

$$3x \equiv 4 \bmod 8$$

- (d) [2 marks] Is Miller-Rabin primality testing algorithm deterministic? Justify your answer.

5. (a) [5 marks] Draw and explain HMAC construction.

- (b) [5 marks] Under a fixed key, for different messages, why is it insecure to use a randomized IV for CBC-MAC tag generation for each of the messages instead of a fixed all zero IV? Explain your answer with an attack.

- (c) [5 marks] Let  $n$  be a large integer. Let a cryptographic hash function  $h$  be defined as:  $h(m) = m \pmod n$ , where the output of  $h$  is regarded as an integer between 0 and  $n-1$ . Show that  $h$  does not satisfy preimage and collision resistant cryptographic hash properties.

6. (a) [3 marks] Alice can use only the shift cipher(given below) on her computer to send a message to a friend.

$$\text{Shift Cipher : } |P| = |C| = |K| = 26$$

$$\text{Encryption : } c = (p + k) \pmod{26}$$

$$\text{Decryption : } p = (c - k) \pmod{26}$$

She thinks that her message will be more secure if she encrypts the message two times, each time with a different key.

1. What is the equation for encryption and decryption now?

2. Is she right in her security assumption? Defend your answer.

- (b) [1 mark] Charlie secretly gets access to Alice's computer and using her cipher types "abcdefghijkl". The screen shows "PQRSTUVWXYZ". If Charlie knows that Alice is using substitution cipher, what type of attack Charlie launched?

- (c) [1 mark] John is reading a mystery book. In the first chapter, the author gives a ciphertext "CIW" and two paragraphs later, the author tells the reader that this is a shift cipher and the plaintext is "flz". In the next chapter, another ciphertext "XVIEWYWI" is given and John immediately found the actual meaning of the ciphertext. What type of attack did John launch here?

36  
19  
2017  
17  
12  
99  
95  
9



(Ques.)

NUMBER THEORY AND CRYPTOGRAPHY

Answer all the questions. Write all parts of any question in one place. Class room  
notations are freely used.

Max. Marks: 20

Duration: 1 Hour

Q. 1 [10 marks] Let irreducible polynomial  $m(x) = x^3 + x + 1$  over  $GF(2)$ . Prove the following:

(a)  $GF(2^3)$  is an integral domain.

(b) For every non-zero element  $a \in GF(2^3)$  there is always a unique element  $b \in GF(2^3)$  such that  $a \cdot b \equiv 1 \pmod{m(x)}$ .

Q. 2 [10 marks] Let a primitive polynomial  $f(x) = x^4 + x + 1$  over  $GF(2)$ .

(a) Construct the Galois field of 16 elements,  $GF(2^4)$ , using the primitive polynomial  $f(x)$ . Compute the powers  $x^i, 0 \leq i \leq 14$  and represent these powers as polynomials of the form  $a_0 + a_1x + a_2x^2 + a_3x^3$ .

(b) Assume that we want to implement an S box using the Galois field from (a). If we would like that our S box is bijective is it a good choice to use function  $S: GF(2^4) \rightarrow GF(2^4)$  defined by  $x \in GF(2^4) \mapsto x^3 \in GF(2^4)$ . (Note that the order of any element divides the order of the group)

Q. 3 [10 marks] Answer the following questions. Write precise answer (Preferably using one line answers. Not more than 3-4 sentences).

(i) What is the difference between an unconditionally secure cipher and computationally secure cipher?

(ii) Briefly describe the difference between chosen plain text and chosen cipher text attacks.

Define confusion and diffusion.

(iii) If  $F$  is a cipher using a finite field (with  $p$  elements), why is that not good enough for security? At least, we need finite fields of the form  $GF(2^n)$ ?

(iv) Assuming you can do  $2^{20}$  encryptions per second and the key size is 40 bits, how long would a brute force attack take to reveal the key? What happens if you know specific properties of the cipher?

\*\*\*\*\*GOOD LUCK\*\*\*\*\*

(93)

## Mid-Semester Examination

### Mathematics for Discrete Domain

Max.Marks 15

Max. Time 1 hours

1. Let  $H, K$  are two subgroups of a group  $G$ , then  $HK$  is a subgroup of  $G$ , iff  $HK = KH$ .  
5
2. Let  $(G, *)$  be a group and except the identity element order of all the other elements  
is 2. Then show that group in abelian.  
4
3. Out of following four permutations, identify same permutations:  
6
  - a.  $A := (3, 2, 4, 5)$
  - b.  $B := (2, 4)(5, 2)(3, 2)$
  - c.  $C := (4, 5)(4, 3)(4, 2)(2, 3)(3, 2)$
  - d.  $D := (3, 2)(3, 1)(1, 3)(3, 5)(3, 4)$

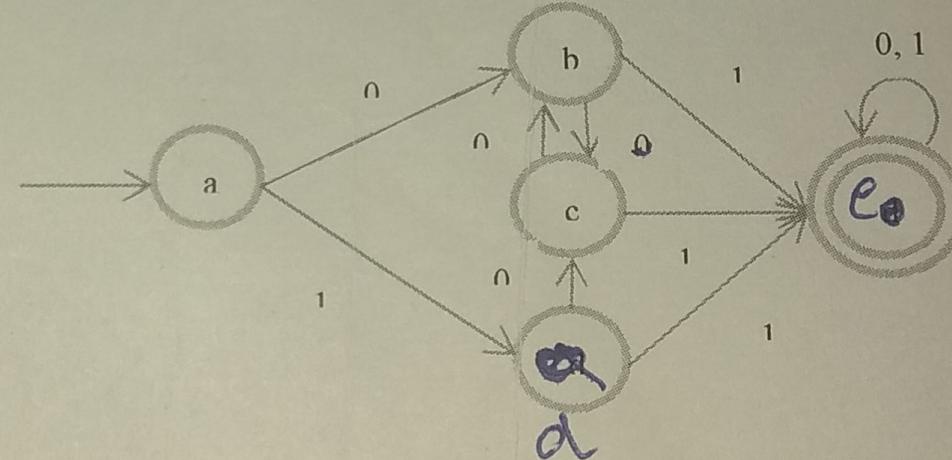
MS

PDPM Indian Institute of Information Technology, Design and Manufacturing Jabalpur  
Language Theory (CS205)  
Quiz-I

Time: 45 Minutes

Marks: 10

4. Construct a minimal DFA which accepts set of all strings over  $\{a, b\}$  in which number of a's are divisible by 3 and number of b's are divisible by 2. 3
5. Construct a Moore machine that takes binary no's as input and produce residue modulo '3' as output. Convert the created Moore machine to Mealy machine.  $3+2=5$
6. Minimize the following DFA 2



Time: 3 hours

Marks: 55

(Attach the question paper with the answer sheet after examination)

1. Consider a CFG  $G = (V, \Sigma, P, S)$  and a string  $w = \text{"he eats a fruit with a spoon"}$  where  $V = (\text{NP}, \text{VP}, V, \text{PP}, N, P)$ ;  $\Sigma = (\text{a, eats, fruit, he, spoon, with})$ ;  $S$  is the starting symbol and  $P$  are finite set of rules, which are as follows:

$$\begin{array}{lllllll} S \rightarrow \text{NP VP} & \text{VP} \rightarrow \text{VP PP} & \text{VP} \rightarrow V \text{ NP} & \text{VP} \rightarrow \text{eats} & \text{PP} \rightarrow P \text{ NP} & & \text{NP} \rightarrow \text{Det N} \\ \text{NP} \rightarrow \text{he} & \text{V} \rightarrow \text{eats} & \text{P} \rightarrow \text{with} & \text{N} \rightarrow \text{fruit} & \text{N} \rightarrow \text{spoon} & & \text{Det} \rightarrow \text{a} \end{array}$$

Is  $w$  in  $L(G)$ ? Use CYK algorithm.

4

2. Construct a PDA for  $L(M_1) = \{w \in \Sigma^* \mid w \text{ is a legal arithmetic expression}\}$  where,  $\Sigma = \{\text{int, +, *, (, )}\}$ . After constructing, take one string ' $w$ ' and verify that ' $w$ ' is accepted by  $M_1$ .

4

3. Construct a T.M.,  $M_2 = (Q, \Sigma, \tau, \delta, q_0, F)$  for converting a unary to a binary number where,  $Q = (q_0, q_1, q_2, q_3, q_4)$ ,  $\Sigma = \{1\}$ ,  $\tau = \{1, X, A, B, \text{blank space}\}$ . After constructing, consider the following example and show if the input is ...1111... it produces output ...BAAXXX...

4

Hints: The A and B in  $\tau$  are used to represent binary 0 and 1 respectively. The 1 in  $\Sigma$  represents unary bit.

Input tape	...	blank space	blank space	blank space	blank space	1	1	1	1	blank space	...
Output tape	...	blank space	B	A	A	X	X	X	X	blank space	...

Let  $A = \{0, 1\}$  and  $L = A^*$ , let  $R = \{0^n 1^n, n > 0\}$ . The language LUR and R are respectively,

- a) Regular, regular
- b) Not regular, regular
- c) Regular, not regular
- d) Not regular, not regular

Justify your answer with an example.

2

5. Write the regular expression of the following language:

$$L = \{a^n \mid n \text{ is divisible by 2 or 3 or } n=5\}$$

1

6. Construct a regular grammar, which can be generated the set of all strings starting with a letter (A to Z) followed by a string of letters or digits (0 to 9).

2

7. Show that the language  $L = \{a^{n^2} \mid n \geq 1\}$  is not CF.

2

8. Construct a PDA 'A' equivalent to the following CFG:  $S \rightarrow 0BB$ ,  $B \rightarrow 0S|1S|0$ . Test whether  $010^4$  is in  $N(A)$ .

3+2=5

9. Consider the following grammar:

$$A \rightarrow A\$B|B \quad B \rightarrow B\#C|C \quad C \rightarrow C@D|D \quad D \rightarrow d$$

2

Write the name of the operators in ascending order according to their precedence. Justify your answer.

(53)

10. Write a CSG but not a CFG for a language  $L = \{a^n b^n c^n\}$  and draw a right-most derivation tree for  $a^2 b^2 c^2$ .  $4+2=6$
11. Prove the following CGF is ambiguous using a string in C programming.  
 $\langle \text{cmd} \rangle \rightarrow (\text{if} \langle \text{bool} \rangle \text{then} \langle \text{cmd} \rangle) \mid (\text{if} \langle \text{bool} \rangle \text{then} \langle \text{cmd} \rangle \text{else} \langle \text{cmd} \rangle)$   $3$
12. Prove Ambiguity problem in CFG is undecidable.  $4$
13. Prove  $L = \{\omega_i \mid \omega_i \text{ is not accepted by } T_i\}$  is not recursively enumerable and  $\bar{L}$  is recursively enumerable but not recursive.  $3+3=6$
14. Consider a right linear grammar  $A \rightarrow aB \quad B \rightarrow aB \mid bB \mid \epsilon$ . Write the left linear grammar of the right linear grammar. Describe the procedure.  $4$
15. Prove that  $R$  (real number) is an uncountable set.  $3$
16. Mention the limitation of non-deterministic grammar. How will you overcome the limitation of the non-deterministic grammar? Use a suitable example to justify your answer.  $1+1+1=3$

-----END-----

Endsem Examination, April 2017

## B. Tech (Computer Science &amp; Engineering) IV Semester, 2017

Course Name: Computer System Organization and Architecture

Maximum Marks – 100

Course Code: CS202

Total Time: 03:00 Hours

**Note:** Attempt all questions. All questions carry equal marks.

**Q.1** a) Program execution time, T, as defined in Basic Performance Equation, is to be examined for a certain high-level language program. The program can be run on a RISC or a CISC computer. Both computers use pipelined instruction execution, but pipelining in the RISC machine is more effective than in the CISC machine. Specifically, the effective value of S in the T expression for the RISC machine is 1.2, but it is only 1.5 for the CISC machine. Both machines have the same clock rate, R. What is the largest allowable value for N, the number of instructions executed on the CISC machine, expressed as a percentage of the N value for the RISC machine, if time for execution on the CISC machine is to be no longer than that on the RISC machine? (05 Marks)

b) Consider the base-3 (ternary) system, in which the unsigned, 5-digit number  $t_4t_3t_2t_1t_0$  has the value  $t_4 \times 3^4 + t_3 \times 3^3 + t_2 \times 3^2 + t_1 \times 3^1 + t_0 \times 3^0$ , with  $0 \leq t_i \leq 2$ . Express each of the decimal values 56, -37, and 122, and as 6-digit, signed, ternary numbers in the 3's-complement system, perform addition on them in all possible pairwise combinations, and state whether or not arithmetic overflow occurs for each operation performed. (06 marks)

c) Consider a memory system that uses a 32-bit address to address at the byte level, plus a cache that uses a 128-byte block size. (03 marks each)

i.) Assume a direct mapped cache with a tag field in the address of 19 bits. Show the address format and determine the following parameters: number of addressable units, number of blocks in main memory, number of blocks in cache.

ii.) Assume an associative cache. Show the address format and determine the following parameters: number of addressable units, number of blocks in main memory, number of blocks in cache, size of tag.

iii.) Assume a four-way set-associative cache with a tag field in the address of 9 bits. Show the address format and determine the following parameters: number of addressable units, number of blocks in main memory, number of blocks in set, number of sets in cache, number of blocks in cache, size of tag.

**Q.2** a) A byte-addressable computer has a small data cache capable of holding eight 32-bit words. Each cache block consists of two 32-bit word. When a given program is executed, the processor reads data from the following sequence of hex addresses:



- 15
- it improves the performance of Virtual Memory? (04 + 04 marks)
- c) Draw a block diagram organization for a 8M x 32 memory implemented using 512K x 8 memory chips. (06 marks)
- Q.3 a) A 1024 x 1024 array of 32-bit numbers is to be "normalized" as follows. For each column, the largest element is found and all elements of the column are divided by this maximum value. Assume that each page in the virtual memory consists of 4K bytes, and that 1M bytes of the main memory are allocated for storing data during this computation.
- How many page faults would occur if the elements of the array are stored in column order in the virtual memory? (03 marks)
  - How many page faults would occur if the elements are stored in row order? (03 marks)
- b) A one-level SRAM cache has  $n$  times shorter cycle time compared to the main memory. Show that it will provide an average memory access speed up of  $n/(1+mn)$ , where  $m$  is the miss rate. (06 marks)
- c) Explain the design mechanism of Fast Carry Lookahead Adder in detail, and also describe its advantages and limitations. (08 marks)
- Q.4 a) Show that the logic expression  $c_n \otimes c_{n-1}$  is a correct indicator of overflow in the addition of 2's-complement integers, by using an appropriate truth table. (04 marks)
- b) Multiply each of the following pairs of signed 2's-complement numbers. In each case, assume that A is the multiplicand and B is the multiplier. (03 marks each)
  - A = 010111 and B = 110110 (using the Booth algorithm.)
  - A = 110011 and B = 101100 (using the Booth algorithm.)
  - A = 110101 and B = 011011 (using the Bit-pair Recording algorithm.)
  - A = 001111 and B = 001111 (using the Bit-pair Recording algorithm.)

c) Divide the following dividend with divisor using Restoring division method. (04 marks)

Dividend : 11010    Divisor : 101

Q.5 a) Draw the block diagram of Simple single processor bus processor organization and three bus processor organization and also compare each other in detail. (08 marks)

b) Write the sequence of control steps required for the Single bus processor for each of the following instructions:

  - Add the contents of memory location NUM to register R1. (03 marks)
  - Add the contents of the memory location whose address is at memory location NUM to register R1. (03 marks)

Assume that each instruction consists of two words. The first word specifies the operation and the addressing mode, and the second word contains the number NUM.

c) What is vertical organization of microinstruction? State the design strategy of a vertical organization based micro-programmed control unit.? (06 marks)

PDPM IIITDM JABALPUR  
CS203 DATABASE DESIGN AND MANAGEMENT  
EndSem Exam April 27, 2017

Part-B

MaxMarks 80

Roll No: 8015196

Name: Rahul Gupta

Time 2.5 hours

Note: You are supposed to give reasons or show the steps in each answer as applicable.

- [2] Tell (with reason) if the following statement is true/false:  
"A foreign key declaration can always be replaced by an equivalent check assertion in SQL."
- [2] Consider the two transactions whose execution is interleaved as follows:

T1	T2
	Read X
Read X	
Read Y	
	Write Y
Write Y	
	Write Z
commit	
	commit

Can this interleaving be generated by a database that uses strict two-phase locking for concurrency control? Justify your choice.

- [3] Consider the following relation Employee and answer the query given below:

id	name	deptt	salary
1	Juhi	CS	14000
2	Manjeet	EM	8000
3	Ladli	CS	10000
4	Some	EE	5000

SELECT max(salary) FROM Employee  
WHERE salary NOT IN (SELECT max(salary)FROM Employee)

- [4] Consider two relations R1(X,Y) and R2(Y,Z) with the only keys as mentioned. Let relation R3(X,Y,Z) be the natural join of R1 and R2. Find the dependencies which must hold in R3.

- [4] Give the resulting table for expression (show intermediate results also):

$$\pi_{A,B}(R * S) * \pi_{A,C}(S * T)$$

where tables R, S, and T are:

R	
A	B
1	2
3	2
5	6
7	8
9	8

S	
B	C
6	2
2	4
8	1
8	3
2	5

T	
A	C
7	1
1	2
9	3
5	4
3	5

6. [5] Below is a schema for a relational database table, written in SQL DDL. However, it has (at least) 5 errors in syntax. What are these errors? (Note: it's not the choice of lower or upper case, either is acceptable in SQL.).

create table film (

filmid	integer,	null primary key , in year ( )
title	varchar(30),	
year	integer	
director name	varchar(30) not null,	
language	varchar(15),	
primary key (filmid),		
foreign key director name references director,		
foreign key (leading actor) references actor		

- [6] Relation R has eight attributes A,B,C,D,E,F,G,H. Fields of R contain only atomic values.  $F = \{CH \rightarrow G, A \rightarrow BC, B \rightarrow CFH, E \rightarrow A, F \rightarrow EG\}$  is the set of functional dependencies that hold for R.

- (a) Find candidate keys of the relation R.
- (b) Find the highest normal form R satisfies.

- [6] Given these contents of the Customers table:

Id	Name	ReferredBy
1	Maya	6
2	Ravindra	4
3	Sarthak	NULL
4	Abeer	NULL
5	Payal	4
6	Pahuni	NULL

Here is a query written to return the list of customers not referred by Abeer:

SELECT Name FROM Customers WHERE ReferredBy <> 4;

- (a). What will be the result of the query? Why?
- (b). What would be a better way to write it?

- [6] Consider the following tables from a database:

Drink(drinkname, manfname) and Sells(shopid, drinkname, priceinrs)

Write an assertion to ensure that "The minimum price charged for products made by Pepsi is Rs. 25."

- [6] Consider a relation Book(bookid, price, topic) storing book id, its price, and the area/topic it belongs to. Suppose you are the owner of this relation and you wish to give user Naman authorization to browse the books with price more than Rs. 2000 and on the topics where less than 20 books are available.

Y7

11. [6] Consider a business environment where you are purchasing items and storing its information in the table Product (id, description, quantity, unitcost). While entering cost of the item in table product you wish to include your profit margin and therefore you store that unitcost of the item on which you will sell it in the market. Consider the following policy of your company to get the profit:

"If the cost is less than Rs. 500, the cost is actually Rs. 550. If the cost is over Rs. 500 but less than Rs. 1000, then our cost becomes Rs. 1100. But if the cost exceeds Rs. 1000, then the cost is increased by 20%.

Complete the following trigger:

CREATE TRIGGER 'update\_cost'

BEGIN

.....  
END

12. [6] Prove that any relation schema R with two attributes, say A and B, is in BCNF.

13. [4] Consider the following Tables:

Person(pid,cid,salary) and Shareholding(pid,cid,nshares)

where pid is person identifier, cid is company identifier, nshares is number of shares.

Each person is employed by exactly one company, but may hold any number of shares of any company.

Write a query in relational algebra to find the id of persons who do not own stocks of the company where they works.

14. [12] Consider the following tables:

Works(Ename,Cname,Salary), Elives(Ename,City), and Locatedin(Cname,City)

where Ename is employee name, Cname is company name, City is city name, Salary is the monthly income of employee, and Mgrname is manager name.

Write the following queries in SQL (in case of renaming of any attribute or table name, rename it as its first letter):

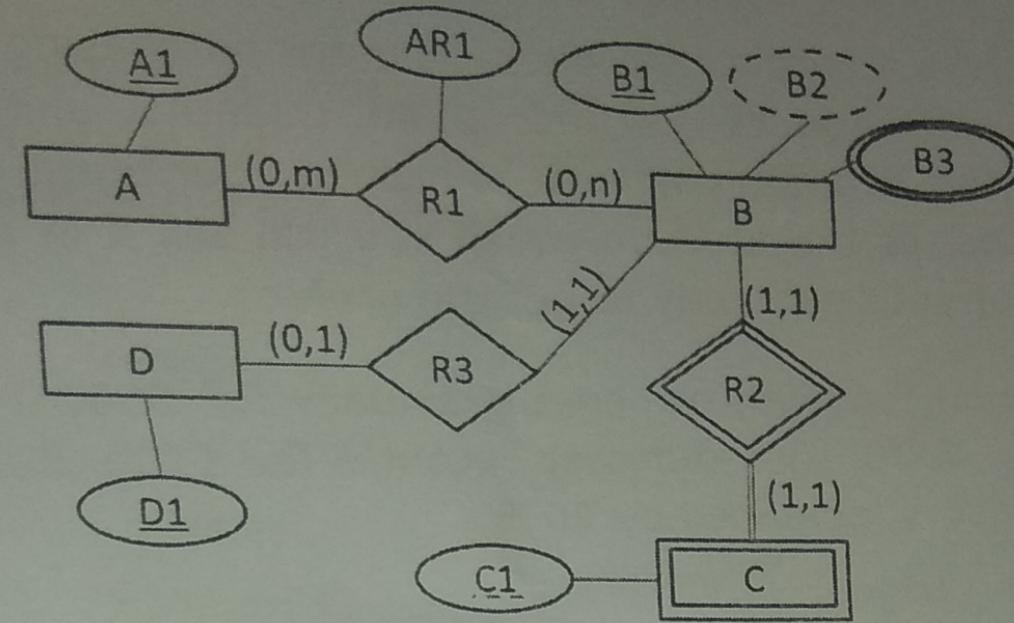
(a). List the name of employees who work in company 'Oracle' along with the cities they live in. (write it through join as well as using subquery)

(b). List the employees who live and work in the same cities. (write it using join)

(c). List the employees having salaries more than all of the employees in 'Oracle' company. (write it without using max function)

15. [8] Convert the following ER model (given on the next page) into relational model keeping the minimum number of tables needed to represent.

97



(M8)

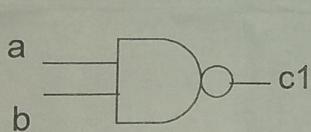
Name:

Roll Number:

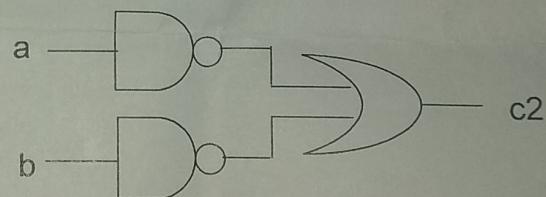
(1) Classify the following 16 logic functions with NPN equivalence.

x	y	f	x	y	f	x	y	f	x	y	f	x	y	f	x	y	f
0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1
0	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0	1	1
1	0	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0	1
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
a																	
x	y	f	x	y	f	x	y	f	x	y	f	x	y	f	x	y	f
0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1
0	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0	1	1
1	0	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

(2) Explain the equivalence of the following two circuits by BDD (Binary Decision Diagram)

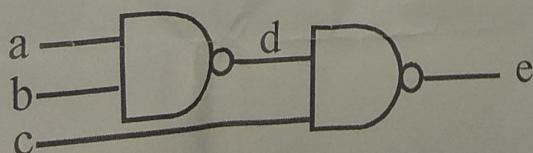


Circuit 1



Circuit 2

(3) Generate CNF from the circuit and obtain the values for a, b, and c which make e to be 1 by a SAT algorithm.



58

(4) Given a software program, discuss the merit and demerit of implementing the software with hardware, such as FPGA. Clarify why FPGA implementation can be faster and more energy efficient. What is the demerit of using FPGA? (around 10-20lines). If possible, use examples to demonstrate your claims.

(5) Compare the merit and demerit between clock gating and power gating. (around 10-20 lines). If possible, use examples to demonstrate your claims.

(6) For the two inputs,  $x$  and  $y$ , we would like to compute  $x^2-y^2$ . Answer the following questions.

(a) Using two of SQUARE functional unit which computes the square of the input and one of ALU which computes either addition or subtraction of the two inputs, design a circuit which computes  $x^2-y^2$ . Here we assume the delay of SQUARE is 8ps and the delay of ALU is 5ps. Try to minimize the total execution time. You have to show the scheduling and its corresponding datapath.

(b) Same as in (a), but assume that we use only one SQUARE and one ALU. Try to minimize the total execution time. You have to show the scheduling and its corresponding datapath.

(c) Using one of MULTIPLIER which computes the multiplication of the two inputs and two of ALU which computes either addition or subtraction of the two inputs, design a circuit which computes  $x^2-y^2$ . Here we assume the delay of MULTIPLIER is 10ps and the delay of ALU is 5ps. Try to minimize the total execution time. You have to show the scheduling and its corresponding datapath.

PDPM-Indian Institute of Information Technology  
 Design and Manufacturing, Jabalpur  
 Machine Learning (CS615 & CS314b)  
 Quiz 2 (11/04/2019)

(51)

Marks: 20

Times: 01 hours

**Q1. [Marks 7.5]** Consider the market basket transactions shown in Table 1

- (a) What is the maximum number of association rules that can be extracted from this data (including rules that have zero support)?
- (b) What is the maximum size of frequent itemsets that can be extracted (assuming  $\text{minsup} > 0$ )?
- (c) Write an expression for the maximum number of size-3 itemsets that can be derived from this data set.
- (d) Find an itemset (of size 2 or larger) that has the largest support.
- (e) Find a pair of items, a and b, such that the rules  $\{a\} \rightarrow \{b\}$  and  $\{b\} \rightarrow \{a\}$  have the same confidence.

**Q2. [Marks 3]** The original association rule mining formulation uses the support and confidence measures to prune uninteresting rules.

- (a) Draw a contingency table for each of the following rules using the transactions shown in Table 2.

Rules:  $\{b\} \rightarrow \{c\}$ ,  $\{a\} \rightarrow \{d\}$ ,  $\{b\} \rightarrow \{d\}$ ,  $\{e\} \rightarrow \{c\}$ ,  $\{c\} \rightarrow \{a\}$ .

- (b) Use the contingency tables in part (a) to compute and rank the rules in decreasing order according to the following measures.

- i. Interest
- ii. IS

**Q3. [Marks 6.5]** Suppose that the data mining task is to cluster points (with  $(x, y)$ ) representing location) into three clusters, where the points are

$A1(2, 10), A2(2, 5), A3(8, 4), B1(5, 8), B2(7, 5), B3(6, 4), C1(1, 2), C2(4, 9)$

The distance function is Euclidean distance. Suppose initially we assign  $A1, B1, C1$  as the center of each cluster, respectively. Use the k-means algorithm to show only

- a. The three cluster centers after the three rounds of execution
- b. The final three clusters

**Q4: [Marks 3]** Define these terms

- a. CF tree and its structure
- b. Radius and Diameter of a cluster
- c. Tradeoff between precision and recall

Table 1

Transaction ID	Items Bought
1	{Milk, Beer, Diapers}
2	{Bread, Butter, Milk}
3	{Milk, Diapers, Cookies}
4	{Bread, Butter, Cookies}
5	{Beer, Cookies, Diapers}
6	{Milk, Diapers, Bread, Butter}
7	{Bread, Butter, Diapers}
8	{Beer, Diapers}
9	{Milk, Diapers, Bread, Butter}
10	{Beer, Cookies}

Milk ->  
 Beer ->  
 Diapers ->  
 Bread ->  
 Butter ->  
 Cookies

Table 2

Transaction ID	Items Bought
1	{a, b, d, e}
2	{b, c, d}
3	{a, b, d, e}
4	{a, c, d, e}
5	{b, c, d, e}
6	{b, d, e}
7	{c, d}
8	{a, b, c}
9	{a, d, e}
10	{b, d}

PDPM-Indian Institute of Information Technology  
Design and Manufacturing, Jabalpur  
Machine Learning (CS615 & CS314b)  
Quiz 1 (29/01/2019)

(52)  
Marks: 20

Times: 01 hours

- Q1. Write down the regularized cost function of linear regression and prove (Marks-8.5)

$$\theta = (X^T X + \lambda I)^{-1} X^T y$$

- Q2. Write down the cost function of Support Vector Machine and explain the role of parameter C with the suitable examples. (Marks-3.0)

- Q3. The sales of a company (in million dollars) for each year are shown in the table below. (Marks-7.5)

x (year)	2005	2006	2007	2008	2009
y (sales)	12	19	29	37	45

- a) Find the least square regression line  $y = a x + b$ .  
b) Use the least squares regression line as a model to estimate the sales of the company in 2012.

- Q4. Find the slope of the line that goes through the points  $(-11, -5)$  and  $(1, -12)$ . (Marks 1.0)

PDPM-Indian Institute of Information Technology Design and Manufacturing,  
Jabalpur

Machine Learning (CS615 & CS314b)  
Mid Term (27/02/2019)

(S3)

Marks: 40

Times: 02 hours

- Q1.** Consider the training examples shown in below Table for a binary (Marks 1) classification problem.

Instance	$a_1$	$a_2$	$a_3$	Target Class
1	T	T	1.0	+
2	T	T	6.0	+
3	T	F	5.0	-
4	F	F	4.0	+
5	F	T	7.0	-
6	F	T	3.0	-
7	F	F	8.0	-
8	T	F	7.0	+
9	F	T	5.0	-

- a. What is the entropy of this collection of training examples with respect to the positive class?
- b. What are the information gains of  $a_1$  and  $a_2$  relative to these training examples?
- c. For  $a_3$ , which is a continuous attribute, compute the information gain for every possible split.
- d. What is the best split (among  $a_1$ ,  $a_2$ , and  $a_3$ ) according to the information gain?
- e. What is the best split (between  $a_1$  and  $a_2$ ) according to the classification error rate?
- f. What is the best split (between  $a_1$  and  $a_2$ ) according to the Gini index?

- Q2.** Consider the data set shown in below Table.

Marks (9)

Record	A	B	C	Class
1	0	0	0	+
2	0	0	1	-
3	0	1	1	-
4	0	1	1	-
5	0	0	1	+
6	1	0	1	+
7	1	0	1	-
8	1	0	1	-
9	1	1	1	+
10	1	0	1	+

(53)

$A=0$   
 $B=1$   
 $C=0$

- a. Estimate the conditional probabilities for  $P(A/+)$ ,  $P(B/+)$ ,  $P(C/+)$ ,  $P(A/-)$ ,  $P(B/-)$ , and  $P(C/-)$
- b. Use the estimate of conditional probabilities given in the previous question to predict the class label for a test sample ( $A = 0, B = 1, C = 0$ ) using the naive Bayes approach.
- c. Estimate the conditional probabilities using the m-estimate approach, with  $p = 1/2$  and  $m = 4$ .
- d. Repeat part (b) using the conditional probabilities given in part (c).
- e. Compare the two methods for estimating probabilities. Which method is better and why?

Q3. Write down the cost function ( $J(\theta)$ ) of logistic regression and prove

(Marks 8)

$$\frac{\partial J(\theta)}{\partial \theta_j} = \frac{1}{m} \sum_{i=1}^m [h_\theta(x^{(i)}) - y^{(i)}] x_j^{(i)}$$

Q4. Explain the following concept using suitable example.

(Marks 6)

- a. Bias and Variance tradeoff
- b. Training data size verses training and test errors
- c. Model complexity verses training and test errors

Q5. Write down the difference between SVM Linear, Polynomial, and RBF kernels? Which kernel generally outperforms than others and why?

(Marks 7)

(34)

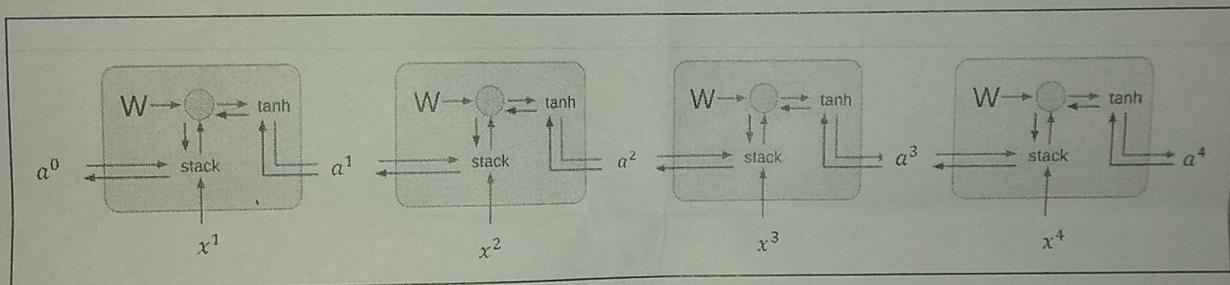
Note: All questions are compulsory.

Time: 40 minutes

Max. Marks: 10  
 Marks

Q.No.

- 1 In YOLO algorithm, a maximum of two objects per grid (cell) are to be detected. The dataset consists of 2 60000 images with 10 class labels divided into sets of 50000 and 10000 for training and testing. For each object, it is planned to have 4 anchor boxes for object detection. What will be the shape of class label vector  $y$  for each input image  $X$ , if class label for an object is represented by a number? Justify your answer by enumerating entries in the label vector. 2
- 2 Are the default boxes of SSD algorithm different from anchor boxes of YOLO algorithm? If yes, illustrate through an example. If no, then what change would you suggest to make the default boxes more useful? 2
- 3 What is the basic difference between next-state computation in a vanilla LSTM model and an attention model? How does this change in the attention model help build a better language model? Explain through an example. 2
- 4 In the following Vanilla RNN, backpropagation is performed as shown throw arrows from  $a^4$  to  $a^0$ . 4



Derive the derivative of loss function  $L$  with respect to  $a^0$ .

56

**PDPM IIIT DM Jabalpur**

CS617: Basics of Deep Learning

Mid Semester Examination: Saturday – February 23, 2019

**Note:** All questions are compulsory. Notations and abbreviations have their usual meanings.

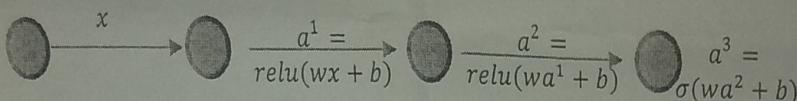
**Time:** 2 hours

**Max. Marks:** 60

**Q.No.**

**Marks**

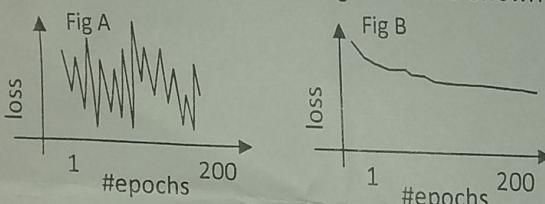
Consider the following network with 2 hidden layers and an output layer for binary classification problem. Each hidden layer contains a single unit and the input layer sends 1-dimensional samples to the network.



- ✓ 1 (a) Find out the expression for derivative of the loss function that would be backpropagated to the input layer. 5

- ✓ 2 (b) If  $x = 1$  and  $w = 0.1, b = 0.4$ . The corresponding label  $y = 1$ , what will be value of the loss? 3

You have specified a minibatch size in the stochastics gradient descent method. You have used two different learning rates  $\alpha_1 = 0.1$  and  $\alpha_2 = 0.01$  for optimization of loss function. Graphs of loss functions for both the learning rates are shown below.



- ✓ 3 (a) Which figure might correspond to  $\alpha_1$  and why? 4  
 (b) What action will you take in case of Fig A and B? Justify your answer. 4

Input volume in a convolution layer is of size  $1024 \times 1024 \times 128$ . You want to apply 256 filters, each of size  $5 \times 5$  with a stride of 1 and padding as 'SAME'. N 4

- (a) How many multiplications will be performed in the convolution layer?  
 (b) Can you devise a different method to reduce the number of multiplications? If yes, what changes will you make in the convolution structure / operations? Justify your answer and compute the total reduction in multiplication operations.

- ✓ 4 (a) Given the following input image to a pooling layer, what type of pooling will you apply to retain the pattern in the image while reducing the size? Compute the output of the pooling layer devised by you. 4

4	4	4	4
4	0	0	4
4	0	0	4
4	4	4	4

- ✓ 4 (b) How does 'VALID' differ from 'SAME' padding? Use a  $3 \times 3$  filter with all entries as '1' to show the change in output of the convolution layer using these two different paddings. 4

- ✓ 5 Write the formula for weight update in gradient descent with momentum, specifying each term used in the expression. 4

6  
56  
What structural changes were made in convolution layers of VGG 6 migrating from VGG 5.  
What was the purpose of changing the structure? Justify your answer using an example.

4

7  
What are the typical applications when you will employ a many-to-one RNN and a one-to-many RNN? Draw the diagram of each type of RNN with flow directions.

4

8  
How does ResNet solve the problem of vanishing gradients using skip \shortcut connections?  
Explain by comparing the backpropagation of cost-gradients of a plain network and a network containing skip \ shortcut connections.

4

9  
Answer each of the following questions in not more than 1 sentence.

(a) Why is it said that Python is portable?

2

(b) What are different backend supports for Keras?

2

(c) How will you add a 2D convolution layer with 32 filters, each of size of  $3 \times 3$ , stride = 1, with 'relu' activation function? Input shape is specified already as input\_shape.

2

(d) What is the difference between model.fit() and model.compile() in Keras?

2

(e) If you have a multiclass classification problem in an image database and you are using a CNN to build the classification model, which type of layer and activation function will you use in the last (output) layer?

2

10  
Is there anything wrong in following code snippets? If yes, identify and write the correct code.

1

(a)

```
import numpy as np
A = np.array([[1, 2, 3, 4],
              [5, 6, 7, 8],
              [9, 1, 2, 3]])
A = A.reshape(3, 2, 3)
```

(b)

```
import numpy as np
a = np.array([[1,1,1],[1,1,1], [1,1,1], [1,1,1]])
b = np.array([2,2,2])
c = a + b
```

1